NETGEAR®

ProSAFE Dual WAN Gigabit SSL VPN Firewall

Model FVS336Gv2

Reference Manual

December 2014
202-10619-03

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*.

Contact your Internet service provider for technical support.

Compliance

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

See the regulatory compliance document before connecting the power supply.

Trademarks

Contents

Chapter 1 Get an Overview of the Features and Hardware and Log In

Chapter 2 Configure the IPv4 Internet and WAN Settings

Chapter 4 Configure the IPv4 LAN Settings

Chapter 5 Configure the IPv6 LAN Settings

Chapter 6 Customize Firewall Protection

Chapter 7 Protect Your Network

Chapter 8 Set Up Virtual Private Networking With IPSec Connections

Chapter 9 Set Up Virtual Private Networking with SSL Connections

Chapter 10 Manage Users, Authentication, and VPN Certificates

Chapter 11 Optimize Performance and Manage Your System

Chapter 12 Monitor System Access and Performance

Appendix C Two-Factor Authentication

Appendix D Default Settings and Technical Specifications

Index

1 Get an Overview of the Features and Hardware and Log In

This chapter provides an overview of the features and capabilities of the NETGEAR ProSAFE® Dual WAN Gigabit SSL VPN Firewall for model FVS336Gv2 and explains how to log in to the device and use its web management interface. The chapter contains the following sections:

- *What Is the ProSAFE Dual WAN Gigabit SSL VPN Firewall?*
- *Key Features and Capabilities*
- *Package Contents*
- *Hardware Features*
- *Choose a Location for the VPN Firewall*
- *Rack-Mount the VPN Firewall with the Mounting Kit*
- *Login Requirements*
- *Log In to the VPN Firewall as an Administrator*
- *Change the Password for the Default Administrator Account*

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

Note: Firmware updates with new features and bug fixes are made available from time to time at *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 ProSAFE Dual WAN Gigabit SSL VPN Firewall?

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

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

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

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

The VPN firewall is a plug-and-play device that you can install and configure in a short time.

Key Features and Capabilities

This section includes the following topics:

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

The VPN firewall provides the following key features and capabilities:

- Two 10/100/1000 Mbps Gigabit Ethernet WAN ports for load balancing and failover protection of your Internet connection, providing increased data rate and increased system reliability

- Built-in four-port 10/100/1000 Mbps Gigabit Ethernet LAN switch for fast data transfer between local network resources and support for up to 200,000 internal or external connections
- Both IPv4 and IPv6 support
- Advanced IPSec VPN and SSL VPN support with support for up to 25 concurrent IPSec VPN tunnels and up to 10 concurrent SSL VPN tunnels
- Bundled with a single-user license of the NETGEAR ProSAFE VPN Client software (VPN01L)
- L2TP tunnel and PPTP tunnel support
- Advanced stateful packet inspection (SPI) firewall with multi-NAT support
- Quality of Service (QoS) and SIP 2.0 support for traffic prioritization, voice, and multimedia
- Extensive protocol support
- One console port for local management
- SNMP support with SNMPv1, SNMPv2c, and SNMPv3, and management optimized for the NETGEAR ProSAFE Network Management Software (NMS200) over a LAN connection
- Front panel LEDs for easy monitoring of status and activity
- Flash memory for firmware upgrade
- Internal universal switching power supply
- Rack-mounting kit for 1U rackmounting

Two WAN Ports for Increased Reliability and Load Balancing

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

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

You can implement the following capabilities with multiple WAN port gateways:

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

For information about planning a network with such capabilities, see *Appendix A, Network Planning for Multiple WAN Ports*.

Advanced VPN Support for Both IPSec and SSL

The VPN firewall supports IPSec and SSL virtual private network (VPN) connections:

- IPSec VPN delivers full network access between a central office and branch offices, or between a central office and telecommuters. Remote access by telecommuters requires the installation of VPN client software on the remote computer.
  - IPSec VPN with broad protocol support for a secure connection to other IPSec gateways and clients.
  - Up to 25 simultaneous IPSec VPN connections.
  - Bundled with a 30-day trial license for the ProSAFE VPN Client software (VPN01L).
- SSL VPN provides remote access for mobile users to selected corporate resources without requiring a preinstalled VPN client on their computers.
  - Uses the familiar Secure Sockets Layer (SSL) protocol, commonly used for e-commerce transactions, to provide client-free access with customizable user portals and support for a wide variety of user repositories.
  - Up to 10 simultaneous SSL VPN connections.
  - Allows browser-based, platform-independent remote access through a number of popular browsers, such as Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari.
  - Provides granular access to corporate resources based on user type or group membership.

A Powerful, True Firewall with Content Filtering

Unlike simple NAT routers, the VPN firewall is a true firewall, using stateful packet inspection (SPI) to defend against hacker attacks. Its firewall features have the following capabilities:

- **DoS protection**. Automatically detects and thwarts denial of service (DoS) attacks such as Ping of Death and SYN flood.
- **Secure firewall**. Blocks unwanted traffic from the Internet to your LAN.
- **Content filtering**. Prevents objectionable content from reaching your computers. You can control access to Internet content by screening for web services, web addresses, and keywords within web addresses.
- **Schedule policies**. Permits scheduling of firewall policies by day and time.
- **Logs security incidents**. Logs security events such as logins and secure logins. You can configure the firewall to email the log to you at specified intervals. You can also configure the VPN firewall to send immediate alert messages to your email address or email pager when a significant event occurs.

Security Features

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

- **Computers hidden by NAT**. NAT opens a temporary path to the Internet for requests originating from the local network. Requests originating from outside the LAN are discarded, preventing users outside the LAN from finding and directly accessing the computers on the LAN.
- **Port forwarding with NAT**. Although NAT prevents Internet locations from directly accessing the computers on the LAN, the VPN firewall allows you to direct incoming traffic to specific computers based on the service port number of the incoming request.
- **DMZ port**. Incoming traffic from the Internet is usually discarded by the VPN firewall unless the traffic is a response to one of your local computers or a service for which you configured an inbound rule. Instead of discarding this traffic, you can use the dedicated demilitarized zone (DMZ) port to forward the traffic to one computer on your network.

Autosensing Ethernet Connections with Auto Uplink

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

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

Extensive Protocol Support

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

- **IP address sharing by NAT**. The VPN firewall allows many networked computers to share an Internet account using only a single IP address, which might be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as Network Address Translation (NAT), allows the use of an inexpensive single-user ISP account.
- **Automatic configuration of attached computers by DHCP**. The VPN firewall dynamically assigns network configuration information, including IP, gateway, and Domain Name Server (DNS) addresses, to attached computers on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of computers on your local network.
- **DNS proxy**. When DHCP is enabled and no DNS addresses are specified, the VPN firewall provides its own address as a DNS server to the attached computers. The firewall

obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.

- **PPP over Ethernet (PPPoE)**. PPPoE is a protocol for connecting remote hosts to the Internet over a DSL connection by simulating a dial-up connection.
- **Quality of Service (QoS)**. The VPN firewall supports QoS, including traffic prioritization and traffic classification with Type of Service (ToS) and Differentiated Services Code Point (DSCP) marking.
- **Layer 2 Tunneling Protocol (L2TP)**. A tunneling protocol that is used to support virtual private networks (VPNs).
- **Point to Point Tunneling Protocol (PPTP)**. Another tunneling protocol that is used to support VPNs.

Easy Installation and Management

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

- **Browser-based management**. Browser-based configuration allows you to easily configure the VPN firewall from almost any type of operating system, such as Windows, Macintosh, or Linux. Online help documentation is built into the browser-based web management interface.
- **Auto-detection of ISP**. The VPN firewall automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- **IPSec VPN Wizard**. The VPN firewall includes the NETGEAR IPSec VPN Wizard so 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 technical support is available at *support.netgear.com*.

Package Contents

The VPN firewall product package contains the following items:

- Dual WAN Gigabit SSL VPN Firewall
- One AC power cable
- One Category 5 (Cat 5) Ethernet cable
- One rack-mounting kit
- *ProSAFE Dual WAN Gigabit SSL VPN Firewall FVS336Gv2 Installation Guide*
- Resource CD, including the following:
  - Application notes and other helpful information
  - ProSAFE VPN Client software (VPN01L)

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

Hardware Features

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

- *Front Panel*
- *Back 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**. Four switched N-way automatic speed negotiating, Auto MDI/MDIX, Gigabit Ethernet ports with RJ-45 connectors
- **WAN Ethernet ports**. Two independent N-way automatic speed negotiating, Auto MDI/MDIX, Gigabit Ethernet ports with RJ-45 connectors

The front panel also contains three groups of status LEDs, including Power and Test LEDs, LAN LEDs, and WAN LEDs, all of which are described in the following table.

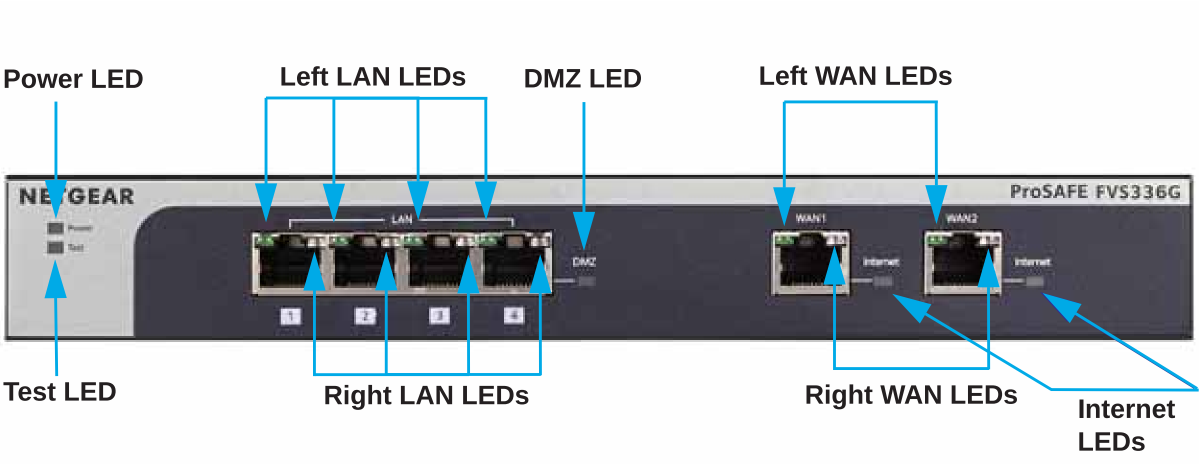


Figure 1. Front panel

Table 1. LED descriptions

LED	Activity	Description
Power	Green	Power is supplied to the VPN firewall.
	Off	Power is not supplied to the VPN firewall.
Test	Amber during startup	Test mode. The VPN firewall is initializing. After approximately two minutes, when the VPN firewall has completed its initialization, the Test LED turns off.
	Amber during any other time	The initialization failed or a hardware failure occurred.
	Blinking amber	The VPN firewall is writing to flash memory during a firmware upgrade or when you reset the VPN firewall to defaults.
	Off	The VPN firewall has booted successfully.
LAN Ports		
Left LED	Green	The LAN port detects a link with a connected Ethernet device.
	Blinking green	The LAN port receives or transmits data.
	Off	The LAN port has no link.
Right LED	Green	The LAN port operates at 1000 Mbps.
	Amber	The LAN port operates at 100 Mbps.
	Off	The LAN port operates at 10 Mbps.
DMZ LED	Green	LAN port 4 operates as a dedicated hardware DMZ port.
	Off	LAN port 4 operates as a normal LAN port.

Table 1. LED descriptions (continued)

LED	Activity	Description
WAN Ports		
Left LED	Green	The WAN port has a valid connection with a device that provides an Internet connection.
	Blinking green	The WAN port receives or transmits data.
	Off	The WAN port has no physical link, that is, no Ethernet cable is plugged into the VPN firewall.
Right LED	Green	The WAN port operates at 1000 Mbps.
	Amber	The WAN port operates at 100 Mbps.
	Off	The WAN port operates at 10 Mbps.
Internet LED	Green	The WAN port has a valid Internet connection.
	Amber	The Internet link is down because the WAN port is in standby mode for failover. Also, before the connection is up, there is an amber color for a short period of time.
	Off	The WAN port is either not enabled or has no link to the Internet.

Back Panel

The back panel of the VPN firewall includes a console port, a cable security lock receptacle, a recessed Factory Defaults reset button, and an AC power connection.

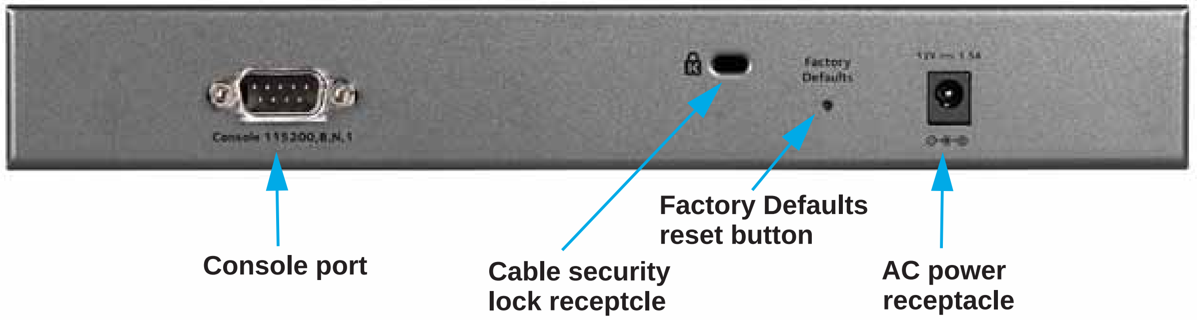


Figure 2. Back panel

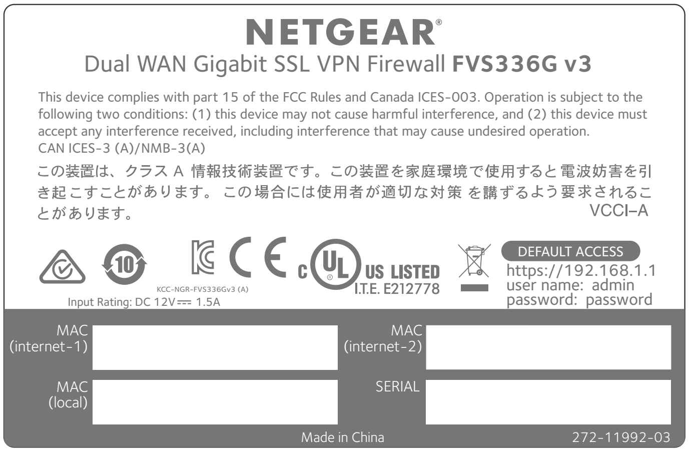
Viewed from left to right, the back panel contains the following components:

- **Console port.** Port for connecting to an optional console terminal. The port has a DB9 male connector. The default baud rate is 115200 K. The pinouts are (2) Tx, (3) Rx, (5) and (7) Gnd. For information about accessing the command-line interface (CLI) using the console port, see *Use the Command-Line Interface* on page 537.
- **Cable security lock receptacle**.

- **Factory Defaults reset button**. To reset the VPN firewall to factory default settings, use a sharp object to press and hold this button for about eight seconds until the front panel Test LED blinks. All configuration settings are lost and the default password is restored.
- **AC power receptacle**. (12V, 1.5A).

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®

Dual WAN Gigabit SSL VPN Firewall **FVS336G v3**

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)

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。 この場合には使用者が適切な対策 を講ずるよう要求されることがあります。
VCCI–A

KCC-NGR-FVS336Gv3 (A)

Input Rating: DC 12V ⎓ 1.5A

US LISTED
I.T.E. E212778

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

MAC (internet-1)

MAC (internet-2)

MAC (local)

SERIAL

Made in China

272-11992-03

Figure 3. Product label on the bottom panel

Choose a Location for the VPN Firewall

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

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

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

Rack-Mount the VPN Firewall with the Mounting Kit

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

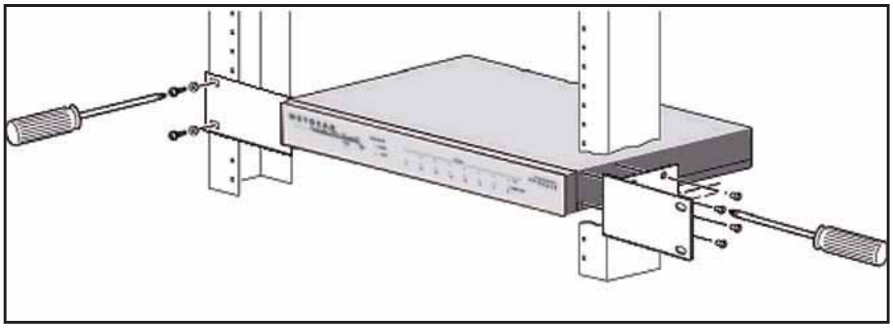


Figure 4. Rack-mounting

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

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

Login Requirements

Before you can log in to VPN firewall, install the VPN firewall in your network by connecting the cables and restarting your network according to the instructions in the *ProSAFE Dual WAN Gigabit SSL VPN Firewall FVS336Gv2 Installation Guide*. You can download a PDF of this guide from *downloadcenter.netgear.com*.

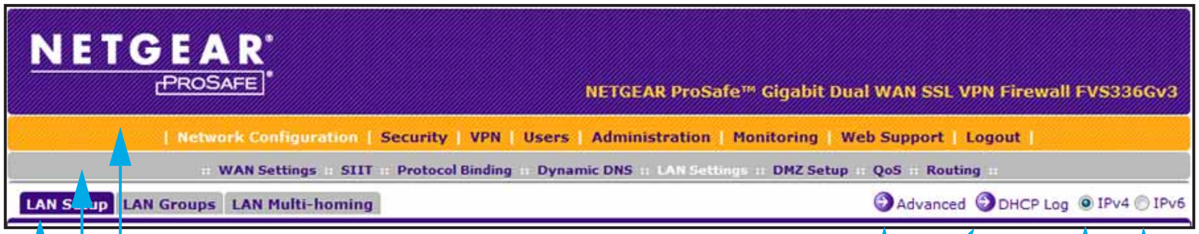
Browser Requirements

To connect to and configure the VPN firewall, you must use the latest version of a web browser such as Google Chrome, Microsoft Internet Explorer, Mozilla Firefox, or Apple Safari with JavaScript, cookies, and SSL enabled.

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

Web Management Interface Overview

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


NETGEAR
PROSAFE
NETGEAR ProSafe™ Gigabit Dual WAN SSL VPN Firewall FVS336Gv3
| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
LAN Setup
LAN Groups
LAN Multi-homing
Advanced
DHCP Log
◉ IPv4 ○ IPv6

First Level: Main navigation menu link (orange)

Second level: Configuration menu link (gray)

Third level: Submenu tab (blue)

Option arrows:
Additional screen for submenu item

IP radio buttons

Figure 5. Screen menus, option arrows, and buttons

The web management interface menu consists of the following levels and components:

- **First 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.
- **Second 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.
- **Third level: Submenu tabs**. Each configuration menu item has one or more submenu tabs that are listed below the gray menu bar. When you select a submenu tab, the text is displayed in white against a blue background.
- **Option arrows**. On the right side of a screen, a white arrow in a blue circle precedes a link in blue letters against a white background. This link provides access to additional screens for a submenu item.
- **IP radio buttons**. The **IPv4** and **IPv6** radio buttons let you select the IP version for the feature to be configured onscreen. Four situations can occur:
  - **Both radio buttons are operational**. ◉ IPv4 ○ IPv6 You can configure the feature onscreen for IPv4 functionality or for IPv6 functionality. After you have correctly configured the feature for both IP versions, the feature can function with both IP versions simultaneously.
  - **The IPv4 radio button is operational but the IPv6 radio button is disabled**. ◉ IPv4 ○ IPv6 You can configure the feature onscreen for IPv4 functionality only.
  - **The IPv6 radio button is operational but the IPv4 radio button is disabled**. ○ IPv4 ◉ IPv6 You can configure the feature onscreen for IPv6 functionality only.

- **Both radio buttons are disabled**. ◉ IPv4 ○ IPv6 IP functionality does not apply.

The bottom of each screen provides action buttons. The nature of a screen determines which action buttons are shown.

Most screens and sections of screens provide an accompanying help screen. To open the help screen, click the ? icon.

All screens that you can access from the SSL VPN menu of the web management interface display a user portal link in the upper right, above the menu bars (User Portal).

When you click the **User Portal** link, the SSL VPN default portal opens. This user portal is not the same as a custom SSL portal login screen that you can build with the SSL VPN Wizard (see *Build an SSL Portal Using the SSL VPN Wizard* on page 427) or manually (see *Manually Set Up or Change an SSL Portal* on page 446).

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 Requirements

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 Requirements

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

For information about restricted IPv6 address, visit the following Internet Assigned Numbers Authority (IANA) web page: *http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml*.

Log In to the VPN Firewall as an Administrator

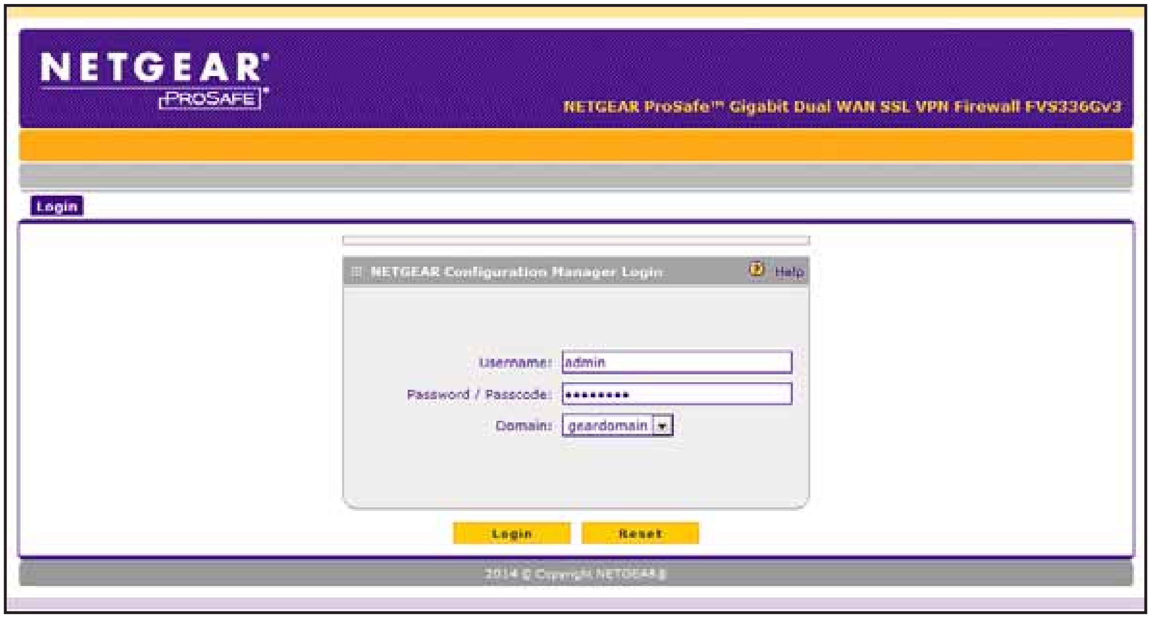
For you to be able to configure the VPN firewall, you must log in initially as an administrator (admin).

- **To log in to the VPN firewall:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.


NETGEAR
PROSAFE
NETGEAR ProSafe™ Gigabit Dual WAN SSL VPN Firewall FVS336Gv3
Login
NETGEAR Configuration Manager Login
Help
Login
Reset
2014 © Copyright NETGEAR®

Username: admin

Password / Passcode: ••••••••••

Domain: geardomain

   If you connect remotely to the VPN firewall with a browser through an SSL connection for the first time, you might get a message about the SSL certificate.

3. If you get a message about the SSL certificate, follow the directions of your browser to accept the SSL certificate.
4. In the **Username** field, type **admin**.

   Use lowercase letters.

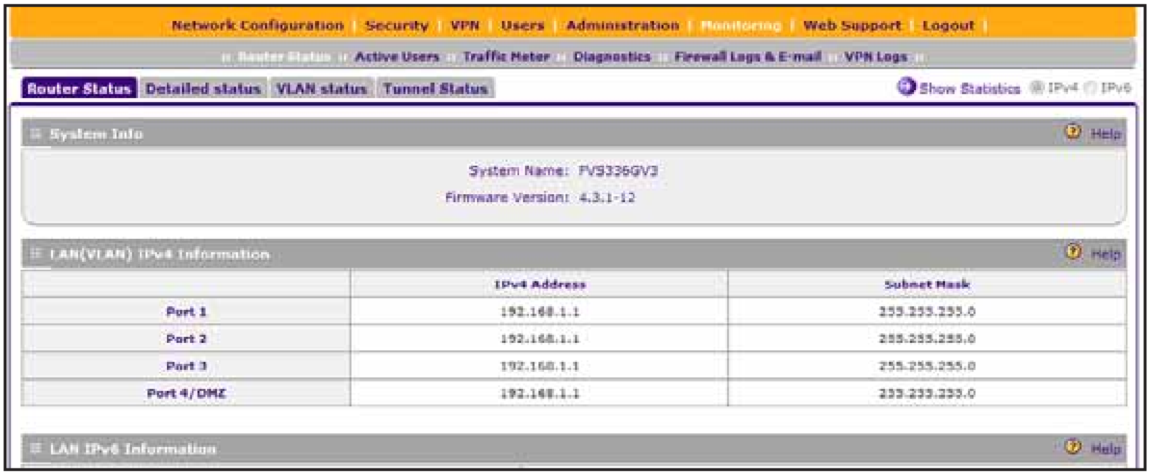
5. In the **Password / Passcode** field, type **password**.

   Use lowercase letters.

   Note: In the **Domain** menu, leave the domain at **geardomain**.

6. Click the **Login** button.

   The web management interface displays, showing the Router Status screen. The following figure shows the top part of the Router Status screen. For more information, see *View the System Status* on page 582.


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: FVS336GV3

Firmware Version: 4.3.1-12

LAN(VLAN) IPv4 Information

	IPv4 Address	Subnet Mask
Port 1	192.168.1.1	255.255.255.0
Port 2	192.168.1.1	255.255.255.0
Port 3	192.168.1.1	255.255.255.0
Port 4/DMZ	192.168.1.1	255.255.255.0

LAN IPv6 Information

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

You are now ready to configure the VPN firewall for your specific network environment. However, NETGEAR recommends that you first change the password for the default administrator account to a secure password.

Change the Password for the Default Administrator Account

The most secure password does not contain dictionary words from any language and is a mixture of letters (both uppercase and lowercase), numbers, and selected special characters. The password can be up to 32 characters in length. However, the password cannot contain a space nor any of the following special characters:

```
` ~ ! # $ & * ( ) - + | \ ; : ' " < >
```

➢ **To modify the password for the default administrator account from default settings to secure settings:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

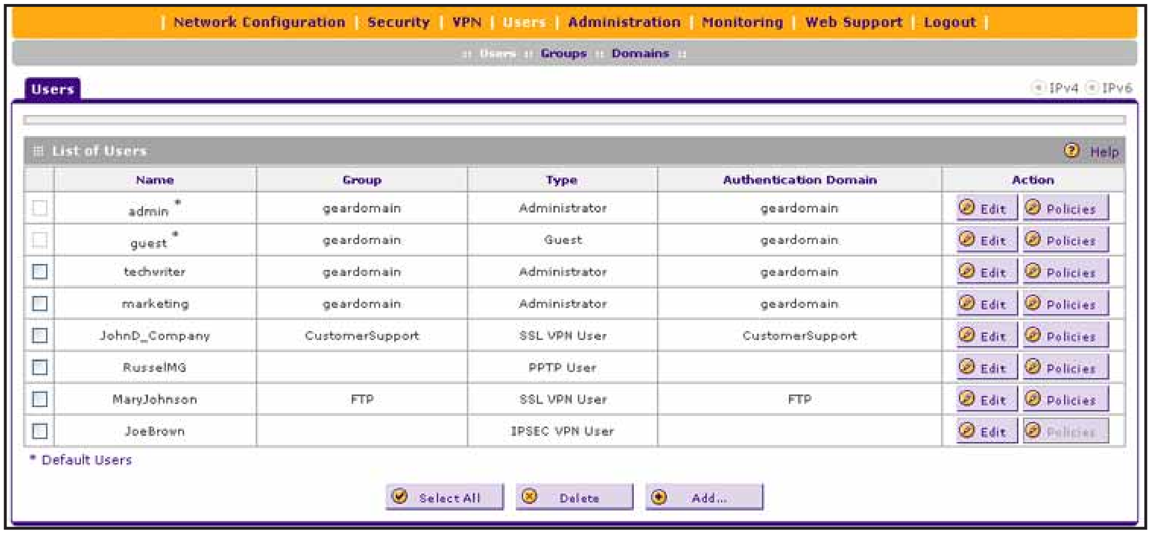
   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type **admin**.
4. In the **Password / Passcode** field, type **password**.
5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Users > Users**.

   The Users screen displays.

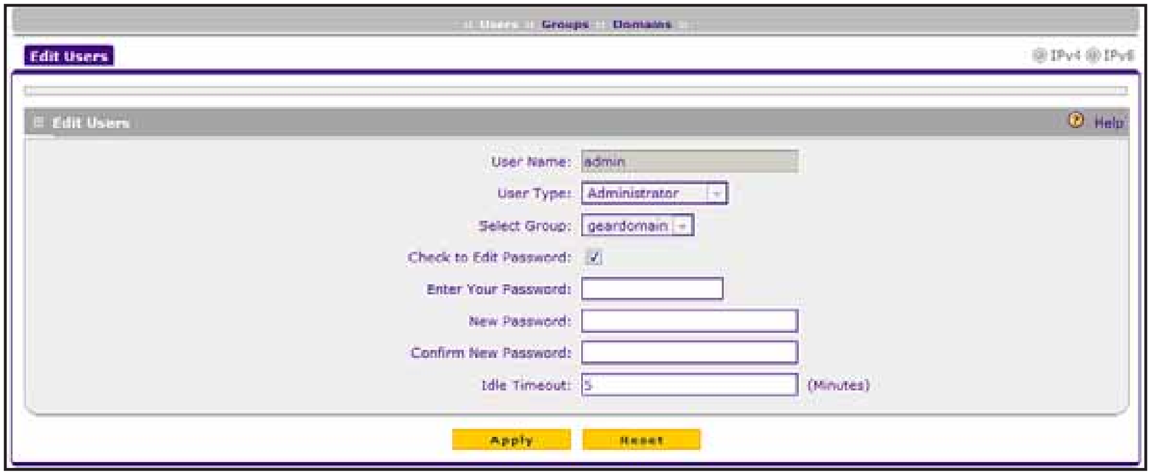

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Users :: Groups :: Domains ::
Users
○ IPv4 ○ IPv6
List of Users
Help
Select All
Delete
Add...

	Name	Group	Type	Authentication Domain	Action
□	admin *	geardomain	Administrator	geardomain	Edit Policies
□	guest *	geardomain	Guest	geardomain	Edit Policies
□	techwriter	geardomain	Administrator	geardomain	Edit Policies
□	marketing	geardomain	Administrator	geardomain	Edit Policies
□	JohnD_Company	CustomerSupport	SSL VPN User	CustomerSupport	Edit Policies
□	RusselMG		PPTP User		Edit Policies
□	MaryJohnson	FTP	SSL VPN User	FTP	Edit Policies
□	JoeBrown		IPSEC VPN User		Edit Policies

* Default Users

7. In the List of Users table, click the **Edit** button for the **admin** default user.

   The Edit Users screen displays.



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)

8. Select the **Check to Edit Password** check box.
9. Configure a new password:
   - In the **Enter Your Password** field, type **admin**.
   - In the **New Password** field, type a new and secure password.
   - In the **Confirm New Password** field, repeat the new password.
10. Click the **Apply** button.

    Your settings are saved.

2. Configure the IPv4 Internet and WAN Settings

2

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

Roadmap to Setting Up IPv4 Internet Connections to Your ISPs

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

The tasks that are required to complete the Internet connection of your VPN firewall depend on whether you use an IPv4 connection, an IPv6 connection, or both to your Internet service provider (ISP). For information about setting up an IPv6 connection, see *Chapter 3, Configure the IPv6 Internet and WAN Settings*.

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

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

➢ **Complete these tasks:**

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

   This task is described in *Manage the IPv4 WAN Routing Mode* on page 30.

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

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

   - *Let the VPN Firewall Automatically Detect and Configure an IPv4 Internet Connection* on page 32
   - *Manually Configure a Static IPv4 Internet Connection* on page 36
   - *Manually Configure a PPPoE IPv4 Internet Connection* on page 39
   - *Manually Configure a PPTP IPv4 Internet Connection* on page 44

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

   This task is described in *Configure Load Balancing or Auto-Rollover for IPv4 Interfaces* on page 48.

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

   This task is described in *Manage Secondary IPv4 WAN Addresses* on page 59.

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

This task is described in *Manage Dynamic DNS Connections* on page 63.

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

   These tasks are described in *Managing Advanced WAN Options* on page 66.

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

   This task is described in *Configure and Enable the WAN IPv4 Traffic Meter* on page 558.

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 (see *Manage the IPv4 WAN Routing Mode*) and then configure the IPv4 Internet connection to your ISP on the WAN ports.

The following sections provide information about configuring the IPv4 Internet connection and WAN settings:

- *Manage the IPv4 WAN Routing Mode*
- *Let the VPN Firewall Automatically Detect and Configure an IPv4 Internet Connection*
- *Manually Configure a Static IPv4 Internet Connection*
- *Manually Configure a PPPoE IPv4 Internet Connection*
- *Manually Configure a PPTP IPv4 Internet Connection*

Manage the IPv4 WAN Routing Mode

By default, IPv4 is supported and functions in NAT mode but can also function in classical routing mode. IPv4 functions the same way in IPv4-only mode that it does in IPv4/IPv6 mode. The latter mode adds IPv6 functionality (see *Manage the IPv6 Routing Mode* on page 88).

The following sections provide information about managing the IPv4 routing mode:

- *Network Address Translation Overview*
- *Classical Routing*
- *Change the IPv4 WAN Routing Mode*

Network Address Translation Overview

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 have only a single public Internet IP address, you must use NAT (the default setting).
- If your ISP has provided you with multiple public IP addresses, you can use one address as the primary shared address for Internet access by your 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 have a valid static Internet IP address.

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

Change the IPv4 WAN Routing Mode

The following procedure describes how to change the IPv4 routing mode. By default, the VPN firewall functions in NAT mode.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

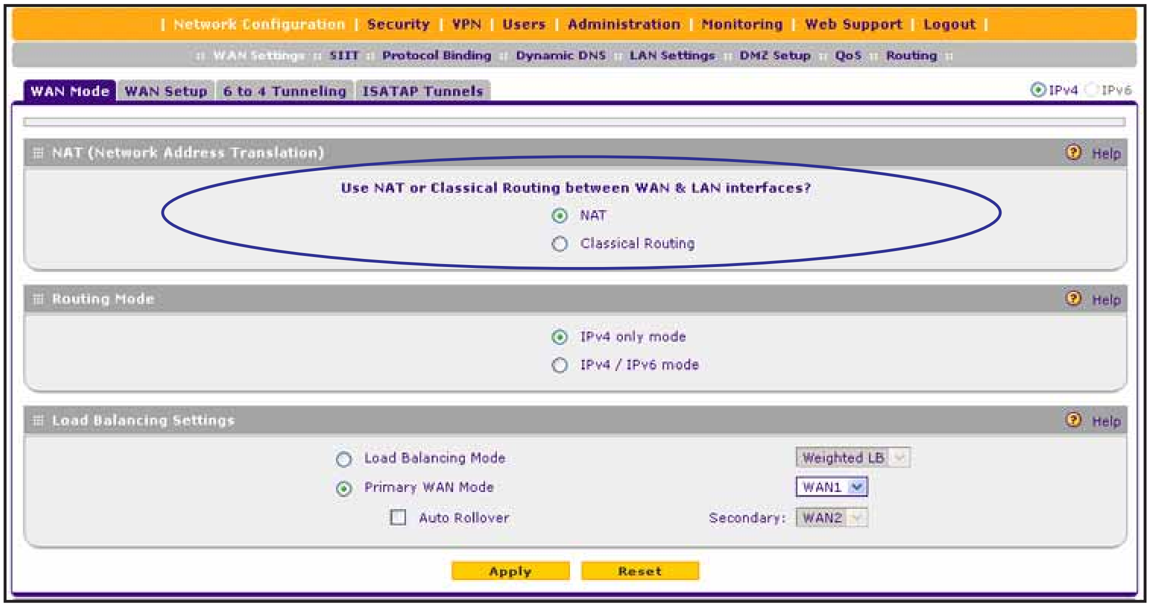
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > WAN Settings > WAN Mode**.

   The WAN Mode screen displays.


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

Load Balancing Settings

○ Load Balancing Mode Weighted LB

● Primary WAN Mode WAN1

□ Auto Rollover Secondary: WAN2

7. In the NAT (Network Address Translation) section, 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.

8. Click the **Apply** button.

   Your settings are saved. The settings apply to all WAN ports.

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

The following procedure describes how you can let your ISP automatically configure the IPv4 WAN addresses of the VPN firewall through a DHCP server.

If your ISP does not support automatic configuration through a DHCP server, you must obtain configuration parameters from your ISP to be able to establish an Internet connection manually. For information about manually configuring the IPv4 WAN addresses, see the following sections:

- *Manually Configure a Static IPv4 Internet Connection*
- *Manually Configure a PPPoE IPv4 Internet Connection*
- *Manually Configure a PPTP IPv4 Internet Connection*

Note: If your ISP requires MAC authentication and another MAC address was previously registered with your ISP, you must configure that MAC address on the VPN firewall (see *Change the Advertised MAC Address of the VPN Firewall* on page 70) before you begin the following procedure.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

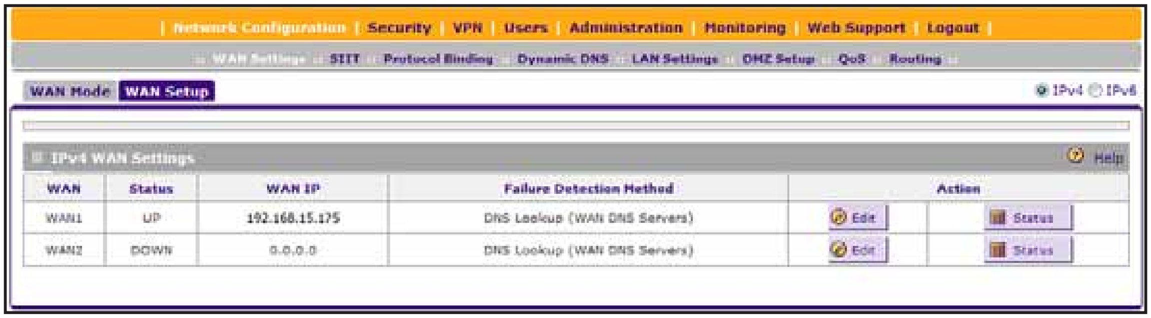
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > WAN Settings > WAN Setup**.

   The WAN Setup screen displays the IPv4 settings.


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

IPv4 WAN Settings

WAN	Status	WAN IP	Failure Detection Method	Action	
WAN1	UP	192.168.15.175	DNS Lookup (WAN DNS Servers)	Edit	Status
WAN2	DOWN	0.0.0.0	DNS Lookup (WAN DNS Servers)	Edit	Status

   The IPv4 WAN Settings table displays the following fields:

   - **WAN**. The WAN interface (WAN1 or WAN2).
   - **Status**. The status of the WAN interface (UP or DOWN).
   - **WAN IP**. The IPv4 address of the WAN interface.

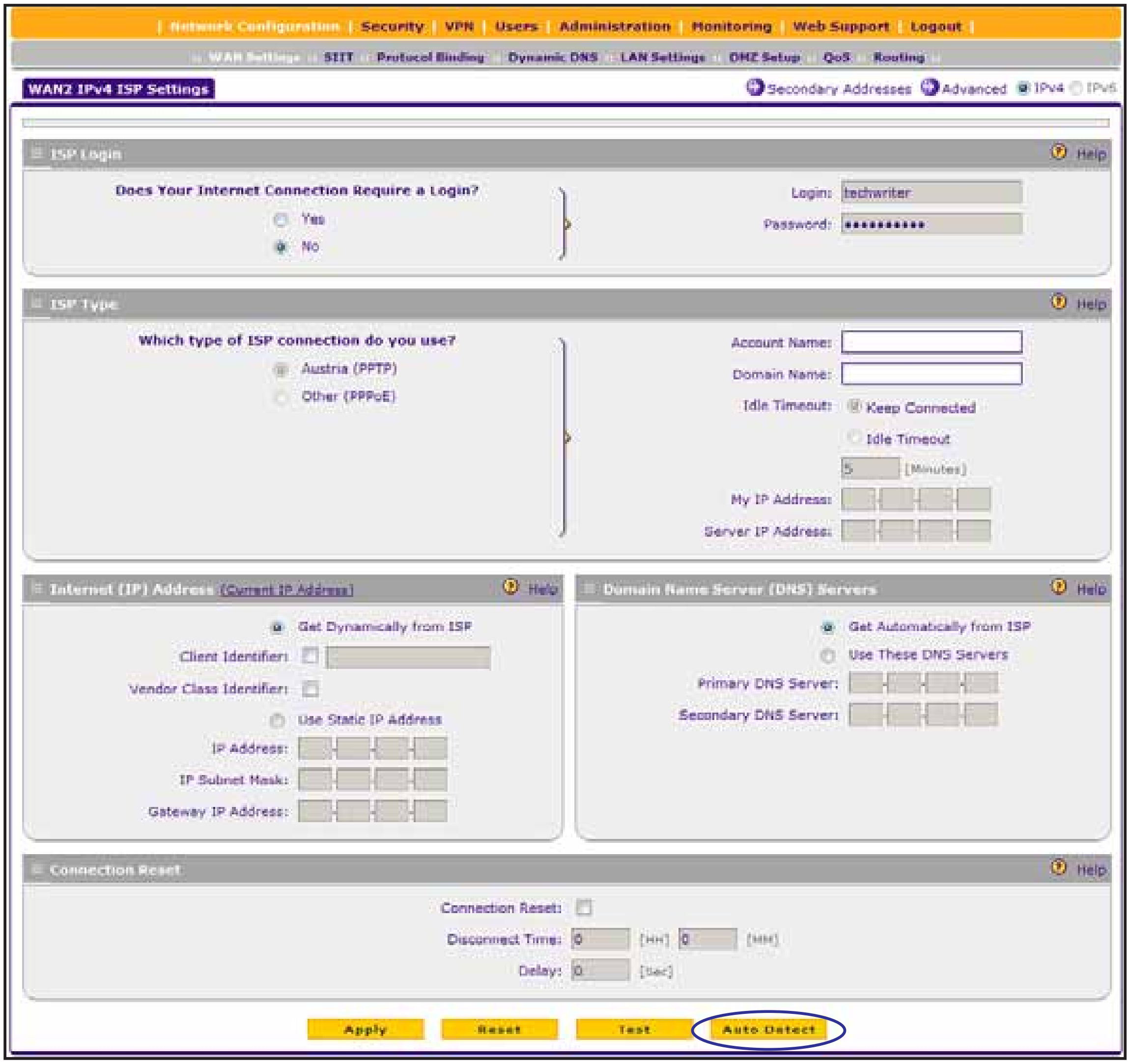
- **Failure Detection Method**. The failure detection method that is active for the WAN interface (see *Configure the Auto-Rollover Mode and Failure Detection Method for IPv4 Interfaces* on page 56).

  Any of the following methods can be displayed: None, DNS Lookup (WAN DNS Servers), DNS Lookup (the configured IP address is displayed), or PING (the configured IP address is displayed).

- **Action**. The **Edit** button provides access to the WAN IPv4 ISP Settings screen (see *Step 7*) for the corresponding WAN interface; the **Status** button provides access to the Connection Status screen (see *Step 9*) for the corresponding WAN interface.

7. In the IPv4 WAN Settings table, click the **Edit** button for the WAN interface for which you want to let the VPN firewall automatically configure the connection to the Internet.

   The WAN IPv4 ISP Settings screen displays. The following figure shows the WAN2 IPv4 ISP Settings screen as an example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
Secondary Addresses
Advanced
Help
Apply
Reset
Test
Auto Detect

WAN2 IPv4 ISP Settings

● IPv4 ○ IPv6

ISP Login

Does Your Internet Connection Require a Login?

○ Yes
● No

Login: techwriter
Password: ●●●●●●●●●●●

ISP Type

Which type of ISP connection do you use?

● Austria (PPTP)
○ Other (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)

8. Click the **Auto Detect** button.

   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 dynamic DHCP, PPPoE, or PPTP connection that requires input from you, it prompts you for the information. With auto detection, it can detect if it is a static line. Then the user needs to enter a static IP address.

     The following table lists the settings that you might have to enter:

Connection Method	Data You Might Have to Enter Manually
Dynamic DHCP	• **Client Identifier**. If your ISP requires client identifier information to assign an IP address using DHCP, select the **Client Identifier** check box and enter the client identifier information in the field. • **Vendor Class Identifier**. If your ISP requires the vendor class identifier information to assign an IP address using DHCP, select the **Vendor Class Identifier** check box.
PPPoE	• **Login** • **Password** • **Account Name** • **Domain Name**
PPTP	• **Login** • **Password** • **Account Name** • **Domain Name** • **My IP Address** • **Server IP Address**

   - 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 (see *Managing Advanced WAN Options* on page 66).

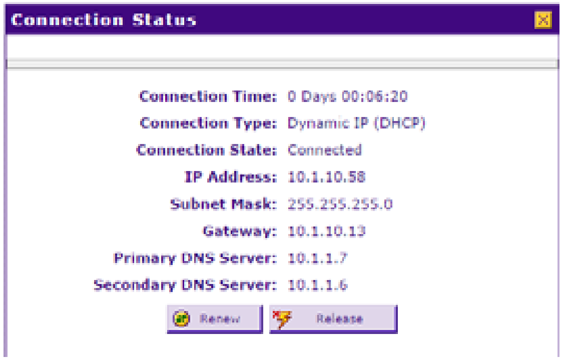
9. Verify the connection:

   a. Select **Network Configuration > WAN Settings > WAN Setup**.

      The WAN Setup screen displays the IPv4 settings (see the figure that is shown in *Step 6*).

   b. In the IPv4 WAN Settings table, click the **Status** button for the WAN interface for which you want to display the connection status.

      The Connection Status pop-up screen displays. The following figure shows a static IP address configuration.



Connection Status

Connection Time: 0 Days 00:06:20
Connection Type: Dynamic IP (DHCP)
Connection State: Connected
IP Address: 10.1.10.58
Subnet Mask: 255.255.255.0
Gateway: 10.1.10.13
Primary DNS Server: 10.1.1.7
Secondary DNS Server: 10.1.1.6

The Connection Status screen shows a valid IP address and gateway. You are connected to the Internet. For more information about the connection status, see *View the WAN Port Status and Terminate or Establish the Internet Connection* on page 594.

If the configuration was not successful, try to manually configure the connection. For more information, see the following sections:

- *Manually Configure a Static IPv4 Internet Connection* on page 36
- *Manually Configure a PPPoE IPv4 Internet Connection* on page 39
- *Manually Configure a PPTP IPv4 Internet Connection* on page 44

Manually Configure a Static IPv4 Internet Connection

To configure a static IPv4 Internet connection, enter the IPv4 address information that your IPv4 ISP gave you. If you do not have this information, contact your IPv4 ISP. For each WAN interface, you need the following information: IP address, IP subnet mask, and IP addresses of the gateway, primary DNS server, and secondary DNS server.

Note: If your ISP requires MAC authentication and another MAC address was previously registered with your ISP, you must configure that MAC address on the VPN firewall (see *Change the Advertised MAC Address of the VPN Firewall*) before you begin the following procedure.

➢ **To manually configure and verify a static IPv4 Internet connection for a WAN interface:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

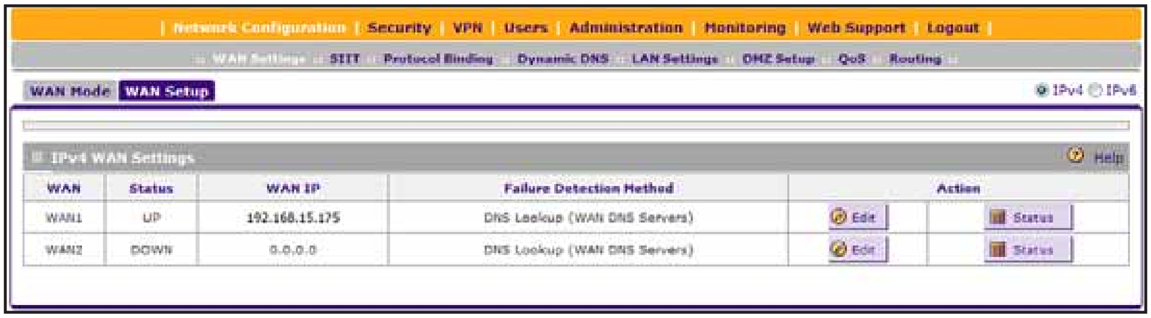
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > WAN Settings > WAN Setup**.

   The WAN Setup screen displays the IPv4 settings.


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

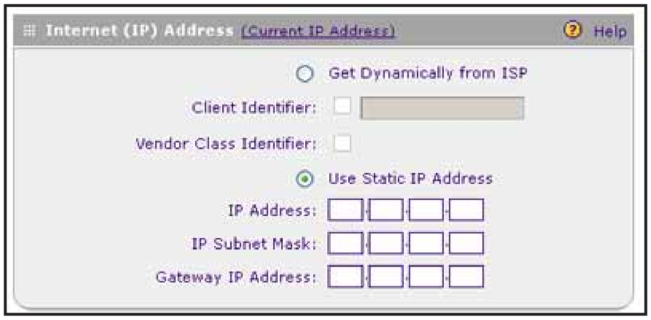
IPv4 WAN Settings

WAN	Status	WAN IP	Failure Detection Method	Action	
WAN1	UP	192.168.15.175	DNS Lookup (WAN DNS Servers)	Edit	Status
WAN2	DOWN	0.0.0.0	DNS Lookup (WAN DNS Servers)	Edit	Status

7. In the IPv4 WAN Settings table, click the **Edit** button for the WAN interface that you want to configure.

   The WAN IPv4 ISP Settings screen displays.

8. In the Internet (IP) Address section, select the **Use Static IP Address** radio button.



○ Get Dynamically from ISP

Client Identifier: □

Vendor Class Identifier: □

● Use Static IP Address

IP Address:

IP Subnet Mask:

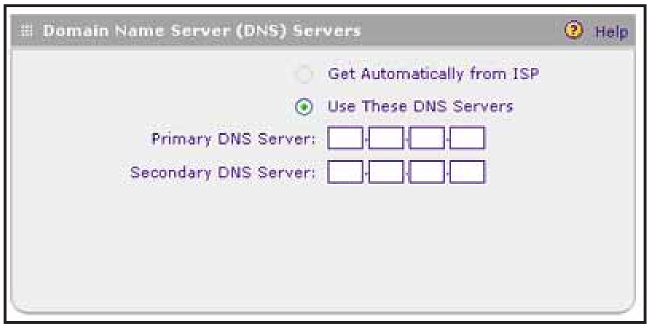
Gateway IP Address:

9. Configure the IP address settings as described in the following table.

Setting	Description
IP Address	The static IP address assigned to you. This address identifies the VPN firewall to your ISP.

Setting	Description
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.

10. Locate the Domain Name Server (DNS) Servers section.



Domain Name Server (DNS) Servers

○ Get Automatically from ISP

● Use These DNS Servers

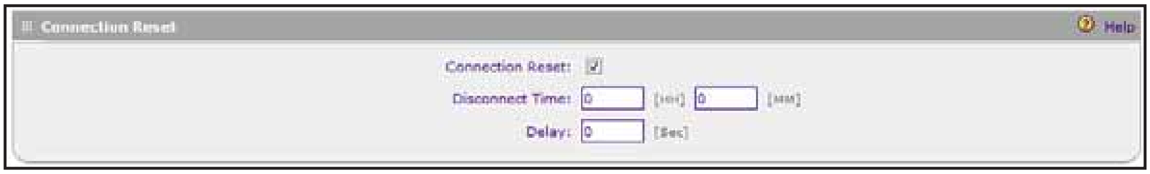
Primary DNS Server: [ ].[ ].[ ].[ ]

Secondary DNS Server: [ ].[ ].[ ].[ ]

> **Note:** When you selected the **Use Static IP Address** radio button in *Step 8*, the **Use These DNS Servers** radio button was selected automatically.

11. Specify the DNS server addresses:
    - **Primary DNS Server**. The IP address of the primary DNS server.
    - **Secondary DNS Server**. The IP address of the secondary DNS server.

12. Locate the Connection Reset section.



Connection Reset

Connection Reset: ☑

Disconnect Time: 0 [HH] 0 [MM]

Delay: 0 [Sec]

13. To configure an automatic connection reset, specify the settings as described in the following table.

Setting	Description
Select the **Connection Reset** check box to specify a time when the 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 must be disconnected.
Delay	Specify the period in seconds after which the connection must be reestablished.

14. Click the **Apply** button.

    Your settings are saved.

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

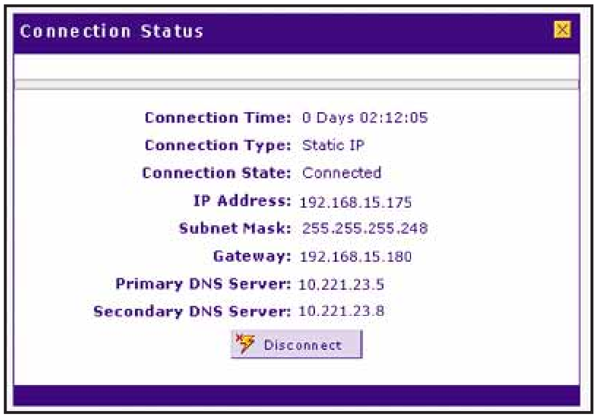
The VPN firewall attempts to make a connection according to the settings that you entered.

16. Verify the connection:
    a. Select **Network Configuration > WAN Settings > WAN Setup**.

       The WAN Setup screen displays the IPv4 settings.

    b. In the IPv4 WAN Settings table, click the **Status** button for the WAN interface for which you want to display the connection status.

       The Connection Status pop-up screen displays.



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. You are connected to the Internet.

Note: If the configuration was not successful, see *Troubleshoot the ISP Connection* on page 615.

Manually Configure a PPPoE IPv4 Internet Connection

If you installed login software, your connection type is most likely PPPoE. To configure a PPPoE IPv4 Internet connection, enter the PPPoE IPv4 information that your IPv4 ISP gave you. If you do not have this information, contact your IPv4 ISP.

For each WAN interface, you need the following information: login name, login password, and if applicable, account name and domain name. If your ISP assigns you a static IP address, you also need the IP address, IP subnet mask, and IP addresses of the primary DNS server and secondary DNS server.

Note: If your ISP requires MAC authentication and another MAC address was previously registered with your ISP, you must configure that MAC address on the VPN firewall (see *Change the Advertised MAC Address of the VPN Firewall* on page 70) before you begin the following procedure.

➢ **To manually configure and verify a PPPoE IPv4 Internet connection for a WAN interface:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

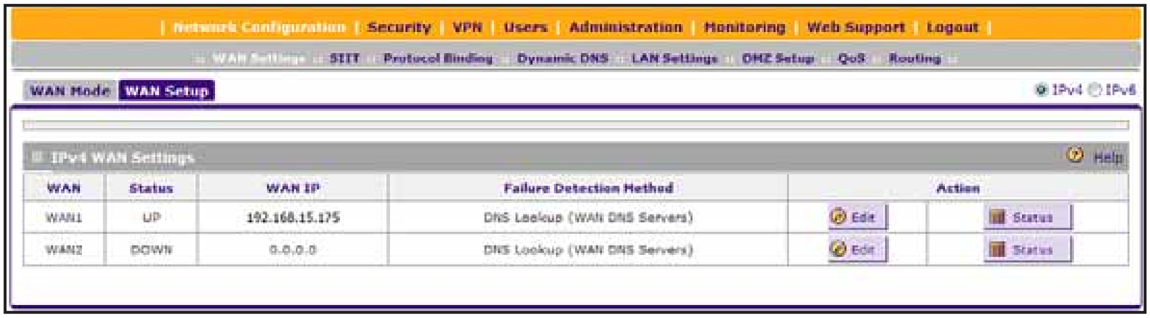
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > WAN Settings > WAN Setup**.

   The WAN Setup screen displays the IPv4 settings.

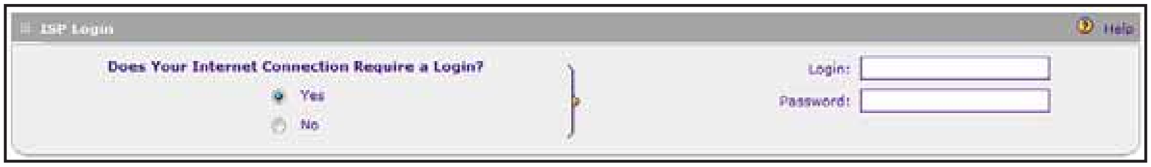

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
WAN Mode
WAN Setup
● IPv4 ○ IPv6
Help

IPv4 WAN Settings

WAN	Status	WAN IP	Failure Detection Method	Action	
WAN1	UP	192.168.15.175	DNS Lookup (WAN DNS Servers)	Edit	Status
WAN2	DOWN	0.0.0.0	DNS Lookup (WAN DNS Servers)	Edit	Status

7. In the WAN IPv4 Settings table, click the **Edit** button for the WAN interface that you want to configure.

   The WAN IPv4 ISP Settings screen displays.
8. In the ISP Login section, select the **Yes** radio button.



ISP Login Help

Does Your Internet Connection Require a Login?

● Yes

○ No

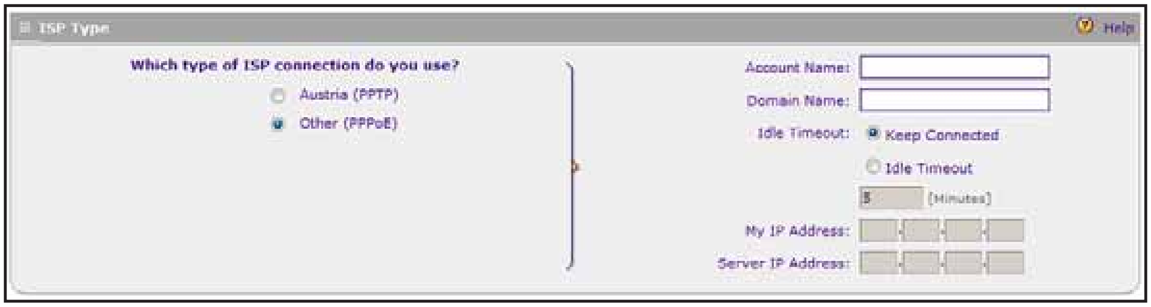
Login:

Password:

9. Enter the login name in the **Login** field and the password in the **Password** field.

   This information is provided by your ISP and is specific for the PPPoE service.

10. In the ISP Type section, select the **Other (PPPoE)** radio button.



ISP Type Help

Which type of ISP connection do you use?

○ Austria (PPTP)

● Other (PPPoE)

Account Name:

Domain Name:

Idle Timeout: ● Keep Connected

○ Idle Timeout

5 (Minutes)

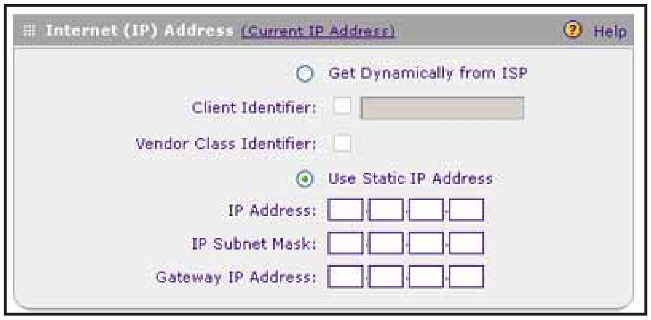
My IP Address:

Server IP Address:

11. Enter the PPPoE settings as described in the following table.

Setting	Description
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	To keep the connection always on, select the **Keep Connected** radio button. 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 method is useful if your ISP charges you based on the period that you have logged in.

12. Locate the Internet (IP) Address section.



Internet (IP) Address (Current IP Address) Help

○ Get Dynamically from ISP

Client Identifier: □

Vendor Class Identifier: □

● Use Static IP Address

IP Address:

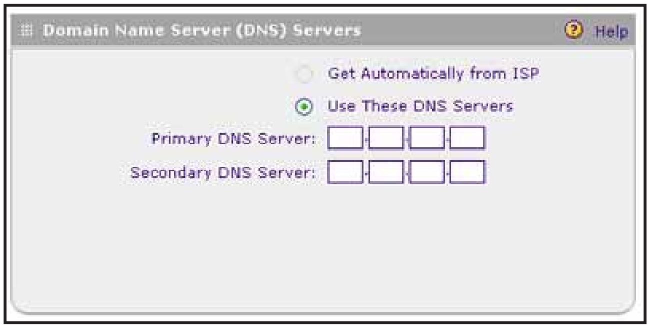
IP Subnet Mask:

Gateway IP Address:

13. Configure the IP address settings as described in the following table.

Setting	Description
Select an IP address radio button: • **Get Dynamically from ISP**. Select this radio button if your ISP has not assigned you a static IP address. The ISP automatically assigns an IP address to the VPN firewall using the DHCP network protocol. • **Use Static IP Address**. Select this radio button if your ISP has assigned you a static (fixed or permanent) IP address. Enter the IP address and subnet mask.	
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.

14. Locate the Domain Name Server (DNS) Servers section.



Domain Name Server (DNS) Servers

○ Get Automatically from ISP

● Use These DNS Servers

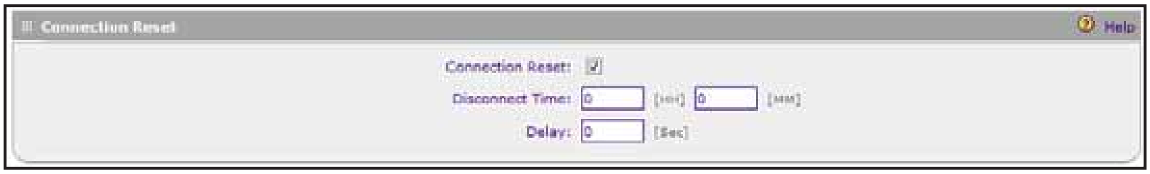
Primary DNS Server: □.□.□.□

Secondary DNS Server: □.□.□.□

15. Specify the DNS settings as described in the following table.

Setting	Description
Select a Domain Name Server (DNS) IP address radio button: • **Get Automatically from ISP**. Select this radio button if your ISP has not assigned you any DNS IP addresses. The ISP automatically assigns the DNS IP addresses to the VPN firewall using the DHCP network protocol. • **Use These DNS Servers**. Select this radio button if your ISP assigned you static (fixed or permanent) DNS IP addresses. Enter the IP addresses in the **Primary DNS Server** and **Secondary DNS Server** fields. **Note:** Make sure that you enter 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.

16. Locate the Connection Reset section.



Connection Reset

Connection Reset: ☑

Disconnect Time: 0 [HH] 0 [MM]

Delay: 0 [Sec]

17. To configure an automatic connection reset, specify the settings as described in the following table.

Setting	Description
Select the **Connection Reset** check box to specify a time when the 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 must be disconnected.
Delay	Specify the period in seconds after which the connection must be reestablished.

18. Click the **Apply** button.

    Your settings are saved.

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

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

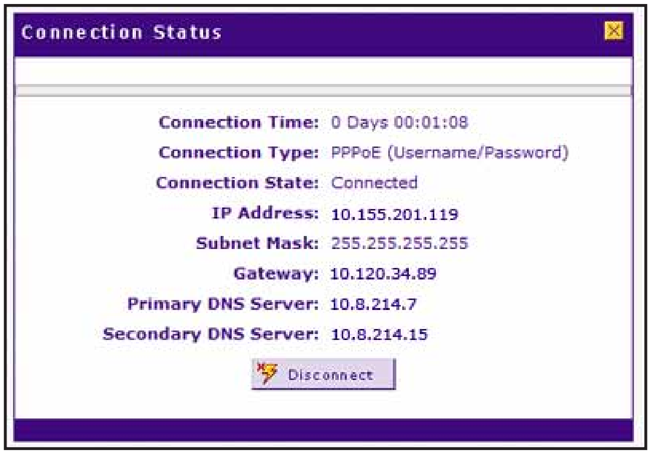
20. Verify the connection:

    a. Select **Network Configuration > WAN Settings > WAN Setup**.

       The WAN Setup screen displays the IPv4 settings.

    b. In the IPv4 WAN Settings table, click the **Status** button for the WAN interface for which you want to display the connection status.

       The Connection Status pop-up screen displays. The IP addresses that are shown in this figure are not related to any other examples in this manual.



Connection Status

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

The Connection Status screen shows a valid IP address and gateway. You are connected to the Internet.

Note: If the configuration was not successful, see *Troubleshoot the ISP Connection* on page 615.

Manually Configure a PPTP IPv4 Internet Connection

To configure a PPTP IPv4 Internet connection, enter the PPTP IPv4 information that your IPv4 ISP gave you. If you do not have this information, contact your IPv4 ISP.

For each WAN interface, you need the following information: login name, login password, the IP address assigned by the ISP to make the connection with the ISP server, the IP address of the ISP server, and, if applicable, account name and domain name.

If your ISP assigns you a static IP address, you also need the static IP address, IP subnet mask, and IP addresses of the primary DNS server and secondary DNS server. A static IP address can be assigned by ISP over PPTP.

Note: If your ISP requires MAC authentication and another MAC address was previously registered with your ISP, you must configure that MAC address on the VPN firewall (see *Change the Advertised MAC Address of the VPN Firewall* on page 70) before you begin the following procedure.

➢ **To manually configure and verify a PPTP IPv4 Internet connection for a WAN interface:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

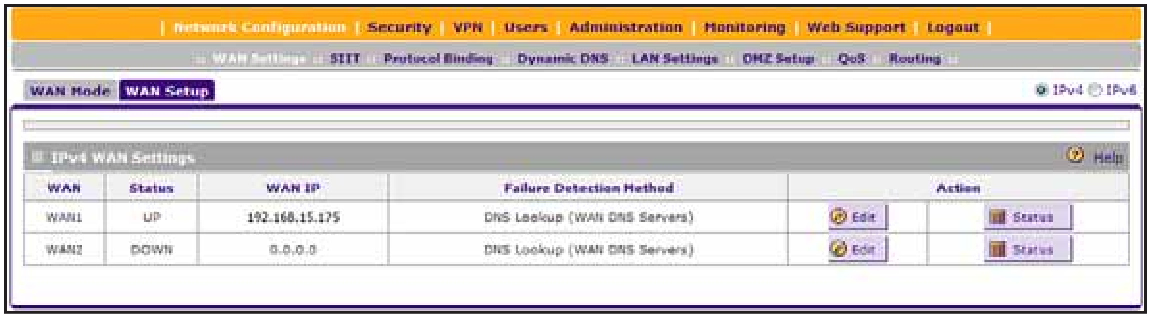
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > WAN Settings > WAN Setup**.

   The WAN Setup screen displays the IPv4 settings.

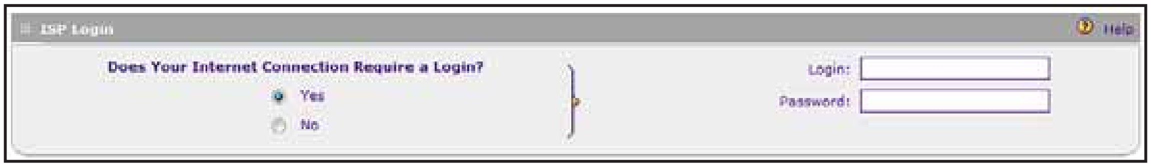

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
WAN Mode
WAN Setup
● IPv4 ○ IPv6
IPv4 WAN Settings
Help

WAN	Status	WAN IP	Failure Detection Method	Action	
WAN1	UP	192.168.15.175	DNS Lookup (WAN DNS Servers)	Edit	Status
WAN2	DOWN	0.0.0.0	DNS Lookup (WAN DNS Servers)	Edit	Status

7. In the WAN IPv4 Settings table, click the **Edit** button for the WAN interface that you want to configure.

   The WAN IPv4 ISP Settings screen displays.

8. In the ISP Login section, select the **Yes** radio button.



Does Your Internet Connection Require a Login?

● Yes
○ No

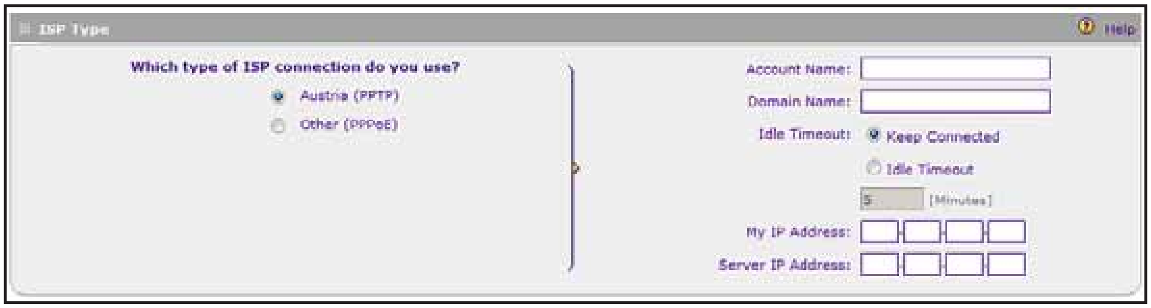
Login:

Password:

9. Enter the login name in the **Login** field and the password in the **Password** field.

   This information is provided by your ISP and is specific for the PPTP service.

10. In the ISP Type section, select the **Austria (PPTP)** radio button.



Which type of ISP connection do you use?

● Austria (PPTP)
○ Other (PPPoE)

Account Name:

Domain Name:

Idle Timeout: ● Keep Connected
○ Idle Timeout
5 (Minutes)

My IP Address:

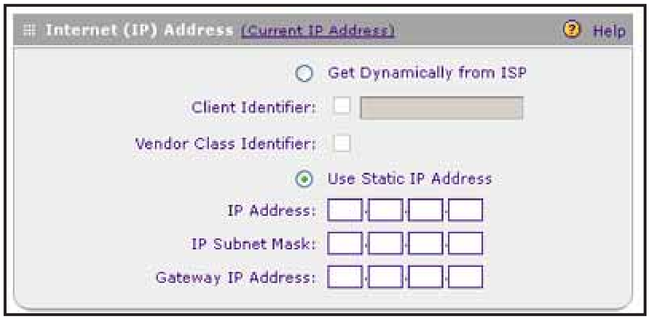
Server IP Address:

11. Enter the PPTP settings as described in the following table.

Setting	Description
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.

Setting	Description
Idle Timeout	Select a connection method radio button: • **Keep Connected**. Select this radio button to keep the connection always on. • **Idle Timeout**. Select this radio button to log out after the connection is idle for a period. In the **Idle Timeout** field, enter the number of minutes to wait before disconnecting. This method is useful if your ISP charges you based on the period that you have logged in.
My IP Address	The IP address assigned by the ISP to make the connection with the ISP server.
Server IP Address	The IP address of the PPTP server.

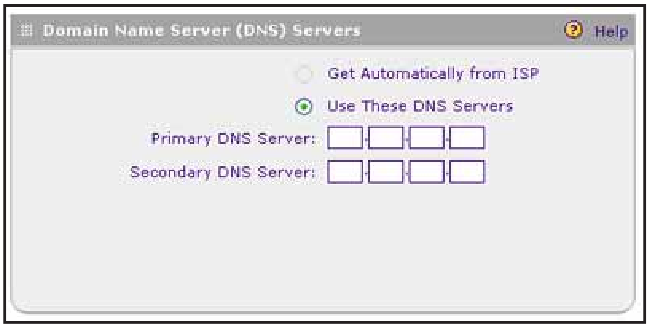
12. Locate the Internet (IP) Address section.


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:

13. Configure the IP address settings as described in the following table.

Setting	Description
Select an IP address radio button: • **Get Dynamically from ISP**. Select this radio button if your ISP has not assigned you a static IP address. The ISP automatically assigns an IP address to the VPN firewall using the DHCP network protocol. • **Use Static IP Address**. Select this radio button if your ISP assigned you a static (fixed or permanent) IP address. Enter the IP address and subnet mask.	
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.

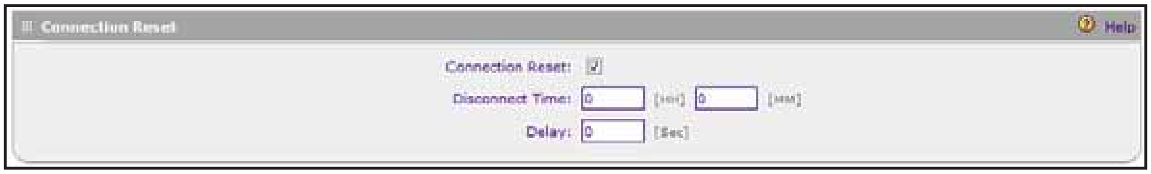
14. Locate the Domain Name Server (DNS) Servers section.



15. Specify the DNS settings as described in the following table.

Setting	Description
Select a Domain Name Server (DNS) radio button: • **Get Automatically from ISP**. Select this radio button if your ISP has not assigned you any DNS IP addresses. The ISP automatically assigns the DNS IP addresses to the VPN firewall using the DHCP network protocol. • **Use These DNS Servers**. Select this radio button if your ISP assigned you static (fixed or permanent) DNS IP addresses. Enter the IP addresses in the **Primary DNS Server** and **Secondary DNS Server** fields. **Note:** Make sure that you enter 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.

16. Locate the Connection Reset section.



Connection Reset: ☑

Disconnect Time: 0 [HH] 0 [MM]

Delay: 0 [Sec]

17. To configure an automatic connection reset, specify the settings as described in the following table.

Setting	Description
Select the **Connection Reset** check box to specify a time when the 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 must be disconnected.
Delay	Specify the period in seconds after which the connection must be reestablished.

18. Click the **Apply** button.

    Your settings are saved.

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

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

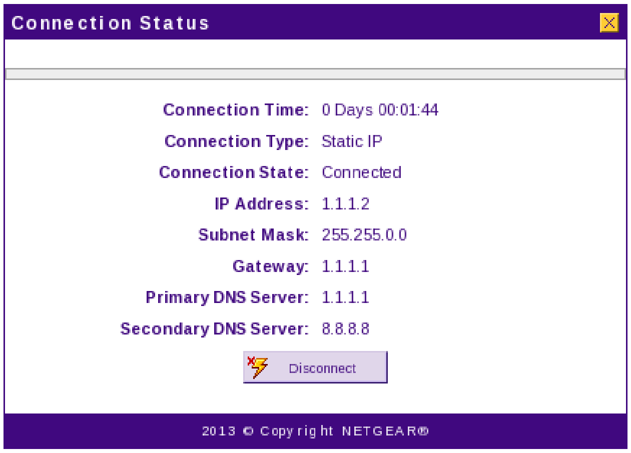
20. Verify the connection:

    a. Select **Network Configuration > WAN Settings > WAN Setup**.

       The WAN Setup screen displays the IPv4 settings.

    b. In the IPv4 WAN Settings table, click the **Status** button for the WAN interface for which you want to display the connection status.

The Connection Status pop-up screen displays. The IP addresses that are shown in this figure are not related to any other examples in this manual.



Connection Time: 0 Days 00:01:44
Connection Type: Static IP
Connection State: Connected
IP Address: 1.1.1.2
Subnet Mask: 255.255.0.0
Gateway: 1.1.1.1
Primary DNS Server: 1.1.1.1
Secondary DNS Server: 8.8.8.8

The Connection Status screen shows a valid IP address and gateway. You are connected to the Internet.

Note: If the configuration was not successful, see *Troubleshoot the ISP Connection* on page 615.

Configure Load Balancing or Auto-Rollover for IPv4 Interfaces

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

The following sections provide information about configuring load balancing and auto-rollover for IPv4 interfaces:

- *Load Balancing and Auto-Rollover for IPv4 WAN Interfaces*
- *Configure Load Balancing Mode and Optional Protocol Binding for IPv4 Interfaces*
- *Configure the Auto-Rollover Mode and Failure Detection Method for IPv4 Interfaces*

Load Balancing and Auto-Rollover for IPv4 WAN Interfaces

The VPN firewall supports the following modes for IPv4 interfaces:

- **Load balancing mode**. The VPN firewall distributes the outbound traffic equally among the WAN interfaces that are functional. You can configure two WAN interfaces. The VPN firewall supports weighted load balancing and round-robin load balancing (see *Configure Load Balancing Mode and Optional Protocol Binding for IPv4 Interfaces* on page 49).

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

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

  If you want to use a redundant ISP link for backup purposes, select the WAN port that must function as the primary link for this mode. Ensure that you also configure the backup WAN port and that you configure the WAN failure detection method to support auto-rollover (see *Configure the Auto-Rollover Mode and Failure Detection Method for IPv4 Interfaces* on page 56).

Note: If the VPN firewall functions in IPv4/IPv6 mode, you cannot configure load balancing. For information about IPv4/IPv6 mode, see *Manage the IPv6 Routing Mode* on page 88.

Configure Load Balancing Mode and Optional Protocol Binding for IPv4 Interfaces

To use two ISP IPv4 links simultaneously, configure load balancing. In load balancing mode, any WAN port carries any outbound protocol unless you configure protocol binding.

The following sections provide information about configuring load balancing mode and optional protocol binding for IPv4 interfaces:

- *Protocol Binding*
- *Configure Load Balancing Mode for IPv4 Interfaces*
- *Configure Protocol Binding Rules for IPv4 Interfaces*
- *Change a Protocol Binding Rule*
- *Manage Existing Protocol Binding Rules*

Protocol Binding

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

Protocol binding addresses two issues:

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

Configure Load Balancing Mode for IPv4 Interfaces

The following procedure describes how to configure load balancing mode, which the VPN firewall supports only for IPv4 WAN interfaces.

➢ **To configure load balancing mode:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

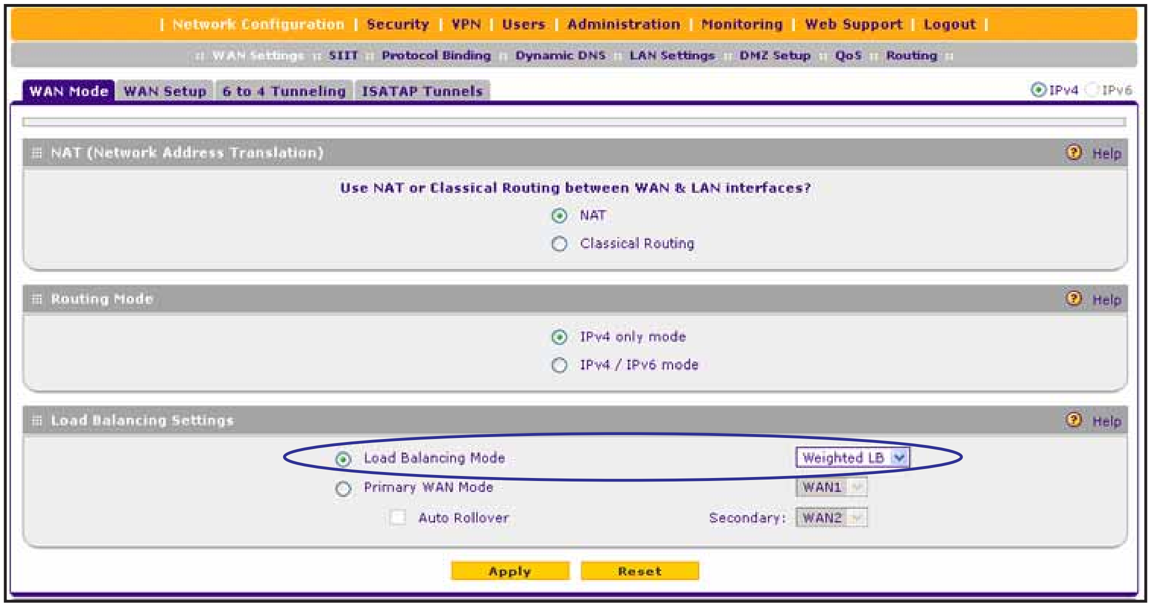
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > WAN Settings > WAN Mode**.

   The WAN Mode screen displays.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
WAN Mode
WAN Setup
6 to 4 Tunneling
ISATAP Tunnels
● IPv4 ○ IPv6
NAT (Network Address Translation)
Help
Routing Mode
Help
Load Balancing Settings
Help
Apply
Reset

Use NAT or Classical Routing between WAN & LAN interfaces?

● NAT

○ Classical Routing

● IPv4 only mode

○ IPv4 / IPv6 mode

● Load Balancing Mode — Weighted LB

○ Primary WAN Mode — WAN1

□ Auto Rollover — Secondary: WAN2

7. In the Load Balancing Settings section, configure the following settings:
   a. Select the **Load Balancing Mode** radio button.
   b. From the corresponding menu on the right, select a load balancing method:
      - **Weighted LB**. With weighted load balancing, balance weights are calculated based on WAN link speed and available WAN bandwidth.

        This is the default setting and most efficient load balancing algorithm.
      - **Round-robin**. With round-robin load balancing, new traffic connections are sent over a WAN link in a serial method irrespective of bandwidth or link speed.

        For example, if the WAN1 and WAN2 interfaces are active in round-robin load balancing mode, an HTTP request could first be sent over the WAN1 interface and then a new FTP session could start on the WAN2 interface. This load balancing method ensures that a single WAN interface does not carry a disproportionate distribution of sessions.
8. Click the **Apply** button.

   Your settings are saved.

Configure Protocol Binding Rules for IPv4 Interfaces

Protocol bindings are optional in a load balancing configuration. The following procedure describes how to configure a protocol binding rule.

➢ **To configure a protocol binding rule:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

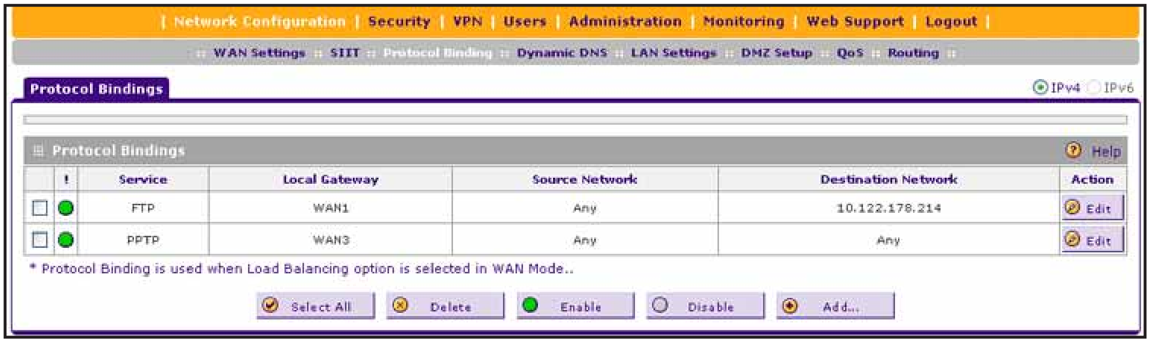
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > Protocol Binding**.

   The Protocol Bindings screen displays. The following figure shows two examples in the Protocol Bindings table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
Protocol Bindings
◉ IPv4 ○ IPv6
Protocol Bindings
Help

	!	Service	Local Gateway	Source Network	Destination Network	Action
□	●	FTP	WAN1	Any	10.122.178.214	Edit
□	●	PPTP	WAN3	Any	Any	Edit

* Protocol Binding is used when Load Balancing option is selected in WAN Mode..

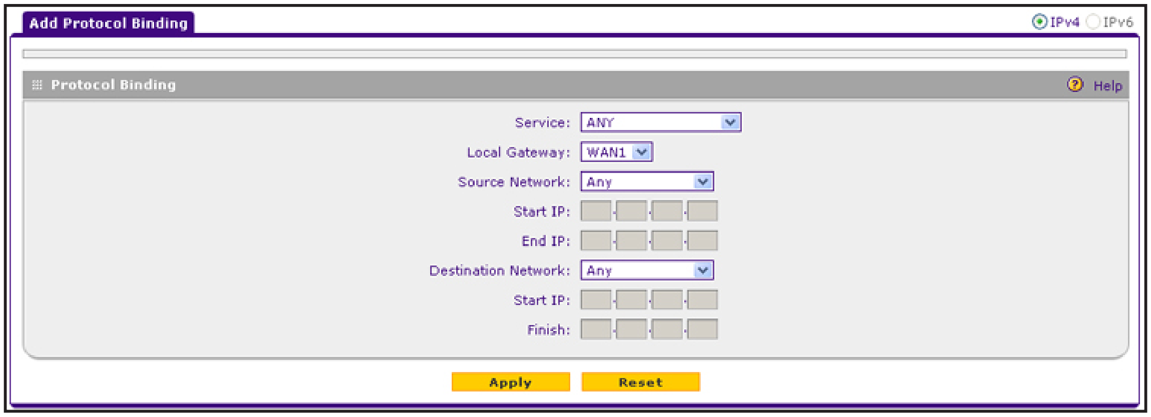
Select All
Delete
Enable
Disable
Add...

The Protocol Bindings table displays the following fields:

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

7. Click the **Add** button below the Protocol Binding table.

   The Add Protocol Binding screen displays.



Service: ANY
Local Gateway: WAN1
Source Network: Any
Start IP:
End IP:
Destination Network: Any
Start IP:
Finish:

8. Configure the protocol binding settings as described in the following table.

Setting	Description
Service	From the menu, select a service or application to be covered by this rule. If the service or application does not appear in the list, you must define it (see *Manage Customized Services* on page 280).
Local Gateway	From the menu, select a WAN interface.
Source Network	The source network settings determine which computers on your network are covered by this rule. Select an option from the **Source Network** menu: • **Any**. All devices on your LAN. • **Single Address**. In the **Start IP** field, enter the IP address to which the rule is applied. • **Address Range**. In the **Start IP** field and **End IP** field, enter the IP addresses for the range to which the rule is applied. • **GROUP1**-**GROUP8** or a **group name**. The rule is applied to the selected group. The group can be a LAN group or an IP LAN group. For information about LAN groups, see *Manage IPv4 LAN Groups and Hosts* on page 132. The **Destination Network** menu displays only IP LAN group names that you added. If you did not add any IP LAN groups, the menu does not display IP LAN groups. For information about IP groups, see *Manage IP Address Groups* on page 288.
Destination Network	The destination network settings determine which Internet locations (based on their IP addresses) are covered by the rule. Select an option from the **Destination Network** menu: • **Any**. All Internet IP addresses. • **Single Address**. In the **Start IP** field, enter the IP address to which the rule is applied. • **Address Range**. In the **Start IP** field and **End IP** field, enter the IP addresses for the range to which the rule is applied. • **Group name**. The rule is applied to the selected IP WAN group. The **Destination Network** menu displays only IP WAN group names that you added. If you did not add any IP WAN groups, the menu does not display IP WAN groups. For information about IP groups, see *Manage IP Address Groups* on page 288.

9. Click the **Apply** button.

Your settings are saved.

The protocol binding rule is added to the Protocol Binding table. The rule is automatically enabled, which is indicated by a green circle in the ! status icon column.

Change a Protocol Binding Rule

The following procedure describes how to change an existing protocol binding rule.

➢ **To change a protocol binding rule:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > Protocol Binding**.

   The Protocol Bindings screen displays.
7. In the Protocol Bindings table, click the **Edit** button for the binding that you want to change.

   The Edit Protocol Bindings screen displays.
8. Change the settings.

   For more information about the settings, see *Configure Protocol Binding Rules for IPv4 Interfaces* on page 51.
9. Click the **Apply** button.

   Your settings are saved. The modified protocol binding displays in the Protocol Bindings table on the Protocol Bindings screen.

Manage Existing Protocol Binding Rules

The following procedure describes how to enable or disable existing protocol binding rules or remove protocol binding rules that you no longer need.

➢ **To enable, disable, or remove one or more protocol binding rules:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > Protocol Binding**.

   The Protocol Bindings screen displays.
7. In the Protocol Bindings table, select the check box to the left of each protocol binding that you want to enable, disable, or remove or click the **Select All** button to select all bindings.
8. Click one of the following buttons:
   - **Enable**. Enables the selected protocol bindings.

     The **!** status icons change from gray circles to green circles, indicating that the selected bindings are enabled. (By default, when you add a binding to the table, the binding is automatically enabled.)
   - **Disable**. Disables the selected protocol bindings.

     The **!** status icons change from green circles to gray circles, indicating that the selected bindings are disabled.
   - **Delete**. Removes the selected protocol bindings.

     The selected bindings are removed from the Protocol Bindings table.

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

Instead of using two WAN interfaces simultaneously in a load balancing configuration, you can use one WAN interface as the primary link and the other WAN interface as the backup link for increased reliability.

The following sections provide information about configuring auto-rollover mode and the failure detection method for IPv4 interfaces:

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

Auto-Rollover Mode and Failure Detection

To use a redundant ISP link for backup purposes, ensure that the backup WAN interface is configured. Then select the WAN interface that must function as the primary link for this mode and configure the WAN failure detection method to support auto-rollover.

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

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

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

Configure Auto-Rollover Mode for IPv4 WAN Interfaces

The following procedure describes how to configure auto-rollover mode for IPv4 WAN interfaces.

➤ **To configure auto-rollover mode for IPv4 WAN interfaces:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

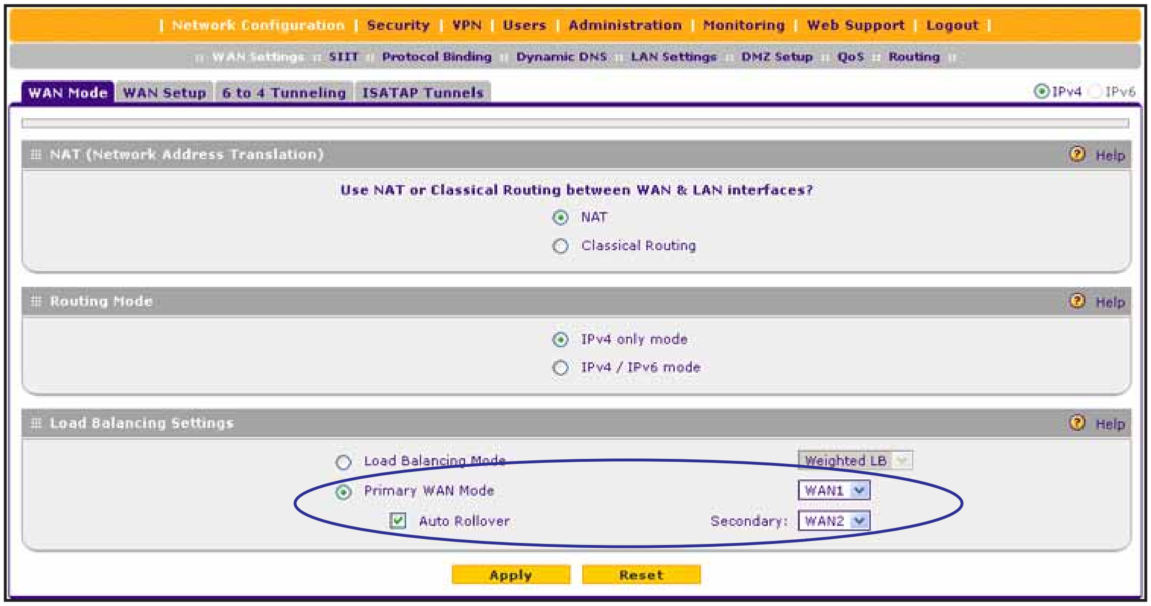
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > WAN Settings > WAN Mode**.

   The WAN Mode screen displays.


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

● IPv4 ○ IPv6

NAT (Network Address Translation)

Use NAT or Classical Routing between WAN & LAN interfaces?

● NAT
○ Classical Routing

Routing Mode

● IPv4 only mode
○ IPv4 / IPv6 mode

Load Balancing Settings

○ Load Balancing Mode Weighted LB
● Primary WAN Mode WAN1
☑ Auto Rollover Secondary: WAN2

7. In the Load Balancing Settings section, configure the following settings:

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

   b. From the corresponding menu on the right, select a WAN interface to function as the primary WAN interface.

      The other WAN interface becomes disabled.

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

   d. From the corresponding menu on the right, select a WAN interface to function as the backup WAN interface.

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

8. Click the **Apply** button.

Your settings are saved.

Configure the Failure Detection Method for IPv4 WAN Interfaces

The following procedure describes how to configure the failure detection method for IPv4 WAN interfaces that function in auto-rollover mode.

➢ **To configure the failure detection method for IPv4 WAN interfaces:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

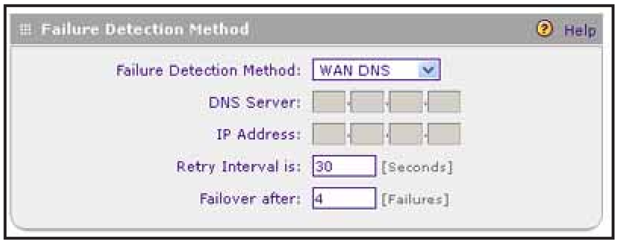
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > WAN Settings > WAN Setup**.

   The WAN Setup screen displays the IPv4 settings.
7. In the WAN IPv4 Settings table, click the **Edit** button for the WAN interface that you selected as the primary WAN interface.

   The WAN IPv4 ISP Settings screen displays.
8. Click the **Advanced** option arrow in the upper right.

   The WAN Advanced Options screen displays for the WAN interface that you selected.
9. Locate the Failure Detection Method section.



Failure Detection Method

Failure Detection Method: WAN DNS

DNS Server:

IP Address:

Retry Interval is: 30 [Seconds]

Failover after: 4 [Failures]

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

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

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

11. Click the **Apply** button.

    Your settings are saved.

Note: You can configure the VPN firewall to generate a WAN status log and email this log to a specified address (see *Manage Logging, Alerts, and Event Notifications* on page 567).

Manage Secondary IPv4 WAN Addresses

The following sections provide information about managing secondary IPv4 WAN addresses:

- *Secondary IPv4 WAN Addresses*
- *Add a Secondary WAN Address to a WAN IPv4 Interface*

- *Remove One or More Secondary WAN Addresses*

Secondary IPv4 WAN Addresses

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

After you configure secondary WAN addresses, you can assign these addresses as follows when you configure firewall rules:

- As a WAN destination IP address for a LAN WAN inbound firewall rule (see *Add LAN WAN Inbound Service Rules* on page 228).
- As a WAN destination IP address for a DMZ WAN inbound firewall rule (see *Add DMZ WAN Inbound Service Rules* on page 237).
- As a NAT IP address for a LAN WAN outbound firewall (see *Add LAN WAN Outbound Service Rules* on page 223).
- As a NAT IP address for a DMZ WAN outbound firewall (see *Add DMZ WAN Outbound Service Rules* on page 233).

For more information about firewall rules, see *Overview of Rules to Block or Allow Specific Kinds of Traffic* on page 210.

Make sure that any secondary WAN addresses are different from the primary WAN, LAN, and DMZ IP addresses that are already configured on the VPN firewall. However, primary and secondary WAN addresses can be in the same subnet.

The following is an example of correctly configured IP addresses:

- **Primary WAN1 IP address**. 10.0.0.1 with subnet 255.0.0.0
- **Secondary WAN1 IP address**. 30.0.0.1 with subnet 255.0.0.0
- **Primary WAN2 IP address**. 20.0.0.1 with subnet 255.0.0.0
- **Secondary WAN2 IP address**. 40.0.0.1 with subnet 255.0.0.0
- **DMZ IP address**. 192.168.10.1 with subnet 255.255.255.0
- **Primary LAN IP address**. 192.168.1.1 with subnet 255.255.255.0
- **Secondary LAN IP address**. 192.168.20.1 with subnet 255.255.255.0

Add a Secondary WAN Address to a WAN IPv4 Interface

The following procedure describes how to add a secondary WAN address to a WAN IPv4 interface.

➢ **To add a secondary WAN address to a WAN IPv4 interface:**

1. On your computer, launch an Internet browser.

2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > WAN Settings > WAN Setup**.

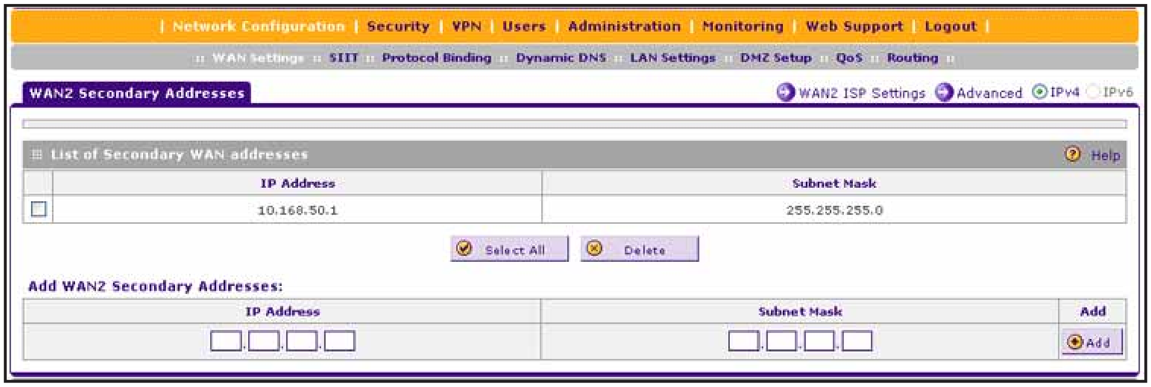
   The WAN Setup screen displays the IPv4 settings.

7. In the WAN IPv4 Settings table, click the **Edit** button for WAN interface for which you want to add a secondary WAN address.

   The WAN IPv4 ISP Settings screen displays.

8. Click the **Secondary Addresses** option arrow in the upper right.

   The WAN Secondary Addresses screen displays for the WAN interface that you selected. The following figure shows the WAN2 Secondary Addresses screen as an example and includes one entry in the List of Secondary WAN addresses table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
WAN2 Secondary Addresses
WAN2 ISP Settings
Advanced
● IPv4 ○ IPv6
Help
Select All
Delete
Add

List of Secondary WAN addresses

	IP Address	Subnet Mask
□	10.168.50.1	255.255.255.0

Add WAN2 Secondary Addresses:

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

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

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

10. Click the **Add** button.

    The secondary IP address is added to the List of Secondary WAN addresses table.

11. Repeat *Step 9* and *Step 10* for each secondary IP address that you want to add to the List of Secondary WAN addresses table.

Remove One or More Secondary WAN Addresses

The following procedure describes how to remove one or more secondary WAN addresses from a WAN IPv4 interface.

➢ **To remove one or more secondary WAN addresses:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > WAN Settings > WAN Setup**.

   The WAN Setup screen displays the IPv4 settings.

7. In the WAN IPv4 Settings table, click the **Edit** button for the WAN interface for which you want to remove one or more secondary WAN addresses.

   The WAN IPv4 ISP Settings screen displays.

8. Click the **Secondary Addresses** option arrow in the upper right.

   The WAN Secondary Addresses screen displays for the WAN interface that you selected.

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

    The selected addresses are removed from the List of Secondary WAN addresses table.

Manage Dynamic DNS Connections

The following sections provide information about managing Dynamic DNS:

- *Dynamic DNS*
- *Configure Dynamic DNS*

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 DynDNS.org, TZO.com, Oray.net, or 3322.org. (The web management interface of the VPN firewall provides links to these DDNS providers.) The VPN firewall firmware includes software that notifies DDNS servers of changes in the WAN IP address so that the services running on this network can be accessed by others on the Internet.

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

After you 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. Consider the following:

- For auto-rollover mode, you need a fully qualified domain name (FQDN) to implement features such as exposed hosts and virtual private networks regardless of whether you have a fixed or dynamic IP address.
- For load balancing mode, you might still need a fully qualified domain name (FQDN) either for convenience or if you have a dynamic IP address.

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

Configure Dynamic DNS

The following procedure describes how to configure dynamic DNS (DDNS) for both WAN interfaces.

➢ **To configure DDNS for both WAN interfaces:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

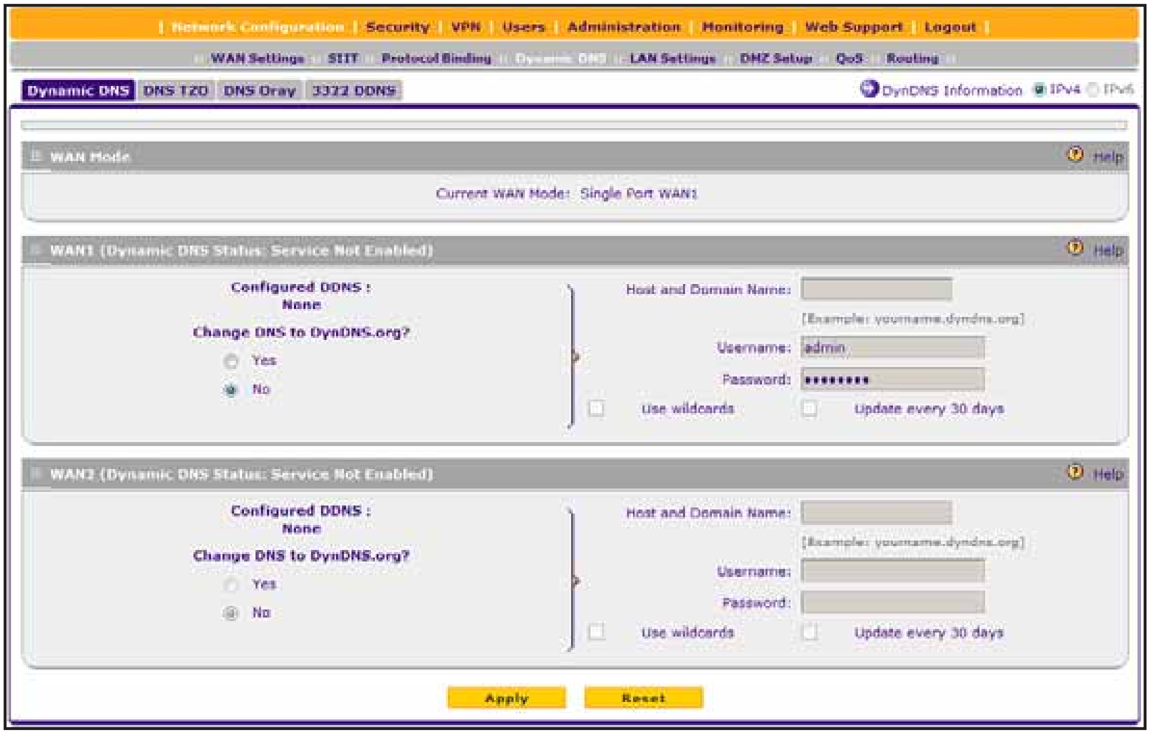
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > Dynamic DNS**.

   The DNS submenu tabs display, with the Dynamic DNS screen in view.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
Dynamic DNS | DNS TZO | DNS Oray | 3322 DDNS
DynDNS Information ● IPv4 ○ IPv6
WAN Mode
Help

Current WAN Mode: Single Port WAN1

WAN1 (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: admin

Password: ••••••••

□ Use wildcards □ Update every 30 days

WAN2 (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:

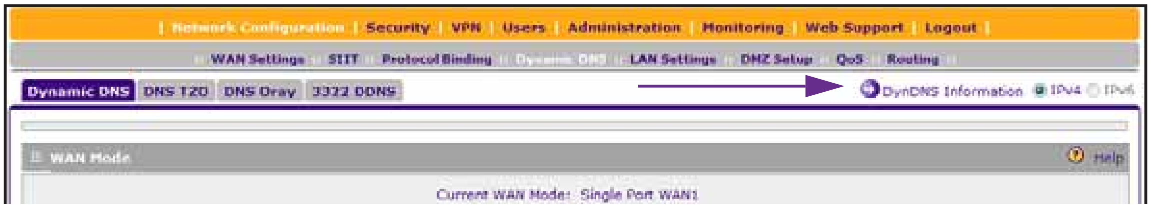
Password:

□ Use wildcards □ Update every 30 days

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

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

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


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
WAN Settings | SIIT | Protocol Binding | Dynamic DNS | LAN Settings | DMZ Setup | QoS | Routing
Dynamic DNS | DNS TZO | DNS Oray | 3322 DDNS
DynDNS Information
● IPv4 ○ IPv6
WAN Mode
Help

Current WAN Mode: Single Port WAN1

9. Visit the website of the DDNS service provider and register for an account (for example, for DynDNS.org, visit *http://www.dyndns.com/*).

10. Configure the DDNS service settings as described in the following table.

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

11. Click the **Apply** button.

Your settings are saved.

Managing Advanced WAN Options

The following sections provide information about managing advanced WAN options:

- *Change the Maximum Transmission Unit Size*
- *Change the Port Speed and Duplex Settings*
- *Change the Advertised MAC Address of the VPN Firewall*
- *Set the WAN Connection Type and Corresponding Speeds*

Note: For information about another advanced WAN option, the failure detection for auto-rollover mode for IPv4 interfaces, see *Configure the Failure Detection Method for IPv4 WAN Interfaces* on page 58.

Change the Maximum Transmission Unit Size

Change the maximum transmit unit (MTU) size only if you have reason to do so or your ISP requests that you do so.

➢ **To change the MTU size:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > WAN Settings > WAN Setup**.

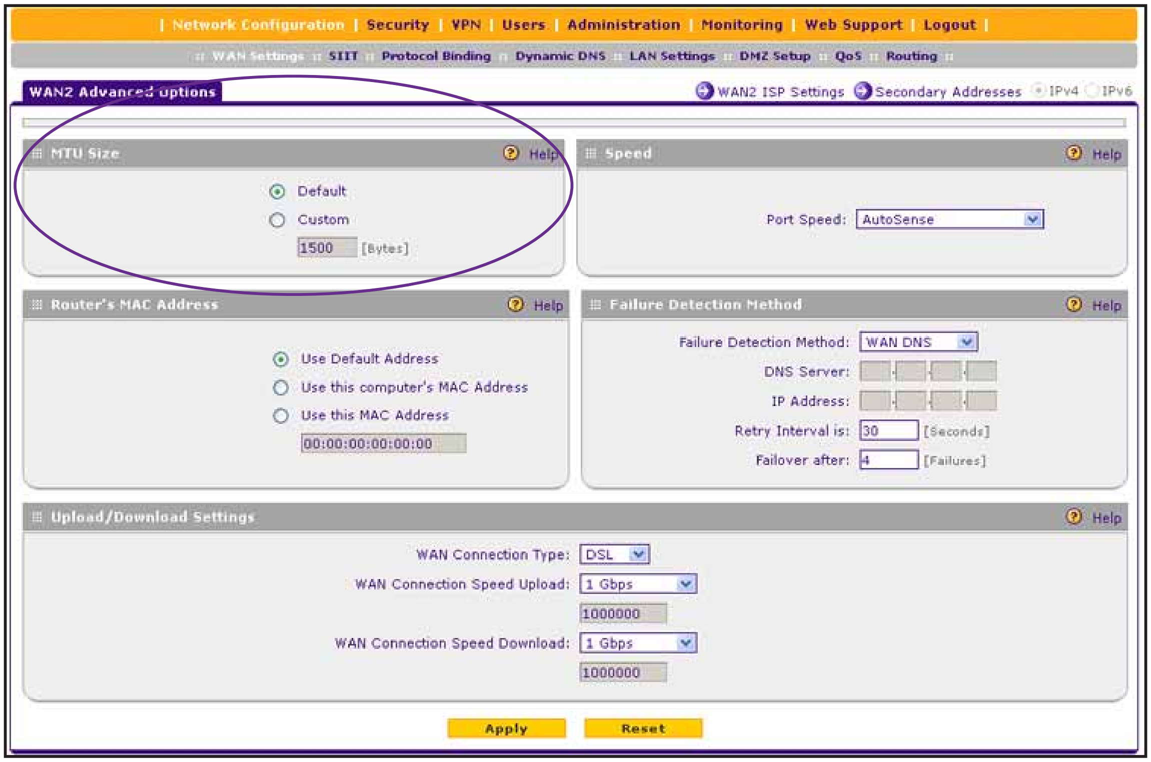
   The WAN Setup screen displays the IPv4 settings.

7. In the WAN IPv4 Settings table, click the **Edit** button for the WAN interface that you want to configure.

   The WAN IPv4 ISP Settings screen displays.

8. Click the **Advanced** option arrow in the upper right.

   The WAN Advanced Options screen displays for the WAN interface that you selected. The following figure shows the WAN2 Advanced Options screen as an example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
WAN2 Advanced options
WAN2 ISP Settings
Secondary Addresses
● IPv4 ○ IPv6
Help
Apply
Reset

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

Failure Detection Method

Failure Detection Method: WAN DNS
DNS Server:
IP Address:
Retry Interval is: 30 [Seconds]
Failover after: 4 [Failures]

Upload/Download Settings

WAN Connection Type: DSL
WAN Connection Speed Upload: 1 Gbps
1000000
WAN Connection Speed Download: 1 Gbps
1000000

9. In the MTU Size section, configure the MTU size:
   - **Default**. Select this radio button for the normal maximum transmit unit (MTU) size. For most Ethernet networks, this value is 1500 bytes, or 1492 bytes for PPPoE connections.
   - **Custom**. Select this radio button and enter an MTU value in the **Bytes** field. For some ISPs, you might need to reduce the MTU, but this is rarely required. Do not change the MTU unless you are sure that it is necessary for your ISP connection.

WARNING:

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

10. Click the **Apply** button.

    Your settings are saved.

Change the Port Speed and Duplex Settings

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.

➢ **To change the port speed and duplex settings:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

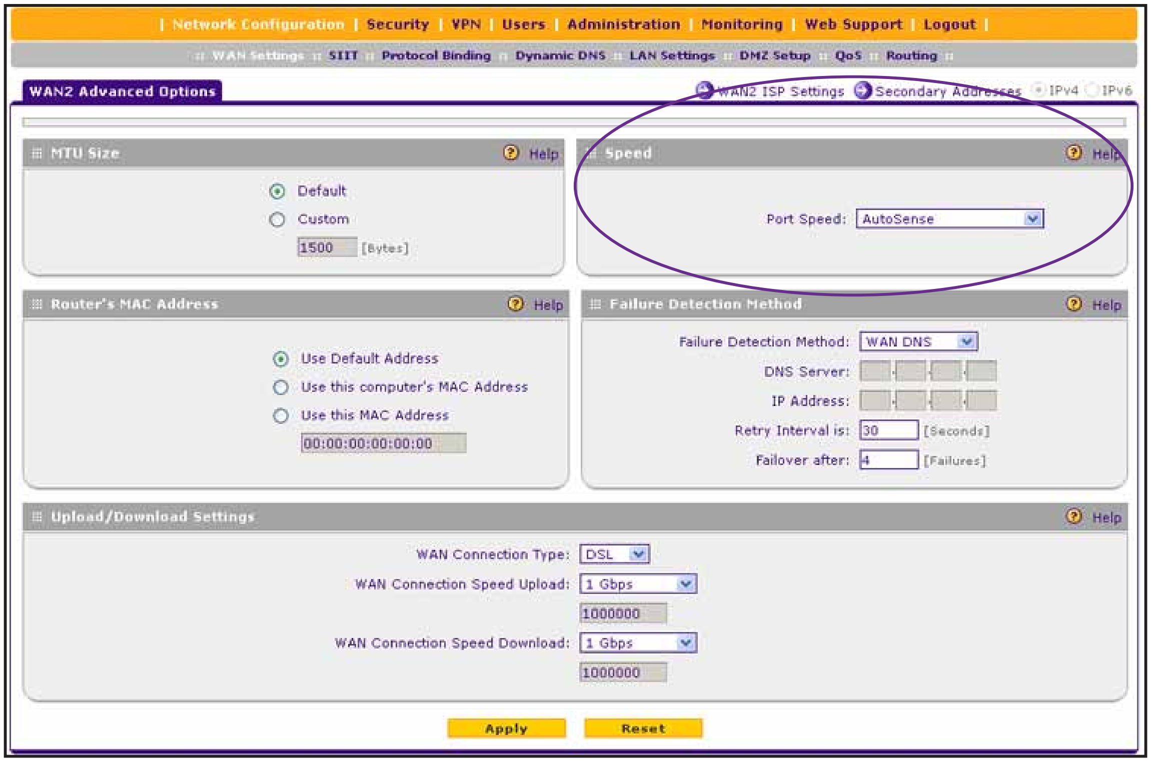
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > WAN Settings > WAN Setup**.

   The WAN Setup screen displays the IPv4 settings.
7. In the WAN IPv4 Settings table, click the **Edit** button for the WAN interface that you want to configure.

   The WAN IPv4 ISP Settings screen displays.
8. Click the **Advanced** option arrow in the upper right.

   The WAN Advanced Options screen displays for the WAN interface that you selected. The following figure shows the WAN2 Advanced Options screen as an example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
WAN2 Advanced Options
WAN2 ISP Settings
Secondary Addresses
IPv4
IPv6
Help
Apply
Reset

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

Failure Detection Method

Failure Detection Method: WAN DNS
DNS Server:
IP Address:
Retry Interval is: 30 [Seconds]
Failover after: 4 [Failures]

Upload/Download Settings

WAN Connection Type: DSL
WAN Connection Speed Upload: 1 Gbps
1000000
WAN Connection Speed Download: 1 Gbps
1000000

9. In the Speed section, if you know the Ethernet port speed of the modem, dish, or router, select it from the **Port Speed** menu.
   - **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. Use the half-duplex settings only if the full-duplex settings do not function correctly.
   - **10BaseT Full_Duplex**. Ethernet speed at full duplex.
   - **100BaseT Half_Duplex**. Fast Ethernet speed at half duplex. Use the half-duplex settings only if the full-duplex settings do not function correctly.
   - **100BaseT Full_Duplex**. Fast Ethernet speed at full duplex.
   - **1000BaseT Full_Duplex**. Gigabit Ethernet speed at full duplex.

⚠ **WARNING:**

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

10. Click the **Apply** button.

    Your settings are saved.

Change the Advertised MAC Address of the VPN Firewall

Each computer or router on your network has a unique 48-bit local Ethernet address. This is also referred to as the computer’s Media Access Control (MAC) address.

If your ISP has MAC authentication enabled, you cannot establish a connection with your ISP if the VPN firewall is not configured with the correct MAC address. If your ISP requires MAC authentication and another MAC address was previously registered with your ISP, you must configure that MAC address on the VPN firewall.

➢ **To configure advanced WAN options:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

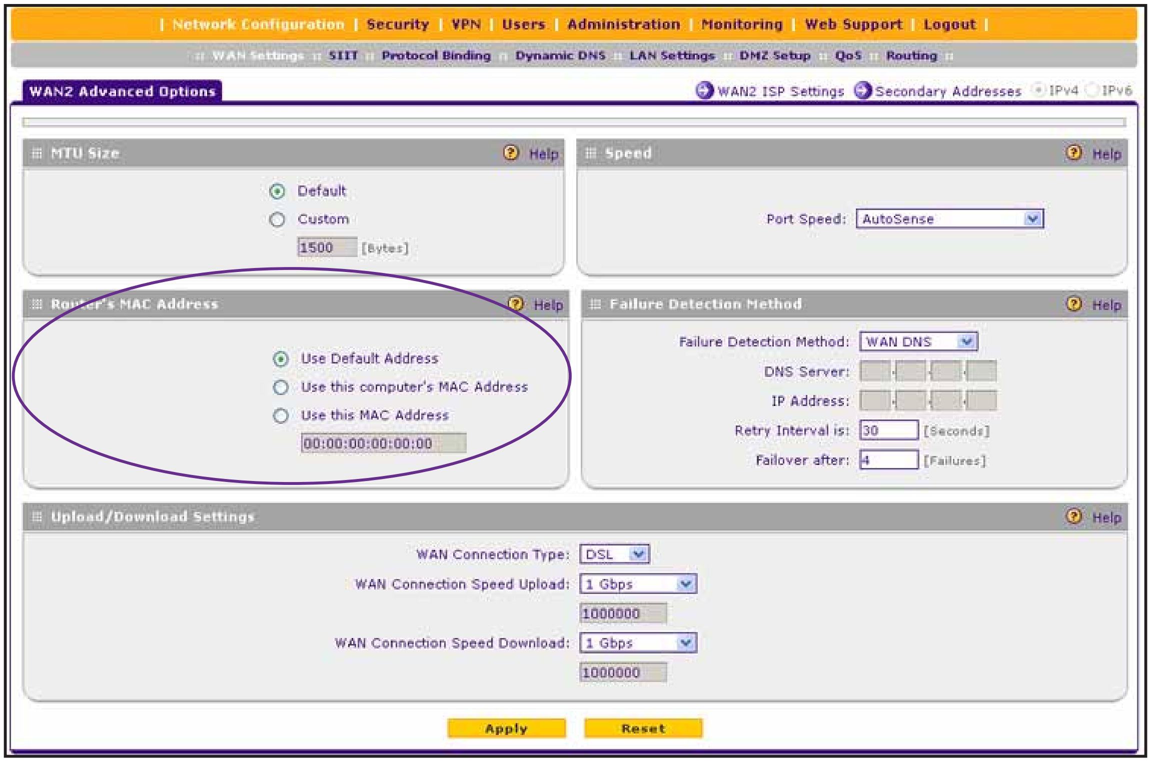
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > WAN Settings > WAN Setup**.

   The WAN Setup screen displays the IPv4 settings.
7. In the WAN IPv4 Settings table, click the **Edit** button for the WAN interface that you want to configure.

   The WAN IPv4 ISP Settings screen displays.
8. Click the **Advanced** option arrow in the upper right.

   The WAN Advanced Options screen displays for the WAN interface that you selected. The following figure shows the WAN2 Advanced Options screen as an example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
WAN2 Advanced Options
WAN2 ISP Settings
Secondary Addresses
Help
Apply
Reset

● 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

Failure Detection Method

Failure Detection Method: WAN DNS
DNS Server:
IP Address:
Retry Interval is: 30 [Seconds]
Failover after: 4 [Failures]

Upload/Download Settings

WAN Connection Type: DSL
WAN Connection Speed Upload: 1 Gbps
1000000
WAN Connection Speed Download: 1 Gbps
1000000

9. In the Router's MAC Address section, enter the settings as described in the following table.

Setting	Description
Use Default Address	To use the VPN firewall's own MAC address, select the **Use Default Address** radio button. This is the default setting.
Use this computer's MAC Address	Select the **Use this computer's MAC Address** radio button to allow the VPN firewall to use the MAC address of the computer you are now using to access the web management interface. This setting is useful if your ISP requires MAC authentication.
Use this MAC Address	Select the **Use this MAC Address** radio button and manually enter the MAC address in the field next to the radio button. You would typically enter the MAC address that your ISP 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.

WARNING:

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

10. Click the **Apply** button.

Your settings are saved.

Set the WAN Connection Type and Corresponding Speeds

The WAN connection type and corresponding upload and download connection speeds in effect limit the rate of traffic that is being forwarded by the VPN firewall.

➢ **To set the WAN connection type and upload and download connection speeds:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

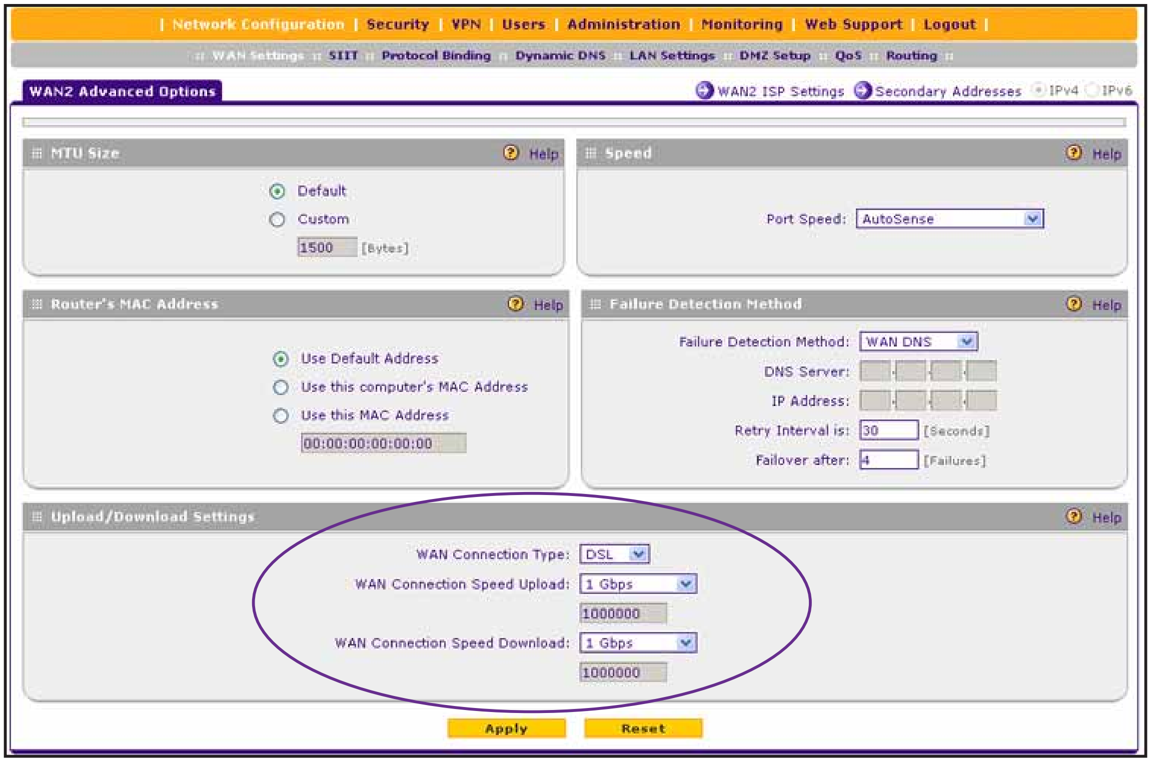
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > WAN Settings > WAN Setup**.

   The WAN Setup screen displays the IPv4 settings.
7. In the WAN IPv4 Settings table, click the **Edit** button for the WAN interface that you want to configure.

   The WAN IPv4 ISP Settings screen displays.
8. Click the **Advanced** option arrow in the upper right.

   The WAN Advanced Options screen displays for the WAN interface that you selected. The following figure shows the WAN2 Advanced Options screen as an example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
WAN2 ISP Settings
Secondary Addresses
IPv4
IPv6
Help
Apply
Reset

WAN2 Advanced Options

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

Failure Detection Method

Failure Detection Method: WAN DNS
DNS Server:
IP Address:
Retry Interval is: 30 [Seconds]
Failover after: 4 [Failures]

Upload/Download Settings

WAN Connection Type: DSL
WAN Connection Speed Upload: 1 Gbps
1000000
WAN Connection Speed Download: 1 Gbps
1000000

9. In the Upload/Download Settings section, enter the settings as described in the following table.

Setting	Description
WAN Connection Type	From the menu, select the type of connection that the VPN firewall uses to connect to the Internet over the selected interface: **DSL**, **ADLS**, **T1**, **T3**, or **Other**.
WAN Connection Speed Upload	From the menu, select the maximum upload speed that your ISP provides for the selected interface. You can select from **56 Kbps** to **1 Gbps**, or you can select **Custom** and enter the speed in Kbps in the field below the **WAN Connection Speed Upload** menu.
WAN Connection Speed Download	From the menu, select the maximum download speed that your ISP provides for the selected interface. You can select from **56 Kbps** to **1 Gbps**, or you can select **Custom** and enter the speed in Kbps in the field below the **WAN Connection Speed Download** menu.

⚠ **WARNING:**

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

10. Click the **Apply** button.

Your settings are saved.

Manage WAN QoS and WAN QoS Profiles

The following sections provide information about managing WAN Quality of Service (QoS) and WAN QoS profiles:

- *WAN QoS*
- *Add a Rate Control WAN QoS Profile*
- *Add a Priority Queue WAN QoS Profile*
- *Enable WAN QoS and Select the WAN QoS Type*
- *Change a QoS Profile*
- *Enable, Disable, or Remove One or More WAN QoS Profiles*

WAN QoS

The VPN firewall can support multiple Quality of Service (QoS) profiles for each WAN interface.

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

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

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

Note: Before you enable WAN QoS, make sure that the WAN connection type and speeds are configured correctly (see *Managing Advanced WAN Options* on page 66).

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

Add a Rate Control WAN QoS Profile

The following procedure describes how to add a rate control QoS profile for a WAN interface.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

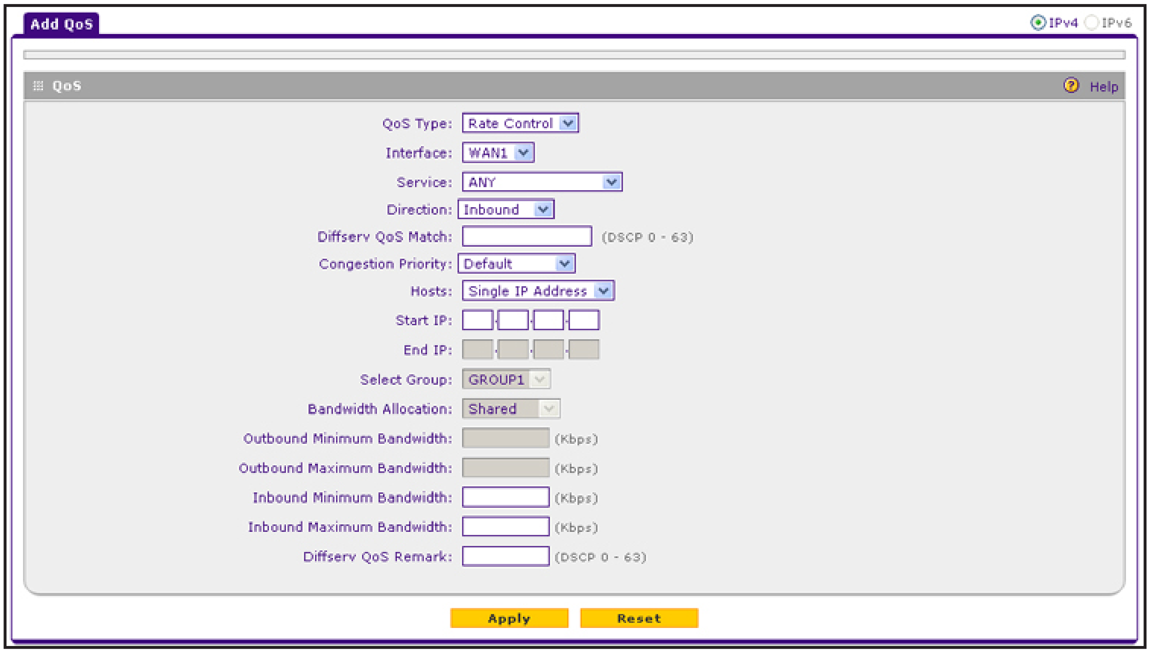
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > QoS**.

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

   The Add QoS screen displays. The following figure shows settings for a rate control QoS profile.



QoS Type: Rate Control
Interface: WAN1
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)

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

Setting	Description
QoS Type	From the menu, select **Rate Control**. For information about the **Priority** selection, see *Add a Priority Queue WAN QoS Profile* on page 78.
Interface	From the menu, select a WAN interface.
Service	From the menu, select a service or application to be covered by this profile. If the service or application does not appear in the list, you must define it (see *Manage Customized Services* on page 280).
Direction	From the menu, select the direction to which rate control is applied: • **Inbound Traffic**. Rate control is applied to inbound traffic only. • **Outbound Traffic**. Rate control is applied to outbound traffic only. • **Both**. Rate control is applied to both outbound and inbound traffic.
Diffserv QoS Match	Enter a DSCP value in the range of 0 through 63. Packets are classified against this value. Leave this field blank to disable packet matching.

Setting	Description
Congestion Priority	From the menu, select the priority queue that determines the allocation of excess bandwidth and the classification level of the packets among other priority queues on the VPN firewall: • **Default**. Traffic is mapped based on the ToS field in the packet's IP header. • **High**. This queue includes the following DSCP values: AF41, AF42, AF43, AF44, and CS4. • **Medium-high**. This queue includes the following DSCP values: AF31, AF32, AF33, AF34, and CS3. • **Medium**. This queue includes the following DSCP values: AF21, AF22, AF23, AF24, and CS2. • **Low**. This queue includes the following DSCP values: AF11, AF12, AF13, AF14, CS1, 0, and all other values.
Hosts	From the menu, select the IP address, range of IP addresses, or group to which the profile is applied, and, if applicable, specify how the bandwidth is allocated: • **Single IP Address**. The profile is applied to a single IP address. Enter the address in the **Start IP** field. • **IP Address Range**. The profile is applied to an IP address range. Enter the first address of the range in the **Start IP** field and the last address of the range in the **End IP** field. From the **Bandwidth Allocation** menu, select how the bandwidth is allocated: - **Shared**. The bandwidth is shared among all IP addresses the range. - **Individual**. The bandwidth is allocated to each IP address in the range. • **Group**. The profile is applied to a LAN group. From the **Select Group** menu, select the LAN group to which the profile is applied. For information about LAN groups, see *Manage IPv4 LAN Groups and Hosts* on page 132. From the **Bandwidth Allocation** menu, select how the bandwidth is allocated: - **Shared**. The bandwidth is shared among all members of a group. - **Individual**. The bandwidth is allocated to each member of a group.
Outbound Minimum Bandwidth	Enter the minimum outbound bandwidth in Kbps that is allocated to the host.
Outbound Maximum Bandwidth	Enter the maximum outbound bandwidth in Kbps that is allocated to the host.
Inbound Minimum Bandwidth	Enter the minimum inbound bandwidth in Kbps that is allocated to the host.
Inbound Maximum Bandwidth	Enter the maximum inbound bandwidth in Kbps that is allocated to the host.
Diffserv QoS Remark	Enter a DSCP value in the range of 0 through 63. Packets are marked with this value. Leave this field blank to disable packet marking.

9. Click the **Apply** button.

   Your settings are saved. The profile is added to the List of QoS Profiles table on the QoS screen.

   You are now ready to enable WAN QoS and select the rate control QoS type (see *Enable WAN QoS and Select the WAN QoS Type* on page 80).

Add a Priority Queue WAN QoS Profile

The following procedure describes how to add a priority queue QoS profile for a WAN interface.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

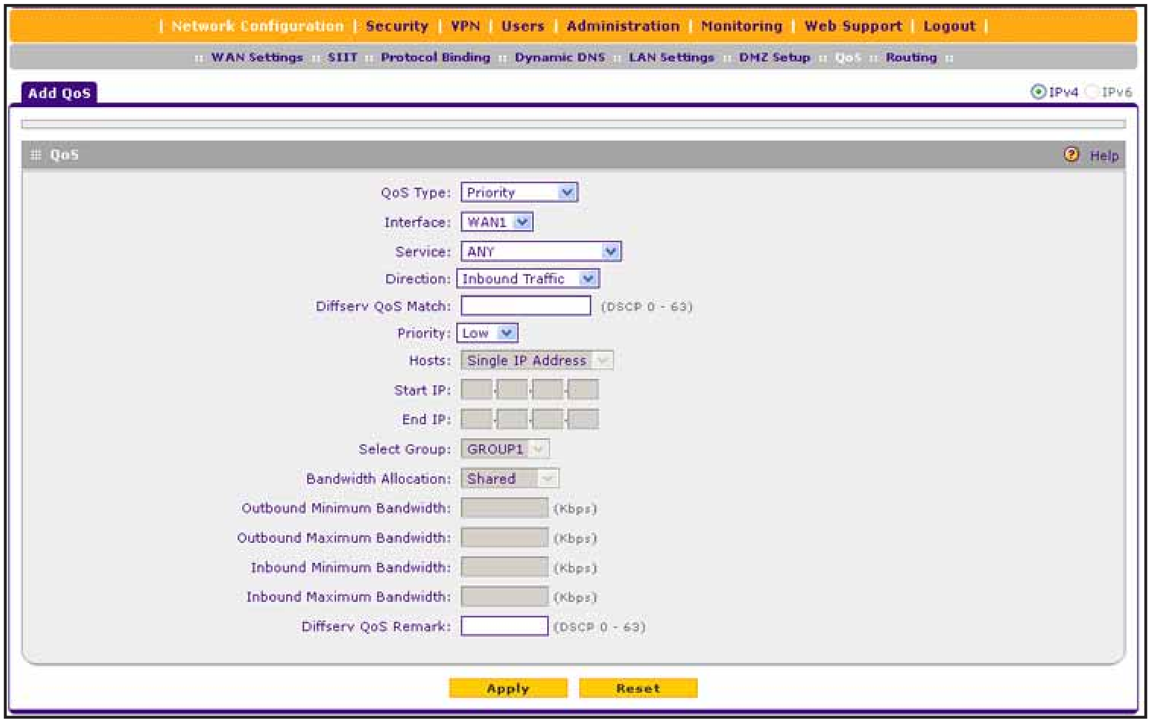
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > QoS**.

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

   The Add QoS screen displays. The following figure shows settings for a priority QoS profile.


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

QoS Type: Priority

Interface: WAN1

Service: ANY

Direction: Inbound Traffic

Diffserv QoS Match: (DSCP 0 - 63)

Priority: Low

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)

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

Setting	Description
QoS Type	From the menu, select **Priority**. For information about the **Rate Control** selection, see *Add a Rate Control WAN QoS Profile* on page 75).
Interface	From the menu, select a WAN interface.
Service	From the menu, select a service or application to be covered by this profile. If the service or application does not appear in the list, you must define it (see *Manage Customized Services* on page 280).
Direction	From the menu, select the direction to which the priority queue is applied: • **Outbound Traffic**. The priority queue is applied to outbound traffic only. • **Inbound Traffic**. The priority queue is applied to inbound traffic only.
Diffserv QoS Match	Enter a DSCP value in the range of 0 through 63. Packets are classified against this value. Leave this field blank to disable packet matching.
Priority	From the menu, select the priority queue that determines the allocation of bandwidth: • **Low**. All services that are assigned a low-priority queue share 10 percent of interface bandwidth. • **High**. All services that are assigned a high-priority queue share 60 percent of interface bandwidth. **Note:** By default, all services are assigned the medium-priority queue, in which they share 30 percent of the interface bandwidth.

Setting	Description
Hosts	These settings do not apply to a priority profile.
Start IP	
End IP	
Select Group	
Bandwidth Allocation	
Outbound Minimum Bandwidth	
Outbound Maximum Bandwidth	
Inbound Minimum Bandwidth	
Inbound Maximum Bandwidth	
Diffserv QoS Remark	Enter a DSCP value in the range of 0 through 63. Packets are marked with this value. Leave this field blank to disable packet marking.

9. Click the **Apply** button.

   Your settings are saved. The profile is added to the List of QoS Profiles table on the QoS screen.

   You are now ready to enable WAN QoS and select the priority QoS type (see *Enable WAN QoS and Select the WAN QoS Type* on page 80).

Enable WAN QoS and Select the WAN QoS Type

Depending on the type of WAN QoS that you want to select, first configure one or more rate control QoS profiles (see *Add a Rate Control WAN QoS Profile* on page 75) or priority control QoS profiles (see *Add a Priority Queue WAN QoS Profile* on page 78) before you enable WAN QoS and select the type of WAN QoS.

Note: When you enable WAN QoS, the performance of the VPN firewall might be affected slightly.

➢ **To enable WAN QoS and select the type of WAN QoS:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

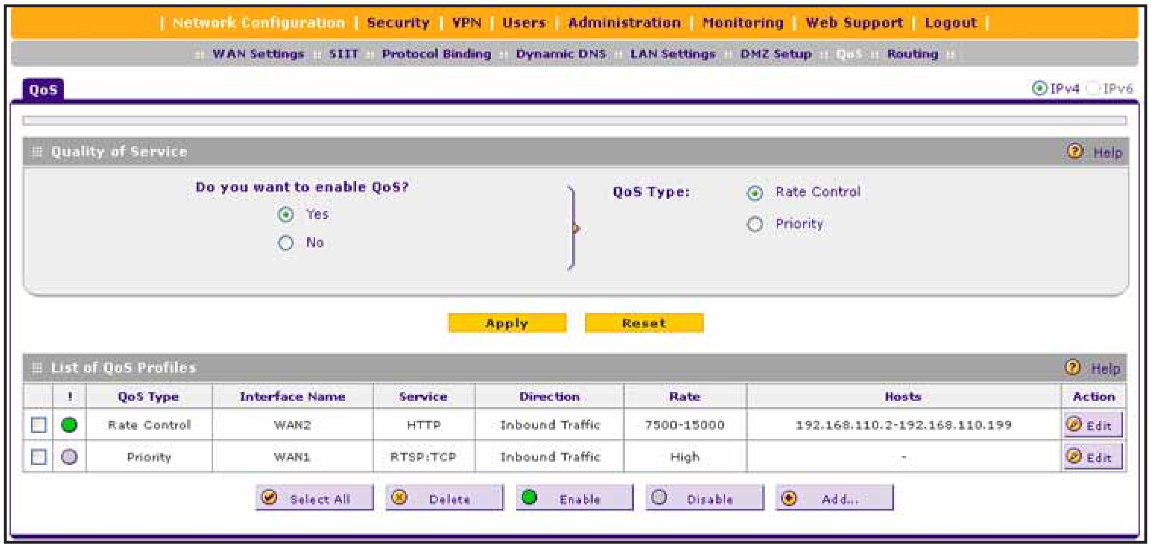
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > QoS**.

   The QoS screen displays. The following figure shows some profiles in the List of QoS Profiles table.



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

Quality of Service

Do you want to enable QoS?
● Yes
○ No

QoS Type:
● Rate Control
○ Priority

List of QoS Profiles

	!	QoS Type	Interface Name	Service	Direction	Rate	Hosts	Action
□	●	Rate Control	WAN2	HTTP	Inbound Traffic	7500-15000	192.168.110.2-192.168.110.199	Edit
□	○	Priority	WAN1	RTSP:TCP	Inbound Traffic	High	-	Edit

7. To enable QoS, select the **Yes** radio button.

   By default, the **No** radio button is selected.

8. Specify the profile type that must be active.
   - **Rate control**. All rate control QoS profiles that you configure are active, but priority QoS profiles are not.
   - **Priority**. All priority QoS profiles that you configure are active, but rate control QoS profiles are not.

9. Click the **Apply** button.

   Your settings are saved.

   The List of QoS Profiles table shows the following columns:

- **QoS Type**. The type of profile, either Rate Control or Priority.
- **Interface Name**. The WAN interface to which the profile applies (WAN1 or WAN2).
- **Service**. The service to which the profile applies.
- **Direction**. The WAN direction to which the profile applies (inbound, outbound, or both).
- **Rate**. The bandwidth rate in Kbps or the priority.
- **Hosts**. The IP address, IP addresses, or group to which the rate control profile applies. (The information in this column does not apply to priority profiles.)
- **Action**. The **Edit** button provides access to the Edit QoS screen for the corresponding profile.

For more information about the information that is shown in the List of QoS Profiles table, see *Add a Rate Control WAN QoS Profile* on page 75 and *Add a Priority Queue WAN QoS Profile* on page 78.

Change a QoS Profile

The following procedure describes how to change an existing WAN QoS profile.

➢ **To change a QoS profile:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > QoS**.

   The QoS screen displays.
7. In the List of QoS Profiles table, click the **Edit** button for the profile that you want to change.

   The Edit QoS screen displays.

8. Change the settings.

   For information about the settings, see *Add a Rate Control WAN QoS Profile* on page 75 and *Add a Priority Queue WAN QoS Profile* on page 78.

9. Click the **Apply** button.

   Your settings are saved. The modified QoS profile displays in the List of QoS Profiles table on the QoS screen.

Enable, Disable, or Remove One or More WAN QoS Profiles

The following procedure describes how to enable or disable existing WAN QoS profiles or remove WAN QoS profiles that you no longer need.

➢ **To enable, disable, or remove one or more WAN QoS profiles:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > QoS**.

   The QoS screen displays.

7. In the List of QoS Profiles table, select the check box to the left of each QoS profile that you want to remove or click the **Select All** button to select all profiles.
8. Click one of the following buttons:
   - **Enable**. Enables the selected WAN QoS profiles.

     The **!** status icons change from gray circles to green circles, indicating that the selected profiles are enabled. (By default, when you add a profile, the profile is automatically enabled.)

   - **Disable**. Disables the selected WAN QoS profiles.

The **!** status icons change from green circles to gray circles, indicating that the selected profiles are disabled.

- **Delete**. Removes the selected WAN QoS profiles.

  The selected profiles are removed from the List of QoS Profiles table.

Additional WAN-Related Configuration Tasks

If you want the ability to manage the VPN firewall remotely, enable remote management (see *Set Up Remote Management Access* on page 534). If you enable remote management, NETGEAR strongly recommends that you change your password (see *Change Passwords and Automatic Logout Period* on page 511).

As an option, you can also set up the traffic meter for each WAN interface (see *Configure and Enable the WAN IPv4 Traffic Meter* on page 558).

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

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

What to Do Next

After you complete setting up the WAN connection for the VPN firewall, you might want to address the important tasks described in the following chapters and sections before you deploy the VPN firewall in your network:

- *Chapter 3, Configure the IPv6 Internet and WAN Settings*
- *Chapter 4, Configure the IPv4 LAN Settings*
- *Configure Authentication Domains, Groups, and User Accounts* on page 488
- *Manage Digital Certificates for VPN Connections* on page 512
- *Use the IPSec VPN Wizard for Client and Gateway Configurations* on page 334
- *Chapter 9, Set Up Virtual Private Networking with SSL Connections*

3. Configure the IPv6 Internet and WAN Settings

3

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

- *Roadmap to Setting Up an IPv6 Internet Connection to Your ISP*
- *Configure the IPv6 Internet Connection and WAN Settings*
- *Manage Tunneling for IPv6 Traffic*
- *Configure Stateless IP/ICMP Translation*
- *Configure Auto-Rollover for IPv6 Interfaces*
- *Additional WAN-Related Configuration Tasks*
- *What to Do Next*

Roadmap to Setting Up an IPv6 Internet Connection to Your ISP

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

The tasks that are required to complete the Internet connection of your VPN firewall depend on whether you use an IPv4 connection, an IPv6 connection, or both to connect to your Internet service provider (ISP). For information about setting up an IPv4 connection, see *Chapter 2, Configure the IPv4 Internet and WAN Settings*.

Note: The VPN firewall supports simultaneous IPv4 and IPv6 connections. You can configure only one WAN interface for IPv6. You can configure the other WAN interface for IPv4.

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

➢ **Complete these tasks:**

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

   This task is described in *Manage the IPv6 Routing Mode* on page 88.

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

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

   - *Use a DHCPv6 Server to Configure an IPv6 Internet Connection Automatically* on page 90
   - *Manually Configure a Static IPv6 Internet Connection* on page 94
   - *Manually Configure a PPPoE IPv6 Internet Connection* on page 97

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

   These tasks are described in the following sections:

   - *Manage 6to4 Automatic Tunneling* on page 101
   - *Manage ISATAP Automatic Tunneling* on page 103

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

   This task is described in *Configure Stateless IP/ICMP Translation* on page 108.

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

   These tasks are described in *Configure Auto-Rollover for IPv6 Interfaces* on page 109.

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

   These tasks are described in *Managing Advanced WAN Options* on page 66 in *Chapter 2*.

Configure the IPv6 Internet Connection and WAN Settings

The following sections provide information about configuring the IPv6 Internet connection and WAN settings:

- *IPv6 Network*
- *Manage the IPv6 Routing Mode*
- *Use a DHCPv6 Server to Configure an IPv6 Internet Connection Automatically*
- *Manually Configure a Static IPv6 Internet Connection*
- *Manually Configure a PPPoE IPv6 Internet Connection*

IPv6 Network

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

- **Native IPv6 network**. Your network is a native IPv6 network if the VPN firewall has an IPv6 address and is connected to an IPv6 ISP and if your network consists of IPv6-only devices. However, because we are in a IPv4-to-IPv6 transition period, native IPv6 is not yet common.
- **Isolated IPv6 network**. If your network is an isolated IPv6 network that is not connected to an IPv6 ISP, you must make sure that the IPv6 packets can travel over the IPv4 Internet backbone; you do this by enabling automatic 6to4 tunneling (see *Manage 6to4 Automatic Tunneling* on page 101).
- **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 *Manage ISATAP Automatic Tunneling* on page 103).

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

After you configured the IPv6 routing mode, you must configure a WAN interface 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 Automatically* on page 90)
- Manual configuration of the network connection (see *Manually Configure a Static IPv6 Internet Connection* on page 94 or *Manually Configure a PPPoE IPv6 Internet Connection* on page 97)

Manage the IPv6 Routing Mode

By default, the VPN firewall does not support the IPv6 mode. You must enable the IPv6 routing mode.

The following sections provide information about managing the IPv6 routing mode:

- *IPv6 Routing Mode*
- *Enable the IPv6 Routing Mode*

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.

The options are as follows:

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

  Load balancing and IPv4/IPv6 mode are mutually exclusive. You can select IPv4/IPv6 mode only when one interface functions in primary WAN mode.

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

Enable the IPv6 Routing Mode

The following procedure describes how to enable the IPv6 routing mode.

- **To enable the IPv6 routing mode:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

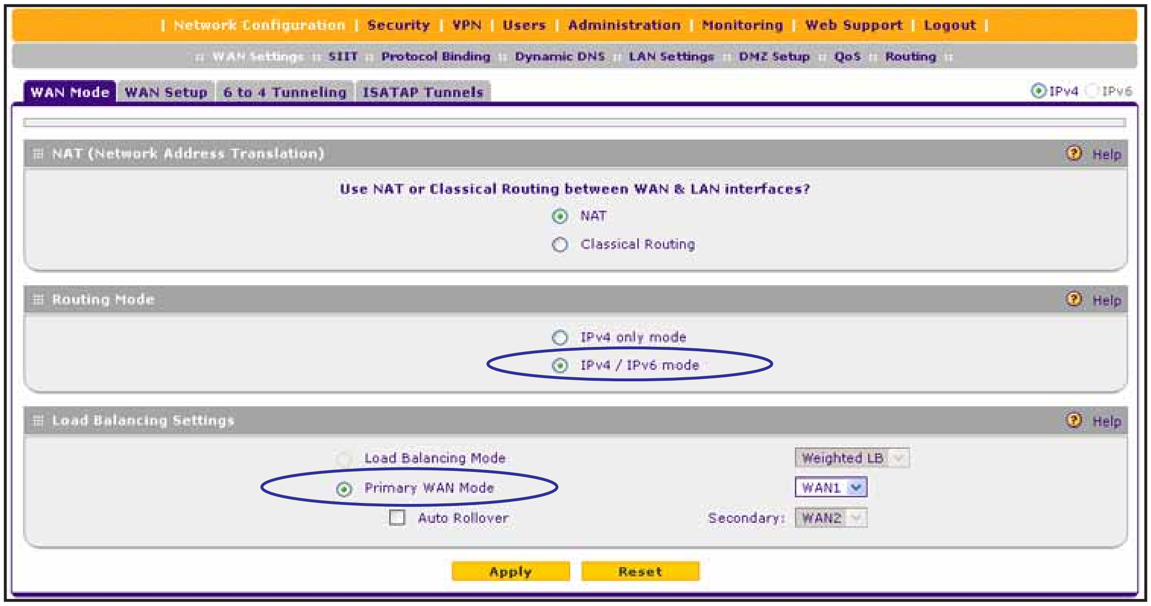
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > WAN Settings > WAN Mode**.

   The WAN Mode screen displays.


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

Load Balancing Settings

○ Load Balancing Mode | Weighted LB

● Primary WAN Mode | WAN1

□ Auto Rollover | Secondary: WAN2

7. In the Routing Mode section, 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.

8. Click the **Apply** button.

   Your settings are saved.

Use a DHCPv6 Server to Configure an IPv6 Internet Connection Automatically

A DHCPv6 server can allow the VPN firewall to autoconfigure its IPv6 Internet settings. The following sections provide information about using a DHCPv6 sever to configure an IPv6 Internet connection automatically:

- *DHCPv6 Server: Stateless and Stateful Autoconfiguration*
- *Let the VPN Firewall Automatically Configure a WAN Interface for IPv6*

DHCPv6 Server: Stateless and Stateful Autoconfiguration

The VPN firewall can autoconfigure its ISP settings through the 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 the ISP DHCPv6 server.

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

  Note: As an option for stateless address autoconfiguration, the ISP DHCPv6 server can assign a prefix through prefix delegation to the VPN firewall. Based on this ISP assignment, the VPN firewall's own stateless DHCPv6 server can assign advertisement prefixes to its IPv6 *LAN* clients through the Router Advertisement Daemon (RADVD). For more information about this LAN configuration option, see *Configure a Stateless DHCPv6 Server Without Prefix Delegation for the LAN* on page 155.

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

Let the VPN Firewall Automatically Configure a WAN Interface for IPv6

The following procedure describes how to let the VPN firewall automatically configure its IPv6 WAN addresses through a DHCPv6 server.

Note: If your ISP requires MAC authentication and another MAC address was previously registered with your ISP, you must configure that MAC address on the VPN firewall (see *Change the Advertised MAC Address of the VPN Firewall* on page 70) before you begin the following procedure.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

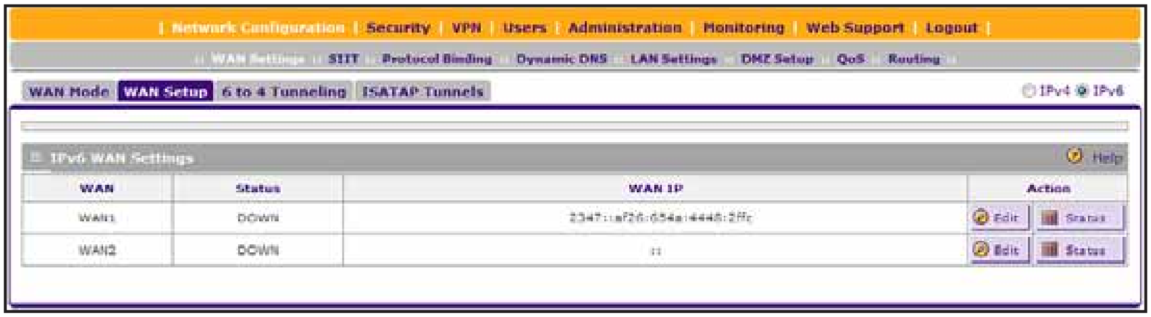
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > WAN Settings > WAN Setup**.

   The WAN Setup screen displays the IPv4 settings.
7. In the upper right, select the **IPv6** radio button.

   The WAN Setup screen displays the IPv6 settings.


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

WAN	Status	WAN IP	Action
WAN1	DOWN	2347::af26:654a:4448:2ffc	Edit Status
WAN2	DOWN	::	Edit Status

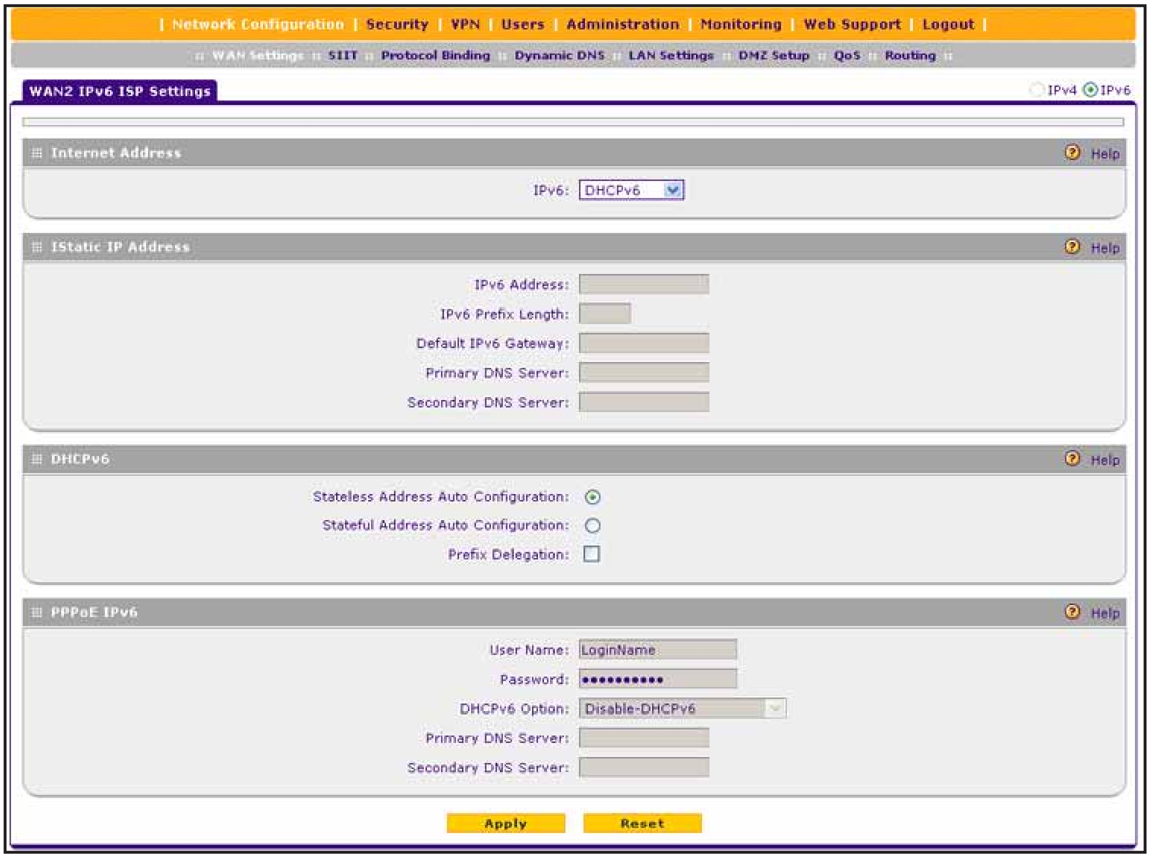
The IPv6 WAN Settings table displays the following fields:

- **WAN**. The WAN interface (WAN1 or WAN2).

- **Status**. The status of the WAN interface (UP or DOWN).
- **WAN IP**. The IPv6 address of the WAN interface.
- **Action**. The **Edit** button provides access to the WAN IPv6 ISP Settings screen (see *Step 8*) for the corresponding WAN interface; the **Status** button provides access to the Connection Status screen (see *Step 13*) for the corresponding WAN interface.

8. In the IPv6 WAN Settings table, click the **Edit** button for the WAN interface for which you want to let the VPN firewall automatically configure the connection to the Internet.

   The WAN IPv6 ISP Settings screen displays. The following figure shows the WAN2 IPv6 ISP Settings screen as an example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
WAN2 IPv6 ISP Settings
○ IPv4 ● IPv6
Help
Apply
Reset

Internet Address

IPv6: DHCPv6

IStatic 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: LoginName
Password: ••••••••••
DHCPv6 Option: Disable-DHCPv6
Primary DNS Server:
Secondary DNS Server:

9. In the Internet Address section, from the **IPv6** menu, select **DHCPv6**.
10. In the DHCPv6 section, select a radio button:
    - **Stateless Address Auto Configuration**. 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 DHCPv6 server.
    - **Stateful Address Auto Configuration**. The VPN firewall obtains an interface address, configuration information such as DNS server information, and other parameters from the ISP DHCPv6 server. The IP address is a dynamic address.
11. If you selected the **Stateless Address Auto Configuration** radio button, you can select the **Prefix Delegation** check box as described below:

- **Prefix delegation check box is selected**. A prefix is assigned by the ISP 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 through the stateless DHCPv6 server in the LAN, see *Manage a Stateless DHCPv6 Server with Prefix Delegation for the LAN* on page 158.

- **Prefix delegation check box is cleared**. Prefix delegation is disabled. This is the default setting.

12. Click the **Apply** button.

    Your settings are saved.

13. Verify the connection:

    a. Select **Network Configuration > WAN Settings > WAN Setup**.

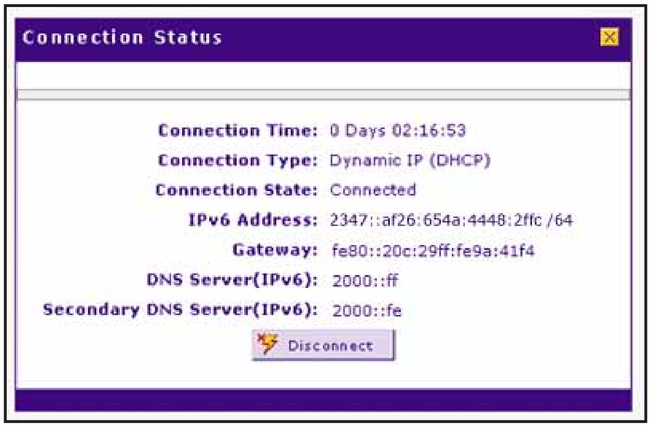
       The WAN Setup screen displays the IPv4 settings.

    b. In the upper right, select the **IPv6** radio button.

       The WAN Setup screen displays the IPv6 settings (see the figure that is shown in *Step 7*).

    c. In the IPv6 WAN Settings table, click the **Status** button for the WAN interface for which you want to display the connection status.

       The Connection Status pop-up screen displays. The following figure shows a dynamic IP address configuration.



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

The Connection Status screen shows a valid IP address and gateway. You are connected to the Internet. For more information about the connection status, see *View the WAN Port Status and Terminate or Establish the Internet Connection* on page 594.

If the configuration was not successful, try to manually configure the connection. For more information, see the following sections:

- *Manually Configure a Static IPv6 Internet Connection* on page 94
- *Manually Configure a PPPoE IPv6 Internet Connection* on page 97

Manually Configure a Static IPv6 Internet Connection

To configure a static IPv6 Internet connection, enter the IPv6 address information that your IPv6 ISP gave you. If you do not have this information, contact your IPv6 ISP.

Note: If your ISP requires MAC authentication and another MAC address was previously registered with your ISP, you must configure that MAC address on the VPN firewall (see *Change the Advertised MAC Address of the VPN Firewall* on page 70) before you begin the following procedure.

➢ **To manually configure a static IPv6 Internet connection for a WAN interface:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

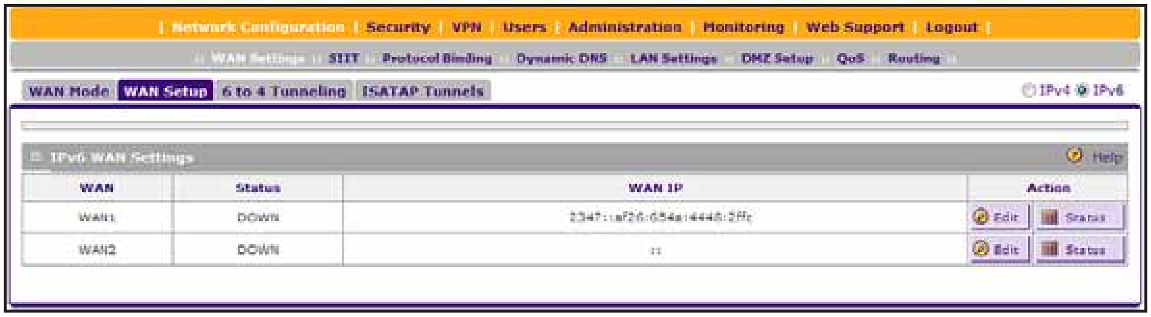
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > WAN Settings > WAN Setup**.

   The WAN Setup screen displays the IPv4 settings.
7. In the upper right, select the **IPv6** radio button.

   The WAN Setup screen displays the IPv6 settings.

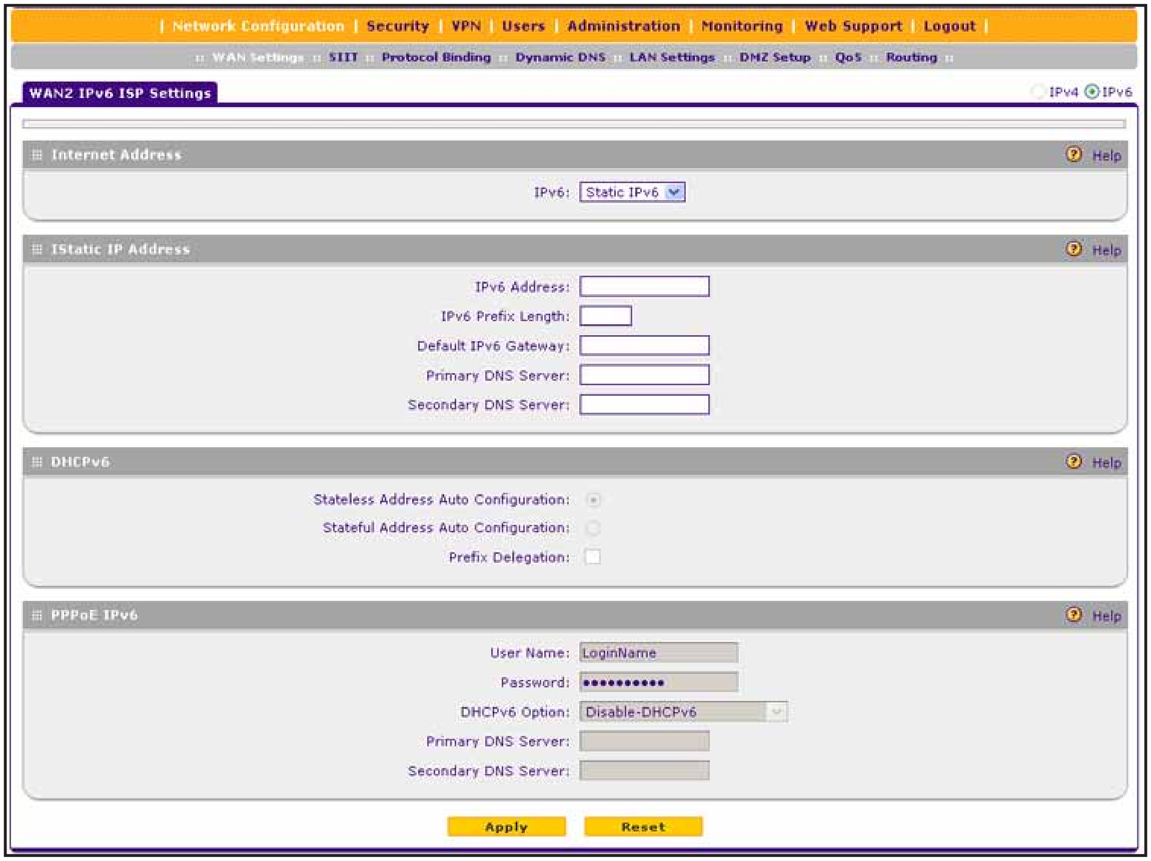

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
WAN Mode
WAN Setup
6 to 4 Tunneling
ISATAP Tunnels
○ IPv4 ● IPv6
Help
Edit
Status

IPv6 WAN Settings

WAN	Status	WAN IP	Action
WAN1	DOWN	2347::af26:654a:4448:2ffc	Edit Status
WAN2	DOWN	::	Edit Status

8. In the IPv6 WAN Settings table, click the **Edit** button for the WAN interface that you want to configure.

   The WAN IPv6 ISP Settings screen displays. The following figure shows the WAN2 IPv6 ISP Settings screen as an example.


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

WAN2 IPv6 ISP Settings

Internet Address

IPv6: Static IPv6

IStatic 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: LoginName
Password: ●●●●●●●●●●●
DHCPv6 Option: Disable-DHCPv6
Primary DNS Server:
Secondary DNS Server:

9. In the Internet Address section, from the **IPv6** menu, select **Static IPv6**.
10. In the Static IP Address section, enter the settings as described in the following table.

Note: If you do not know your static IPv6 address information, contact your IPv6 ISP.

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.

11. Click the **Apply** button.

    Your settings are saved.

12. Verify the connection:

    a. Select **Network Configuration > WAN Settings > WAN Setup**.

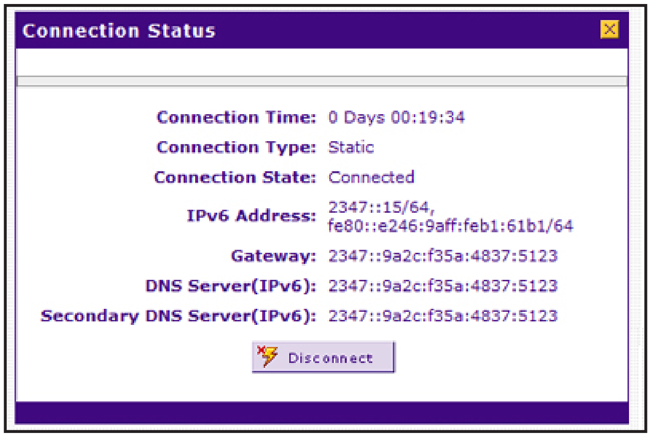
       The WAN Setup screen displays the IPv4 settings.

    b. In the upper right, select the **IPv6** radio button.

       The WAN Setup screen displays the IPv6 settings (see the figure that is shown in *Step 7*).

    c. In the IPv6 WAN Settings table, click the **Status** button for the WAN interface for which you want to display the connection status.

       The Connection Status pop-up screen displays. The following figure shows a static IP address configuration. The IP addresses that are shown in this figure are not related to any other examples in this manual.



Connection Time: 0 Days 00:19:34
Connection Type: Static
Connection State: Connected
IPv6 Address: 2347::15/64, fe80::e246:9aff:feb1:61b1/64
Gateway: 2347::9a2c:f35a:4837:5123
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. You are connected to the Internet. For more information about the connections status, see *View the WAN Port Status and Terminate or Establish the Internet Connection* on page 594.

Note: If the configuration was not successful, see *Troubleshoot the ISP Connection* on page 615.

Manually Configure a PPPoE IPv6 Internet Connection

To configure a PPPoE IPv6 Internet connection, enter the PPPoE IPv6 information that your IPv6 ISP gave you. If you do not have this information, contact your IPv6 ISP.

Note: If your ISP requires MAC authentication and another MAC address was previously registered with your ISP, you must configure that MAC address on the VPN firewall (see *Change the Advertised MAC Address of the VPN Firewall* on page 70) before you begin the following procedure.

➢ **To manually configure a PPPoE IPv6 Internet connection for a WAN interface:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

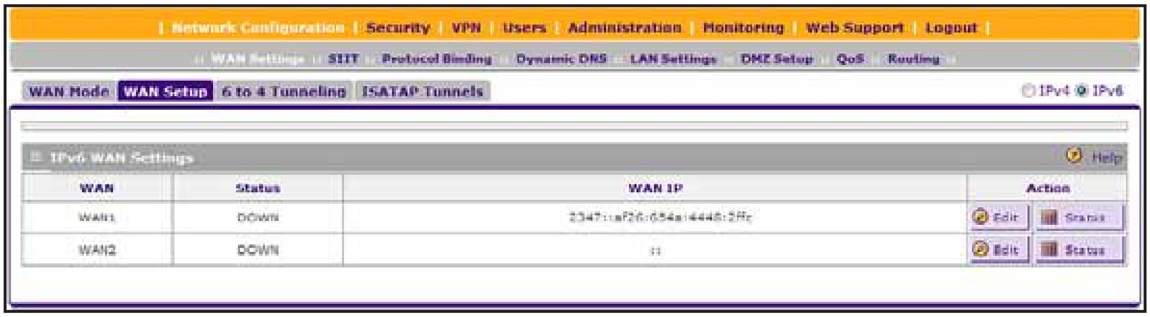
   The Router Status screen displays.

6. Select **Network Configuration > WAN Settings > WAN Setup**.

   The WAN Setup screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The WAN Setup screen displays the IPv6 settings.

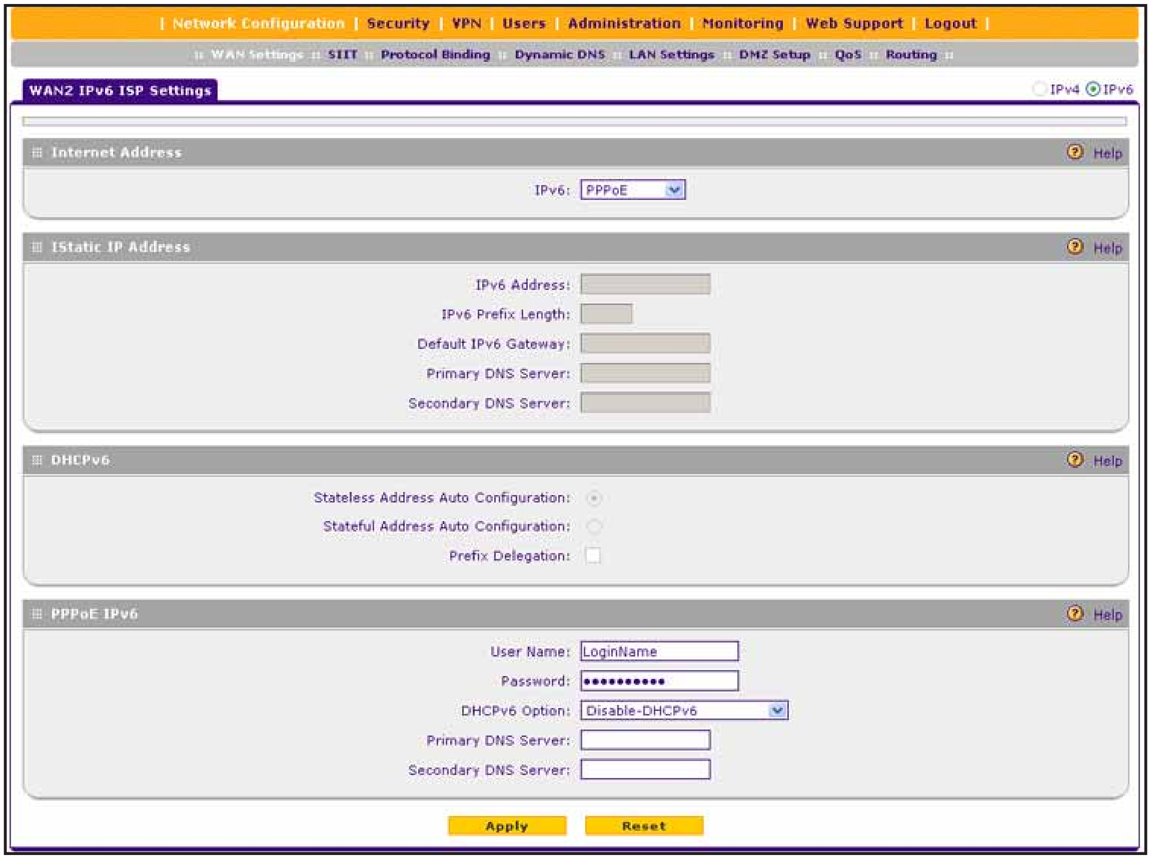

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
WAN Mode
WAN Setup
6 to 4 Tunneling
ISATAP Tunnels
○ IPv4 ● IPv6
Help

IPv6 WAN Settings

WAN	Status	WAN IP	Action
WAN1	DOWN	2347::af26:654a:4448:2ffc	Edit Status
WAN2	DOWN	::	Edit Status

8. In the IPv6 WAN Settings table, click the **Edit** button for the WAN interface that you want to configure.

   The WAN IPv6 ISP Settings screen displays. The following figure shows the WAN2 IPv6 ISP Settings screen as an example.


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

WAN2 IPv6 ISP Settings

○ IPv4 ● IPv6

Internet Address

IPv6: PPPoE

IStatic 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: LoginName
Password: ●●●●●●●●●●●
DHCPv6 Option: Disable-DHCPv6
Primary DNS Server:
Secondary DNS Server:

9. In the Internet Address section, from the **IPv6** menu, select **PPPoE**.
10. In the PPPoE IPv6 section, enter the settings as described in the following table.

Note: If you do not know your PPPoE IPv6 information, contact your IPv6 ISP.

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

Setting	Description
DHCPv6 Option	From the **DHCPv6 Optio**n menu, select a DHCPv6 server option, 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 WAN address by using a combination of locally available information and router advertisements but receives DNS server information from the ISP DHCPv6 server. Router advertisements include a prefix that identifies the subnet that is associated with the WAN port. The IP address is formed by combining this prefix and the MAC address of the WAN port. The IP address is a dynamic address. • **DHCPv6 StatefulMode**. The VPN firewall obtains an interface address, configuration information such as DNS server information, and other parameters from the ISP's DHCPv6 server. The IP address is a dynamic address. • **DHCPv6 Prefix Delegation**. The VPN firewall obtains a prefix from the ISP 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 to IPv6 LAN clients, see *Manage a Stateless DHCPv6 Server with Prefix Delegation for the LAN* on page 158.
Primary DNS Server	If you selected **Disable-DHCPv6** from the **DHCPv6 Options** menu, the IPv6 IP address of the ISP primary DNS server.
Secondary DNS Server	If you selected the **Disable-DHCPv6** from the **DHCPv6 Options** menu, the IPv6 IP address of the ISP secondary DNS server.

11. Click the **Apply** button.

    Your settings are saved.

12. Verify the connection:

    a. Select **Network Configuration > WAN Settings > WAN Setup**.

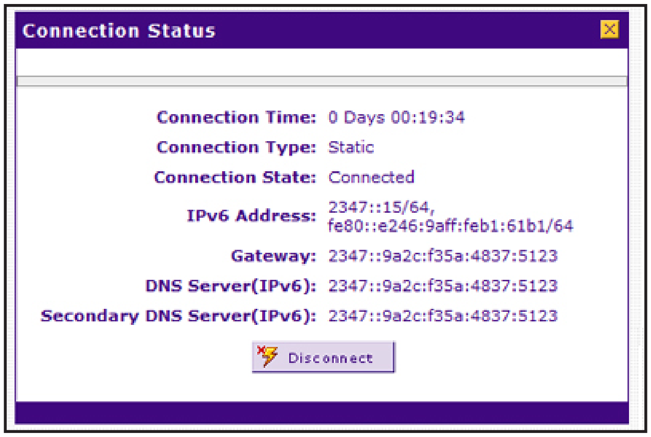
       The WAN Setup screen displays the IPv4 settings.

    b. In the upper right, select the **IPv6** radio button.

       The WAN Setup screen displays the IPv6 settings (see the figure that is shown in *Step 7*).

    c. In the IPv6 WAN Settings table, click the **Status** button for the WAN interface for which you want to display the connection status.

       The Connection Status pop-up screen displays. The following figure shows a static IP address configuration, but the screen for PPPoE is similar. The IP addresses that are shown in this figure are not related to any other examples in this manual.



Connection Status

Connection Time: 0 Days 00:19:34

Connection Type: Static

Connection State: Connected

IPv6 Address: 2347::15/64,
fe80::e246:9aff:feb1:61b1/64

Gateway: 2347::9a2c:f35a:4837:5123

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. You are connected to the Internet. For more information about the connection status, see *View the WAN Port Status and Terminate or Establish the Internet Connection* on page 594.

Note: If the configuration was not successful, see *Troubleshoot the ISP Connection* on page 615.

Manage Tunneling for IPv6 Traffic

The following sections provide information about managing tunneling for IPv6 traffic:

- *Manage 6to4 Automatic Tunneling*
- *Manage ISATAP Automatic Tunneling*
- *View the Tunnel Status and Tunnel IPv6 Addresses*

Manage 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.

The following sections provide information about managing 6to4 automatic tunneling:

- *6to4 Tunnel*
- *Enable 6to4 Automatic Tunneling*

6to4 Tunnel

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.

Note: If the VPN firewall functions as the endpoint for 6to4 tunnels in your network, make sure that the VPN firewall has a static IPv4 address (see *Manually Configure a Static IPv4 Internet Connection* on page 36). A dynamic IPv4 address can cause routing problems on the 6to4 tunnels.

Note: If you do not use a stateful DHCPv6 server in your LAN, you 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 153.

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 Tunnel IPv6 Addresses* on page 107).

Enable 6to4 Automatic Tunneling

The following procedure describes how to enable 6to4 automatic tunneling.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

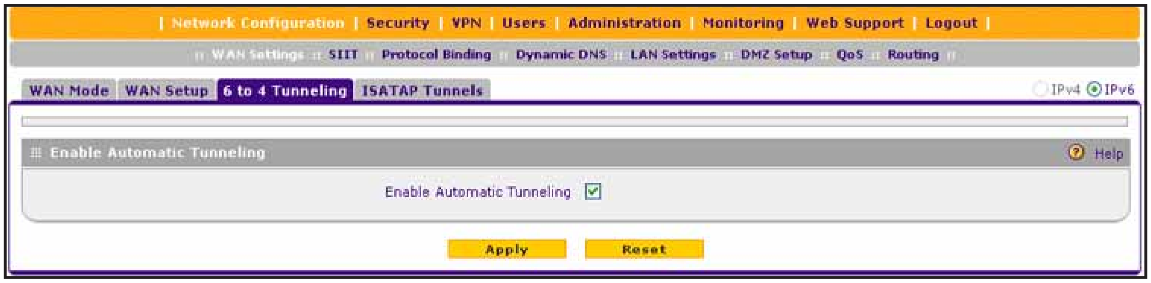
If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

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

   The 6 to 4 Tunneling screen displays.


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

Enable Automatic Tunneling ☑

7. Select the **Enable Automatic Tunneling** check box.
8. Click the **Apply** button.

   Your settings are saved.

Manage 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.

The following sections provide information about managing ISATAP automatic tunneling:

- *ISATAP Tunnel*
- *Configure an ISATAP Tunnel*
- *Change an ISATAP Tunnel*
- *Remove One or More ISATAP Tunnels*

ISATAP Tunnel

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 intrasite, that is, between addresses in the LAN. For more information about link-local addresses, see *Manage the IPv6 LAN* on page 153.

Note: 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 153.

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.

Configure an ISATAP Tunnel

The following procedure describes how to configure an ISATAP tunnel.

➤ **To configure an ISATAP tunnel:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

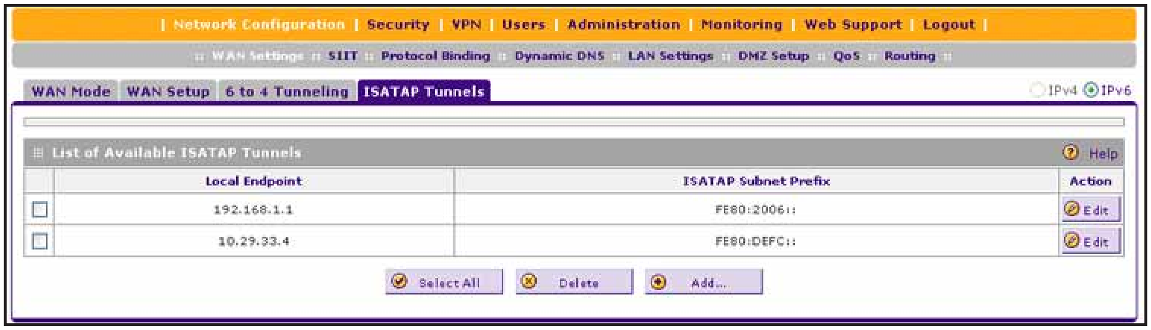
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > WAN Settings > ISATAP Tunnels**.

   The ISATAP Tunnels screen displays. The following figure shows some examples.

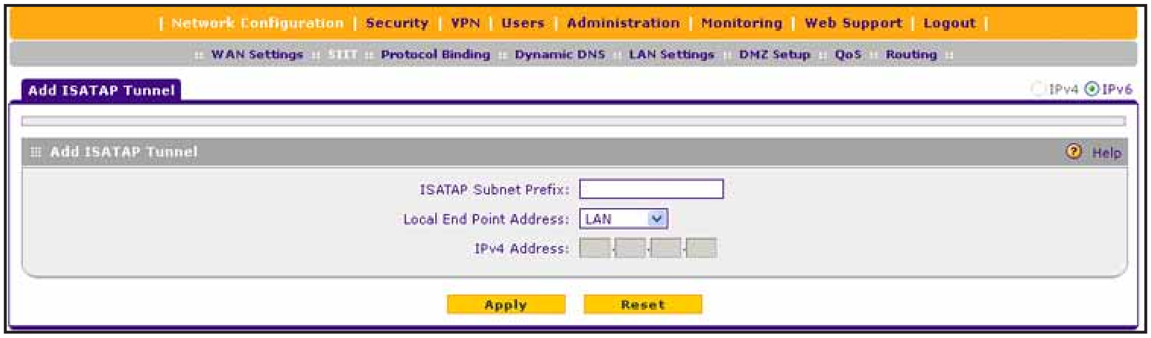

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
WAN Mode
WAN Setup
6 to 4 Tunneling
ISATAP Tunnels
○ IPv4 ● IPv6
Help
Select All
Delete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

List of Available ISATAP Tunnels

	Local Endpoint	ISATAP Subnet Prefix	Action
□	192.168.1.1	FE80:2006::	Edit
□	10.29.33.4	FE80:DEFC::	Edit

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

   The Add ISATAP Tunnel screen displays.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: 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:

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

Setting	Description
ISATAP Subnet Prefix	The IPv6 prefix for the tunnel.
Local End Point Address	From the menu, 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** menu, enter the IPv4 address.

9. Click the **Apply** button.

   Your settings are saved. The tunnel is added to the List of Available ISATAP Tunnels table on the ISATAP Tunnels screen.

Change an ISATAP Tunnel

The following procedure describes how to change an existing ISATAP tunnel.

➢ **To change an ISATAP tunnel:**

1. On your computer, launch an Internet browser.

2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

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

   The ISATAP Tunnels screen displays.

7. In the List of Available ISATAP tunnels table, click the **Edit** button for the tunnel that you want to change.

   The Edit ISATAP Tunnel screen displays.

8. Change the settings.

   For more information about the settings, see *Configure an ISATAP Tunnel* on page 104.

9. Click the **Apply** button.

   Your settings are saved. The modified tunnel settings display in the List of Available ISATAP Tunnels table on the ISATAP Tunnels screen.

Remove One or More ISATAP Tunnels

The following procedure describes how to remove one or more ISATAP tunnels that you no longer need.

➢ **To remove one or more ISATAP tunnels:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

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

   The ISATAP Tunnels screen displays.

7. In the List of Available ISATAP Tunnels table, select the check box to the left of each tunnel that you want to remove or click the **Select All** button to select all tunnels.
8. Click the **Delete** button.

   The selected tunnels are removed from the List of Available ISATAP Tunnels table.

View the Tunnel Status and Tunnel IPv6 Addresses

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. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

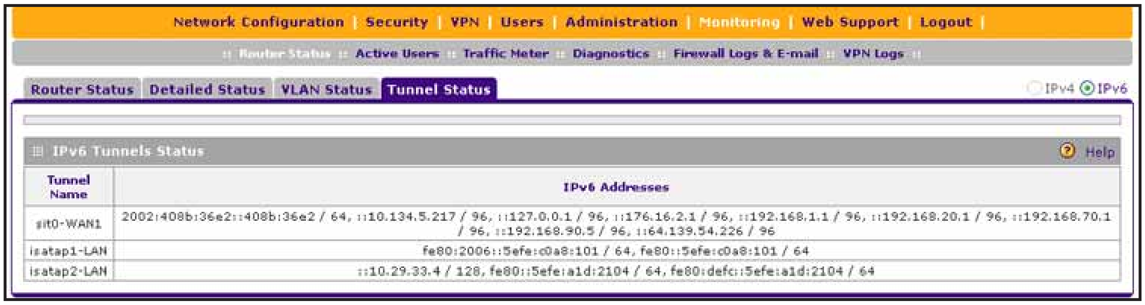
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

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

   The Tunnel Status screen displays.


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

IPv6 Tunnels Status

Tunnel Name	IPv6 Addresses
sit0-WAN1	2002:408b:36e2::408b:36e2 / 64, ::10.134.5.217 / 96, ::127.0.0.1 / 96, ::176.16.2.1 / 96, ::192.168.1.1 / 96, ::192.168.20.1 / 96, ::192.168.70.1 / 96, ::192.168.90.5 / 96, ::64.139.54.226 / 96
isatap1-LAN	fe80:2006::5efe:c0a8:101 / 64, fe80::5efe:c0a8:101 / 64
isatap2-LAN	::10.29.33.4 / 128, fe80::5efe:a1d:2104 / 64, fe80:defc::5efe:a1d:2104 / 64

The IPv6 Tunnel Status table shows the following fields:

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

Configure Stateless IP/ICMP Translation

The following sections provide information about Stateless IP/ICMP Translation:

- *Stateless IP/ICMP Translation*
- *Configure Stateless IP/ICMP Translation*

Stateless IP/ICMP Translation

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

SIIT functions with IPv4-translated addresses, which are addresses of the format 0::ffff:0:0:0/96 for IPv6-enabled devices. You can substitute an IPv4 address in the format a.b.c.d for part of the IPv6 address so that the IPv4-translated address becomes 0::ffff:0:a.b.c.d/96.

For SIIT to function, the routing mode must be IPv4/IPv6. NETGEAR’s implementation of SIIT lets you configure a single IPv4 address. 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.

Configure Stateless IP/ICMP Translation

For SIIT to function, the routing mode must be IPv4/IPv6 (see *Manage the IPv6 Routing Mode* on page 88). The following procedure describes how to configure SIIT.

➢ **To configure SIIT:**

1. On your computer, launch an Internet browser.

2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

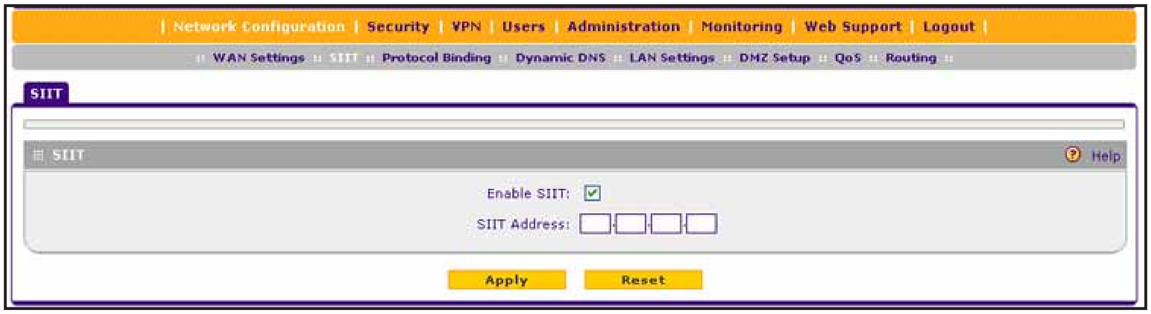
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > SIIT**.

   The SIIT screen displays.



Enable SIIT: ☑

SIIT Address: □.□.□.□

7. Select the **Enable SIIT** check box.
8. In the **SIIT Address** fields, enter the IPv4 address that must be used in the IPv4-translated address for IPv6 devices.
9. Click the **Apply** button.

   Your settings are saved.

Configure Auto-Rollover for IPv6 Interfaces

The following sections provide information about configuring auto-rollover for IPv6 interfaces:

- *Auto-Rollover for IPv6 WAN Interfaces*
- *Configure Auto-Rollover Mode for IPv6 WAN Interfaces*
- *Configure the Failure Detection Method for IPv6 WAN Interfaces*

Auto-Rollover for IPv6 WAN Interfaces

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

The VPN firewall supports the following modes for IPv6 interfaces:

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

  If you want to use a redundant ISP link for backup purposes, select the WAN port that must function as the primary link for this mode. Ensure that you also configure the backup WAN port and that you configure the WAN failure detection method to support auto-rollover.

Note: If the VPN firewall functions in IPv4/IPv6 mode, you cannot configure load balancing. For information about IPv4/IPv6 mode, see *Manage the IPv6 Routing Mode* on page 88.

To use a redundant ISP link for backup purposes, ensure that the backup WAN interface is configured. Then select the WAN interface that must function as the primary link for this mode and configure the WAN failure detection method to support auto-rollover.

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

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

Configure Auto-Rollover Mode for IPv6 WAN Interfaces

The following procedure describes how you can configure auto-rollover mode for IPv6 WAN interfaces.

➢ **To configure auto-rollover mode for IPv6 WAN interfaces:**

1. On your computer, launch an Internet browser.

2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

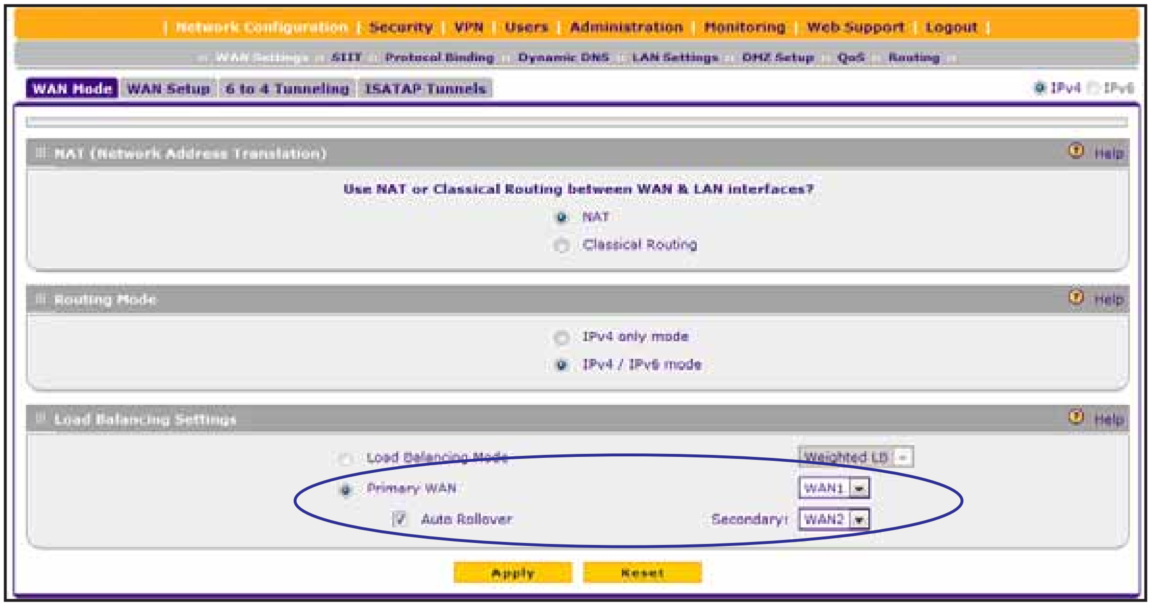
5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > WAN Settings > WAN Mode**.

   The WAN Mode screen displays.

   Note: The **IPv6** radio button is disabled. However, you can configure auto-rollover mode for IPv6 interfaces with the **IPv4** radio button selected.


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

Load Balancing Settings

○ Load Balancing Mode Weighted LB

● Primary WAN WAN1

☑ Auto Rollover Secondary: WAN2

7. In the Load Balancing Settings section, configure the following settings:

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

   b. From the corresponding menu on the right, select a WAN interface to function as the primary WAN interface.

The other WAN interface becomes disabled.

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

d. From the corresponding menu on the right, select a WAN interface to function as the backup WAN interface.

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

8. Click the **Apply** button.

   Your settings are saved.

Configure the Failure Detection Method for IPv6 WAN Interfaces

The following procedure describes how to configure the failure detection method for IPv6 WAN interfaces that function in auto-rollover mode.

➢ **To configure the failure detection method for IPv6 WAN interfaces:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > WAN Settings > WAN Setup**.

   The WAN Setup screen displays the IPv4 settings.
7. In the upper right, select the **IPv6** radio button.

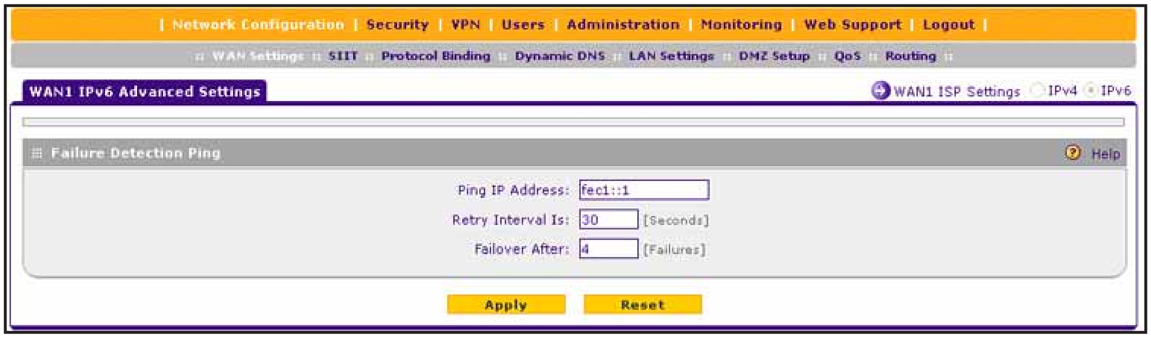
   The WAN Setup screen displays the IPv6 settings.

8. In the IPv6 WAN Settings table, click the **Edit** button for the WAN interface that you selected as the primary WAN interface.

   The WAN IPv6 ISP Settings screen displays.

9. Click the **Advanced** option arrow in the upper right.

   The WAN IPv6 Advanced Settings screen displays for the WAN interface that you selected.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
WAN1 IPv6 Advanced Settings
WAN1 ISP Settings ○ IPv4 ● IPv6
Failure Detection Ping
Help
Apply
Reset

Ping IP Address: fec1::1

Retry Interval Is: 30 [Seconds]

Failover After: 4 [Failures]

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

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

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

11. Click the **Apply** button.

    Your settings are saved.

Note: You can configure the VPN firewall to generate a WAN status log and email this log to a specified address (see *Manage Logging, Alerts, and Event Notifications* on page 567).

Additional WAN-Related Configuration Tasks

If you want the ability to manage the VPN firewall remotely, enable remote management (see *Set Up Remote Management Access* on page 534). If you enable remote management, NETGEAR strongly recommends that you change your password (see *Change Passwords and Automatic Logout Period* on page 511).

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

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

What to Do Next

After you complete setting up the IPv6 WAN connection for the VPN firewall, the important tasks that are described in the following chapter and sections you might want to address before you deploy the VPN firewall in your network:

- *Chapter 2, Configure the IPv4 Internet and WAN Settings*
- *Chapter 4, Configure the IPv4 LAN Settings*
- *Configure Authentication Domains, Groups, and User Accounts* on page 488
- *Manage Digital Certificates for VPN Connections* on page 512
- *Use the IPSec VPN Wizard for Client and Gateway Configurations* on page 334
- *Chapter 9, Set Up Virtual Private Networking with SSL Connections*

Configure the IPv4 LAN Settings

4

This chapter describes how to configure the IPv4 LAN features of your VPN firewall. The chapter contains the following sections:

Manage IPv4 Virtual LANs and DHCP Options

The following sections provide information about managing IPv4 VLANs and DHCP options:

- *IPv4 LANs and VLANs*
- *Port-Based VLANs*
- *Assign VLAN Profiles*
- *VLAN DHCP*
- *Manage VLAN Profiles*
- *Configure Unique VLAN MAC Addresses*
- *Disable the Broadcast of ARP Packets for the Default VLAN*

IPv4 LANs and VLANs

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 has set up the VLANs.

VLANs have a number of advantages:

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

Port-Based VLANs

The VPN firewall supports port-based VLANs. Port-based VLANs confine broadcast traffic to the LAN ports.

Even though a LAN port can be a member of more than one VLAN, the port can have only one VLAN ID as its port VLAN identifier (PVID). By default, all four LAN ports of the VPN firewall are assigned to the default VLAN, or VLAN 1. Therefore, by default, all four LAN ports have the default PVID 1. However, you can assign another PVID to a LAN port (see *Assign VLAN Profiles* on page 116).

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

You cannot remove the VPN firewall's default VLAN. All untagged traffic is routed through the default VLAN (VLAN 1), 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.

In a typical scenario for a configuration with an IP phone that has two Ethernet ports, one port is connected to the VPN firewall, and 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.

Assign VLAN Profiles

The following procedure describes how to assign existing VLAN profiles (which includes the default VLAN) to LAN ports.

➤ **To assign VLAN profiles to LAN ports:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

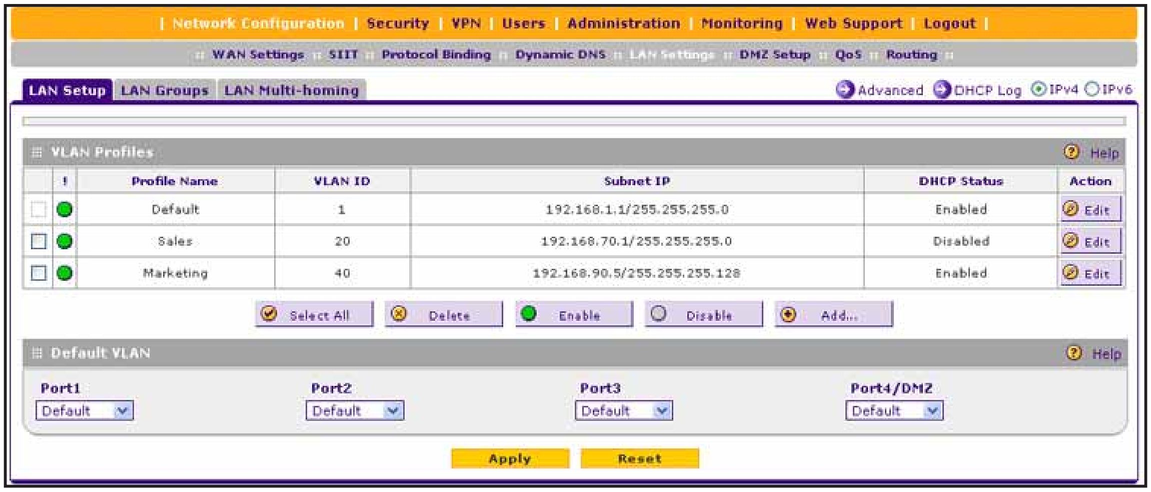
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > LAN Settings**.

   The LAN submenu tabs display, with the LAN Setup screen in view, displaying the IPv4 settings. The following figure shows some VLAN profiles as an example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: 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

VLAN Profiles

	!	Profile Name	VLAN ID	Subnet IP	DHCP Status	Action
□	●	Default	1	192.168.1.1/255.255.255.0	Enabled	Edit
□	●	Sales	20	192.168.70.1/255.255.255.0	Disabled	Edit
□	●	Marketing	40	192.168.90.5/255.255.255.128	Enabled	Edit

Default VLAN

Port1	Port2	Port3	Port4/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** button, which provides access to the Edit VLAN Profile screen.

7. In the Default VLAN section, assign a VLAN profile to a LAN port by selecting a VLAN profile from a port menu.

   The enabled VLAN profile displays in the menu.

8. To assign a VLAN profile to another LAN port, repeat *Step 7*.
9. Click the **Apply** button.

   Your settings are saved.

Note: After you assign an active VLAN profile to LAN ports, all outbound traffic is allowed and all inbound traffic is discarded except responses to requests from the LAN side. For information about how to change these default traffic rules, see *Chapter 6, Customize Firewall Protection*.

VLAN DHCP

For each VLAN, you must specify the Dynamic Host Configuration Protocol (DHCP) options (see *Manage VLAN Profiles* on page 119).

For information about configuring the DHCP options for the VPN firewall’s default VLAN, or VLAN 1, see *Configure the IPv4 Internet Connection and WAN Settings* on page 30.

The following sections provide information about VLAN DHCP concepts:

- *DHCP Servers*
- *DHCP Relay*
- *DNS Proxy*
- *LDAP Servers*

DHCP Servers

The default VLAN (VLAN 1) has the DHCP server option enabled by default, allowing the VPN firewall to assign IP, DNS server, WINS server, and default gateway addresses to all computers connected to the VPN firewall’s LAN. The assigned default gateway address is the LAN address of the VPN firewall. IP addresses are assigned to the attached computers from a pool of addresses that you 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 define
- 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 configure a WINS server for the DHCP server)
- 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. These are the DNS servers that the VPN firewall detected during the automatic configuration of the IPv4 Internet connection or that you configured manually for the WAN interfaces (see *Configure the IPv4 Internet Connection and WAN Settings* on page 30).

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 Servers

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.

Manage VLAN Profiles

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.

Note: For information about how to manage VLANs, see *Port-Based VLANs* on page 116.

The following sections provide information about managing VLAN profiles:

- *Add a VLAN Profile*
- *Change a VLAN Profile*
- *Enable, Disable, or Delete Existing VLAN Profiles*

Add a VLAN Profile

The following procedure describes how to add a VLAN profile with an IP address, associate ports with the VLAN profile, and configure optional settings such as DHCP settings, a DNS proxy, and inter-VLAN routing.

➢ **To add a VLAN profile:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

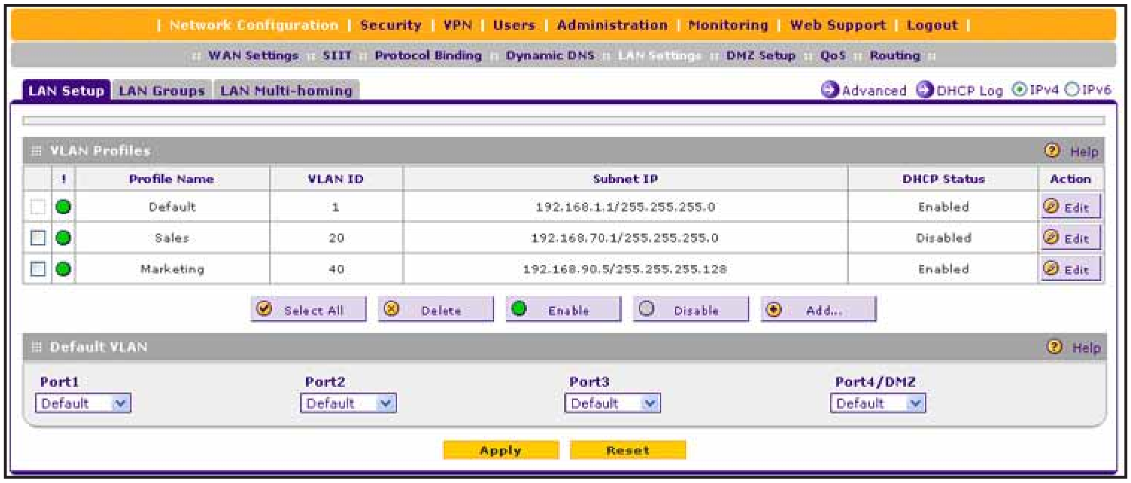
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > LAN Settings**.

   The LAN submenu tabs display, with the LAN Setup screen in view, displaying the IPv4 settings. The following figure contains some VLAN profiles as an example.

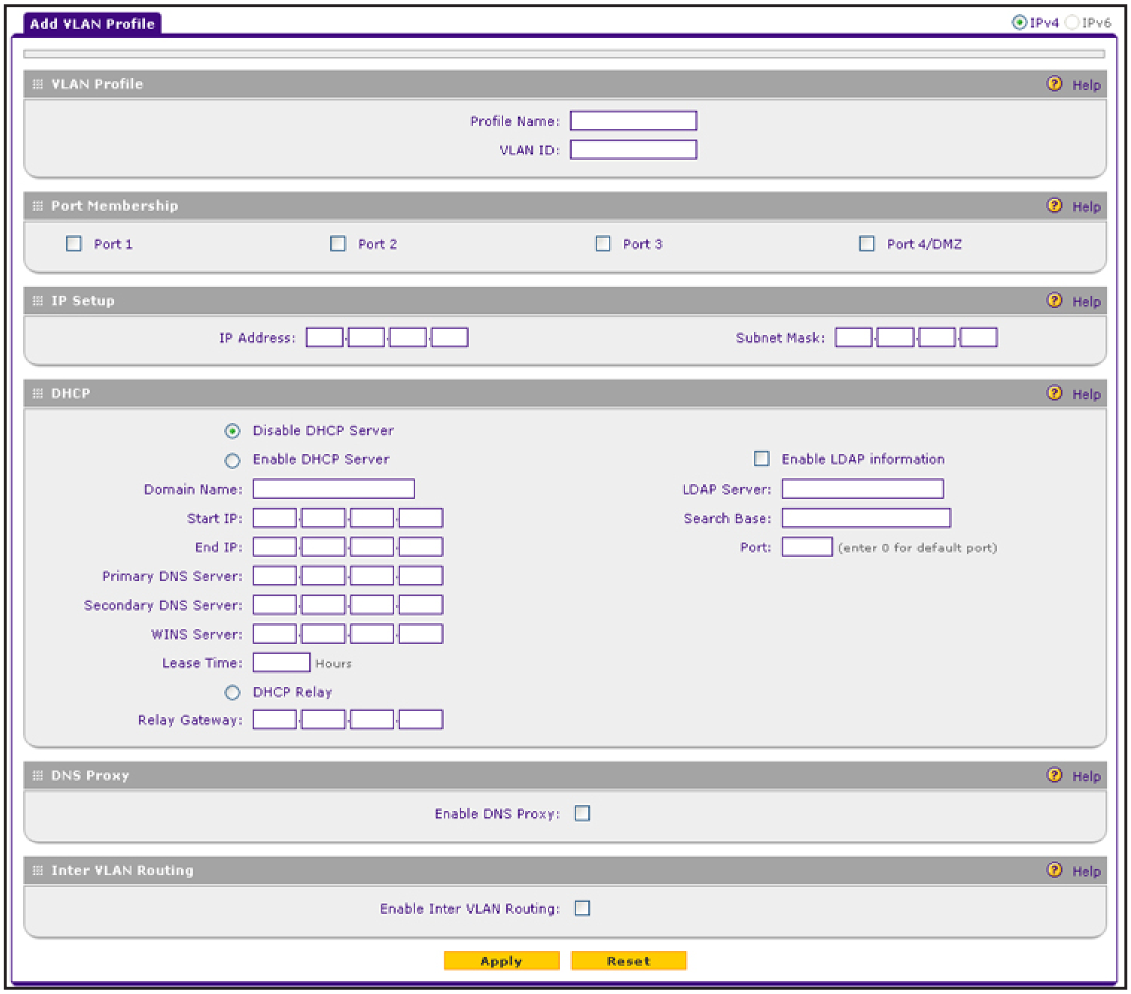

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
LAN Setup
LAN Groups
LAN Multi-homing
Advanced
DHCP Log
● IPv4 ○ IPv6
VLAN Profiles
Help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

	!	Profile Name	VLAN ID	Subnet IP	DHCP Status	Action
□	●	Default	1	192.168.1.1/255.255.255.0	Enabled	Edit
□	●	Sales	20	192.168.70.1/255.255.255.0	Disabled	Edit
□	●	Marketing	40	192.168.90.5/255.255.255.128	Enabled	Edit

Port1	Port2	Port3	Port4/DMZ
Default	Default	Default	Default

7. Click the **Add** button.

The Add VLAN Profile screen displays.



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

Setting	Description
VLAN Profile	
Profile Name	Enter a unique name for the VLAN profile.
VLAN ID	Enter a unique ID number for the VLAN profile. No two VLANs can have the same VLAN ID number. **Note:** You can enter VLAN IDs from 2 to 4089. VLAN ID 1 is reserved for the default VLAN; VLAN ID 4094 is reserved for the DMZ interface.
Port Membership	
Port 1, Port 2, Port 3, Port 4 / 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 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	
Select one of the following radio buttons: • **Disable DHCP Server**. If another device in the LAN functions as the Dynamic Host Configuration Protocol (DHCP) server for the VLAN, or if you intend to manually configure the network settings of all computers in the VLAN, 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. • **Enable DHCP Server**. To enable the VPN firewall to function as the DHCP server for the VLAN, select the **Enable DHCP Server** radio button. (For the default VLAN, the DHCP server is enabled by default.) Complete the **Start IP Address**, **End IP Address**, and **Lease Time** fields. The **Domain Name**, **Primary DNS Server**, **Secondary DNS Server**, and **WINS Server** fields are optional, as is the **Enable LDAP information** check box and associated fields. • **DHCP Relay**. To use a DHCP server somewhere else in your network as the DHCP server for the VLAN, select the **DHCP Relay** radio button. In the **Relay Gateway** field, enter the IP address of the DHCP server.	

Setting	Description
Domain Name	This setting is optional. Enter the domain name of the VPN firewall.
Start IP Address	Enter the start IP address. This address specifies the first of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address between this address and the end IP address. For the default VLAN, the default start IP address is 192.168.1.100.
End IP Address	Enter the end IP address. This address specifies the last of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN is assigned an IP address between the start IP address and this IP address. For the default VLAN, the default end IP address is 192.168.1.254. The start and end DHCP IP addresses 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.
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, enter the following objects: 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:** If you clear the **Enable DNS Proxy** check box for the VLAN, all computers in the VLAN receive the DNS IP addresses of the ISP but without the DNS proxy IP address.

Setting	Description
Inter VLAN Routing	
Enable Inter VLAN Routing	This setting is optional. To ensure that traffic is routed only to VLANs for which inter-VLAN routing is enabled, select the **Enable Inter VLAN Routing** check box. This feature is disabled by default. When you clear the **Enable Inter VLAN Routing** check box, traffic from this VLAN is not routed to other VLANs, and traffic from other VLANs is not routed to this VLAN.

9. Click the **Apply** button.

   Your settings are saved.

Change a VLAN Profile

The following procedure describes how to change an existing VLAN profile.

➢ **To change a VLAN profile:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > LAN Settings**.

   The LAN submenu tabs display, with the LAN Setup screen in view, displaying the IPv4 settings.
7. In the VLAN profiles table, click the **Edit** button for the VLAN profile that you want to change.

   The Edit VLAN Profile screen displays.
8. Change the settings.

   For information about the settings, see *Add a VLAN Profile* on page 120.

9. Click the **Apply** button.

   Your settings are saved. The modified VLAN profile displays in the VLAN Profiles table on the LAN Setup screen.

Enable, Disable, or Delete Existing VLAN Profiles

The following procedure describes how to enable or disable existing VLAN profiles or remove VLAN profiles that you no longer need.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > LAN Settings**.

   The LAN submenu tabs display, with the LAN Setup screen in view, displaying the IPv4 settings.
7. In the VLAN Profiles table, select the check box to the left of each VLAN profile that you want to enable, disable, or remove or click the **Select All** button to select all profiles.

   Note: You cannot select the default VLAN profile, that is, you cannot disable or remove the default VLAN profile.
8. Click one of the following buttons:
   - **Enable**. Enables the selected VLAN profiles.

     The **!** status icons change from gray circles to green circles, indicating that the selected profiles are enabled. By default, when you add a profile to the table, the profile is automatically enabled.
   - **Disable**. Disables the selected VLAN profiles.

The **!** status icons change from green circles to gray circles, indicating that the selected profiles are disabled.

- **Delete**. Removes the selected VLAN profiles.

  The selected profiles are removed from the VLAN Profiles table.

Configure Unique VLAN MAC Addresses

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.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

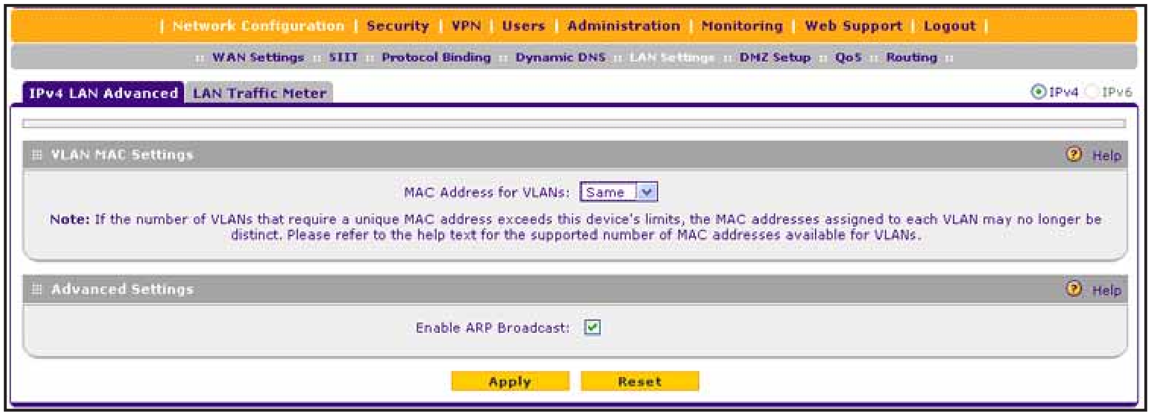
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > LAN Settings**.

   The LAN submenu tabs display, with the LAN Setup screen in view, displaying the IPv4 settings.
7. Click the **Advanced** option arrow in the upper right.

   The IPv4 LAN Advanced screen displays.


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

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.

Enable ARP Broadcast: ☑

8. From the **MAC Address for VLANs** menu, select **Unique**.

   The default setting is **Same**.

9. Click the **Apply** button.

   Your settings are saved. VLANs have unique MAC addresses.

Note: If you attempt to configure more than 16 VLANs, the MAC addresses that are assigned to each VLAN might no longer be distinct.

Disable the Broadcast of ARP Packets for the Default VLAN

You can 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). By default, the broadcast of ARP packets is enabled for the default VLAN.

➢ **To disable the broadcast of ARP packets for the default VLAN:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

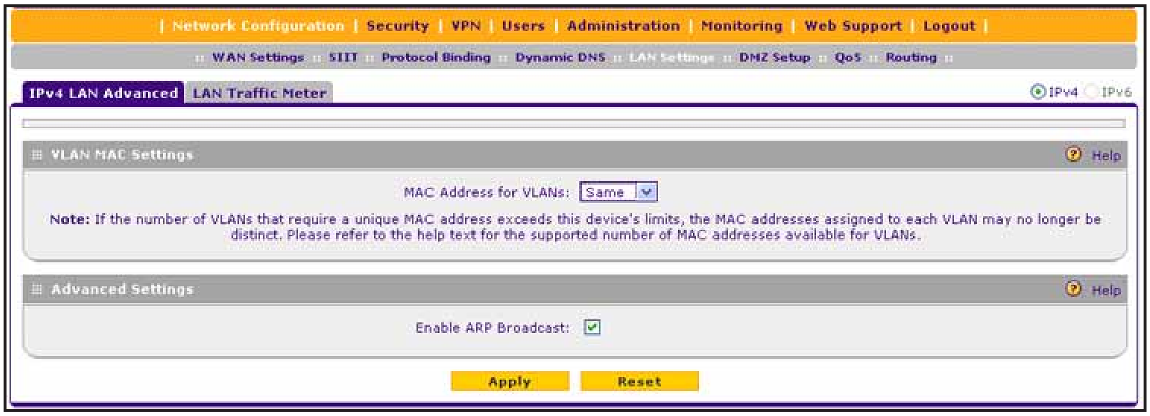
   The Router Status screen displays.

6. Select **Network Configuration > LAN Settings**.

   The LAN submenu tabs display, with the LAN Setup screen in view, displaying the IPv4 settings.

7. Click the **Advanced** option arrow in the upper right.

   The IPv4 LAN Advanced screen displays.


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

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.

Enable ARP Broadcast: ☑

8. Clear the **Enable ARP Broadcast** check box.
9. Click the **Apply** button.

   Your settings are saved. The broadcast of ARP packets for the default VLAN is disabled.

Manage IPv4 Multihome LAN IP Addresses on the Default VLAN

The following sections provide information about managing IPv4 multihome LAN IP addresses on the default VLAN:

- *IPv4 Multihome LAN IP Addresses*
- *Add a Secondary LAN IPv4 Address*
- *Change a Secondary LAN IPv4 Address*
- *Remove One or More Secondary LAN IPv4 Addresses*

IPv4 Multihome LAN IP Addresses

If computers use different IPv4 networks in the LAN (for example, 172.124.10.0 and 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.

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

Add a Secondary LAN IPv4 Address

The following procedure describes how to add a secondary LAN IPv4 address.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

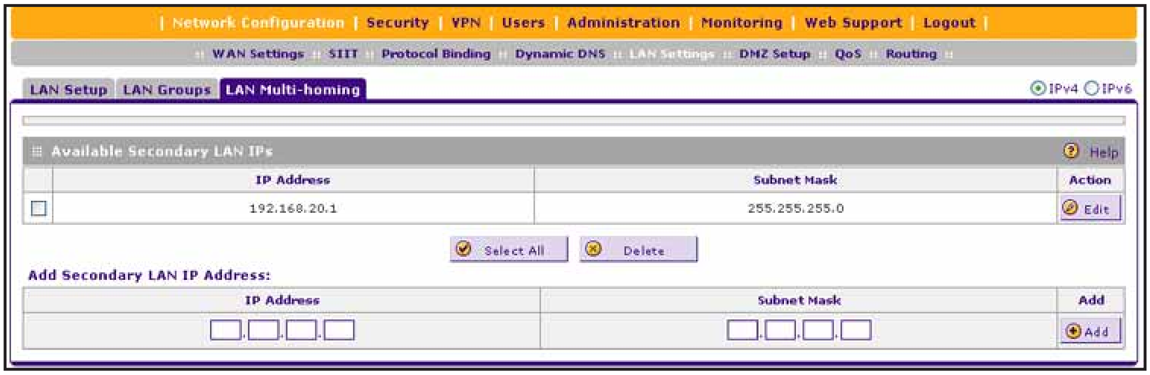
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > LAN Settings > LAN Multi-homing**.

   The LAN Multi-homing screen displays the IPv4 settings. The following figure shows one example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: 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
□	192.168.20.1	255.255.255.0	Edit

Add Secondary LAN IP Address:

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

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

7. 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.
8. Click the **Add** button.

   The secondary IP address is added to the Available Secondary LAN IPs table.
9. Repeat *Step 7* and *Step 8* for each secondary IP address that you want to add to the Available Secondary LAN IPs table.

Note: You cannot configure secondary IP addresses in the DHCP server. For the hosts on the secondary subnets, you must manually configure the IP addresses, gateway IP address, and DNS server IP addresses.

Change a Secondary LAN IPv4 Address

The following procedure describes how to change an existing secondary LAN IPv4 address.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > LAN Settings > LAN Multi-homing**.

   The LAN Multi-homing screen displays the IPv4 settings.

7. In the Available Secondary LAN IPs table, click the **Edit** button for the secondary IP address that you want to change.

   The Edit LAN Multi-homing screen displays.

8. Change the IP address, subnet mask, or both:
   - **IP Address**. Change the secondary address that you want to assign to the LAN ports.
   - **Subnet Mask**. Change the subnet mask for the secondary IP address.

9. Click the **Apply** button.

   Your settings are saved. The modified secondary IP address displays in the Available Secondary LAN IPs table on the LAN Multi-homing screen.

Remove One or More Secondary LAN IPv4 Addresses

The following procedure describes how to remove one or more existing secondary LAN IPv4 address that you no longer need.

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

1. On your computer, launch an Internet browser.

2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

The Router Status screen displays.

6. Select **Network Configuration > LAN Settings > LAN Multi-homing**.

   The LAN Multi-homing screen displays the IPv4 settings.

7. In the Available Secondary LAN IPs table, select the check box to the left of each secondary IP address that you want to remove, or click the **Select All** button to select all secondary IP addresses.

8. Click the **Delete** button.

   The selected addresses are removed from the Available Secondary LAN IPs table.

Manage IPv4 LAN Groups and Hosts

The following sections provide information about managing IPv4 LAN groups and hosts:

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

Network Database

The VPN firewall contains a list of all computers and network devices to which it assigned dynamic IP addresses or that it discovered by other means. This list also contains all computers and network devices for which you entered IP addresses manually. Collectively, these entries make up the network database.

The network database is updated by these methods:

- **DHCP client requests**. When the DHCP server is enabled, it accepts and responds to DHCP client requests from computers and other network devices. These requests also generate an entry in the network database. This is an advantage of enabling the DHCP server feature.
- **Scanning the network**. The local network is scanned using Address Resolution Protocol (ARP) requests. The ARP scan detects active devices that are not DHCP clients. However, if the VPN firewall receives a reply to an ARP request from a device with an active firewall that blocks the device name, the VPN firewall might not be able to determine the device name.

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

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

A network database has the following advantages:

- 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 addresses that are allocated by the DHCP server never change, you do not need to assign a fixed IP address to a computer to ensure that it always has the same IP address.
- A computer is identified by its MAC address—not its IP address. The network database uses the MAC address to identify each computer or device. Therefore, changing a computer’s IP address does not affect any restrictions applied to that computer.
- You can assign control over computers to groups and individuals:
    - You can assign computers to groups (see *Manage the Network Database* on page 133) 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 210).
    - You can select groups that are allowed access to URLs that you have blocked for other groups, or the other way around, block access to URLs that you have allowed access to for groups (see *Manage Content Filtering* on page 306).
    - You can create firewall rules to apply to a single computer (see *Enable Source MAC Filtering* on page 312). Because the MAC address is used to identify each computer, users cannot avoid these restrictions by changing their IP address.

DHCP Address Reservation

When you specify a reserved IP address for a device on the LAN and bind that IP address to the MAC address of the device, that device always receives the same IP address each time it accesses the VPN firewall’s DHCP server. Assign reserved IP addresses to servers and access points that require permanent IP address settings.

A reserved IP address must be outside of the DHCP server pool. A reserved address is not assigned until the next time the device contacts the VPN firewall’s DHCP server. You can force the device to contact the VPN firewall’s DHCP server by rebooting the device or by releasing and renewing the DHCP connection of the device.

For information about setting up address reservation with a binding, see *View or Add Devices Manually to the Network Database* on page 134. For information about how to display saved bindings, see *View and Set Up an IPv4/MAC Binding* on page 316 and *View and Set Up IPv6/MAC Bindings* on page 320.

Manage the Network Database

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

The following sections provide information about managing the network database:

- *View or Add Devices Manually to the Network Database*
- *Change Device Settings Manually in the Network Database*

- *Remove One or More Devices from the Network Database*

View or Add Devices Manually to the Network Database

The following procedure describes how to view or add devices manually to the network database.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

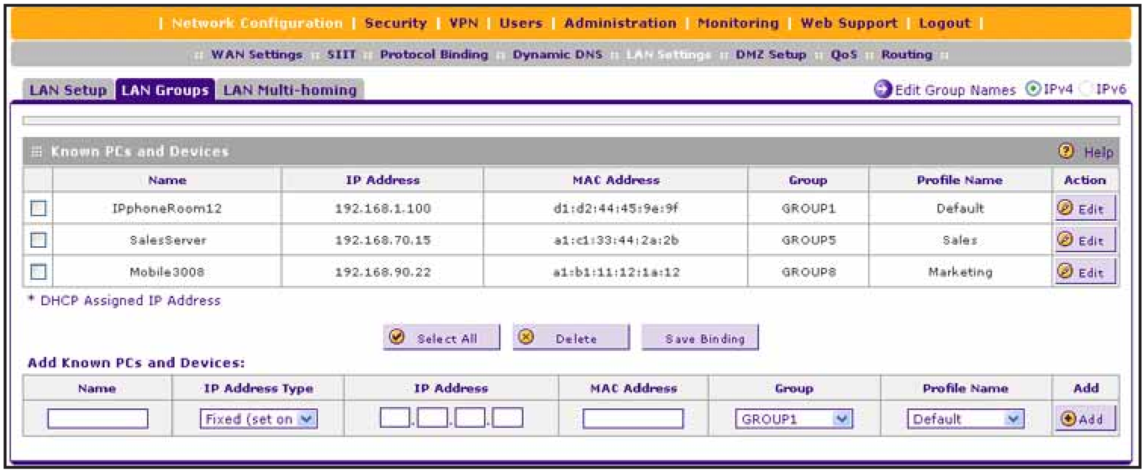
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > LAN Settings > LAN Groups**.

   The LAN Groups screen displays. The following figure shows some manually added devices in the Known PCs and Devices table as an example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: 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
□	IPphoneRoom12	192.168.1.100	d1:d2:44:45:9e:9f	GROUP1	Default	Edit
□	SalesServer	192.168.70.15	a1:c1:33:44:2a:2b	GROUP5	Sales	Edit
□	Mobile3008	192.168.90.22	a1:b1:11:12:1a:12	GROUP8	Marketing	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

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

- **Check box**. Allows you to select the computer or device in the table.
- **Name**. The name of the computer or device. For computers that do not support the NetBIOS protocol, the name is displayed as *Unknown* (you can change 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 has changed.
- **MAC Address**. The MAC address of the computer or device's network interface.
- **Group**. Each computer or device can be assigned to a single LAN group. By default, a computer or device is assigned to Group 1. However, you can select a different LAN group.
- **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). However, you can select a different VLAN.
- **Action**. The **Edit** button, which provides access to the Edit Groups and Hosts screen.

7. In the Add Known PCs and Devices section, enter the settings as described in the following table.

Setting	Description
Name	Enter the name of the computer or device.
IP Address Type	From the menu, select how the computer or device receives its IP address: • **Fixed (set on PC)**. The IP address is statically assigned on the computer or device. • **Reserved (DHCP Client)**. The DHCP server of the VPN firewall always assigns the specified IP address to this client during the DHCP negotiation (see also *DHCP Address Reservation* on page 133). **Note:** For both types of IP addresses, the VPN firewall reserves the IP address for the associated MAC address.
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** menu.

Setting	Description
MAC Address	Enter the MAC address of the computer's or device's network interface. The MAC address format is six colon-separated pairs of hexadecimal characters (0–9 and a–f), such as 01:23:d2:6f:89:ab.
Group	From the menu, select the group to which the computer or device is assigned. (Group 1 is the default group.)
Profile Name	From the menu, select the name of the VLAN profile to which the computer or device is assigned.

8. Click the **Add** button.

   The computer or device is added to the Known PCs and Devices table.

9. (Optional) Save the binding between the IP address and MAC address for the entry that you just added:

   a. Select the check box for the table entry.

   b. Click the **Save Binding** button.

   The binding is saved.

Change Device Settings Manually in the Network Database

The following procedure describes how to change the settings manually for a device in the network database.

➢ **To change the settings for a device manually in the network database:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

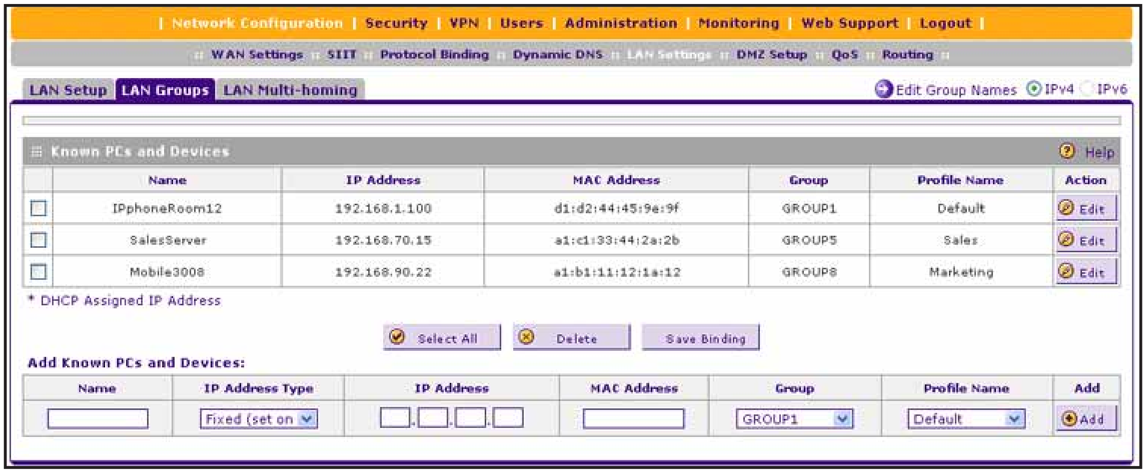
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > LAN Settings > LAN Groups**.

The LAN Groups screen displays. The following figure shows some manually added devices in the Known PCs and Devices table as an example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: 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
□	IPphoneRoom12	192.168.1.100	d1:d2:44:45:9e:9f	GROUP1	Default	Edit
□	SalesServer	192.168.70.15	a1:c1:33:44:2a:2b	GROUP5	Sales	Edit
□	Mobile3008	192.168.90.22	a1:b1:11:12:1a:12	GROUP8	Marketing	Edit

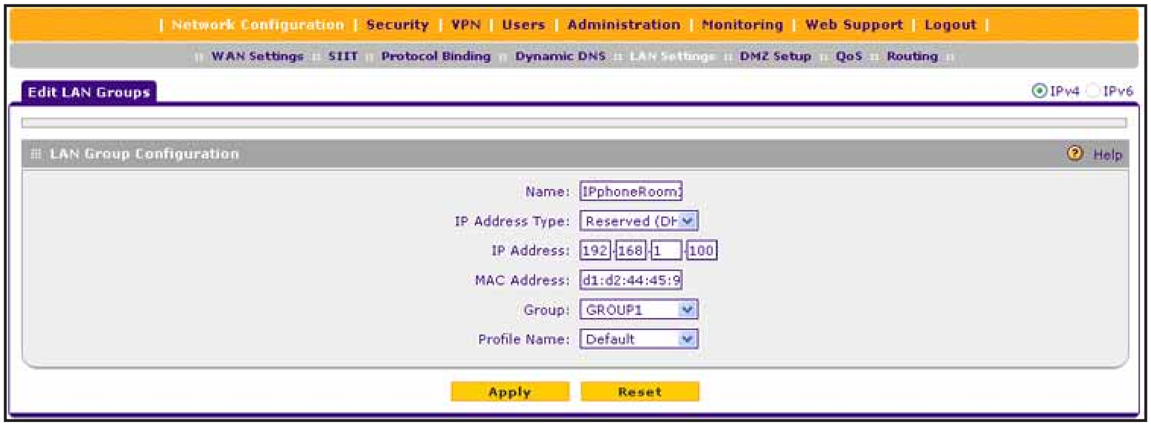
* DHCP Assigned IP Address

Add Known PCs and Devices:

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

7. In the Known PCs and Devices table, click the **Edit** button for the device that you want to change.

   The Edit LAN Groups screen displays. The following figure shows an example.


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

LAN Group Configuration

Name: IPphoneRoom1
IP Address Type: Reserved (DH
IP Address: 192.168.1.100
MAC Address: d1:d2:44:45:9
Group: GROUP1
Profile Name: Default

8. Change the settings.

   For information about the settings, see *View or Add Devices Manually to the Network Database* on page 134.

9. Click the **Apply** button.

   Your settings are saved. The modified device displays in the Known PCs and Devices table on the LAN Groups screen.

Remove One or More Devices from the Network Database

The following procedure describes how to remove one or more devices from the network database.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > LAN Settings > LAN Groups**.

   The LAN Groups screen displays.
7. In the Known PCs and Devices table, select the check box to the left of each device that you want to remove or click the **Select All** button to select all devices.
8. Click the **Delete** button.

   The selected devices are removed from the Known PCs and Devices table.
9. If you remove IP and MAC addresses for which saved bindings exist, you also must remove the saved bindings:

   a. Select **Security > Address Filter > IP/MAC Binding**.

      The IP/MAC Binding screen displays the IPv4 settings.

   b. In the IP/MAC Bindings table, select the check box to the left of each IP/MAC binding that you want to remove or click the **Select All** button to select all bindings.

   c. Click the **Delete** button.

      The selected bindings are removed from the IP/MAC Bindings table.

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, for example, GlobalMarketing and GlobalSales.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

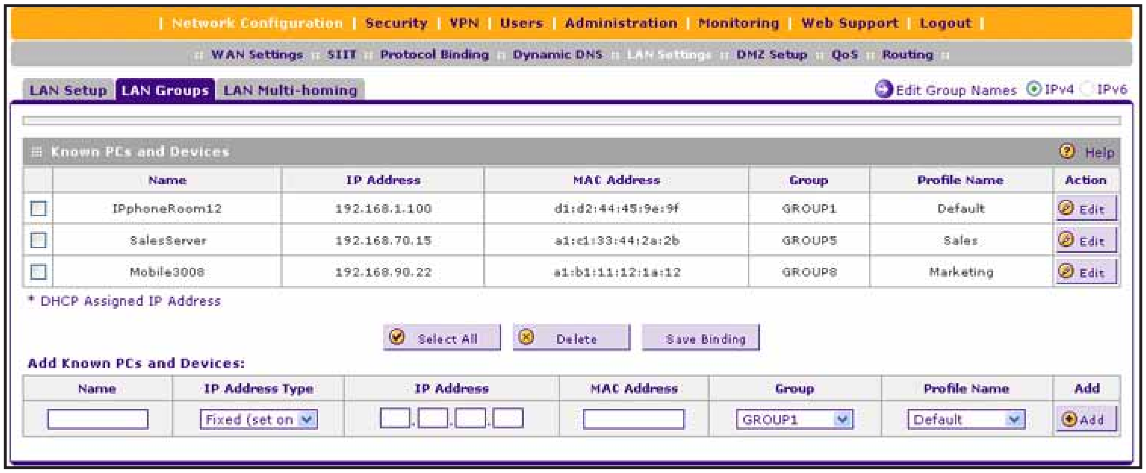
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > LAN Settings > LAN Groups**.

   The LAN Groups screen displays. The following figure shows some manually added devices in the Known PCs and Devices table as an example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
LAN Setup
LAN Groups
LAN Multi-homing
Edit Group Names
● IPv4 ○ IPv6
Known PCs and Devices
Help

	Name	IP Address	MAC Address	Group	Profile Name	Action
□	IPphoneRoom12	192.168.1.100	d1:d2:44:45:9e:9f	GROUP1	Default	Edit
□	SalesServer	192.168.70.15	a1:c1:33:44:2a:2b	GROUP5	Sales	Edit
□	Mobile3008	192.168.90.22	a1:b1:11:12:1a:12	GROUP8	Marketing	Edit

* DHCP Assigned IP Address

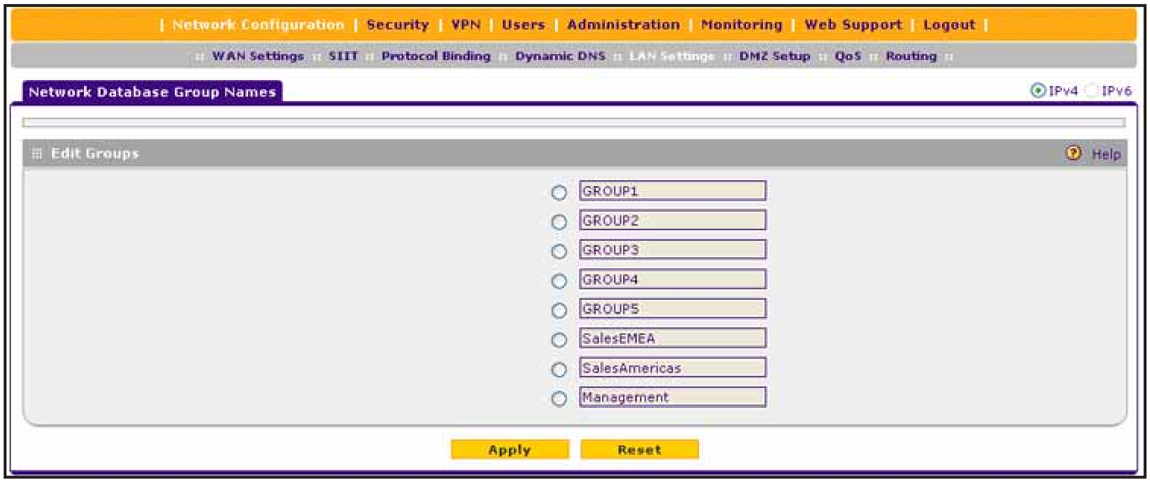
Select All
Delete
Save Binding

Add Known PCs and Devices:

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

7. Click the **Edit Group Names** option arrow.

   The following figure shows some examples.


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

○ GROUP1
○ GROUP2
○ GROUP3
○ GROUP4
○ GROUP5
○ SalesEMEA
○ SalesAmericas
○ Management

8. Select the radio button next to the group name that you want to change.

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

9. 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.

10. Click the **Apply** button.

    Your settings are saved.

Manage the DMZ Port for IPv4 Traffic

The following sections provide information about managing the DMZ port for IPv4 traffic:

- *IPv4 DMZ*
- *Enable and Configure the DMZ Port for IPv4 Traffic*

IPv4 DMZ

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

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

Using a DMZ port is also helpful with online games and videoconferencing applications that are incompatible with NAT. The VPN firewall is programmed to recognize some of these applications and to work correctly with them, but 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.

Note the following about the DMZ port:

- The VPN firewall has a separate firewall security profile for the DMZ port. This security profile is also physically independent of the standard firewall security component that is used for the LAN.
- When you enable the DMZ port for IPv4 traffic, IPv6 traffic, or both, the DMZ LED next to LAN port 4 (see *Front Panel* on page 18) lights green to indicate that the DMZ port is enabled.

For information about how to define the DMZ WAN rules and LAN DMZ rules, see *Add DMZ WAN Rules* on page 233 and *Add LAN DMZ Rules* on page 242, respectively.

Enable and Configure the DMZ Port for IPv4 Traffic

You can enable the hardware DMZ port (LAN port 4) and configure an IPv4 address and subnet mask for the DMZ port.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

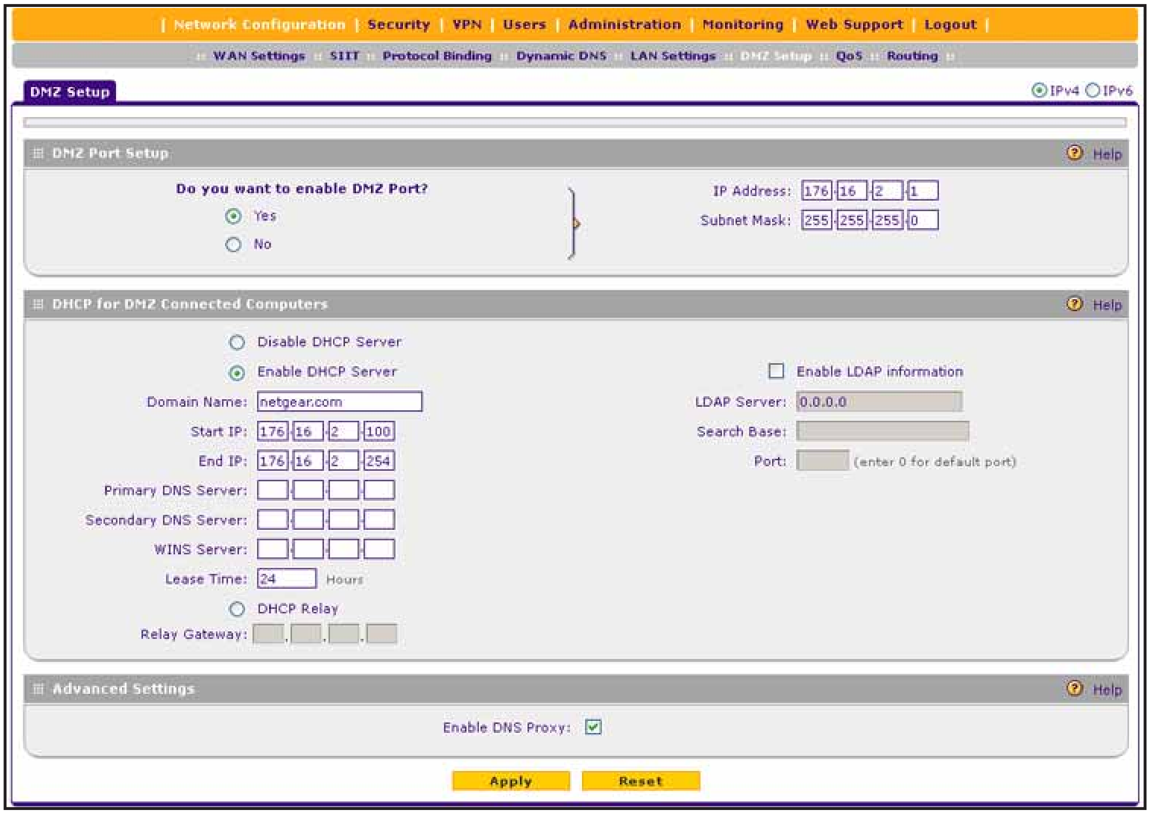
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > DMZ Setup**.

   The DMZ Setup screen displays the IPv4 settings.


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

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: ☑

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

Setting	Description
DMZ Port Setup	
Select the **Yes** radio button to configure the DMZ port settings. Complete the following fields: • **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. **Note:** By default, the DMZ port is disabled. After you configure the DMZ port, you can select the **No** radio button to disable the DMZ port without losing the DMZ configuration.	

Setting	Description
DHCP for DMZ Connected Computers	
Select one of the following radio buttons: • **Disable DHCP Server**. If another device in the DMZ functions as the Dynamic Host Configuration Protocol (DHCP) server for the DMZ, or if you intend to manually configure the network settings of all computers in the DMZ, select the **Disable DHCP Server** radio button to disable the DHCP server. This is the default setting. • **Enable DHCP Server**. To enable the VPN firewall to function as the DHCP server for the DMZ, select the **Enable DHCP Server** radio button. Complete the **Start IP Address**, **End IP Address**, and **Lease Time** fields. The **Domain Name**, **Primary DNS Server**, **Secondary DNS Server**, and **WINS Server** fields are optional, as is the **Enable LDAP information** check box and associated fields. • **DHCP Relay**. To use a DHCP server somewhere else in your network as the DHCP server for the DMZ, select the **DHCP Relay** radio button. In the **Relay Gateway** field, enter the IP address of the DHCP server.	
Domain Name	This setting is optional. Enter the domain name of the VPN firewall.
Start IP Address	Enter the start IP address. This address specifies the first of the contiguous addresses in the IP address pool. Any new DHCP client joining the DMZ is assigned an IP address between this address and the end IP address. The default IP address 176.16.2.100.
End IP Address	Enter the end IP address. This address specifies the last of the contiguous addresses in the IP address pool. Any new DHCP client joining the DMZ 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 DMZ 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.

Setting	Description
Enable LDAP information	To enable the DHCP server in the DMZ 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, enter the following objects: cn=Johnson,dc=Netgear,dc=net • **Port**. The port number for the LDAP server. The default setting is 0 (zero).
Advanced Settings	
Enable DNS Proxy	This setting is optional. To enable the VPN firewall to provide a DMZ IP address for DNS address name resolution, select the **Enable DNS Proxy** check box. This check box is selected by default. **Note:** If you clear the **Enable DNS Proxy** check box for the DMZ, all computers in the DMZ receive the DNS IP addresses of the ISP but without the DNS proxy IP address.

8. Click the **Apply** button.

   Your settings are saved.

Manage Static IPv4 Routing

The following sections provide information about managing static IPv4 routing:

- *Static IPv4 Routes*
- *Add a Static IPv4 Route*
- *Change a Static IPv4 Route*
- *Remove One or More Static IPv4 Routes*
- *Configure the Routing Information Protocol*
- *IPv4 Static Route Example*

Static IPv4 Routes

Static routes provide routing information to your VPN firewall. Under normal circumstances, the VPN firewall has 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 have configured (see *Manage IPv4 Multihome LAN IP Addresses on the Default VLAN* on page 128). Therefore, you do not need to manually add an IPv4 static route between a VLAN and a secondary IPv4 address.

Add a Static IPv4 Route

The following procedure describes how to add an IPv4 static route to the VPN firewall.

➢ **To add an IPv4 static route to the VPN firewall:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

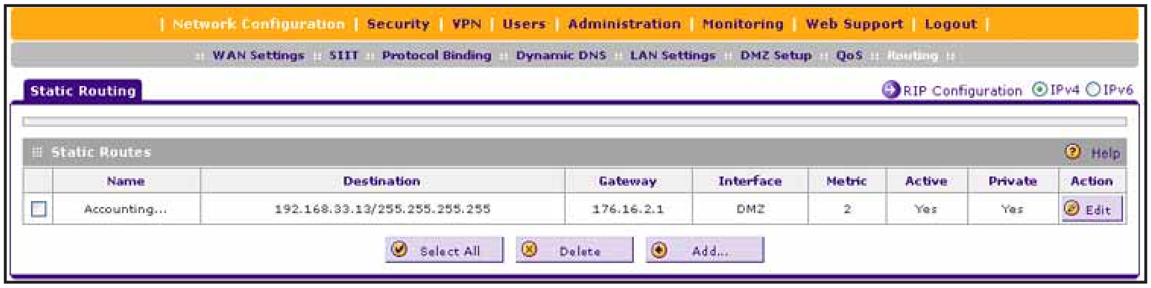
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > Routing**.

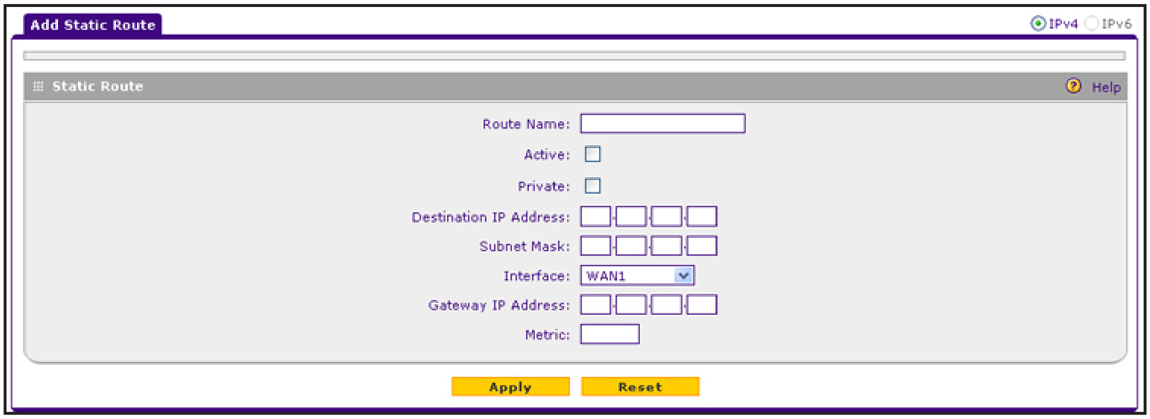
   The Static Routing screen displays the IPv4 settings. The following figure shows one example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
Static Routing
RIP Configuration
● IPv4 ○ IPv6
Static Routes
Help

	Name	Destination	Gateway	Interface	Metric	Active	Private	Action
□	Accounting...	192.168.33.13/255.255.255.255	176.16.2.1	DMZ	2	Yes	Yes	Edit

7. Click the **Add** button.

   The Add Static Route screen displays.



Add Static Route

● IPv4 ○ IPv6

Static Route

Route Name:

Active: □

Private: □

Destination IP Address:

Subnet Mask:

Interface: WAN1

Gateway IP Address:

Metric:

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

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:** You can add a route to the table and make the route inactive if you do not need it. 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	From the menu, select the physical or virtual network interface (the WAN1 or WAN2 interface, a VLAN, or the DMZ interface) through which the route is accessible.
Gateway IP Address	The gateway IP address through which the destination host or network can be reached.
Metric	The priority of the route. Select a value between 2 and 15. If multiple routes to the same destination exist, the route with the lowest metric is used.

9. Click the **Apply** button.

Your settings are saved. The new static route is added to the Static Routes table.

Change a Static IPv4 Route

The following procedure describes how to change an existing IPv4 static route.

➢ **To change an IPv4 static route:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > Routing**.

   The Static Routing screen displays the IPv4 settings.
7. In the Static Routes table, click the **Edit** button for the route that you want to change.

   The Edit Static Route screen displays.
8. Change the settings.

   For information about the settings, see *Add a Static IPv4 Route* on page 145.
9. Click the **Apply** button.

   Your settings are saved. The modified route displays in the Static Routes table on the Static Routes screen.

Remove One or More Static IPv4 Routes

The following procedure describes how to remove one or more existing IPv4 static routes that you no longer need.

➢ **To remove one or more static IPv4 routes:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

The VPN firewall factory default IP address is 192.168.1.1.

The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > Routing**.

   The Static Routing screen displays the IPv4 settings.

7. In the Static Routes table, select the check box to the left of each route that you want to remove or click the **Select All** button to select all routes.
8. Click the **Delete** button.

   The selected routes are removed from the Static Routes table.

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. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

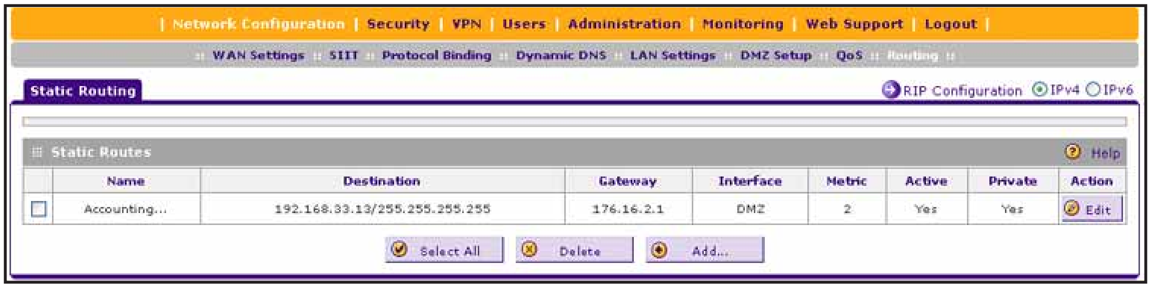
If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > Routing**.

   The Static Routing screen displays the IPv4 settings. The following figure shows one example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
Static Routing
RIP Configuration
Help
Select All
Delete
Add...

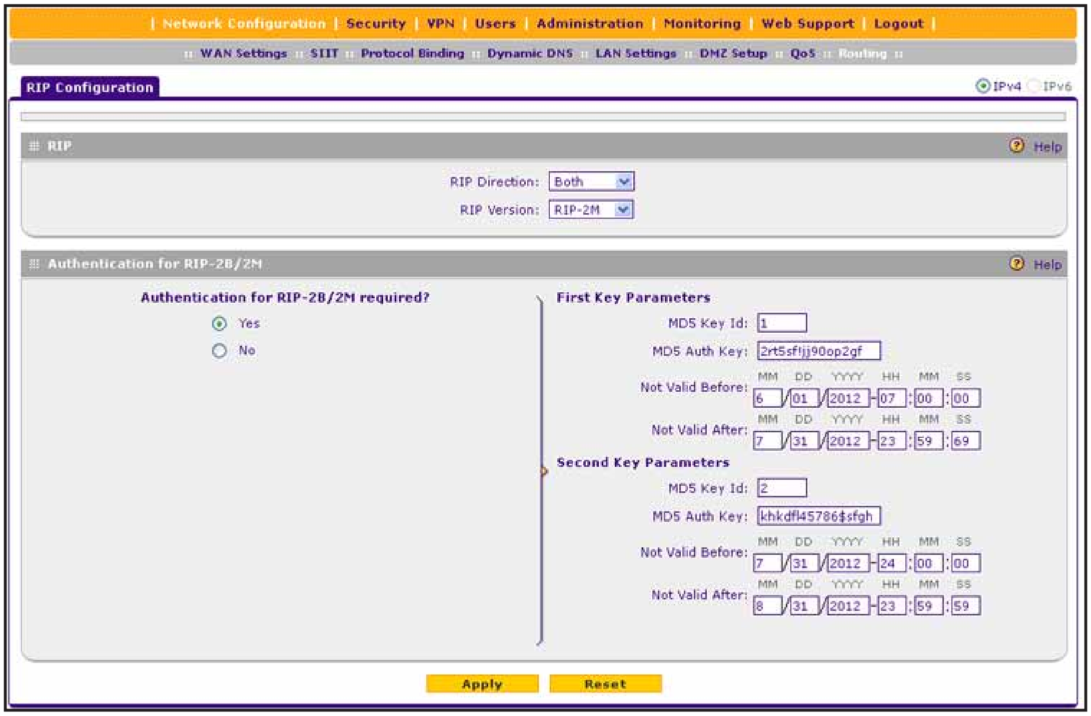
● IPv4 ○ IPv6

Static Routes

	Name	Destination	Gateway	Interface	Metric	Active	Private	Action
□	Accounting...	192.168.33.13/255.255.255.255	176.16.2.1	DMZ	2	Yes	Yes	Edit

7. Click the **RIP Configuration** option arrow in the upper right.

   The RIP Configuration screen displays. The following figure shows some examples.


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

● IPv4 ○ IPv6

RIP

RIP Direction: Both

RIP Version: RIP-2M

Authentication for RIP-2B/2M

Authentication for RIP-2B/2M required?

● Yes

○ No

First Key Parameters

MD5 Key Id: 1

MD5 Auth Key: 2rt5sf!jj90op2gf

Not Valid Before: 6 / 01 / 2012 - 07 : 00 : 00 (MM DD YYYY HH MM SS)

Not Valid After: 7 / 31 / 2012 - 23 : 59 : 69 (MM DD YYYY HH MM SS)

Second Key Parameters

MD5 Key Id: 2

MD5 Auth Key: khkdfl45786$sfgh

Not Valid Before: 7 / 31 / 2012 - 24 : 00 : 00 (MM DD YYYY HH MM SS)

Not Valid After: 8 / 31 / 2012 - 23 : 59 : 59 (MM DD YYYY HH MM SS)

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

Setting	Description
RIP	
RIP Direction	From the **RIP Direction** menu, select the direction in which the VPN firewall sends and receives RIP packets: • **None**. The VPN firewall neither advertises its route table nor accepts any RIP packets from other routers. This effectively disables RIP and is the default setting. • **In Only**. The VPN firewall accepts RIP information from other routers but does not advertise its routing table. • **Out Only**. The VPN firewall advertises its routing table but does not accept RIP information from other routers. • **Both**. The VPN firewall advertises its routing table and also processes RIP information received from other routers.
RIP Version	By default, the RIP version is set to **Disabled**. From the **RIP Version** menu, select the version: • **RIP-1**. Classful routing that does not include subnet information. This is the most commonly supported version. • **RIP-2**. Routing that supports subnet information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format: - **RIP-2B**. Sends the routing data in RIP-2 format and uses subnet broadcasting. - **RIP-2M**. Sends the routing data in RIP-2 format and uses multicasting.
Authentication for RIP-2B/2M	
Authentication for 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.

9. Click the **Apply** button.

Your settings are saved.

IPv4 Static Route Example

In this example, we assume the following:

- The VPN firewall’s primary Internet access is through a cable modem to an ISP.
- The VPN firewall is on a local LAN with IP address 192.168.1.100.
- The VPN firewall connects to a remote network where you 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 must 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 must be forwarded to the local LAN IP address (192.168.1.100).
- A metric value of 1 must 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.

Configure the IPv6 LAN Settings

5

This chapter describes how to configure the IPv6 LAN features of your VPN firewall. The chapter contains the following sections:

- *Manage the IPv6 LAN*
- *Manage IPv6 Multihome LAN IP Addresses*
- *Manage the DMZ Port for IPv6 Traffic*
- *Manage Static IPv6 Routing*

Manage the IPv6 LAN

The following sections provide information about managing the IPv6 LAN:

- *IPv6 LANs*
- *DHCPv6 LAN Server Concepts and Configuration Roadmap*
- *Configure a Stateless DHCPv6 Server Without Prefix Delegation for the LAN*
- *Manage a Stateless DHCPv6 Server with Prefix Delegation for the LAN*
- *Manage a Stateful DHCPv6 Server and IPv6 Address Pools for the LAN*
- *Manage the IPv6 Router Advertisement Daemon for the LAN*

IPv6 LANs

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.)

The VPN firewall (or any other router) never forwards traffic with site-local or link-local addresses, 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). For more information about link-local unicast addresses, see *Manage ISATAP Automatic Tunneling* on page 103.

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.

To forward traffic from sources with a site local or link-local unicast address in the LAN, you must use a DHCPv6 server. (By default, the DHCPv6 server is disabled.) For information about the DHCPv6 server options that the VPN firewall provides, see *DHCPv6 LAN Server Concepts and Configuration Roadmap* on page 153.

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

DHCPv6 LAN Server Concepts and Configuration Roadmap

The IPv6 clients in the LAN can autoconfigure their own IPv6 address or obtain an IPv6 address through the VPN firewall’s DHCPv6 server.

The VPN firewall provides three DHCPv6 options for the LAN. The following sections provide information about the DHCPv6 options for the LAN:

- *Concept: Stateless DHCPv6 Server Without Prefix Delegation for the LAN*
- *Concept: Stateless DHCPv6 Server With Prefix Delegation for the LAN*
- *Concept: Stateful DHCPv6 Server for the LAN*

Concept: Stateless DHCPv6 Server Without Prefix Delegation for the LAN

The IPv6 clients in the LAN generate their own IP address by using a combination of locally available information and router advertisements from the Router Advertisement Daemon (RADVD), but receive DNS server information from the DHCPv6 server.

In a stateless DHCPv6 server configuration without prefix delegation, the RADVD advertises the following advertisement prefixes:

- If you enabled the ISP DHCPv6 server to assign a prefix through prefix delegation to the VPN firewall, the advertisement prefixes that are based on the ISPs assignment.
- Advertisement prefixes that you add manually for the RADVD.

For stateless DHCPv6 without prefix delegation, you must enable and configure the RADVD.

➢ **To set up a stateless DHCPv6 server without prefix delegation in the LAN, complete these tasks:**

1. Enable the ISP DHCPv6 server to assign a prefix through prefix delegation to the VPN firewall (see *Use a DHCPv6 Server to Configure an IPv6 Internet Connection Automatically* on page 90). This task is optional (see also *Step 4*).
2. Configure the stateless DHCP server without prefix delegation (see *Configure a Stateless DHCPv6 Server Without Prefix Delegation for the LAN* on page 155).
3. Enable and configure the RADVD (see *Manage the IPv6 Router Advertisement Daemon for the LAN* on page 171).
4. If you did not enable the ISP DHCPv6 server to assign a prefix through prefix delegation to the VPN firewall, manually add advertisement prefixes to the RADVD (see *View Automatically Added Advertisement Prefixes for the LAN and Manually Add Advertisement Prefixes* on page 175).

Note: If you do enable the ISP DHCPv6 server to assign a prefix through prefix delegation to the VPN firewall, you still can manually add advertisement prefixes to the RADVD.

Concept: Stateless DHCPv6 Server With Prefix Delegation for the LAN

As an option for a stateless DHCPv6 server, you can enable prefix delegation. Note that this is prefix delegation by the DHCPv6 server in the LAN, not by the ISP DHCPv6 sever in the WAN. After you specify a prefix and a prefix length for the DHCPv6 server, the VPN firewall’s stateless DHCPv6 server assigns prefixes to its IPv6 LAN clients through the RADVD.

For stateless DHCPv6 with prefix delegation, you must enable and configure the RADVD, but you do not need to add advertisement prefixes to the RADVD because the DHCPv6 server assigns the prefixes that you specify for the DHCPv6 server.

- **To set up a stateless DHCPv6 server with prefix delegation in the LAN, complete these tasks:**

1. Configure the stateless DHCP server with prefix delegation (see *Manage a Stateless DHCPv6 Server with Prefix Delegation for the LAN* on page 158).
2. Specify prefixes and a prefix lengths for the DHCPv6 server (see *Manually Add IPv6 LAN Prefixes for Prefix Delegation* on page 163).
3. Enable and configure the RADVD (see *Manage the IPv6 Router Advertisement Daemon for the LAN* on page 171).

Concept: Stateful DHCPv6 Server for the LAN

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 (see).

The IP address is a dynamic address that the DHCPv6 server assigns from IPV6 address pools that you must configure.

Enable RADVD for default route where configuring prefixes is optional.

- **To set up a stateful DHCPv6 server in the LAN, complete these tasks:**

1. Configure the stateful DHCPv6 server (see *Manage a Stateful DHCPv6 Server and IPv6 Address Pools for the LAN* on page 165).
2. Add one or more IPv6 address pools for the DHCPv6 server (see *Add an IPv6 LAN Address Pool* on page 168).

Configure a Stateless DHCPv6 Server Without Prefix Delegation for the LAN

With a stateless DHCPv6 server in the LAN, the IPv6 clients in the LAN generate their own IP address by using a combination of locally available information and router advertisements from the Router Advertisement Daemon (RADVD), but receive DNS server information from the DHCPv6 server.

If you configure a stateless DHCPv6 server in the LAN, you also must enable the RADVD and configure advertisement prefixes (see *Manage the IPv6 Router Advertisement Daemon for the LAN* on page 171).

For more information about a stateless DHCPv6 server for the LAN, see *Concept: Stateless DHCPv6 Server Without Prefix Delegation for the LAN* on page 154.

- **To configure a stateless DHCPv6 server without prefix delegation and IPv6 settings for the LAN:**

1. On your computer, launch an Internet browser.

2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

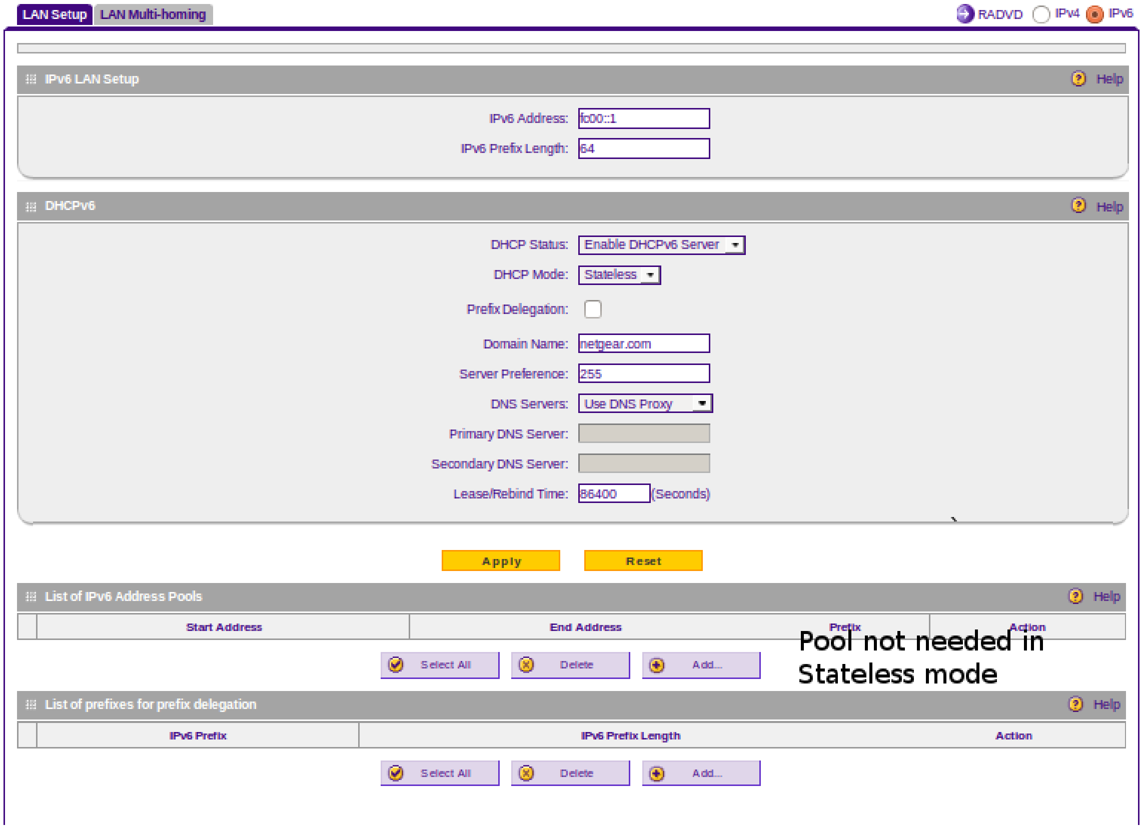
   The Router Status screen displays.

6. Select **Network Configuration > LAN Settings**.

   The LAN Setup screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The LAN Setup screen displays the IPv6 settings. The following figure shows some examples.



IPv6 LAN Setup

IPv6 Address: fc00::1

IPv6 Prefix Length: 64

DHCPv6

DHCP Status: Enable 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

Pool not needed in Stateless mode

List of prefixes for prefix delegation

	IPv6 Prefix	IPv6 Prefix Length	Action

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

Setting	Description
IPv6 LAN Setup	
IPv6 Address	Enter the LAN IPv6 address. The default address is fc00::1. (For more information, see *IPv6 LANs* on page 153.)
IPv6 Prefix Length	Enter the IPv6 prefix length, for example, 10 or 64. The default prefix length is 64.
DHCPv6	
DHCP Status	Enable the DHCPv6 server by selecting **Enable DHCPv6 Server** from the **DHCP Status** menu. The default menu selection is **Disable DHCPv6 Server**.
DHCP Mode	From the **DHCP Mode** menu, select **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. When you enable the stateless DHCP server for the LAN, you must also enable and configure the RADVD for the LAN. For more information, see *Manage the IPv6 Router Advertisement Daemon for the LAN* on page 171.

Setting	Description
Prefix Delegation	Leave the **Prefix Delegation** check box cleared. Prefix delegation is disabled in the LAN. This is the default setting. For information about using the stateless DHCPv6 server with prefix delegation, see *Manage a Stateless DHCPv6 Server with Prefix Delegation for the LAN* on page 158.
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	From the **DNS Server** menu, select a DNS server option: • **Use DNS Proxy**. The VPN firewall acts as a proxy for all DNS requests and communicates with the ISP DNS servers that you configure. For information about specifying the ISP DNS servers, see *Manually Configure a Static IPv6 Internet Connection* on page 94. • **Use DNS from ISP**. The VPN firewall uses the ISP DNS servers that you configure. For information about specifying the ISP DNS servers, see *Manually Configure a Static IPv6 Internet Connection* on page 94. • **Use below**. When you select this option, the **Primary DNS Server** and **Secondary 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).

9. Click the **Apply** button.

   Your settings are saved.

Manage a Stateless DHCPv6 Server with Prefix Delegation for the LAN

The following sections provide information about managing a stateless DHCPv6 server with prefix delegation for the LAN:

- *Stateless DHCPv6 Server and Prefix Delegation for the LAN*
- *Configure a Stateless DHCPv6 Server with Prefix Delegation*
- *Manually Add IPv6 LAN Prefixes for Prefix Delegation*
- *Change an IPv6 LAN Prefix for Prefix Delegation*
- *Remove One or More IPv6 LAN Prefixes for Prefix Delegation*

Stateless DHCPv6 Server and Prefix Delegation for the LAN

As an option for a stateless DHCPv6 server, you can enable prefix delegation. Note that this is prefix delegation by the DHCPv6 server in the LAN, not by the ISP DHCPv6 sever in the WAN. After you specify a prefix and a prefix length for the DHCPv6 server, the VPN firewall's stateless DHCPv6 server assigns prefixes to its IPv6 LAN clients through the RADVD.

For stateless DHCPv6 with prefix delegation, you must enable and configure the RADVD (see *Manage the IPv6 Router Advertisement Daemon for the LAN* on page 171) but you do not need to add advertisement prefixes to the RADVD because the DHCPv6 server assigns the prefixes that you specify for the DHCPv6 server.

For more information about stateless DHCPv6 servers, see *DHCPv6 LAN Server Concepts and Configuration Roadmap* on page 153.

Configure a Stateless DHCPv6 Server with Prefix Delegation

The following procedure describes how to configure a stateless DHCPv6 server with prefix delegation and IPv6 settings for the LAN.

➢ **To configure a stateless DHCPv6 server with prefix delegation and IPv6 settings for the LAN:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.

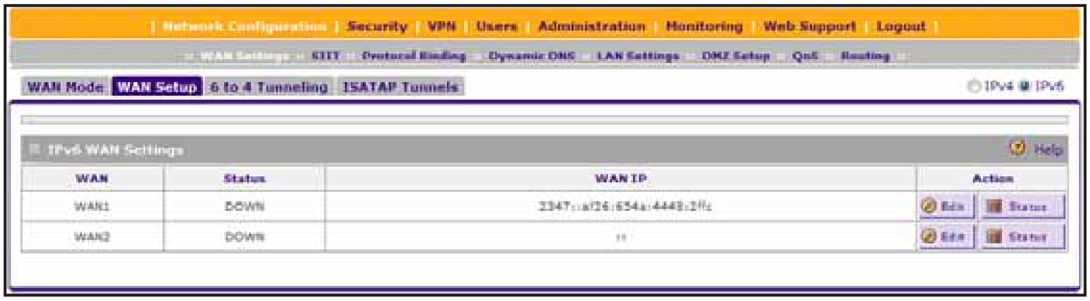
   Note: If the VPN firewall cannot acquire a prefix from the ISP, the VPN firewall's stateless DHCPv6 server cannot assign prefixes to its IPv6 LAN clients.
6. Verify that the VPN firewall allows the ISP DHCPv6 server to assign prefixes through prefix delegation (you can manually add prefixes to the RADVD):

   a. Select **Network Configuration > WAN Settings > WAN Setup**.

      The WAN Setup screen displays the IPv4 settings.

b. In the upper right, select the **IPv6** radio button.

   The WAN Setup screen displays the IPv6 settings.

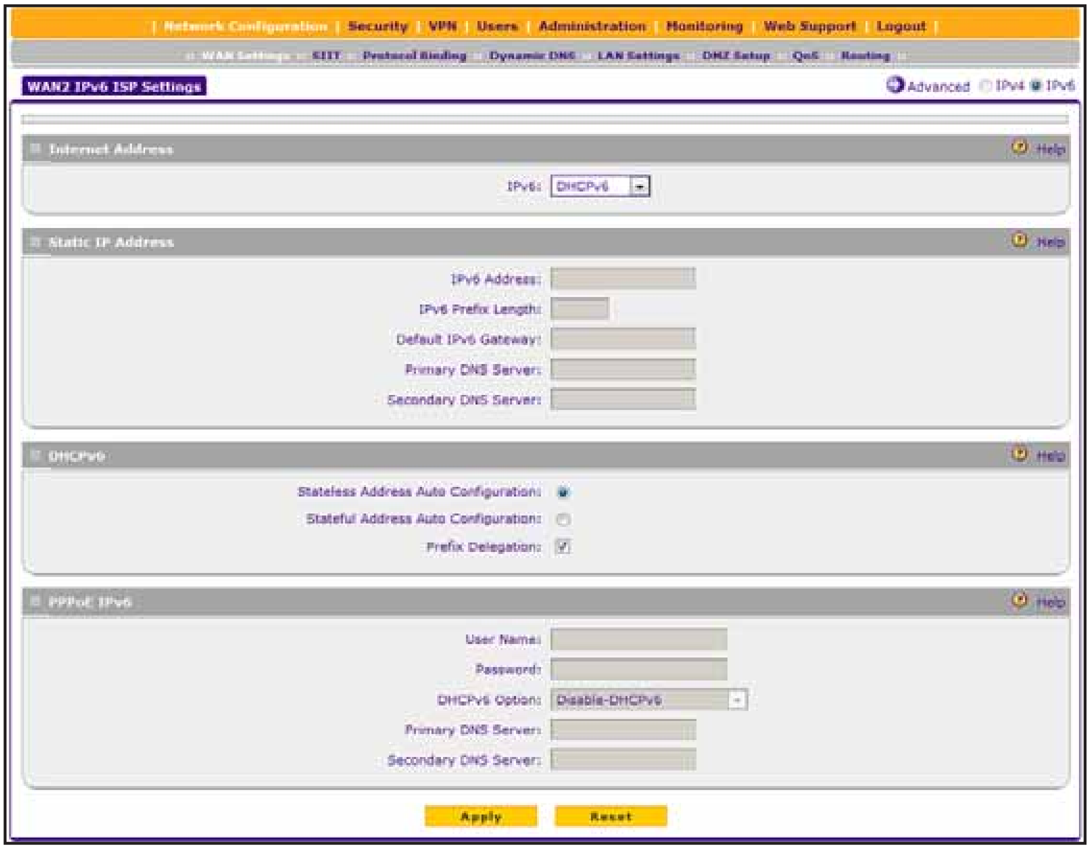

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
WAN Settings | SIIT | Protocol Binding | Dynamic DNS | LAN Settings | DMZ Setup | QoS | Routing
WAN Mode
WAN Setup
6 to 4 Tunneling
ISATAP Tunnels
○ IPv4 ● IPv6
Help

IPv6 WAN Settings

WAN	Status	WAN IP	Action
WAN1	DOWN	2347::af26:654a:4448:2ffc	Edit Status
WAN2	DOWN	::	Edit Status

c. In the WAN IPv6 Settings table, click the **Edit** button for the WAN interface for which you want to check the WAN configuration.

   The WAN IPv6 ISP Settings screen displays. The following figure shows the WAN2 IPv6 ISP Settings screen as an example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
WAN Settings | SIIT | Protocol Binding | Dynamic DNS | LAN Settings | DMZ Setup | QoS | Routing
WAN2 IPv6 ISP Settings
Advanced ○ IPv4 ● IPv6
Help
Apply
Reset

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:

d. In the Internet Address section, make sure that the selection from the **IPv6** menu is **DHCPv6**.

e. In the DHCPv6 section, make sure that the **Stateless Address Auto Configuration** radio button is selected.

f. Make sure that the **Prefix Delegation** check box is selected.

g. If you made any changes, click the **Apply** button.

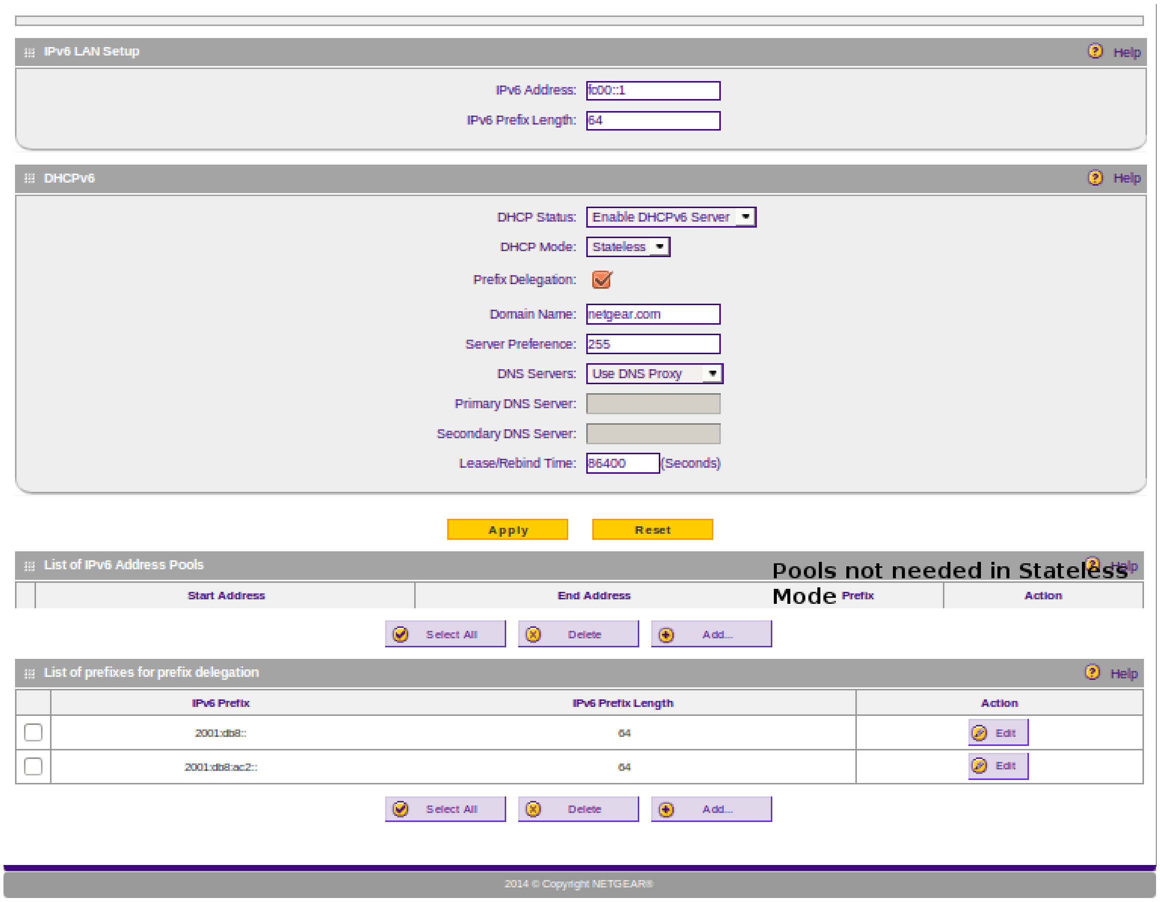
Your settings are saved.

7. Select **Network Configuration > LAN Settings**.

The LAN Setup screen displays the IPv4 settings.

8. In the upper right, select the **IPv6** radio button.

The LAN Setup screen displays the IPv6 settings. The following figure shows some examples.



IPv6 LAN Setup

IPv6 Address: fc00::1

IPv6 Prefix Length: 64

DHCPv6

DHCP Status: Enable 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

Pools not needed in Stateless Mode

	Start Address	End Address	Prefix	Action

List of prefixes for prefix delegation

	IPv6 Prefix	IPv6 Prefix Length	Action
□	2001:db8::	64	Edit
□	2001:db8:ac2::	64	Edit

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

Setting	Description
IPv6 LAN Setup	
IPv6 Address	Enter the LAN IPv6 address. The default address is fc00::1. (For more information, see *IPv6 LANs* on page 153.)
IPv6 Prefix Length	Enter the IPv6 prefix length, for example, 10 or 64. The default prefix length is 64.

Setting	Description
DHCPv6	
DHCP Status	Enable the DHCPv6 server by selecting **Enable DHCPv6 Server** from the **DHCP Status** menu. The default menu selection is **Disable DHCPv6 Server**.
DHCP Mode	From the **DHCP Mode** menu, select **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. When you enable the stateless DHCP server for the LAN, you must also enable and configure the RADVD for the LAN. For more information, see *Manage the IPv6 Router Advertisement Daemon for the LAN* on page 171.
Prefix Delegation	Select the **Prefix Delegation** check box. By default, prefix delegation is disabled in the LAN. When you enable prefix delegation, the stateless DHCPv6 server assigns prefixes to its IPv6 LAN clients. For information about adding more prefixes, see *Manually Add IPv6 LAN Prefixes for Prefix Delegation* on page 163.
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	From the **DNS Server** menu, select a DNS server option: • **Use DNS Proxy**. The VPN firewall acts as a proxy for all DNS requests and communicates with the ISP DNS servers that you configure. For information about specifying the ISP DNS servers, see *Manually Configure a Static IPv6 Internet Connection* on page 94. • **Use DNS from ISP**. The VPN firewall uses the ISP DNS servers that you configure. For information about specifying the ISP DNS servers, see *Manually Configure a Static IPv6 Internet Connection* on page 94. • **Use below**. When you select this option, the **Primary DNS Server** and **Secondary 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).

10. Click the **Apply** button.

    Your settings are saved.

Manually Add IPv6 LAN Prefixes for Prefix Delegation

As an option, you can also manually add prefixes to enable the DHCPv6 server to assign these prefixes to its IPv6 LAN clients.

➤ **To add an IPv6 prefix manually for prefix delegation:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

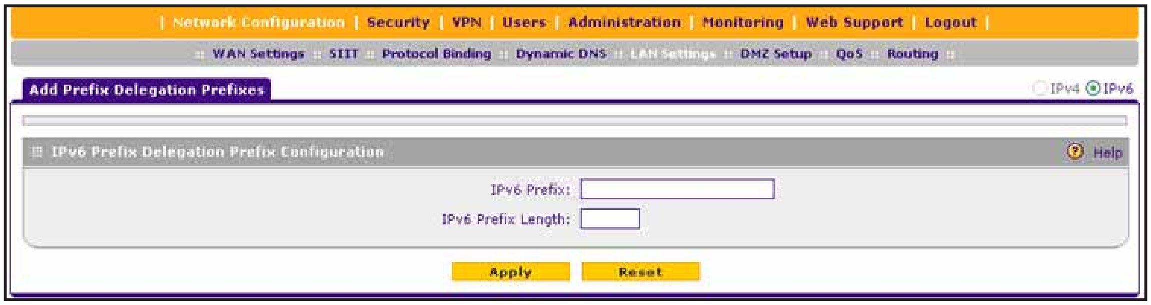
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > LAN Settings**.

   The LAN Setup screen displays the IPv4 settings.
7. In the upper right, select the **IPv6** radio button.

   The LAN Setup screen displays the IPv6 settings.
8. Click the **Add** button.

   The Add Prefix Delegation Prefixes screen displays.


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

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

10. Click the **Apply** button.

    Your settings are saved. The new prefix is added to the List of Prefixes for Prefix Delegation table on the LAN Setup screen for IPv6.

Change an IPv6 LAN Prefix for Prefix Delegation

The following procedure describes how to change an existing IPv6 LAN prefix for prefix delegation.

➢ **To change a prefix for prefix delegation:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > LAN Settings**.

   The LAN Setup screen displays the IPv4 settings.
7. In the upper right, select the **IPv6** radio button.

   The LAN Setup screen displays the IPv6 settings.
8. In the List of prefixes for prefix delegation table, click the **Edit** button for the prefix that you want to change.

   The Edit Prefix Delegation Prefixes screen displays.
9. Modify the prefix, prefix length, or both:
   - **IPv6 Prefix**. Modify the prefix.
   - **IPv6 Prefix Length**. Modify the IPv6 prefix length.
10. Click the **Apply** button.

    Your settings are saved. The modified prefix displays in the List of prefixes for prefix delegation table on the LAN Setup screen.

Remove One or More IPv6 LAN Prefixes for Prefix Delegation

The following procedure describes how to remove one or more prefixes that you no longer need for prefix delegation.

➢ **To remove one or more prefixes for prefix delegation:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > LAN Settings**.

   The LAN Setup screen displays the IPv4 settings.
7. In the upper right, select the **IPv6** radio button.

   The LAN Setup screen displays the IPv6 settings.
8. In the List of Prefixes for Prefix Delegation table, select the check box to the left of each prefix that you want to remove or click the **Select All** button to select all prefixes.
9. Click the **Delete** button.

   The selected prefixes are removed from the List of prefixes for prefix delegation table.

Manage a Stateful DHCPv6 Server and IPv6 Address Pools for the LAN

The following sections provide information about managing a stateful DHCPv6 server and IPv6 address pools for the LAN:

- *Stateful DHCPv6 Server and IPv6 Address Pool for the LAN*
- *Configure a Stateful DHCPv6 Server for the LAN*
- *Add an IPv6 LAN Address Pool*
- *Change an IPv6 LAN Address Pool*

- *Remove One or More IPv6 LAN Address Pools*

Stateful DHCPv6 Server and IPv6 Address Pool for the LAN

With a 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 also must configure IPv6 address pools (see *Add an IPv6 LAN Address Pool* on page 168) so that the DHCPv6 server can assign IPv6 addresses from these pools.

For more information about stateful DHCPv6 servers, see *DHCPv6 LAN Server Concepts and Configuration Roadmap* on page 153.

Configure a Stateful DHCPv6 Server for the LAN

The following procedure describes how to configure a stateful DHCPv6 server and corresponding IPv6 settings for the LAN.

➤ **To configure a stateful DHCPv6 server and corresponding IPv6 settings for the LAN:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

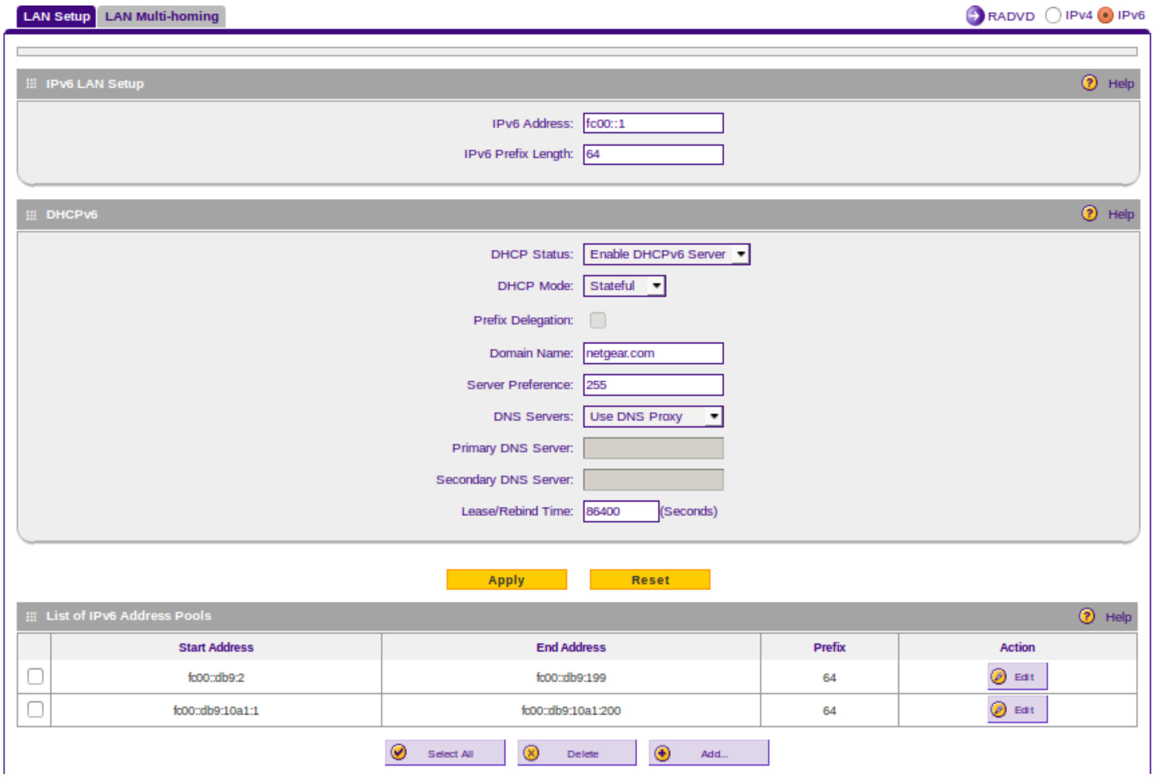
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > LAN Settings**.

   The LAN Setup screen displays the IPv4 settings.
7. In the upper right, select the **IPv6** radio button.

   The LAN Setup screen displays the IPv6 settings. The following figure shows some examples.



IPv6 LAN Setup

IPv6 Address: fc00::1

IPv6 Prefix Length: 64

DHCPv6

DHCP Status: Enable DHCPv6 Server

DHCP Mode: Stateful

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
□	fc00::db9:2	fc00::db9:199	64	Edit
□	fc00::db9:10a1:1	fc00::db9:10a1:200	64	Edit

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

Setting	Description
IPv6 LAN Setup	
IPv6 Address	Enter the LAN IPv6 address. The default address is fc00::1. (For more information, see *IPv6 LANs* on page 153.)
IPv6 Prefix Length	Enter the IPv6 prefix length, for example, 10 or 64. The default prefix length is 64.
DHCPv6	
DHCP Status	Enable the DHCPv6 server by selecting **Enable DHCPv6 Server** from the **DHCP Status** menu. The default menu selection is **Disable DHCPv6 Server**.
DHCP Mode	From the **DHCP Mode** menu, select **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. For stateful DHCPv6, you must add one or more IPv6 address pools (see *Add an IPv6 LAN Address Pool* on page 168). **Note:** If you select **Stateful** from the **DHCP Mode** menu, the **Prefix Delegation** check box is disabled.
Domain Name	Enter the domain name of the DHCP server.

Setting	Description
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	From the **DNS Server** menu, select a DNS server option: • **Use DNS Proxy**. The VPN firewall acts as a proxy for all DNS requests and communicates with the ISP DNS servers that you configure. For information about specifying the ISP DNS servers, see *Manually Configure a Static IPv6 Internet Connection* on page 94. • **Use DNS from ISP**. The VPN firewall uses the ISP DNS servers that you configure. For information about specifying the ISP DNS servers, see *Manually Configure a Static IPv6 Internet Connection* on page 94. • **Use below**. When you select this option, the **Primary DNS Server** and **Secondary 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).

9. Click the **Apply** button.

   Your settings are saved.

Add an IPv6 LAN Address Pool

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. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > LAN Settings**.

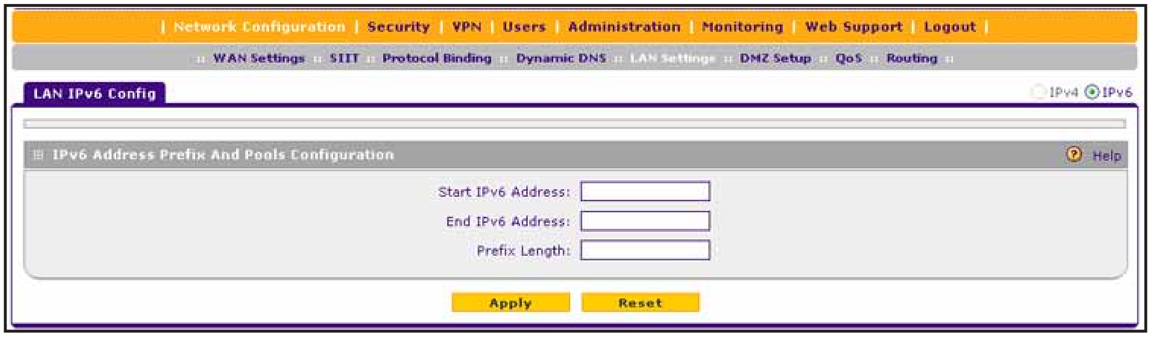
   The LAN Setup screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The LAN Setup screen displays the IPv6 settings.

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

   The LAN IPv6 Config screen displays.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: 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

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

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.

10. Click the **Apply** button.

    Your settings are saved. The new IPv6 address pool is added to the List of IPv6 Address Pools table on the LAN Setup screen for IPv6.

Change an IPv6 LAN Address Pool

The following procedure describes how to change an existing IPv6 LAN address pool.

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

1. On your computer, launch an Internet browser.

2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > LAN Settings**.

   The LAN Setup screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The LAN Setup screen displays the IPv6 settings.

8. In the List of IPv6 Address Pools table, click the **Edit** button for the address pool that you want to change.

   The LAN IPv6 Config screen displays.

9. Change the settings.

   For information about the settings, see *Add an IPv6 LAN Address Pool* on page 168.

10. Click the **Apply** button.

    Your settings are saved. The modified address pool displays in the List of IPv6 Address Pools table on the LAN Setup screen.

Remove One or More IPv6 LAN Address Pools

The following procedure describes how you can remove one or more existing IPv6 LAN address pools that you no longer need.

➢ **To remove one or more IPv6 LAN address pools:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > LAN Settings**.

   The LAN Setup screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The LAN Setup screen displays the IPv6 settings.

8. In the List of IPv6 Address Pools table, select the check box to the left of each address pool that you want to remove, or click the **Select All** button to select all address pools.
9. Click the **Delete** button.

   The selected address pools are removed from the List of IPv6 Address Pools table.

Manage the IPv6 Router Advertisement Daemon for the LAN

If you do not configure stateful DHCPv6 for the LAN but use stateless DHCPv6, you must enable the Router Advertisement Deamon (RADVD).

This requirement applies to both a stateless DHCPv6 server without prefix delegation and a stateless DHCPv6 server with prefix delegation.

If you enabled the ISP DHCPv6 server to assign a prefix through prefix delegation to the VPN firewall (see *Use a DHCPv6 Server to Configure an IPv6 Internet Connection Automatically* on page 90), you do not need to add advertisement prefixes but have the option do so. However, if you did not enable the ISP DHCPv6 server to assign a prefix through prefix delegation to the VPN firewall, you must add advertisement prefixes.

The following sections provide information about managing the IPv6 RADVD for the LAN:

- *IPv6 Router Advertisement Daemon for the LAN*
- *Configure the IPv6 Router Advertisement Daemon for the LAN*
- *View Automatically Added Advertisement Prefixes for the LAN and Manually Add Advertisement Prefixes*
- *Change an Advertisement Prefix for the LAN*
- *Remove One or More Advertisement Prefixes for the LAN*

IPv6 Router Advertisement Daemon for the LAN

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 shows how the VPN firewall obtains information in the LAN if you configure a stateless DHCPv6 server and the RADVD.

Table 2. DHCPv6 and RADVD interaction in the LAN

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

[a] *Both the DHCPv6 server and the RADVD can assign IP addresses.*

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.

Configure the IPv6 Router Advertisement Daemon for the LAN

The following procedure describes how to configure the Router Advertisement Daemon (RADVD) for the LAN.

➢ **To configure the RADVD for the LAN:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

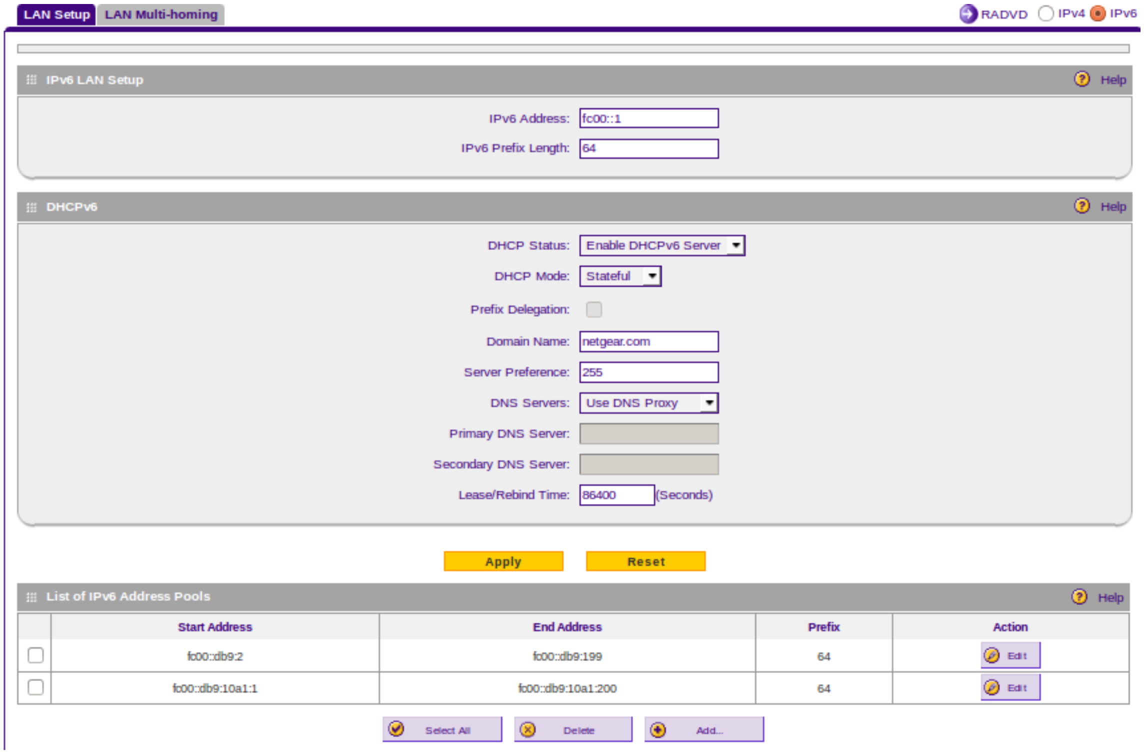
   The Router Status screen displays.

6. Select **Network Configuration > LAN Settings**.

   The LAN Setup screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The LAN Setup screen displays the IPv6 settings. The following figure shows some examples.



IPv6 LAN Setup

IPv6 Address: fc00::1

IPv6 Prefix Length: 64

DHCPv6

DHCP Status: Enable DHCPv6 Server

DHCP Mode: Stateful

Prefix Delegation: □

Domain Name: netgear.com

Server Preference: 255

DNS Servers: Use DNS Proxy

Primary DNS Server:

Secondary DNS Server:

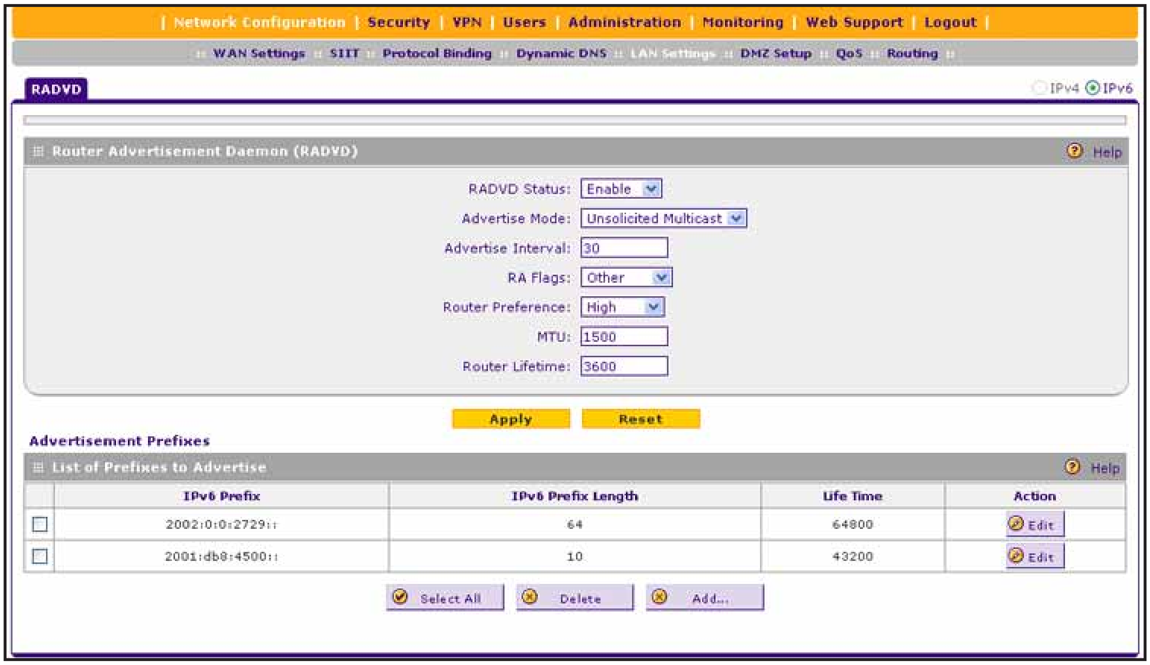
Lease/Rebind Time: 86400 (Seconds)

List of IPv6 Address Pools

	Start Address	End Address	Prefix	Action
□	fc00::db9:2	fc00::db9:199	64	Edit
□	fc00::db9:10a1:1	fc00::db9:10a1:200	64	Edit

8. Click the **RADVD** option arrow in the upper right.

   The following figure shows some examples.


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

Router Advertisement Daemon (RADVD)

RADVD Status: Enable
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
□	2002:0:0:2729::	64	64800	Edit
□	2001:db8:4500::	10	43200	Edit

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

Setting	Description
RADVD Status	From the **RADVD Status** menu, select **Enable**. The RADVD is enabled, and the RADVD fields are available. The default selection is **Disable**. The RADVD is disabled, and the RADVD fields are masked out.
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.

Setting	Description
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 must remain valid. Enter the router lifetime in seconds. This is the period that the advertised prefixes are valid for route determination. The default period is 3600 seconds (one hour). The minimum value is 30 seconds; the maximum value is 9000 seconds.

10. Click the **Apply** button.

    Your settings are saved.

View Automatically Added Advertisement Prefixes for the LAN and Manually Add Advertisement Prefixes

If you enabled the ISP DHCPv6 server to assign a prefix through prefix delegation to the VPN firewall (see *Use a DHCPv6 Server to Configure an IPv6 Internet Connection Automatically* on page 90), you do not need to add advertisement prefixes but have the option do so.

If you did not enable the ISP DHCPv6 server to assign a prefix through prefix delegation to the VPN firewall, you must add advertisement prefixes. You must configure the prefixes that are advertised in the LAN router advertisements (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 view automatically added advertisement prefixes and add an advertisement prefix for the LAN:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

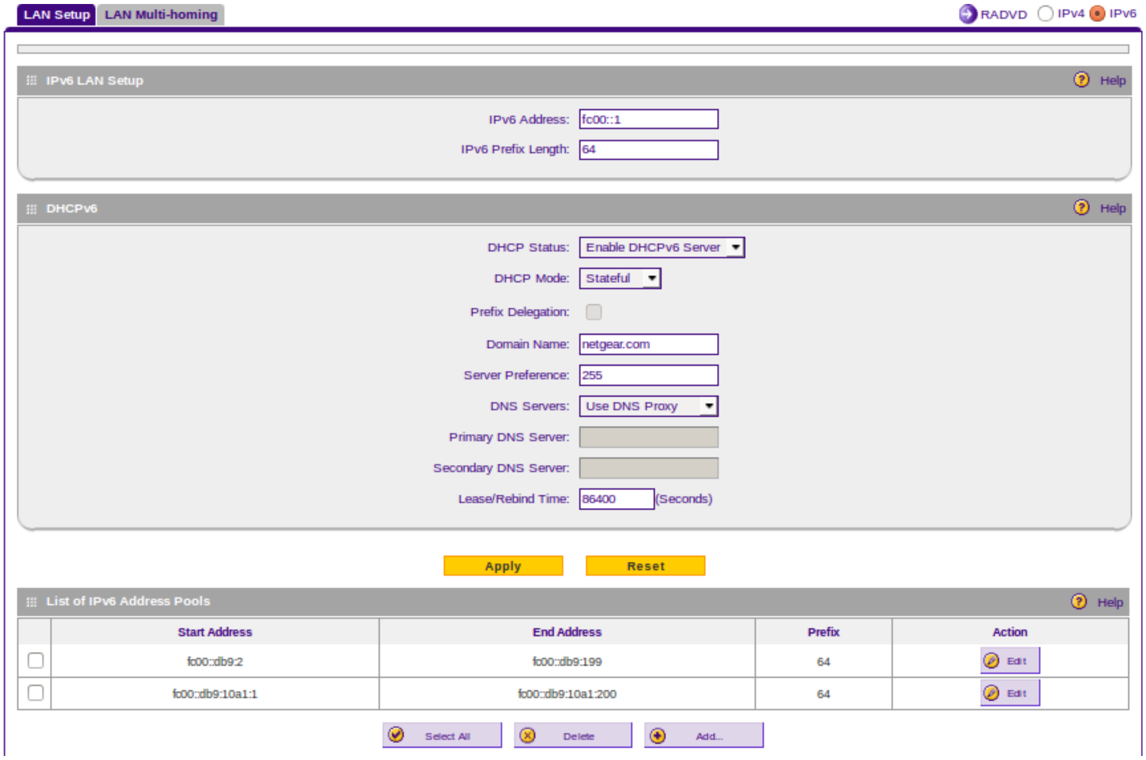
   The Router Status screen displays.

6. Select **Network Configuration > LAN Settings**.

   The LAN Setup screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The LAN Setup screen displays the IPv6 settings. The following figure shows some examples.



IPv6 LAN Setup

IPv6 Address: fc00::1

IPv6 Prefix Length: 64

DHCPv6

DHCP Status: Enable DHCPv6 Server

DHCP Mode: Stateful

Prefix Delegation: □

Domain Name: netgear.com

Server Preference: 255

DNS Servers: Use DNS Proxy

Primary DNS Server:

Secondary DNS Server:

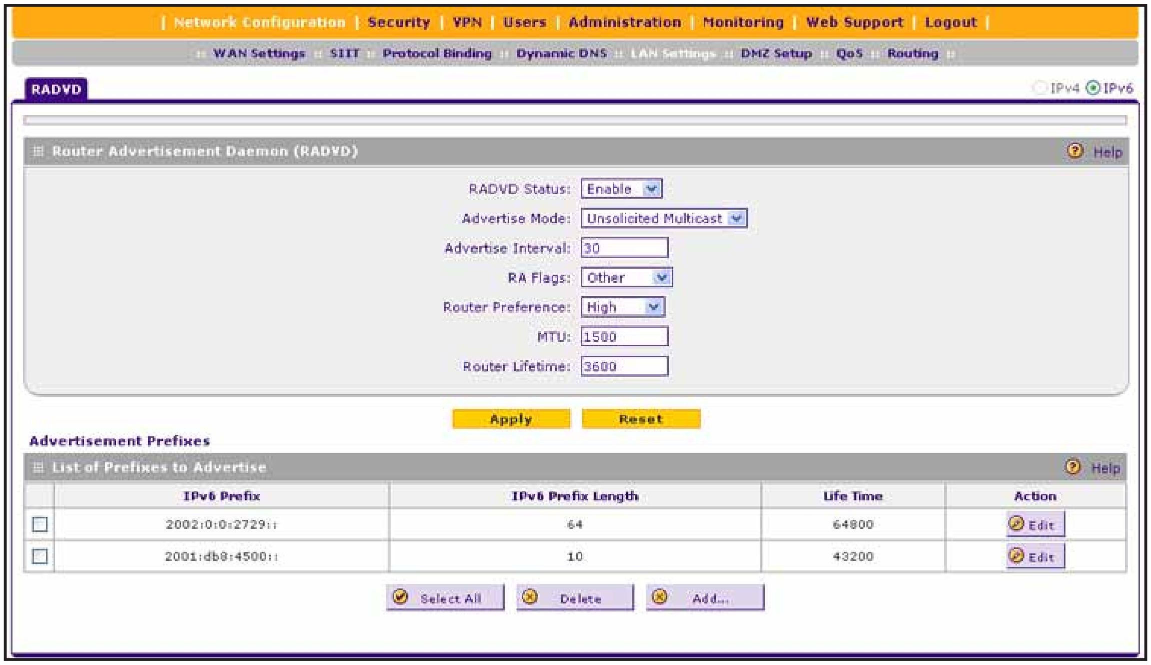
Lease/Rebind Time: 86400 (Seconds)

List of IPv6 Address Pools

	Start Address	End Address	Prefix	Action
□	fc00::db9:2	fc00::db9:199	64	Edit
□	fc00::db9:10a1:1	fc00::db9:10a1:200	64	Edit

8. Click the **RADVD** option arrow in the upper right.

   The following figure shows some examples.


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

Router Advertisement Daemon (RADVD)

RADVD Status: Enable

Advertise Mode: Unsolicited Multicast

Advertise Interval: 30

RA Flags: Other

Router Preference: High

MTU: 1500

Router Lifetime: 3600

Advertisement Prefixes

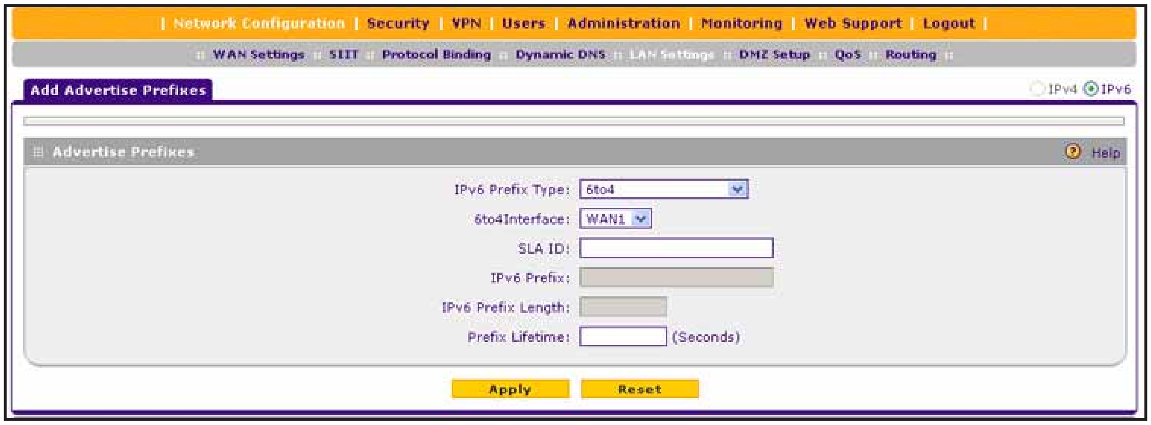
List of Prefixes to Advertise

	IPv6 Prefix	IPv6 Prefix Length	Life Time	Action
□	2002:0:0:2729::	64	64800	Edit
□	2001:db8:4500::	10	43200	Edit

If you enabled the ISP DHCPv6 server to assign a prefix through prefix delegation to the VPN firewall (see *Use a DHCPv6 Server to Configure an IPv6 Internet Connection Automatically* on page 90), the advertisement prefixes that are based on the ISPs assignment are shown in the List of Prefixes to Advertise table. Advertisement prefixes that you add manually also show in the table.

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

   The Add Advertise Prefixes screen displays.


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

Advertise Prefixes

IPv6 Prefix Type: 6to4

6to4Interface: WAN1

SLA ID:

IPv6 Prefix:

IPv6 Prefix Length:

Prefix Lifetime: (Seconds)

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

Setting	Description
IPv6 Prefix Type	Select the IPv6 prefix type: • **6to4**. The prefix is for a 6to4 address. You must select a WAN interface from the **6to4Interface** menu and complete the **SLA ID** field and **Prefix Lifetime** field. The other fields are masked out. • **Global/Local/ISATAP**. The prefix is for a global, local, or ISATAP address. This 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 **6to4Interface** menu and **SLA ID** field are masked out.
6to4Interface	Select a WAN interface from the menu.
SLA ID	Enter the site level aggregation identifier (SLA ID) for the 6to4 address prefix that must be included in the advertisement.
IPv6 Prefix	Enter the IPv6 prefix for the VPN firewall's LAN that must be included in the advertisement.
IPv6 Prefix Length	Enter the IPv6 prefix length (typically 64) that must 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 must remain valid. Enter the prefix lifetime in seconds that must be included in the advertisement. The minimum period is 0 seconds; the maximum period is 65536 seconds.

11. Click the **Apply** button.

    Your settings are saved. The new advertisement prefix is added to the List of Prefixes to Advertise table on the RADVD screen for the LAN.

Change an Advertisement Prefix for the LAN

The following procedure describes how to change an existing advertisement prefix for the LAN.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > LAN Settings**.

   The LAN Setup screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The LAN Setup screen displays the IPv6 settings.

8. Click the **RADVD** option arrow in the upper right.

   The RADVD screen for the LAN displays.

9. In the List of Prefixes to Advertise table, click the **Edit** button for the advertisement prefix that you want to change.

   The Add Advertisement Prefix screen displays.

10. Change the settings.

    For information about the settings, see *View Automatically Added Advertisement Prefixes for the LAN and Manually Add Advertisement Prefixes* on page 175.

11. Click the **Apply** button.

    Your settings are saved. The modified advertisement prefix displays in the List of Prefixes to Advertise table on the RADVD screen for the LAN.

Remove One or More Advertisement Prefixes for the LAN

The following procedure describes how to remove one or more advertisement prefixes that you no longer need for the LAN.

➢ **To remove one or more advertisement prefixes for the LAN:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > LAN Settings**.

   The LAN Setup screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The LAN Setup screen displays the IPv6 settings.

8. Click the **RADVD** option arrow in the upper right.

   The RADVD screen for the LAN displays.

9. In the List of Prefixes to Advertise table, select the check box to the left of each advertisement prefix that you want to remove or click the **Select All** button to select all advertisement prefixes.

10. Click the **Delete** button.

    The selected advertisement prefixes are removed from the List of Prefixes to Advertise table.

Manage IPv6 Multihome LAN IP Addresses

The following sections provide information about managing IPv6 multihome LAN IP addresses:

- *IPv6 Multihome LAN IP Addresses*
- *Add a Secondary LAN IPv6 Address*
- *Change a Secondary LAN IPv6 Address*
- *Remove One or More Secondary LAN IPv6 Addresses*

IPv6 Multihome LAN IP Addresses

If you have computers using different IPv6 networks in the LAN (for example, 2000::2 or 2000::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.

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

Add a Secondary LAN IPv6 Address

The following procedure describes how to add a secondary LAN IPv6 address.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

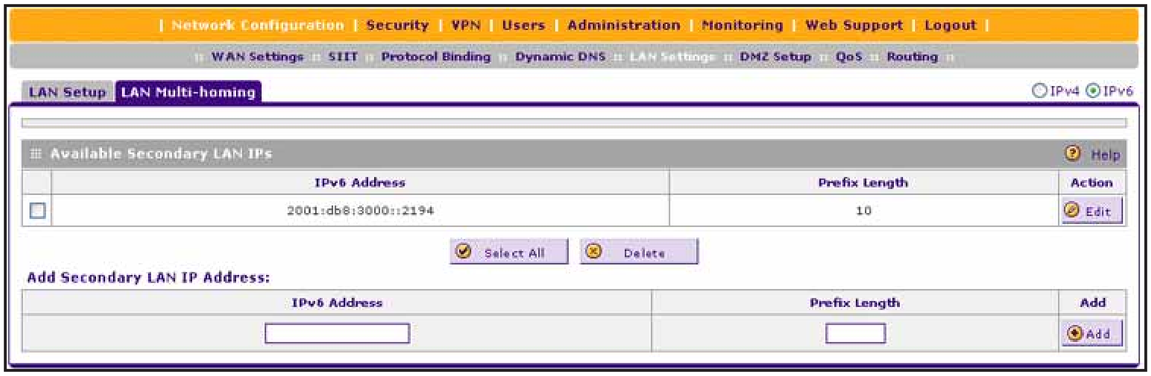
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > LAN Settings > LAN Multi-homing**.

   The LAN Multi-homing screen displays the IPv4 settings.
7. In the upper right, select the **IPv6** radio button.

   The LAN Multi-homing screen displays the IPv6 settings. The following figure shows one example.


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

Available Secondary LAN IPs

	IPv6 Address	Prefix Length	Action
□	2001:db8:3000::2194	10	Edit

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.

8. 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.
9. Click the **Add** button.

   The secondary IP address is added to the Available Secondary LAN IPs table.
10. Repeat *Step 8* and *Step 9* for each secondary IP address that you want to add to the Available Secondary LAN IPs table.

Note: You cannot configure secondary IP addresses 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.

Change a Secondary LAN IPv6 Address

The following procedure describes how to change an existing secondary LAN IPv6 address.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > LAN Settings > LAN Multi-homing**.

   The LAN Multi-homing screen displays the IPv4 settings.
7. In the upper right, select the **IPv6** radio button.

   The LAN Multi-homing screen displays the IPv6 settings.

8. In the Available Secondary LAN IPs table, click the **Edit** button for the secondary IP address that you want to change.

   The Edit LAN Multi-homing screen displays.

9. Modify the IP address or prefix length, or both:
   - **IPv6 Address**. Modify the secondary address that is assigned to the LAN ports.
   - **Prefix Length**. Modify the prefix length for the secondary IP address.

10. Click the **Apply** button.

    Your settings are saved. The modified secondary IP address displays in the Available Secondary LAN IPs table on the LAN Multi-homing screen.

Remove One or More Secondary LAN IPv6 Addresses

The following procedure describes how to remove one or more existing secondary LAN IPv6 addresses that you no longer need.

➢ **To remove one or more secondary LAN IPv6 addresses:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > LAN Settings > LAN Multi-homing**.

   The LAN Multi-homing screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The LAN Multi-homing screen displays the IPv6 settings.

8. In the Available Secondary LAN IPs table, select the check box to the left of each secondary IP address that you want to remove or click the **Select All** button to select all secondary IP addresses.

9. Click the **Delete** button.

   The selected secondary IPv6 addresses are removed from the Available Secondary LAN IPs table.

Manage the DMZ Port for IPv6 Traffic

The following sections provide information about managing the DMZ port for IPv6 traffic:

- *IPv6 DMZ*
- *Manage a Stateless DHCPv6 Server with Prefix Delegation for the DMZ*
- *Manage a Stateful DHCPv6 Server and IPv6 Address Pools for the DMZ*

IPv6 DMZ

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

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

Using a DMZ port is also helpful with online games and videoconferencing applications that are incompatible with NAT. The VPN firewall is programmed to recognize some of these applications and to work correctly with them but 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.

Note the following about the DMZ port:

- The VPN firewall has a separate firewall security profile for the DMZ port. This security profile is also physically independent of the standard firewall security component that is used for the LAN.
- When you enable the DMZ port for IPv4 traffic, IPv6 traffic, or both, the DMZ LED next to LAN port 4 (see *Front Panel* on page 18) lights green to indicate that the DMZ port is enabled.

For information about how to define the DMZ WAN rules and LAN DMZ rules, see *Add DMZ WAN Rules* on page 233 and *Add LAN DMZ Rules* on page 242, respectively.

The IPv6 clients in the DMZ can autoconfigure their own IPv6 address or obtain an IPv6 address through the VPN firewall’s DHCPv6 server for the LAN.

For the IPv6 DMZ, the VPN firewall provides two DHCPv6 server options:

- **Stateless DHCPv6 server**. The IPv6 clients in the DMZ generate their own IP address by using a combination of locally available information and router advertisements, but receive DNS server information from the DHCPv6 server (see *Configure a Stateless DHCPv6 Server for the DMZ* on page 185).

For stateless DHCPv6, you also must configure the RADVD and advertisement prefixes for the DMZ (see *Manage the IPv6 Router Advertisement Daemon for the DMZ* on page 188).

- **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 (see *Configure a Stateful DHCPv6 Server for the DMZ* on page 198). The IP address is a dynamic address.

  For stateful DHCPv6, you also must configure IPv6 address pools for the DMZ (see *Add an IPv6 DMZ Address Pool* on page 200).

Manage a Stateless DHCPv6 Server with Prefix Delegation for the DMZ

The following sections provide information about managing a stateless DHCPv6 server with prefix delegation for the DMZ:

- *Stateless DHCPv6 Server and Prefix Delegation for the DMZ*
- *Configure a Stateless DHCPv6 Server for the DMZ*
- *Manage the IPv6 Router Advertisement Daemon for the DMZ*

Stateless DHCPv6 Server and Prefix Delegation for the DMZ

For a stateless DHCPv6 server for the DMZ, 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 also must configure the RADVD and advertisement prefixes for the DMZ (see *Manage the IPv6 Router Advertisement Daemon for the DMZ* on page 188).

For more information about stateless DHCPv6 servers, see *DHCPv6 LAN Server Concepts and Configuration Roadmap* on page 153.

Configure a Stateless DHCPv6 Server for the DMZ

The following procedure describes how to configure a stateless DHCPv6 server for the DMZ.

➢ **To configure a stateless DHCPv6 server for the DMZ:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

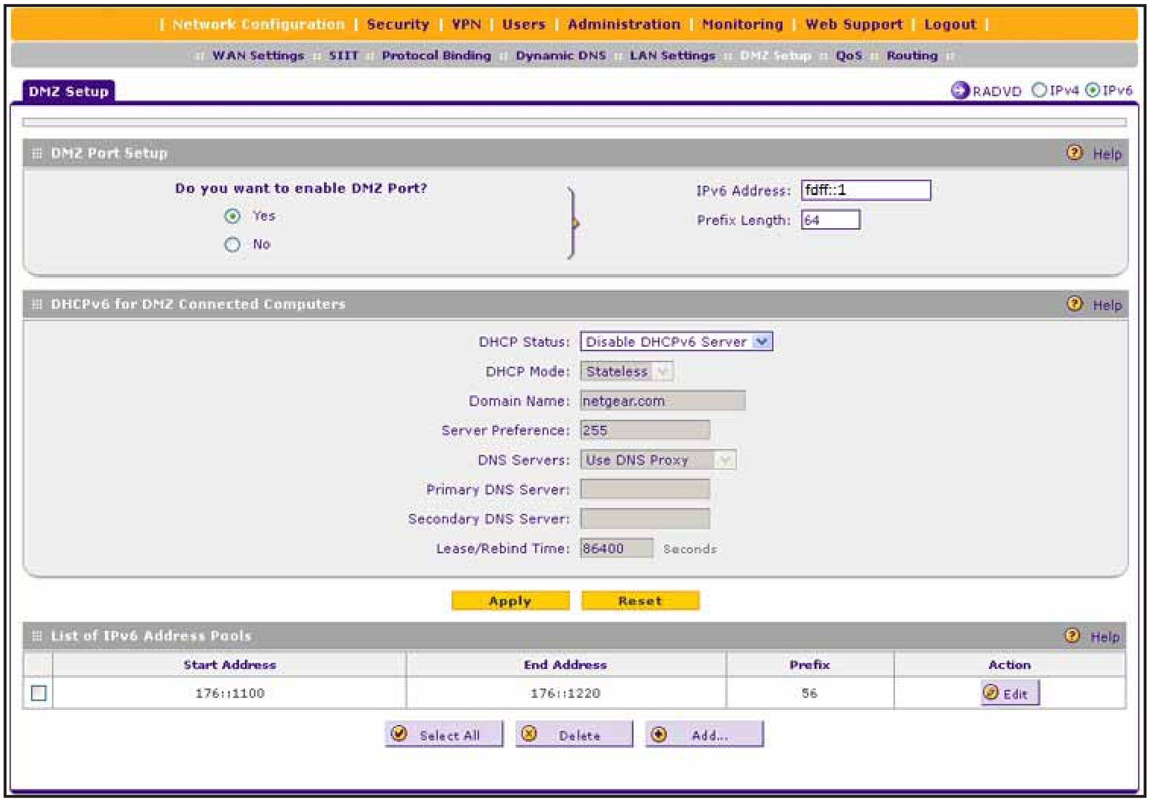
   The Router Status screen displays.

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

   The DMZ Setup screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The DMZ Setup screen displays the IPv6 settings. The following figure shows an example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
DMZ Setup
RADVD ○ IPv4 ● IPv6
DMZ Port Setup
Help
DHCPv6 for DMZ Connected Computers
Help
Apply
Reset
List of IPv6 Address Pools
Help
Edit
Select All
Delete
Add...

Do you want to enable DMZ Port?

● Yes

○ No

IPv6 Address: fdff::1

Prefix Length: 64

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

	Start Address	End Address	Prefix	Action
□	176::1100	176::1220	56	Edit

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

Setting	Description
DMZ Port Setup	
Select the **Yes** radio button to configure the DMZ port settings. Complete the following fields: • **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 fdff::1. • **Prefix Length**. Enter the IPv6 prefix length, for example, 10 or 64. The default prefix length for the DMZ port is 64. **Note:** By default, the DMZ port is disabled. After you configure the DMZ port, you can select the **No** radio button to disable the DMZ port without losing the DMZ configuration.	
DHCPv6 for DMZ Connected Computers	
DHCP Status	Enable the DHCPv6 server by selecting **Enable DHCPv6 Server** from the **DHCP Status** menu. The default menu selection is **Disable DHCPv6 Server**.
DHCP Mode	From the **DHCP Mode** menu, select **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 *Manage the IPv6 Router Advertisement Daemon for the DMZ* on page 188).
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.

Setting	Description
DNS Server	From the **DNS Server** menu, select a DNS server option: • **Use DNS Proxy**. The VPN firewall acts as a proxy for all DNS requests and communicates with the ISP DNS servers that you configure. For information about specifying the ISP DNS servers, see *Manually Configure a Static IPv6 Internet Connection* on page 94. • **Use DNS from ISP**. The VPN firewall uses the ISP DNS servers that you configure. For information about specifying the ISP DNS servers, see *Manually Configure a Static IPv6 Internet Connection* on page 94. • **Use below**. When you select this option, the **Primary DNS Server** and **Secondary 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).

9. Click the **Apply** button.

   Your settings are saved.

Manage the IPv6 Router Advertisement Daemon for the DMZ

Note: If you use a stateless DHCPv6 server for the DMZ, you must configure the Router Advertisement Deamon (RADVD) and advertisement prefixes for the DMZ.

The Router Advertisement Daemon (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.

The following sections provide information about managing the IPv6 RADVD for the DMZ:

- *IPv6 Router Advertisement Daemon for the DMZ*
- *Configure the IPv6 Router Advertisement Daemon for the DMZ*
- *Add an Advertisement Prefix for the DMZ*
- *Change an Advertisement Prefix for the DMZ*
- *Remove One or More Advertisement Prefixes for the DMZ*

IPv6 Router Advertisement Daemon for the DMZ

Hosts and routers in the DMZ use NDP to determine the link-layer addresses and related information of neighbors in the DMZ 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 3. DHCPv6 and RADVD interaction in the DMZ

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

[a] *Both the DHCPv6 server and the RADVD can assign IP addresses.*

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.

Configure the IPv6 Router Advertisement Daemon for the DMZ

The following procedure describes how to configure the Router Advertisement Daemon (RADVD) for the DMZ.

➢ **To configure the RADVD for the DMZ:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

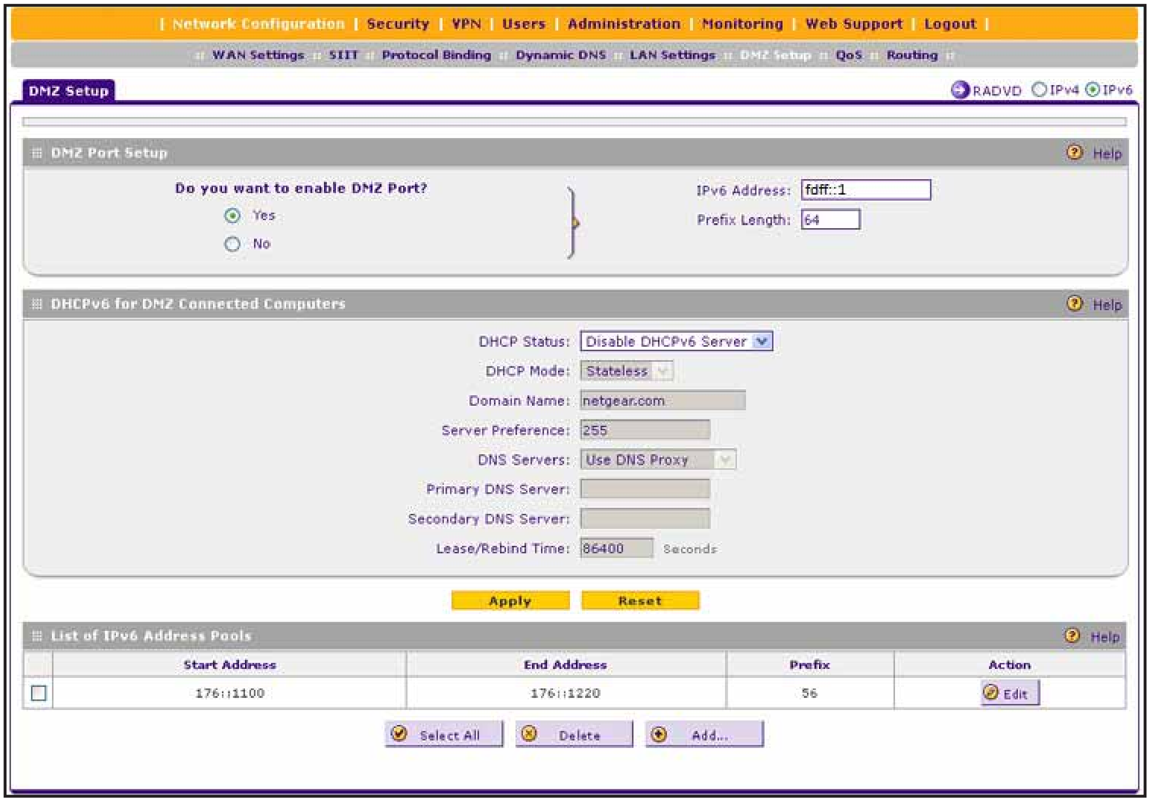
   The Router Status screen displays.

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

   The DMZ Setup screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The DMZ Setup screen displays the IPv6 settings. The following figure shows an example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: 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: fdff::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:

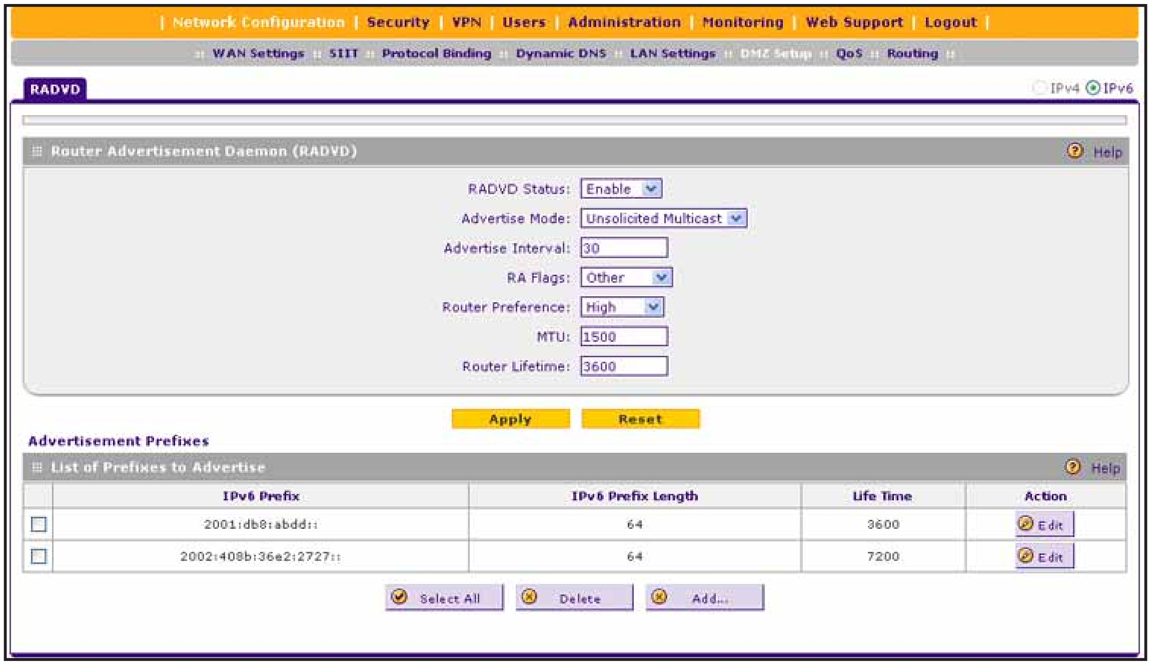
Lease/Rebind Time: 86400 Seconds

List of IPv6 Address Pools

	Start Address	End Address	Prefix	Action
□	176::1100	176::1220	56	Edit

8. Click the **RADVD** option arrow in the upper right.

   The RADVD screen for the DMZ displays. The following figure shows some examples.


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

Router Advertisement Daemon (RADVD)

RADVD Status: Enable
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
□	2001:db8:abdd::	64	3600	Edit
□	2002:408b:36e2:2727::	64	7200	Edit

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

Setting	Description
RADVD Status	From the **RADVD Status** menu, select **Enable**. The RADVD is enabled and the RADVD fields are available. The default selection is **Disable**. The RADVD is disabled and the RADVD fields are masked out.
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.

Setting	Description
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 must remain valid. Enter the router lifetime in seconds. This is the period that the advertised prefixes are valid for route determination. The default period is 3600 seconds (one hour). The minimum value is 30 seconds; the maximum value is 9000 seconds.

10. Click the **Apply** button.

    Your settings are saved.

Add an Advertisement Prefix for the DMZ

You must configure the prefixes that are advertised in the DMZ router advertisements (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. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

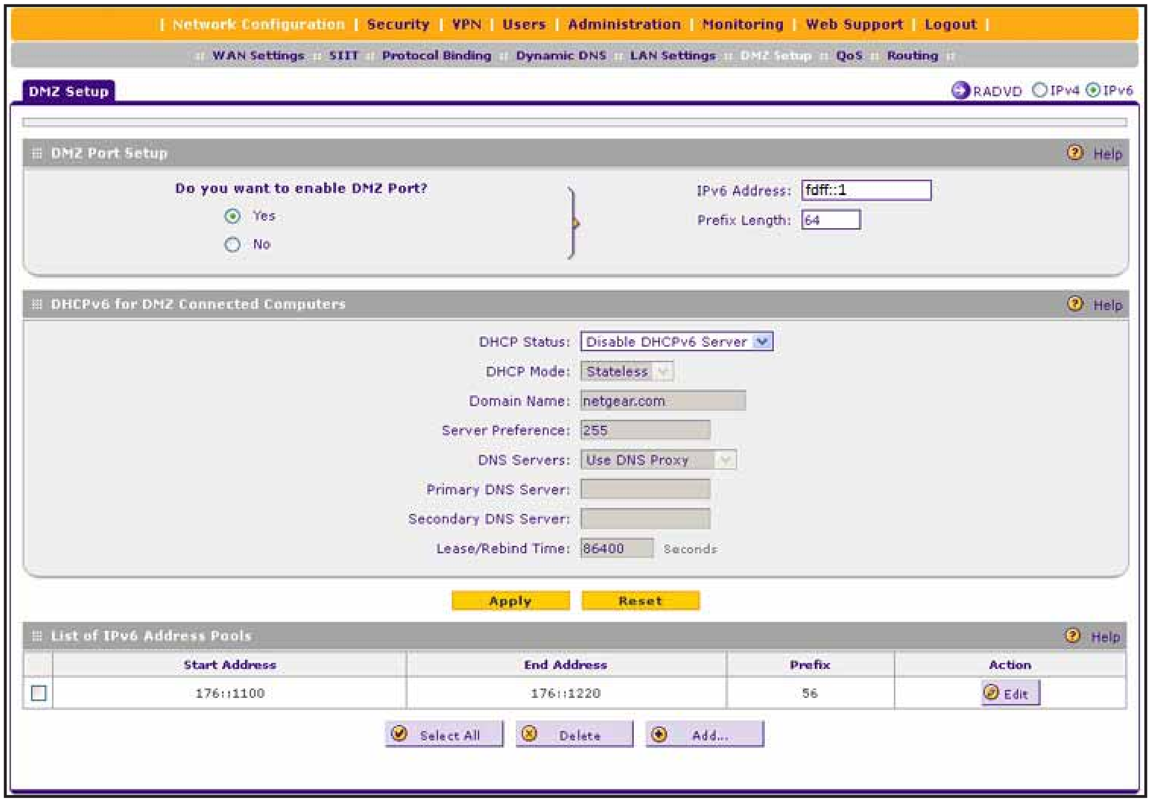
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > DMZ Setup**.

   The DMZ Setup screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The DMZ Setup screen displays the IPv6 settings. The following figure shows an example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: 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: fdff::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:

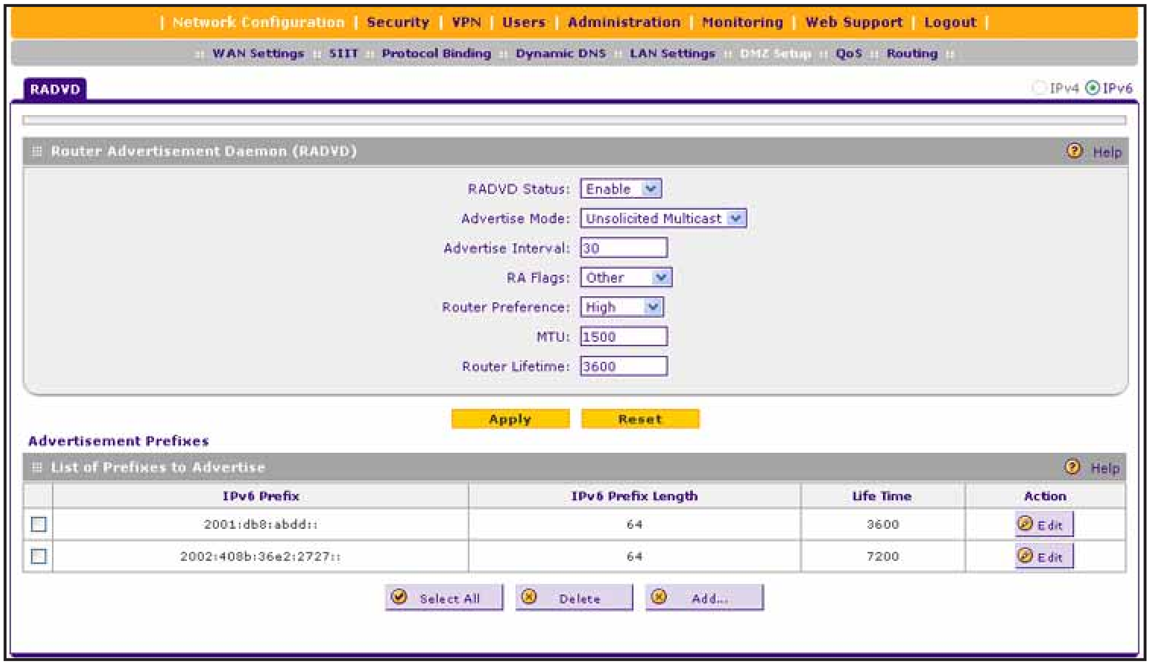
Lease/Rebind Time: 86400 Seconds

List of IPv6 Address Pools

	Start Address	End Address	Prefix	Action
□	176::1100	176::1220	56	Edit

8. Click the **RADVD** option arrow in the upper right.

   The RADVD screen for the DMZ displays. The following figure shows some examples.


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

Router Advertisement Daemon (RADVD)

RADVD Status: Enable

Advertise Mode: Unsolicited Multicast

Advertise Interval: 30

RA Flags: Other

Router Preference: High

MTU: 1500

Router Lifetime: 3600

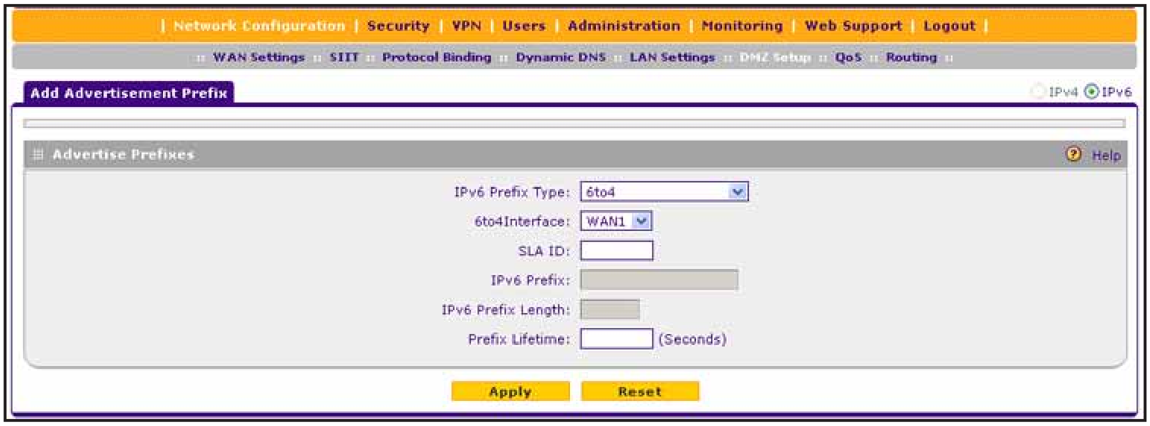
Advertisement Prefixes

List of Prefixes to Advertise

	IPv6 Prefix	IPv6 Prefix Length	Life Time	Action
□	2001:db8:abdd::	64	3600	Edit
□	2002:408b:36e2:2727::	64	7200	Edit

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

The Add Advertisement Prefix screen displays.


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

Advertise Prefixes

IPv6 Prefix Type: 6to4

6to4Interface: WAN1

SLA ID:

IPv6 Prefix:

IPv6 Prefix Length:

Prefix Lifetime: (Seconds)

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

Setting	Description
IPv6 Prefix Type	Select the IPv6 prefix type: • **6to4**. The prefix is for a 6to4 address. You must select a WAN interface from the **6to4Interface** menu and complete the **SLA ID** field and **Prefix Lifetime** field. The other fields are masked out. • **Global/Local/ISATAP**. The prefix is for a global, local, or ISATAP address. This 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 **6to4Interface** menu and **SLA ID** field are masked out.
6to4Interface	Select a WAN interface from the menu.
SLA ID	Enter the site level aggregation identifier (SLA ID) for the 6to4 address prefix that must be included in the advertisement.
IPv6 Prefix	Enter the IPv6 prefix for the VPN firewall’s DMZ that must be included in the advertisement.
IPv6 Prefix Length	Enter the IPv6 prefix length (typically 64) that must 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 must remain valid. Enter the prefix lifetime in seconds that must be included in the advertisement. The minimum period is 0 seconds; the maximum period is 65536 seconds.

11. Click the **Apply** button.

    Your settings are saved. The new IPv6 address pool is added to the List of Prefixes to Advertise table on the RADVD screen for the DMZ.

Change an Advertisement Prefix for the DMZ

The following procedure describes how to change an existing advertisement prefix for the DMZ.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

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

   The DMZ Setup screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The DMZ Setup screen displays the IPv6 settings.

8. Click the **RADVD** option arrow in the upper right.

   The RADVD screen for the DMZ displays.

9. In the List of Prefixes to Advertise table, click the **Edit** button for the advertisement prefix that you want to change.

   The Edit Advertisement Prefix screen displays.

10. Change the settings.

    For information about the settings, see *Add an Advertisement Prefix for the DMZ* on page 192.

11. Click the **Apply** button.

    Your settings are saved. The modified advertisement prefix displays in the List of Prefixes to Advertise table on the RADVD screen for the DMZ.

Remove One or More Advertisement Prefixes for the DMZ

The following procedure describes how to remove one or more advertisement prefixes that you no longer need for the DMZ.

➢ **To remove one or more advertisement prefixes for the DMZ:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

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

   The DMZ Setup screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The DMZ Setup screen displays the IPv6 settings.

8. Click the **RADVD** option arrow in the upper right.

   The RADVD screen for the DMZ displays.

9. In the List of Prefixes to Advertise table, select the check box to the left of each advertisement prefix that you want to remove or click the **Select All** button to select all advertisement prefixes.

10. Click the **Delete** button.

    The selected IPv6 address pools are removed from the List of Prefixes to Advertise table.

Manage a Stateful DHCPv6 Server and IPv6 Address Pools for the DMZ

The following sections provide information about managing a stateful DHCPv6 server and IPv6 address pools for the DMZ:

- *Stateful DHCPv6 Server and IPv6 Address Pool for the DMZ*
- *Configure a Stateful DHCPv6 Server for the DMZ*
- *Add an IPv6 DMZ Address Pool*
- *Change an IPv6 DMZ Address Pool*
- *Stateful DHCPv6 Server and IPv6 Address Pool for the DMZ*

Stateful DHCPv6 Server and IPv6 Address Pool for the DMZ

For a stateful DHCPv6 server for the DMZ, 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 also must configure IPv6 address pools for the DMZ (see *Add an IPv6 DMZ Address Pool* on page 200) so that the DHCPv6 server can assign IPv6 addresses from these pools.

For more information about stateful DHCPv6 servers, see *DHCPv6 LAN Server Concepts and Configuration Roadmap* on page 153.

Configure a Stateful DHCPv6 Server for the DMZ

The following procedure describes how to configure a stateful DHCPv6 server and corresponding IPv6 settings for the DMZ.

➢ **To configure a stateful DHCPv6 server and corresponding IPv6 settings for the DMZ:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

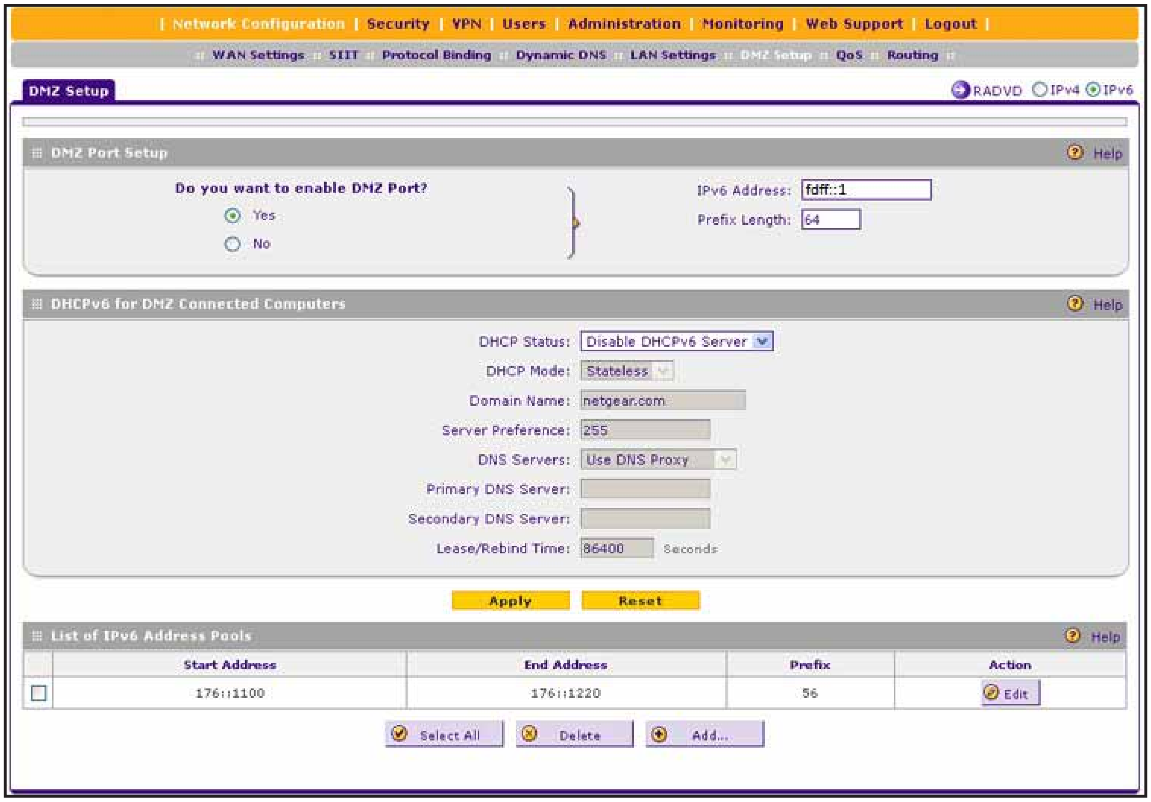
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > DMZ Setup**.

   The DMZ Setup screen displays the IPv4 settings.
7. In the upper right, select the **IPv6** radio button.

   The DMZ Setup screen displays the IPv6 settings. The following figure shows an example.


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

○ IPv4 ● IPv6

DMZ Port Setup

Do you want to enable DMZ Port?

● Yes

○ No

IPv6 Address: fdff::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
□	176::1100	176::1220	56	Edit

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

Setting	Description
DMZ Port Setup	
Select the **Yes** radio button to configure the DMZ port settings. Complete the following fields: • **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 fdff::1. • **Prefix Length**. Enter the IPv6 prefix length, for example, 10 or 64. The default prefix length for the DMZ port is 64. **Note:** By default, the DMZ port is disabled. After you configure the DMZ port, you can select the **No** radio button to disable the DMZ port without losing the DMZ configuration.	
DHCPv6 for DMZ Connected Computers	
DHCP Status	Enable the DHCPv6 server by selecting **Enable DHCPv6 Server** from the **DHCP Status** menu. The default menu selection is **Disable DHCPv6 Server**.
DHCP Mode	From the **DHCP Mode** menu, select **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. For stateful DHCPv6, you must add one or more IPv6 address pools (see *Add an IPv6 DMZ Address Pool* on page 200).

Setting	Description
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 Server	From the **DNS Server** menu, select a DNS server option: • **Use DNS Proxy**. The VPN firewall acts as a proxy for all DNS requests and communicates with the ISP DNS servers that you configure. For information about specifying the ISP DNS servers, see *Manually Configure a Static IPv6 Internet Connection* on page 94. • **Use DNS from ISP**. The VPN firewall uses the ISP DNS servers that you configure. For information about specifying the ISP DNS servers, see *Manually Configure a Static IPv6 Internet Connection* on page 94. • **Use below**. When you select this option, the **Primary DNS Server** and **Secondary 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).

9. Click the **Apply** button.

   Your settings are saved.

Add an IPv6 DMZ Address Pool

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

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

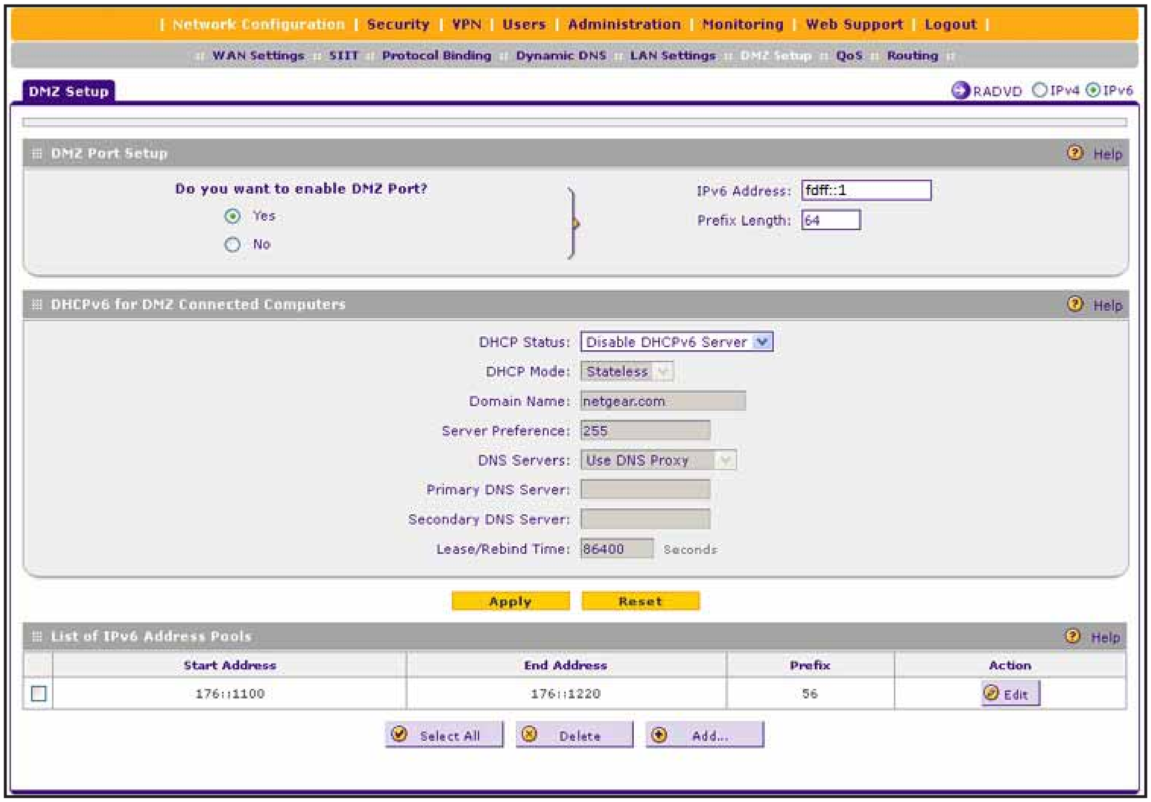
   The Router Status screen displays.

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

   The DMZ Setup screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The DMZ Setup screen displays the IPv6 settings. The following figure shows an example.


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

DMZ Port Setup

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

IPv6 Address: fdff::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

Apply Reset

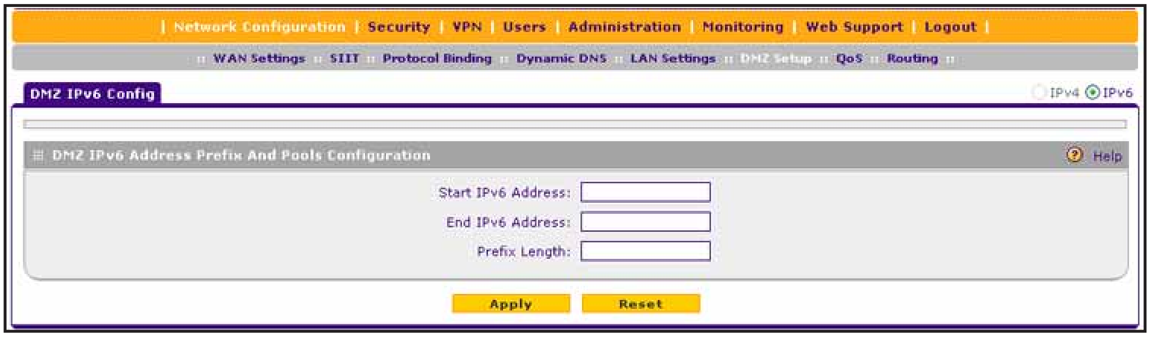
List of IPv6 Address Pools

	Start Address	End Address	Prefix	Action
□	176::1100	176::1220	56	Edit

Select All Delete Add...

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

   The DMZ IPv6 Config screen displays.


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

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

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.

10. Click the **Apply** button.

    Your settings are saved. The new IPv6 address pool is added to the List of IPv6 Address Pools table on the DMZ Setup (IPv6) screen.

Change an IPv6 DMZ Address Pool

The following procedure describes how to change an existing IPv6 DMZ address pool.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

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

   The DMZ Setup screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The DMZ Setup screen displays the IPv6 settings.

8. In List of IPv6 Address Pools table, click the **Edit** button for the address pool that you want to change.

   The DMZ IPv6 Config screen displays.

9. Change the settings.

   For information about the settings, see *Add an IPv6 DMZ Address Pool* on page 200.

10. Click the **Apply** button.

    Your settings are saved. The modified address pool displays in the List of IPv6 Address Pools table on the DMZ Setup screen.

Remove One or More IPv6 DMZ Address Pools

The following procedure describes how to remove one or more existing IPv6 DMZ address pools that you no longer need.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

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

   The DMZ Setup screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The DMZ Setup screen displays the IPv6 settings.

8. In List of IPv6 Address Pools table, select the check box to the left of each address pool that you want to remove or click the **Select All** button to select all address pools.
9. Click the **Delete** button.

   The selected IPv6 address pools are removed from the List of IPv6 Address Pools table.

Manage Static IPv6 Routing

The following sections provide information about managing static IPv6 routing:

- *Add a Static IPv6 Route*
- *Change a Static IPv6 Route*
- *Remove One or More Static IPv6 Routes*

Note: 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.

Add a Static IPv6 Route

The following procedure describes how to add an IPv6 static route to the VPN firewall.

➢ **To add a static IPv6 route to the VPN firewall:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

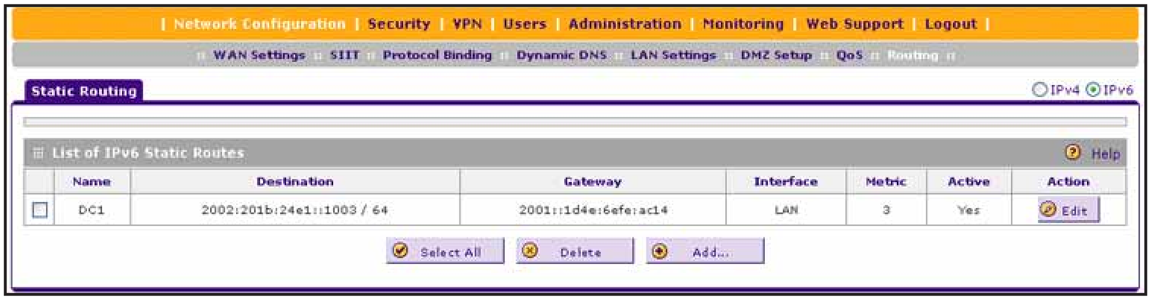
   The Router Status screen displays.

6. Select **Network Configuration > Routing**.

   The Static Routing screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The Static Routing screen displays the IPv6 settings. The following figure contains an example.

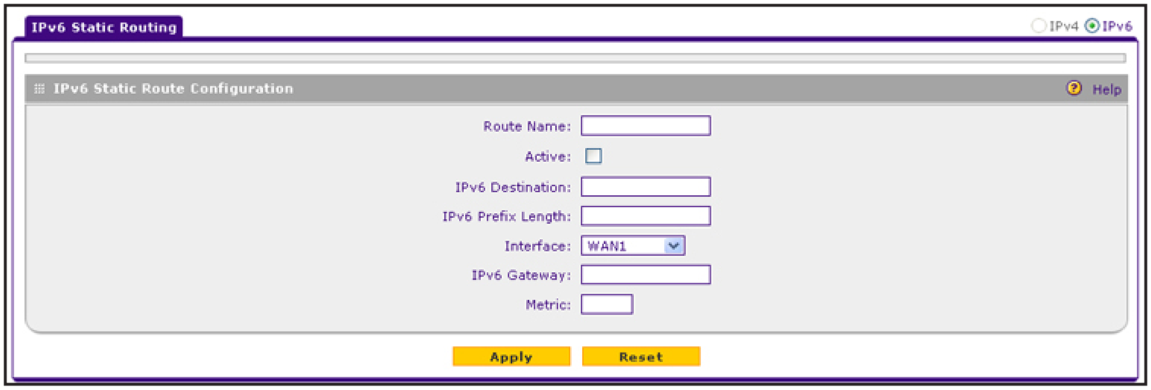


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
Static Routing
○ IPv4 ● IPv6
List of IPv6 Static Routes
Help

	Name	Destination	Gateway	Interface	Metric	Active	Action
□	DC1	2002:201b:24e1::1003 / 64	2001::1d4e:6efe:ac14	LAN	3	Yes	Edit

8. Click the **Add** button under the Static Routes table.

   The IPv6 Static Routing screen displays.



Route Name:	
Active:	□
IPv6 Destination:	
IPv6 Prefix Length:	
Interface:	WAN1
IPv6 Gateway:	
Metric:	

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

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:** You can add a route to the table and make the route inactive if do not need it. 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.

Setting	Description
Interface	From the menu, select the physical or virtual network interface (the WAN1 or WAN2 interface, a sit0 Tunnel, LAN interface, or DMZ interface) through which the route is accessible.
IPv6 Gateway	The gateway IPv6 address through which the destination host or network can be reached.
Metric	The priority of the route. Select a value between 2 and 15. If multiple routes to the same destination exist, the route with the lowest metric is used.

10. Click the **Apply** button.

    Your settings are saved. The new static route is added to the List of IPv6 Static Routes table on the Static Routing screen for IPv6.

Change a Static IPv6 Route

The following procedure describes how to change an existing IPv6 static route.

➢ **To change an IPv6 static route:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > Routing**.

   The Static Routing screen displays the IPv4 settings.
7. In the upper right, select the **IPv6** radio button.

   The Static Routing screen displays the IPv6 settings.
8. In the List of IPv6 Static Routes table, click the **Edit** button for the route that you want to change.

The Edit IPv6 Static Routing screen displays.

9. Change the settings.

   For information about the settings, see *Add a Static IPv6 Route* on page 204.

10. Click the **Apply** button.

    Your settings are saved. The modified route displays in the List of IPv6 Static Routes table on the Static Routes screen.

Remove One or More Static IPv6 Routes

The following procedure describes how to remove one or more existing IPv6 static routes that you no longer need.

➢ **To remove one or more static IPv6 routes:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > Routing**.

   The Static Routing screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The Static Routing screen displays the IPv6 settings.

8. In the List of IPv6 Static Routes table, select the check box to the left of each route that you want to remove or click the **Select All** button to select all routes.
9. Click the **Delete** button.

   The selected routes are removed from the List of IPv6 Static Routes table.

6. Customize Firewall Protection

6

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

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 such as LAN groups and IP groups.

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.

Although firewall rules (also refereed to as service 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 210), you can further refine your control by using the following features and capabilities of the VPN firewall:

- Groups and hosts (see *Manage IPv4 LAN Groups and Hosts* on page 132)
- Firewall objects (see *Manage Firewall Objects* on page 279)
- Allowing or blocking sites (see *Manage Content Filtering* on page 306)
- Source MAC filtering (see *Enable Source MAC Filtering* on page 312)
- Port triggering (see *Manage Port Triggering* on page 325)

Some firewall settings might affect the performance of the VPN firewall. For more information, see *Performance Management* on page 527.

You can configure the VPN firewall to log and email denial of access, general attack, and other information to a specified email address. For information about how to configure logging and notifications, see *Manage Logging, Alerts, and Event Notifications* on page 567.

⚠ WARNING:

Make sure that you first configure the IPv4 WAN routing mode (see *Manage the IPv4 WAN Routing Mode* on page 30) before you configure custom firewall rules. If you change the IPv4 WAN routing mode, all LAN WAN and DMZ WAN inbound rules revert to default settings.

Overview of Rules to Block or Allow Specific Kinds of Traffic

The following sections provide overviews of rules to block and allow specific kinds of traffic:

- *Firewall Rules*
- *Outbound Rules — Service Blocking*
- *Settings for Outbound Rules*
- *Inbound Rules — Port Forwarding*
- *Settings for Inbound Rules*

Firewall Rules

The following sections provide information about firewall rule concepts:

- *Firewall Rules Overview*
- *Default LAN WAN Rules*
- *Default DMZ WAN Rules*
- *Default LAN DMZ Rules*
- *Number of Rules Supported*
- *Categories of Service*
- *Order of Precedence*

Firewall Rules Overview

Firewall rules (also referred to as service rules) are used to block or allow specific traffic passing through from one side to the other. You can apply the firewall rules for blocking and allowing traffic on the VPN firewall to LAN WAN traffic, DMZ WAN traffic, and LAN DMZ traffic.

Inbound rules (WAN to LAN or DMZ) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Outbound rules (LAN or DMZ to WAN) determine what outside resources local users can have access to.

Default LAN WAN Rules

The VPN firewall has two default LAN WAN rules, one for inbound traffic and one for outbound traffic:

- **Inbound**. Block all access from the Internet (the WAN) except responses to requests from the LAN.
- **Outbound**. Allow all access from the LAN to the Internet.

  For information about changing the default LAN WAN outbound rule, see *Change the Default Outbound Policy for LAN WAN Traffic* on page 220.

Default DMZ WAN Rules

For DMZ WAN traffic, the default policy is to block all traffic from and to the Internet.

You can change the default policy by adding DMZ WAN firewall rules that allow specific types of traffic to go out from the DMZ to the Internet (outbound) or to come in from the Internet to the DMZ (inbound). Alternately, for outbound traffic, you can allow all outbound traffic and then block only specific services from passing through the VPN firewall. (Do not use this approach for inbound traffic.)

Default LAN DMZ Rules

For LAN DMZ traffic, the default policy is to block all traffic between the LAN and the DMZ.

You can change the default policy by adding LAN DMZ firewall rules that allow specific types of traffic to go out from the LAN to the DMZ (outbound) or to come in from the DMZ to the LAN (inbound). Alternately, for outbound traffic, you can allow all outbound traffic and then block only specific services from passing through the VPN firewall. (Do not use this approach for inbound traffic.)

Number of Rules Supported

You can configure up to 600 firewall rules on the VPN firewall.

Table 4. Number of supported firewall rule configurations

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

Categories of Service

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 *Manage Customized Services* on page 280).
- **Quality of Service (QoS) priorities**. Each service has its own native priority that impacts its quality of performance and tolerance for jitter or delays. You can change the QoS priority, which changes the traffic mix through the system (see *Manage Quality of Service*

Profiles for IPv4 Firewall Rules on page 293 and *Default Quality of Service Priorities for IPv6 Firewall Rules* on page 298).

- **Bandwidth profiles**. After you configure a bandwidth profile (see *Manage Bandwidth Profiles for IPv4 Traffic* on page 299), you can assign it to a rule.

Order of Precedence

When you define a new rule, the rule is added to the VPN firewall’s configuration and displayed in a table. For any traffic that attempts to pass through the VPN firewall, the packet information is subjected to the rules in the order that they are displayed in the table, beginning at the top of the table and proceeding to the bottom of the table. In some cases, the order of precedence of two or more rules might be important in determining the disposition of a packet. For example, you must place the most strict rules (those with the most specific services or addresses) at the top of the table. For information about how change the order of precedence of rules, see *Manage Existing Firewall Rules* on page 250.

Note: Inbound LAN WAN rules take precedence over inbound DMZ WAN rules. When an inbound packet matches an inbound LAN WAN rule, the VPN firewall does not match the packet against inbound DMZ WAN rules.

Outbound Rules — Service Blocking

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

The VPN firewall has a default outbound LAN WAN rule, which allow all access from the LAN side to the outside, that is, outbound traffic is allowed. For information about changing the default outbound rule, see *Change the Default Outbound Policy for LAN WAN Traffic* on page 220.

For more conceptual information about firewall protection, see *Firewall Protection* on page 209.

Tip: For information about 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 312.

Settings for Outbound Rules

The following table describes the components that let you configure rules for outbound traffic. For information about the actual procedures to configure outbound rules, see the following sections:

- *Add LAN WAN Outbound Service Rules* on page 223
- *Add DMZ WAN Outbound Service Rules* on page 233
- *Add LAN DMZ Outbound Service Rules* on page 242

Table 5. 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 (see *Manage Customized Services* on page 280).	All rules
Action	The action for outgoing connections covered by this rule. The options are as follows: • **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 menu is activated only when you select **BLOCK by schedule, otherwise allow** or **ALLOW by schedule, otherwise block** as the action. For information about how to configure time schedules, see *Define a Schedule* on page 292.	All rules when BLOCK by schedule, otherwise allow or ALLOW by schedule, otherwise block is selected as the action
LAN Users	The settings that determine which computers on your network are affected by this rule. The options are as follows: • **Any**. All computers and devices on your LAN are covered by this rule. • **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. For information about assigning devices to groups, see *Manage the Network Database* on page 133. Groups apply only to IPv4 rules. • **IP Group**. Select the IP group to which the rule applies. For information about assigning IP addresses to groups, see *Manage IP Address Groups* on page 288.	LAN WAN rules LAN DMZ rules

Table 5. Outbound rules overview (continued)

Setting	Description	Outbound Rules
WAN Users	The settings that determine which Internet locations are covered by the rule, based on their IP address. The options are as follows: • **Any**. All Internet IP addresses are covered by this rule. • **Single address**. Enter the required address in the **Start** field. • **Address range**. Enter the required addresses the **Start** and **Finish** fields. • **IP Group**. Select the IP group to which the rule applies. For information about assigning IP addresses to groups, see *Manage IP Address Groups* on page 288.	LAN WAN rules DMZ WAN rules
DMZ Users	The settings that determine which DMZ computers on the DMZ network are covered by this rule. The options are as follows: • **Any**. All computers and devices on your DMZ network are covered by this rule. • **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 Profile or QoS Priority	The priority assigned to IP packets of this service. The priorities are defined by *Type of Service in the Internet Protocol Suite standards*, RFC 1349. The QoS profile determines the priority of a service, which, in turn, determines the quality of that service for the traffic passing through the firewall. The VPN firewall marks the Type of Service (ToS) field as defined in the QoS profiles that you create. For more information, see *Manage Quality of Service Profiles for IPv4 Firewall Rules* on page 293 and *Default Quality of Service Priorities for IPv6 Firewall Rules* on page 298. **Note:** For IPv4 traffic, the VPN firewall does not provide default QoS profiles. That is, if you want to use QoS for IPv4 traffic, you must create QoS profiles. For IPv6 traffic, the VPN firewall does provide QoS profiles but you cannot change them. A QoS profile becomes active only when you apply it to a nonblocking inbound or outbound firewall rule. **Note:** When you apply a QoS profile to a firewall rule for the first time, the performance of the VPN firewall might be affected slightly. **Note:** QoS profiles and QoS priorities do not apply to LAN DMZ rules.	QoS Profile: • IPv4 LAN WAN rules • IPv4 DMZ WAN rules Qos Priority: • IPv6 LAN WAN rules • IPv6 DMZ WAN rules

Table 5. Outbound rules overview (continued)

Setting	Description	Outbound Rules
Bandwidth Profile	Bandwidth limiting determines how the data is sent to and from your host. The purpose of bandwidth limiting is to provide a solution for limiting the outgoing and incoming traffic, thus preventing the LAN users from consuming all the bandwidth of the Internet link. For more information, see *Manage Bandwidth Profiles for IPv4 Traffic* on page 299. For outbound traffic, you can configure bandwidth limiting only on the WAN interface for a LAN WAN rule. **Note:** When you enable a bandwidth profile, the performance of the VPN firewall might be affected slightly. **Note:** Bandwidth limiting does not apply to the DMZ interface.	IPv4 LAN WAN rules
Log	The setting that determines whether packets covered by this rule are logged. The options are as follows: • **Always**. Always log traffic that matches this rule. This is useful when you are debugging your rules. • **Never**. Never log traffic that matches this rule.	All rules
NAT IP	The setting that specifies whether the source address of the outgoing packets on the WAN is autodetected, is assigned the address of the WAN interface, or is a different IP address. You can specify these settings only for outbound traffic of the WAN interface. The options are as follows: • **Auto**. The source address of the outgoing packets is autodetected through the configured routing and load balancing rules. • **WAN Interface Address**. All the outgoing packets on the WAN are assigned to the address of the specified WAN interface. • **Single Address**. All the outgoing packets on the WAN are assigned to the specified IP address, for example, a secondary WAN address that you have configured. **Note:** The **NAT IP** menu is available only when the WAN mode is NAT. **Note:** If you select **Single Address** from the **NAT IP** menu, the IP address specified must fall under the WAN subnet.	IPv4 LAN WAN rules IPv4 DMZ WAN rules

Inbound Rules — Port Forwarding

The VPN firewall has a default inbound LAN WAN rule, which blocks all access from outside except responses to requests from the LAN side.

If you have enabled Network Address Translation (NAT), your network presents *one* IP address only to the Internet, and outside users cannot directly access any of your local computers (LAN users). For information about configuring NAT, see *Network Address Translation Overview* on page 30. 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 known as port forwarding.

⚠ WARNING:

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

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). By default, 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. For information about changing this default behavior, see *Manage Protection Against Common Network Attacks* on page 266.

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

- If your external IP address is assigned dynamically by your ISP (DHCP enabled), the IP address might change periodically as the DHCP lease expires. Consider using Dynamic DNS so that external users can always find your network (see *Manage Dynamic DNS Connections* on page 63).
- If the IP address of the local server computer is assigned by DHCP, it might change when the computer is rebooted. To avoid this situation, configure a reserved IP address that is bound to the MAC address of the server (see *DHCP Address Reservation* on page 133).
- Local computers must access the local server by using the computers' local LAN addresses. Attempts by local computers to access the server using the external WAN IP address fail.

For more conceptual information about firewall protection, see *Firewall Protection* on page 209.

Tip: For information about yet another way to allow certain types of inbound traffic that would otherwise be blocked by the firewall, see *Manage Port Triggering* on page 325.

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

Settings for Inbound Rules

The following table describes the components that let you configure rules for inbound traffic. For information about the actual procedures to configure inbound rules, see the following sections:

- *Add LAN WAN Inbound Service Rules* on page 228
- *Add DMZ WAN Inbound Service Rules* on page 237
- *Add LAN DMZ Inbound Service Rules* on page 246

Table 6. 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 (see *Manage Customized Services* on page 280).	All rules
Action	The action for outgoing connections covered by this rule. The options are as follows: • **BLOCK always** • **BLOCK by schedule, otherwise allow** • **ALLOW always** • **ALLOW by schedule, otherwise block** **Note:** Any inbound traffic that is not blocked by rules you create is allowed by the default rule.	All rules
Select Schedule	The time schedule (that is, Schedule1, Schedule2, or Schedule3) that is used by this rule. This menu is activated only when you select **BLOCK by schedule, otherwise allow** or **ALLOW by schedule, otherwise block** as the action. For information about how to configure time schedules, see *Define a Schedule* on page 292.	All rules when BLOCK by schedule, otherwise allow or ALLOW by schedule, otherwise block is selected as the action
Send to LAN Server	The LAN server address determines which computer on your network is hosting this service rule. (You can also translate this address to a port number.) The options are as follows: • **Single address**. Enter the required address in the **Start** field to apply the rule to a single device on your LAN. • **Address range**. Enter the required addresses in the **Start** and **Finish** fields to apply the rule to a range of devices.	IPv4 LAN WAN rules
Send to DMZ Server	The DMZ server address determines which computer on your network is hosting this service rule. (You can also translate this address to a port number.)	IPv4 DMZ WAN rules
Translate to Port Number	If the LAN server or DMZ server that is hosting the service is using a port other than the default port for the service, you can select this setting and specify a port number. If the service is using the default port, you do not need to select this setting.	IPv4 LAN WAN rules IPv4 DMZ WAN rules

Table 6. Inbound rules overview (continued)

Setting	Description	Inbound Rules
WAN Destination IP Address	The setting that determines the destination IP address applicable to incoming traffic. This is the public IP address that maps to the internal LAN server. This can be either the address of the WAN interface or another public IP address. You can also enter an address range. Enter the required addresses in the **Start** and **Finish** fields to apply the rule to a range of devices.	IPv4 LAN WAN rules IPv4 DMZ WAN rules
LAN Users	These settings apply to a LAN WAN inbound rule when the WAN mode is classical routing and determine which computers on your network are covered by this rule. The options are as follows: • **Any**. All computers and devices on your LAN are covered by this rule. • **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. For information about assigning devices to groups, see *Manage the Network Database* on page 133. Groups apply only to IPv4 rules. • **IP Group**. Select the IP group to which the rule applies. For information about assigning IP addresses to groups, see *Manage IP Address Groups* on page 288. **Note:** For IPv4 LAN WAN inbound rules, this field does not apply when the WAN mode is NAT because your network presents only *one* IP address to the Internet.	LAN WAN rules LAN DMZ rules
WAN Users	The settings that determine which Internet locations are covered by the rule, based on their IP address. The options are as follows: • **Any**. All Internet IP addresses are covered by this rule. • **Single address**. Enter the required address in the **Start** field. • **Address range**. Enter the required addresses in the **Start** and **Finish** fields. • **IP Group**. Select the IP group to which the rule applies. For information about assigning IP addresses to groups, see *Manage IP Address Groups* on page 288.	LAN WAN rules DMZ WAN rules

Table 6. Inbound rules overview (continued)

Setting	Description	Inbound Rules
DMZ Users	The settings that determine which DMZ computers on the DMZ network are covered by this rule. The options are as follows: • **Any**. All computers and devices on your DMZ network are covered by this rule. • **Single address**. Enter the required address in the **Start** field to apply the rule to a single computer on the DMZ network. • **Address range**. Enter the required addresses in the **Start** and **Finish** fields to apply the rule to a range of DMZ computers. **Note:** For IPv4 DMZ WAN inbound rules, this field does not apply when the WAN mode is NAT because your network presents only *one* IP address to the Internet.	DMZ WAN rules LAN DMZ rules
QoS Profile	The priority assigned to IP packets of this service. The priorities are defined by *Type of Service in the Internet Protocol Suite standards*, RFC 1349. The QoS profile determines the priority of a service, which, in turn, determines the quality of that service for the traffic passing through the firewall. The VPN firewall marks the Type of Service (ToS) field as defined in the QoS profiles that you create. For more information, see *Manage Quality of Service Profiles for IPv4 Firewall Rules* on page 293. **Note:** For IPv4 traffic, the VPN firewall does not provide default QoS profiles. That is, if you want to use QoS for IPv4 traffic, you must create QoS profiles. For IPv6 traffic, the VPN firewall does provide QoS profiles but you cannot change them. A QoS profile becomes active only when you apply it to a nonblocking inbound or outbound firewall rule. **Note:** When you apply a QoS profile to a firewall rule for the first time, the performance of the VPN firewall might be affected slightly. **Note:** QoS profiles do not apply to LAN DMZ rules.	IPv4 LAN WAN rules IPv4 DMZ WAN rules

Table 6. Inbound rules overview (continued)

Setting	Description	Inbound Rules
Log	The setting that determines whether packets covered by this rule are logged. The options are as follows: • **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 *Manage Bandwidth Profiles for IPv4 Traffic* on page 299. For inbound traffic, you can configure bandwidth limiting only on the LAN interface for a LAN WAN rule. **Note:** When you enable a bandwidth profile, the performance of the VPN firewall might be affected slightly. **Note:** Bandwidth limiting does not apply to the DMZ interface.	IPv4 LAN WAN rules

Change the Default Outbound Policy for LAN WAN Traffic

The default outbound policy allows all traffic to the Internet to pass through. You can then apply firewall rules 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.

The following sections provide information about changing the default outbound policy for LAN WAN traffic:

- *Change the Default LAN WAN Outbound Policy for IPv4 Traffic*
- *Change the Default LAN WAN Outbound Policy for IPv6 Traffic*

Change the Default LAN WAN Outbound Policy for IPv4 Traffic

The following procedure describes how to change the default outbound policy for IPv4 traffic from the LAN to the WAN.

➢ **To change the default outbound policy for LAN WAN IPv4 traffic:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

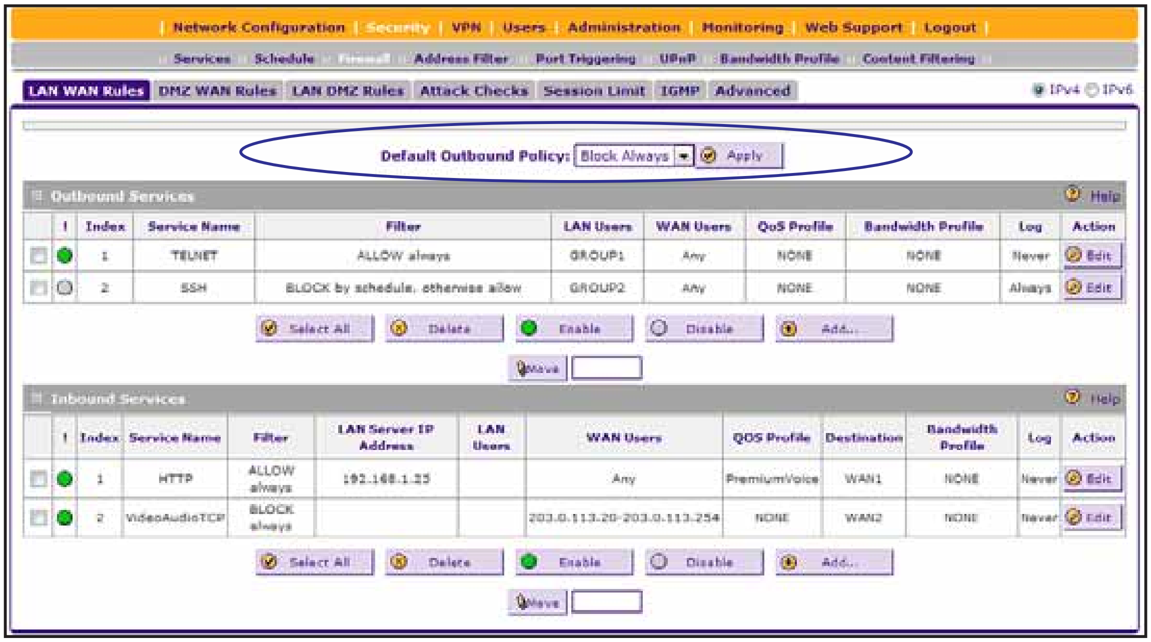
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > Firewall**.

   The Firewall submenu tabs display with the LAN WAN Rules screen in view, displaying the IPv4 settings. The following figure shows examples.


| 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 | IGMP | Advanced
● IPv4 ○ IPv6
Apply
Help
Select All | Delete | Enable | Disable | Add...
Move

Default Outbound Policy: Block Always

Outbound Services

	!	Index	Service Name	Filter	LAN Users	WAN Users	QoS Profile	Bandwidth Profile	Log	Action
□	●	1	TELNET	ALLOW always	GROUP1	Any	NONE	NONE	Never	Edit
□	○	2	SSH	BLOCK by schedule, otherwise allow	GROUP2	Any	NONE	NONE	Always	Edit

Inbound Services

	!	Index	Service Name	Filter	LAN Server IP Address	LAN Users	WAN Users	QOS Profile	Destination	Bandwidth Profile	Log	Action
□	●	1	HTTP	ALLOW always	192.168.1.25		Any	PremiumVoice	WAN1	NONE	Never	Edit
□	●	2	VideoAudioTCP	BLOCK always			203.0.113.20-203.0.113.254	NONE	WAN2	NONE	Never	Edit

7. From the **Default Outbound Policy** menu, select **Block Always**.

   By default, **Allow Always** is selected.

8. Click the **Apply** button.

   Your settings are saved.

Change the Default LAN WAN Outbound Policy for IPv6 Traffic

The following procedure describes how to change the default outbound policy for IPv6 traffic from the LAN to the WAN.

- **To change the default outbound policy for LAN WAN IPv6 traffic:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

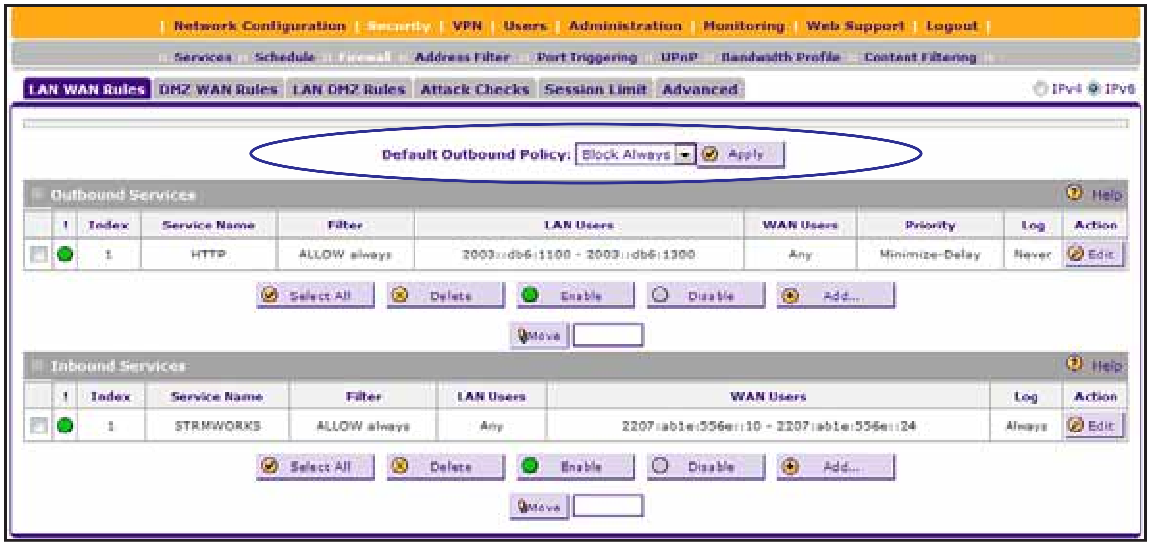
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Firewall**.

   The Firewall submenu tabs display with the LAN WAN Rules screen in view, displaying the IPv4 settings.
7. In the upper right, select the **IPv6** radio button.

   The LAN WAN Rules screen displays the IPv6 settings. The following figure shows examples.



Default Outbound Policy: Block Always

Outbound Services

	!	Index	Service Name	Filter	LAN Users	WAN Users	Priority	Log	Action
□	●	1	HTTP	ALLOW always	2003::db6:1100 - 2003::db6:1300	Any	Minimize-Delay	Never	Edit

Inbound Services

	!	Index	Service Name	Filter	LAN Users	WAN Users	Log	Action
□	●	1	STRMWORKS	ALLOW always	Any	2207:ab1e:556e::10 - 2207:ab1e:556e::24	Always	Edit

8. From the **Default Outbound Policy** menu, select **Block Always**.

   By default, **Allow Always** is selected.

9. Click the **Apply** button.

   Your settings are saved.

Add LAN WAN Rules

The following sections provide information about managing LAN WAN rules:

- *Add LAN WAN Outbound Service Rules*
- *Add LAN WAN Inbound Service Rules*

Add 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 a schedule.

⚠ 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.

The following sections provide information about adding LAN WAN outbound service rules:

- *Add an IPv4 LAN WAN Outbound Rule*

- *Add an IPv6 LAN WAN Outbound Rule*

Add an IPv4 LAN WAN Outbound Rule

The following procedure describes how to add an IPv4 LAN WAN outbound rule.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

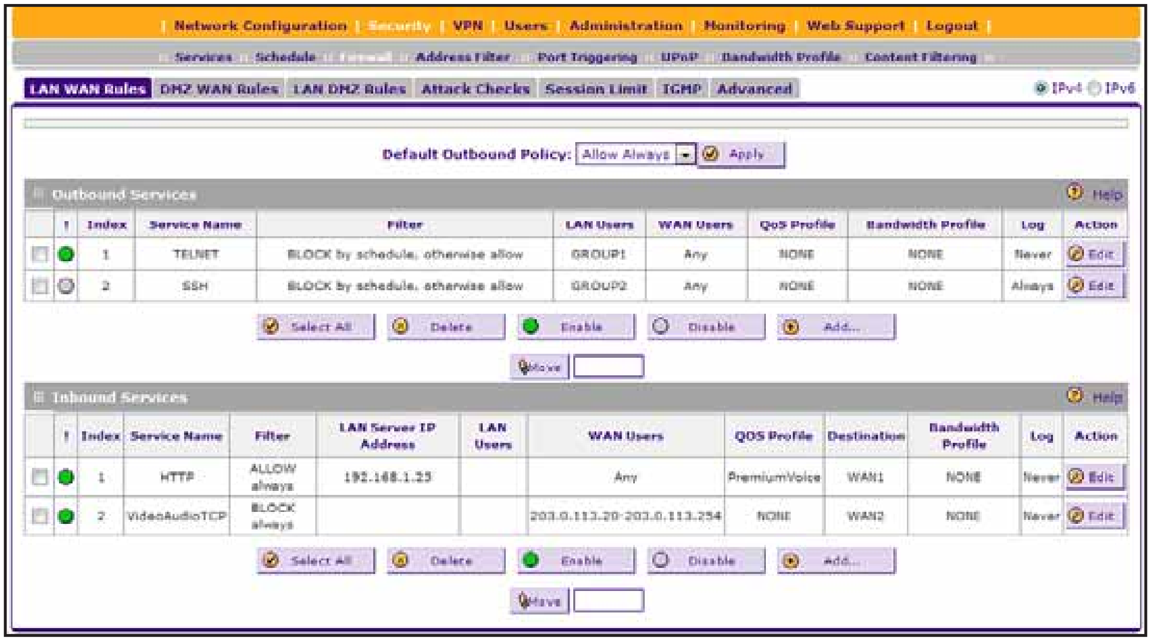
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Firewall**.

   The Firewall submenu tabs display with the LAN WAN Rules screen in view, displaying the IPv4 settings. The following figure shows examples.


| 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
IGMP
Advanced
● IPv4 ○ IPv6
Apply
Help
Select All
Delete
Enable
Disable
Add...
Move

Default Outbound Policy: Allow Always

Outbound Services

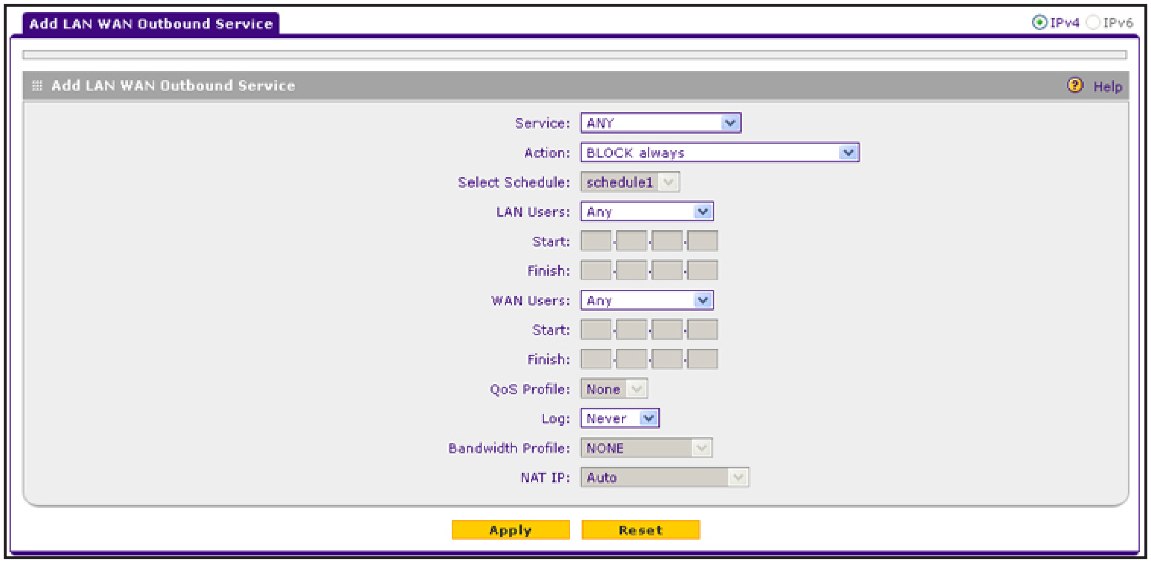
	!	Index	Service Name	Filter	LAN Users	WAN Users	QoS Profile	Bandwidth Profile	Log	Action
□	●	1	TELNET	BLOCK by schedule, otherwise allow	GROUP1	Any	NONE	NONE	Never	Edit
□	○	2	SSH	BLOCK by schedule, otherwise allow	GROUP2	Any	NONE	NONE	Always	Edit

Inbound Services

	!	Index	Service Name	Filter	LAN Server IP Address	LAN Users	WAN Users	QOS Profile	Destination	Bandwidth Profile	Log	Action
□	●	1	HTTP	ALLOW always	192.168.1.25		Any	PremiumVoice	WAN1	NONE	Never	Edit
□	●	2	VideoAudioTCP	BLOCK always			203.0.113.20-203.0.113.254	NONE	WAN2	NONE	Never	Edit

7. Under the Outbound Services table, click the **Add** button.

   The Add LAN WAN Outbound Service screen for IPv4 displays.



Add LAN WAN Outbound Service

Service:	ANY
Action:	BLOCK always
Select Schedule:	schedule1
LAN Users:	Any
Start:	
Finish:	
WAN Users:	Any
Start:	
Finish:	
QoS Profile:	None
Log:	Never
Bandwidth Profile:	NONE
NAT IP:	Auto

8. Make your selections from the menus and enter the settings.

   For more information about the menus and settings, see *Settings for Outbound Rules* on page 212.

The following table lists the menus that apply to an IPv4 LAN WAN outbound rule.

Menus that apply to all IPv4 LAN WAN outbound rules	Menus that apply only when your selection from the Action menu is *not* BLOCK always
Service	Select Schedule **Note:** This menu is available only when the selection from the **Action** menu includes *by schedule*.
Action	QoS Profile
LAN Users	Bandwidth Profile
WAN Users	NAT IP **Note:** This menu is available only when the WAN mode is NAT.
Log	

9. Click the **Apply** button.

   Your settings are saved. The new rule is added to the Outbound Services table on the LAN WAN Rules screen.

Add an IPv6 LAN WAN Outbound Rule

The following procedure describes how to add an IPv6 LAN WAN outbound rule.

➢ To add an IPv6 LAN WAN outbound rule:

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

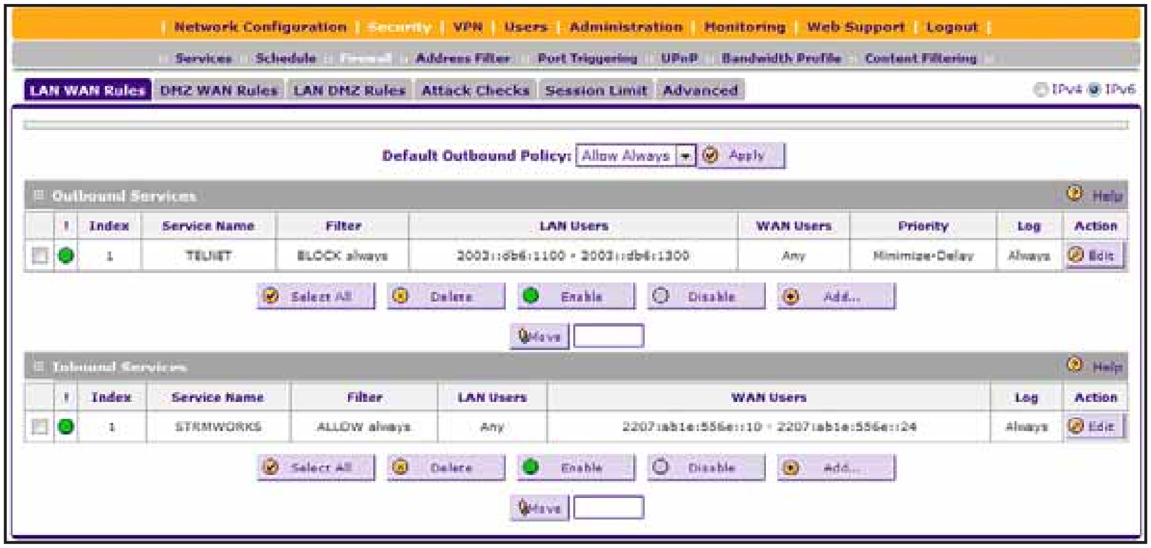
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Firewall**.

The Firewall submenu tabs display with the LAN WAN Rules screen in view, displaying the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The LAN WAN Rules screen displays the IPv6 settings.


| 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...
Move

Default Outbound Policy: Allow Always

Outbound Services

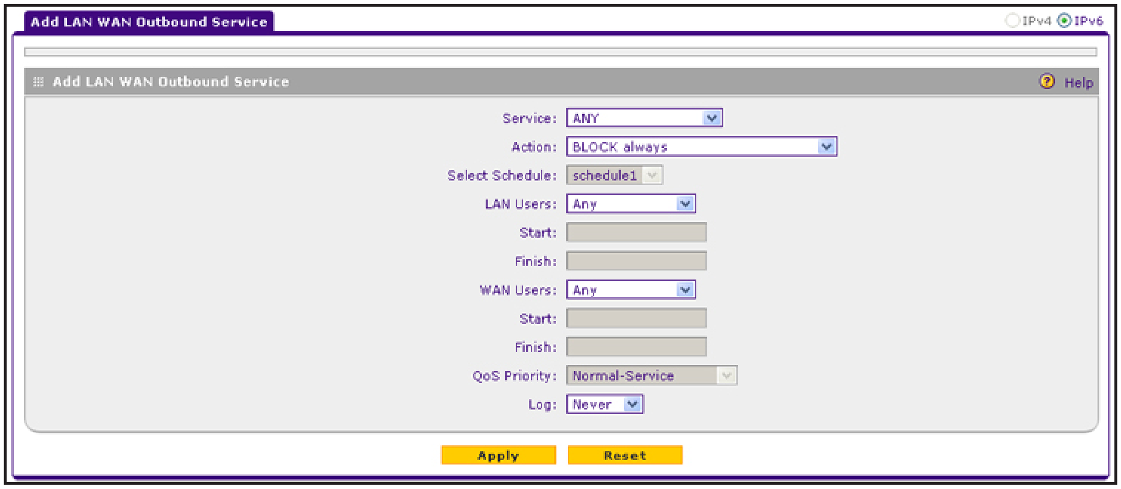
	!	Index	Service Name	Filter	LAN Users	WAN Users	Priority	Log	Action
□	●	1	TELNET	BLOCK always	2003::db6:1100 - 2003::db6:1300	Any	Minimize-Delay	Always	Edit

Inbound Services

	!	Index	Service Name	Filter	LAN Users	WAN Users	Log	Action
□	●	1	STRMWORKS	ALLOW always	Any	2207:ab1e:556e::10 - 2207:ab1e:556e::24	Always	Edit

8. Under the Outbound Services table, click the **Add** button.

   The Add LAN WAN Outbound Service screen for IPv6 displays.



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

9. Make your selections from the menus and enter the settings.

   For more information about the menus and settings, see *Settings for Outbound Rules* on page 212.

The following table lists the menus that apply to an IPv6 LAN WAN outbound rule.

Menus that apply to all IPv6 LAN WAN outbound rules	Menus that apply only when your selection from the Action menu is *not* BLOCK always
Service	Select Schedule **Note:** This menu is available only when the selection from the **Action** menu includes *by schedule*.
Action	QoS Priority
LAN Users	
WAN Users	
Log	

10. Click the **Apply** button.

    Your settings are saved. The new rule is added to the Outbound Services table on the LAN WAN Rules screen.

Add LAN WAN Inbound Service Rules

By default, all inbound traffic (from the Internet to the LAN) is blocked. 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.

WARNING:

Make sure that you first configure the IPv4 WAN routing mode (see *Manage the IPv4 WAN Routing Mode* on page 30) before you configure custom firewall rules. If you change the IPv4 WAN routing mode, all LAN WAN inbound rules revert to default settings.

The following sections provide information about adding LAN WAN inbound service rules:

- *Add an IPv4 LAN WAN Inbound Rule*
- *Add an IPv6 LAN WAN Inbound Rule*

Add an IPv4 LAN WAN Inbound Rule

The following procedure describes how you can add an IPv4 LAN WAN inbound rule.

➢ To add an IPv4 LAN WAN inbound rule:

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

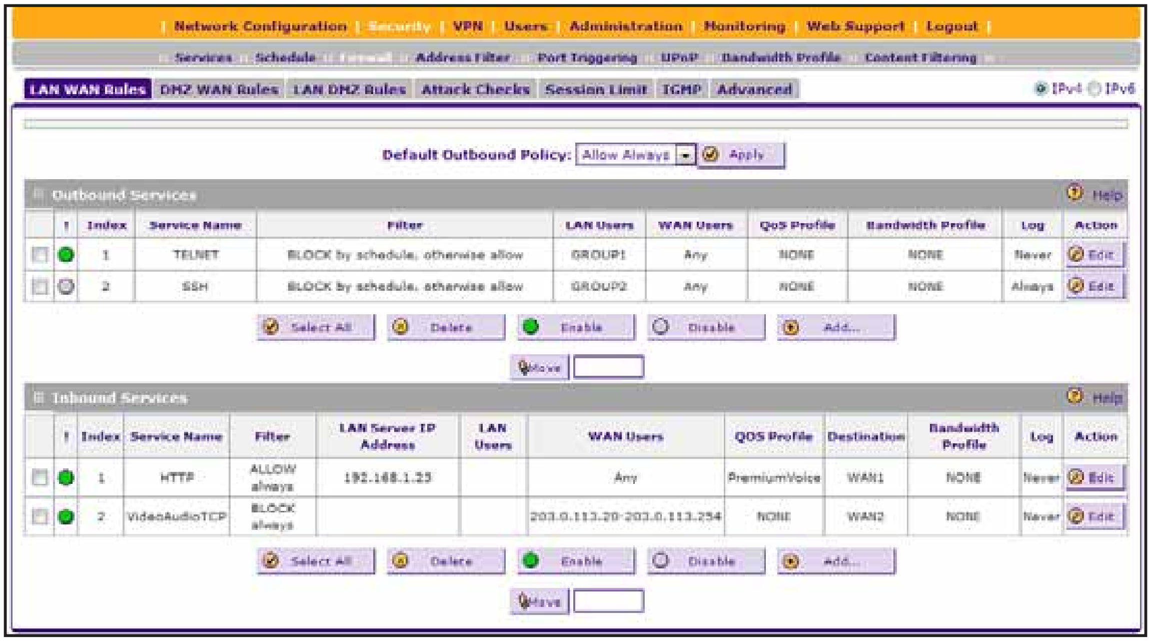
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Firewall**.

   The Firewall submenu tabs display with the LAN WAN Rules screen in view, displaying the IPv4 settings. The following figure shows some examples.


| 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 | IGMP | Advanced
◉ IPv4 ○ IPv6

Default Outbound Policy: Allow Always ▾ Apply

Outbound Services

	!	Index	Service Name	Filter	LAN Users	WAN Users	QoS Profile	Bandwidth Profile	Log	Action
□	●	1	TELNET	BLOCK by schedule, otherwise allow	GROUP1	Any	NONE	NONE	Never	Edit
□	○	2	SSH	BLOCK by schedule, otherwise allow	GROUP2	Any	NONE	NONE	Always	Edit

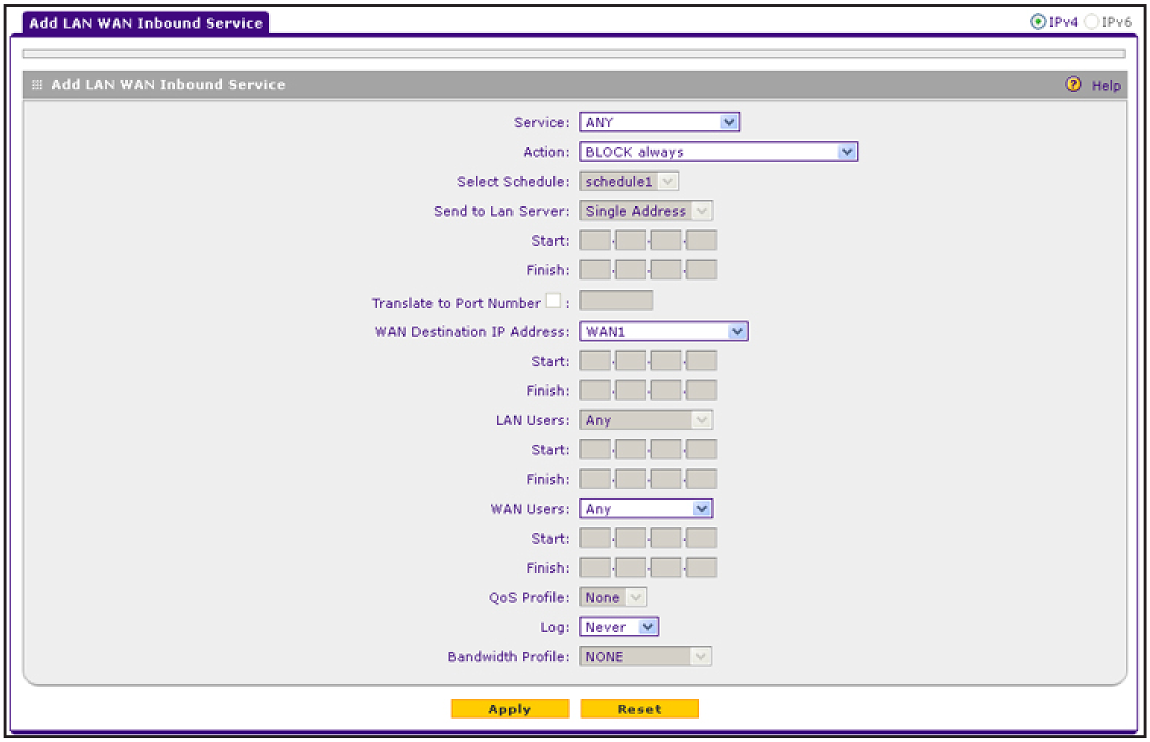
Select All
Delete
Enable
Disable
Add...
Move

Inbound Services

	!	Index	Service Name	Filter	LAN Server IP Address	LAN Users	WAN Users	QOS Profile	Destination	Bandwidth Profile	Log	Action
□	●	1	HTTP	ALLOW always	192.168.1.23		Any	PremiumVoice	WAN1	NONE	Never	Edit
□	●	2	VideoAudioTCP	BLOCK always			203.0.113.20-203.0.113.254	NONE	WAN2	NONE	Never	Edit

7. Under the Inbound Services table, click the **Add** button.

   The Add LAN WAN Inbound Service screen for IPv4 displays.



Add LAN WAN Inbound Service

● IPv4 ○ IPv6

Add LAN WAN Inbound Service

Help

Service:	ANY
Action:	BLOCK always
Select Schedule:	schedule1
Send to Lan Server:	Single Address
Start:	
Finish:	
Translate to Port Number □ :	
WAN Destination IP Address:	WAN1
Start:	
Finish:	
LAN Users:	Any
Start:	
Finish:	
WAN Users:	Any
Start:	
Finish:	
QoS Profile:	None
Log:	Never
Bandwidth Profile:	NONE

Apply Reset

8. Make your selections from the menus and enter the settings.

   For more information about the menus and settings, see *Settings for Inbound Rules* on page 217.

   The following table lists the menus that apply to an IPv4 LAN WAN inbound rule.

Menus that apply to all IPv4 LAN WAN inbound rules	Menus that apply only when your selection from the Action menu is *not* BLOCK always
Service	Select Schedule **Note:** This menu is available only when the selection from the **Action** menu includes *by schedule*.
Action	Send to Lan Server
WAN Destination IP Address	Translate to Port Number
LAN Users **Note:** This menu 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.	QoS Profile

Menus that apply to all IPv4 LAN WAN inbound rules	Menus that apply only when your selection from the Action menu is *not* BLOCK always
WAN Users	Bandwidth Profile
Log	

9. Click the **Apply** button.

   Your settings are saved. The new rule is added to the Inbound Services table on the LAN WAN Rules screen.

Add an IPv6 LAN WAN Inbound Rule

The following procedure describes how to add an IPv6 LAN WAN inbound rule.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

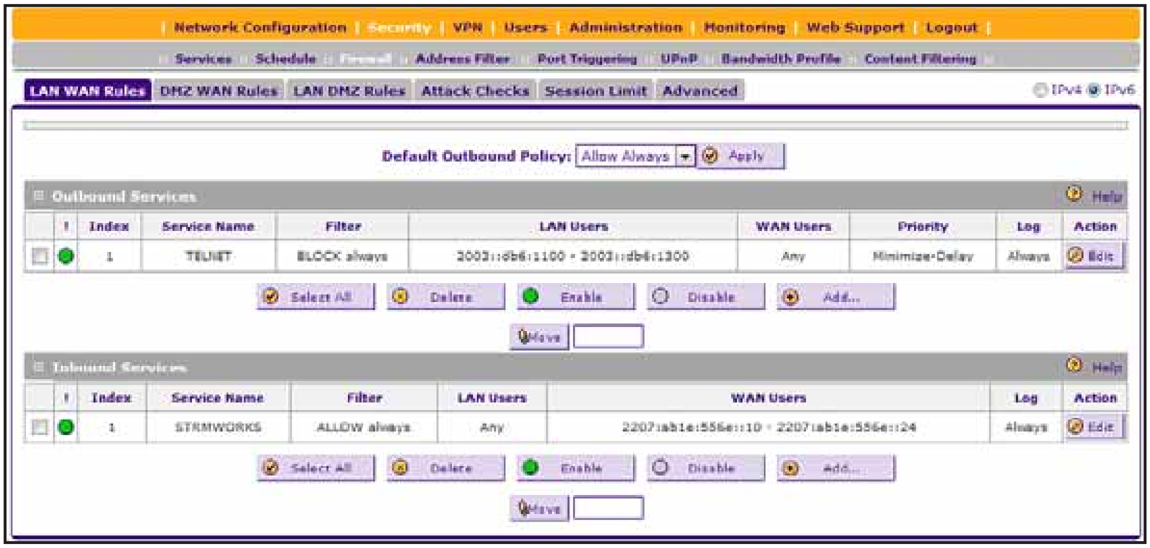
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Firewall**.

   The Firewall submenu tabs display with the LAN WAN Rules screen in view, displaying the IPv4 settings.
7. In the upper right, select the **IPv6** radio button.

   The LAN WAN Rules screen displays the IPv6 settings.


| 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...
Move

Default Outbound Policy: Allow Always

Outbound Services

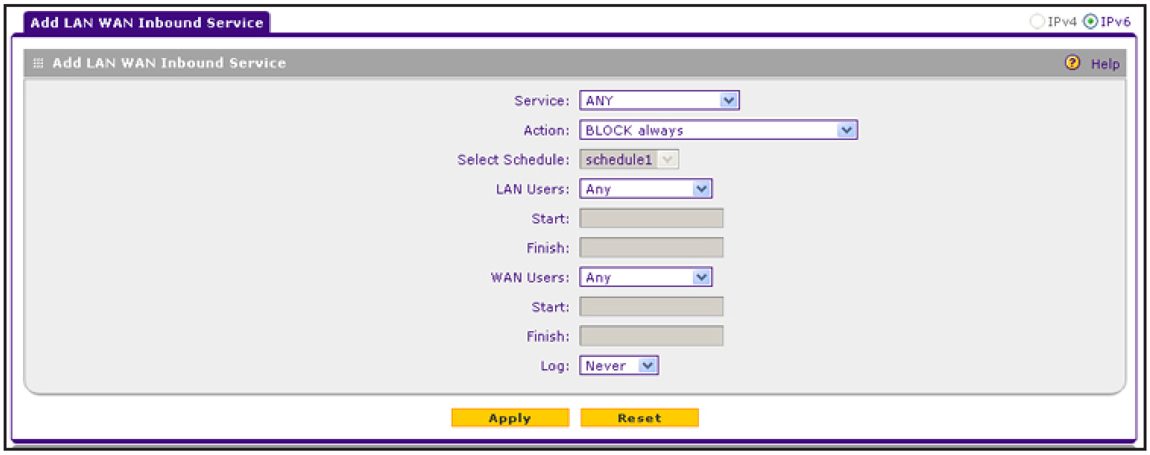
	!	Index	Service Name	Filter	LAN Users	WAN Users	Priority	Log	Action
□	●	1	TELNET	BLOCK always	2003::db6:1100 - 2003::db6:1300	Any	Minimize-Delay	Always	Edit

Inbound Services

	!	Index	Service Name	Filter	LAN Users	WAN Users	Log	Action
□	●	1	STRMWORKS	ALLOW always	Any	2207:ab1e:556e::10 - 2207:ab1e:556e::24	Always	Edit

8. Under the Inbound Services table, click the **Add** button.

   The Add LAN WAN Inbound Service screen for IPv6 displays.



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

9. Make your selections from the menus and enter the settings.

   For more information about the menus and settings, see *Settings for Inbound Rules* on page 217.

   The following table lists the menus that apply to an IPv6 LAN WAN inbound rule.

Menus that apply to all IPv6 LAN WAN inbound rules	Menus that apply only when your selection from the Action menu is *not* BLOCK always
Service	Select Schedule **Note:** This menu is available only when the selection from the **Action** menu includes *by schedule*.
Action	

Menus that apply to all IPv6 LAN WAN inbound rules	Menus that apply only when your selection from the Action menu is *not* BLOCK always
LAN Users	
WAN Users	
Log	

10. Click the **Apply** button.

    Your settings are saved. The new rule is added to the Inbound Services table on the LAN WAN Rules screen.

Add DMZ WAN Rules

The following sections provide information about managing DMZ WAN rules:

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

Add DMZ WAN Outbound Service Rules

For DMZ WAN traffic, the default outbound policy is to block all traffic to the Internet.

You can change the default policy by adding DMZ WAN firewall rules that allow specific types of traffic to go out from the DMZ to the Internet. Alternately, you can allow all outbound traffic and then block only specific services from passing through the VPN firewall.

You can allow or block access based on the service or application, source or destination IP addresses, and time of day.

The following sections provide information about adding DMZ WAN outbound service rules:

- *Add an IPv4 DMZ WAN Outbound Rule*
- *Add an IPv6 DMZ WAN Outbound Rule*

Add an IPv4 DMZ WAN Outbound Rule

The following procedure describes how to add an IPv4 DMZ WAN outbound rule.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

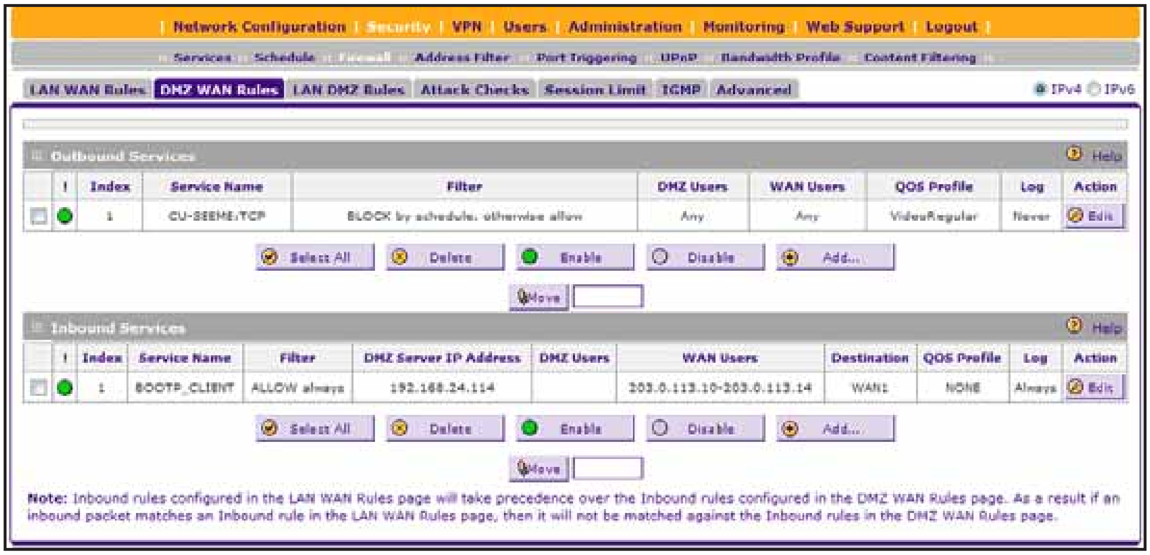
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > Firewall > DMZ WAN Rules**.

   The DMZ WAN Rule screen displays the IPv4 settings. The following figure shows some examples.


| 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
ICMP
Advanced
● IPv4 ○ IPv6
Help
Select All
Delete
Enable
Disable
Add...
Move

Outbound Services

	!	Index	Service Name	Filter	DMZ Users	WAN Users	QOS Profile	Log	Action
□	●	1	CU-SEEME:TCP	BLOCK by schedule, otherwise allow	Any	Any	VideoRegular	Never	Edit

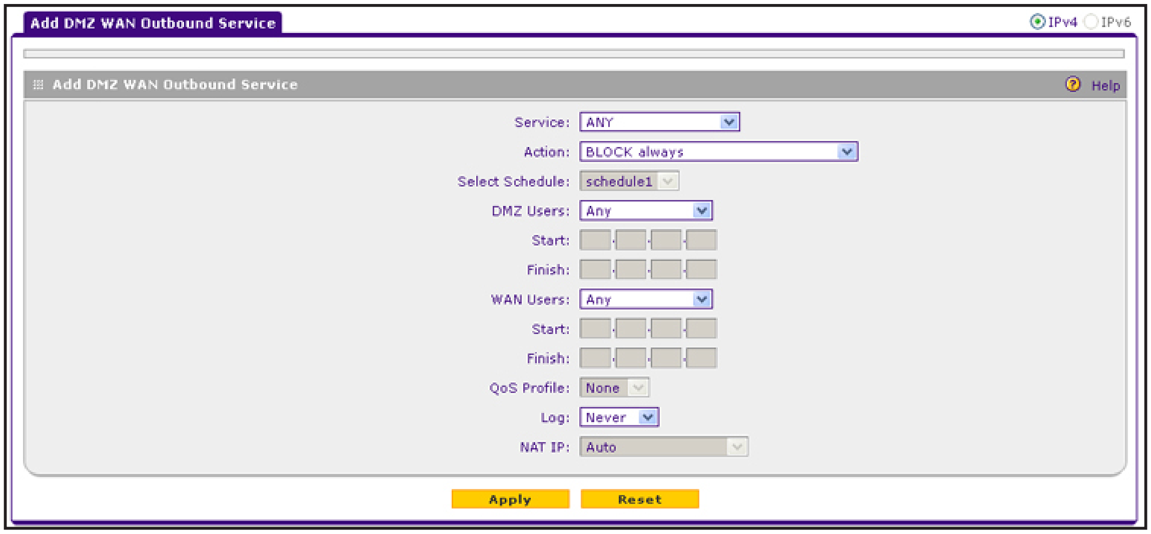
Inbound Services

	!	Index	Service Name	Filter	DMZ Server IP Address	DMZ Users	WAN Users	Destination	QOS Profile	Log	Action
□	●	1	BOOTP_CLIENT	ALLOW always	192.168.24.114		203.0.113.10-203.0.113.14	WAN1	NONE	Always	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.

7. Under the Outbound Services table, click the **Add** button.

   The Add DMZ WAN Outbound Service screen for IPv4 displays.



Add DMZ WAN Outbound Service

● IPv4 ○ IPv6

Add DMZ WAN Outbound Service

Help

Service: ANY

Action: BLOCK always

Select Schedule: schedule1

DMZ Users: Any

Start:

Finish:

WAN Users: Any

Start:

Finish:

QoS Profile: None

Log: Never

NAT IP: Auto

8. Make your selections from the menus and enter the settings.

   For more information about the menus and settings, see *Settings for Outbound Rules* on page 212.

   The following table lists the menus that apply to an IPv4 DMZ WAN outbound rule.

Menus that apply to all IPv4 DMZ WAN outbound rules	**Menus that apply only when your selection from the Action menu is *not* BLOCK always**
Service	Select Schedule **Note:** This menu is available only when the selection from the **Action** menu includes *by schedule*.
Action	QoS Profile
DMZ Users	NAT IP **Note:** This menu is available only when the WAN mode is NAT.
WAN Users	
Log	

9. Click the **Apply** button.

   Your settings are saved. The new rule is added to the Outbound Services table on the DMZ WAN Rules screen.

Add an IPv6 DMZ WAN Outbound Rule

The following procedure describes how to add an IPv64 DMZ WAN outbound rule.

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

1. On your computer, launch an Internet browser.

2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

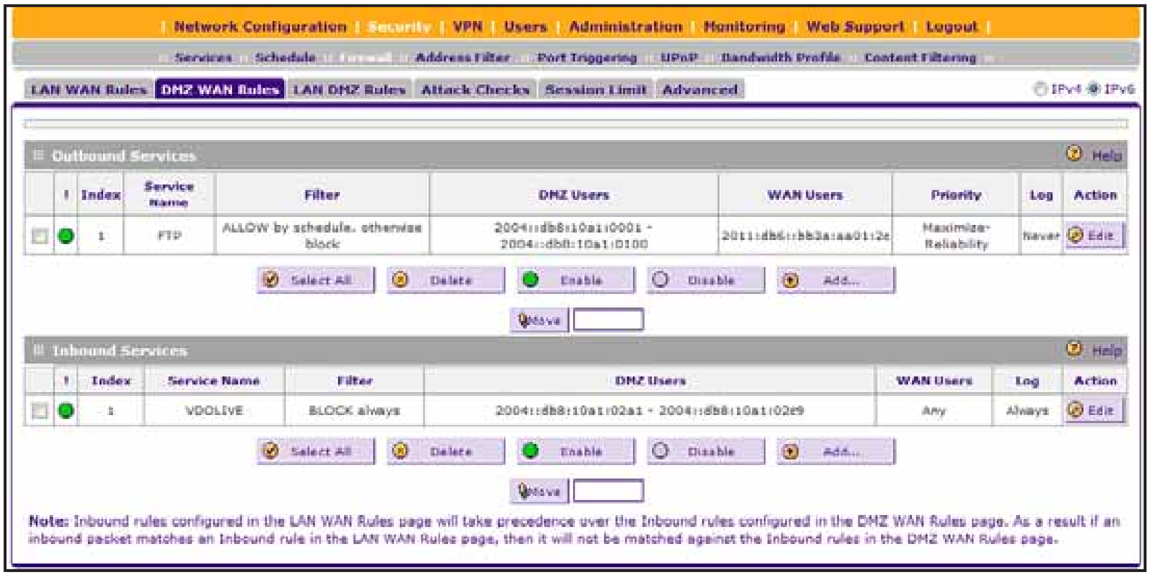
   The Router Status screen displays.

6. Select **Security > Firewall > DMZ WAN Rules**.

   The DMZ WAN Rules screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The DMZ WAN Rules screen displays the IPv6 settings.


| 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...
Move
Inbound Services
Help
Select All
Delete
Enable
Disable
Add...
Move

Outbound Services

	!	Index	Service Name	Filter	DMZ Users	WAN Users	Priority	Log	Action
□	●	1	FTP	ALLOW by schedule, otherwise block	2004::db8:10a1:0001 - 2004::db8:10a1:0100	2011:db6::bb3a:aa01:2e	Maximize-Reliability	Never	Edit

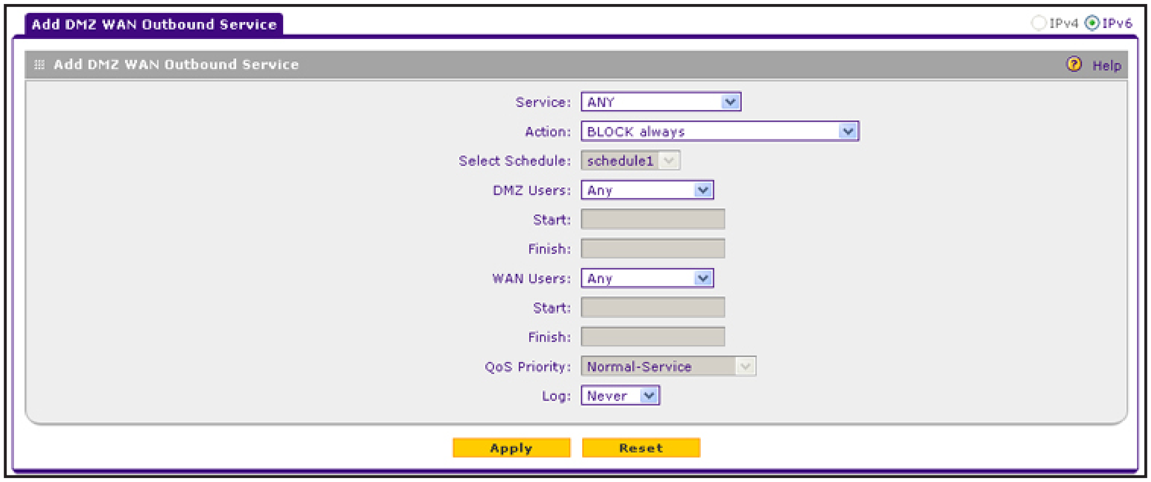
Inbound Services

	!	Index	Service Name	Filter	DMZ Users	WAN Users	Log	Action
□	●	1	VDOLIVE	BLOCK always	2004::db8:10a1:02a1 - 2004::db8:10a1:02e9	Any	Always	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.

8. Under the Outbound Services table, click the **Add** button.

   The Add DMZ WAN Outbound Service screen for IPv6 displays.



Service: ANY
Action: BLOCK always
Select Schedule: schedule1
DMZ Users: Any
Start:
Finish:
WAN Users: Any
Start:
Finish:
QoS Priority: Normal-Service
Log: Never

9. Make your selections from the menus and enter the settings.

   For more information about the menus and settings, see *Settings for Outbound Rules* on page 212.

   The following table lists the menus that apply to an IPv6 DMZ WAN outbound rule.

Menus that apply to all IPv6 DMZ WAN outbound rules	Menus that apply only when your selection from the Action menu is *not* BLOCK always
Service	Select Schedule **Note:** This menu is available only when the selection from the **Action** menu includes *by schedule*.
Action	QoS Priority
DMZ Users	
WAN Users	
Log	

10. Click the **Apply** button.

    Your settings are saved. The new rule is added to the Outbound Services table on the DMZ WAN Rules screen.

Add DMZ WAN Inbound Service Rules

For DMZ WAN traffic, the default inbound policy is to block all traffic from the Internet.

You can change the default policy by adding DMZ WAN firewall rules that allow specific types of traffic to come in from the Internet to the DMZ (inbound). You can allow access based on the service or application, source or destination IP addresses, and time of day.

Note: Inbound LAN WAN rules take precedence over inbound DMZ WAN rules. When an inbound packet matches an inbound LAN WAN rule, the VPN firewall does not match the packet against inbound DMZ WAN rules.

⚠ **WARNING:**

Make sure that you first configure the IPv4 WAN routing mode (see *Manage the IPv4 WAN Routing Mode* on page 30) before you configure custom firewall rules. If you change the IPv4 WAN routing mode, all DMZ WAN inbound rules revert to default settings.

The following sections provide information about adding DMZ WAN inbound service rules:

- *Add an IPv4 DMZ WAN Inbound Rule*
- *Add an IPv6 DMZ WAN Inbound Rule*

Add an IPv4 DMZ WAN Inbound Rule

The following procedure describes how to add an IPv4 DMZ WAN inbound rule.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

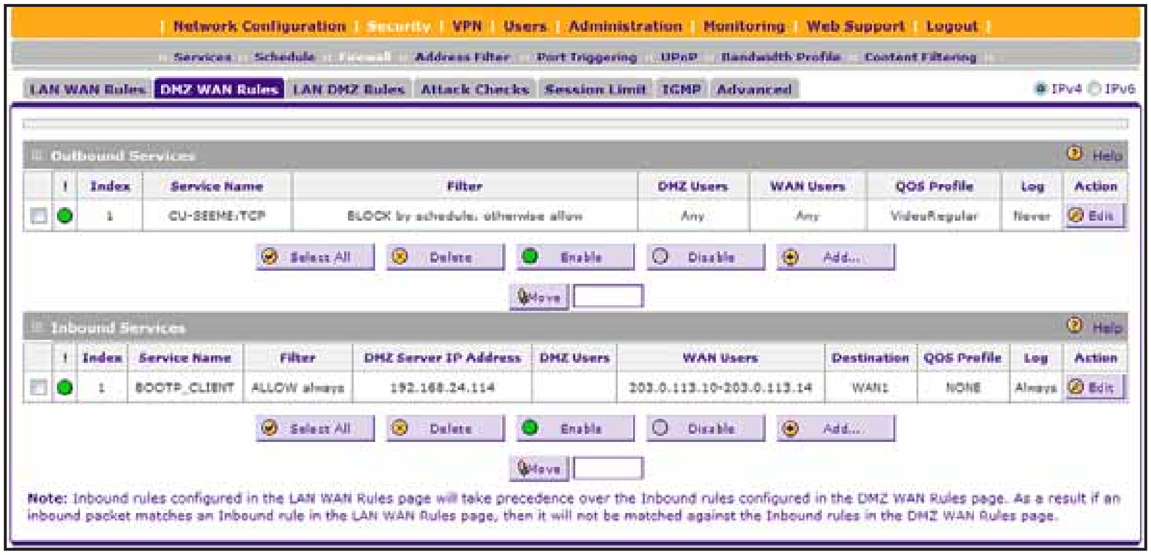
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Firewall > DMZ WAN Rules**.

   The DMZ WAN Rules screen displays the IPv4 settings.


| 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 | IGMP | Advanced
● IPv4 ○ IPv6
Help
Select All
Delete
Enable
Disable
Add...
Move

Outbound Services

	!	Index	Service Name	Filter	DMZ Users	WAN Users	QOS Profile	Log	Action
□	●	1	CU-SEEME:TCP	BLOCK by schedule, otherwise allow	Any	Any	VideoRegular	Never	Edit

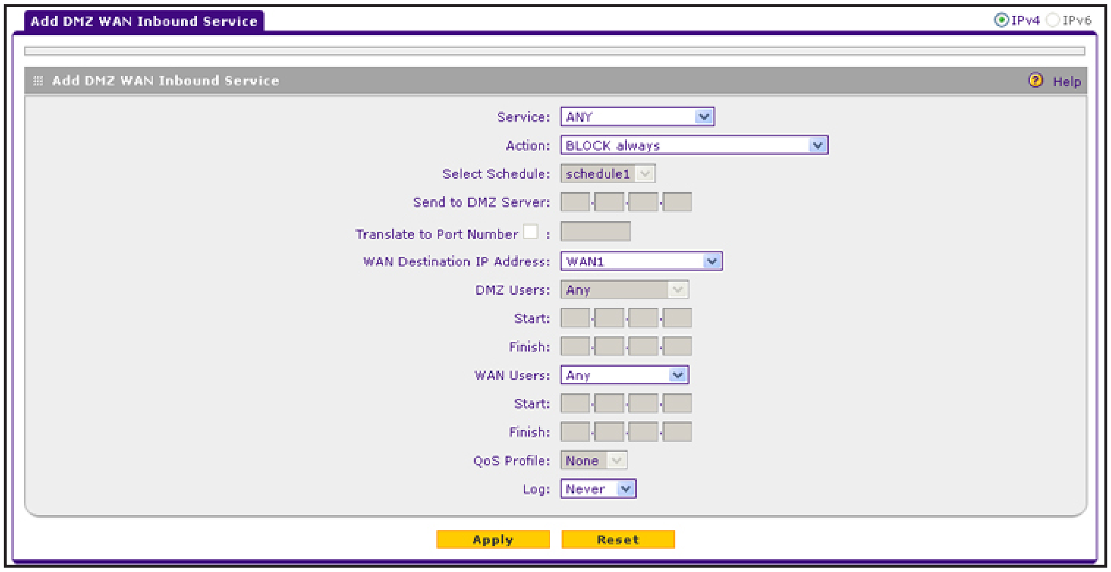
Inbound Services

	!	Index	Service Name	Filter	DMZ Server IP Address	DMZ Users	WAN Users	Destination	QOS Profile	Log	Action
□	●	1	BOOTP_CLIENT	ALLOW always	192.168.24.114		203.0.113.10-203.0.113.14	WAN1	NONE	Always	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.

7. Under the Inbound Services table, click the **Add** button.

   The Add DMZ WAN Inbound Service screen for IPv4 displays.



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:	WAN1
DMZ Users:	Any
Start:	
Finish:	
WAN Users:	Any
Start:	
Finish:	
QoS Profile:	None
Log:	Never

8. Make your selections from the menus and enter the settings.

   For more information about the menus and settings, see *Settings for Inbound Rules* on page 217.

The following table lists the menus that apply to an IPv4 DMZ WAN inbound rule.

Menus that apply to all IPv4 DMZ WAN inbound rules	Menus that apply only when your selection from the Action menu is *not* BLOCK always
Service	Select Schedule **Note:** This menu is available only when the selection from the **Action** menu includes *by schedule*.
Action	Send to DMZ Server
WAN Destination IP Address	Translate to Port Number
DMZ Users **Note:** This menu 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.	QoS Profile
WAN Users	
Log	

9. Click the **Apply** button.

   Your settings are saved. The new rule is added to the Inbound Services table on the DMZ WAN Rules screen.

Add an IPv6 DMZ WAN Inbound Rule

The following procedure describes how to add an IPv6 DMZ WAN inbound rule.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

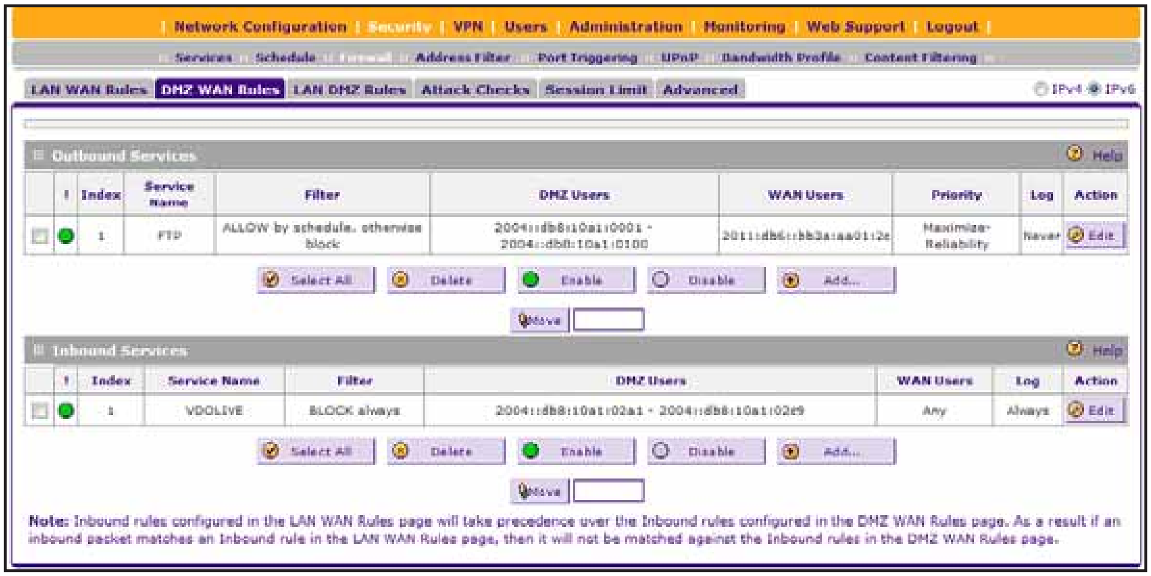
The Router Status screen displays.

6. Select **Security > Firewall > DMZ WAN Rules**.

   The DMZ WAN Rule screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The DMZ WAN Rule screen displays the IPv6 settings.


| 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

	!	Index	Service Name	Filter	DMZ Users	WAN Users	Priority	Log	Action
□	●	1	FTP	ALLOW by schedule, otherwise block	2004::db8:10a1:0001 - 2004::db8:10a1:0100	2011:db6::bb3a:aa01:2e	Maximize-Reliability	Never	Edit

Select All
Delete
Enable
Disable
Add...
Move
Help

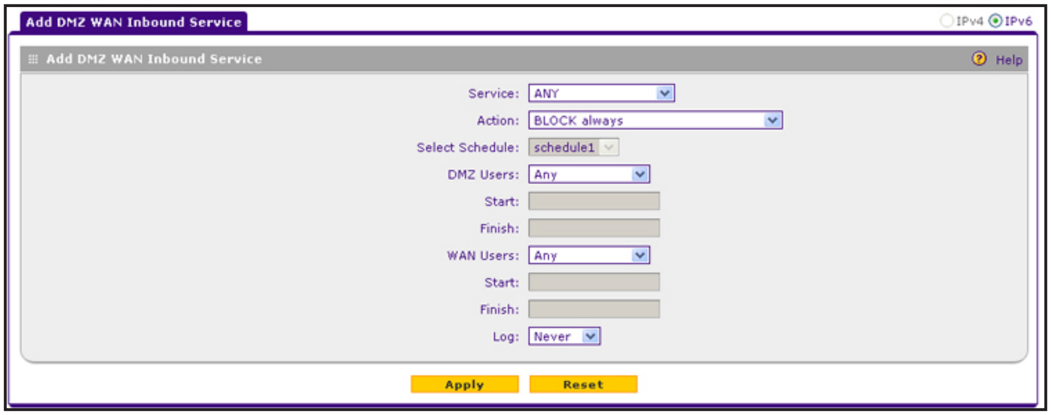
Inbound Services

	!	Index	Service Name	Filter	DMZ Users	WAN Users	Log	Action
□	●	1	VDOLIVE	BLOCK always	2004::db8:10a1:02a1 - 2004::db8:10a1:02e9	Any	Always	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.

8. Under the Outbound Services table, click the **Add** button.

   The Add DMZ WAN Inbound Service screen for IPv6 displays.



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

9. Make your selections from the menus and enter the settings.

   For more information about the menus and settings, see *Settings for Inbound Rules* on page 217.

The following table lists the menus that apply to an IPv6 DMZ WAN inbound rule.

Menus that apply to all IPv6 DMZ WAN inbound rules	Menus that apply only when your selection from the Action menu is *not* BLOCK always
Service	Select Schedule **Note:** This menu is available only when the selection from the **Action** menu includes *by schedule*.
Action	
DMZ Users	
WAN Users	
Log	

10. Click the **Apply** button.

    Your settings are saved. The new rule is added to the Inbound Services table on the DMZ WAN Rules screen.

Add LAN DMZ Rules

The following sections provide information about managing LAN DMZ rules:

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

Add LAN DMZ Outbound Service Rules

For LAN DMZ traffic, the default outbound policy is to block all traffic to the DMZ.

You can change the default policy by adding LAN DMZ firewall rules that allow specific types of traffic to go out from the LAN to the DMZ. Alternately, you can allow all outbound traffic and then block only specific services from passing through the VPN firewall.

You can allow or block access based on the service or application, source or destination IP addresses, and time of day.

The following sections provide information about adding LAN DMZ outbound service rules:

- *Add an IPv4 LAN DMZ Outbound Rule*
- *Add an IPv6 LAN DMZ Outbound Rule*

Add an IPv4 LAN DMZ Outbound Rule

The following procedure describes how to add an IPv4 LAN DMZ outbound rule.

➤ **To add an IPv4 LAN DMZ outbound rule:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

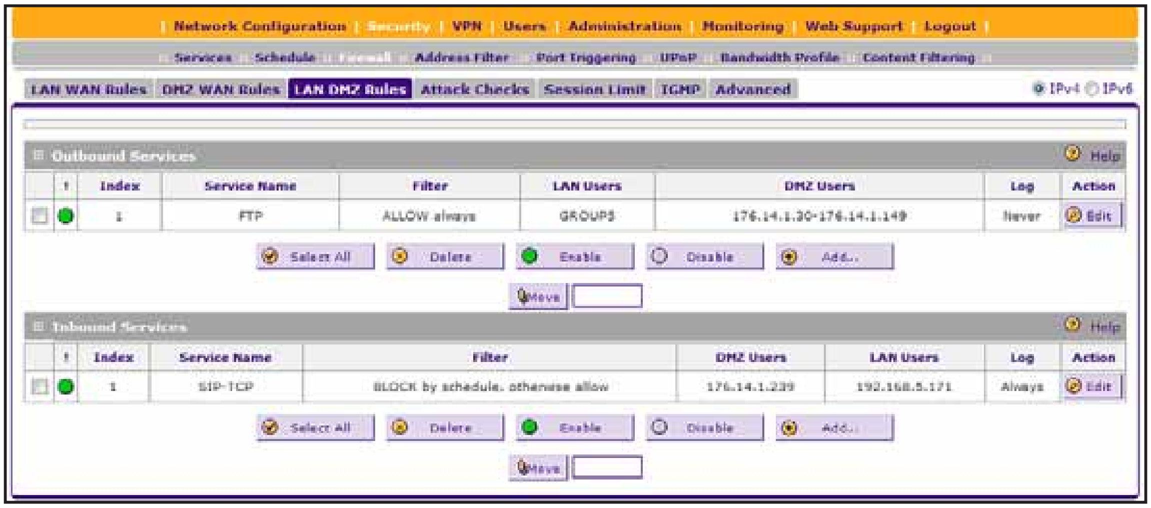
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Firewall > LAN DMZ Rules**.

   The LAN DMZ Rules screen displays the IPv4 settings.


| 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 | IGMP | Advanced
● IPv4 ○ IPv6
Outbound Services
Help

	!	Index	Service Name	Filter	LAN Users	DMZ Users	Log	Action
□	●	1	FTP	ALLOW always	GROUPS	176.14.1.20-176.14.1.149	Never	Edit

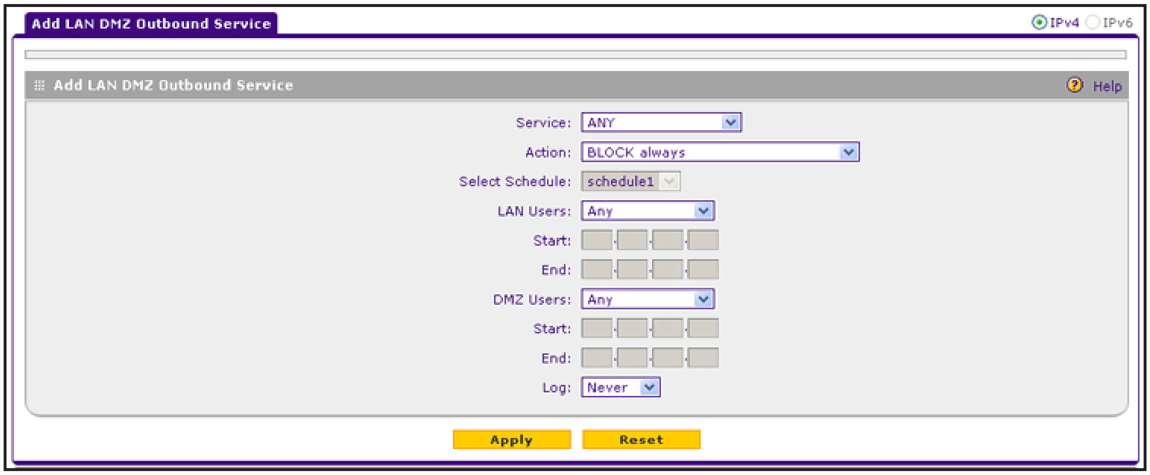
Select All
Delete
Enable
Disable
Add...
Move
Inbound Services
Help

	!	Index	Service Name	Filter	DMZ Users	LAN Users	Log	Action
□	●	1	SIP-TCP	BLOCK by schedule, otherwise allow	176.14.1.239	192.168.5.171	Always	Edit

Select All
Delete
Enable
Disable
Add...
Move

7. Under the Outbound Services table, click the **Add** button.

   The Add LAN DMZ Outbound Service screen for IPv4 displays.



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

8. Make your selections from the menus and enter the settings.

   For more information about the menus and settings, see *Settings for Outbound Rules* on page 212.

   The following table lists the menus that apply to an IPv4 LAN DMZ outbound rule.

Menus that apply to all IPv4 LAN DMZ outbound rules	Menus that apply only when your selection from the Action menu is *not* BLOCK always
Service	Select Schedule **Note:** This menu is available only when the selection from the **Action** menu includes *by schedule*.
Action	
LAN Users	
DMZ Users	
Log	

9. Click the **Apply** button.

   Your settings are saved. The new rule is added to the Outbound Services table on the LAN DMZ Rules screen.

Add an IPv6 LAN DMZ Outbound Rule

The following procedure describes how to add an IPv6 LAN DMZ outbound rule.

➤ **To add an IPv6 LAN DMZ outbound rule:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

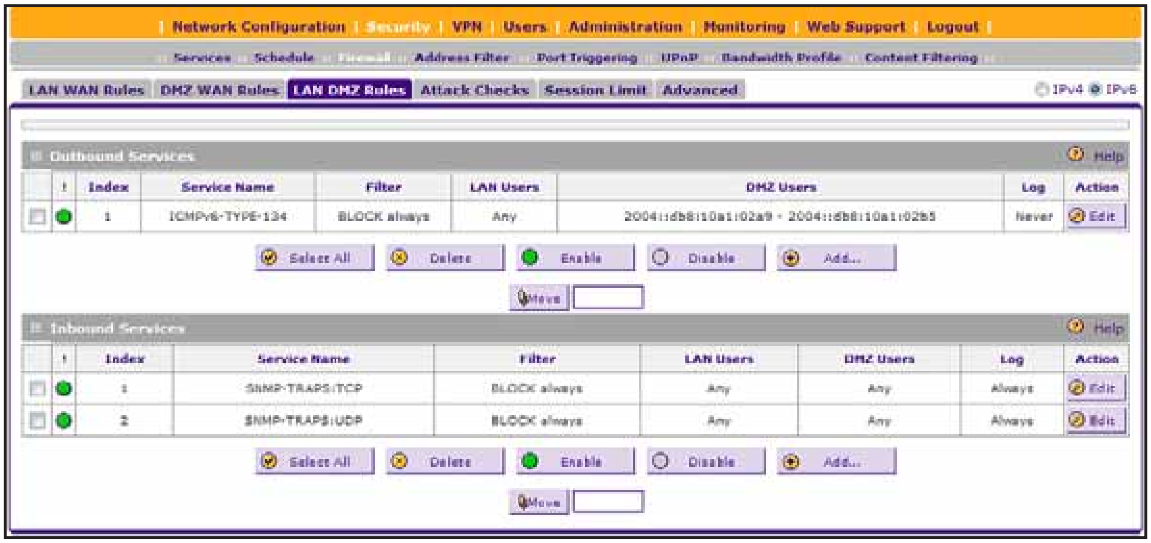
   The Router Status screen displays.

6. Select **Security > Firewall > LAN DMZ Rules**.

   The LAN DMZ Rules screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The LAN DMZ Rules screen displays the IPv6 settings.


| 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...
Move

Outbound Services

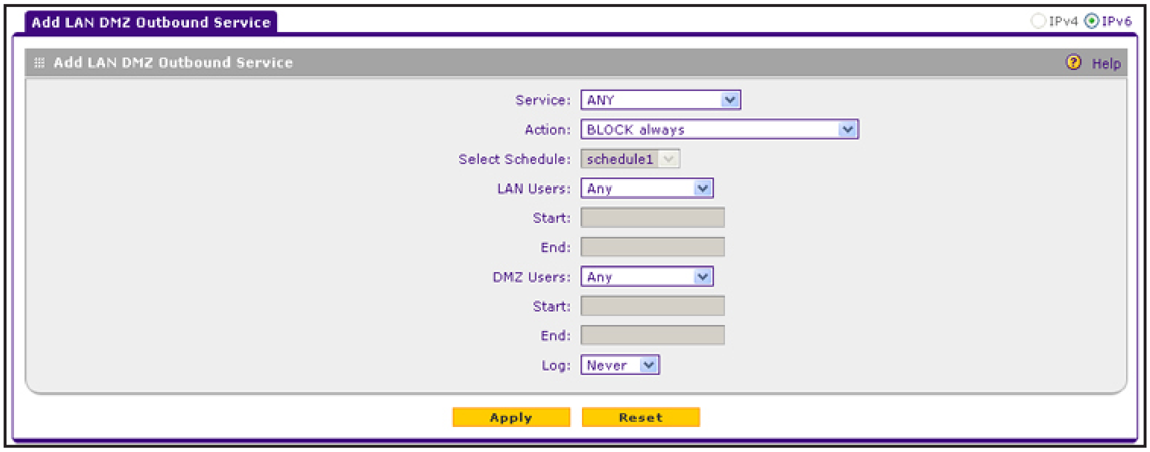
	!	Index	Service Name	Filter	LAN Users	DMZ Users	Log	Action
□	●	1	ICMPv6-TYPE-134	BLOCK always	Any	2004::db8:10a1:02a9 - 2004::db8:10a1:02b5	Never	Edit

Inbound Services

	!	Index	Service Name	Filter	LAN Users	DMZ Users	Log	Action
□	●	1	SNMP-TRAPS:TCP	BLOCK always	Any	Any	Always	Edit
□	●	2	SNMP-TRAPS:UDP	BLOCK always	Any	Any	Always	Edit

8. Under the Outbound Services table, click the **Add** button.

   The Add LAN DMZ Outbound Service screen for IPv6 displays.



Service: ANY
Action: BLOCK always
Select Schedule: schedule1
LAN Users: Any
Start:
End:
DMZ Users: Any
Start:
End:
Log: Never

9. Make your selections from the menus and enter the settings.

   For more information about the menus and settings, see *Settings for Outbound Rules* on page 212.

   The following table lists the menus that apply to an IPv6 LAN DMZ outbound rule.

Menus that apply to all IPv6 LAN DMZ outbound rules	Menus that apply only when your selection from the Action menu is *not* BLOCK always
Service	Select Schedule **Note:** This menu is available only when the selection from the **Action** menu includes *by schedule*.
Action	
LAN Users	
DMZ Users	
Log	

10. Click the **Apply** button.

    Your settings are saved. The new rule is added to the Outbound Services table on the LAN DMZ Rules screen.

Add LAN DMZ Inbound Service Rules

For LAN DMZ traffic, the inbound default policy is to block all traffic to the LAN.

You can change the default policy by adding LAN DMZ firewall rules that allow specific types of traffic to come in from the DMZ to the LAN. You can allow access based on the service or application, source or destination IP addresses, and time of day.

The following sections provide information about adding LAN DMZ inbound service rules:

- *Add an IPv4 LAN DMZ Inbound Rule*
- *Add an IPv6 LAN DMZ Inbound Rule*

Add an IPv4 LAN DMZ Inbound Rule

The following procedure describes how to add an IPv4 LAN DMZ inbound rule.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

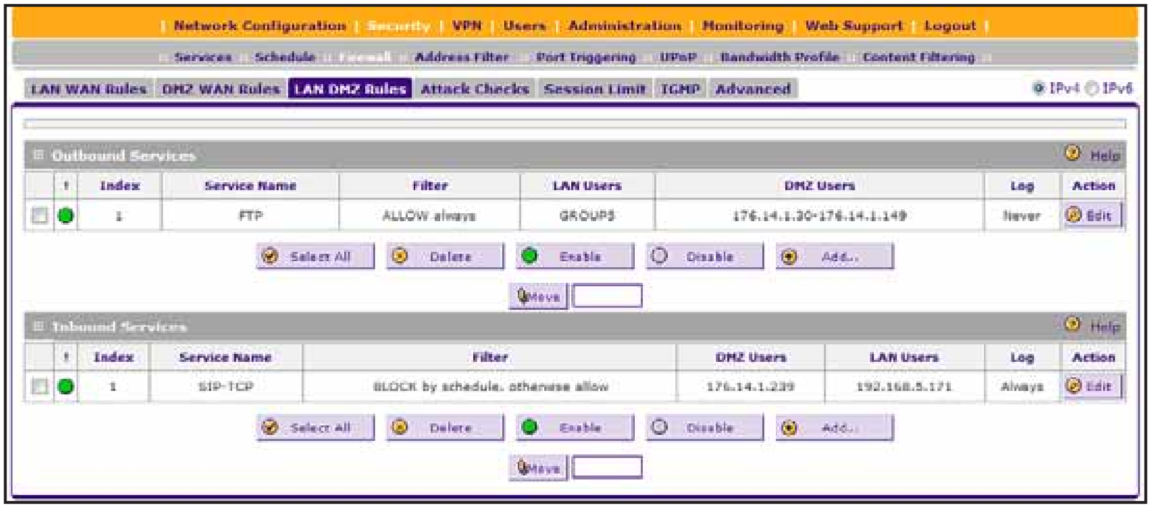
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Firewall > LAN DMZ Rules**.

   The LAN DMZ Rules screen displays the IPv4 settings.


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 | IGMP | Advanced
● IPv4 ○ IPv6
Help
Select All
Delete
Enable
Disable
Add...
Move

Outbound Services

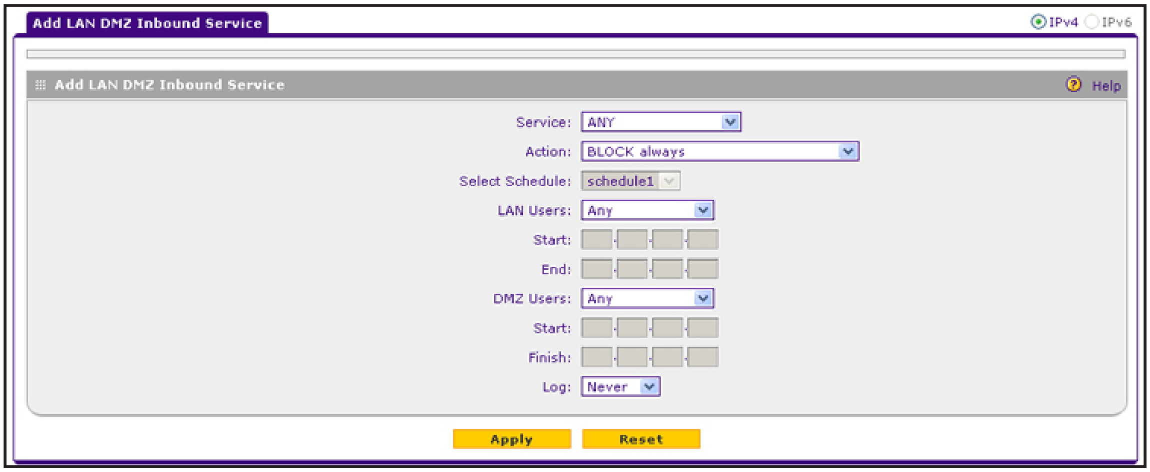
	!	Index	Service Name	Filter	LAN Users	DMZ Users	Log	Action
□	●	1	FTP	ALLOW always	GROUPS	176.14.1.30-176.14.1.149	Never	Edit

Inbound Services

	!	Index	Service Name	Filter	DMZ Users	LAN Users	Log	Action
□	●	1	SIP-TCP	BLOCK by schedule, otherwise allow	176.14.1.239	192.168.5.171	Always	Edit

7. Under the Inbound Services table, click the **Add** button.

   The Add LAN DMZ Inbound Service screen for IPv4 displays.



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

8. Make your selections from the menus and enter the settings.

   For more information about the menus and settings, see *Settings for Inbound Rules* on page 217.

   The following table lists the menus that apply to an IPv4 LAN DMZ inbound rule.

Menus that apply to all IPv4 LAN DMZ inbound rules	Menus that apply only when your selection from the Action menu is *not* BLOCK always
Service	Select Schedule **Note:** This menu is available only when the selection from the **Action** menu includes *by schedule*.
Action	
LAN Users	
DMZ Users	
Log	

9. Click the **Apply** button.

   Your settings are saved. The new rule is added to the Inbound Services table on the LAN DMZ Rules screen.

Add an IPv6 LAN DMZ Inbound Rule

The following procedure describes how to add an IPv6 LAN DMZ inbound rule.

➤ **To add an IPv6 LAN DMZ inbound rule:**

1. On your computer, launch an Internet browser.

2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

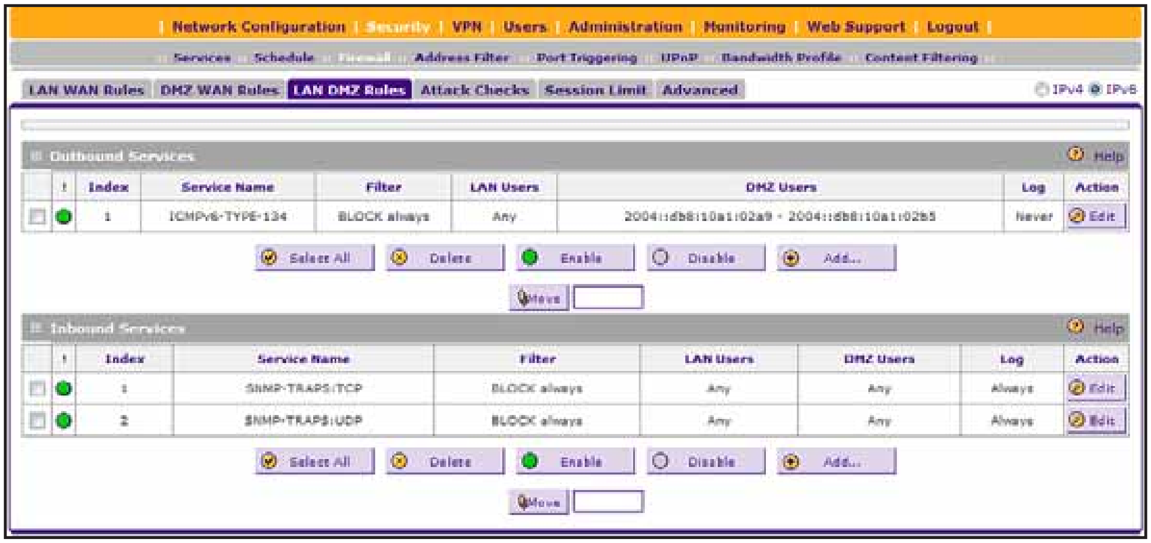
   The Router Status screen displays.

6. Select **Security > Firewall > LAN DMZ Rules**.

   The LAN DMZ Rules screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The LAN DMZ Rules screen displays the IPv6 settings.


| 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...
Move
Help
Select All
Delete
Enable
Disable
Add...
Move

Outbound Services

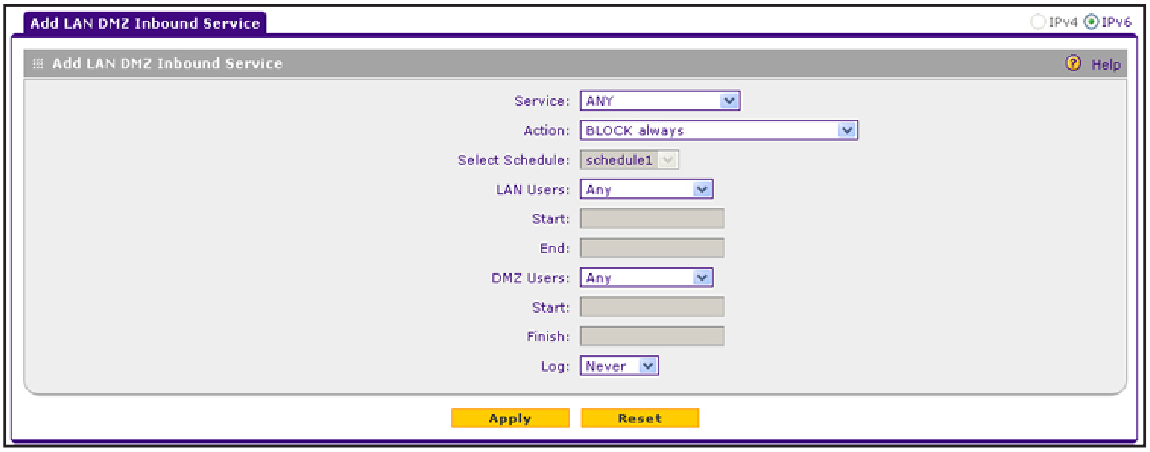
	!	Index	Service Name	Filter	LAN Users	DMZ Users	Log	Action
□	●	1	ICMPv6-TYPE-134	BLOCK always	Any	2004::db8:10a1:02a9 - 2004::db8:10a1:02b5	Never	Edit

Inbound Services

	!	Index	Service Name	Filter	LAN Users	DMZ Users	Log	Action
□	●	1	SNMP-TRAPS:TCP	BLOCK always	Any	Any	Always	Edit
□	●	2	SNMP-TRAPS:UDP	BLOCK always	Any	Any	Always	Edit

8. Under the Inbound Services table, click the **Add** button.

   The Add LAN DMZ Inbound Service screen for IPv6 displays.



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

9. Make your selections from the menus and enter the settings.

   For more information about the menus and settings, see *Settings for Inbound Rules* on page 217.

   The following table lists the menus that apply to an IPv6 LAN DMZ inbound rule.

Menus that apply to all IPv6 LAN DMZ inbound rules	Menus that apply only when your selection from the Action menu is *not* BLOCK always
Service	Select Schedule **Note:** This menu is available only when the selection from the **Action** menu includes *by schedule*.
Action	
LAN Users	
DMZ Users	
Log	

10. Click the **Apply** button.

    Your settings are saved. The new rule is added to the Inbound Services table on the LAN DMZ Rules screen.

Manage Existing Firewall Rules

After you add an outbound or inbound firewall rule for IPv4 or IPv6 traffic, you can perform the following actions with the rule:

- Change the rule
- Increase or lower the priority of the rule
- Disable the rule
- Enable the rule

- Remove the rule

➢ **To manage an existing rule:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Firewall**.

   The Firewall submenu tabs display with the LAN WAN Rules screen in view, displaying the IPv4 settings.

   The IPv4 outbound service rules display in the upper table. The IPv4 inbound service rules display in the lower table.
7. To manage a rule other than a LAN WAN rule, click one of the following tabs:
   - **DMZ WAN Rules**. Click the tab for a DMZ WAN rule.

     The DMZ WAN Rules screen displays the IPv4 rules.
   - **DMZ LAN Rules**. Click the tab for a DMZ LAN rule.

     The DMZ LAN Rules screen displays the IPv4 rules.

   The IPv4 outbound service rules display in the upper table. The IPv4 inbound service rules display in the lower table.
8. To manage an IPv6 rule instead of an IPv4 rule, in the upper right, select the **IPv6** radio button.

   The screen displays the IPv6 settings. The IPv6 outbound service rules display in the upper table. The IPv6 inbound service rules display in the lower table.

9. Take one of the actions that are described in the following table.

Action	Steps
Change a rule	1. In the leftmost column of the table, select the check box for the rule. 2. On the same row in the table, click the **Edit** button. The screen that lets you change the settings displays. 3. Change the settings. For information about the settings, see one of the following sections: - *Settings for Outbound Rules* on page 212 - *Settings for Inbound Rules* on page 217 - *Add LAN WAN Rules* on page 223 - *Add DMZ WAN Rules* on page 233 - *Add LAN DMZ Rules* on page 242. 4. Click the **Apply** button. Your settings are saved. The updated rule displays in the corresponding table in the Inbound Services or Outbound Services section.
Change the order of precedence for a rule	1. In the leftmost column of the table, select the check box for the rule. 2. In the field next to the **Move** button, enter the new numerical position for the rule. 3. Click the **Move** button. The rule moves to the new position in the table and your settings are saved.
Disable one or more rules	1. In the leftmost column of the table, select one or more check boxes, or to select all rules, click the **Select All** button. 2. Click the **Disable** button. The selected rules are disabled and your settings are saved. The green circle to the left of each rule turns gray.
Enable one or more rules	1. In the leftmost column of the table, select one or more check boxes, or to select all rules, click the **Select All** button. 2. Click the **Enable** button. The selected rules are enabled and your settings are saved. The gray circle to the left of each rule turns green. **Note:** By default, when a rule is added to a table, the rule is automatically enabled.
Remove one or more rules	1. In the leftmost column of the table, select one or more check boxes, or to select all rules, click the **Select All** button. 2. Click the **Delete** button. The selected rules are removed from the table and your settings are saved.

Examples of Firewall Rules

The following sections provide examples of firewall rules:

- *Examples of Inbound Firewall Rules*
- *Examples of Outbound Firewall Rules*

Examples of Inbound Firewall Rules

The following sections provide examples of IPv4 and IPv6 LAN WAN inbound rules:

- *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 Inbound Rule: Set Up One-to-One NAT Mapping*
- *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.

➢ **To set up a firewall rule to host a local public web server on your network:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

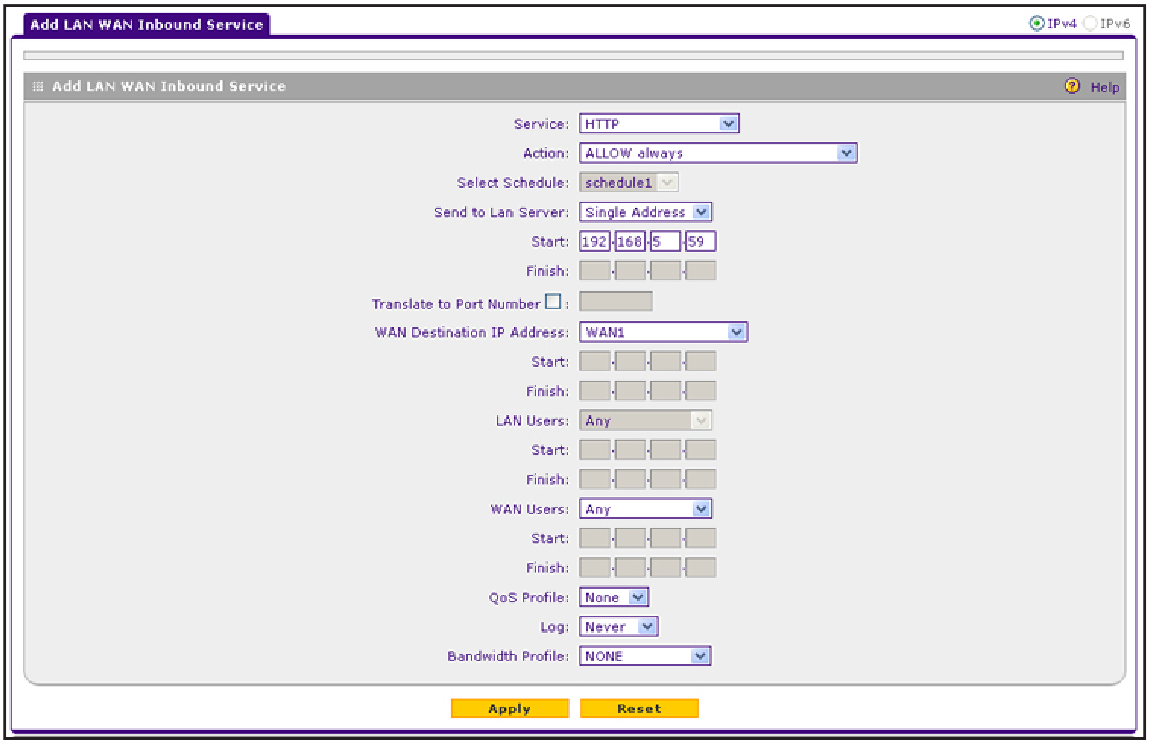
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Firewall**.

   The Firewall submenu tabs display with the LAN WAN Rules screen in view, displaying the IPv4 settings.
7. Under the Inbound Services table, click the **Add** button.

   The Add LAN WAN Inbound Service screen for IPv4 displays.



Service:	HTTP
Action:	ALLOW always
Select Schedule:	schedule1
Send to Lan Server:	Single Address
Start:	192 . 168 . 5 . 59
Finish:	
Translate to Port Number □ :	
WAN Destination IP Address:	WAN1
Start:	
Finish:	
LAN Users:	Any
Start:	
Finish:	
WAN Users:	Any
Start:	
Finish:	
QoS Profile:	None
Log:	Never
Bandwidth Profile:	NONE

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

Setting	Description
Service	From the menu, select **HTTP**.
Action	From the menu, select **ALLOW always**.
Send to LAN Server	From the menu, select **Single address**. In the **Start** field, enter the LAN IP address of the server that must function as a public web server.
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 public web server on the LAN. From the menu, select the WAN interface that you want to use.
WAN Users	From the menu, select **Any**.
QoS Profile	You can leave the selection from the menu at **None**.
Log	You can leave the selection from the menu at **Never**.
Bandwidth Profile	You can leave the selection from the menu at **NONE**.

9. Click the **Apply** button.

   Your settings are saved. The new rule is added to the Inbound Services table on the LAN WAN Rules screen.

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. In the example, CU-SeeMe connections are allowed only from a specified range of external IP addresses and according to a schedule.

➢ **To set up a firewall rule to host a local public web server on your network:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

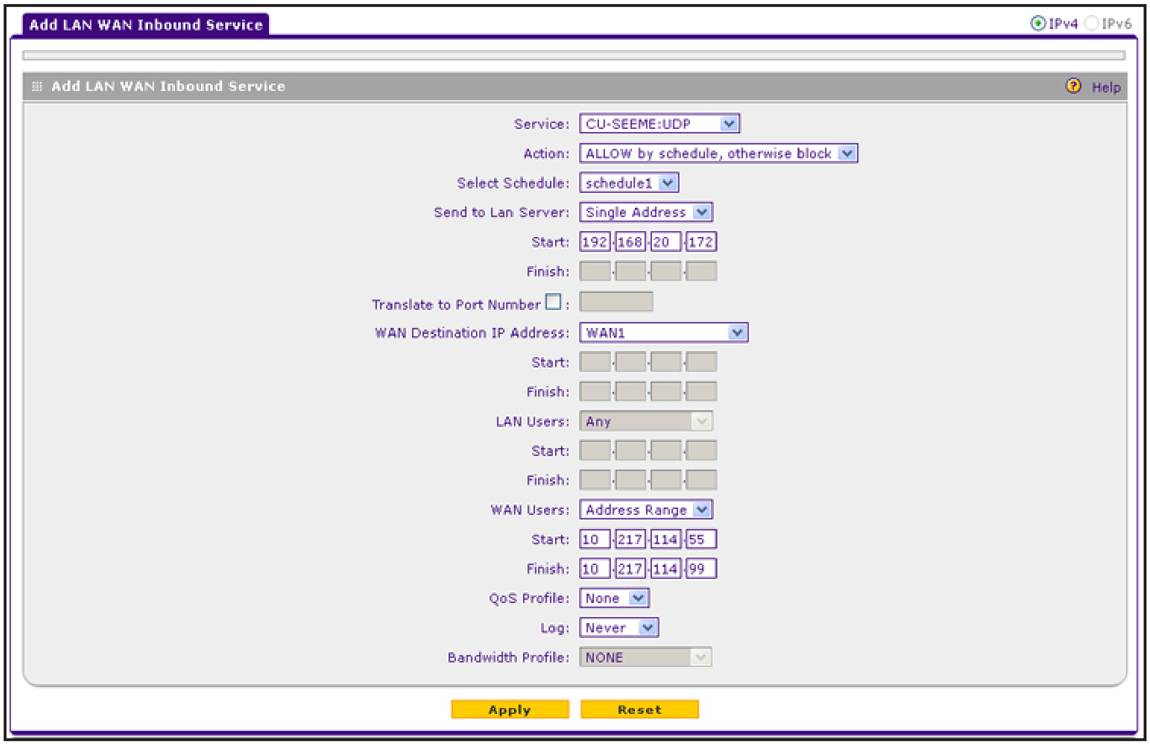
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Firewall**.

   The Firewall submenu tabs display with the LAN WAN Rules screen in view, displaying the IPv4 settings.
7. Under the Inbound Services table, click the **Add** button.

   The Add LAN WAN Inbound Service screen for IPv4 displays.



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: 192.168.20.172

Finish:

Translate to Port Number □:

WAN Destination IP Address: WAN1

Start:

Finish:

LAN Users: Any

Start:

Finish:

WAN Users: Address Range

Start: 10.217.114.55

Finish: 10.217.114.99

QoS Profile: None

Log: Never

Bandwidth Profile: NONE

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

Setting	Description
Service	From the menu, select **CU-SEEME:UDP**.
Action	From the menu, select **ALLOW by schedule, otherwise block**. (If you do not want to use a schedule, select **ALLOW always**.)
Select Schedule	From the menu, select a schedule. For information about how to configure schedules, see *Define a Schedule* on page 292.
Send to LAN Server	From the menu, select **Single address**. In the **Start** field, enter the LAN IP address of the server that receives the video traffic.
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 server on the LAN that receives the video traffic. From the menu, select the WAN interface that you want to use.
WAN Users	From the menu, select **Address Range**. In the **Start** and **Finish** fields, specify the WAN address range from which the VPN firewall accepts video traffic.
QoS Profile	You can leave the selection from the menu at **None**.

Setting	Description
Log	You can leave the selection from the menu at **Never**.
Bandwidth Profile	You can leave the selection from the menu at **NONE**.

9. Click the **Apply** button.

   Your settings are saved. The new rule is added to the Inbound Services table on the LAN WAN Rules screen.

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

In this example, you configure multi-NAT 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. (Instead of on the LAN, you could also configure this web server in the DMZ.)

The example uses the following addressing scheme:

- NETGEAR VPN firewall:
  - WAN IP address. 10.1.0.118
  - LAN IP address subnet. 192.168.1.1 with subnet 255.255.255.0
- Web server computer on the VPN firewall's LAN:
  - LAN IP address. 192.168.1.2
  - Access to the web server is through the public IP address. 10.168.50.1

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

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > WAN Settings > WAN Setup**.

   The WAN Setup screen displays the IPv4 settings.

7. In the WAN IPv4 Settings table, click the **Edit** button for the WAN interface for which you want to add a secondary WAN address.

   The WAN IPv4 ISP Settings screen displays.

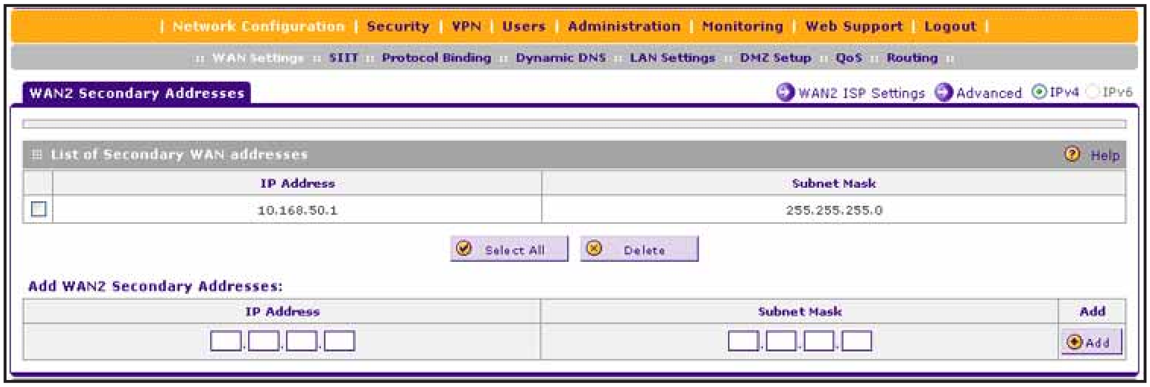
8. Click the **Secondary Addresses** option arrow in the upper right.

   The WAN Secondary Addresses screen displays for the WAN interface that you selected.

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

10. Click the **Add** button.

    The secondary IP address is added to the List of Secondary WAN addresses table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
WAN2 Secondary Addresses
WAN2 ISP Settings
Advanced
IPv4
IPv6
Help
Select All
Delete
Add

List of Secondary WAN addresses

	IP Address	Subnet Mask
□	10.168.50.1	255.255.255.0

Add WAN2 Secondary Addresses:

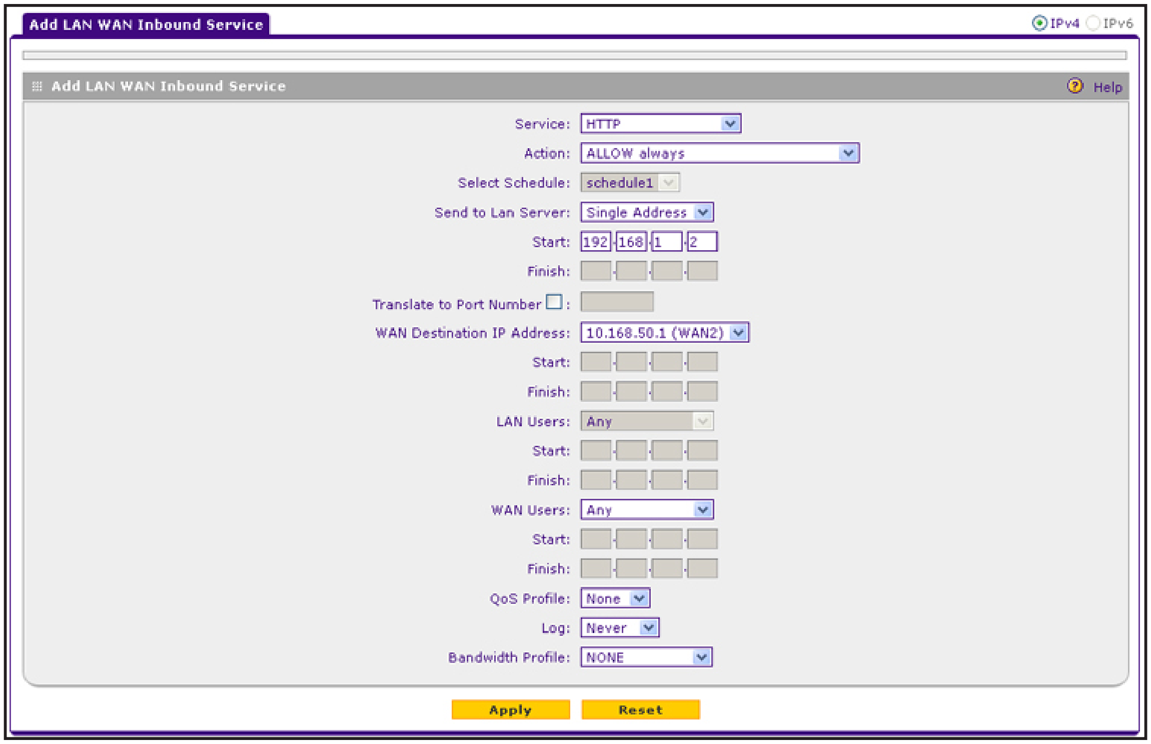
IP Address	Subnet Mask	Add
□.□.□.□	□.□.□.□	Add

11. Select **Security > Firewall**.

    The Firewall submenu tabs display with the LAN WAN Rules screen in view, displaying the IPv4 settings.

12. Under the Inbound Services table, click the **Add** button.

    The Add LAN WAN Inbound Service screen for IPv4 displays.



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: 10.168.50.1 (WAN2)
Start:
Finish:
LAN Users: Any
Start:
Finish:
WAN Users: Any
Start:
Finish:
QoS Profile: None
Log: Never
Bandwidth Profile: NONE

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

Setting	Description
Service	From the menu, select **HTTP**.
Action	From the menu, select **ALLOW always**.
Send to LAN Server	From the menu, select **Single address**. In the **Start** field, enter the LAN IP address of the web server.
WAN Destination IP Address	From the menu, select the secondary WAN IP address that you added in *Step 9* and *Step 10*.
WAN Users	From the menu, select **Any**.
QoS Profile	You can leave the selection from the menu at **None**.
Log	You can leave the selection from the menu at **Never**.
Bandwidth Profile	You can leave the selection from the menu at **NONE**.

14. Click the **Apply** button.

Your settings are saved. The new rule is added to the Inbound Services table on the LAN WAN Rules screen.

15. To test the connection from a computer on the Internet, type **http://<*IP_address*>**.

<*IP_address*> is the public IP address that you mapped to your web server. The home page of your web server displays.

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

If you want to restrict incoming reverse Telnet (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.

➤ **To restrict RTelnet traffic from a single WAN user to a single LAN user:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

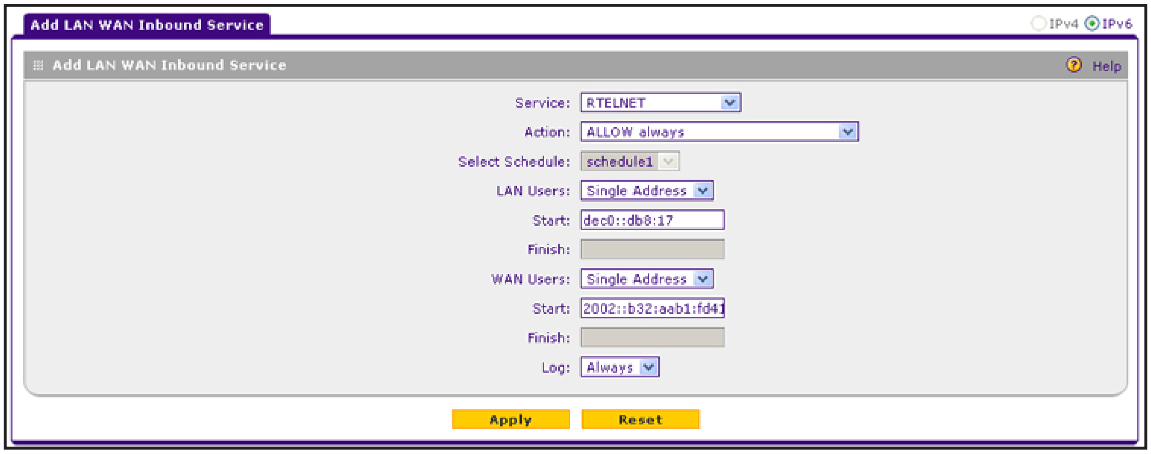
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Firewall**.

   The Firewall submenu tabs display with the LAN WAN Rules screen in view, displaying the IPv4 settings.
7. In the upper right, select the **IPv6** radio button.

   The LAN WAN Rules screen displays the IPv6 settings.
8. Under the Inbound Services table, click the **Add** button.

   The Add LAN WAN Inbound Service screen for IPv6 displays.



Service: RTELNET

Action: ALLOW always

Select Schedule: schedule1

LAN Users: Single Address

Start: dec0::db8:17

Finish:

WAN Users: Single Address

Start: 2002::b32:aab1:fd41

Finish:

Log: Always

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

Setting	Description
Service	From the menu, select **RTelnet**.
Action	From the menu, select **ALLOW always**.
LAN Users	From the menu, select **Single address**. In the **Start** field, enter the LAN IPv6 address that accepts RTelnet traffic.
WAN Users	From the menu, select **Single Address**. In the **Start** field, enter the WAN IPv6 address from which the VPN firewall accepts RTelnet traffic.
Log	From the menu, select **Always**. VPN firewall logs all RTelnet traffic that is covered by this rule.

10. Click the **Apply** button.

    Your settings are saved. The new rule is added to the Inbound Services table on the LAN WAN Rules screen.

Examples of Outbound Firewall Rules

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

The following sections provide examples of IPv4 LAN WAN and IPv6 DMZ WAN outbound rules:

- *IPv4 LAN WAN Outbound Rule: Block Instant Messenger*
- *IPv6 DMZ WAN Outbound Rule: Allow a Group of DMZ User to Access an FTP Site on the Internet*

IPv4 LAN WAN Outbound Rule: Block Instant Messenger

If you want to block Instant Messenger usage by employees during specific hours such as 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. You can also enable the VPN firewall to log any attempt to use Instant Messenger during the blocked period.

➢ **To block Instant Messenger according to a schedule and log attempts to access Instant Messenger:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

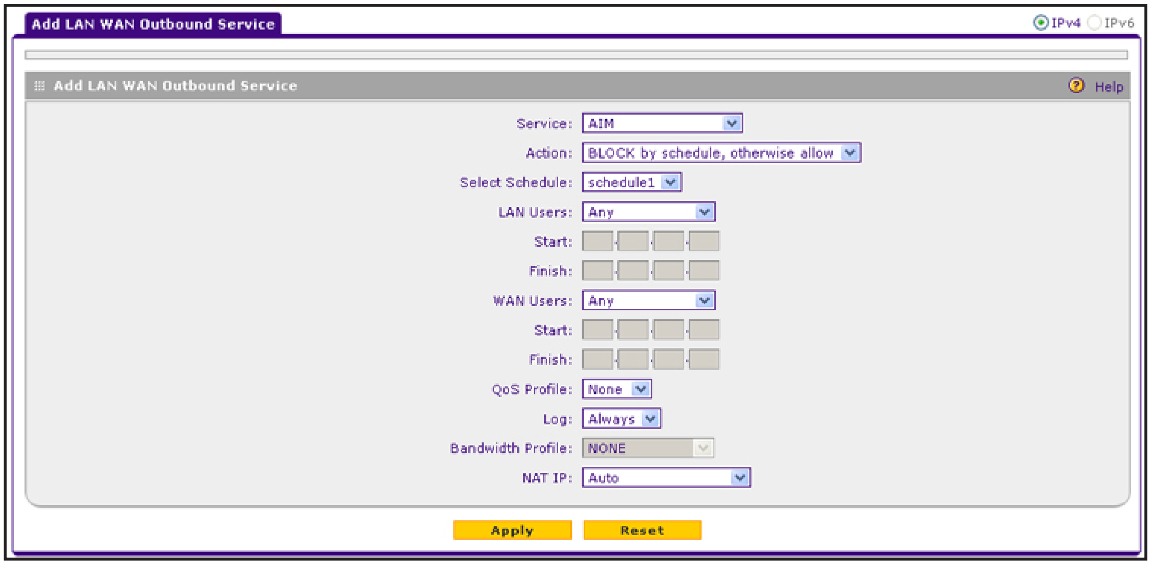
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Firewall**.

   The Firewall submenu tabs display with the LAN WAN Rules screen in view, displaying the IPv4 settings.
7. Under the Outbound Services table, click the **Add** button.

   The Add LAN WAN Outbound Service screen for IPv4 displays.



Service: AIM
Action: BLOCK by schedule, otherwise allow
Select Schedule: schedule1
LAN Users: Any
Start:
Finish:
WAN Users: Any
Start:
Finish:
QoS Profile: None
Log: Always
Bandwidth Profile: NONE
NAT IP: Auto

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

Setting	Description
Service	From the menu, select **AIM**.
Action	From the menu, select **BLOCK by schedule, otherwise allow**.
Select Schedule	From the menu, select a schedule. For information about how to configure schedules, see *Define a Schedule* on page 292.
LAN Users	From the menu, select **Any**. This rule affects all LAN users.
WAN Users	From the menu, select **Any**. This rule affects all WAN users.
QoS Profile	You can leave the selection from the menu at **None**.
Log	From the menu, select **Always**. VPN firewall logs all attempt to access Instant Messenger during the period that this rule is in effect.
Bandwidth Profile	You can leave the selection from the menu at **NONE**.
NAT IP	You can leave the selection from the menu at **Auto**.

9. Click the **Apply** button.

   Your settings are saved. The new rule is added to the Outbound Services table on the LAN WAN Rules screen.

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 specific hours such as 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. You can also configure the QoS profile to maximize the throughput.

- **To allows a group of users on the DMZ access to an FTP site on the Internet:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

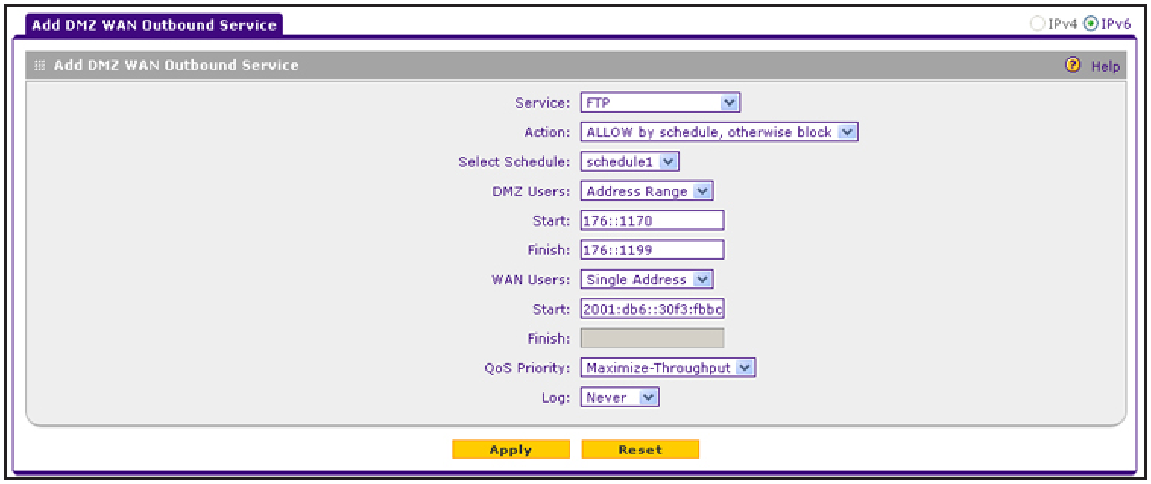
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Firewall > DMZ WAN Rules**.

   The DMZ WAN Rules screen displays the IPv4 settings.
7. In the upper right, select the **IPv6** radio button.

   The DMZ WAN Rules screen displays the IPv6 settings.
8. Under the Outbound Services table, click the **Add** button.

   The Add DMZ WAN Outbound Service screen for IPv6 displays.



Service: FTP

Action: ALLOW by schedule, otherwise block

Select Schedule: schedule1

DMZ Users: Address Range

Start: 176::1170

Finish: 176::1199

WAN Users: Single Address

Start: 2001:db6::30f3:fbbc

Finish:

QoS Priority: Maximize-Throughput

Log: Never

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

Setting	Description
Service	From the menu, select **FTP**.
Action	From the menu, select **ALLOW by schedule, otherwise block**.
Select Schedule	From the menu, select a schedule. For information about how to configure schedules, see *Define a Schedule* on page 292.
DMZ Users	From the menu, select **Address Range**. In the **Start** and **Finish** fields, specify the DMZ IPv6 address range for the users that are allowed to access the FTP server.
WAN Users	From the menu, select **Single Address**. In the **Start** field, enter the WAN IPv6 address of the FTP server on the Internet.
Log	You can leave the selection from the menu at **Never**.
QoS Priority	From the menu, select **Maximize-Throughput**. For more information about QoS priorities for IPv6 traffic, see *Default Quality of Service Priorities for IPv6 Firewall Rules* on page 298.

10. Click the **Apply** button.

    Your settings are saved. The new rule is added to the Outbound Services table on the DMZ WAN Rules screen.

Configure Other Firewall Features

The following sections provide information about other firewall features:

- *Manage Protection Against Common Network Attacks*
- *Manage VPN Pass-Through*

- *Set Limits for IPv4 Sessions*
- *Manage Time-Out Periods for TCP, UDP, and ICMP Sessions*
- *Manage Multicast Pass-Through*
- *Manage the Application Level Gateway for SIP Sessions*

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

Manage Protection Against Common Network Attacks

For IPv4 traffic, you can specify whether the VPN firewall is protected against common attacks in the WAN and LAN networks. For IPv6 traffic, the only option is to specify the ping settings for the WAN ports.

The following sections provide information about managing protection against common network attacks:

- *Manage Protection Against IPv4 Network Attacks*
- *Manage the Ping Settings for the IPv6 WAN Ports*

Manage Protection Against IPv4 Network Attacks

The following procedure describes how to manage protection against IPv4 network attacks by setting up WAN and LAN security checks, including the ping settings for the IPv4 WAN ports.

➢ **To manage protection against IPv4 attacks for your network environment:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

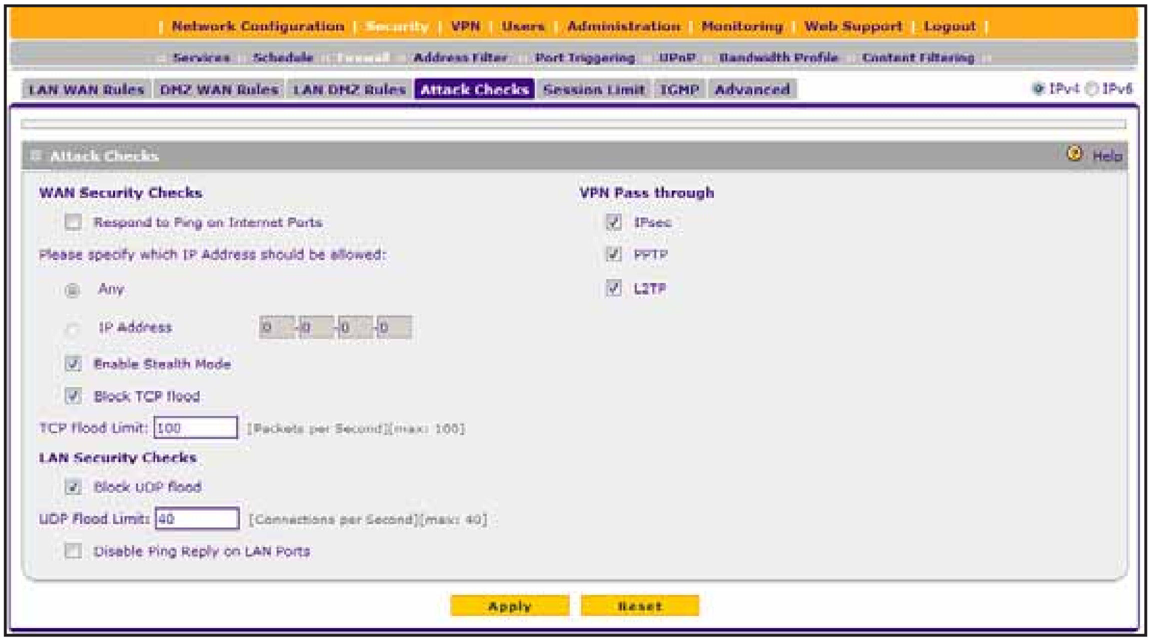
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Firewall > Attack Checks**.

The Attack Checks screen displays the IPv4 settings.


| 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 | IGMP | Advanced
● IPv4 ○ IPv6
Attack Checks
Help
Apply
Reset

WAN Security Checks

□ Respond to Ping on Internet Ports

Please specify which IP Address should be allowed:

● Any

○ IP Address 0 . 0 . 0 . 0

☑ Enable Stealth Mode

☑ Block TCP flood

TCP Flood Limit: 100 [Packets per Second][max: 100]

LAN Security Checks

☑ Block UDP flood

UDP Flood Limit: 40 [Connections per Second][max: 40]

□ Disable Ping Reply on LAN Ports

VPN Pass through

☑ IPsec

☑ PPTP

☑ L2TP

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

Setting	Description
WAN Security Checks	
Respond to Ping on Internet Ports	Select the **Respond to Ping on Internet Ports** check box to enable the VPN firewall to respond to a ping from the Internet to its IPv4 address. A ping can be used as a diagnostic tool. Keep this check box cleared unless you have a specific reason to enable the VPN firewall to respond to a ping from the Internet. If you select the **Respond to Ping on Internet Ports** check box, specify the IP address on which a ping is allowed: • **Any**. A ping is allowed on any IP address. This is the default setting. • **IP Address**. A ping is allowed only on a single IP address, which you must specify in the **IP Address** field.
Enable Stealth Mode	Select the **Enable Stealth Mode** check box to prevent the VPN firewall from responding to port scans from the WAN, thus making it less susceptible to discovery and attacks. By default, the **Enable Stealth Mode** check box is selected.
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. By default, the **Block TCP flood** check box is selected. In the **TCP Flood Limit** field, enter the number of packets per second that defines a SYN flood attack. You can enter a number from 1 to 100. The default value is 100. The VPN firewall drops TCP packets that exceed the specified number of packets per second. 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.

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. By default, the **Block UDP flood** check box is selected. In the **UDP Flood Limit** field, enter the number of connections per second that defines a UDP flood. You can enter a number from 1 to 40. The default value is 40. The VPN firewall drops UDP packets that exceed the specified number of connections per second. A UDP flood is a form of denial of service attack that can be initiated when one device sends many UDP packets to random ports on a remote host. As a result, the distant host does the following: 1. Checks for the application listening at that port. 2. Sees that no application is listening at that port. 3. Replies with an ICMP Destination Unreachable packet. When the victimized system is flooded, it is forced to send many ICMP packets, eventually making it unreachable by other clients. The attacker might also spoof the IP address of the UDP packets, ensuring that the excessive ICMP return packets do not reach the attacker, thus making the attacker’s network location anonymous.
Disable Ping Reply on LAN Ports	Select the **Disable Ping Reply on LAN Ports** check box to prevent the VPN firewall from responding to a ping on a LAN port. A ping can be used as a diagnostic tool. Keep this check box cleared unless you have a specific reason to prevent the VPN firewall from responding to a ping on a LAN port.

8. Click the **Apply** button.

   Your settings are saved.

Manage the Ping Settings for the IPv6 WAN Ports

The following procedure describes how to manage a WAN security check for IPv6 traffic by specifying the ping settings for the WAN ports. By default, the VPN firewall does not allow pings on the IPv6 WAN ports. Keep this setting unless you have a specific reason to enable the VPN firewall to respond to a ping from the Internet.

➢ **To allow pings on the IPv6 WAN ports and specify the ping settings:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

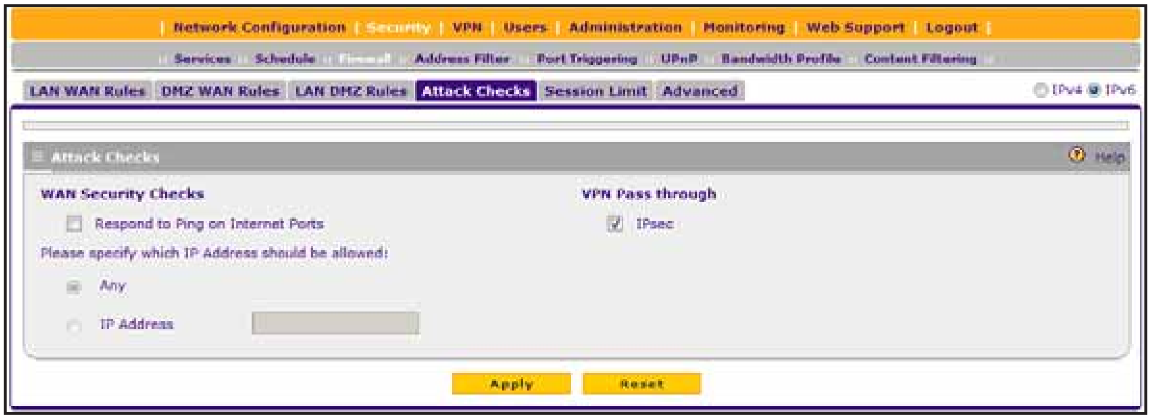
   The Router Status screen displays.

6. Select **Security > Firewall > Attack Checks**.

   The Attack Checks screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The Attack Checks screen displays the IPv6 settings.


| 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
Attack Checks
Help
Apply
Reset

○ IPv4 ● IPv6

WAN Security Checks

□ Respond to Ping on Internet Ports

Please specify which IP Address should be allowed:

● Any

○ IP Address

VPN Pass through

☑ IPsec

8. Select the **Respond to Ping on Internet Ports** check box.
9. Specify the IP addresses from which a ping is allowed by selecting one of the following radio buttons:
   - **Any**. A ping is allowed on any IP address. This is the default setting.
   - **IP Address**. A ping is allowed only on a single IP address, which you must specify in the **IP Address** field.
10. Click the **Apply** button.

    Your settings are saved.

Manage VPN Pass-Through

By default VPN pass-through is enabled on the VPN firewall. However, you can change the VPN pass-through settings for your network environment.

The following sections provide information about managing VPN pass-through:

- *VPN Pass-Through*

- *Manage VPN Pass-Through in the IPv4 Network*
- *Manage VPN Pass-Through in the IPv6 Network*

VPN Pass-Through

When the VPN firewall functions in NAT mode, all packets going to a 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 must 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 VPN pass-through.

By default, VPN pass-through is allowed on the VPN firewall, enabling VPN traffic that is initiated from the LAN to reach the WAN, irrespective of the default firewall outbound policy and custom firewall rules.

For IPv4 traffic, you can specify whether to allow or block VPN pass-through for IPSec, PPTP, and L2TP traffic. For IPv6 traffic, the only option is to specify whether to allow or block VPN pass-through for IPSec traffic.

Manage VPN Pass-Through in the IPv4 Network

The following procedure describes how to manage VPN pass-through for IPv4 traffic. By default, all types of VPN pass-through are allowed on the VPN firewall.

➢ **To manage VPN pass-through for IPv4 traffic:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

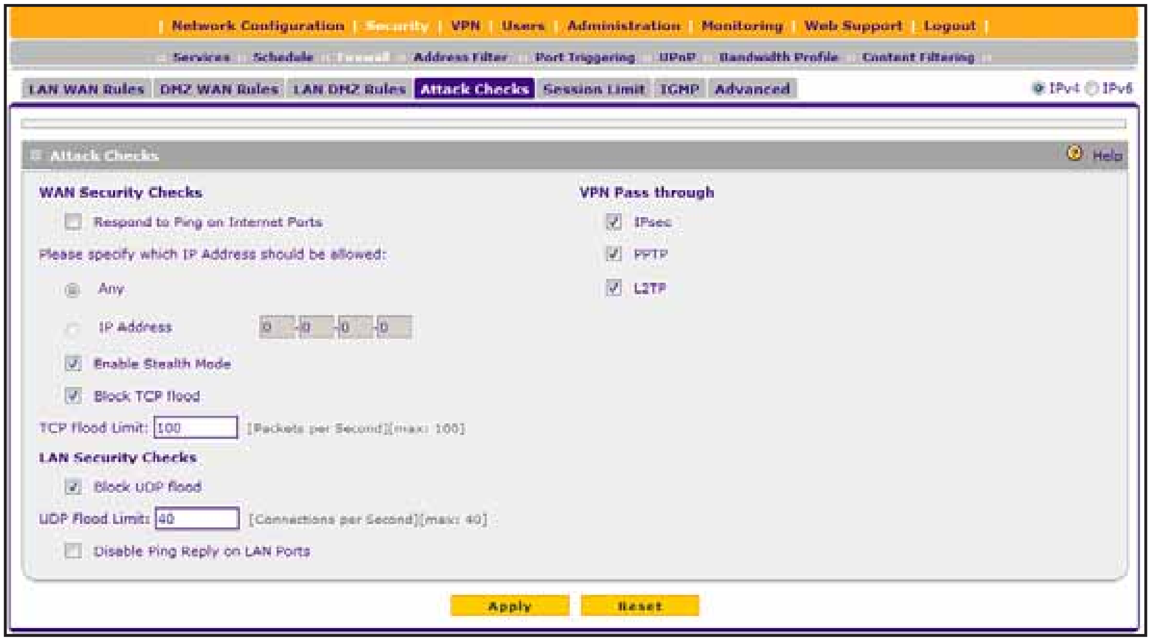
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Firewall > Attack Checks**.

   The Attack Checks screen displays the IPv4 settings.


| 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 | IGMP | Advanced
Help
Apply
Reset

● IPv4 ○ IPv6

Attack Checks

WAN Security Checks

□ Respond to Ping on Internet Ports

Please specify which IP Address should be allowed:

● Any

○ IP Address 0 . 0 . 0 . 0

☑ Enable Stealth Mode

☑ Block TCP flood

TCP Flood Limit: 100 [Packets per Second][max: 100]

LAN Security Checks

☑ Block UDP flood

UDP Flood Limit: 40 [Connections per Second][max: 40]

□ Disable Ping Reply on LAN Ports

VPN Pass through

☑ IPsec

☑ PPTP

☑ L2TP

7. To block VPN pass-through, clear any of the following check boxes, which are selected by default to allow VPN pass-through:
   - **IPSec**. Clearing this check box disables NAT filtering for IPSec tunnels.
   - **PPTP**. Clearing this check box disables NAT filtering for PPTP tunnels.
   - **L2TP**. Clearing this check box disables NAT filtering for L2TP tunnels.
8. Click the **Apply** button.

   Your settings are saved.

Manage VPN Pass-Through in the IPv6 Network

The following procedure describes how to manage VPN pass-through for IPv6 traffic. By default, VPN pass-through for IPsec is allowed on the VPN firewall, enabling IPSec VPN traffic that is initiated from the LAN to reach the WAN, irrespective of the default firewall outbound policy and custom firewall rules.

➢ **To manage IPv6 attack checks for your network environment:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

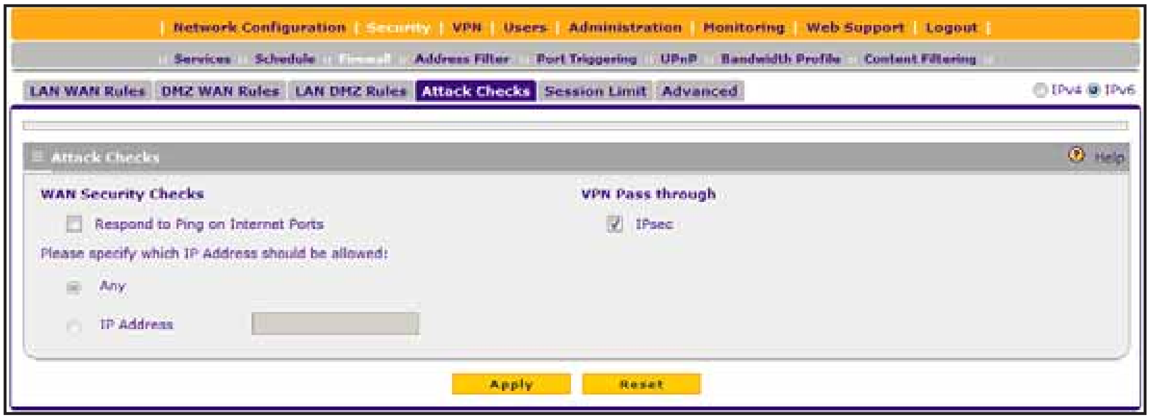
   The Router Status screen displays.

6. Select **Security > Firewall > Attack Checks**.

   The Attack Checks screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The Attack Checks screen displays the IPv6 settings.


| 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

Please specify which IP Address should be allowed:

● Any

○ IP Address

VPN Pass through

☑ IPsec

8. To block VPN pass-through for IPSec traffic, clear the **IPsec** check box, which is selected by default to allow VPN pass-through for IPSec traffic.

9. Click the **Apply** button.

   Your settings 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. On your computer, launch an Internet browser.

2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

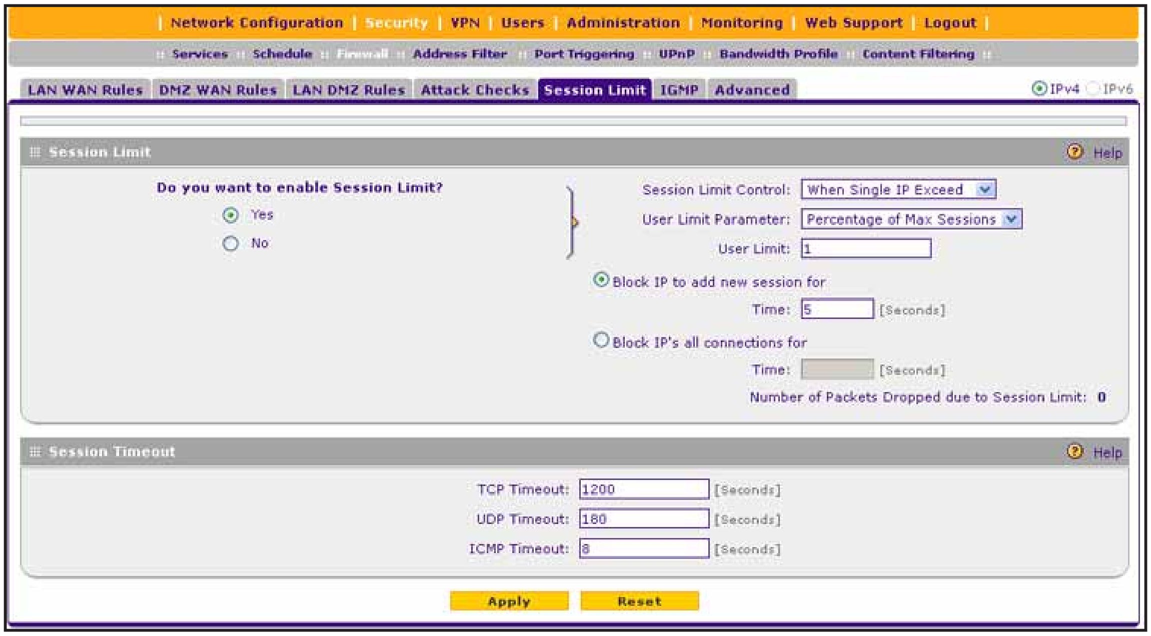
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > Firewall > Session Limit**.

   The Session Limit screen displays.


| 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
IGMP
Advanced
◉ IPv4 ○ IPv6
Help
Apply
Reset

Session Limit

Do you want to enable Session Limit?

◉ Yes

○ No

Session Limit Control: When Single IP Exceed

User Limit Parameter: Percentage of Max Sessions

User Limit: 1

◉ Block IP to add new session for

Time: 5 [Seconds]

○ Block IP's all connections for

Time: [Seconds]

Number of Packets Dropped due to Session Limit: 0

Session Timeout

TCP Timeout: 1200 [Seconds]

UDP Timeout: 180 [Seconds]

ICMP Timeout: 8 [Seconds]

7. Select the **Yes** radio button.

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

Setting	Description
Session Limit	
Session Limit Control	From the menu, select an option: • **When single IP exceeds**. When the limit is reached, no new session is allowed from the IP address. A new session is allowed only when an existing session is terminated or times out. You must specify the action and period by selecting one of the following radio buttons: - **Block IP to add new session for**. No new session is allowed from the IP address for a period. In the **Time** field, specify the period in seconds. - **Block IP's all connections for**. All sessions from the IP address are terminated, and new sessions are blocked for a period. In the **Time** field, specify the period in seconds. • **Single IP Cannot Exceed**. When the limit is reached, no new session is allowed from the IP address for a specified period, or all sessions from the IP address are terminated and new sessions are blocked for a specified period.
User Limit Parameter	From the menu, select an 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 selection from the **User Limit Parameter** is **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 selection from the **User Limit Parameter** is **Number of Sessions**, the number specifies an absolute value. **Note:** Some protocols such as FTP and RSTP create two sessions per connection, which you must consider when you configure a session limit.
Total Number of Packets Dropped due to Session Limit	This is a nonconfigurable counter that displays the total number of dropped packets when the session limit is reached.

9. Click the **Apply** button.

   Your settings are saved.

Manage Time-Out Periods for TCP, UDP, and ICMP Sessions

For IPv4 traffic, a TCP, UDP, or ICMP session expires if the VPN firewall does not process data for the session during the time-out period.

➢ **To manage the time-out periods for TCP, UDP, and ICMP sessions:**

1. On your computer, launch an Internet browser.

2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

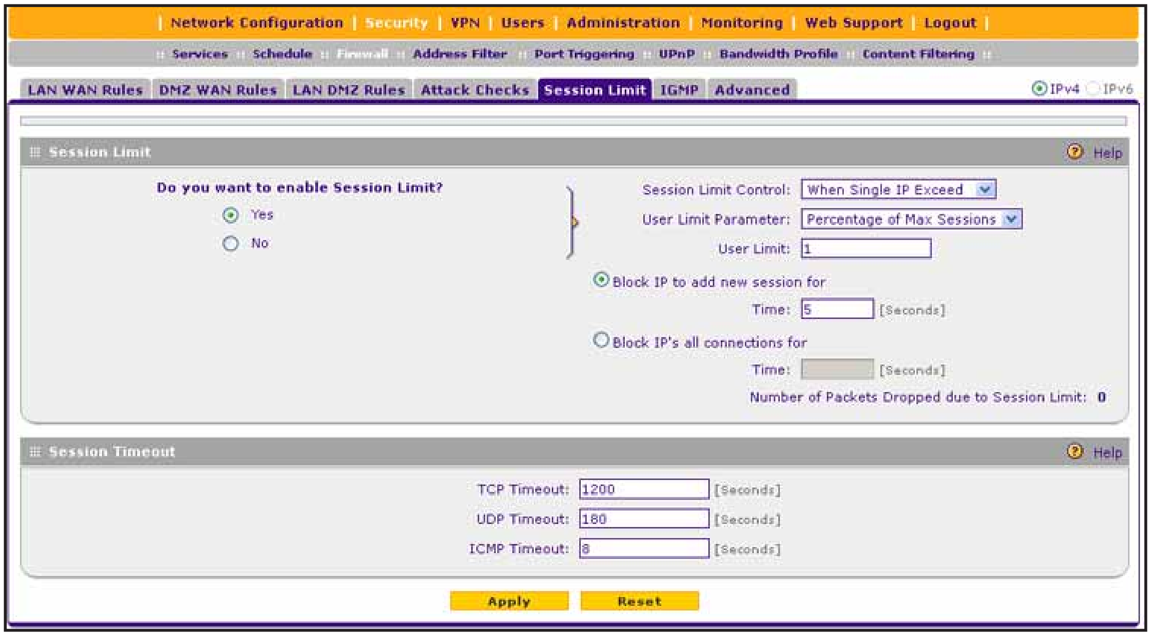
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > Firewall > Session Limit**.

   The Session Limit screen displays.


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 | IGMP | Advanced
Help
Help
Apply
Reset

● IPv4 ○ IPv6

Session Limit

Do you want to enable Session Limit?
● Yes
○ No

Session Limit Control: When Single IP Exceed
User Limit Parameter: Percentage of Max Sessions
User Limit: 1

● Block IP to add new session for
Time: 5 [Seconds]

○ Block IP's all connections for
Time: [Seconds]

Number of Packets Dropped due to Session Limit: 0

Session Timeout

TCP Timeout: 1200 [Seconds]
UDP Timeout: 180 [Seconds]
ICMP Timeout: 8 [Seconds]

7. In the Session Timeout section, enter the time-out periods in the following fields:
   - **TCP Timeout**. Enter a period in seconds.

     For TCP traffic, the default time-out period is 3600 seconds.
   - **UDP Timeout**.

     For UDP traffic, the default time-out period is 180 seconds.

- **ICMP Timeout**.

  For ICMP traffic, the default time-out period is 8 seconds.

8. Click the **Apply** button.

   Your settings are saved.

Manage Multicast Pass-Through

Multicast pass-through is supported for IPv4 traffic only. The following sections provide information about managing multicast pass-through:

- *Multicast Pass-Through*
- *Enable and Configure Multicast Pass-Through*
- *Remove One or More Multicast Source Addresses*

Multicast Pass-Through

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.

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

Enable and Configure Multicast Pass-Through

The following procedure describes how to enable and configure multicast pass-through for IPv4 traffic. By default, multicast pass-through is disabled.

➢ **To enable and configure multicast pass-through:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

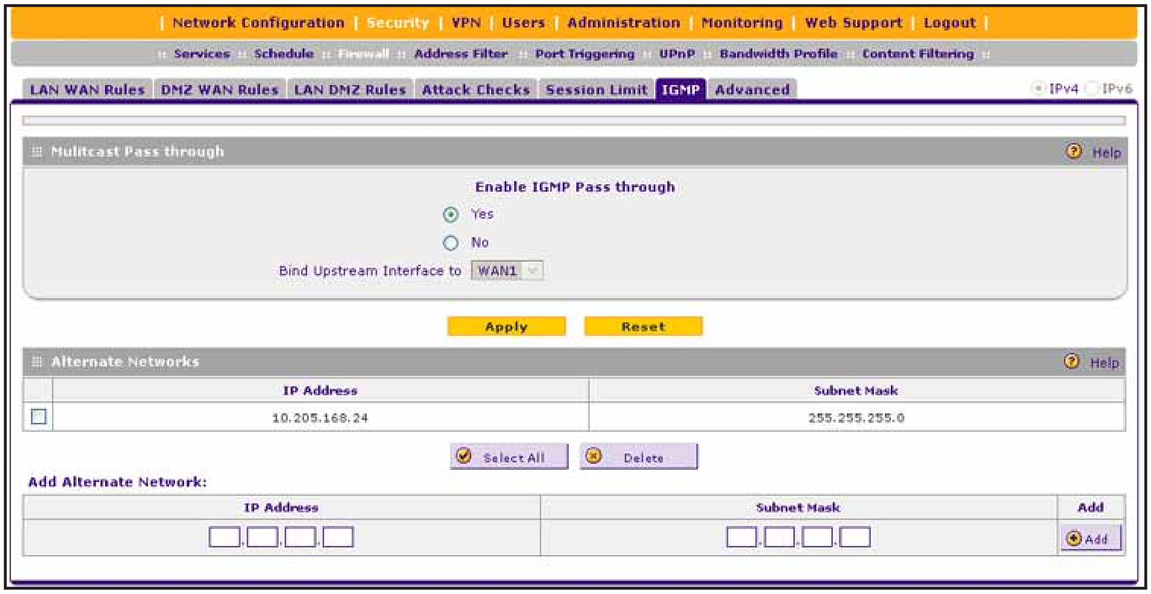
If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > Firewall > IGMP**.

   The IGMP screen displays. The following figure shows one alternate network 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
IGMP
Advanced
● IPv4 ○ IPv6
Help
Apply
Reset
Help
Select All
Delete
Add

Mulitcast Pass through

Enable IGMP Pass through

● Yes

○ No

Bind Upstream Interface to WAN1

Alternate Networks

	IP Address	Subnet Mask
□	10.205.168.24	255.255.255.0

Add Alternate Network:

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

7. Select the **Yes** radio button.

8. If you configured load balancing (see *Configure Load Balancing Mode and Optional Protocol Binding for IPv4 Interfaces* on page 49), from the **Bind Upstream Interface** menu, select the upstream interface (WAN1, the default, or WAN2) to which multicast traffic must be bound.

   Only a single interface can function as the upstream interface.

   Note: When you change the WAN mode to load balancing while multicast pass-through is already enabled, multicast traffic is bound to the active interface of the previous WAN mode.

9. Click the **Apply** button.

   Multicast pass-through is enabled.

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

    a. In the Alternate Networks section, below the table, enter the following settings:

       - **IP Address**. Enter the multicast source IP address.
       - **Subnet Mask**. Enter the subnet mask for the multicast source address.

b. Click the **Add** button.

   The multicast source address is added to the Alternate Networks table.

c. Repeat *Step a* and *Step b* for each multicast source address that you must add to the Alternate Networks table.

Remove One or More Multicast Source Addresses

The following procedure describes how to remove one or more multicast source addresses that you no longer need for a PPPoE or PPTP configuration.

➢ **To remove one or more multicast source addresses:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Firewall > IGMP**.

   The IGMP screen displays.
7. In the Alternate Networks table, select the check box to the left of each address that you want to remove or click the **Select All** button to select all addresses.
8. Click the **Delete** button.

   The selected addresses are removed from the Alternate Networks table.

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. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

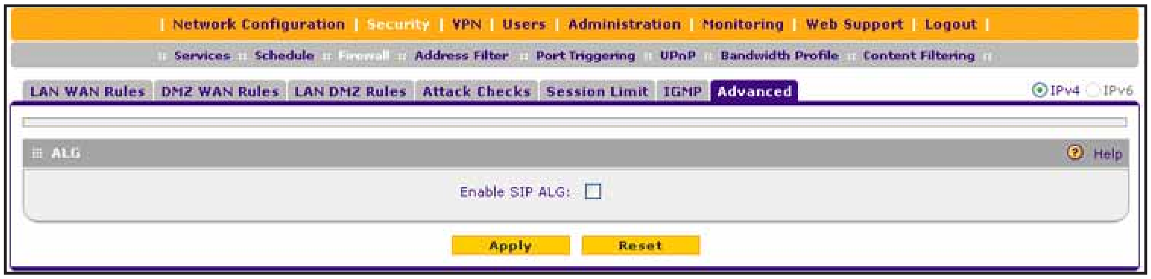
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Firewall > Advanced**.

   The Advanced screen displays.


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 | IGMP | Advanced
● IPv4 ○ IPv6
ALG
Help
Apply
Reset

Enable SIP ALG: □

7. Select the **Enable SIP ALG** check box.
8. Click the **Apply** button.

   Your settings are saved.

Manage Firewall Objects

The following sections provide information about firewall objects:

- *Firewall Objects*
- *Manage Customized Services*
- *Manage Service Groups*
- *Manage IP Address Groups*
- *Define a Schedule*

- *Manage Quality of Service Profiles for IPv4 Firewall Rules*
- *Default Quality of Service Priorities for IPv6 Firewall Rules*
- *Manage Bandwidth Profiles for IPv4 Traffic*

Firewall Objects

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

- **Services**. A service narrows down a firewall rule to an application and a port number. For information about managing customized services, see *Manage Customized Services* on page 280.
- **Service Groups**. A service groups narrows down a firewall rule to a group of services. For information about managing service groups, see *Manage Service Groups* on page 284.
- **IP groups**. An IP group is a LAN group or a WAN group to which you add individual IP addresses. You can narrow down a firewall rule to such an IP group. For information about managing IP groups, *Manage IP Address Groups* on page 288.
- **Schedules**. A schedule narrows down the period during which a firewall rule is applied. For information about managing schedules, see *Define a Schedule* on page 292.
- **QoS profiles and priorities**. A Quality of Service (QoS) profile defines the relative priority of an IP packet for traffic that matches a firewall rule.

  For information about creating QoS profiles for IPv4 firewall rules, see *Manage Quality of Service Profiles for IPv4 Firewall Rules* on page 293.

  For information about predefined QoS priorities that are available for IPv6 firewall rules, see *Default Quality of Service Priorities for IPv6 Firewall Rules* on page 298.
- **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 *Manage Bandwidth Profiles for IPv4 Traffic* on page 299.

Manage Customized Services

Services are functions performed by server computers at the request of client computers. You can configure up to 124 custom services.

The following sections provide information about managing customized services:

- *Services Overview*
- *Add a Customized Service*
- *Change a Customized Service*
- *Remove One or More Customized Services*

Services Overview

Examples of web servers that provide web services include the following: web servers provide web pages, time servers provide time and date information, and game hosts provide 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. You can add additional services and applications for use in defining firewall rules.

To define a new service, you must first determine which port number or range of numbers is used by the application. You can usually find this information by contacting the publisher of the application, user groups, or newsgroups. When you have the port number information, you can add the new service.

Add a Customized Service

The following procedure describes how to add a customized service that you then can use as an object for a firewall rule.

➢ **To add a customized service:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

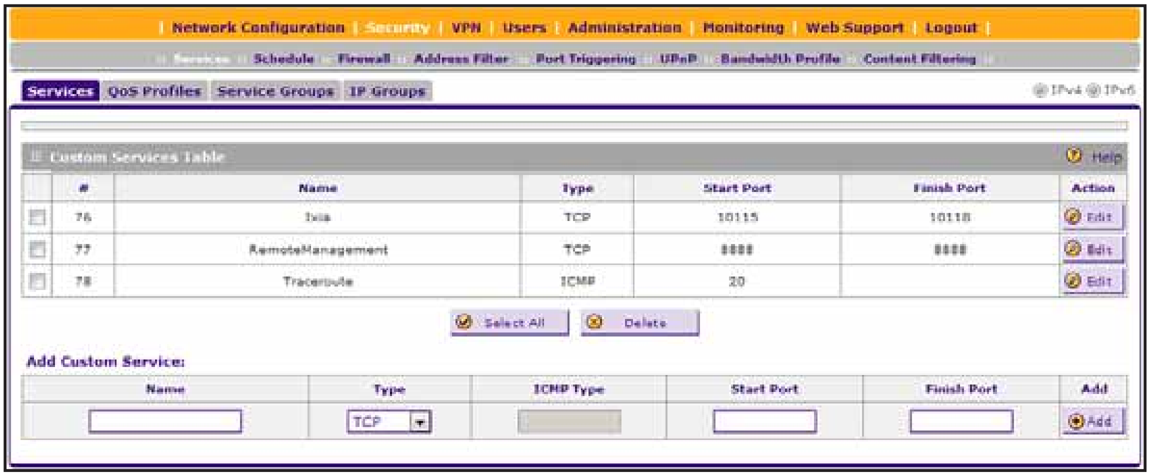
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > Services**.

   The Services screen displays. The Custom Services Table shows the user-defined services. The following figure shows some examples.


| 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
□	76	Ixia	TCP	10115	10118	Edit
□	77	RemoteManagement	TCP	8888	8888	Edit
□	78	Traceroute	ICMP	20		Edit

Add Custom Service:

Name	Type	ICMP Type	Start Port	Finish Port	Add
	TCP				Add

7. In the Add Customer Service section, enter the settings as described in the following table.

Setting	Description
Name	A descriptive name of the service for identification and management purposes.
Type	From the **Type** menu, select the Layer 3 protocol that the service uses as its transport protocol: **TCP**, **UDP**, **ICMP**, or **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** menu.
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** menu.
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** menu.

8. Click the **Apply** button.

   Your settings are saved. The new custom service is added to the Custom Services table.

Change a Customized Service

The following procedure describes how to change an existing customized service.

➢ **To change a service:**

1. On your computer, launch an Internet browser.

2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

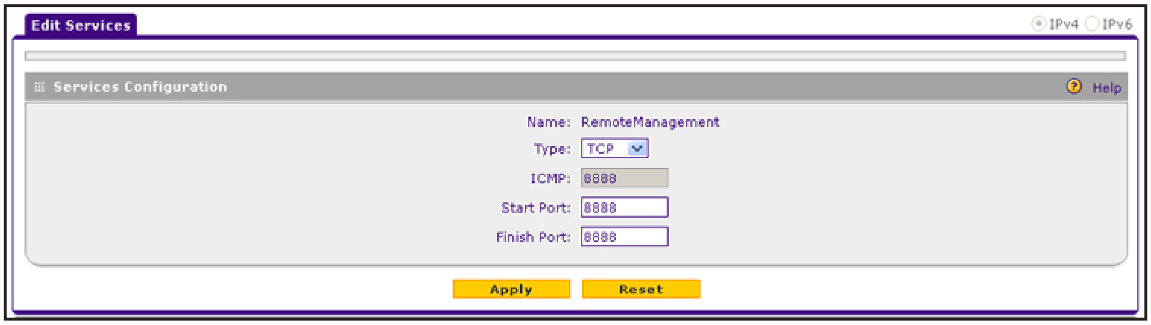
   The Router Status screen displays.

6. Select **Security > Services**.

   The Services screen displays.

7. In the Custom Services table, click the **Edit** button for the service that you want to change.

   The Edit Service screen displays.



Name: RemoteManagement
Type: TCP
ICMP: 8888
Start Port: 8888
Finish Port: 8888

8. Change the settings.

   For information about the settings, see *Add a Customized Service* on page 281.

9. Click the **Apply** button.

   Your settings are saved. The modified service displays in the Custom Services table on the Services screen.

Remove One or More Customized Services

The following procedure describes how to remove one or more customized services that you no longer need as objects for firewall rules.

➢ **To remove one or more customized services:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Services**.

   The Services screen displays.
7. In the Custom Services table, select the check box to the left of each service that you want to remove, or click the **Select All** button to select all services.
8. Click the **Delete** button.

   The selected services are removed from the Custom Services table.

Manage Service Groups

You can combine default and customized services into service groups. The following sections provide information about managing customized services:

- *Service Groups Overview*
- *Add a Service Group*
- *Change a Service Group*
- *Remove One or More Service Groups*

Service Groups Overview

A service group can contain a collection of predefined and customized services. (TCP and UDP customized services can be included in a service group.) You use a service group as a firewall object to which you apply a firewall rule.

One advantage of a service group is that you can create a single firewall object with multiple noncontiguous ports (for example ports 3000, 4000, and 5000) and apply the object in a single firewall rule. For example, in a configuration with 10 web servers, each of which requires the same three port-forwarding rules, you can create a service group for the port-forwarding rules and an IP group for the web servers (see *Manage IP Address Groups* on page 288) and then create only one firewall rule.

Add a Service Group

The following procedure describes how to add a service group that you then can use as an object for a firewall rule.

➤ **To add a service group:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

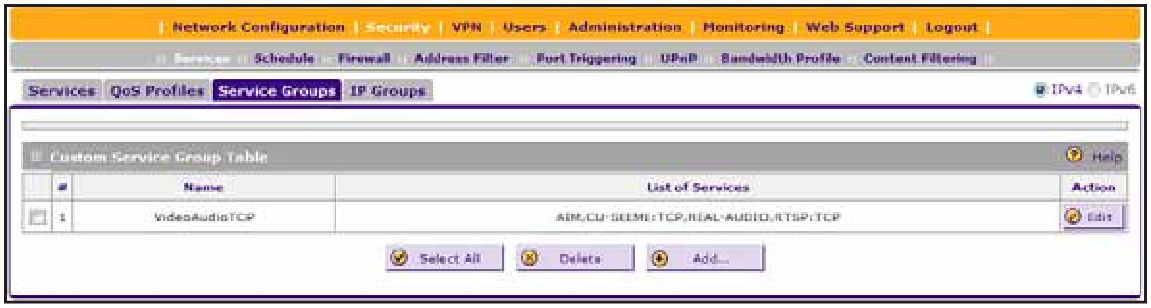
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Security > Services > Service Groups**.

   The Service Groups screen displays. The following figure shows an example.

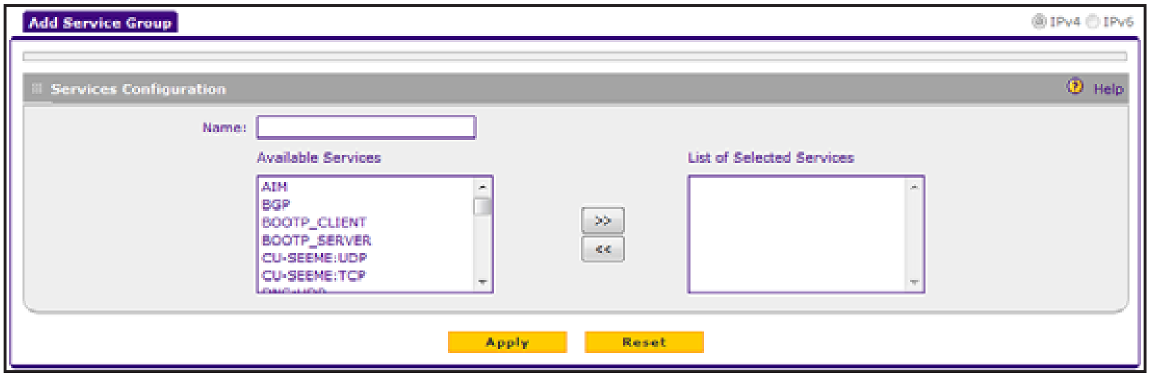

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
Services | Schedule | Firewall | Address Filter | Port Triggering | UPnP | Bandwidth Profile | Content Filtering |
Services
QoS Profiles
Service Groups
IP Groups
● IPv4 ○ IPv6
Help
Select All
Delete
Add...

Custom Service Group Table

	#	Name	List of Services	Action
□	1	VideoAudioTCP	AIM,CU-SEEME:TCP,REAL-AUDIO,RTSP:TCP	Edit

7. Under the Custom Service Group table, click the **Add** button.

   The Add Service Group screen displays.



8. In the **Name** field, enter a name for the service.
9. Specify the services for the group by use the move buttons (**<<** and **>>**) to move services between the **Available Services** field and the **List of Selected Services** field.

   Note: You cannot combine TCP and UDP services in the same group.

10. Click the **Apply** button.

    Your settings are saved. The new service group displays in the Custom Services Group table on the Service Groups screen.

Change a Service Group

The following procedure describes how to change an existing service group.

➢ **To change a service group:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Security > Services > Service Groups**.

   The Service Group screen displays.

7. In the Custom Service Group Table, click the **Edit** button for the service group that you want to change.

   The Edit Service Group screen displays.

8. Change the settings.

   For information about the settings, see *Add a Service Group* on page 285.

9. Click the **Apply** button.

   Your settings are saved. The modified service group displays in the Custom Service Group Table on the Service Group screen.

Remove One or More Service Groups

The following procedure describes how to remove one or more service groups that you no longer need as objects for firewall rules.

➢ **To remove one or more service groups:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Security > Services > Service Groups**.

   The Service Groups screen displays.

7. In the Custom Service Group Table, select the check box to the left of each service group that you want to remove or click the **Select All** button to select all service groups.
8. Click the **Delete** button.

   The selected service groups are removed from the Custom Service Group Table.

Manage IP Address Groups

You can combine individual IP addresses into IP address groups. The following sections provide information about managing IP address groups:

- *IP Address Groups Overview*
- *Add an IP Address Group*
- *Change an IP Address Group*
- *Remove One or More IP Address Groups*

IP Address Groups Overview

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

An example of how you can use an IP group is as follows:

In a configuration with 10 web servers, each of which requires the same three port-forwarding rules, you can create a service group for the port-forwarding rules (see *Manage Service Groups* on page 284) and an IP group for the web servers, and then create only one firewall rule.

Add an IP Address Group

The following procedure describes how to add an IP group that you then can use as an object for a firewall rule.

➢ **To add an IP group:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

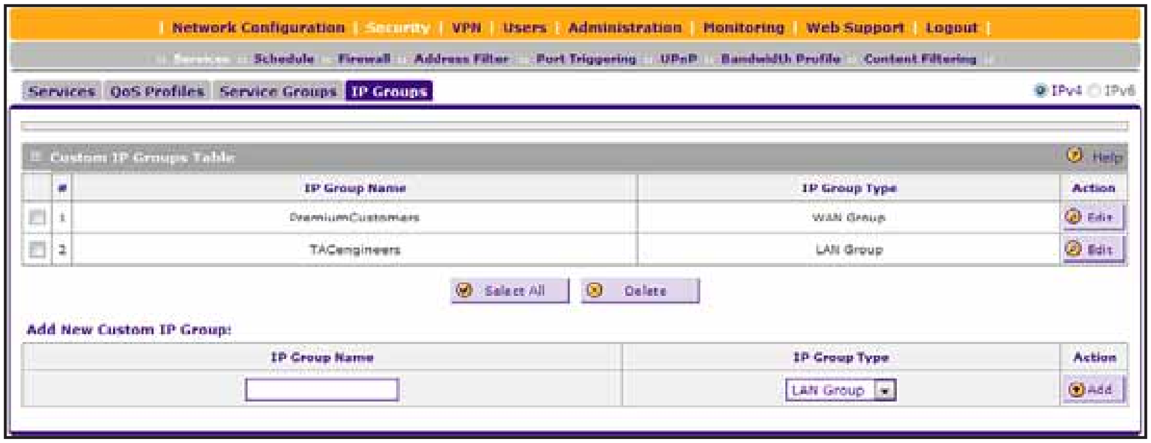
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > Services > IP Groups**.

   The IP Groups screen displays. The following figure shows two groups in the Custom IP Groups Table as examples.



| 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 IP Groups Table

	#	IP Group Name	IP Group Type	Action
□	1	PremiumCustomers	WAN Group	Edit
□	2	TACengineers	LAN Group	Edit

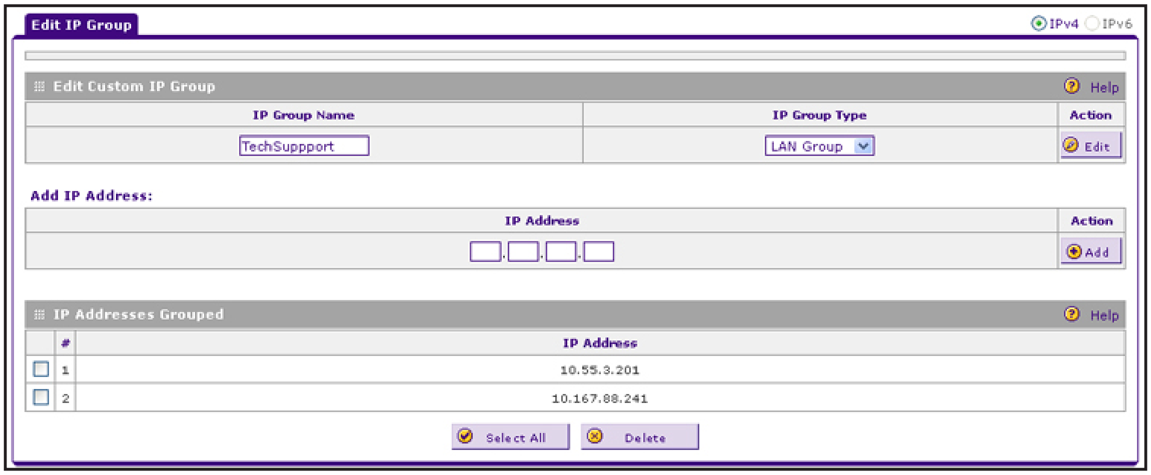
Add New Custom IP Group:

IP Group Name	IP Group Type	Action
	LAN Group	Add

7. In the Add New Custom IP Group section, do the following:
   - In the **IP Group Name** field, enter a name for the group.
   - From the **IP Group Type** menu, select **LAN Group** or **WAN Group**.
8. Click the **Apply** button.

   Your settings are saved. The new IP group is displayed in the Custom IP Groups Table.
9. In the Custom IP Groups Table, click the **Edit** button for the IP group that you just created.

   The Edit IP Group screen displays. The following figure shows two IP addresses in the IP Addresses Grouped table as examples.



Edit Custom IP Group

IP Group Name	IP Group Type	Action
TechSuppport	LAN Group	Edit

Add IP Address:

IP Address	Action
___.___.___.___	Add

IP Addresses Grouped

	#	IP Address
□	1	10.55.3.201
□	2	10.167.88.241

10. In the **IP Address** field, type an IP address.
11. Click the **Add** button.

    The IP address is added to the IP Addresses Grouped table.

12. Repeat the previous two steps to add more IP addresses to the IP Addresses Grouped table.
13. Click the **Edit** button again.

    The IP Groups screen displays. The group configuration is complete.

Change an IP Address Group

The following procedure describes how you can change an existing IP group.

➢ **To change an IP group:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Services > IP Groups**.

   The IP Groups screen displays.
7. In the Custom IP Groups Table, click the **Edit** button for the IP group that you want to change.

   The Edit IP Group screen displays.
8. Change the settings.

   You can change the group name and you can change the group type. You cannot change an IP address that is associated with the group but you can remove the IP address and replace it with another IP address.
9. To remove one or more IP addresses that are associated with the group and add new IP addresses, do the following:
   a. In the IP Addresses Grouped table, select the check box to the left of each IP address that you want to remove, or click the **Select All** button to select all IP addresses.
   b. Click the **Delete** button.

The selected IP addresses are removed from the IP Addresses Grouped table.

c. In the **IP Address** field, type an IP address.

d. Click the **Add** button.

The IP address is added to the IP Addresses Grouped table.

e. To add another IP address, repeat *Step c* and *Step d*.

10. Click the **Edit** button again.

Your settings are saved and the IP Groups screen displays. The modified IP group displays in the Custom IP Groups Table.

Remove One or More IP Address Groups

The following procedure describes how to remove one or more IP groups that you no longer need as objects for firewall rules.

➢ **To remove one or more IP groups:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Services > IP Groups**.

   The IP Groups screen displays.
7. In the Custom IP Groups table, select the check box to the left of the IP group that you want to remove, or click the **Select All** button to select all groups.
8. Click the **Delete** button.

   The selected groups are removed from the Custom IP Groups table.

Define a Schedule

Schedules define the time frames under which firewall rules are applied. Three schedules, Schedule 1, Schedule 2, and Schedule 3, can be defined, and you can select any one of these when defining firewall rules.

Other than the tab that you click to specify the schedule that you want to configure, the procedure to define Schedule 2 and Schedule 3 is identical to the procedure to define Schedule 1.

➢ **To define Schedule 1:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

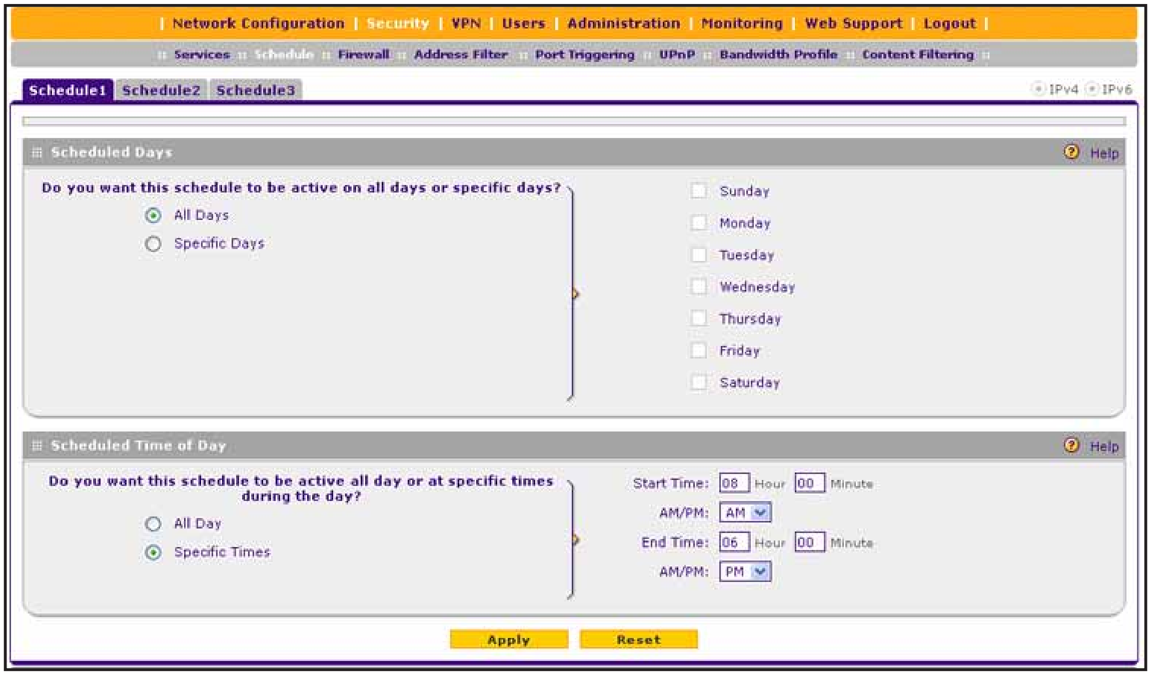
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Services > Schedule 1**.

   The Schedule1 screen displays.


| 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: 08 Hour 00 Minute
AM/PM: AM
End Time: 06 Hour 00 Minute
AM/PM: PM

7. In the Scheduled Days section, select a radio button:
   - **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.
8. In the Scheduled Time of Day section, select a radio button:
   - **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, complete the **Start Time** and **End Time** fields and select the meridiem from the **AM/PM** menu to define the time during which the schedule is in effect.
9. Click the **Apply** button.

   Your settings are saved to Schedule 1.

Manage Quality of Service Profiles for IPv4 Firewall Rules

When multiple connections are scheduled for simultaneous transmission on the VPN firewall, a Quality of Service (QoS) profile can define the relative priority of an IPv4 packet.

The following sections provide information about managing quality of service profiles for IPv4 firewall rules:

- *IPv4 QoS Profiles Overview*
- *Add an IPv4 QoS Profile*

- *Change an IPv4 QoS Profile*
- *Remove One or More IPv4 QoS Profiles*

IPv4 QoS Profiles Overview

A QoS profile becomes active only when it is associated with a nonblocking inbound or outbound firewall rule or service and IPv4 traffic that matches the firewall rule or service is processed by the VPN firewall. The *Type of Service in the Internet Protocol Suite standards*, RFC 1349, defines the priorities.

You can assign a QoS profile to the following IPv4 firewall rules:

- LAN WAN outbound rules (see *Add an IPv4 LAN WAN Outbound Rule* on page 224)
- LAN WAN inbound rules (see *Add an IPv4 LAN WAN Inbound Rule* on page 229)
- DMZ WAN outbound rules (see *Add an IPv4 DMZ WAN Outbound Rule* on page 233)
- DMZ WAN inbound rules (see *Add an IPv4 DMZ WAN Inbound Rule* on page 238)

Note: When you apply a QoS profile to a firewall rule for the first time, the performance of the VPN firewall might be affected slightly.

The VPN firewall does not provide any default QoS profiles for IPv4 traffic. If you want to use QoS for IPv4 traffic, you must add QoS profiles. You *could* create QoS profiles similar to the default QoS priorities that the VPN firewall provides for IPv6 traffic (see *Default Quality of Service Priorities for IPv6 Firewall Rules*).

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

Add an IPv4 QoS Profile

The following procedure describes how to add an IPv4 QoS profile that you then can use as an object for a firewall rule.

➢ **To add an IPv4 QoS profile:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

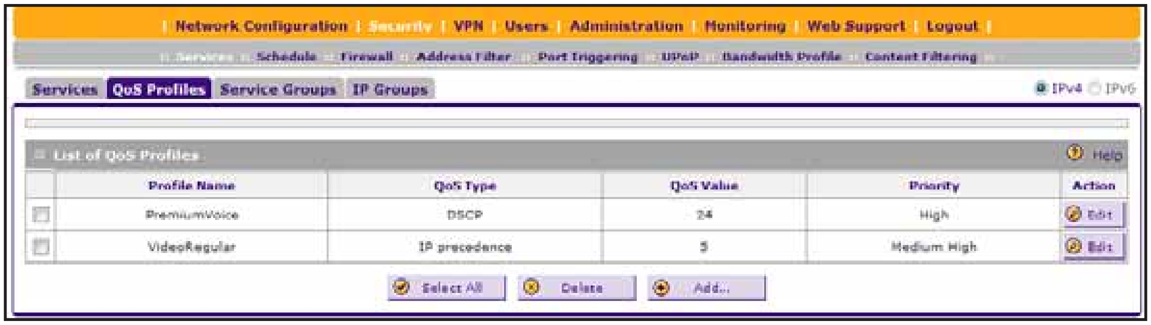
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > Services > QoS Profiles**.

   The QoS Profile screen displays. The following figure shows some user-define profiles in the List of QoS Profiles table as examples.

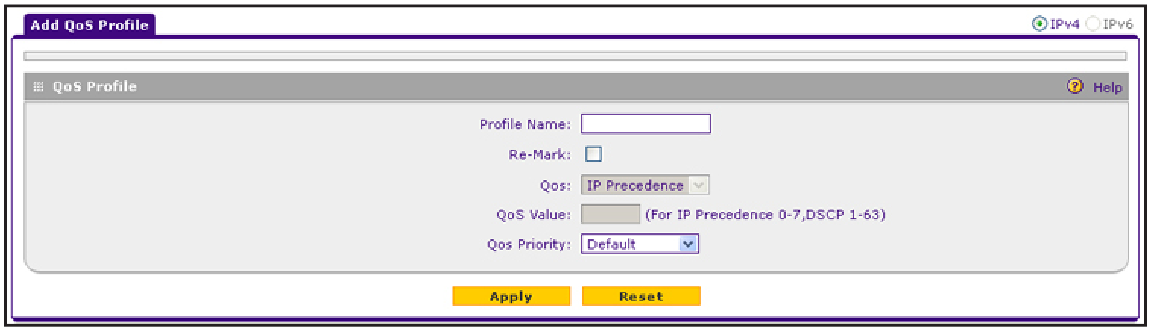

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile :: Content Filtering ::
Services
QoS Profiles
Service Groups
IP Groups
● IPv4 ○ IPv6
Help
Select All
Delete
Add...

List of QoS Profiles

	Profile Name	QoS Type	QoS Value	Priority	Action
□	PremiumVoice	DSCP	24	High	Edit
□	VideoRegular	IP precedence	5	Medium High	Edit

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

   The Add QoS Profile screen displays.



QoS Profile

Profile Name:	
Re-Mark:	□
Qos:	IP Precedence
QoS Value:	(For IP Precedence 0-7,DSCP 1-63)
Qos Priority:	Default

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

Setting	Description
Profile Name	A descriptive name of the QoS profile for identification and management purposes.
Re-Mark	Select the **Re-Mark** check box to set the Differentiated Services (DiffServ) mark in the Type of Service (ToS) byte of an IP header by specifying the QoS type (IP precedence or DHCP) and QoS value. Make a selection from the **QoS** menu and enter a value in the **QoS Value** field: • **QoS**. Select a traffic classification method: - **IP Precedence**. A legacy method that sets the priority in the ToS byte of an IP header. - **DSCP**. A method that sets the Differentiated Services Code Point (DSCP) in the Differentiated Services (DS) field (which is the same as the ToS byte) of an IP header. • **QoS Value**. Enter the QoS value that the VPN firewall must compare against the QoS value in the ToS or DiffServ byte of an IP header. The QoS value that you must enter depends on your selection from the **QoS** menu: - For IP Precedence, select a value from 0 to 7. - For DSCP, select a value from 1 to 63. If you clear the **Re-Mark** check box (which is the default setting), the QoS profile is specified only by the QoS priority.
QoS Priority	The QoS priority represents the classification level of the packet among the priority queues within the VPN firewall. If you select **Default**, packets are mapped based on the ToS bits in their IP headers. From the **QoS Priority** menu, select a priority queue: • **Default** • **High** • **Medium High** • **Medium** • **Low**

9. Click the **Apply** button.

   Your settings are saved. The new QoS profile is added to the List of QoS Profiles table.

Change an IPv4 QoS Profile

The following procedure describes how to change an existing IPv4 QoS profile.

➤ **To change an IPv4 QoS profile:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > Services > QoS Profiles**.

   The QoS Profiles screen displays.

7. In the List of QoS Profiles table, click the **Edit** button for the QoS profile that you want to change.

   The Edit QoS Profile screen displays.

8. Change the settings.

   For information about the settings, see *Add an IPv4 QoS Profile* on page 294.

9. Click the **Apply** button.

   Your settings are saved. The modified QoS profile displays in the List of QoS Profiles table on the QoS Profiles screen.

Remove One or More IPv4 QoS Profiles

The following procedure describes how to remove one or more IPv4 QoS profiles that you no longer need as objects for firewall rules.

➢ **To remove one or more IPv4 QoS profiles:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > Services > QoS Profiles**.

   The QoS Profiles screen displays.

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

   The selected profiles are removed from the List of QoS Profiles table.

Default Quality of Service Priorities for IPv6 Firewall Rules

A QoS default profile becomes active only when it is associated with a nonblocking outbound firewall rule or service and IPv6 traffic that matches the firewall rule or service is processed by the VPN firewall.

For IPv6 firewall rules and services, you cannot configure QoS profiles. The VPN firewall provides default QoS priorities that you can assign to the following IPv6 firewall rules:

- LAN WAN outbound rules (see *Add an IPv6 LAN WAN Outbound Rule* on page 226)
- DMZ WAN outbound rules (see *Add an IPv6 DMZ WAN Outbound Rule* on page 235)

Note: When you apply a QoS profile to a firewall rule for the first time, the performance of the VPN firewall might be affected slightly.

The QoS priorities are preconfigured and you cannot change them:

- **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 that has 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.

Manage Bandwidth Profiles for IPv4 Traffic

Bandwidth profiles determine how fast or slow data is communicated with the hosts. The following sections provide information about managing quality of service profiles for IPv4 firewall rules:

- *Bandwidth Profiles Overview*
- *Add and Enable a Bandwidth Profile*
- *Change a Bandwidth Profile*
- *Remove One or More Bandwidth Profiles*

Bandwidth Profiles Overview

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. You can use a single bandwidth profile 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 the following happens:

- If the rule has a bandwidth profile specification, the device creates a bandwidth class in the kernel.
- If multiple connections correspond to the same firewall rule, the connections all share the same bandwidth class.

An exception occurs for an individual bandwidth profile if the classes are per-source IP address classes. The source IP address is the IP address of the first packet that is transmitted for the connection. So for outbound firewall rules, the source IP address is the LAN-side IP address; for inbound firewall rules, the source IP address is the WAN-side IP address. The class is removed when all the connections that are using the class expire.

After you create a bandwidth profile, you can assign the bandwidth profile to the following firewall rules:

- LAN WAN outbound rules for IPv4 (see *Add an IPv4 LAN WAN Outbound Rule* on page 224).
- LAN WAN inbound rules for IPv4 (see *Add an IPv4 LAN WAN Inbound Rule* on page 229).

Note: For bandwidth profiles to functions correctly, make sure that you configure the WAN upload and download settings correctly. For more information, see *Managing Advanced WAN Options* on page 66.

Add and Enable a Bandwidth Profile

The following procedure describes how to add and enable a bandwidth profile that you then can use as an object for a firewall rule.

Note: When you enable a bandwidth profile, the performance of the VPN firewall might be affected slightly.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

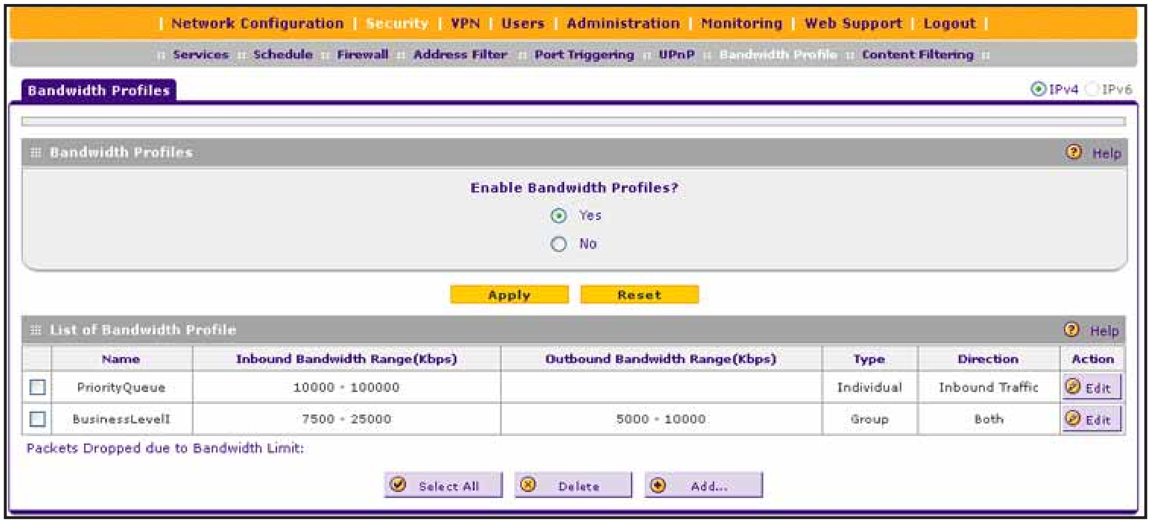
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Bandwidth Profiles**.

   The Bandwidth Profiles screen displays. The following figure shows some examples.


| 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
Bandwidth Profiles
Help
Apply
Reset
List of Bandwidth Profile
Help
Select All
Delete
Add...

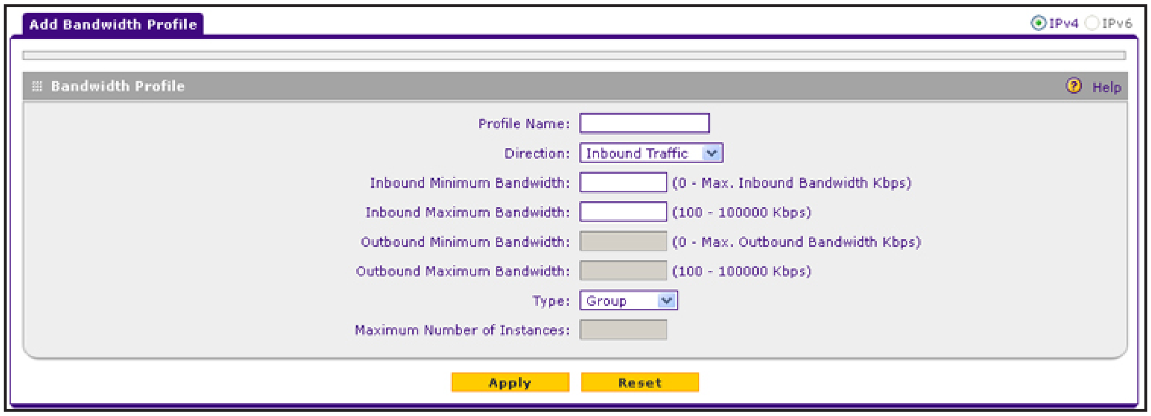
Enable Bandwidth Profiles?
● Yes
○ No

	Name	Inbound Bandwidth Range(Kbps)	Outbound Bandwidth Range(Kbps)	Type	Direction	Action
□	PriorityQueue	10000 - 100000		Individual	Inbound Traffic	Edit
□	BusinessLevel1	7500 - 25000	5000 - 10000	Group	Both	Edit

Packets Dropped due to Bandwidth Limit:

7. Under the List of Bandwidth Profiles table, click the **Add** button.

   The Add Bandwidth Profile screen displays.



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
Maximum Number of Instances:

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

Setting	Description
Profile Name	A descriptive name of the bandwidth profile for identification and management purposes.
Direction	From the **Direction** menu, select the traffic direction for the bandwidth profile: • **Inbound Traffic**. The bandwidth profile applies only to inbound traffic. Specify the inbound minimum and maximum bandwidths. • **Outbound Traffic**. The bandwidth profile applies only to outbound traffic. Specify the outbound minimum and maximum bandwidths. • **Both**. The bandwidth profile applies to both outbound and inbound traffic. Specify both the outbound and inbound minimum and maximum bandwidths.
Inbound Minimum Bandwidth	The inbound minimum allocated bandwidth in Kbps. The VPN firewall does not provide a default setting.

Setting	Description
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. The VPN firewall does not provide a default setting.
Outbound Minimum Bandwidth	The outbound minimum allocated bandwidth in Kbps. The VPN firewall does not provide a default setting.
Outbound Maximum Bandwidth	The outbound maximum allowed bandwidth in Kbps. The maximum allowable bandwidth is 100,000 Kbps and you cannot configure less than 100 Kbps. The VPN firewall does not provide a default setting.
Type	From the **Type** menu, 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. In the **Maximum Number of Instances** field, specify the maximum number of class instances.
Maximum Number of Instances	If you select **Individual** from the **Type** menu, you must specify the maximum number of class instances that can be created by the individual bandwidth profile. **Note:** If the number of users exceeds the configured number of instances, the same bandwidth is shared among all the users of that bandwidth profile.

9. Click the **Apply** button.

   Your settings are saved. The new bandwidth profile is added to the List of Bandwidth Profiles table.

10. In the Bandwidth Profiles section, select the **Yes** radio button under Enable Bandwidth Profiles?

    By default, the **No** radio button is selected.

11. Click the **Apply** button.

    Your settings are saved.

Change a Bandwidth Profile

The following procedure describes how to change an existing bandwidth profile.

➢ **To change a bandwidth profile:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > Bandwidth Profiles**.

   The Bandwidth Profiles screen displays.

7. In the List of Bandwidth Profiles table, click the **Edit** button for the bandwidth profile that you want to change.

   The Edit Bandwidth Profile screen displays.

8. Change the settings.

   For information about the settings, see *Add and Enable a Bandwidth Profile* on page 300.

9. Click the **Apply** button.

   Your settings are saved. The modified bandwidth profile displays in the List of Bandwidth Profiles table on the Bandwidth Profiles screen.

Remove One or More Bandwidth Profiles

The following procedure describes how to remove one or more bandwidth profiles that you no longer need as objects for firewall rules.

➢ **To remove one or more bandwidth profiles:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > Bandwidth Profiles**.

   The Bandwidth Profiles screen displays.

7. In the List of Bandwidth Profiles table, select the check box to the left of each bandwidth profile that you want to remove or click the **Select All** button to select all profiles.

8. Click the **Delete** button.

   The selected bandwidth profiles are removed from the List of Bandwidth Profiles table.

Protect Your Network

7

This chapter describes how to protect your network through features other than the firewall. The chapter contains the following sections:

- *Manage Content Filtering*
- *Enable Source MAC Filtering*
- *Manage IP/MAC Bindings*
- *Manage Port Triggering*
- *Enable Universal Plug and Play*

Manage Content Filtering

To restrict internal LAN users from access to certain sites on the Internet, you can use the content filtering and web component blocking features of the VPN firewall.

The following sections provide information about how to manage content filtering:

- *Content Filtering Overview*
- *Enable Content Filtering and Select Web Components*
- *Manage Keywords and Domain Names That Must Be Blocked*
- *Manage Domain Names That You Trust*
- *Manage Keyword Blocking for LAN Groups*

Content Filtering Overview

By default, content filtering and web component blocking 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.

The VPN firewall provides several types of blocking:

- **Web component blocking**. Even trusted sites 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 feature 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 feature 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 feature blocks cookies from being created by a website.

Note: Many websites require that cookies be accepted for the site to be accessed correctly. Blocking cookies might interfere with useful functions provided by these websites.

- **Keyword blocking (domain name blocking)**. You can specify up to 32 words to block. If any of these words appear in the website name (URL) or in a newsgroup name, the website or newsgroup is blocked by the VPN firewall.

  You can apply keyword blocking to one or more LAN groups. Requests from computers in groups for which keyword blocking is enabled are blocked. Blocking does not occur for computers in groups for which keyword blocking is disabled.

  If you bypass keyword blocking for trusted domains, computers in groups for which keyword blocking is enabled can access trusted domains even if the domain includes a blocked keyword.

  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.

Enable Content Filtering and Select Web Components

The following procedure describes how to enable content filtering and select web components that must be blocked, such as proxy servers, Java applets, ActiveX applets, and cookies.

➢ **To enable content filtering and select web components that must be blocked:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

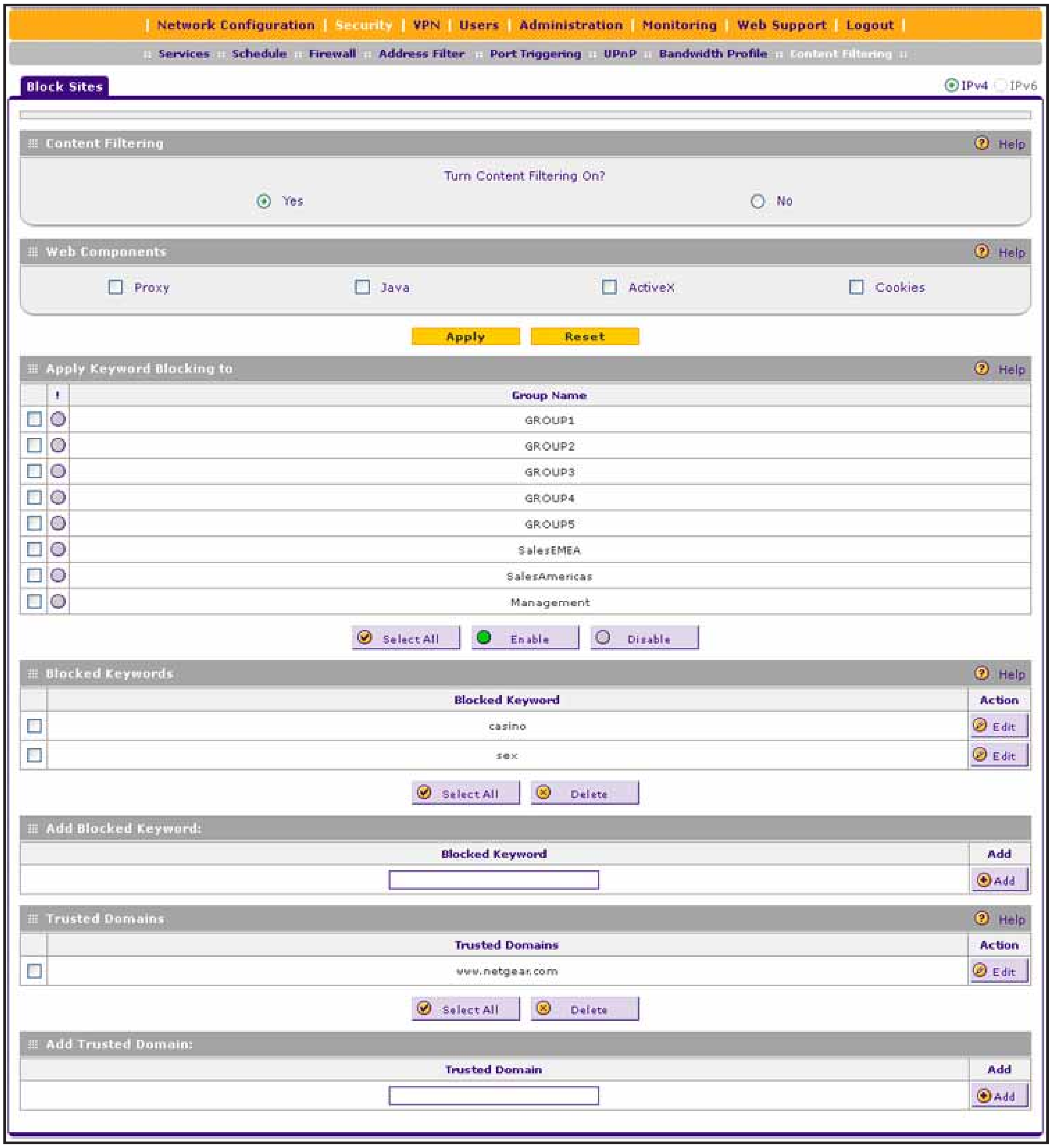
If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > Content Filtering**.

   The Block Sites screen displays. The following figure shows some examples.


| 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
□	○	SalesEMEA
□	○	SalesAmericas
□	○	Management

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

7. In the Content Filtering section, select the **Yes** radio button.

8. In the Web Components section, select the check boxes for the components that you want to block:
   - **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.

   By default, none of these components are blocked, that is, none of these check boxes are selected. For more information about these components, see *Content Filtering Overview* on page 306.

9. Click the **Apply** button.

   Your settings are saved. Content filtering and blocking of the selected web components is enabled. The screen controls are activated.

Manage Keywords and Domain Names That Must Be Blocked

You cannot manage keywords and domain names for blocking if content filtering is not enabled. Make sure that content filtering is enabled (see *Enable Content Filtering and Select Web Components* on page 307).

➢ **To manage keywords and domain names that must be blocked:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > Content Filtering**.

   The Blocked Sites screen displays.

7. To compose the list of blocked keywords and domain names, add, change, or remove keywords and domain names:
   - **Add**. To add a keyword or domain name, do the following:
     a. In the Add Blocked Keyword section, in the **Blocked Keyword** field, enter a keyword or domain name.
     b. Click the **Add** button.

        The keyword or domain name is added to the Blocked Keyword table.
   - **Change**. To change a keyword or domain name, do the following:
     a. In the Blocked Keyword table, select the keyword or domain name that you want to change.
     b. Click the associated **Edit** button.

        The Edit Blocked Keyword screen displays.
     c. Change the keyword or domain name.
     d. Click the **Apply** button.

        The changed keyword or domain name displays in the Blocked Keyword table.
   - **Remove**. To remove one or more keywords or domain names, do the following:
     a. In the Blocked Keyword table, select one or more keywords or domain names that you want to remove or click the **Select All** button to select all keywords and domain names.
     b. Click the **Delete** button.

        The selected keywords and domain names are removed from the Blocked Keyword table.

Manage Domain Names That You Trust

You cannot manage trusted domains if content filtering is not enabled. Make sure that content filtering is enabled (see *Enable Content Filtering and Select Web Components* on page 307).

➢ **To manage domains that you trust:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > Content Filtering**.

   The Blocked Sites screen displays.

7. To compose the list of trusted domain names, add, change, or remove domains:
   - **Add**. To add a trusted domain, do the following:
     a. In the Add Trusted Domain section, in the **Trusted Domains** field, enter a domain name.
     b. Click the **Add** button.

        The domain is added to the Trusted Domains table.
   - **Change**. To change a trusted domain, do the following:
     a. In the Trusted Domains table, select the domain that you want to change.
     b. Click the associated **Edit** button.

        The Edit Trusted Domains screen displays.
     c. Change the domain.
     d. Click the **Apply** button.

        The changed domain displays in the Trusted Domains table.
   - **Remove**. To remove one or more trusted domains, do the following:
     a. In the Trusted Domains table, select one or more domains that you want to remove or click the **Select All** button to select all keywords.
     b. Click the **Delete** button.

        The selected domains are removed from the Trusted Domains table.

Manage Keyword Blocking for LAN Groups

You cannot manage keyword blocking for LAN groups if content filtering is not enabled. Make sure that content filtering is enabled (see *Enable Content Filtering and Select Web Components* on page 307).

➢ **To manage keyword blocking for LAN groups:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > Content Filtering**.

   The Blocked Sites screen displays.

7. 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.

Note: If you changed the LAN group names (see *Change Group Names in the Network Database* on page 139), the new names are displayed on the Block Sites screen.

8. Activate or deactivate keyword blocking for the selected groups:
   - **Activate**. Click the **Enable** button.

     Keyword blocking is activated for the selected groups.
   - **Decativate**. Click the **Disable** button.

     Keyword blocking is deactivated for the selected groups.

Enable Source MAC Filtering

You can permit or block traffic 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 you enable the source MAC address filter, depending on the selected policy, traffic is either permitted or blocked if it comes from any computers or devices whose MAC addresses are listed in MAC Addresses table.

Note: For additional ways of restricting outbound traffic, see *Outbound Rules — Service Blocking* on page 212.

➢ **To enable MAC filtering and manage MAC addresses to be permitted or blocked:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

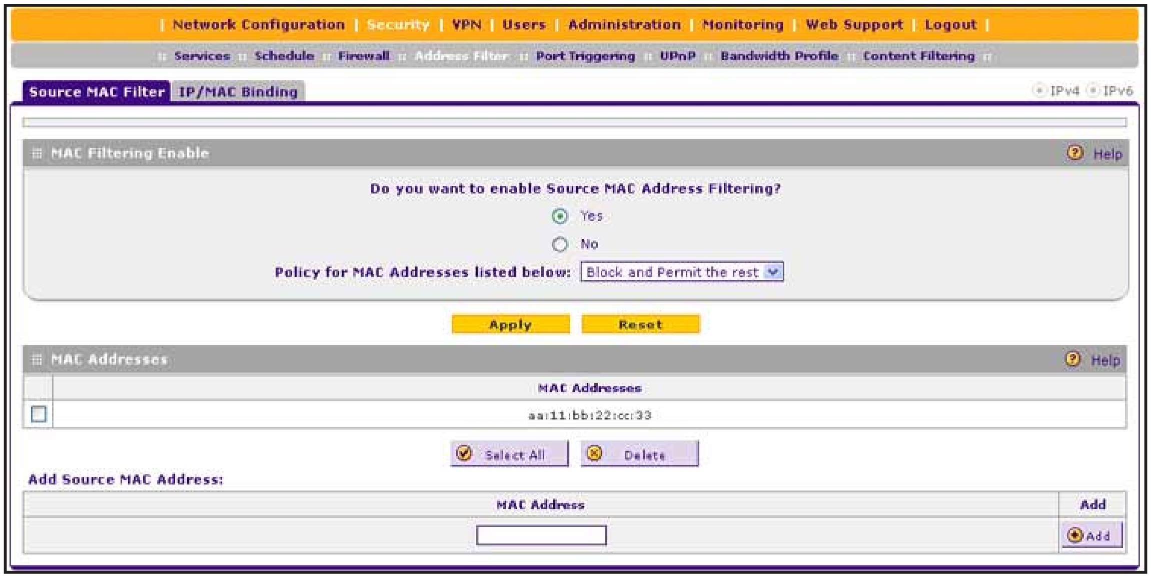
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Address Filter**.

   The Address Filter submenu tabs display, with the Source MAC Filter screen in view. The following figure shows one address in the MAC Addresses table as an example.


| 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
MAC Filtering Enable
Help
Apply
Reset
MAC Addresses
Help
Select All
Delete
Add

Do you want to enable Source MAC Address Filtering?

● Yes

○ No

Policy for MAC Addresses listed below: Block and Permit the rest

	MAC Addresses
□	aa:11:bb:22:cc:33

Add Source MAC Address:

MAC Address	Add
	Add

7. Select the **Yes** radio button.
8. From the **Policy for MAC Addresses listed below** menu, select an option:
   - **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.

9. Click the **Apply** button.

   Your settings are saved. The **MAC Address** field in the Add Source MAC Address section becomes available.

10. Build your list of source MAC addresses to be permitted or blocked:

    - To add a MAC address to the MAC Addresses table, do the following:

      a. In the **MAC Address** field, enter the MAC address.

         Enter the MAC address in the format xx:xx:xx:xx:xx:xx, in which x is a numeric (0 to 9) or a letter between a and f (inclusive), for example, aa:11:bb:22:cc:33.

WARNING:

If you select Permit and Block the rest from the menu, add the MAC address of the computer from which you are accessing the web management interface as the first MAC address in the MAC Addresses table; otherwise, you are locked out of the web management interface.

      b. Click the **Add** button.

         The MAC address is added to the MAC Addresses table.

    - To remove a MAC address form the MAC Addresses table, do the following:

      a. Select the check box to the left of each MAC address that you want to remove or click the **Select All** button to remove all MAC addresses.

      b. Click the **Delete** button.

         The selected MAC addresses are removed from the MAC Addresses table.

Manage IP/MAC Bindings

The following sections provide information about managing IP/MAC bindings:

- *IP/MAC Binding Overview*
- *Manage IP/MAC Bindings for IPv4 Traffic*
- *Manage IP/MAC Bindings for IPv6 Traffic*

IP/MAC Binding Overview

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, enable the IP/MAC binding feature. 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 enable the logging option for the IP/MAC binding feature, the VPN firewall logs these packets before they are dropped. The VPN firewall displays the total number of dropped packets that violate either the IP-to-MAC binding or the MAC-to-IP binding.

Note: You can also bind IP addresses to MAC addresses for DHCP assignment on the LAN Groups submenu. See *Manage the Network Database* on page 133.

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 possible scenarios can occur in relation to the addresses in the IP/MAC Bindings table:

- Host 1 has not changed its IP and MAC addresses. A packet coming from Host 1 has IP and MAC addresses that match those in the IP/MAC Bindings table.
- Host 2 has changed its MAC address to 00:01:02:03:04:09. The packet has an IP address that matches the IP address in the IP/MAC Bindings table but a MAC address that does not match the MAC address in the IP/MAC Bindings table.
- Host 3 has changed its IP address to 192.168.10.15. The packet has a MAC address that matches the MAC address in the IP/MAC Bindings table but an IP address that does not match the IP address in the IP/MAC Bindings table.

In this example, the VPN firewall blocks the traffic coming from Host 2 and Host 3 but allows the traffic coming from Host 1 to any external network. The total count of dropped packets is displayed.

Manage IP/MAC Bindings for IPv4 Traffic

The following sections provide information about managing IP/MAC bindings for IPv4 traffic:

- *View and Set Up an IPv4/MAC Binding*
- *Change an IPv4/MAC Binding*
- *Remove One or More IPv4/MAC Bindings*
- *Change the IP/MAC Binding Polling Interval for IPv4 Traffic and View the Number of Dropped Packets*

View and Set Up an IPv4/MAC Binding

The following procedure describes how to view existing IPv4/MAC bindings and set up a binding between a MAC address and an IPv4 address.

➢ **To view existing bindings and set up a binding between a MAC address and an IPv4 address:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

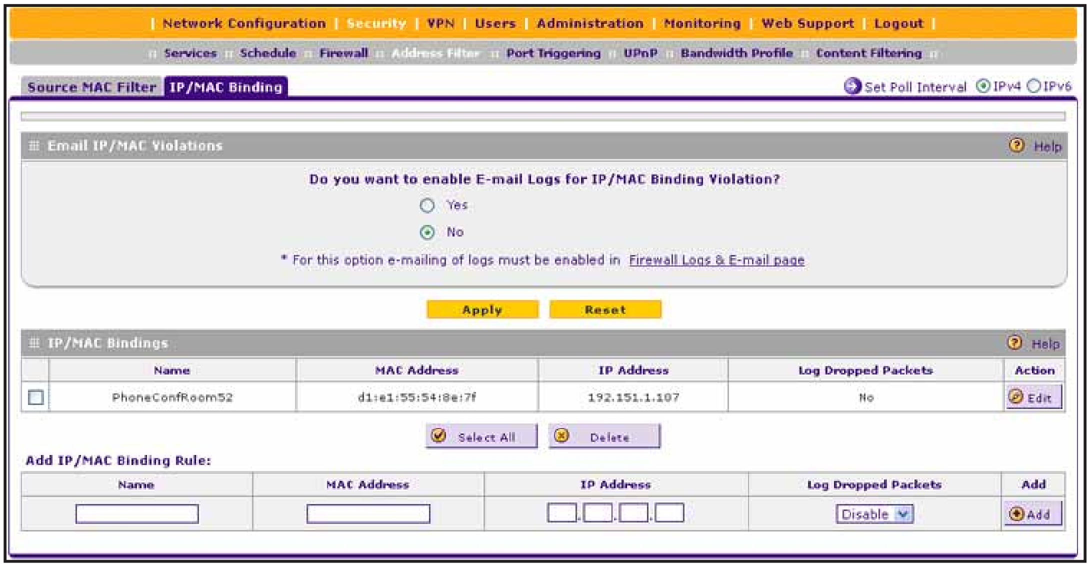
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Address Filter > IP/MAC Binding**.

   The IP/MAC Binding screen displays the IPv4 settings. The following figure shows a binding in the IP/MAC Bindings table 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 ::
Source MAC Filter
IP/MAC Binding
Set Poll Interval
Email IP/MAC Violations
Help
Apply
Reset
IP/MAC Bindings
Help
Select All
Delete

● IPv4 ○ IPv6

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
□	PhoneConfRoom52	d1:e1:55:54:8e:7f	192.151.1.107	No	Edit

Add IP/MAC Binding Rule:

Name	MAC Address	IP Address	Log Dropped Packets	Add
		. . .	Disable	Add

7. In the Email IP/MAC Violations section, specify if you want to enable email logs for IP/MAC binding violations by selecting one of the following radio buttons:
   - **Yes**. The VPN firewall does email IP/MAC binding violations.

     As an option, click the **Firewall Logs & E-mail page** link to ensure that emailing of logs is enabled (see *Enable and Schedule Emailing of Logs* on page 569).
   - **No**. The VPN firewall does not email IP/MAC binding violations.

Note: You must specify only once whether you want IP/MAC binding violations for IPv4 traffic to be logged and emailed. Your selection applies to all IPv4 IP/MAC bindings.

8. Click the **Apply** button.

   Your settings are saved.
9. In the IP/MAC Bindings sections, enter the settings as described in the following table.

Setting	Description
Name	A descriptive name of the binding for identification and management purposes.
MAC Address	The MAC address of the computer or device that is bound to the IP address.
IP Address	The IPv4 address of the computer or device that is bound to the MAC address.
Log Dropped Packets	To log the dropped packets, select **Enable** from the menu. The default setting is **Disable**.

10. Click the **Add** button.

    Your settings are saved. The new IP/MAC rule is added to the IP/MAC Bindings table.

Change an IPv4/MAC Binding

The following procedure describes how to change an existing binding between a MAC address and an IPv4 address.

➢ **To change a binding between a MAC address and an IPv4 address:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > Address Filter > IP/MAC Binding**.

   The IP/MAC Binding screen displays the IPv4 settings.

7. In the IP/MAC Bindings table, click the **Edit** button for the IP/MAC binding that you want to change.

   The Edit IP/MAC Binding screen displays.

8. Change the settings.

   You can change the MAC address, IPv4 address, and logging status. For more information about the settings, see *View and Set Up an IPv4/MAC Binding* on page 316.

9. Click the **Apply** button.

   Your settings are saved. The modified IP/MAC binding displays in the IP/MAC Bindings table on the IP/MAC Binding screen.

Remove One or More IPv4/MAC Bindings

The following procedure describes how to remove one or more bindings between MAC addresses and IPv4 addresses that you no longer need.

➢ **To remove one or more bindings between MAC addresses and IPv4 addresses:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > Address Filter > IP/MAC Binding**.

   The IP/MAC Binding screen displays the IPv4 settings.

7. In the IP/MAC Bindings table, select the check box to the left of each IP/MAC binding that you want to remove or click the **Select All** button to select all bindings.
8. Click the **Delete** button.

   The selected bindings are removed from the IP/MAC Bindings table.

Change the IP/MAC Binding Polling Interval for IPv4 Traffic and View the Number of Dropped Packets

The following procedure describes how to change the polling interval for the process that checks and enforces IP/MAC bindings for IPv4 traffic and view the number of dropped packets as a result of invalidated IP/MAC bindings.

➢ **Change the IP/MAC binding polling interval for IPv4 traffic and view the number of dropped packets:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

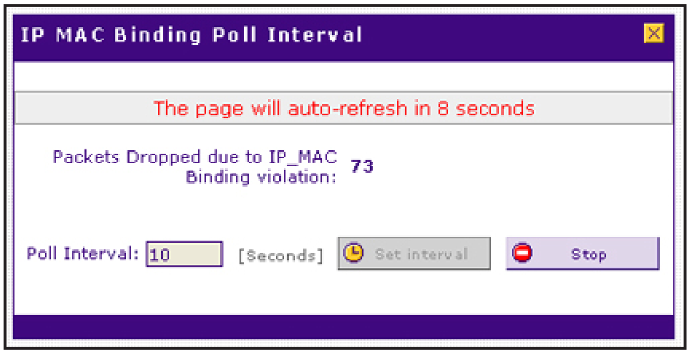
   The Router Status screen displays.

6. Select **Security > Address Filter > IP/MAC Binding**.

   The IP/MAC Binding screen displays the IPv4 settings.

7. Click the **Set Poll Interval** option arrow in the upper right.

   The IP MAC Binding Poll Interval pop-up screen displays.



The page will auto-refresh in 8 seconds

Packets Dropped due to IP_MAC Binding violation: 73

Poll Interval: 10 [Seconds]

The pop-up screen displays the dropped IPv4 packets.

8. Click the **Stop** button.
9. Wait for the confirmation that the operation succeeded.
10. In the **Poll Interval** field, enter new poll interval in seconds.
11. Click the **Set Interval** button.
12. Close the pop-up screen.

Manage IP/MAC Bindings for IPv6 Traffic

The following sections provide information about managing IP/MAC bindings for IPv6 traffic:

- *View and Set Up IPv6/MAC Bindings*
- *Change an IPv6/MAC Binding*
- *Remove One or More IPv6/MAC Bindings*
- *Change the IP/MAC Binding Polling Interval for IPv6 Traffic and View the Number of Dropped Packets*

View and Set Up IPv6/MAC Bindings

The following procedure describes how to view existing IPv6/MAC bindings and set up a binding between a MAC address and an IPv6 address.

➢ **To view existing bindings and set up a binding between a MAC address and an IPv6 address:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

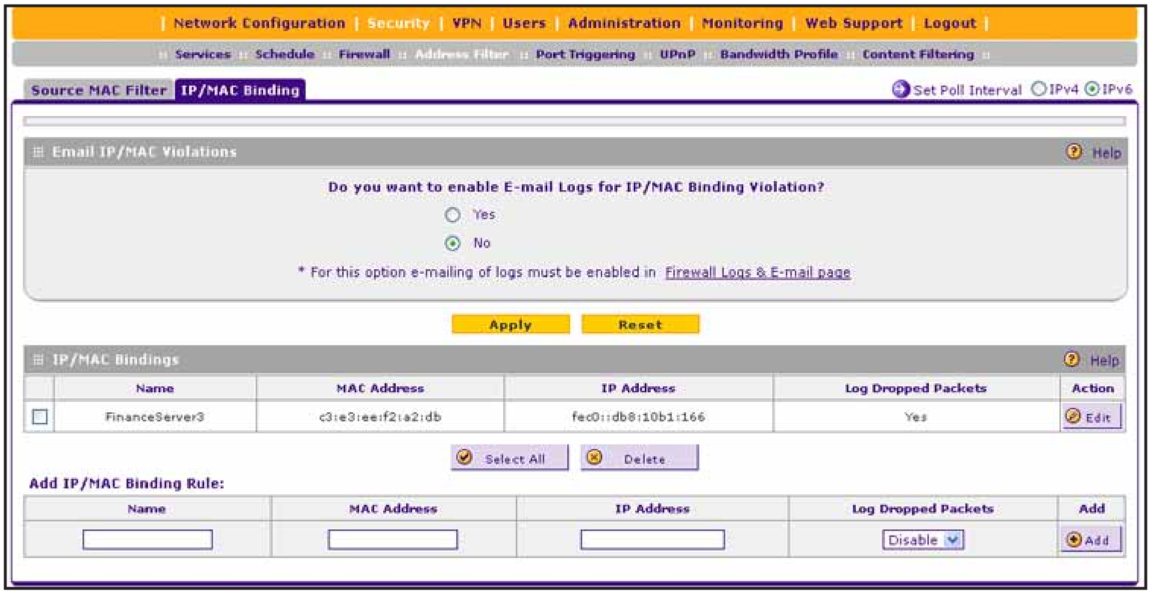
   The Router Status screen displays.

6. Select **Security > Address Filter > IP/MAC Binding**.

   The IP/MAC Binding screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The IP/MAC Binding screen displays the IPv6 settings. The following figure shows a binding in the IP/MAC Binding table as an example.



○ IPv4 ● IPv6

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
□	FinanceServer3	c3:e3:ee:f2:a2:db	fec0::db8:10b1:166	Yes	Edit

Add IP/MAC Binding Rule:

Name	MAC Address	IP Address	Log Dropped Packets	Add
			Disable	Add

8. In the Email IP/MAC Violations section, specify if you want to enable email logs for IP/MAC binding violations by selecting one of the following radio buttons:
   - **Yes**. The VPN firewall does email IP/MAC binding violations.

     As an option, click the **Firewall Logs & E-mail page** link to ensure that emailing of logs is enabled (see *Enable and Schedule Emailing of Logs* on page 569).
   - **No**. The VPN firewall does not email IP/MAC binding violations.

Note: You must specify only once whether you want IP/MAC binding violations for IPv6 traffic to be logged and emailed. Your selection applies to all IPv6 IP/MAC bindings.

9. Click the **Apply** button.

   Your settings are saved.

10. In the IP/MAC Bindings section, enter the settings as described in the following table.

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 menu. The default setting is **Disable**.

11. Click the **Add** button.

    The new IP/MAC rule is added to the IP/MAC Bindings table.

Change an IPv6/MAC Binding

The following procedure describes how to change an existing binding between a MAC address and an IPv6 address.

➢ **To change a binding between a MAC address and an IPv6 address:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

The Router Status screen displays.

6. Select **Security > Address Filter > IP/MAC Binding**.

   The IP/MAC Binding screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The IP/MAC Binding screen displays the IPv6 settings.

8. In the IP/MAC Bindings table, click the **Edit** button for the IP/MAC binding that you want to change.

   The Edit IP/MAC Binding screen displays.

9. Change the settings.

   You can change the MAC address, IPv6 address, and logging status. For more information about the settings, see *View and Set Up IPv6/MAC Bindings* on page 320.

10. Click the **Apply** button.

    Your settings are saved. The modified IP/MAC binding displays in the IP/MAC Bindings table on the IP/MAC Binding screen.

Remove One or More IPv6/MAC Bindings

The following procedure describes how to remove one or more bindings between MAC addresses and IPv6 addresses that you no longer need.

➢ **To remove a binding between a MAC address and an IPv6 address:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > Address Filter > IP/MAC Binding**.

   The IP/MAC Binding screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The IP/MAC Binding screen displays the IPv6 settings.

8. In the IP/MAC Bindings table, select the check box to the left of each IP/MAC binding that you want to remove or click the **Select All** button to select all bindings.
9. Click the **Delete** button.

   The selected bindings are removed from the IP/MAC Bindings table.

Change the IP/MAC Binding Polling Interval for IPv6 Traffic and View the Number of Dropped Packets

The following procedure describes how to change the polling interval for the process that checks and enforces IP/MAC bindings for IPv6 traffic and view the number of dropped packets as a result of invalidated IP/MAC bindings.

➢ **To change the IP/MAC binding polling interval for IPv6 traffic and view the number of dropped packets:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > Address Filter > IP/MAC Binding**.

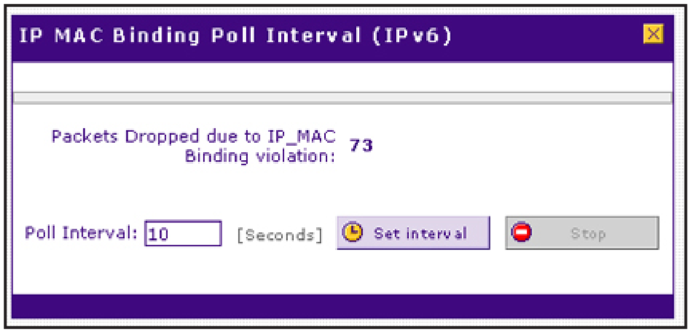
   The IP/MAC Binding screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The IP/MAC Binding screen displays the IPv6 settings.

8. Click the **Set Poll Interval** option arrow in the upper right.

   The IP MAC Binding Poll Interval (IPv6) pop-up screen displays.



IP MAC Binding Poll Interval (IPv6)
Packets Dropped due to IP_MAC Binding violation: 73
Poll Interval: 10 [Seconds]
Set interval
Stop

The pop-up screen displays the dropped IPv6 packets.

9. Click the **Stop** button.
10. Wait for the confirmation that the operation succeeded.
11. In the **Poll Interval** field, enter new poll interval in seconds.
12. Click the **Set Interval** button.
13. Close the pop-up screen.

Manage Port Triggering

The following sections provide information about managing port triggering:

- *Port Triggering Overview*
- *Add a Port Triggering Rule*
- *Change a Port Triggering Rule*
- *Remove One or More Port Triggering Rules*
- *Display the Status of Active Port Triggering Rules*

Port Triggering Overview

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 that the application uses.

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 you defined for port triggering.
2. The VPN firewall records this connection, opens the additional incoming port or ports that are associated with the port triggering rule, 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 port triggering rule 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 about port triggering:

- Only one computer can use a port triggering application at any time.
- After a computer has finished using a port triggering application, there is a short time-out period before the application can be used by another computer. This time-out period is required so that the VPN firewall can determine that the application has terminated.

Note: For additional ways of allowing inbound traffic, see *Inbound Rules — Port Forwarding* on page 215.

Add a Port Triggering Rule

The following procedure describes how to add a port triggering rule.

➢ **To add a port triggering rule:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

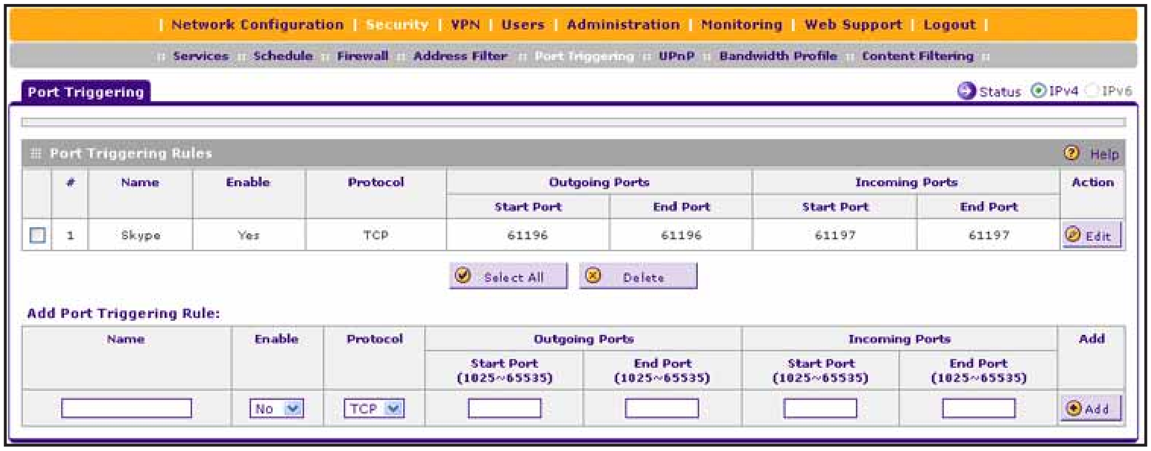
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Port Triggering**.

The Port Triggering screen displays. The following figure shows a rule in the Port Triggering Rules table 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 ::
Port Triggering
Status ● IPv4 ○ IPv6
Port Triggering Rules
Help
Select All
Delete
Add Port Triggering Rule:

	#	Name	Enable	Protocol	Outgoing Ports		Incoming Ports		Action
					Start Port	End Port	Start Port	End Port	
□	1	Skype	Yes	TCP	61196	61196	61197	61197	Edit

Name	Enable	Protocol	Outgoing Ports		Incoming Ports		Add
			Start Port (1025~65535)	End Port (1025~65535)	Start Port (1025~65535)	End Port (1025~65535)	
	No	TCP					Add

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

Setting	Description
Name	A descriptive name of the rule for identification and management purposes.
Enable	From the menu, select **Yes** to enable the rule. You can define a rule but keep it disabled it by selecting **No** from the menu.
Protocol	From the menu, select the protocol to which the rule applies: • **TCP**. The rule applies to an application that uses the Transmission Control Protocol (TCP). • **UDP**. The rule applies to an application that uses the User Datagram Protocol (UDP).
Outgoing Ports	Specify the outgoing ports: • **Start Port**. The start port (1025–65535) of the range for triggering. • **End Port**. The end port (1025–65535) of the range for triggering.
Incoming Ports	Specify the incoming ports: • **Start Port**. The start port (1025–65535) of the range for triggering. • **End Port**. The end port (1025–65535) of the range for triggering.

8. Click the **Add** button.

   Your settings are saved and the new port triggering rule is added to the Port Triggering Rules table.

Change a Port Triggering Rule

The following procedure describes how to change an existing port triggering rule.

➢ **To change a port triggering rule:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Port Triggering**.

   The Port Triggering screen displays.
7. In the Port Triggering Rules table, click the **Edit** button for the port triggering rule that you want to change.

   The Edit Port Triggering Rule screen displays.
8. Change the settings.

   For information about the settings, see *Add a Port Triggering Rule* on page 326.
9. Click the **Apply** button.

   Your settings are saved. The modified port triggering rule displays in the Port Triggering Rules table on the Port Triggering screen.

Remove One or More Port Triggering Rules

The following procedure describes how to remove one or more port triggering rules that you no longer need.

➢ **To remove one or more port triggering rules:**

1. On your computer, launch an Internet browser.

2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > Port Triggering**.

   The Port Triggering screen displays.

7. In the Port Triggering Rules table, select the check box to the left of each port triggering rule that you want to remove or click the **Select All** button to select all rules.
8. Click the **Delete** button.

   The selected rules are removed from the Port Triggering Rules table.

Display the Status of Active Port Triggering Rules

The following procedure describes how to display the status of active port triggering rules, including the rule number, LAN IP address, open ports, and the time that the ports remain open.

➢ **To display the status of active port triggering rules:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

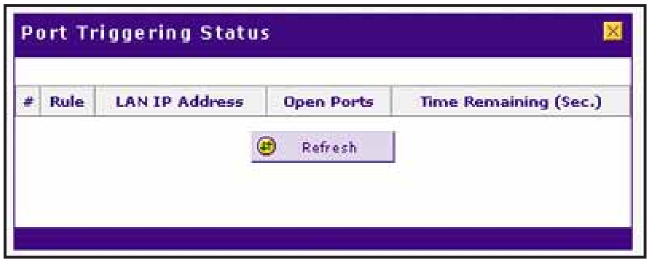
   The Router Status screen displays.

6. Select **Security > Port Triggering**.

   The Port Triggering screen displays.

7. Click the **Status** option arrow in the upper right.

   The Port Triggering Status pop-up screen displays.



Port Triggering Status

#	Rule	LAN IP Address	Open Ports	Time Remaining (Sec.)

The pop-up screen displays the status of the port triggering rules.

Enable Universal Plug and Play

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

Note: UPnP is supported for IPv4 devices only and is disabled by default.

➢ **To enable UPnP:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

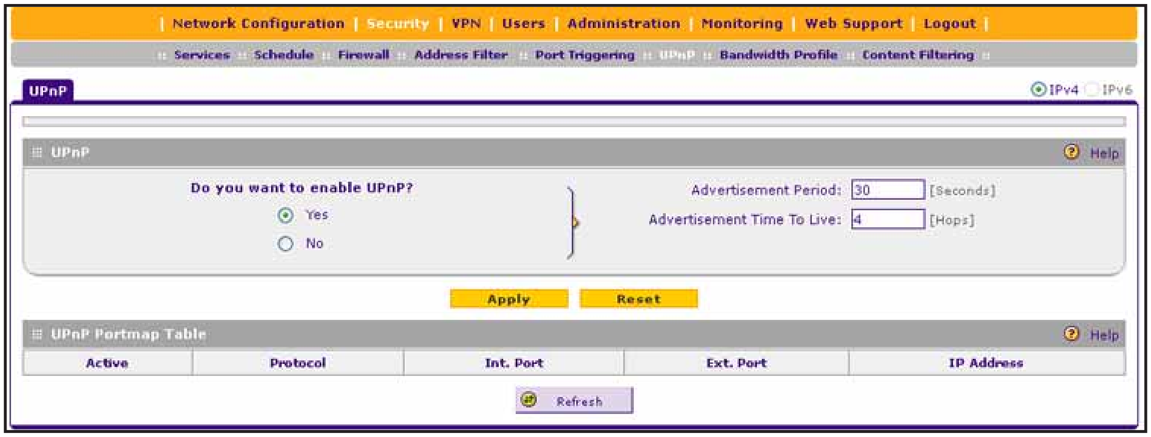
If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Security > UPnP**.

   The UPnP screen displays.


| 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
Apply
Reset
:: UPnP Portmap Table
Help
Refresh

Do you want to enable UPnP?

● Yes

○ No

Advertisement Period: 30 [Seconds]

Advertisement Time To Live: 4 [Hops]

Active	Protocol	Int. Port	Ext. Port	IP Address

The UPnP Portmap Table 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.
- **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.

7. To enable the UPnP feature, select the **Yes** radio button.

   By default, the **No** radio button is selected and the feature is disabled.

8. Complete the following fields:
   - **Advertisement Period**. Enter the period in seconds that specifies how often the VPN firewall must broadcast its UPnP information to all devices within its range. The default setting is 30 seconds.
   - **Advertisement Time to Live**. Enter a number that specifies how many steps (hops) each UPnP packet is allowed to propagate before being discarded. Small values limit the UPnP broadcast range. The default setting is 4 hops.

9. Click the **Apply** button.

   Your settings are saved.

Click the **Refresh** button. The content of the UPnP Portmap Table refreshes. Any UPnP devices that accessed the VPN firewall and that were automatically detected by the VPN firewall display in the UPnP Portmap Table.

Set Up Virtual Private Networking With IPSec Connections

8

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:

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

Dual WAN Port Systems

If two WAN ports are configured for either IPv4 or IPv6, you can enable either auto-rollover mode for increased system reliability or load balancing mode for optimum bandwidth efficiency. The selection of the WAN mode determines how you must configure the VPN features.

If the WAN ports function in auto-rollover mode, you must use fully qualified domain names (FQDNs) in VPN policies. FQDNs are also required for VPN tunnel failover. If the WAN ports function in load balancing mode, you cannot configure VPN tunnel failover. In load balancing mode, FQDNs are optional if the WAN IP addresses are static but mandatory if the WAN IP addresses are dynamic.

For more information about the IP addressing requirements for VPNs in the dual WAN modes, see *Planning for Virtual Private Networks* on page 632.

For information about how to select and configure a Dynamic DNS service for resolving FQDNs, see *Manage Dynamic DNS Connections* on page 63.

For information about configuring auto-rollover and load balancing, see the following sections:

- *Configure Load Balancing or Auto-Rollover for IPv4 Interfaces* on page 48
- *Configure Auto-Rollover for IPv6 Interfaces* on page 109 (load balancing is not supported for IPv6 interfaces)

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

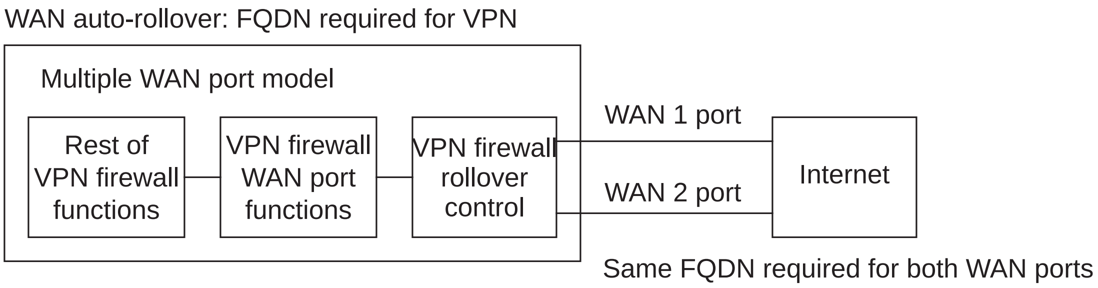

WAN auto-rollover: FQDN required for VPN
Multiple WAN port model
Rest of VPN firewall functions
VPN firewall WAN port functions
VPN firewall rollover control
WAN 1 port
WAN 2 port
Internet
Same FQDN required for both WAN ports

Figure 6. WAN auto-rollover: FQDN required for VPN

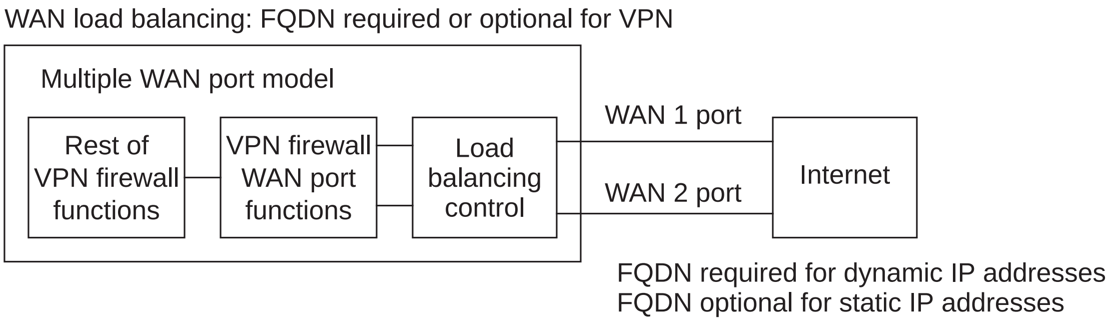

WAN load balancing: FQDN required or optional for VPN
Multiple WAN port model
Rest of VPN firewall functions
VPN firewall WAN port functions
Load balancing control
WAN 1 port
WAN 2 port
Internet
FQDN required for dynamic IP addresses
FQDN optional for static IP addresses

Figure 7. WAN load balancing: FQDN required or optional for VPN

The following table summarizes the WAN addressing requirements (FQDN or IP address) for a VPN tunnel in either dual WAN mode.

Table 7. IP addressing for VPNs in dual WAN port systems

Configuration and WAN IP Address		Rollover Mode[a]	Load Balancing Mode
VPN Telecommuter (client to gateway)	Fixed	FQDN required	FQDN allowed (optional)
	Dynamic	FQDN required	FQDN required
VPN Gateway-to-Gateway (gateway to gateway)	Fixed	FQDN required	FQDN allowed (optional)
	Dynamic	FQDN required	FQDN required
VPN Telecommuter (client to gateway through a NAT router)	Fixed	FQDN required	FQDN allowed (optional)
	Dynamic	FQDN required	FQDN required

[a] After a rollover, all tunnels must be reestablished using the new WAN IP address.

Use the IPSec VPN Wizard for Client and Gateway Configurations

You can use the IPSec VPN Wizard to configure multiple gateway or client VPN tunnel policies.

The following sections provide information about how to create IPSec VPN connections with the IPSec VPN Wizard and NETGEAR ProSAFE VPN Client software:

- *IPSec VPN Wizard Overview*
- *View the IPSec VPN Wizard Default Values*
- *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*

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.

IPSec VPN Wizard Overview

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.

Tip: To ensure that VPN tunnels stay active, after completing the wizard, manually change the VPN policy to enable keep-alives. The VPN firewall 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 412.

Tip: For DHCP WAN configurations, first set up the tunnel with IP addresses. After you validate the connection, you can use the wizard to create new policies using the FQDN for the WAN addresses.

View the IPSec VPN Wizard Default Values

The IPSec VPN Wizard default values are the settings that the IPSec VPN Wizard uses when you set up a VPN connection. Except for the local WAN ID and remote WAN ID, you cannot change the default settings when you use the IPSec VPN Wizard. However, these values work for most configurations.

If you must use other values, configure the IPSec VPN connection manually (see *Manage IPSec VPN Policies Manually* on page 365).

In such a situation, you can also first configure the IPSec VPN connection with the IPSec VPN Wizard and the default values. The IPSec VPN Wizard generates a VPN policy and an IKE policy automatically. Then, you can adjust the VPN policy, IKE policy, or both with your custom values.

➢ **To view the IPSec VPN Wizard default values:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

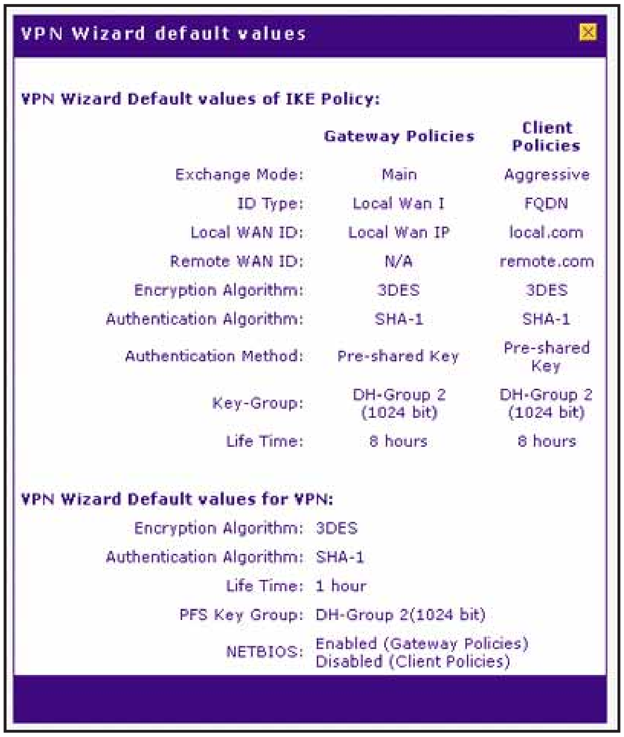
The Router Status screen displays.

6. Select **VPN > IPSec VPN > VPN Wizard**.

   The VPN Wizard screen displays the IPv4 settings.

7. Click the **VPN Wizard default values** option arrow in the upper right.

   The VPN Wizard default values pop-up screen displays. The default values are the same for IPv4 and IPv6.



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)

Create an IPv4 Gateway-to-Gateway VPN Tunnel with the Wizard

The following figure shows an example of an IPv4 gateway-to-gateway IPSec VPN connection and the following procedure describes how to set up an IPv4 gateway-to-gateway VPN tunnel using the VPN Wizard.

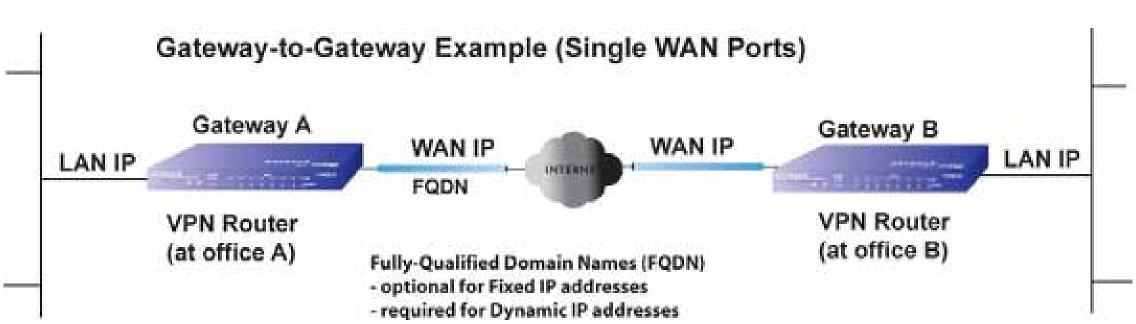

Gateway-to-Gateway Example (Single WAN Ports)
LAN IP
Gateway A
VPN Router
(at office A)
WAN IP
FQDN
INTERNET
WAN IP
Gateway B
VPN Router
(at office B)
LAN IP
Fully-Qualified Domain Names (FQDN)
- optional for Fixed IP addresses
- required for Dynamic IP addresses

Figure 8. Example of an IPv4 gateway-to-gateway IPSec VPN connection

➢ **To set up an IPv4 gateway-to-gateway VPN tunnel using the VPN Wizard:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

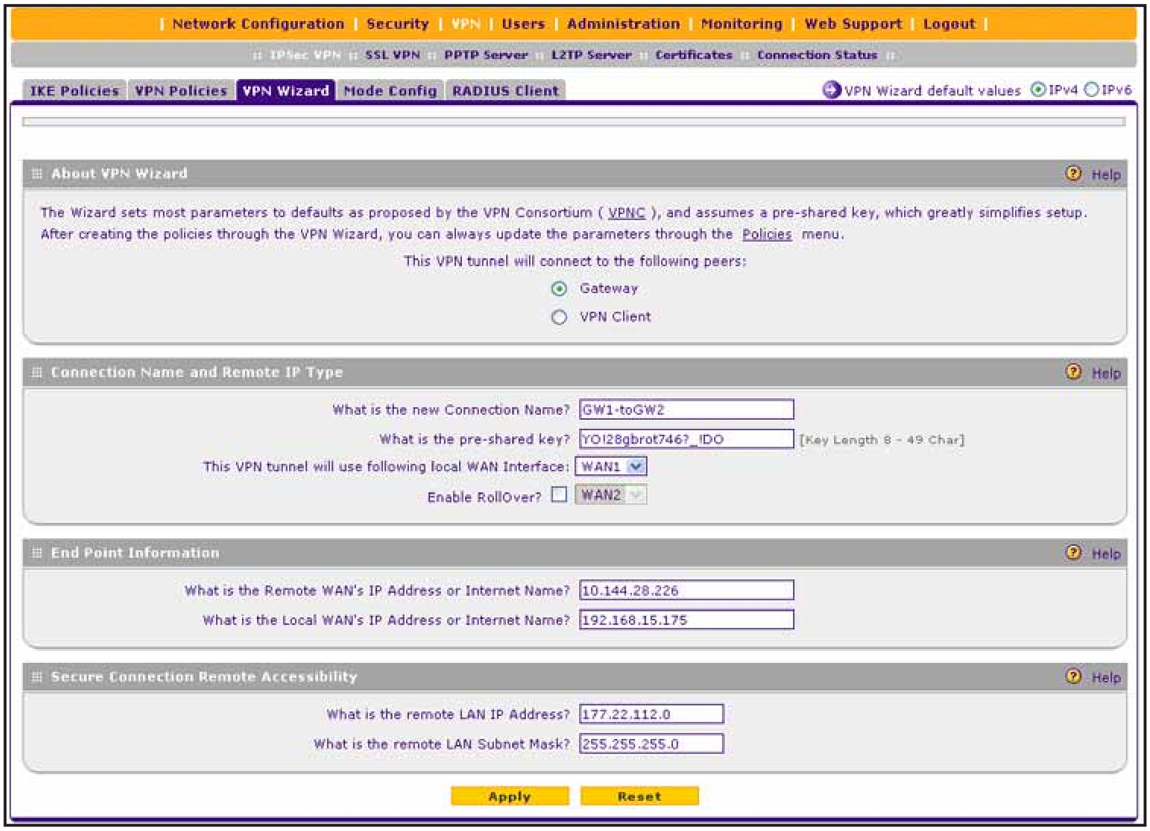
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > IPSec VPN > VPN Wizard**.

   The VPN Wizard screen displays the IPv4 settings. The following figure shows an example that does not relate to other examples in this manual.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: 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? GW1-toGW2

What is the pre-shared key? YO!28gbrot746?_!DO [Key Length 8 - 49 Char]

This VPN tunnel will use following local WAN Interface: WAN1

Enable RollOver? □ WAN2

End Point Information

What is the Remote WAN's IP Address or Internet Name? 10.144.28.226

What is the Local WAN's IP Address or Internet Name? 192.168.15.175

Secure Connection Remote Accessibility

What is the remote LAN IP Address? 177.22.112.0

What is the remote LAN Subnet Mask? 255.255.255.0

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

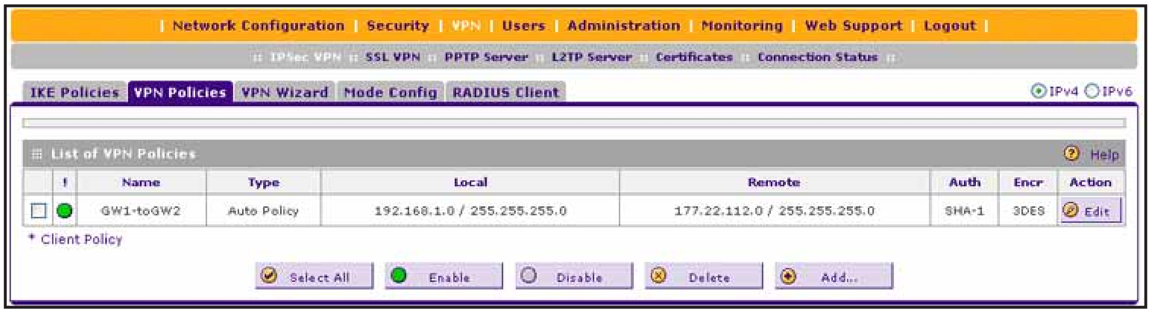
Setting	Description
About VPN Wizard	
This VPN tunnel will connect to the following peers	Select the **Gateway** radio button. The local WAN port’s IP address or Internet name displays in the End Point Information section.
Connection Name and Remote IP Type	
What is the new Connection Name?	Enter a descriptive name for the connection. This name helps 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. This key must also be entered on the remote VPN gateway. The key must have a minimum length of 8 characters and must not exceed 49 characters.

Setting	Description
This VPN tunnel will use the following local WAN Interface	Select a WAN interface from the menu. The VPN tunnel uses the WAN interface as the local endpoint.
	To enable VPN rollover, select the **Enable RollOver?** check box. The menu to the right of the check box automatically selects the WAN interface that is available for rollover. Configuring VPN rollover is optional. With VPN rollover, if the WAN interface that functions as the local endpoint goes down, the VPN tunnel is reestablished on the other WAN interface. **Note:** If the VPN firewall is configured to function in WAN auto-rollover mode, you can use the VPN Wizard to configure VPN rollover and do not need to configure VPN rollover manually.
End Point Information[a]	
What is the Remote WAN’s IP Address or Internet Name?	Enter the IPv4 address or Internet name (FQDN) of the WAN interface on the remote VPN tunnel endpoint.
What is the Local WAN’s IP Address or Internet Name?	When you select the **Gateway** radio button in the About VPN Wizard section, the IPv4 address of the VPN firewall’s active WAN interface is automatically entered and you do not need to enter it manually.
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. The VPN firewall does not support a combination of an IP address and an FQDN.*

8. Click the **Apply** button.

   Your settings are saved. The VPN Policies screen displays the IPv4 settings with the new, automatically generated VPN policy in the List of VPN Policies table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
◉ IPv4 ○ IPv6
Help
Select All
Enable
Disable
Delete
Add...

List of VPN Policies

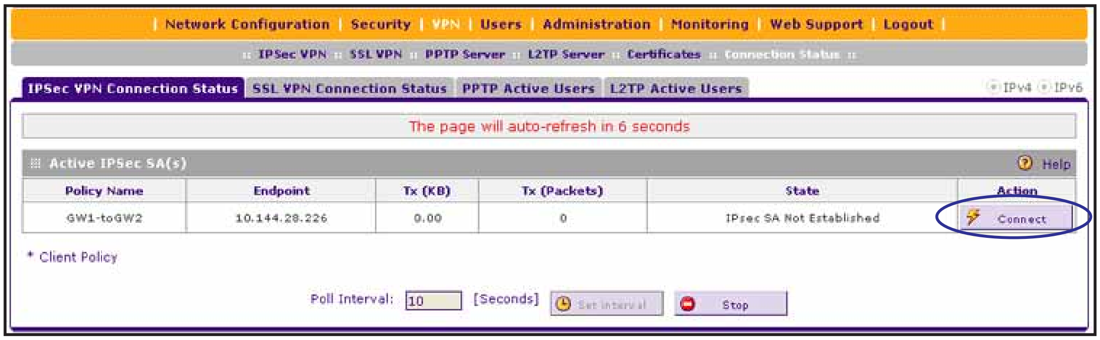
	!	Name	Type	Local	Remote	Auth	Encr	Action
□	●	GW1-toGW2	Auto Policy	192.168.1.0 / 255.255.255.0	177.22.112.0 / 255.255.255.0	SHA-1	3DES	Edit

* Client Policy

9. On the remote gateway, configure a VPN policy that allows connection to the VPN firewall.

The configuration steps depend on the remote gateway.

10. On the VPN firewall, activate the IPSec VPN connection:
    a. Select **VPN > Connection Status**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
IPSec VPN Connection Status
SSL VPN Connection Status
PPTP Active Users
L2TP Active Users
○ IPv4 ○ IPv6

The page will auto-refresh in 6 seconds

Active IPSec SA(s)

Policy Name	Endpoint	Tx (KB)	Tx (Packets)	State	Action
GW1-toGW2	10.144.28.226	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** button.

    The IPSec VPN connection becomes active.

Note: If you use an FQDN as the tunnel endpoint address on the VPN firewall, if the Dynamic DNS service is slow to update its servers when your DHCP WAN address changes, the VPN tunnel fails because the FQDN does not resolve to your new address. If you have the option to configure the update interval for the Dynamic DNS service, set it to an appropriately short time.

Create an IPv6 Gateway-to-Gateway VPN Tunnel with the Wizard

The following figure shows an example of an IPv6 gateway-to-gateway IPSec VPN connection and the following procedure describes how to set up an IPv6 gateway-to-gateway VPN tunnel using the VPN Wizard.

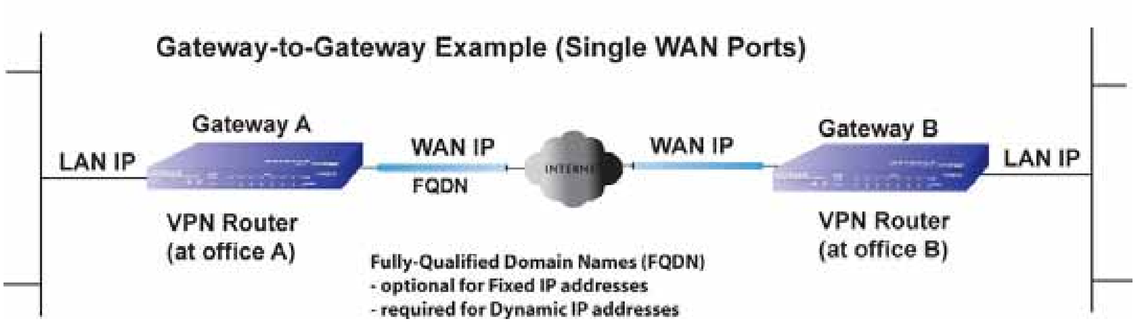

Gateway-to-Gateway Example (Single WAN Ports)
Gateway A
LAN IP
WAN IP
FQDN
INTERNET
WAN IP
Gateway B
LAN IP
VPN Router
(at office A)
VPN Router
(at office B)
Fully-Qualified Domain Names (FQDN)
- optional for Fixed IP addresses
- required for Dynamic IP addresses

Figure 9. Example of an IPv6 gateway-to-gateway IPSec VPN connection

➢ **To set up an IPv6 gateway-to-gateway VPN tunnel using the VPN Wizard:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

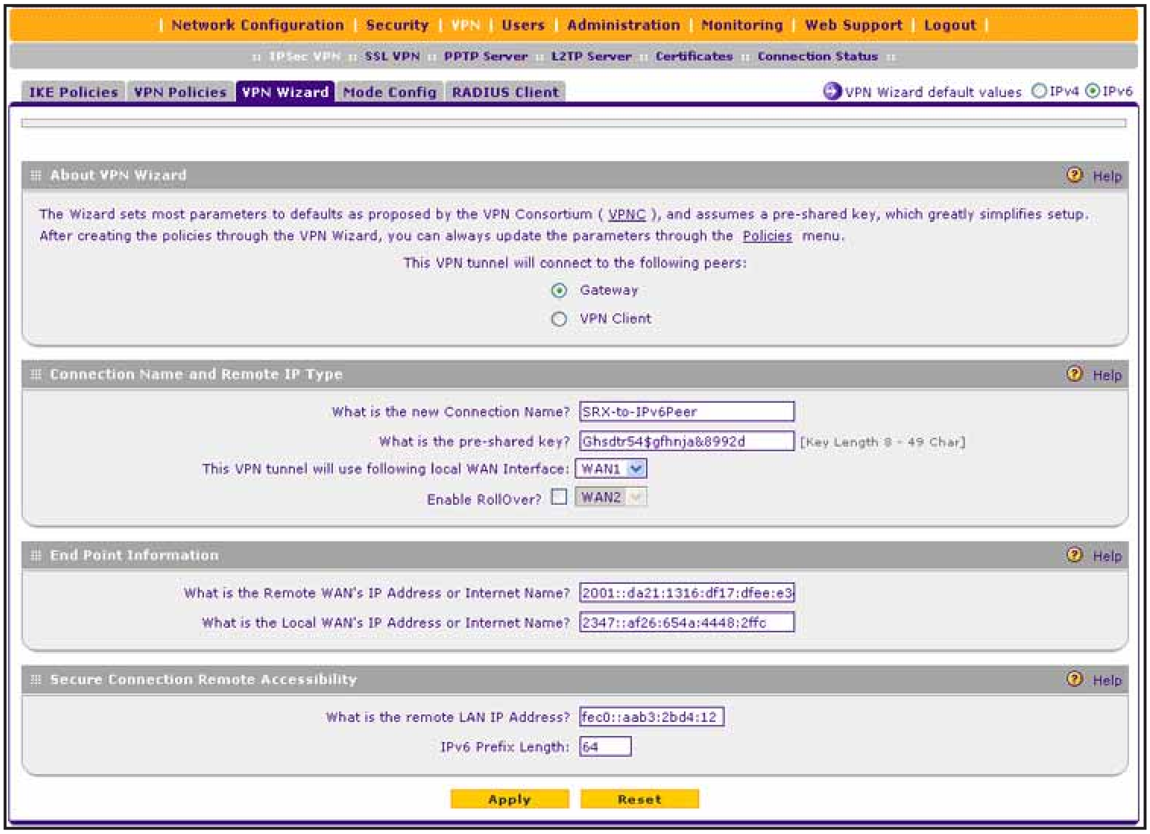
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > IPSec VPN > VPN Wizard**.

   The VPN Wizard screen displays the IPv4 settings.
7. In the upper right, select the **IPv6** radio button.

   The VPN Wizard screen displays the IPv6 settings. The following figure shows an example that does not relate to other examples in this manual.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
Help
Apply
Reset

VPN Wizard default values ○ 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? SRX-to-IPv6Peer

What is the pre-shared key? Ghsdtr54$gfhnja&8992d [Key Length 8 - 49 Char]

This VPN tunnel will use following local WAN Interface: WAN1

Enable RollOver? □ WAN2

End Point Information

What is the Remote WAN's IP Address or Internet Name? 2001::da21:1316:df17:dfee:e3

What is the Local WAN's IP Address or Internet Name? 2347::af26:654a:4448:2ffc

Secure Connection Remote Accessibility

What is the remote LAN IP Address? fec0::aab3:2bd4:12

IPv6 Prefix Length: 64

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

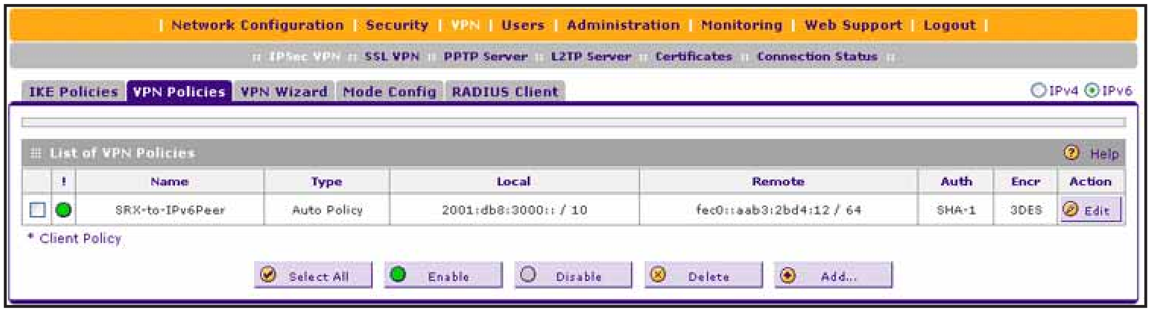
Setting	Description
About VPN Wizard	
This VPN tunnel will connect to the following peers	Select the **Gateway** radio button. The local WAN port’s IP address or Internet name displays in the End Point Information section.
Connection Name and Remote IP Type	
What is the new Connection Name?	Enter a descriptive name for the connection. This name helps 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. This key must also be entered on the remote VPN gateway. The key must have a minimum length of 8 characters and must not exceed 49 characters.

Setting	Description
This VPN tunnel will use the following local WAN Interface	Select a WAN interface from the menu. The VPN tunnel uses the WAN interface as the local endpoint.
	To enable VPN rollover, select the **Enable RollOver?** check box. The menu to the right of the check box automatically selects the WAN interface that is available for rollover. Configuring VPN rollover is optional. With VPN rollover, if the WAN interface that functions as the local endpoint goes down, the VPN tunnel is reestablished on the other WAN interface. **Note:** If the VPN firewall is configured to function in WAN auto-rollover mode, you can use the VPN Wizard to configure VPN rollover and do not need to configure VPN rollover manually.
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 and you do not need to enter it manually.
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. The VPN firewall does not support a combination of an IP address and an FQDN.

9. Click the **Apply** button.

   Your settings are saved. The VPN Policies screen displays the IPv6 settings with the new, automatically generated VPN policy in the List of VPN Policies table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
○ IPv4 ● IPv6
Help
* Client Policy
Select All
Enable
Disable
Delete
Add...

List of VPN Policies

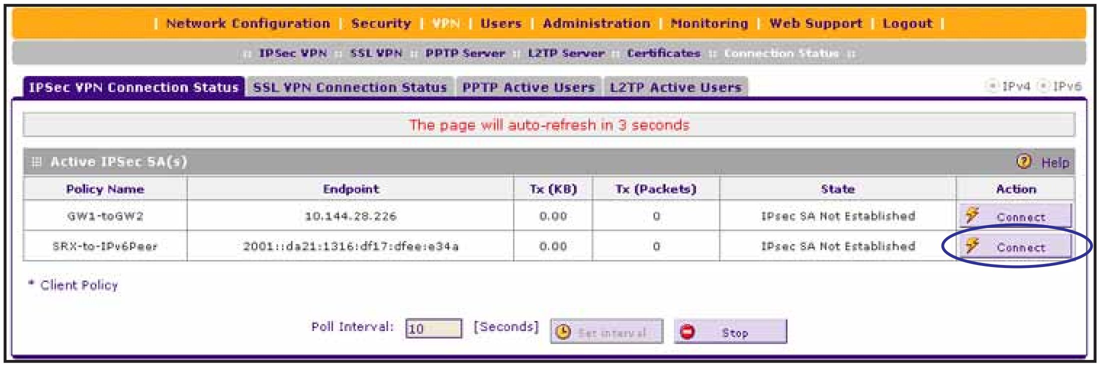
	!	Name	Type	Local	Remote	Auth	Encr	Action
□	●	SRX-to-IPv6Peer	Auto Policy	2001:db8:3000:: / 10	fec0::aab3:2bd4:12 / 64	SHA-1	3DES	Edit

10. On the remote gateway, configure a VPN policy that allows connection to the VPN firewall.

    The configuration steps depend on the remote gateway.

11. On the VPN firewall, activate the IPSec VPN connection:

    a. Select **VPN > Connection Status**.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
IPSec VPN Connection Status
SSL VPN Connection Status
PPTP Active Users
L2TP Active Users
○ IPv4 ○ IPv6
Help
Set interval
Stop

The page will auto-refresh in 3 seconds

Active IPSec SA(s)

Policy Name	Endpoint	Tx (KB)	Tx (Packets)	State	Action
GW1-toGW2	10.144.28.226	0.00	0	IPsec SA Not Established	Connect
SRX-to-IPv6Peer	2001::da21:1316:df17:dfee:e34a	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** button.

    The IPSec VPN connection becomes active.

Note: If you use an FQDN as the tunnel endpoint address on the VPN firewall, if the Dynamic DNS service is slow to update its servers when your DHCP WAN address changes, the VPN tunnel fails because the FQDN does not resolve to your new address. If you have the option to configure the update interval for the Dynamic DNS service, set it to an appropriately short time.

Create an IPv4 Client-to-Gateway VPN Tunnel with the Wizard

The following sections provide information about creating an IPv4 client-to-gateway VPN tunnel with the VPN Wizard:

- *Client-to-Gateway Tunnels*
- *Use the VPN Wizard to Configure the Gateway for a Client Tunnel*
- *Use the NETGEAR ProSAFE VPN Client Wizard to Create a Secure Connection to the VPN Firewall*
- *Manually Create a Secure Connection to the VPN Firewall Using the NETGEAR ProSAFE VPN Client*

Client-to-Gateway Tunnels

The following figure shows an example of an IPv4 client-to-gateway IPSec VPN connection.

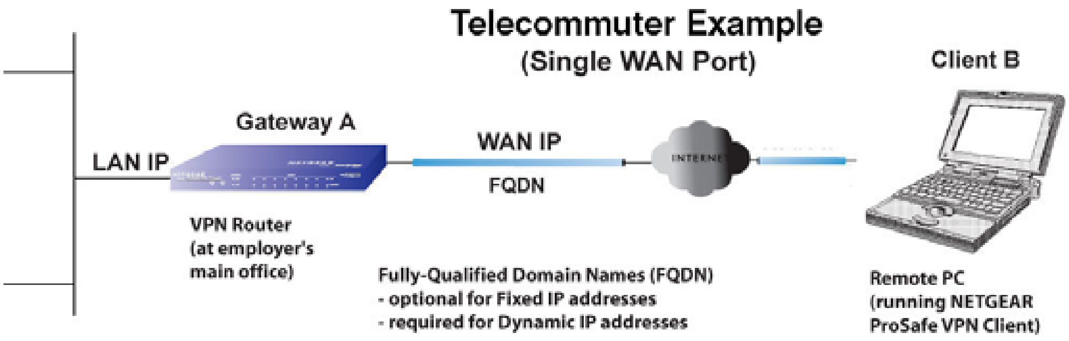


Figure 10. Example of an IPv4 client-to-gateway IPSec VPN connection

The VPN firewall supports client connections with the NETGEAR ProSAFE VPN Client, which is an application that you can install on a computer.

The VPN firewall is bundled with a single-user license of the NETGEAR ProSAFE VPN Client software (VPN01L). For information about the NETGEAR ProSAFE VPN Client, including information about multi-user licenses, visit *http://www.netgear.com/business/products/security/vpn-software.aspx*.

Note: The NETGEAR ProSAFE VPN Client supports IPv4 only; a future release of the VPN Client might support IPv6.

Setting up an IPv4 client-to-gateway connection includes two tasks:

1. On the VPN firewall, use the IPSec VPN Wizard to set up a connection to the client (see *Use the VPN Wizard to Configure the Gateway for a Client Tunnel* on page 345).
2. On the computer that has the VPN ProSAFE Client installed, set up a connection to the VPN firewall. You can use one of two methods, which are described in the following sections:
   - *Use the NETGEAR ProSAFE VPN Client Wizard to Create a Secure Connection to the VPN Firewall* on page 349
   - *Manually Create a Secure Connection to the VPN Firewall Using the NETGEAR ProSAFE VPN Client* on page 354

Use the VPN Wizard to Configure the Gateway for a Client Tunnel

The following procedure describes how to set up thew VPN firewall for a client-to-gateway VPN tunnel using the VPN Wizard.

Note: In this section, the NETGEAR ProSAFE VPN Client is referred to as the VPN client.

➢ **To set up the VPN firewall for a client-to-gateway VPN tunnel using the VPN Wizard:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

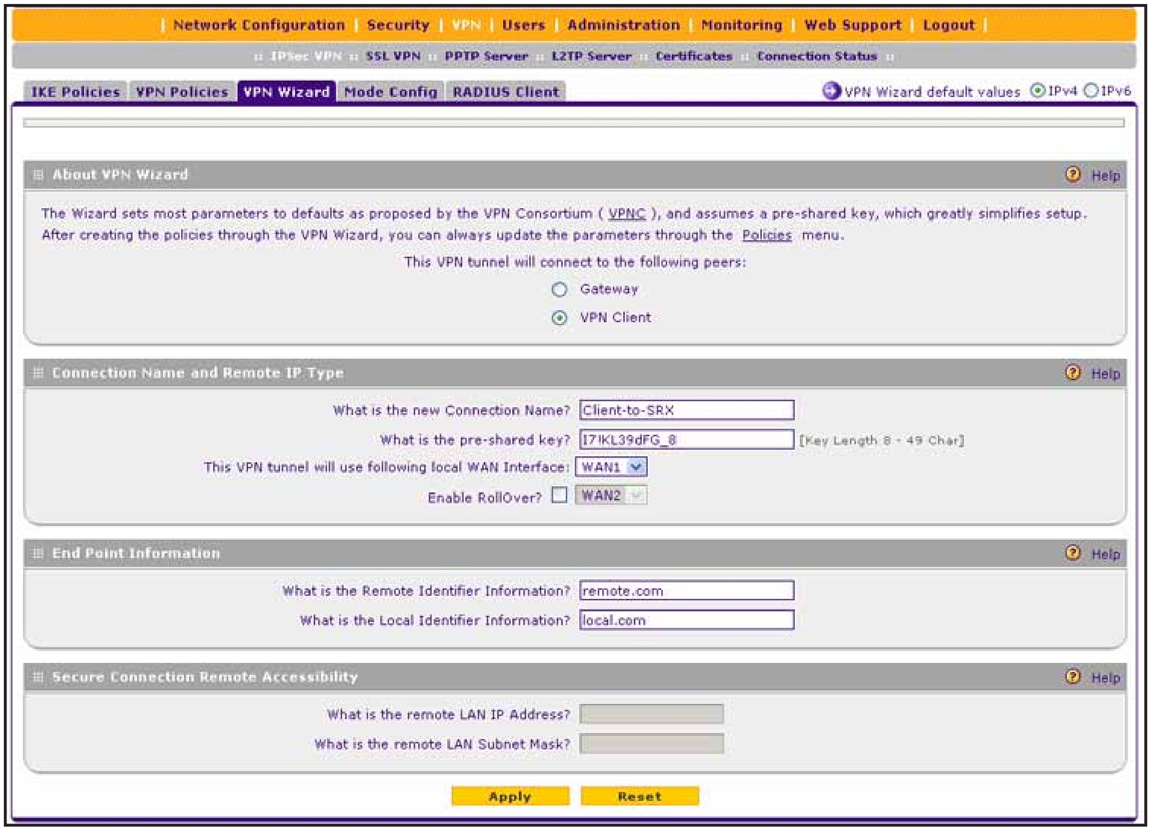
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > IPSec VPN > VPN Wizard**.

   The VPN Wizard screen displays the IPv4 settings. The following figure shows an example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
Help
Apply
Reset

VPN Wizard default values ● 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-SRX

What is the pre-shared key? I7!KL39dFG_8 [Key Length 8 - 49 Char]

This VPN tunnel will use following local WAN Interface: WAN1

Enable RollOver? □ WAN2

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?

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

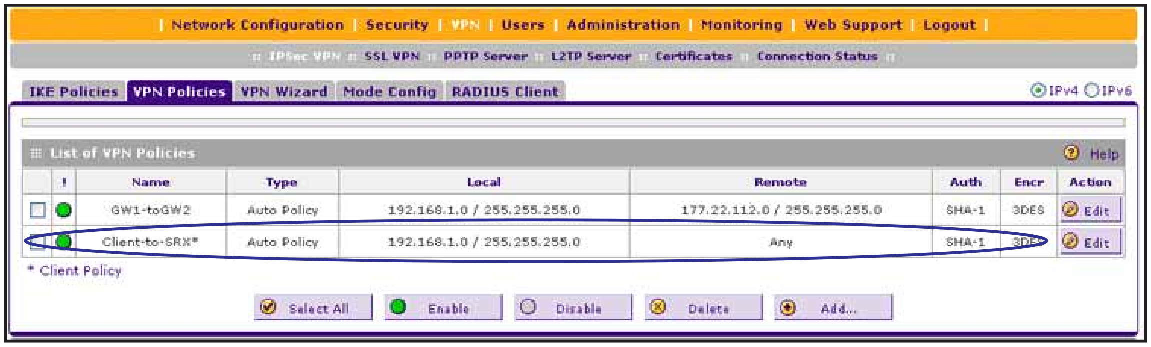
Setting	Description
About VPN Wizard	
This VPN tunnel will connect to the following peers	Select the **VPN Client** radio button. The default remote FQDN (remote.com) and the default local FQDN (local.com) display in the End Point Information section.
Connection Name and Remote IP Type	
What is the new Connection Name?	Enter a descriptive name for the connection. This name helps 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. This key must also be entered on the VPN client. The key must have a minimum length of 8 characters and must not exceed 49 characters.

Setting	Description
This VPN tunnel will use the following local WAN Interface	Select a WAN interface from the menu. The VPN tunnel uses the WAN interface as the local endpoint.
	To enable VPN rollover, select the **Enable RollOver?** check box. The menu to the right of the check box automatically selects the WAN interface that is available for rollover. Configuring VPN rollover is optional. With VPN rollover, if the WAN interface that functions as the local endpoint goes down, the VPN tunnel is reestablished on the other WAN interface. **Note:** If the VPN firewall is configured to function in WAN auto-rollover mode, you can use the VPN Wizard to configure VPN rollover and do not need to configure VPN rollover manually.
End Point Information[a]	
What is the Remote Identifier Information?	When you select the **VPN 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 **VPN 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 and do not apply to 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. The VPN firewall does not support a combination of an IP address and an FQDN.*

8. Click the **Apply** button.

   Your settings are saved. The VPN Policies screen displays the IPv4 settings with the new, automatically generated VPN policy in the List of VPN Policies table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
● IPv4 ○ IPv6
List of VPN Policies
Help
Select All
Enable
Disable
Delete
Add...

	!	Name	Type	Local	Remote	Auth	Encr	Action
□	●	GW1-toGW2	Auto Policy	192.168.1.0 / 255.255.255.0	177.22.112.0 / 255.255.255.0	SHA-1	3DES	Edit
□	●	Client-to-SRX*	Auto Policy	192.168.1.0 / 255.255.255.0	Any	SHA-1	3DES	Edit

* Client Policy

9. Collect the information that you must use to configure the VPN client.

   You can print the following table to keep track of this information.

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 ProSAFE VPN Client Wizard to Create a Secure Connection to the VPN Firewall

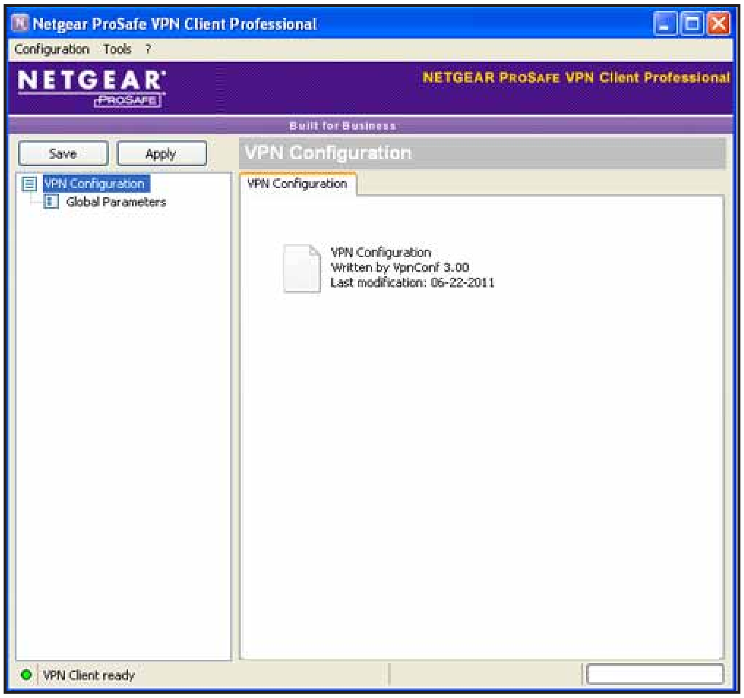
Note: In this section, the NETGEAR ProSAFE VPN Client is referred to as the VPN client.

The VPN client lets you set up the VPN connection manually (see *Manually Create a Secure Connection to the VPN Firewall Using the NETGEAR ProSAFE VPN Client* on page 354) or with the integrated Configuration Wizard, which is the easier and preferred method. However, in some situations you might prefer the manual configuration, which provides more control over the configuration process.

The Configuration Wizard configures the default settings and provides basic interoperability so that the VPN client can easily communicate with the VPN firewall (or a third-party VPN device). The Configuration Wizard does not let you enter the local and remote IDs, so you must manually enter this information.

➢ **To use the VPN Configuration Wizard to set up a VPN connection between the VPN client and the VPN firewall:**

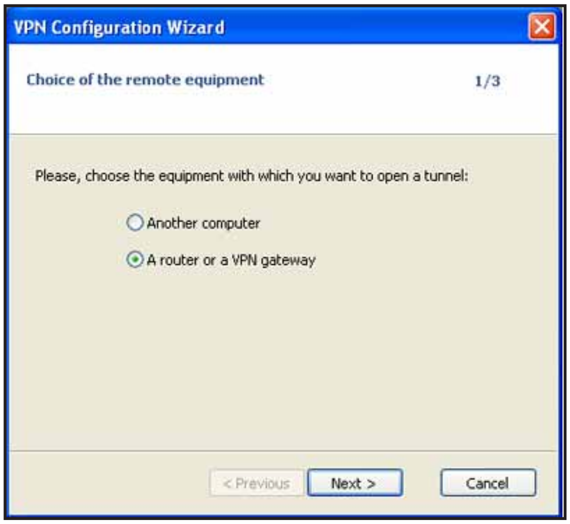
1. On the computer that has the VPN client installed, right-click the VPN client icon in your Windows system tray and select **Configuration Panel**.



VPN Configuration
Written by VpnConf 3.00
Last modification: 06-22-2011

VPN Client ready

2. From the main menu, select **Configuration > Wizard**.

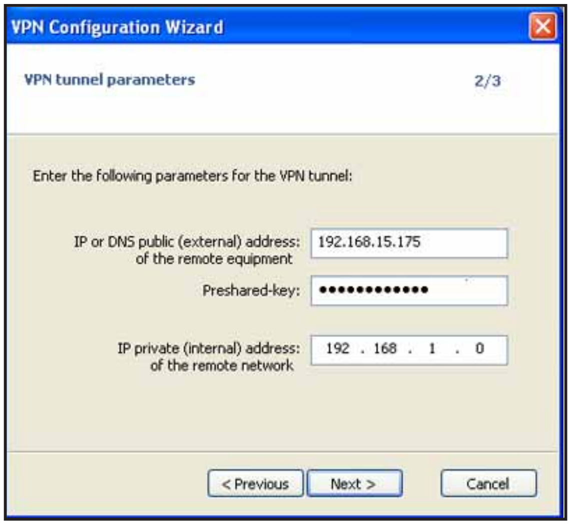


Please, choose the equipment with which you want to open a tunnel:

○ Another computer

● A router or a VPN gateway

3. Select the **A router or a VPN gateway** radio button.
4. Click the **Next** button.



Enter the following parameters for the VPN tunnel:

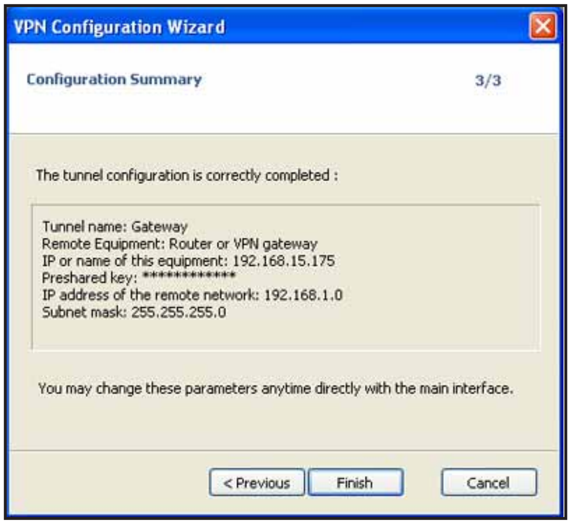
IP or DNS public (external) address: of the remote equipment: 192.168.15.175

Preshared-key: ●●●●●●●●●●●●●

IP private (internal) address: of the remote network: 192 . 168 . 1 . 0

5. 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.
6. Click the **Next** button.

   The Configuration Summary screen displays a summary of the new VPN configuration.



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.

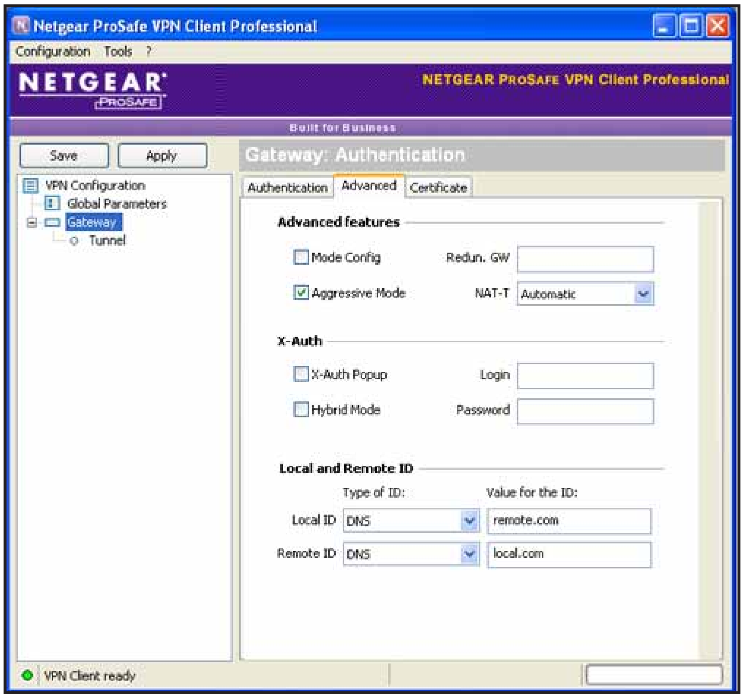
7. Click the **Finish** button.

   The Configuration Panel screen displays.
8. Specify the local and remote IDs:

a. In the tree list pane of the Configuration Panel screen, click **Gateway** (the default name given to the authentication phase).

The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default.

b. Click the **Advanced** tab in the Authentication pane.



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

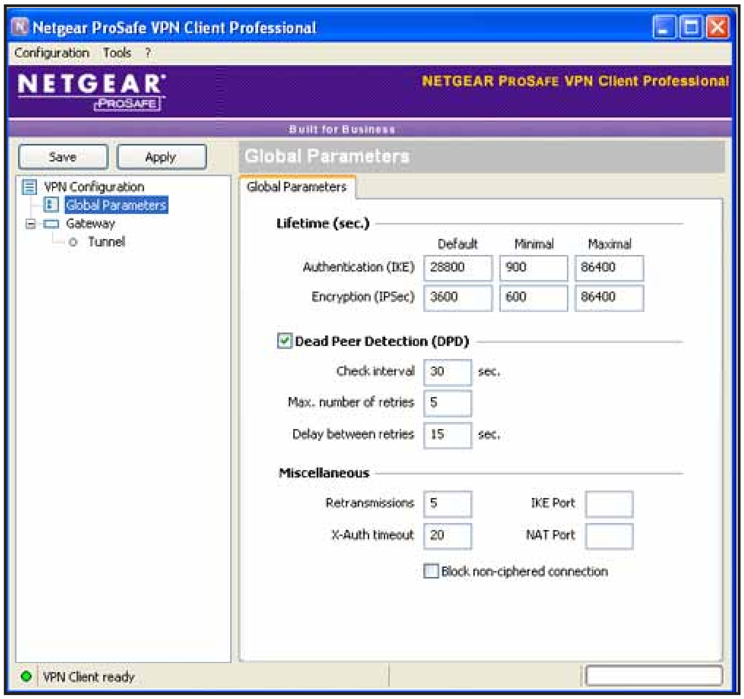
c. Specify the settings that are described in the following table.

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	From the menu, select **Automatic**. The VPN client and VPN firewall can now negotiate NAT-T.

Setting	Description
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the **Local ID** menu because you specified FQDN in the VPN firewall configuration. As the value of the ID, enter **remote.com** as the local ID for the VPN client. **Note:** The remote ID on the VPN firewall is the local ID on the VPN client. It might be less confusing to configure an FQDN such as client.com as the remote ID on the VPN firewall and then enter client.com as the local ID on the VPN client.
Remote ID	As the type of ID, select **DNS** from the **Remote ID** menu 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. Configure the global parameters:

   a. In the tree list pane 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

X-Auth timeout: 20

IKE Port:

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.

10. Click the **Save** button.

    Your settings are saved and the VPN client configuration is complete.

    For information about testing the new VPN tunnel connection, see *Test the Connection and View Connection and Status Information* on page 360.

Manually Create a Secure Connection to the VPN Firewall Using the NETGEAR ProSAFE VPN Client

Note: In this section, the NETGEAR ProSAFE VPN Client is referred to as the VPN client.

The VPN client lets you set up the VPN connection with the integrated Configuration Wizard (see *Use the NETGEAR ProSAFE VPN Client Wizard to Create a Secure Connection to the VPN Firewall* on page 349), which is the easier and preferred method, or manually. In some situations you might prefer the manual configuration, which provides more control over the configuration process.

Manually configuring a VPN connection between the VPN client and the VPN firewall involves three tasks that are described in the following procedure:

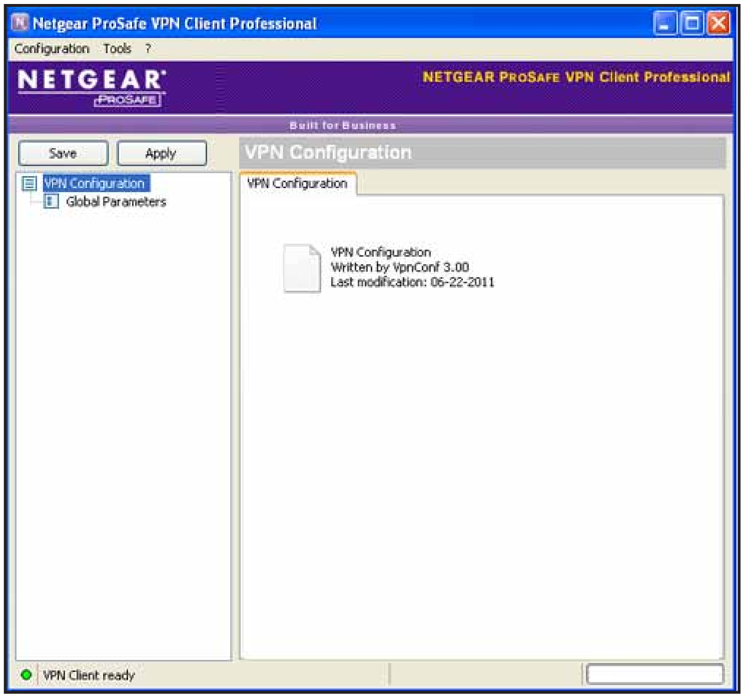
1. Configure the authentication settings (phase 1 settings).
2. Create the IPSec configuration (phase 2 settings).

   Note: On the VPN firewall, the IPSec configuration (phase 2 settings) is referred to as the IKE settings.

3. Configure the global parameters.

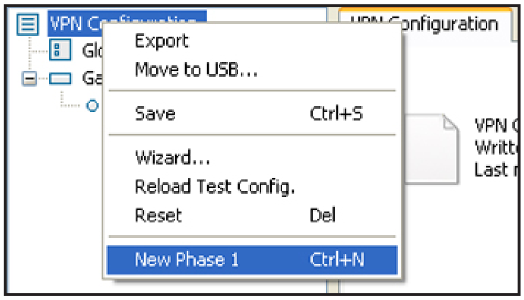
➢ **To manually set up a VPN connection between the VPN client and the VPN firewall:**

1. On the computer that has the VPN client installed, 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

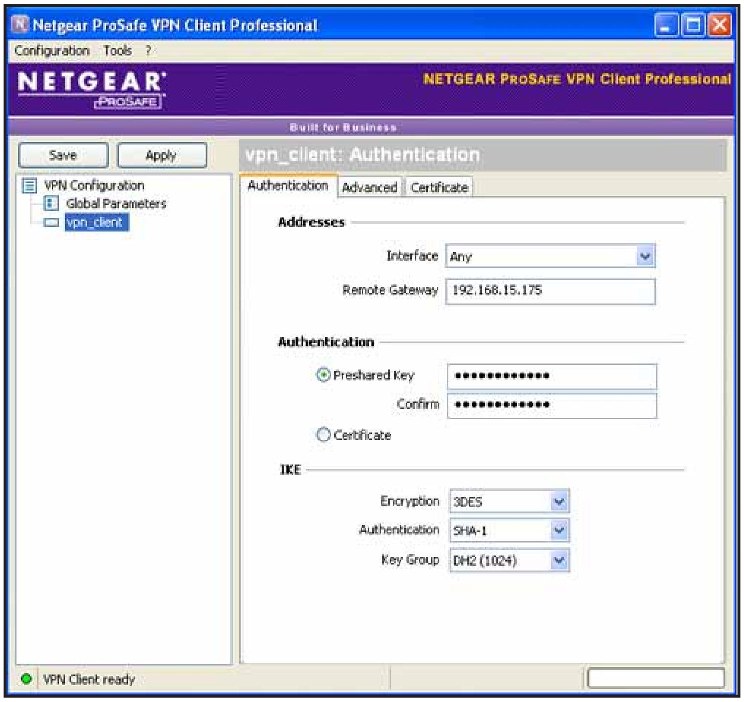
2. In the tree list pane of the Configuration Panel screen, right-click **VPN Configuration**, and select **New Phase 1**.



3. Change the name of the authentication phase (the default name is Gateway):
   a. Right-click the authentication phase name.
   b. Select **Rename**.
   c. Type **vpn_client**.
   d. Click anywhere in the tree list pane.

Note: This is the name for the authentication phase that is used only for the VPN client, not during IKE negotiation. You can view and change this name in the tree list pane. This name must be a unique name.

The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default.



Addresses

Interface: Any

Remote Gateway: 192.168.15.175

Authentication

● Preshared Key: •••••••••••••

Confirm: •••••••••••••

○ Certificate

IKE

Encryption: 3DES

Authentication: SHA-1

Key Group: DH2 (1024)

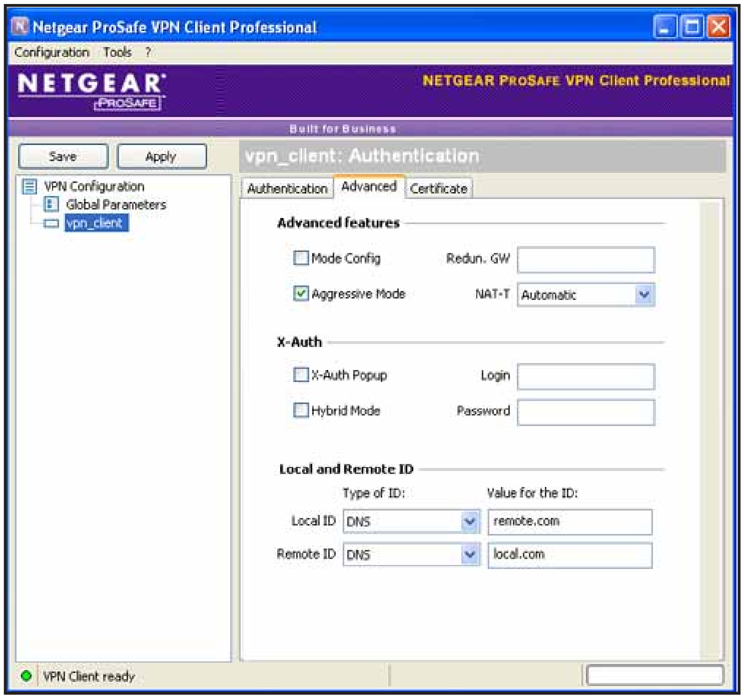
4. Specify the settings that are described in the following table.

Setting	Description
Interface	From the menu, select **Any**.
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 and configure the following settings: 1. Enter the pre-shared key that you already specified on the VPN firewall. For example, enter **I7!KL39dFG_8**. 2. In the **Confirm** field, enter the pre-shared key again.
Encryption	From the menu, select the **3DES** encryption algorithm.
Authentication	From the menu, select the **SHA1** authentication algorithm.
Key Group	From the menu, 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. Click the **Save** button.

   Your settings are saved.

6. Click the **Advanced** tab in the Authentication pane.



vpn_client: 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	remote.com
Remote ID	DNS	local.com

VPN Client ready

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

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	From the menu, select **Automatic**. The VPN client and VPN firewall can now negotiate NAT-T.
Local and Remote ID	
Local ID	As the type of ID, select **DNS** from the **Local ID** menu because you specified FQDN in the VPN firewall configuration. As the value of the ID, enter **remote.com** as the local ID for the VPN client. **Note:** The remote ID on the VPN firewall is the local ID on the VPN client. It might be less confusing to configure an FQDN such as client.com as the remote ID on the VPN firewall and then enter client.com as the local ID on the VPN client.
Remote ID	As the type of ID, select **DNS** from the **Remote ID** menu because you specified an FQDN in the VPN firewall configuration. As the value of the ID, enter **local.com** as the remote ID for the VPN firewall. **Note:** The local ID on the VPN firewall is the remote ID on the VPN client. It might be less confusing to configure an FQDN such as router.com as the local ID on the VPN firewall and then enter router.com as the remote ID on the VPN client.

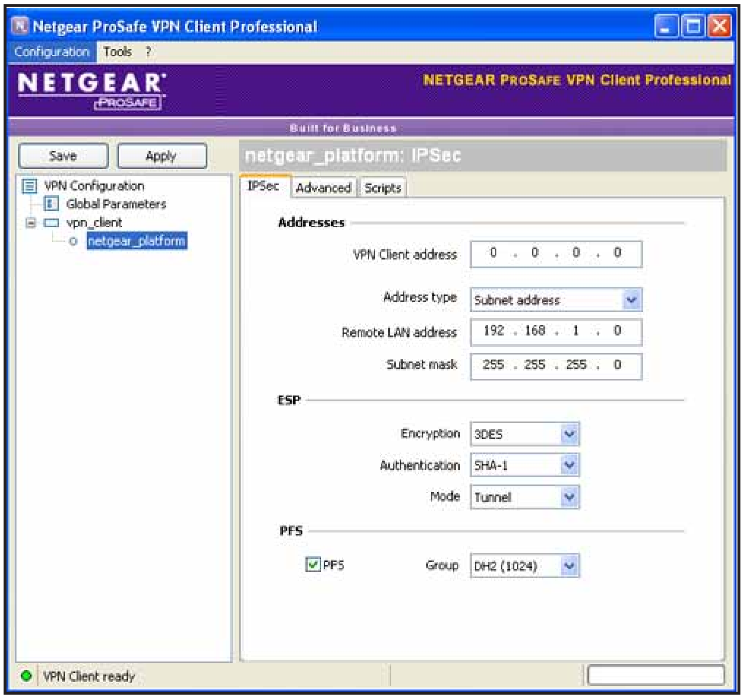
8. Click the **Save** button.

Your settings are saved. Continue the manual configuration of the VPN client with the IPSec configuration.

9. In the tree list pane of the Configuration Panel screen, right-click the **vpn_client** authentication phase name and select **New Phase 2**.
10. Change the name of the IPSec configuration (the default name is Tunnel):
    a. Right-click the IPSec configuration name.
    b. Select **Rename**.
    c. Type **netgear_platform**.
    d. Click anywhere in the tree list pane.

Note: This is the name for the IPSec configuration that is used only for the VPN client, not during IPSec negotiation. You can view and change this name in the tree list pane. This name must be a unique name.

The IPSec pane displays in the Configuration Panel screen, with the IPSec tab selected by default:



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)

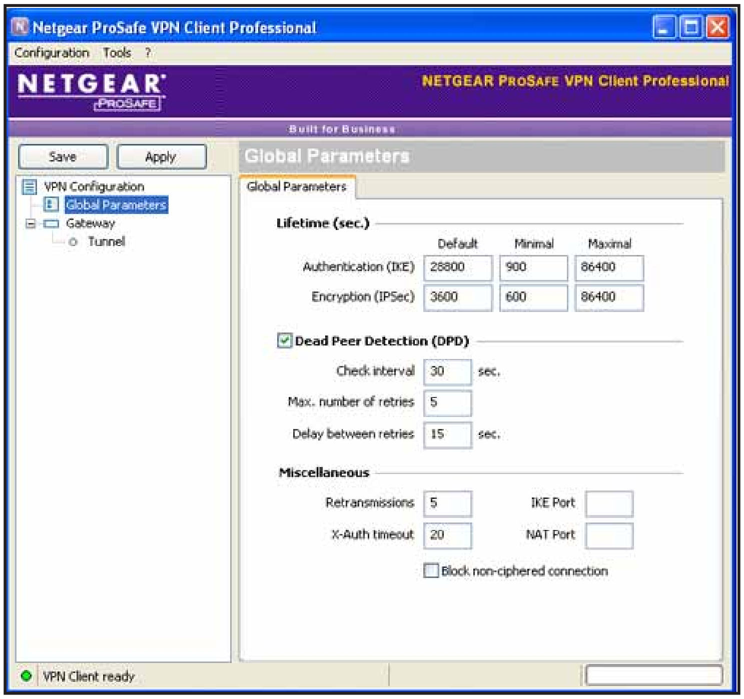
11. Specify the settings that are described in the following table.

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 opens a tunnel appears in the LAN with this IP address.
Address Type	From the menu, select **Subnet address**. 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.
Encryption	From the menu, select **3DES** as the encryption algorithm.
Authentication	From the menu, select **SHA-1** as the authentication algorithm.
Mode	From the menu, select **Tunnel** as the encapsulation mode.
PFS and Group	Select the **PFS** check box and from the menu, select the **DH2 (1024)** key group. **Note:** On the VPN firewall, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).

12. Click the **Save** button.

    Your settings are saved. Continue the manual configuration of the VPN client with the global parameters.

13. In the tree list pane 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

14. 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.
15. Click the **Save** button.

    Your settings are saved. The manual configuration of the VPN firewall is now complete.

    For information about testing the new VPN tunnel connection, see *Test the Connection and View Connection and Status Information* on page 360.

Test the Connection and View Connection and Status Information

The following sections provide information about how to test VPN tunnel connections and view connection and status information:

- *Test the NETGEAR ProSAFE VPN Client VPN Tunnel Connection*
- *NETGEAR ProSAFE VPN Client Status and Log Information*
- *View the VPN Firewall IPSec VPN Connection Status and Terminate or Establish Tunnels*
- *View the VPN Firewall IPSec VPN Log*

Test the NETGEAR ProSAFE VPN Client VPN Tunnel Connection

Note: In this section, the NETGEAR ProSAFE VPN Client is referred to as the VPN client.

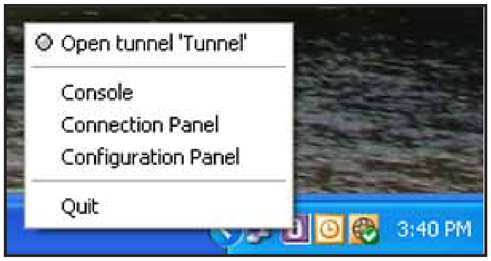
After you configure the IPSec VPN connection on the VPN firewall and the VPN client, you can test the VPN tunnel connection.

The following procedure assumes that you use the default authentication phase name *Gateway* and the default IPSec configuration name *Tunnel*.

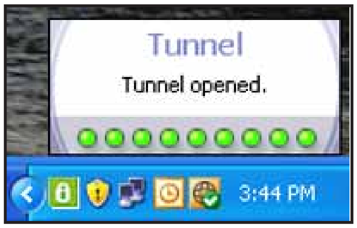
If you configured the connection manually and changed the names, use *vpn_client* (or any other name that you configured) as the authentication phase name and *netgear_platform* (or any other name that you configured) as the IPSec configuration name.

➢ **To initiate a VPN tunnel connection on the VPN client:**

On the computer that has the VPN client installed, right-click the system tray icon, and select **Open tunnel 'Tunnel'**.



When the tunnel opens successfully, the *Tunnel opened* message displays above the system tray.


Tunnel

Tunnel opened.

After the VPN client is launched, it displays an icon in the system tray that indicates whether a tunnel is opened, using a color code.

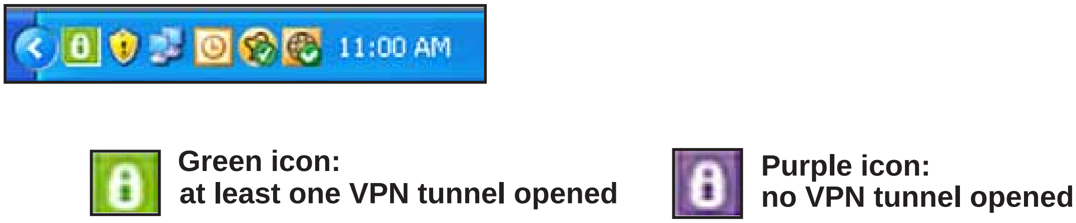


Figure 11. VPN client system tray color codes

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. For more information, see the following sections:

- *NETGEAR ProSAFE VPN Client Status and Log Information* on page 362
- *View the VPN Firewall IPSec VPN Connection Status and Terminate or Establish Tunnels* on page 363
- *View the VPN Firewall IPSec VPN Log* on page 364

NETGEAR ProSAFE VPN Client Status and Log Information

Note: In this section, the NETGEAR ProSAFE VPN Client is referred to as the VPN client.

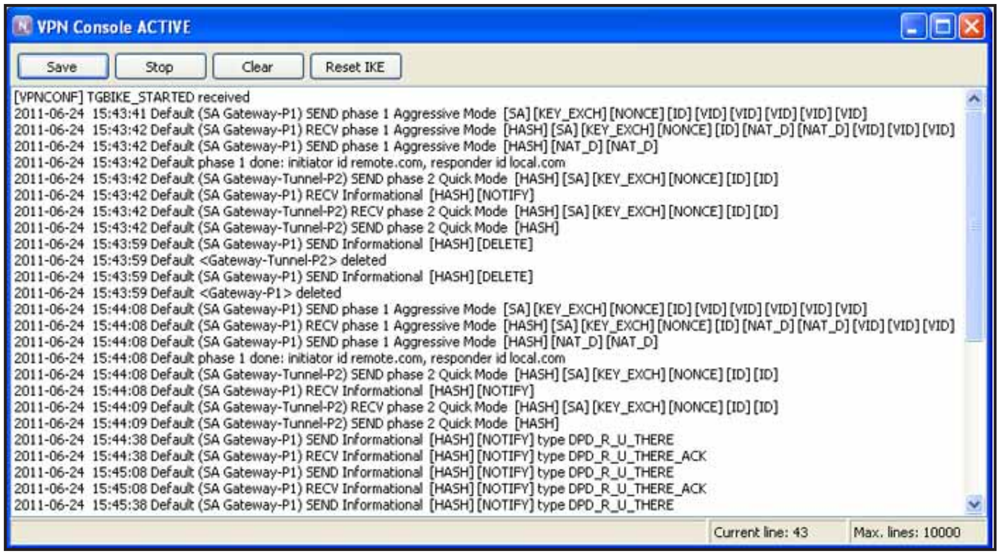
The VPN console on the VPN client displays notifications and, if errors occur, error messages that are detected on the client side. If problems occur during the VPN tunnel establishment process, these error messages can help you to determine what the problem is. (Misconfigration is the most common problem.)

For more information about notifications and error messages, see the *NETGEAR ProSafe VPN Client User Manual*, which you can download from *downloadcenter.netgear.com*.

➢ **To view detailed negotiation and error information on the VPN client:**

On the computer that has the VPN client installed, right-click the VPN client icon in the system tray and select **Console**.

The VPN 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 and Terminate or Establish Tunnels

You can view the connection status of all IPSec VPN tunnel sessions on the VPN firewall. For a gateway-to-gateway connection, you can terminate or establish a tunnel. For a client-to-gateway connection, you can terminate a tunnel.

➢ **To view the status of IPSec VPN tunnels on the VPN firewall and terminate or establish tunnels:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

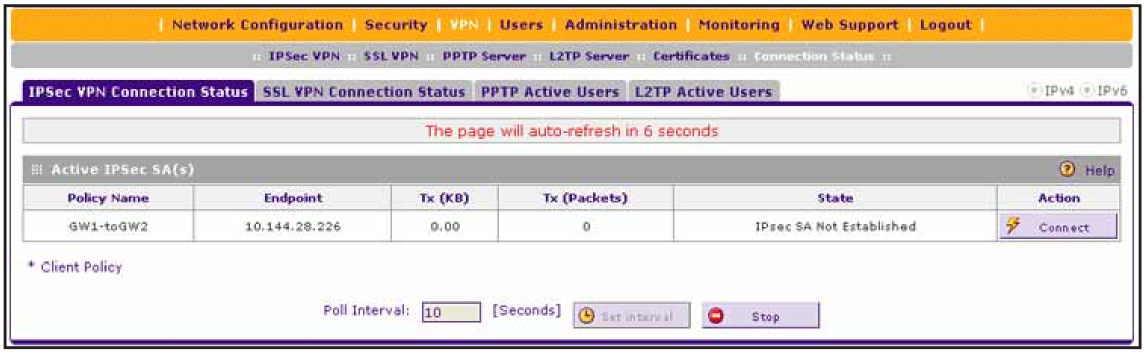
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > Connection Status**.

The Connection Status submenu tabs display with the IPSec VPN Connection Status screen in view. The following figure shows an IPSec security association (SA) as an example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
IPSec VPN Connection Status
SSL VPN Connection Status
PPTP Active Users
L2TP Active Users
○ IPv4 ○ IPv6
Help
Connect
Set interval
Stop

The page will auto-refresh in 6 seconds

Active IPSec SA(s)

Policy Name	Endpoint	Tx (KB)	Tx (Packets)	State	Action
GW1-toGW2	10.144.28.226	0.00	0	IPsec SA Not Established	Connect

* Client Policy

Poll Interval: 10 [Seconds]

The Active IPSec SA(s) table lists each active connection with the information that is described in the following table.

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 is established, the status is IPSec SA Not Established.
Action	The **Connect** button lets you initiate the VPN tunnel connection. The **Disconnect** button lets you terminate the VPN tunnel connection.

7. To disable an active gateway-to-gateway or client-to-gateway VPN IPsec tunnel, in the Active IPSec SA(s) table, click the corresponding **Disconnect** button for policy name.
8. To disable another tunnel, repeat *Step 7*.
9. To establish a gateway-to-gateway VPN IPsec tunnel, in the Active IPSec SA(s) table, click the corresponding **Connect** button for the policy name.
10. To establish another tunnel, repeat *Step 9*.

View the VPN Firewall IPSec VPN Log

The IPSec VPN log on the VPN firewall displays notifications and, if errors occur, error messages that are detected on the VPN firewall side. If problems occur during the VPN tunnel establishment process, these error messages can help you to determine what the problem is. (Misconfigration is the most common problem.)

➢ **To display the IPSec VPN log on the VPN firewall:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

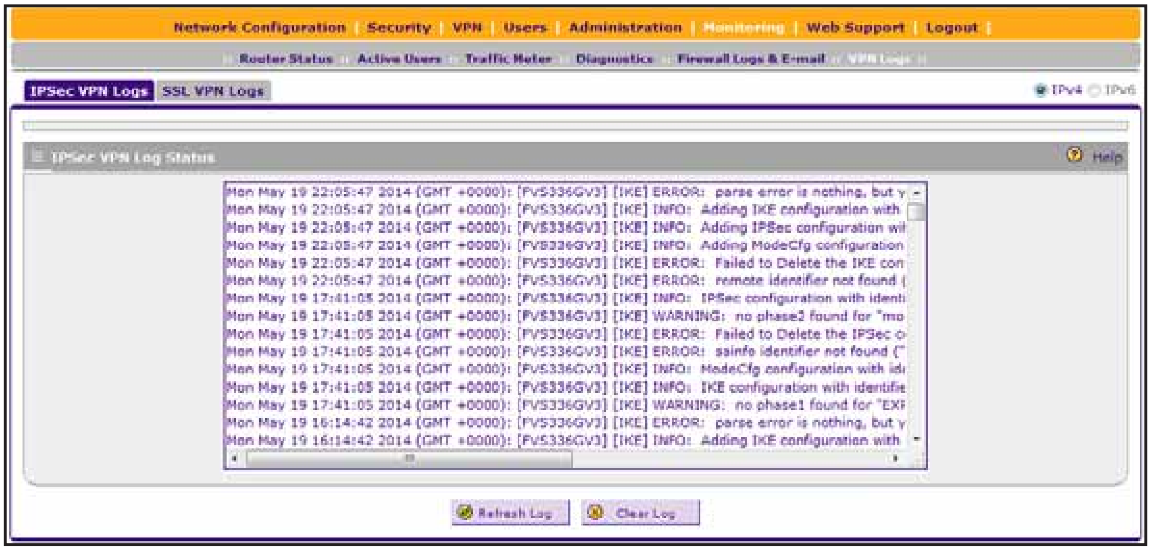
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Monitoring > VPN Logs > IPSec VPN Logs**.

   The IPSec VPN Logs screen displays.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
Router Status | Active Users | Traffic Meter | Diagnostics | Firewall Logs & E-mail | VPN Logs |
IPSec VPN Logs
SSL VPN Logs
● IPv4 ○ IPv6
IPSec VPN Log Status
Help
Refresh Log
Clear Log

```
Mon May 19 22:05:47 2014 (GMT +0000): [FVS336GV3] [IKE] ERROR:  parse error is nothing, but y
Mon May 19 22:05:47 2014 (GMT +0000): [FVS336GV3] [IKE] INFO:  Adding IKE configuration with
Mon May 19 22:05:47 2014 (GMT +0000): [FVS336GV3] [IKE] INFO:  Adding IPSec configuration wi
Mon May 19 22:05:47 2014 (GMT +0000): [FVS336GV3] [IKE] INFO:  Adding ModeCfg configuration
Mon May 19 22:05:47 2014 (GMT +0000): [FVS336GV3] [IKE] ERROR:  Failed to Delete the IKE con
Mon May 19 22:05:47 2014 (GMT +0000): [FVS336GV3] [IKE] ERROR:  remote identifier not found (
Mon May 19 17:41:05 2014 (GMT +0000): [FVS336GV3] [IKE] INFO:  IPSec configuration with identi
Mon May 19 17:41:05 2014 (GMT +0000): [FVS336GV3] [IKE] WARNING:  no phase2 found for "mo
Mon May 19 17:41:05 2014 (GMT +0000): [FVS336GV3] [IKE] ERROR:  Failed to Delete the IPSec c
Mon May 19 17:41:05 2014 (GMT +0000): [FVS336GV3] [IKE] ERROR:  sainfo identifier not found ("
Mon May 19 17:41:05 2014 (GMT +0000): [FVS336GV3] [IKE] INFO:  ModeCfg configuration with id
Mon May 19 17:41:05 2014 (GMT +0000): [FVS336GV3] [IKE] INFO:  IKE configuration with identifie
Mon May 19 17:41:05 2014 (GMT +0000): [FVS336GV3] [IKE] WARNING:  no phase1 found for "EXF
Mon May 19 16:14:42 2014 (GMT +0000): [FVS336GV3] [IKE] ERROR:  parse error is nothing, but y
Mon May 19 16:14:42 2014 (GMT +0000): [FVS336GV3] [IKE] INFO:  Adding IKE configuration with
```

Manage IPSec VPN Policies Manually

After you have used the VPN Wizard to set up a VPN tunnel, a VPN policy and an IKE policy are stored in separate policy tables. The name that you selected as the VPN tunnel connection name during the VPN Wizard setup identifies both the VPN policy and IKE policy.

You can change existing policies or manually add new VPN and IKE policies directly in the policy tables.

The following sections provide information about managing IPSec VPN policies manually:

- *Manage IKE Policies*
- *Manage VPN Policies*

Manage IKE Policies

The following sections provide information about managing IKE policies:

- *IKE Policies*
- *View the IKE Policies*
- *Manually Add an IKE Policy*
- *Associate a Manually added IKE policy with an Existing VPN Policy*
- *Change an IKE Policy*
- *Remove One or More IKE Policies*

IKE Policies

The Internet Key Exchange (IKE) protocol performs negotiations between two VPN devices and provides automatic management of the keys that are used for IPSec connections.

An automatically generated VPN policy (auto policy) must use the IKE negotiation protocol. However, a manually generated VPN policy (manual policy) cannot use the IKE negotiation protocol.

An IKE policy is activated when the following sequence of events occurs:

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 for the VPN auto policy is used to start negotiations with the remote VPN gateway.
3. An IKE session is established, using the security association (SA) settings that are specified in a matching IKE policy:
   - Keys and other settings are exchanged.
   - An IPSec SA is established, using the settings that are specified in the VPN policy.

The VPN tunnel is then available for data transfer.

When you use the VPN Wizard to set up a VPN tunnel, an IKE policy is also added automatically and is given the same name as the new VPN connection name.

You can change existing IKE policies manually and add new IKE policies.

View the IKE Policies

The following procedure describes how to view the IKE policies that were automatically added and that you manually added.

➤ **To view the IKE policies:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

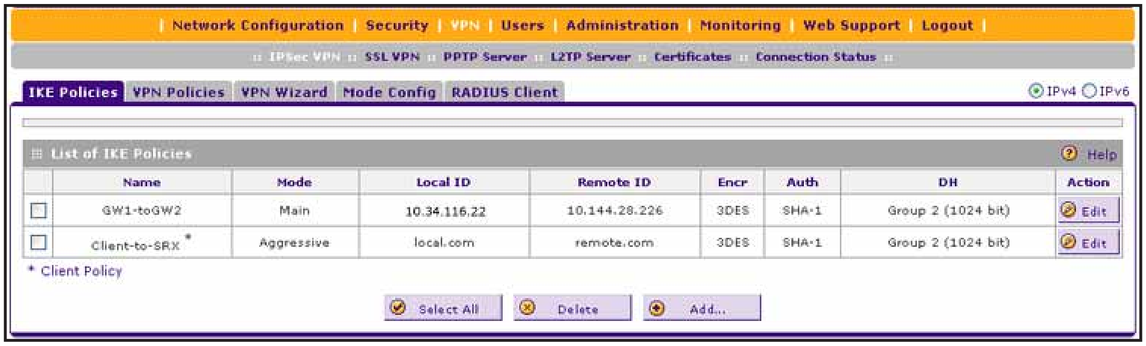
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > IPSec VPN**.

   The IPSec VPN submenu tabs display with the IKE Policies screen in view, displaying the IPv4 settings.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: 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
□	GW1-toGW2	Main	10.34.116.22	10.144.28.226	3DES	SHA-1	Group 2 (1024 bit)	Edit
□	Client-to-SRX *	Aggressive	local.com	remote.com	3DES	SHA-1	Group 2 (1024 bit)	Edit

* Client Policy

7. To display the IPv6 settings instead of the IPv4 settings, in the upper right, select the **IPv6** radio button.

   The IKE Policies screen displays the IPv6 settings.

Each policy contains the settings that are described in the following table. These settings apply to both IPv4 and IPv6 IKE policies. For more information about these settings, see *Manually Add an IKE Policy* on page 368.

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

Manually Add an IKE Policy

The following procedure describes how to add an IKE policy manually.

➢ **To manually add an IKE policy for IPv4 or IPv6:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

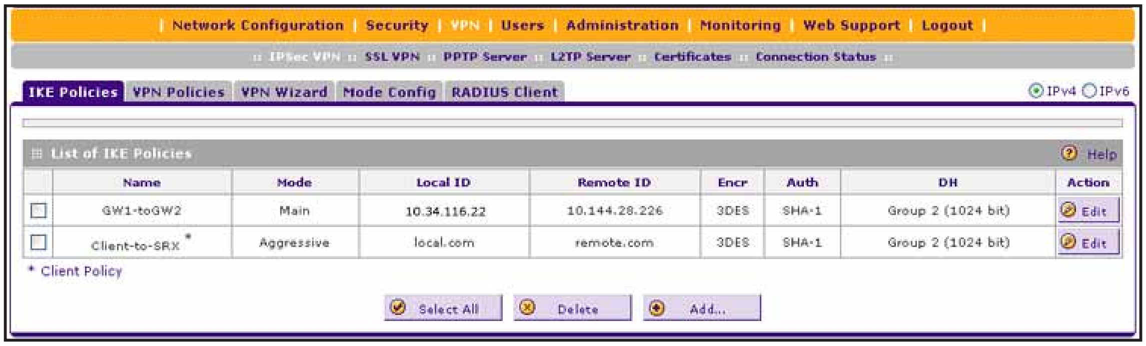
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

The Router Status screen displays.

6. Select **VPN > IPSec VPN**.

   The IPSec VPN submenu tabs display with the IKE Policies screen for IPv4 in view.



	Name	Mode	Local ID	Remote ID	Encr	Auth	DH	Action
□	GW1-toGW2	Main	10.34.116.22	10.144.28.226	3DES	SHA-1	Group 2 (1024 bit)	Edit
□	Client-to-SRX *	Aggressive	local.com	remote.com	3DES	SHA-1	Group 2 (1024 bit)	Edit

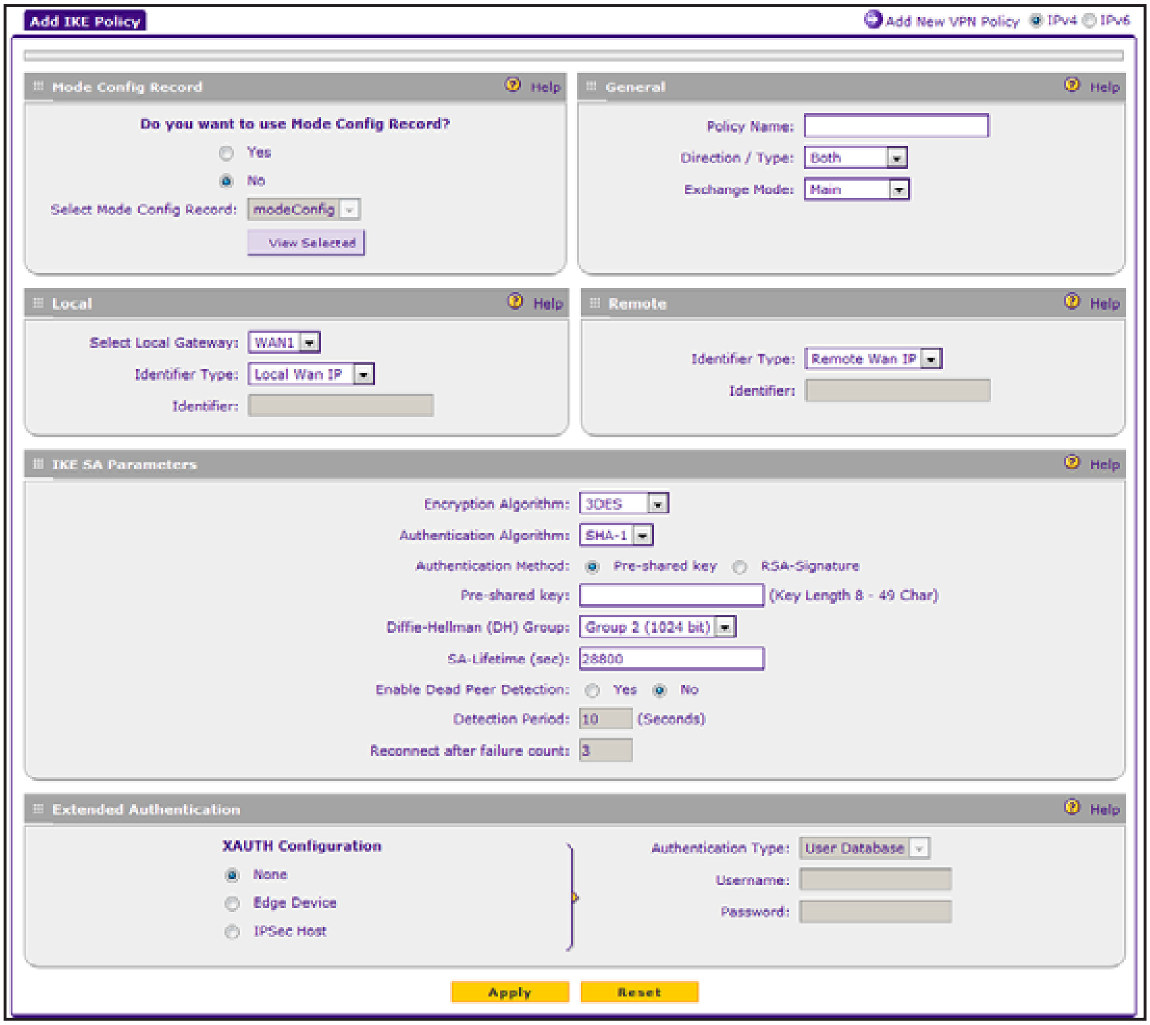
* Client Policy

7. To add an IKE policy for IPv6 instead of IPv4, in the upper right, select the **IPv6** radio button.

   The IKE Policies screen displays the IPv6 settings.

8. Under the List of IKE Policies table, click the **Add** button.

   The Add IKE Policy screen displays. The Add IKE Policy screen for IPv4 is identical to the Add IKE Policy screen for IPv6.



Add IKE Policy

Add New VPN Policy ● IPv4 ○ IPv6

Mode Config Record

Do you want to use Mode Config Record?

○ Yes

● No

Select Mode Config Record: modeConfig

View Selected

General

Policy Name:

Direction / Type: Both

Exchange Mode: Main

Local

Select Local Gateway: WAN1

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. Enter the settings as described in the following table.

   Other than the nature of the IP addresses, the settings that you must enter for IPv4 and IPv6 settings are identical.

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 Overview* on page 394. Select a radio button: • **No**. If you did not define a Mode Config record, leave the **No** radio button selected, which disables Mode Config for this IKE policy. This is the default setting. • **Yes**. If you defined a Mode Config record and want to use it for this IKE policy, select the **Yes** radio button. From the **Select Mode Config Record** menu, select a Mode Config record, which allows the VPN firewall to assign IP addresses to remote VPN clients. 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. **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 menu, select one of the Mode Config records that you defined (see *Configure Mode Config Operation on the VPN Firewall* on page 395). **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 menu, 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 menu, select the mode of exchange between the VPN firewall and the remote VPN endpoint: • **Main**. This mode is slower than the Aggressive mode but more secure. • **Aggressive**. This mode is faster than the Main mode but less secure.
Local	
Select Local Gateway	Select a WAN interface from the menu to specify the WAN interface for the local gateway.

Setting	Description
Identifier Type	From the menu, select an ISAKMP identifier 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 from the **Identifier Type** menu, enter the IP address, email address, FQDN, or distinguished name.
Remote	
Identifier Type	From the menu, select an ISAKMP identifier 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** menu, enter the IP address, email address, FQDN, or distinguished name.
IKE SA Parameters	
Encryption Algorithm	From the menu, 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 menu, 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.
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 must have uploaded (see *Manage VPN Self-Signed Certificates* on page 516). When you select **RSA-Signature**, the **Pre-shared key** field is masked out.
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.

Setting	Description
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 menu, 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	Select a radio button to specify whether Dead Peer Detection (DPD) is enabled: • **No**. This feature is disabled. This is the default setting. • **Yes**. This feature is enabled. When the VPN firewall detects an IKE connection failure, it removes 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. **Note:** For more information, see *Manage Keep-Alives and Dead Peer Detection* on page 411.
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.
Extended Authentication	
XAUTH Configuration	Select a radio button to specify whether Extended Authentication (XAUTH) is enabled and, if enabled, which device is used to verify user account information: • **None**. XAUTH is disabled. This the default setting. • **Edge Device**. The VPN firewall functions as a VPN concentrator on which one or more gateway tunnels terminate. The authentication modes that are available for this configuration are User Database, RADIUS PAP, or RADIUS CHAP. • **IPSec Host**. The VPN firewall functions as a VPN client of the remote gateway. In this configuration, the VPN firewall is authenticated by a remote gateway with a user name and password combination. **Note:** For more information about XAUTH and its authentication modes, see *Enable and Configure Extended Authentication for VPN Clients* on page 389.

Setting	Description
Authentication Type	If you select **Edge Device** from the **AUTH Configuratio**n menu, you must select an authentication type from the **Authentication Type** menu: • **User Database**. XAUTH occurs through the VPN firewall's user database. For information about adding users, see *Manage User Accounts* on page 498. • **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 *Configure the RADIUS Servers for the VPN Firewall's RADIUS Client* on page 392. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see *Configure the RADIUS Servers for the VPN Firewall's RADIUS Client* on page 392.
Username	The user name for XAUTH.
Password	The password for XAUTH.

10. Click the **Apply** button.

    Your settings are saved. The IKE policy is added to the List of IKE Policies table.

Associate a Manually added IKE policy with an Existing VPN Policy

The following procedure describes you can add an IKE policy that you added manually with an existing VPN policy. An IKE policy that is not associated with a VPN policy is inactive.

➢ **To associate a manually added IKE policy with an existing VPN policy:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > IPSec VPN > VPN Policies**.

The VPN Policies screen displays the IPV4 settings.

7. To change a VPN policy for IPv6 instead of IPv4, in the upper right, select the **IPv6** radio button.

   The VPN Policies screen displays the IPv6 settings.

   Note: You can associate an IKE policy only with an Auto policy.

8. In the List of VPN Policies table, click the **Edit** button for the VPN policy with which you want to associate the IKE policy.

   The Edit VPN Policy screen displays.

9. In the Auto Policy Parameters section, from the **Select IKE Policy** menu, select the IKE policy.
10. Click the **Apply** button.

    Your settings are saved. The IKE policy is now associated with the VPN policy.

Change an IKE Policy

The following procedure describes how you can change an existing IKE policy that was added either automatically or manually.

➢ **To change an IKE policy:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

   Note: You cannot change an IKE policy for which the associated VPN policy is active.

6. If the IKE policy that you want to change is associated with a VPN policy, first disable the VPN policy:

   a. Select **VPN > IPSec VPN > VPN Policies**.

      The VPN Policies screen displays the IPv4 settings.

   b. To disable a VPN policy for IPv6 instead of IPv4, in the upper right, select the **IPv6** radio button.

      The VPN Policies screen displays the IPv6 settings.

   c. In the List of VPN policies table, select the VPN policy that is associated with the IKE policy that you want to change.

   Note: When you use the VPN IPsec Wizard, the VPN and IKE policies that are added automatically have the same name.

   d. Click the **Disable** button.

      The VPN policy is disabled. The green circle to the left of the VPN policy turns gray.

7. Select **VPN > IPSec VPN**.

   The IPSec VPN submenu tabs display with the IKE Policies screen for IPv4 in view.

8. To change an IKE policy for IPv6 instead of IPv4, in the upper right, select the **IPv6** radio button.

   The IKE Policies screen for IPv6 displays.

9. In the List of IKE Policies table, click the **Edit** button for the IKE policy that you want to change.

   The Edit IKE Policy screen displays.

10. Change the settings.

    For information about the settings, see *Manually Add an IKE Policy* on page 368.

11. Click the **Apply** button.

    Your settings are saved. The modified IKE policy displays in the List of IKE Policies table on the IKE Policies screen.

12. If you disabled the VPN policy with which the IKE policy that you changed is associated, reenable the VPN policy:

    a. Select **VPN > IPSec VPN > VPN Policies**.

       The VPN Policies screen displays the IPv4 settings.

    b. To reenable a VPN policy for IPv6 instead of IPv4, in the upper right, select the **IPv6** radio button.

       The VPN Policies screen displays the IPv6 settings.

    c. In the List of VPN policies table, select the VPN policy that is associated with the IKE policy that you changed.

    d. Click the **Enable** button.

The VPN policy is reenabled. The gray circle to the left of the VPN policy turns green.

Remove One or More IKE Policies

The following procedure describes how you can remove one or more IKE policies that you no longer need.

⚠ **WARNING:**

If you remove an IKE policy that is associated with a VPN policy but do not replace it with another IKE policy that you associate with the same VPN policy, the VPN policy does not function anymore.

➢ **To remove one or more IKE polices:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.

   Note: You cannot remove an IKE policy for which the associated VPN policy is active.
6. If the IKE policy that you want to remove is associated with a VPN policy, first disable the VPN policy:

   a. Select **VPN > IPSec VPN > VPN Policies**.

      The VPN Policies screen displays the IPv4 settings.

   b. To disable a VPN policy for IPv6 instead of IPv4, in the upper right, select the **IPv6** radio button.

      The VPN Policies screen displays the IPv6 settings.

c. In the List of VPN policies table, select the VPN policy that is associated with the IKE policy that you want to change.

Note: When you use the VPN IPsec Wizard, the VPN and IKE policies that are added automatically have the same name.

d. Click the **Disable** button.

The VPN policy is disabled. The green circle to the left of the VPN policy turns gray.

7. Select **VPN > IPSec VPN**.

   The IPSec VPN submenu tabs display with the IKE Policies screen for IPv4 in view.

8. To remove an IKE policy for IPv6 instead of IPv4, in the upper right, select the **IPv6** radio button.

   The IKE Policies screen for IPv6 displays.

9. In the List of IKE Policies table, select the check box to the left of each policy that you want to remove, or click the **Select All** button to select all IKE policies.
10. Click the **Delete** button.

    The selected IKE policies are removed from the List of IKE Policies table.

    For information about adding an IKE policy, see *Manually Add an IKE Policy* on page 368.

    For information about associating an IKE policy with an existing VPN policy, see *Associate a Manually added IKE policy with an Existing VPN Policy* on page 374.

Manage VPN Policies

The following sections provide information about managing VPN policies:

- *VPN Policies Overview*
- *View the VPN Policies*
- *Manually Add a VPN Policy*
- *Change a VPN Policy*
- *Enable, Disable, or Remove One or More Existing VPN Policies*

VPN Policies Overview

A VPN policy specifies the IP address or FQDN of the local VPN gateway and the IP address or FQDN of the remote VPN gateway and the authentication and encryption that is used to establish the tunnel. In addition, after the IPSec negotiations are complete and the VPN tunnel is established, the VPN policy specifies the type of authentication and encryption that is used to transfer the traffic securely.

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. A manual VPN policy cannot use the Internet Key Exchange (IKE) negotiation protocol.

- **Auto**. Some settings for the VPN tunnel are generated automatically through the use of the IKE protocol to perform negotiations between the two VPN endpoints (the local ID endpoint and the remote ID endpoint). You still must manually enter all settings on the remote VPN endpoint (unless the remote VPN endpoint also has a VPN Wizard). Unlike a manual VPN policy, an automatically generated VPN policy must use the IKE negotiation protocol.

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 (see *Manage Digital Certificates for VPN Connections* on page 512). For gateways to use a CA to perform authentication, each VPN gateway must have a certificate from the CA. Both a public key and a private key exist for each certificate. 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.

These are the rules for VPN policy use:

- Traffic covered by a policy is automatically sent through a VPN tunnel.
- When traffic is covered by two or more policies, the first matching policy is used. (In this situation, the order of the policies is important. However, if you have only one policy for each remote VPN endpoint, the policy order is not important.)
- The VPN tunnel is created according to the settings in the security association (SA).
- The remote VPN endpoint must have a matching SA; otherwise, it refuses the connection.

View the VPN Policies

The following procedure describes how to view the VPN policies that were automatically added and that you manually added.

➢ **To view the VPN policies:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

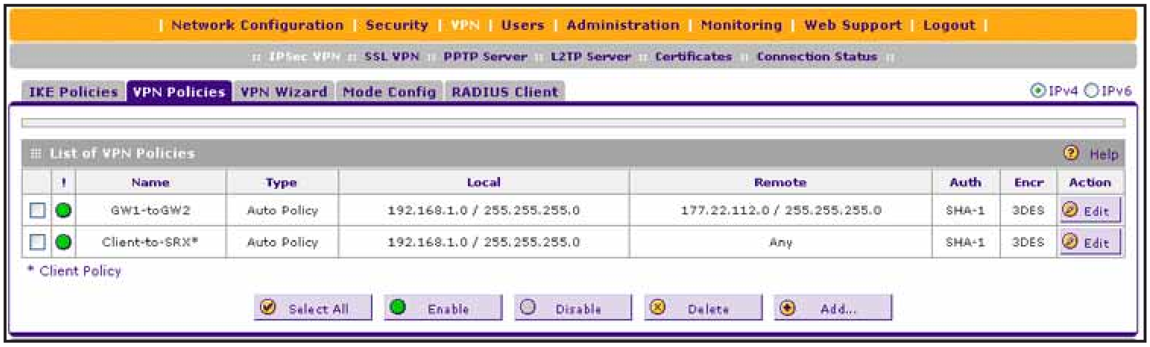
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **VPN > IPSec VPN > VPN Policies**.

   The VPN Policies screen displays the IPv4 settings. The following figure shows some examples.



| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
◉ IPv4 ○ IPv6

List of VPN Policies

	!	Name	Type	Local	Remote	Auth	Encr	Action
□	●	GW1-toGW2	Auto Policy	192.168.1.0 / 255.255.255.0	177.22.112.0 / 255.255.255.0	SHA-1	3DES	Edit
□	●	Client-to-SRX*	Auto Policy	192.168.1.0 / 255.255.255.0	Any	SHA-1	3DES	Edit

* Client Policy

Help
Select All
Enable
Disable
Delete
Add...

7. To display the IPv6 settings, in the upper right, select the **IPv6** radio button.

   The VPN Policies screen displays the IPv6 settings.

   Each policy contains the settings that are described in the following table. These settings apply to both IPv4 and IPv6 VPN policies. For more information about these settings, see *Manually Add a VPN Policy* on page 381.

Item	Description
! (Status)	Indicates whether the policy is enabled (green circle) or disabled (gray circle). For information about enabling and disabling VPN policies, see *Enable, Disable, or Remove One or More Existing VPN Policies* on page 387.
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 in *VPN Policies Overview* on page 378. (Auto is used during VPN Wizard configuration).
Local	The 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	The 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.)

Item	Description
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.

Manually Add a VPN Policy

The following procedure describes how to add a VPN policy manually.

➢ **To manually add a VPN policy:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

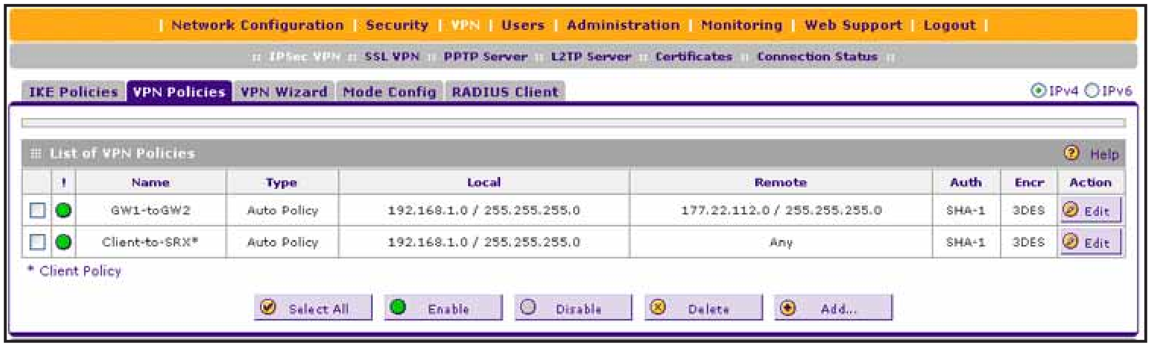
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > IPSec VPN > VPN Policies**.

   The VPN Policies screen displays the IPV4 settings.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
◉ IPv4 ○ IPv6
Help
Select All
Enable
Disable
Delete
Add...

List of VPN Policies

	!	Name	Type	Local	Remote	Auth	Encr	Action
□	●	GW1-toGW2	Auto Policy	192.168.1.0 / 255.255.255.0	177.22.112.0 / 255.255.255.0	SHA-1	3DES	Edit
□	●	Client-to-SRX*	Auto Policy	192.168.1.0 / 255.255.255.0	Any	SHA-1	3DES	Edit

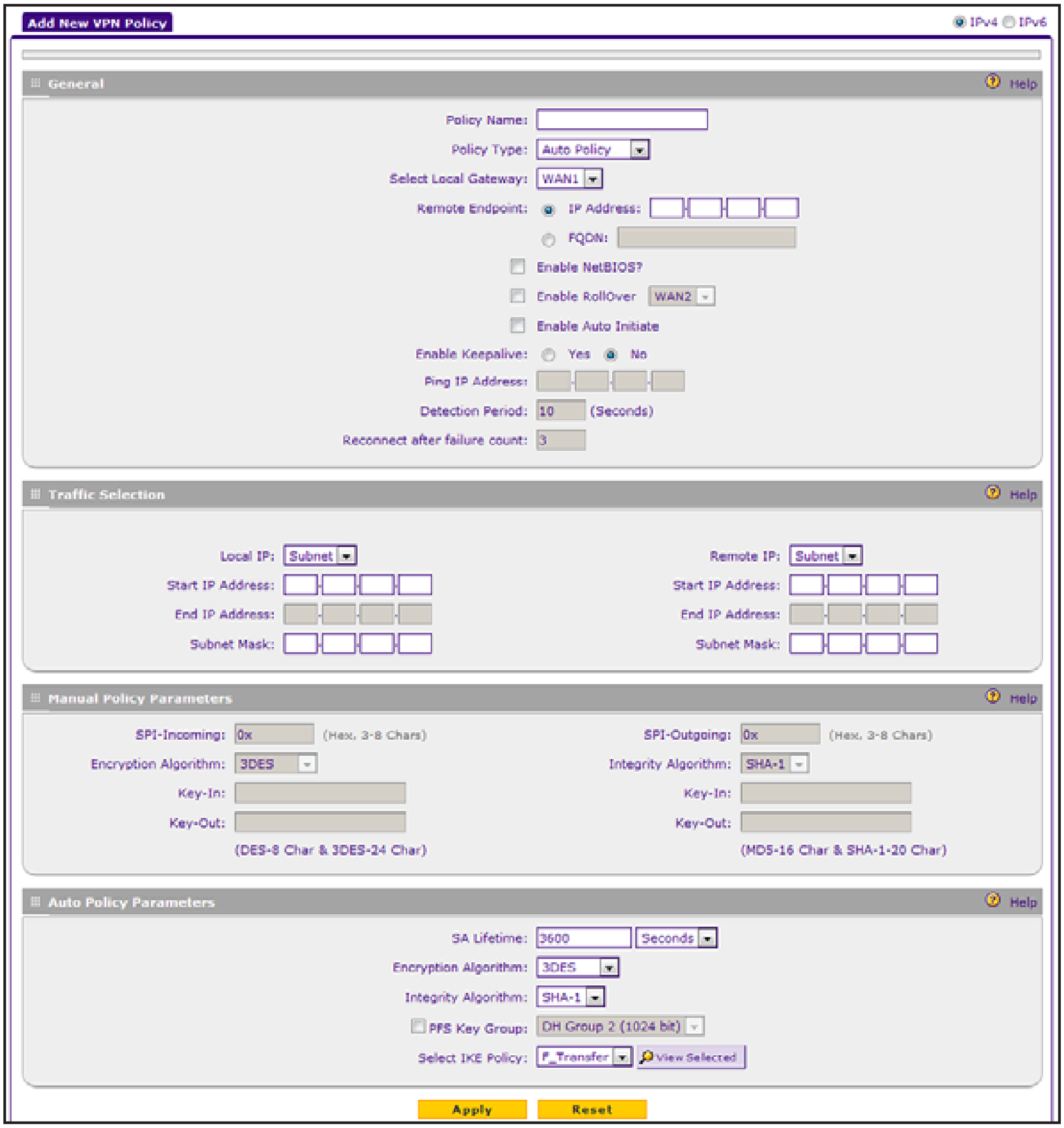
* Client Policy

7. To add a VPN policy for IPv6, in the upper right, select the **IPv6** radio button.

   The VPN Policies screen displays the IPV6 settings.

8. Under the List of VPN Policies table, click the **Add** button.

   The Add New VPN Policy screen displays. The Add New VPN Policy screen for IPv4 and the Add New VPN Policy screen for IPv6 are almost identical.



Add New VPN Policy

● IPv4 ○ IPv6

General

Policy Name:
Policy Type: Auto Policy
Select Local Gateway: WAN1
Remote Endpoint: ● IP Address:
○ FQDN:
□ Enable NetBIOS?
□ Enable RollOver WAN2
□ Enable Auto Initiate
Enable Keepalive: ○ Yes ● No
Ping IP Address:
Detection Period: 10 (Seconds)
Reconnect after failure count: 3

Traffic Selection

Local IP: Subnet
Start IP Address:
End IP Address:
Subnet Mask:

Remote IP: Subnet
Start IP Address:
End IP Address:
Subnet Mask:

Manual Policy Parameters

SPI-Incoming: 0x (Hex, 3-8 Chars)
Encryption Algorithm: 3DES
Key-In:
Key-Out:
(DES-8 Char & 3DES-24 Char)

SPI-Outgoing: 0x (Hex, 3-8 Chars)
Integrity Algorithm: SHA-1
Key-In:
Key-Out:
(MD5-16 Char & SHA-1-20 Char)

Auto Policy Parameters

SA Lifetime: 3600 Seconds
Encryption Algorithm: 3DES
Integrity Algorithm: SHA-1
□ PFS Key Group: DH Group 2 (1024 bit)
Select IKE Policy: F_Transfer

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

Other than the nature of the IP addresses, the settings that you must enter for IPv4 and IPv6 are identical with one exception. The IPv4 settings require a subnet mask but the IPv6 settings require a prefix length.

Setting	Description
General	
Policy Name	A descriptive name of the VPN policy for identification and management purposes. **Note:** The name is not supplied to the remote VPN endpoint.
Policy Type	From the menu, select a policy type: • **Auto Policy**. Some settings (the ones in the Manual Policy Parameters section) for the VPN tunnel are generated automatically. • **Manual Policy**. All settings must be specified manually, including the ones in the Manual Policy Parameters section.
Select Local Gateway	Select a WAN interface from the menu to specify the WAN interface for the local gateway.
Remote Endpoint	Select a radio button to specify how the remote endpoint is defined: • **IP Address**. Enter the IP address of the remote endpoint in the corresponding field to the right of the radio button. • **FQDN**. Enter the FQDN of the remote endpoint in the corresponding field to the right of the radio button.
Enable NetBIOS?	Select this check box to enable NetBIOS broadcasts to travel over the VPN tunnel. This feature is disabled by default. For more information about NetBIOS, see *Configure NetBIOS Bridging with IPSec VPN* on page 416.
Enable RollOver?	Select this check box to allow the VPN tunnel to roll over to the other WAN interface when the WAN mode is set to Auto-Rollover and an actual rollover occurs. This feature is disabled by default. Select a WAN interface from the menu.
Enable Auto Initiate	Select this check box to enable the VPN tunnel to autoestablish itself without the presence of any traffic. **Note:** For autoinitiation, 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 *Manually Add an IKE Policy* on page 368.

Setting	Description
Enable Keepalive	Select a radio button to specify if keep-alive is enabled: • **No**. Keep-alive requests are disabled for the VPN tunnel. This is the default setting. • **Yes**. Keep-alive requests are enabled for the VPN tunnel. Periodically, the VPN firewall sends keep-alive requests (ping packets) to the remote endpoint to keep the tunnel alive. You must specify the information in the following fields: - **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 counts**. 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. **Note:** For more information, see *Manage Keep-Alives and Dead Peer Detection* on page 411.
Traffic Selection	
Local IP	From the menu, 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, specify 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 menu, select the address or addresses that are part of the VPN tunnel on the remote endpoint. The selections for the **Remote IP** menu are the same as for the **Local IP** menu (see the previous row in this table).
Manual Policy Parameters **Note:** These fields apply only when you select **Manual Policy** from the **Policy Type** menu. When you specify the settings for the fields in this section, a security association (SA) is created.	
SPI-Incoming	The security parameters index (SPI) for the inbound policy. Enter a hexadecimal value between 3 and 8 characters (for example, 0x1234).

Setting	Description
Encryption Algorithm	From the menu, 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.
Key-Out	The encryption key for the outbound policy. The length of the key depends on the selected encryption algorithm: • **3DES**. Enter 24 characters. • **DES**. Enter 8 characters. • **AES-128**. Enter 16 characters. • **AES-192**. Enter 24 characters. • **AES-256**. Enter 32 characters.
SPI-Outgoing	The security parameters index (SPI) for the outbound policy. Enter a hexadecimal value between 3 and 8 characters (for example, 0x1234).
Integrity Algorithm	From the menu, 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.

Setting	Description
Auto Policy Parameters **Note:** These fields apply only when you select **Manual Policy** from the **Policy Type** menu.	
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 **SA Lifetime** menu on the right, select how you must specify the SA lifetime in the **SA Lifetime** field on the left: • **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 menu, select one 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.
Integrity Algorithm	From the menu, 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 the **PFS Key Group** check box on the left to enable Perfect Forward Secrecy (PFS and select a Diffie-Hellman (DH) group from the corresponding menu on the right. The DH Group sets the strength of the algorithm in bits. The higher the group, the more secure the exchange. From the menu, 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.

10. Click the **Apply** button.

    Your settings are saved. The VPN policy is added to the List of VPN Policies table.

Change a VPN Policy

The following procedure describes how to change an existing VPN policy that was added either automatically or manually.

➢ To change a VPN policy:

1. On your computer, launch an Internet browser.

2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **VPN > IPSec VPN > VPN Policies**.

   The VPN Policies screen displays the IPv4 settings.

7. To change a VPN policy for IPv6 instead of IPv4, in the upper right, select the **IPv6** radio button.

   The VPN Policies screen displays the IPv6 settings.

8. In the List of VPN Policies table, click the **Edit** button for the VPN policy that you want to change.

   The Edit VPN Policy screen displays.

9. Change the settings.

   For information about the settings, see *Manually Add a VPN Policy* on page 381.

10. Click the **Apply** button.

    Your settings are saved. The modified VPN policy displays in the List of VPN Policies table on the VPN Policies screen.

Enable, Disable, or Remove One or More Existing VPN Policies

The following procedure describes how to enable or disable one or more existing VPN policies or remove one or more VPN policies that you no longer need.

➢ **To enable, disable, or remove one or more VPN polices:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **VPN > IPSec VPN > VPN Policies**.

   The VPN Policies screen displays the IPv4 settings.

7. To change a VPN policy for IPv6 instead of IPv4, in the upper right, select the **IPv6** radio button.

   The VPN Policies screen displays the IPv6 settings.

8. In the List of VPN Policies table, select the check box to the left of each policy that you want to either enable, disable, or remove or click the **Select All** button to select all VPN policies.
9. Take one of the following actions:
   - Click the **Enable** button.

     The selected VPN policies are enabled. The green circle to the left of each selected VPN policy turns green.

   - Click the **Disable** button.

     The selected VPN policies are disabled. The green circle to the left of each selected VPN policy turns gray.

   - Click the **Delete** button.

     The selected VPN policies are removed from the List of VPN Policies table.

Configure Extended Authentication (XAUTH)

The following sections provide information about how to configure extended authentication (XAUTH):

- *Extended Authentication Overview*
- *Enable and Configure Extended Authentication for VPN Clients*
- *RADIUS*
- *Configure the RADIUS Servers for the VPN Firewall’s RADIUS Client*

Extended Authentication Overview

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. Extended authentication (XAUTH) provides the mechanism for requesting individual authentication information from the user. The VPN firewall's 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 change an IKE policy. The VPN firewall provides two types of XAUTH:

- **Edge device**. The VPN firewall functions as a VPN concentrator on which one or more gateway tunnels terminate. Specify the authentication type that must be used during verification of the credentials of the remote VPN gateways: the VPN firewall's user database, an external RADIUS-PAP server, or an external RADIUS-CHAP server.
- **IPSec host**. The VPN firewall functions as a VPN client of the remote gateway. Authentication occurs at 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.

After you have enabled XAUTH, you must establish user accounts in the VPN firewall's local user database to be authenticated against XAUTH or you must enable a RADIUS-CHAP or RADIUS-PAP server.

If you use a RADIUS-PAP server for authentication, XAUTH first checks the VPN firewall local user database for the user credentials. If the user account is not present, the VPN firewall then connects to a RADIUS server.

Enable and Configure Extended Authentication for VPN Clients

The following procedure describes how to enable and configure extended authentication (XAUTH) for VPN clients.

➢ **To enable and configure XAUTH:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. If the IKE policy for which you want to configure XAUTH is associated with a VPN policy, first disable the VPN policy:

   a. Select **VPN > IPSec VPN > VPN Policies**.

      The VPN Policies screen displays the IPv4 settings.

   b. To disable a VPN policy for IPv6 instead of IPv4, in the upper right, select the **IPv6** radio button.

      The VPN Policies screen displays the IPv6 settings.

   c. In the List of VPN policies table, select the VPN policy that is associated with the IKE policy that you want to change.

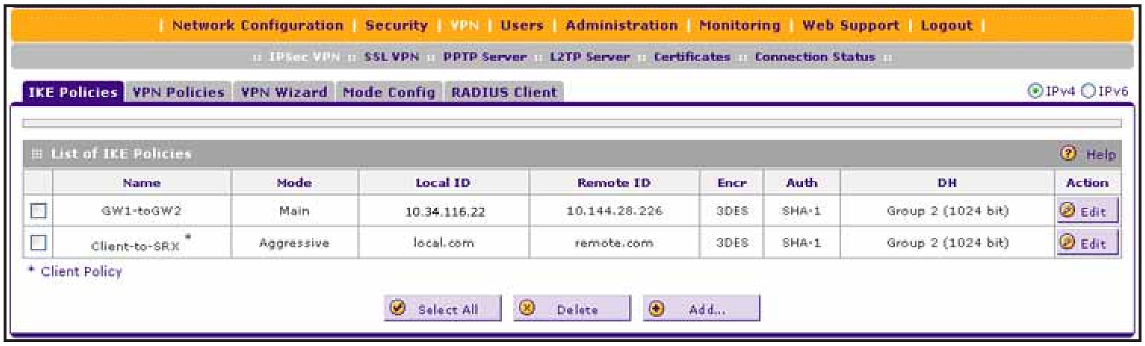
   Note: When you use the VPN IPsec Wizard, the VPN and IKE policies that are added automatically have the same name.

   d. Click the **Disable** button.

      The VPN policy is disabled. The green circle to the left of the VPN policy turns gray.

7. Select **VPN > IPSec VPN**.

   The IPSec VPN submenu tabs display with the IKE Policies screen for IPv4 in view.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
● IPv4 ○ IPv6
Help
Select All
Delete
Add...

List of IKE Policies

	Name	Mode	Local ID	Remote ID	Encr	Auth	DH	Action
□	GW1-toGW2	Main	10.34.116.22	10.144.28.226	3DES	SHA-1	Group 2 (1024 bit)	Edit
□	Client-to-SRX *	Aggressive	local.com	remote.com	3DES	SHA-1	Group 2 (1024 bit)	Edit

* Client Policy

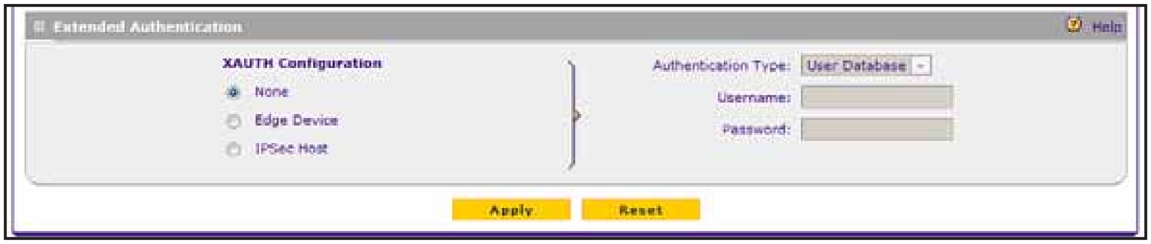
8. To change an IKE policy for IPv6 instead of IPv4, in the upper right, select the **IPv6** radio button.

   The IKE Policies screen for IPv6 displays.

9. In the List of IKE Policies table, click the **Edit** button for the IKE policy for which you want to enable and configure XAUTH.

   The Edit IKE Policy screen displays.

10. Locate the Extended Authentication section.



Extended Authentication

XAUTH Configuration

● None

○ Edge Device

○ IPSec Host

Authentication Type: User Database

Username:

Password:

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

Setting	Description
Select a radio button to specify whether Extended Authentication (XAUTH) is enabled and, if enabled, which device is used to verify user account information: • **None**. XAUTH is disabled. This the default setting. • **Edge Device**. The VPN firewall functions as a VPN concentrator on which one or more gateway tunnels terminate. The authentication modes that are available for this configuration are **User Database**, **RADIUS PAP**, and **RADIUS CHAP**. • **IPSec Host**. The VPN firewall functions as a VPN client of the remote gateway. In this configuration, the VPN firewall is authenticated by a remote gateway with a user name and password combination.	
Authentication Type	For an Edge Device configuration, from the menu, select an authentication type: • **User Database**. XAUTH occurs through the VPN firewall's local user database. For information about adding users, see *Manage User Accounts* on page 498. • **Radius PAP**. XAUTH occurs through RADIUS Password Authentication Protocol (PAP). The VPN firewall first checks its local user database. If the user account is not present in the local user database, the VPN firewall connects to a RADIUS server. For more information, see *Configure the RADIUS Servers for the VPN Firewall's RADIUS Client* on page 392. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see *Configure the RADIUS Servers for the VPN Firewall's RADIUS Client* on page 392.
Username	The user name for XAUTH.
Password	The password for XAUTH.

12. Click the **Apply** button.

    Your settings are saved.

13. If you disabled the VPN policy with which the IKE policy for which you configured XAUTH is associated, reenable the VPN policy:

    a. Select **VPN > IPSec VPN > VPN Policies**.

       The VPN Policies screen displays the IPv4 settings.

    b. To reenable a VPN policy for IPv6 instead of IPv4, in the upper right, select the **IPv6** radio button.

       The VPN Policies screen displays the IPv6 settings.

    c. In the List of VPN policies table, select the VPN policy that is associated with the IKE policy that you changed.

d. Click the **Enable** button.

The VPN policy is reenabled. The gray circle to the left of the VPN policy turns green.

RADIUS

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.

After you configure the RADIUS servers for the VPN firewall's RADIUS client (see *Configure the RADIUS Servers for the VPN Firewall's RADIUS Client* on page 392), you can select the RADIUS authentication protocol (PAP or CHAP) when you add or change an IKE policy. For more information, see *Manually Add an IKE Policy* on page 368 and *Change an IKE Policy* on page 375.

Configure the RADIUS Servers for the VPN Firewall's RADIUS Client

The following procedure describes how to configure the primary and backup RADIUS servers for the VPN firewall's RADIUS client, which is used for extended authentication.

➤ **To configure primary and backup RADIUS servers for the VPN firewall's RADIUS client:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

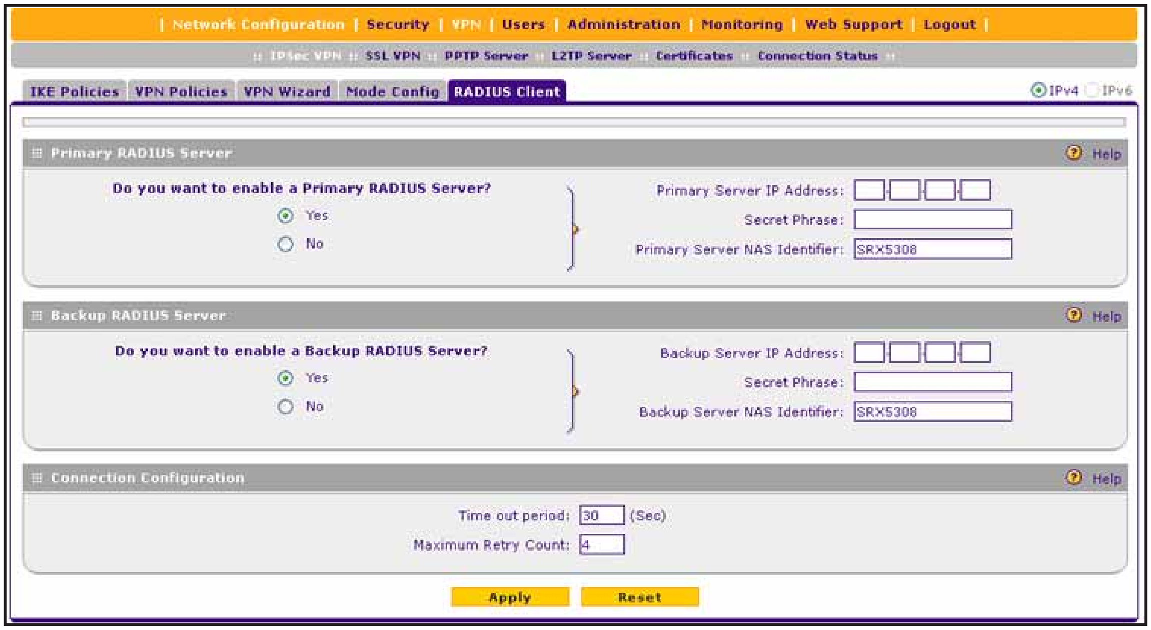
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **VPN > IPSec VPN > RADIUS Client**.

   The RADIUS Client screen displays.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
● IPv4 ○ IPv6
Help
Apply
Reset

Primary RADIUS Server

Do you want to enable a Primary RADIUS Server?
● Yes
○ No

Primary Server IP Address:
Secret Phrase:
Primary Server NAS Identifier: SRX5308

Backup RADIUS Server

Do you want to enable a Backup RADIUS Server?
● Yes
○ No

Backup Server IP Address:
Secret Phrase:
Backup Server NAS Identifier: SRX5308

Connection Configuration

Time out period: 30 (Sec)
Maximum Retry Count: 4

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

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. By default, **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. 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 the **Primary Server NAS Identifier** field.
Backup RADIUS Server	

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. By default, 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. 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 the **Backup Server NAS Identifier** field.
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.

8. Click the **Apply** button.

   Your settings are saved.

Assign IPv4 Addresses to Remote Users

The following sections provide information about how to configure Mode Config:

- *Mode Config Overview*
- *Configure Mode Config Operation on the VPN Firewall*
- *Configure the NETGEAR ProSAFE VPN Client for Mode Config Operation*
- *Test the Mode Config Connection*
- *Change a Mode Config Record*
- *Remove One or More Mode Config Records*

Mode Config Overview

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. The VPN firewall assigns to remote users IP addresses from a secured network space so that the 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.

During the establishment of a VPN tunnel, 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 you specify in the Traffic Tunnel Security Level section of the Mode Config record. For more information, see *Configure Mode Config Operation on the VPN Firewall* on page 395.

Note: After configuring a Mode Config record, you must manually add or change an IKE policy and select the newly created Mode Config record (see *Configure Mode Config Operation on the VPN Firewall* on page 395).

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. The following procedure lets you create a new IKE policy rather than adding the Mode Config record to an existing IKE policy.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

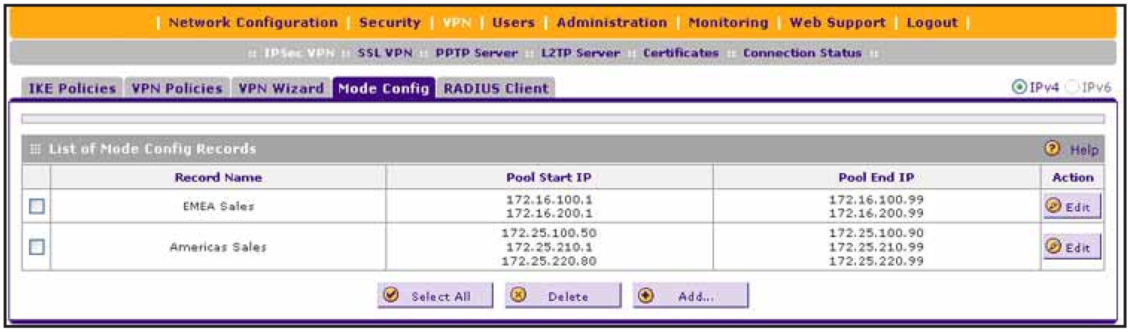
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > IPSec VPN > Mode Config**.

The Mode Config screen displays.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
● IPv4 ○ IPv6
Help
Select All
Delete
Add...

List of Mode Config Records

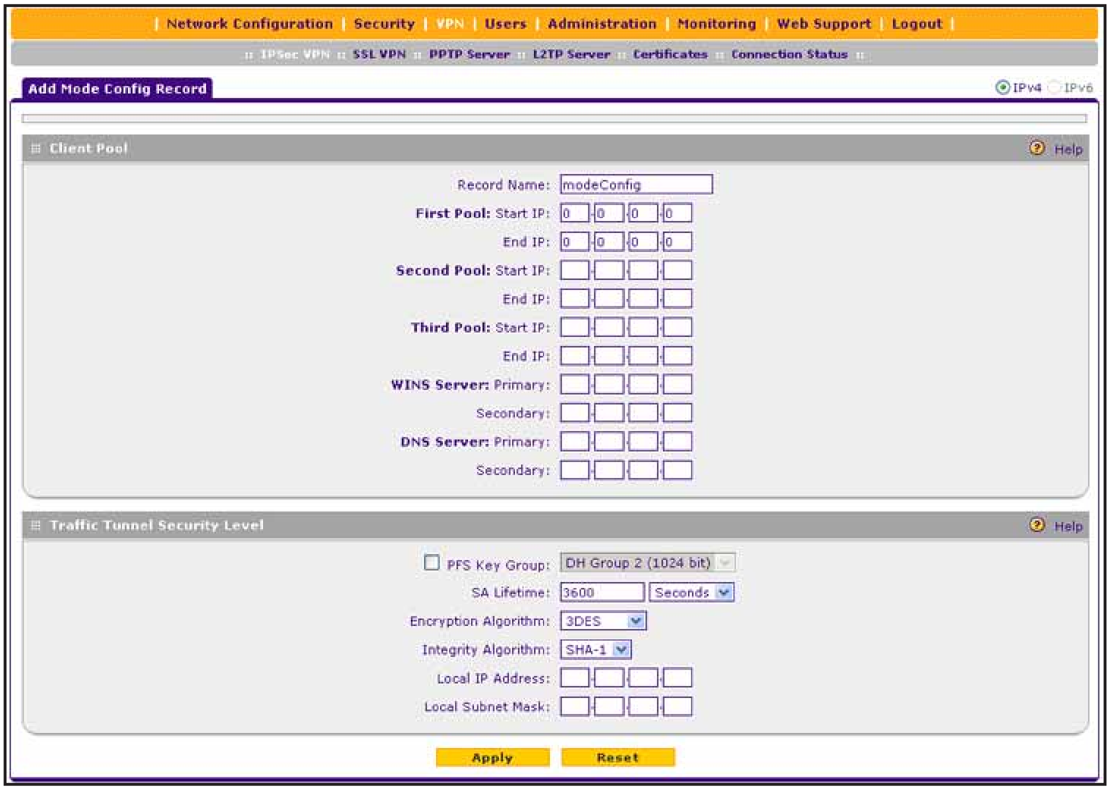
	Record Name	Pool Start IP	Pool End IP	Action
□	EMEA Sales	172.16.100.1 172.16.200.1	172.16.100.99 172.16.200.99	Edit
□	Americas Sales	172.25.100.50 172.25.210.1 172.25.220.80	172.25.100.90 172.25.210.99 172.25.220.99	Edit

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

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

7. Under the List of Mode Config Records table, click the **Add** button.

   The Add Mode Config Record screen displays.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
Add Mode Config Record
● IPv4 ○ IPv6
Help
Help
Apply
Reset

Client Pool

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:

Traffic Tunnel Security Level

□ 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:

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

Setting	Description
Client Pool	
Record Name	A descriptive name of the Mode Config record for identification and management purposes.
First Pool	Assign at least one range of IP pool addresses in the **First Pool** fields to enable the VPN firewall to allocate these to remote VPN clients. The **Second Pool** and **Third Pool** fields are optional. To specify any client pool, enter the starting IP address for the pool in the **Starting IP** field, and enter the ending IP address for the pool in the **Ending IP** field. **Note:** No IP pool must be within the range of the local network IP addresses. Use a different range of private IP addresses such as 172.16.xxx.xx.
Second Pool	
Third Pool	
WINS Server	If there is a WINS server on the local network, enter its IP address in the **Primary** field. You can enter the IP address of a second WINS server in the **Secondary** field.
DNS Server	In the **Primary** field, enter the IP address of the DNS server that is used by remote VPN clients. You can enter the IP address of a second DNS server in the **Secondary** field.
Traffic Tunnel Security Level **Note:** Generally, the default settings work well for a Mode Config configuration.	
PFS Key Group	Select the **PFS Key Group** check box on the left to enable Perfect Forward Secrecy (PFS), and select a Diffie-Hellman (DH) group from the corresponding menu on the right. The DH Group sets the strength of the algorithm in bits. The higher the group, the more secure the exchange. From the menu, select the 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 **SA Lifetime** menu on the right, select how you must specify the SA lifetime in the **SA Lifetime** field on the left: • **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 menu, 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.

Setting	Description
Integrity Algorithm	From the menu, 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 to which remote VPN clients have access. If you do not specify a local IP address, the VPN firewall's default LAN IP address is used (by default, 192.168.1.1).
Local Subnet Mask	The local subnet mask. Typically, this is 255.255.255.0. **Note:** If you do not specify a local IP address, you do not need to specify a subnet either.

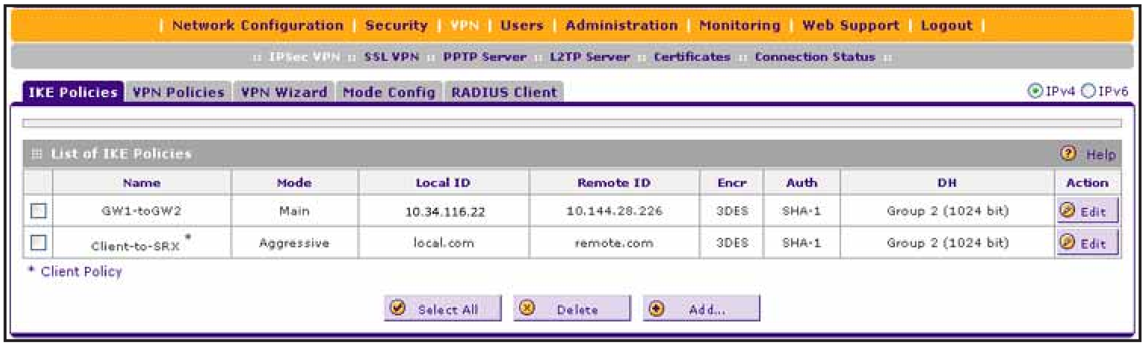
9. Click the **Apply** button.

   Your settings are saved. The new Mode Config record is added to the List of Mode Config Records table.

   Continue the Mode Config configuration procedure by configuring an IKE policy. (You can also change an existing IKE policy.)

10. Select **VPN > IPSec VPN**.

    The IPSec VPN submenu tabs display with the IKE Policies screen for IPv4 in view.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
VPN Wizard
Mode Config
RADIUS Client
● IPv4 ○ IPv6
List of IKE Policies
Help
Select All
Delete
Add...

	Name	Mode	Local ID	Remote ID	Encr	Auth	DH	Action
□	GW1-toGW2	Main	10.34.116.22	10.144.28.226	3DES	SHA-1	Group 2 (1024 bit)	Edit
□	Client-to-SRX *	Aggressive	local.com	remote.com	3DES	SHA-1	Group 2 (1024 bit)	Edit

* Client Policy

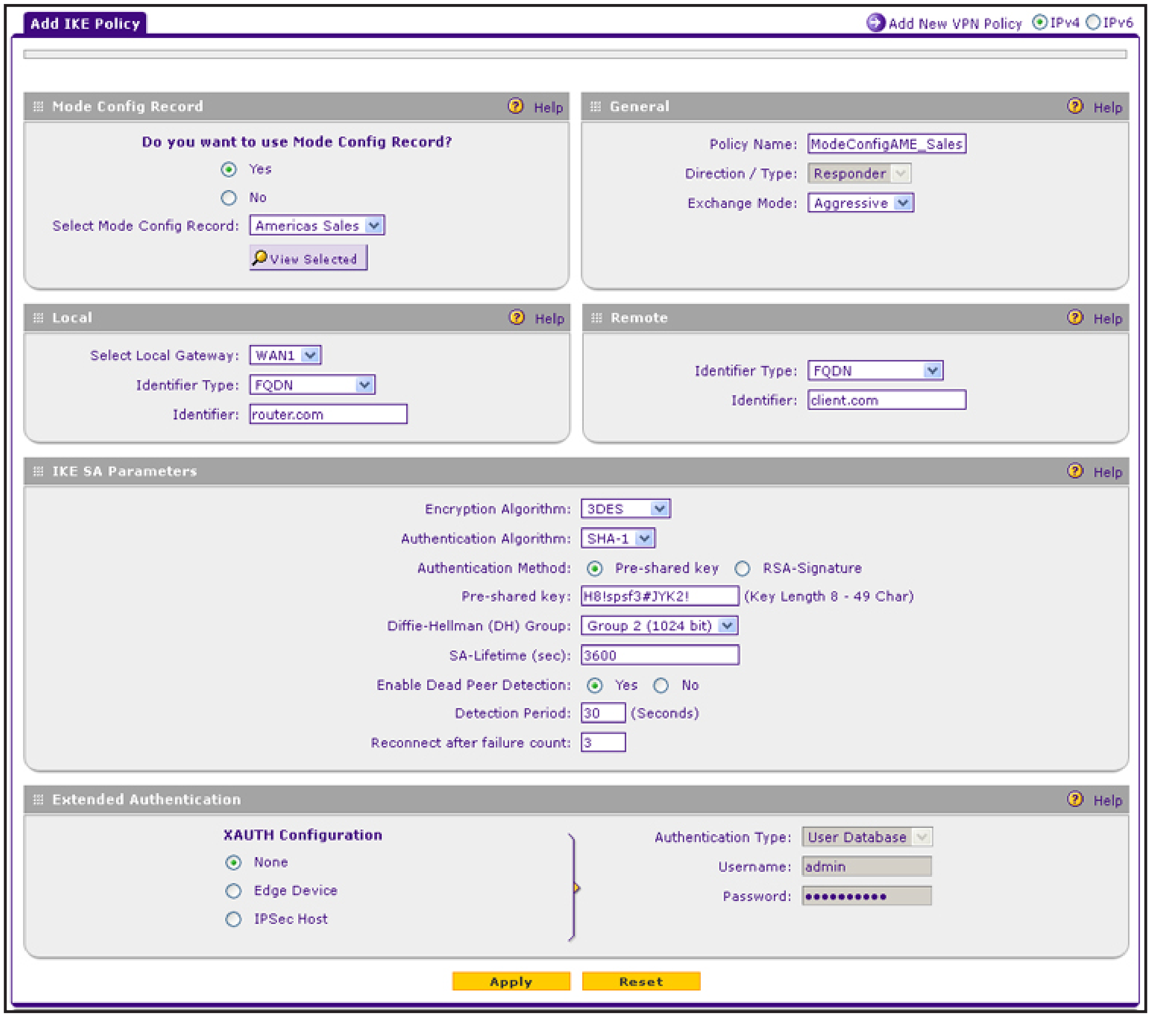
11. To add an IKE policy for IPv6 instead of IPv4, in the upper right, select the **IPv6** radio button.

    The IKE Policies screen for IPv6 displays.

12. Under the List of IKE Policies table, click the **Add** button.

    The Add IKE Policy screen displays. The Add IKE Policy screen for IPv4 is identical to the Add IKE Policy screen for IPv6.

Note: You can configure an IPv6 IKE policy to assign IPv4 addresses to clients, but you cannot assign IPv6 addresses to clients.



Mode Config Record

Do you want to use Mode Config Record?

● Yes

○ No

Select Mode Config Record: Americas Sales

View Selected

General

Policy Name: ModeConfigAME_Sales

Direction / Type: Responder

Exchange Mode: Aggressive

Local

Select Local Gateway: WAN1

Identifier Type: FQDN

Identifier: router.com

Remote

Identifier Type: FQDN

Identifier: client.com

IKE SA Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

Authentication Method: ● Pre-shared key ○ RSA-Signature

Pre-shared key: H8!spsf3#JYK2! (Key Length 8 - 49 Char)

Diffie-Hellman (DH) Group: Group 2 (1024 bit)

SA-Lifetime (sec): 3600

Enable Dead Peer Detection: ● Yes ○ No

Detection Period: 30 (Seconds)

Reconnect after failure count: 3

Extended Authentication

XAUTH Configuration

● None

○ Edge Device

○ IPSec Host

Authentication Type: User Database

Username: admin

Password: ••••••••••

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

Note: The IKE policy settings that are described in the following table are specifically for a Mode Config configuration. For information about general IKE policy settings, see *Manually Add an IKE Policy* on page 368.

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 menu, select the Mode Config record that you created in *Step 9*. This example uses NA Sales.

Setting	Description
General	
Policy Name	A descriptive name of the IKE policy for identification and management purposes. This example uses ModeConfigAME_Sales. **Note:** The name is not supplied to the remote VPN endpoint.
Direction / Type	Responder is automatically selected when you select the Mode Config record in the Mode Config Record section. 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	
Select Local Gateway	Select a WAN interface from the menu to specify the WAN interface for the local gateway.
Identifier Type	From the menu, select **FQDN**. **Note:** Mode Config requires that the VPN firewall (that is, the local endpoint) is defined by an FQDN.
Identifier	Enter an FQDN for the VPN firewall. This example uses router.com.
Remote	
Identifier Type	From the menu, 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. This example uses client.com.
IKE SA Parameters	
Encryption Algorithm	To negotiate the security association (SA), from the menu, select the **3DES** algorithm.
Authentication Algorithm	From the menu, select the **SHA-1** algorithm to be used in the VPN header for the authentication process.
Authentication Method	Select **Pre-shared key** as the authentication method, and enter a key in the **Pre-shared key** field.
Pre-shared key	A key with a minimum length of 8 characters and no more than 49 characters. Do not use a double quote ("), single quote ('), or space in the key. This example uses H8!spsf3#JYK2!.
Diffie-Hellman (DH) Group	The DH Group sets the strength of the algorithm in bits. From the menu, select **Group 2 (1024 bit)**.
SA-Lifetime (sec)	The period in seconds for which the IKE SA is valid. When the period times out, the next rekeying occurs. The default setting is 28800 seconds (eight hours). However, for a Mode Config configuration, NETGEAR recommends 3600 seconds (one hour).

Setting	Description
Enable Dead Peer Detection	Select a radio button to specify whether Dead Peer Detection (DPD) is enabled: • **No**. This feature is disabled. This is the default setting. • **Yes**. This feature is enabled. When the VPN firewall detects an IKE connection failure, it removes 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. **Note:** For more information, see *Manage Keep-Alives and Dead Peer Detection* on page 411.
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.
Extended Authentication	
XAUTH Configuration	Select a radio button to specify whether Extended Authentication (XAUTH) is enabled and, if enabled, which device is used to verify user account information: • **None**. XAUTH is disabled. This the default setting. • **Edge Device**. The VPN firewall functions as a VPN concentrator on which one or more gateway tunnels terminate. The authentication modes that are available for this configuration are User Database, RADIUS PAP, and RADIUS CHAP. • **IPSec Host**. The VPN firewall functions as a VPN client of the remote gateway. In this configuration, the VPN firewall is authenticated by a remote gateway with a user name and password combination. **Note:** For more information about XAUTH and its authentication modes, see *Enable and Configure Extended Authentication for VPN Clients* on page 389.
Authentication Type	If you select **Edge Device** from the **AUTH Configuration** menu, you must select an authentication type from the **Authentication Type** menu: • **User Database**. XAUTH occurs through the VPN firewall's user database. For information about adding users, see *Manage User Accounts* on page 498. • **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 *Configure the RADIUS Servers for the VPN Firewall's RADIUS Client* on page 392. • **Radius CHAP**. XAUTH occurs through RADIUS Challenge Handshake Authentication Protocol (CHAP). For more information, see *Configure the RADIUS Servers for the VPN Firewall's RADIUS Client* on page 392.
Username	The user name for XAUTH.
Password	The password for XAUTH.

14. Click the **Apply** button.

Your settings are saved. The IKE policy that includes the Mode Config record is added to the List of IKE Policies table. You can associate the IKE policy with a VPN policy.

Configure the NETGEAR ProSAFE VPN Client for Mode Config Operation

Note: In this section, the NETGEAR ProSAFE VPN Client is referred to as the VPN client.

When the Mode Config feature is enabled, the following information is negotiated between the VPN client and the VPN firewall during the authentication phase:

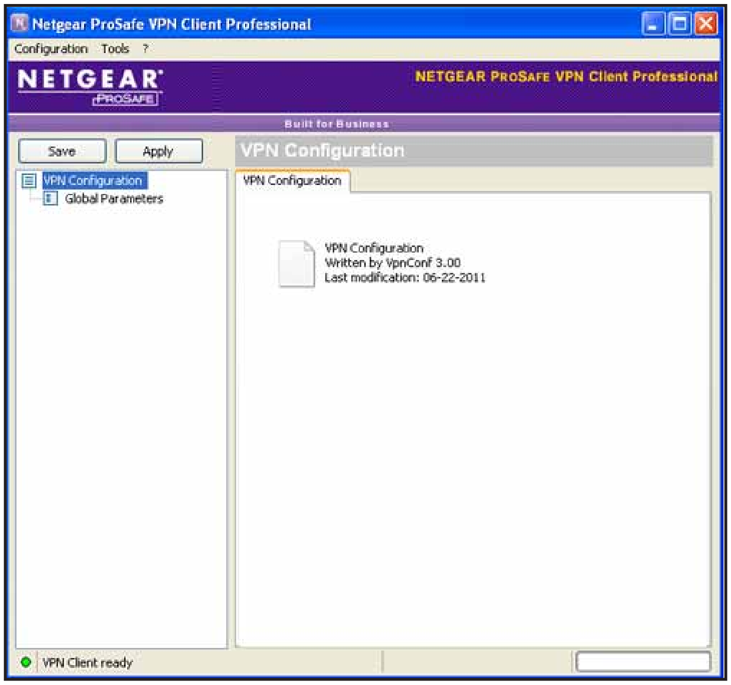
- Virtual IP address of the VPN client
- DNS server address (optional)
- WINS server address (optional)

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 (see *Test the Mode Config Connection* on page 408).

Note: An IP address that is allocated to a VPN client is released only after the VPN client has gracefully disconnected or after the SA liftetime for the connection has timed out.

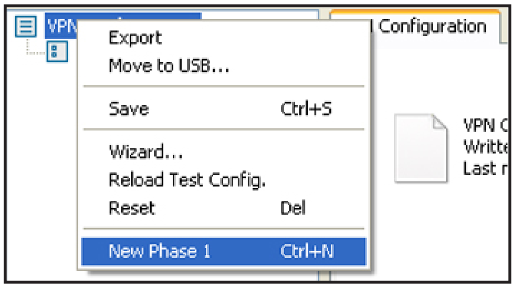
➢ **To use the Configuration Wizard to set up a VPN connection between the VPN client and the VPN firewall with a Mode Config configuration:**

1. On the computer that has the VPN client installed, 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

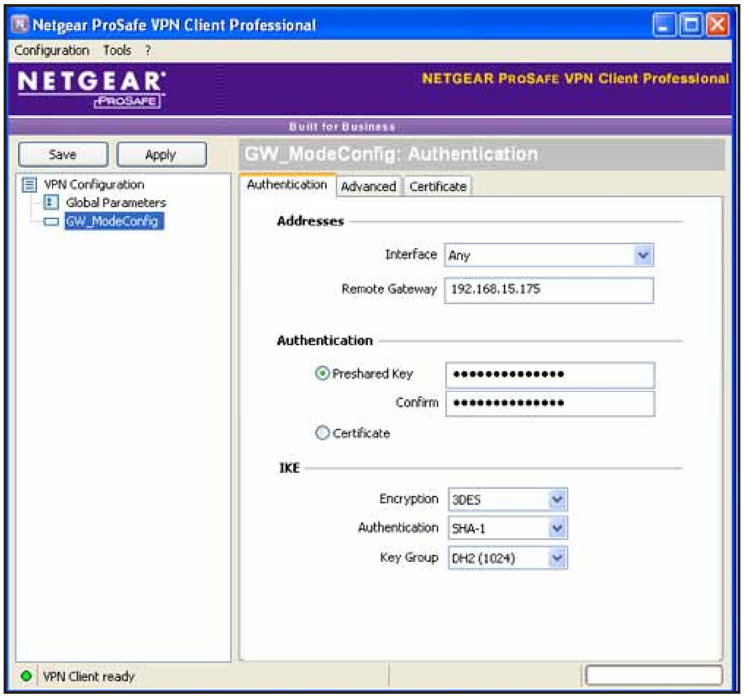
2. In the tree list pane of the Configuration Panel screen, right-click **VPN Configuration**, and select **New Phase 1**.



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.

Note: This is the name for the authentication phase that is used only for the VPN client, not during IKE negotiation. You can view and change this name in the tree list pane. This name must be a unique name.

The Authentication pane displays in the Configuration Panel screen, with the Authentication tab selected by default.



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)

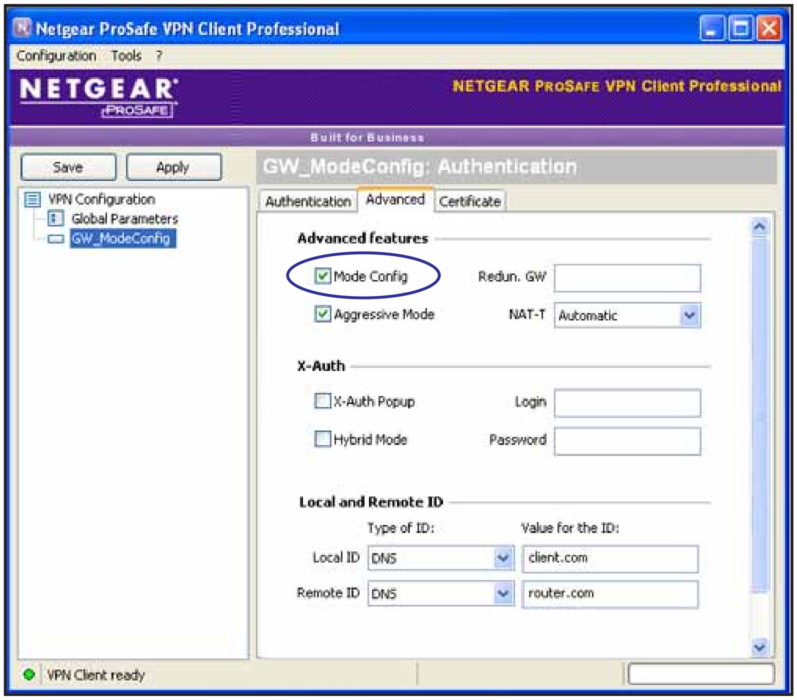
4. Specify the settings that are described in the following table.

Setting	Description
Interface	From the menu, select **Any**.
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 and configure the following settings: 1. Enter the pre-shared key that you already specified on the VPN firewall. For example, enter **H8!spsf3#JYK2!**. 2. In the **Confirm** field, enter the pre-shared key again.
Encryption	From the menu, select the **3DES** encryption algorithm.
Authentication	From the menu, select the **SHA1** authentication algorithm.
Key Group	From the menu, 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. Click the **Save** button.

   Your settings are saved.

6. 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	client.com
Remote ID	DNS	router.com

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

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	From the menu, select **Automatic** to enable the VPN client and VPN firewall to negotiate NAT-T.
Local and Remote ID	
Local ID	From the **Local ID** menu, select **DNS** as the type of ID 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	From the **Remote ID** menu, select **DNS** as the type of ID because you specified an FQDN in the VPN firewall configuration. As the value of the ID, enter **router.com** as the remote ID for the VPN firewall. **Note:** The local ID on the VPN firewall is the remote ID on the VPN client.

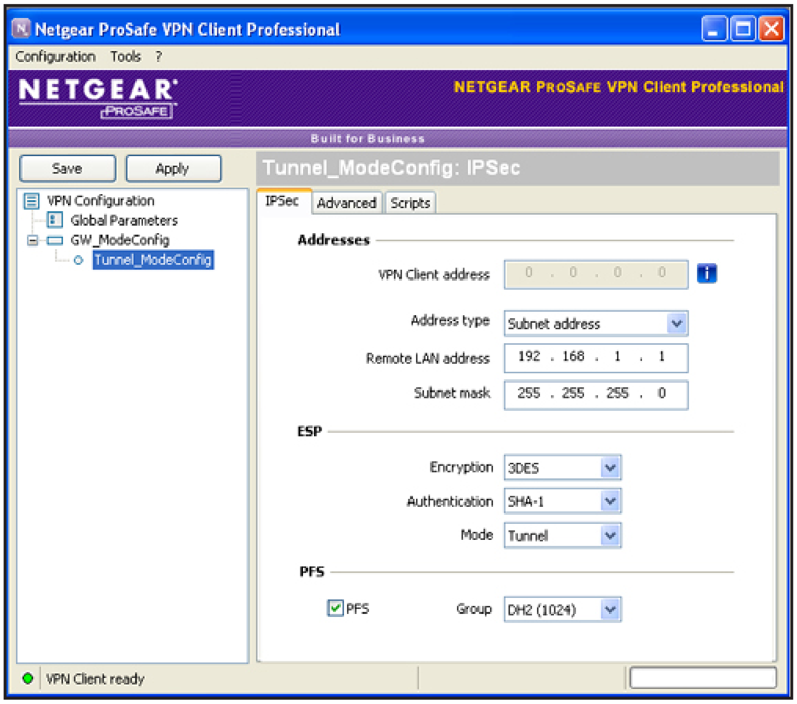
8. Click the **Save** button.

   Your settings are saved. Continue the Mode Config configuration of the VPN client with the IPSec configuration.

9. In the tree list pane of the Configuration Panel screen, right-click the **GW_ModeConfig** authentication phase name and select **New Phase 2**.
10. Change the name of the IPSec configuration (the default is Tunnel):
    a. Right-click the IPSec configuration name.
    b. Select **Rename**.
    c. Type **Tunnel_ModeConfig**.
    d. Click anywhere in the tree list pane.

Note: This is the name for the IPSec configuration that is used only for the VPN client, not during IPSec negotiation. You can view and change this name in the tree list pane. This name must be a unique name.

The IPSec pane displays in the Configuration Panel screen, with the IPSec tab selected by default:



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)

VPN Client ready

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

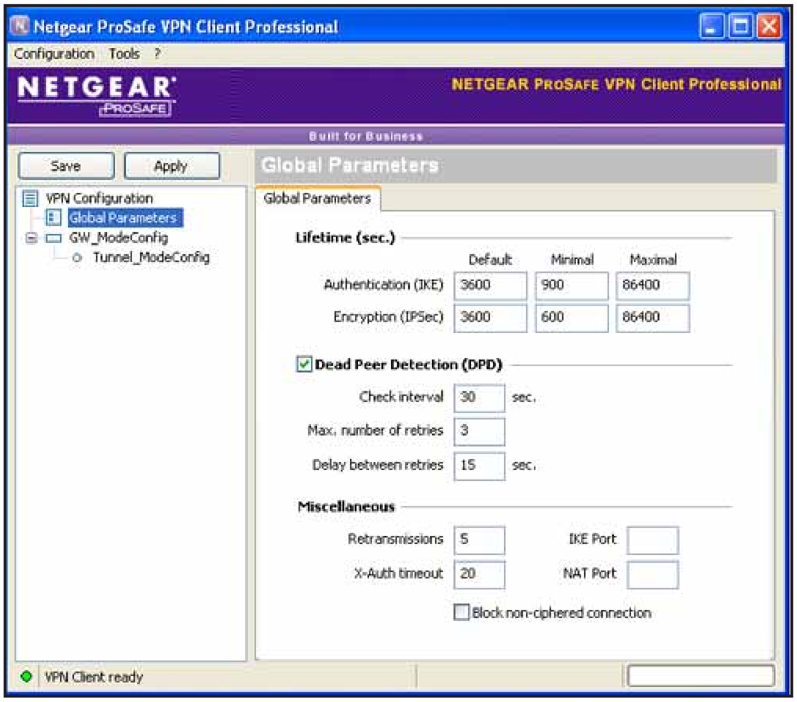
Setting	Description
VPN Client address	This field is masked out because Mode Config is selected. After an IPSec connection is established, the IP address that is issued by the VPN firewall displays in this field (see *Test the Mode Config Connection* on page 408).
Address Type	From the menu, select **Subnet address**.

Setting	Description
Remote LAN address	The address that you must enter depends on whether you specified a local IP address for the Mode Config record on the VPN firewall: • If you did not specify a local IP address for the Mode Config record, enter the VPN firewall's default LAN IP address in the **Remote LAN Address** field as the remote host address that opens the VPN tunnel. For example, enter **192.168.1.1**. • If you specified a local IP address for the Mode Config record, enter that address in the **Remote LAN Address** field as the remote host address that opens the VPN tunnel. For more information about the local LAN address for the Mode Config record, see *Configure Mode Config Operation on the VPN Firewall* on page 395, specifically the description of the **Local IP Address** field on the Add Mode Config Record screen.
Subnet mask	The address that you must enter depends on whether you specified a local subnet mask for the Mode Config record on the VPN firewall: • If you did not specify a local subnet mask for the Mode Config record, in the **Subnet mask** field, enter the VPN firewall's default LAN subnet mask. For example, enter **255.255.255.0**. • If you specified a local subnet mask for the Mode Config record, in the **Subnet mask** field, enter that subnet mask. For more information about the local subnet mask for the Mode Config record, see *Configure Mode Config Operation on the VPN Firewall* on page 395, specifically the description of the **Local Subnet Mask** field on the Add Mode Config Record screen.
Encryption	From the menu, select **3DES** as the encryption algorithm.
Authentication	From the menu, select **SHA-1** as the authentication algorithm.
Mode	From the menu, select **Tunnel** as the encapsulation mode.
PFS and Group	Select the **PFS** check box and from the menu, select the **DH2 (1024)** key group. **Note:** On the VPN firewall, this key group is referred to as Diffie-Hellman Group 2 (1024 bit).

12. Click the **Save** button.

    Your settings are saved. Continue the Mode Config configuration of the VPN client with the global parameters.

13. Click **Global Parameters** in the left column of the Configuration Panel screen. The Global Parameters pane displays in the Configuration Panel screen:



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

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

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

    - **Encryption (IPSec)**, **Default**. Enter **3600** seconds.
15. 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.
16. Click the **Save** button.

    Your settings are saved.

    The Mode Config configuration of the VPN client is now complete.

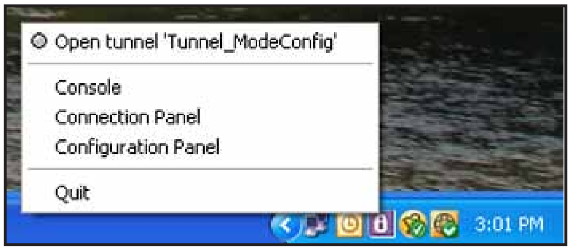
Test the Mode Config Connection

Note: In this section, the NETGEAR ProSAFE VPN Client is referred to as the VPN client.

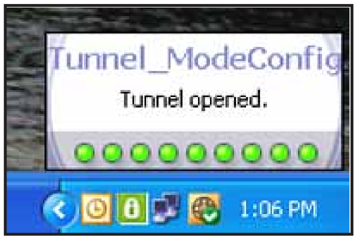
After you have set up the Mode Config configuration on both the VPN client and the VPN firewall, test the configuration to make sure that the VPN firewall does assign an IP address to the VPN client.

➤ **To test the Mode Config connection from the VPN client to the VPN firewall:**

1. On the computer that has the VPN client installed, right-click the system tray icon and select **Open tunnel ‘Tunnel_ModeConfig’**.



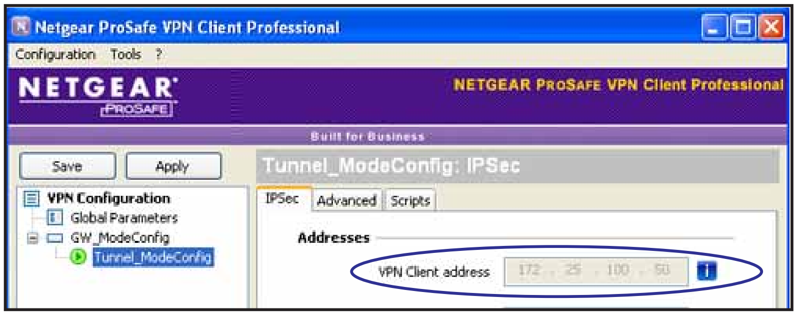
When the tunnel opens successfully, the *Tunnel opened* message displays above the system tray and the VPN client displays a green icon in the system tray.


Tunnel_ModeConfig

Tunnel opened.

2. Verify that the VPN firewall issues an IP address to the VPN client.
3. In the tree list pane of the Configuration Panel screen, right-click the IPSec configuration.

In the following figure, the name of the IPSec configuration is GW_ModeConfig. (The default name is Tunnel.) The figure shows the upper part of the IPSec pane of the VPN client only.



Tunnel_ModeConfig: IPSec

Addresses

VPN Client address 172 . 25 . 100 . 50

This IP address displays in the **VPN Client address** field.

4. From the client computer, try to access a device or web address on the LAN of the VPN firewall.

Change a Mode Config Record

The following procedure describes how to change an existing Mode Config record.

Note: Before you change a Mode Config record, make sure that it is not used in an IKE policy. If it is, temporarily remove the Mode Config record from the IKE policy. For information about how to change an IKE policy, see *Change an IKE Policy* on page 375.

➢ **To change a Mode Config record:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > IPSec VPN > Mode Config**.

   The Mode Config screen displays.
7. In the List of Mode Config Records table, click the **Edit** button for the record that you want to change.

   The Edit Mode Config Record screen displays.
8. Change the settings.

   For information about the settings, *Configure Mode Config Operation on the VPN Firewall* on page 395.
9. Click the **Apply** button.

   Your settings are saved. The modified Mode Config record displays in the List of Mode Config Records table on the Mode Config screen.

Remove One or More Mode Config Records

The following procedure describes how to remove one or more Mode Config records that you do no longer need in IKE policies.

Note: Before you remove a Mode Config record, make sure that it is not used in an IKE policy. If it is, remove the Mode Config record from the IKE policy. For information about how to change an IKE policy, see *Change an IKE Policy* on page 375.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > IPSec VPN > Mode Config**.

   The Mode Config screen displays.
7. In the List of Mode Config Records table, select the check box to the left of each record that you want to remove or click the **Select All** button to select all records.
8. Click the **Delete** button.

   The selected Mode Config records are removed from the List of Mode Config Records table.

Manage Keep-Alives and Dead Peer Detection

The following sections provide information about how to configure keep-alives and Dead Peer Detection:

- *Keep-Alive and Dead Peer Detection Overview*
- *Configure Keep-Alives*
- *Configure Dead Peer Detection*

Keep-Alive and Dead Peer Detection Overview

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.

DPD lets the VPN firewall maintain the IKE SA by exchanging periodic messages with the remote VPN peer. For DPD to function, the peer VPN device on the other end of the tunnel also must support DPD.

The keep-alive feature, though less reliable than DPD, does not require any support from the peer device. The keep-alive feature maintains the IPSec SA by sending periodic ping requests to a host across the tunnel and monitoring the replies.

Configure Keep-Alives

The following procedure describes how to configure the keep-alive feature for an existing VPN policy.

➢ **To configure the keep-alive feature for an existing VPN policy:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > IPSec VPN > VPN Policies**.

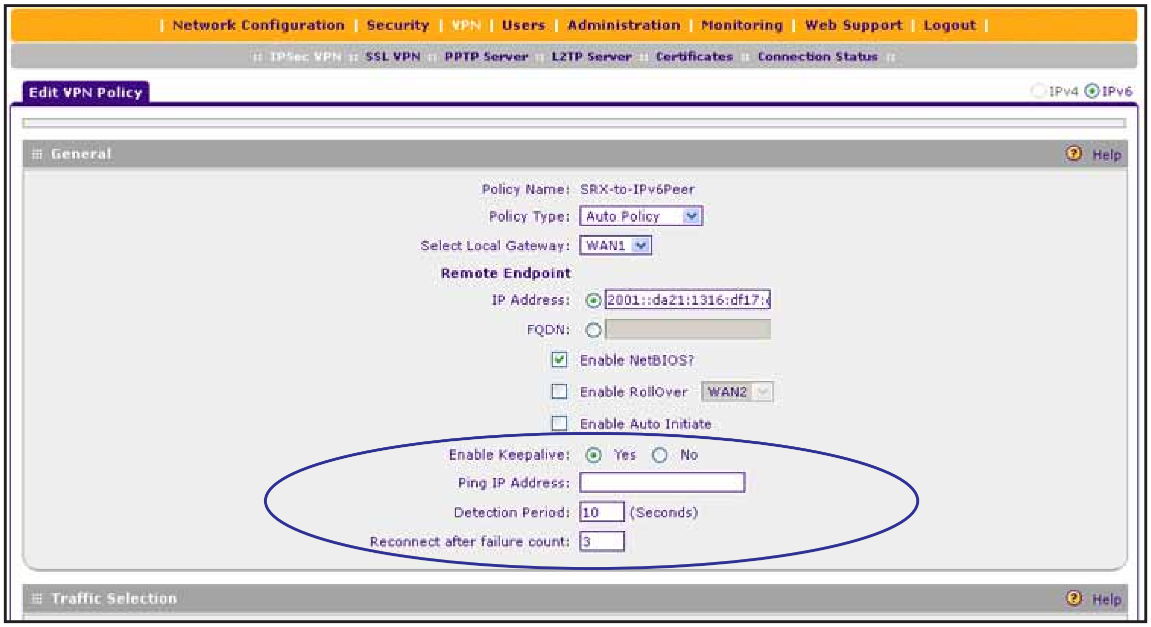
The VPN Policies screen displays the IPv4 settings.

7. To change a VPN policy for IPv6 instead of IPv4, in the upper right, select the **IPv6** radio button.

   The VPN Policies screen displays the IPv6 settings.

8. In the List of VPN Policies table, click the **Edit** button for the VPN policy that you want to change.

   The Edit VPN Policy screen displays. The following figure shows only the top part with the General section of the Edit VPN Policy screen for IPv6. The Edit VPN Policy screen for IPv4 is identical to the Edit VPN Policy screen for IPv6.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
Edit VPN Policy
○ IPv4 ● IPv6
General
Help
Traffic Selection
Help

Policy Name: SRX-to-IPv6Peer
Policy Type: Auto Policy
Select Local Gateway: WAN1
Remote Endpoint
IP Address: ● 2001::da21:1316:df17:(
FQDN: ○
☑ Enable NetBIOS?
☐ Enable RollOver WAN2
☐ Enable Auto Initiate
Enable Keepalive: ● Yes ○ No
Ping IP Address:
Detection Period: 10 (Seconds)
Reconnect after failure count: 3

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

Setting	Description
Enable Keepalive	To enable the keep-alive feature, select the **Yes** radio button. Periodically, the VPN firewall sends keep-alive requests (ping packets) to the remote endpoint to keep the tunnel alive.
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.

10. Click the **Apply** button.

    Your settings are saved.

Configure Dead Peer Detection

The following procedure describes how to configure Dead Peer Detection for an existing IKE policy.

➢ **To configure Dead Peer Detection for an existing IKE policy:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. If the IKE policy for which you want to configure Dead Peer Detection is associated with a VPN policy, first disable the VPN policy:

   a. Select **VPN > IPSec VPN > VPN Policies**.

      The VPN Policies screen displays the IPv4 settings.

   b. To disable a VPN policy for IPv6 instead of IPv4, in the upper right, select the **IPv6** radio button.

      The VPN Policies screen displays the IPv6 settings.

   c. In the List of VPN policies table, select the VPN policy that is associated with the IKE policy that you want to change.

   Note: When you use the VPN IPsec Wizard, the VPN and IKE policies that are added automatically have the same name.

   d. Click the **Disable** button.

      The VPN policy is disabled. The green circle to the left of the VPN policy turns gray.
7. Select **VPN > IPSec VPN**.

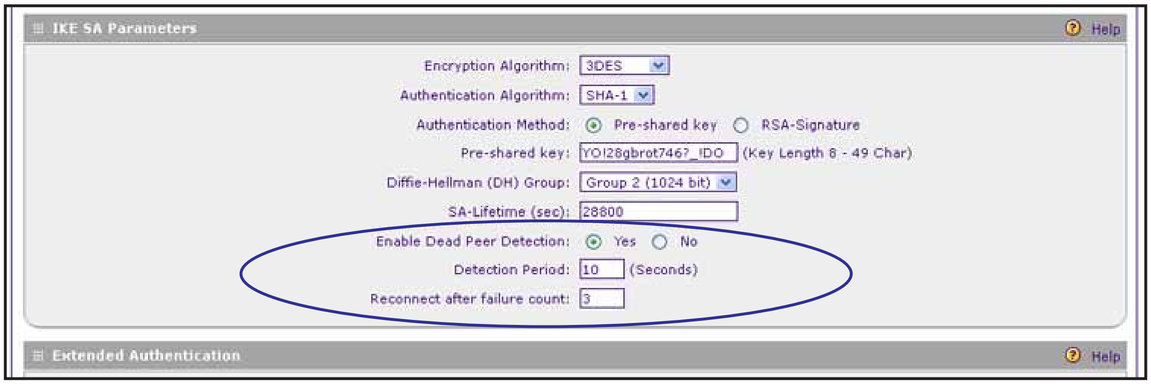
   The IPSec VPN submenu tabs display with the IKE Policies screen for IPv4 in view.

8. To change an IKE policy for IPv6 instead of IPv4, in the upper right, select the **IPv6** radio button.

   The IKE Policies screen for IPv6 displays.

9. In the List of IKE Policies table, click the **Edit** button for the IKE policy that you want to change.

   The Edit IKE Policy screen displays. The following figure shows only the IKE SA Parameters section. The Edit IKE Policy for IP4 and the Edit IKE Policy for IPv6 are identical.



IKE SA Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

Authentication Method: ● Pre-shared key ○ RSA-Signature

Pre-shared key: YO!28gbrot746?_!DO (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

10. In the IKE SA Parameters section, locate the Dead Peer Detection fields and enter the settings as described the following table.

Setting	Description
Enable Dead Peer Detection	To enable Dead Peer Detection, select the **Yes** radio button. If the VPN firewall detects an IKE connection failure, it removes 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.

11. Click the **Apply** button.

    Your settings are saved.

12. If you disabled the VPN policy with which the IKE policy for which you configured Dead Peer Detection is associated, reenable the VPN policy:

    a. Select **VPN > IPSec VPN > VPN Policies**.

       The VPN Policies screen displays the IPv4 settings.

    b. To reenable a VPN policy for IPv6 instead of IPv4, in the upper right, select the **IPv6** radio button.

The VPN Policies screen displays the IPv6 settings.

c. In the List of VPN policies table, select the VPN policy that is associated with the IKE policy that you changed.

d. Click the **Enable** button.

The VPN policy is reenabled. The gray circle to the left of the VPN policy turns green.

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 an existing VPN tunnel:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

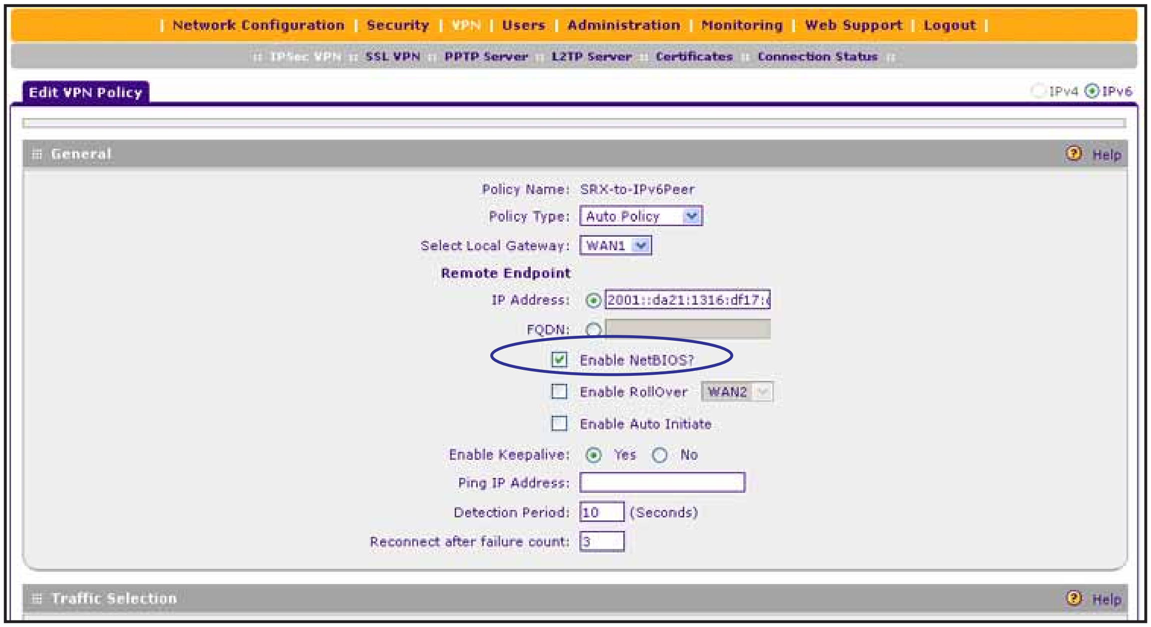
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > IPSec VPN > VPN Policies**.

   The VPN Policies screen displays the IPv4 settings.
7. To change a VPN policy for IPv6 instead of IPv4, in the upper right, select the **IPv6** radio button.

   The VPN Policies screen displays the IPv6 settings.
8. In the List of VPN Policies table, click the **Edit** button for the VPN policy that you want to change.

The Edit VPN Policy screen displays. The following figure shows only the top part with the General section of the Edit VPN Policy screen for IPv6. The Edit VPN Policy screen for IPv4 is identical to the Edit VPN Policy screen for IPv6.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
Edit VPN Policy
○ IPv4 ● IPv6
General
Help
Traffic Selection
Help

Policy Name: SRX-to-IPv6Peer
Policy Type: Auto Policy
Select Local Gateway: WAN1
Remote Endpoint
IP Address: ● 2001::da21:1316:df17:
FQDN: ○
☑ Enable NetBIOS?
☐ Enable RollOver WAN2
☐ Enable Auto Initiate
Enable Keepalive: ● Yes ○ No
Ping IP Address:
Detection Period: 10 (Seconds)
Reconnect after failure count: 3

9. Select the **Enable NetBIOS?** check box.
10. Click the **Apply** button.

    Your settings are saved.

Manage the PPTP Server

The following sections provide information about how to manage the PPTP server:

- *PPTP Servers Overview*
- *Enable and Configure the PPTP Server*
- *View the Active PPTP Users and Disconnect Active Users*

PPTP Servers Overview

As an alternate to IPSec VPN and L2TP tunnels, you can configure a Point-to-Point Tunnel Protocol (PPTP) server on the VPN firewall to allow users to access PPTP clients over PPTP tunnels. A maximum of 25 simultaneous PPTP user sessions are supported. (The very first IP address of the PPTP address pool is used for distribution to the VPN firewall.)

A PPTP user typically initiates a tunnel request; the PPTP server accommodates the tunnel request and assigns an IP address to the user. After a PPTP tunnel is established, the user can connect to a PPTP client that is located behind the VPN firewall.

You must enable the PPTP server on the VPN firewall, specify a PPTP server address pool, and create PPTP user accounts. (PPTP users are authenticated through local authentication with geardomain.) For information about how to create PPTP user accounts, see *Manage User Accounts* on page 498.

Enable and Configure the PPTP Server

The following procedure describes how to enable and configure the PPTP server.

➢ **To enable the PPTP server and configure the PPTP server pool, authentication, and encryption:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

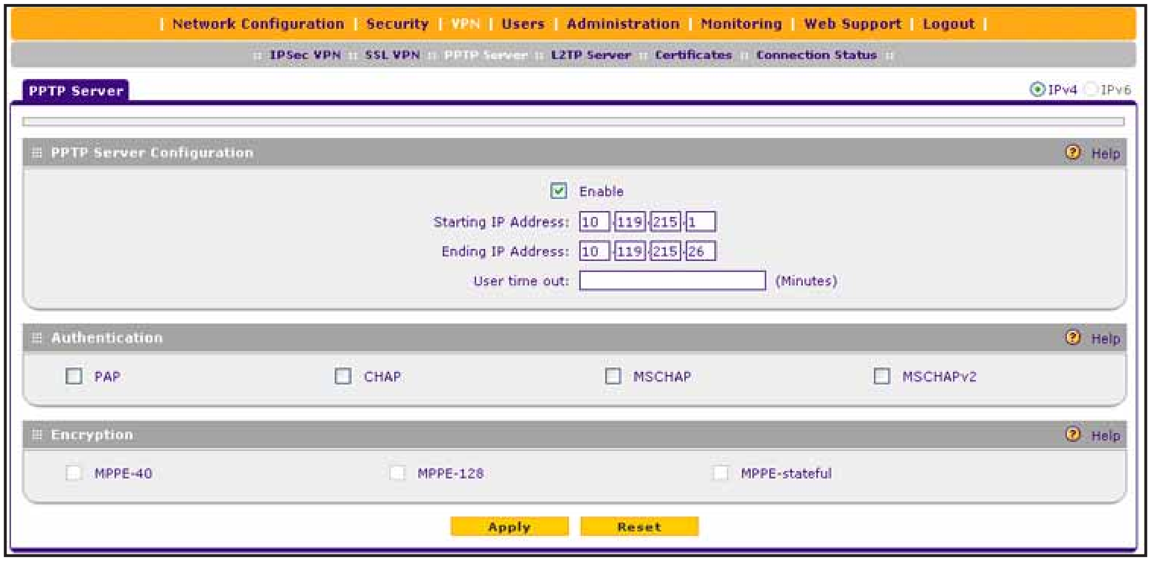
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > PPTP Server**.

   The PPTP Server screen displays. The following figure shows an example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
PPTP Server
● IPv4 ○ IPv6
PPTP Server Configuration
Help
Authentication
Help
Encryption
Help
Apply
Reset

☑ Enable

Starting IP Address: 10 . 119 . 215 . 1

Ending IP Address: 10 . 119 . 215 . 26

User time out: (Minutes)

□ PAP □ CHAP □ MSCHAP □ MSCHAPv2

□ MPPE-40 □ MPPE-128 □ MPPE-stateful

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

Setting	Description
PPTP Server	
Enable	To enable the PPTP server, select the **Enable** check box.
Start IP Address	Type the first IP address of the address pool.
End IP Address	Type the last IP address of the address pool. A maximum of 26 contiguous addresses can be part of the pool. (The first address of the pool cannot be assigned to a user.)
User time out	Enter the time-out period in seconds, from 0 to 999 seconds. The default is 0 seconds. If there is no traffic from a user, the connection is disconnected after the specified period.
Authentication	
Select one or more of the following authentication methods to authenticate PPTP users: • **PAP**. RADIUS-Password Authentication Protocol (PAP). • **CHAP**. RADIUS-Challenge Handshake Authentication Protocol (CHAP). • **MSCHAP**. RADIUS-Microsoft CHAP (MSCHAP). • **MSCHAPv2**. RADIUS-Microsoft CHAP version 2 (MSCHAPv2).	
Encryption	
If the authentication is MSCHAP or MSCHAPv2, the PPTP server can support Microsoft Point-to-Point Encryption (MPPE). Select one or more of the following types of MPPE: • **MPPE-40**. MPPE 40-bit encryption. • **MPPE-128**. MPPE 128-bit encryption. This is the most secure type of MPPE encryption. • **MPPE-stateful**. Stateful MPPE encryption. This is the least secure type of MPPE encryption.	

8. Click the **Apply** button.

   Your settings are saved.

View the Active PPTP Users and Disconnect Active Users

The following procedure describes how to view all active PPTP users and disconnect active PPTP users.

- **To view all active PPTP users and disconnect active PPTP users:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

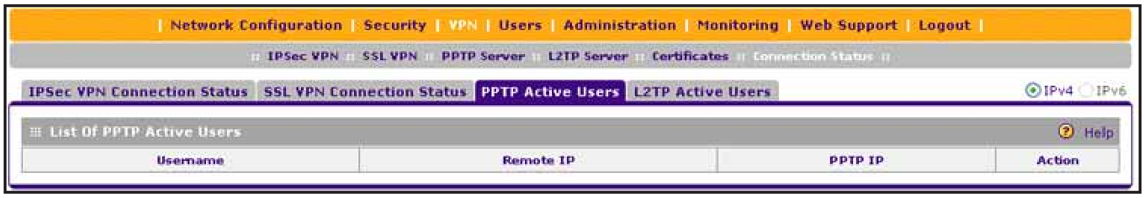
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > Connection Status > PPTP Active Users**.

   The PPTP Active Users screen displays. The following figure does not show any active users.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
IPSec VPN Connection Status
SSL VPN Connection Status
PPTP Active Users
L2TP Active Users
● IPv4 ○ IPv6
Help

List Of PPTP Active Users

Username	Remote IP	PPTP IP	Action

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

Item	Description
Username	The name of the PPTP user that you defined (see *Manage User Accounts* on page 498).
Remote IP	The remote client’s IP address.

Item	Description
PPTP IP	The IP address that is assigned by the PPTP server on the VPN firewall.
Action	The **Disconnect** button lets you terminate an active PPTP connection. (This button displays only if an active PPTP connection exists.)

7. To disable an active PPTP user, in the List of PPTP Active Users table, click the corresponding **Disconnect** button.

   The user is disconnected.

8. To disable another active PPTP user, repeat *Step 7*.

Manage the L2TP Server

The following sections provide information about how to manage the L2TP server:

- *L2TP Servers Overview*
- *Enable and Configure the L2TP Server*
- *View the Active L2TP Users and Disconnect Active Users*

L2TP Servers Overview

As an alternate to IPSec VPN tunnels, you can configure a Layer 2 Tunneling Protocol (L2TP) server on the VPN firewall to allow users to access L2TP clients over L2TP tunnels. A maximum of 25 simultaneous L2TP user sessions are supported. (The very first IP address of the L2TP address pool is used for distribution to the VPN firewall.)

An L2TP Access Concentrator (LAC) typically initiates a tunnel to fulfill a connection request from an L2TP user; the L2TP server accommodates the tunnel request. After an L2TP tunnel is established, the L2TP user can connect to an L2TP client that is located behind the VPN firewall.

Note: IPSec VPN provides stronger authentication and encryption than L2TP. (Packets that traverse the L2TP tunnel are not encapsulated by IPSec.)

You 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 *Manage User Accounts* on page 498.

Enable and Configure the L2TP Server

The following procedure describes how to enable and configure the L2TP server.

➢ **To enable the L2TP server and configure the L2TP server pool:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

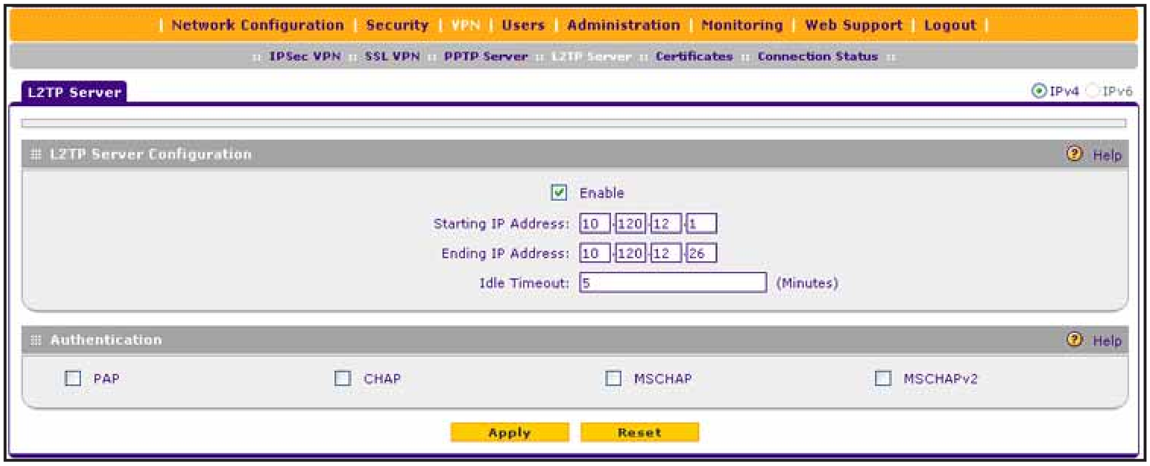
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > L2TP Server**.

   The L2TP Server screen displays. The following figure shows an example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
L2TP Server
Help
Help
Apply
Reset

● IPv4 ○ IPv6

L2TP Server Configuration

☑ Enable

Starting IP Address: 10 . 120 . 12 . 1

Ending IP Address: 10 . 120 . 12 . 26

Idle Timeout: 5 (Minutes)

Authentication

□ PAP □ CHAP □ MSCHAP □ MSCHAPv2

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

Setting	Description
L2TP Server Configuration	
Enable	To enable the L2TP server, select the **Enable** check box.
Starting IP Address	The first IP address of the pool. This address is used for distribution to the VPN firewall.

Setting	Description
Ending IP Address	The last IP address of the pool. A maximum of 26 contiguous addresses is supported. (The first address of the pool cannot be assigned to a user.)
Idle Timeout	The period after which an idle user is automatically logged out of the L2TP server. The default idle time-out period is 5 minutes.
Authentication	
Select one or more of the following authentication methods to authenticate L2TP users: • **PAP**. RADIUS-Password Authentication Protocol (PAP). • **CHAP**. RADIUS-Challenge Handshake Authentication Protocol (CHAP). • **MSCHAP**. RADIUS-Microsoft CHAP (MSCHAP). • **MSCHAPv2**. RADIUS-Microsoft CHAP version 2 (MSCHAPv2).	

8. Click the **Apply** button.

   Your settings are saved.

View the Active L2TP Users and Disconnect Active Users

The following procedure describes how to view all active L2TP users and disconnect active L2TP users.

➢ **To view all active L2PTP users and disconnect active L2TP users:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

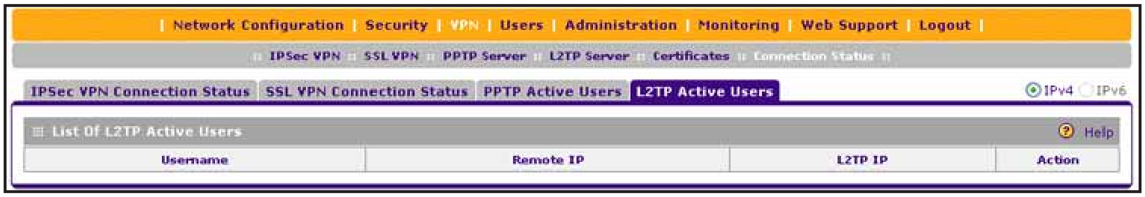
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **VPN > Connection Status > L2TP Active Users**.

   The L2TP Active Users screen displays. The following figure does not show any active users.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
IPSec VPN
SSL VPN
PPTP Server
L2TP Server
Certificates
Connection Status
IPSec VPN Connection Status
SSL VPN Connection Status
PPTP Active Users
L2TP Active Users
● IPv4 ○ IPv6
List Of L2TP Active Users
Help

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.

Item	Description
Username	The name of the L2TP user that you have defined (see *Manage User Accounts* on page 498).
Remote IP	The client’s IP address on the remote L2TP Access Concentrator (LAC).
L2TP IP	The IP address that is assigned by the L2TP server on the VPN firewall.
Action	The **Disconnect** button lets you terminate an active L2TP connection. (This button displays only if an active L2TP connection exists.)

7. To disable an active L2TP user, in the List of L2TP Active Users table, click the corresponding **Disconnect** button.

   The user is disconnected.

8. To disable another active L2TP user, repeat *Step 7*.

9. Set Up Virtual Private Networking with SSL Connections

9

This chapter describes how to use the SSL VPN solution of the VPN firewall to provide remote access for mobile users to their corporate resources. The chapter contains the following sections:

- *SSL VPN Portals Overview*
- *Build an SSL Portal Using the SSL VPN Wizard*
- *Access a Custom SSL VPN Portal*
- *Manually Set Up or Change an SSL Portal*

SSL VPN Portals Overview

The following sections provide concept information about the SSL VPN portal:

- *SSL VPN Capabilities*
- *SSL Tunnels*
- *SSL Port Forwarding*
- *Build and Access an SSL Portal*

SSL VPN Capabilities

The VPN firewall integrates a hardware-based SSL VPN engine that can provide mobile users remote access to their corporate resources. With SSL VPN, remote users do not need to install a VPN client on their computers. Using the familiar Secure Sockets Layer (SSL) protocol, which is common for e-commerce transactions, the VPN firewall can authenticate itself to an SSL-enabled client, such as a standard web browser.

When the authentication and encryption negotiation are successful, the server and client establish an encrypted connection. With support for up to five dedicated SSL VPN tunnels, the VPN firewall allows users to easily access the remote network from virtually any available platform. You can customize a secure user portal and assign a level of SSL service.

The VPN firewall's SSL VPN portal can provide two levels of SSL service to the remote user: SSL VPN tunnel and SSL port forwarding. The SSL VPN portal can present the remote user with one or both of these SSL service levels, depending on how you set up the configuration.

SSL Tunnels

With an SSL VPN tunnel, the VPN firewall provides full network connectivity of a VPN tunnel using the remote user's browser. The SSL capability of the user's browser provides authentication and encryption, establishing a secure connection to the VPN firewall. Upon successful connection, an ActiveX-based SSL VPN client is downloaded to the remote computer to allow the remote user to virtually join the corporate network.

The SSL VPN client provides a point-to-point (PPP) connection between the client and the VPN firewall, and a virtual network interface is created on the user's computer. The VPN firewall assigns the computer an IP address and DNS server IP addresses, allowing the remote computer to access network resources in the same manner as if it were connected directly to the corporate network, subject to any policy restrictions that you configure.

SSL Port Forwarding

Like an SSL VPN tunnel, SSL port forwarding is a web-based client that is installed transparently and then creates a virtual, encrypted tunnel to the remote network. However, port forwarding differs from an SSL VPN tunnel in several ways:

- Port forwarding supports only TCP connections, not UDP connections or connections using other IP protocols.
- Port forwarding detects and reroutes individual data streams on the user’s computer to the port forwarding connection rather than opening up a full tunnel to the corporate network.
- Port forwarding offers more fine-grained management than an SSL VPN tunnel. You define individual applications and resources that are available to remote users.

Note: Any applications and services that you do not select for SSL port forwarding are not visible from the SSL VPN portal. However, if users know the IP address of an application or service, they can still access it unless you create SSL VPN access policies to prevent access to the application or service. For information about access policies, see *Configure User, Group, and Global Policies* on page 473.

Build and Access an SSL Portal

You can either use the SSL VPN Wizard to build a basic portal or you can build the portal manually, which gives you more granularity. If you use the SSL VPN Wizard to build a basic portal, you can also refine the portal settings manually after you have set up the portal. For more information, see the following sections:

- *Build an SSL Portal Using the SSL VPN Wizard*
- *Manually Set Up or Change an SSL Portal*

After you built the custom portal, you access it at a different URL from the default SSL VPN portal that provides access to the web management interface. For example, if your SSL VPN portal is hosted at https://vpn.company.com and you create a portal layout named Support, then users access the subsite at https://vpn.company.com/portal/Support. For more information, see *Access a Custom SSL VPN Portal* on page 440.

Note: All screens that you can access from the **SSL VPN** menu of the web management interface display a user portal link in the upper right, above the menu bars (User Portal). When you click the **User Portal** link, the SSL VPN default portal opens. This default portal is not the same as a custom SSL portal login screen that you can build with the SSL VPN Wizard or manually.

Build an SSL Portal Using the SSL VPN Wizard

The following sections provide information about using the SSL VPN Wizard to build an SSL portal:

- *SSL VPN Wizard Overview*
- *Build an SSL Portal with the SSL VPN Wizard*

SSL VPN Wizard Overview

This section provides an overview of the SSL VPN Wizard. For more information about how to set up a portal, see *Build an SSL Portal with the SSL VPN Wizard* on page 429.

The SSL VPN Wizard helps you set up an SSL VPN client connection by guiding you through six screens, the last of which lets you save the SSL VPN policy:

- **Step 1 of 6**. Create the portal layout and theme.

  In Step 1, you specify the banner that the portal displays and whether the portal provides full network connectivity, access to specific defined network services through port forwarding, or both. In addition, you can set up HTTP meta tags for cache control and ActiveX web cache cleaner.

- **Step 2 of 6**. Create a new domain for SSL users.

  In Step 2, you create a new domain for the portal and specify the type of authentication. You can also use the default domain (geardomain).

- **Step 3 of 6**. Create a new SSL user.

  In Step 3, you create one new SSL VPN user account for the portal and the selected domain. You must create one user account; otherwise, the SSL VPN Wizard cannot create the portal. After the portal is created, you can provide more SSL VPN users access to the portal.

  The VPN firewall automatically adds a user policy that permits access for the user account that you define with the SSL VPN Wizard.

- **Step 4 of 6**. Set up a client address range and client routes.

  The settings in Step 4 apply only if the portal provides full network connectivity. These settings do not apply if the portal provides access to specific defined network services through port forwarding.

  In Step 4, you set up the client IP address range. For split tunnel mode, you must also set up client routes to specific networks that are accessible to clients. Client routes do not apply to full tunnel mode because clients have access to the entire LAN network.

- **Step 5 of 6**. Set up port forwarding.

  The settings in Step 5 apply only if the portal provides access to specific defined network services through port forwarding. These settings do not apply if the portal provides full network connectivity.

  In Step 5, you set up the local IP address of the server for the network service or application and the associated TCP port number. You can also set up an FQDN for the service or application.

- **Step 6 of 6**. Verify and save the settings.

After you built the SSL portal with the SSL VPN Wizard, you can refine the portal and its associated settings through the following tasks:

- Add SSL VPN users that are allowed to access the SSL portal (see *Manage User Accounts* on page 498.
- Add more applications and services for SSL port forwarding (see *Configure Applications for SSL VPN Port Forwarding* on page 453).
- Add network resource objects such as groups of IP addresses, IP address ranges, and application of services for easier configuration of SSL access policies (see *Manage Network Resource Objects to Simplify Policies* on page 467).
- Add SSL access policies to reinforce that users access only the applications and services that you assigned to the SSL portal (see *Configure User, Group, and Global Policies* on page 473).

Build an SSL Portal with the SSL VPN Wizard

The SSL VPN Wizard lets you build an SSL portal by guiding you through six screens.

➢ **To build an SSL portal with the SSL VPN Wizard:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

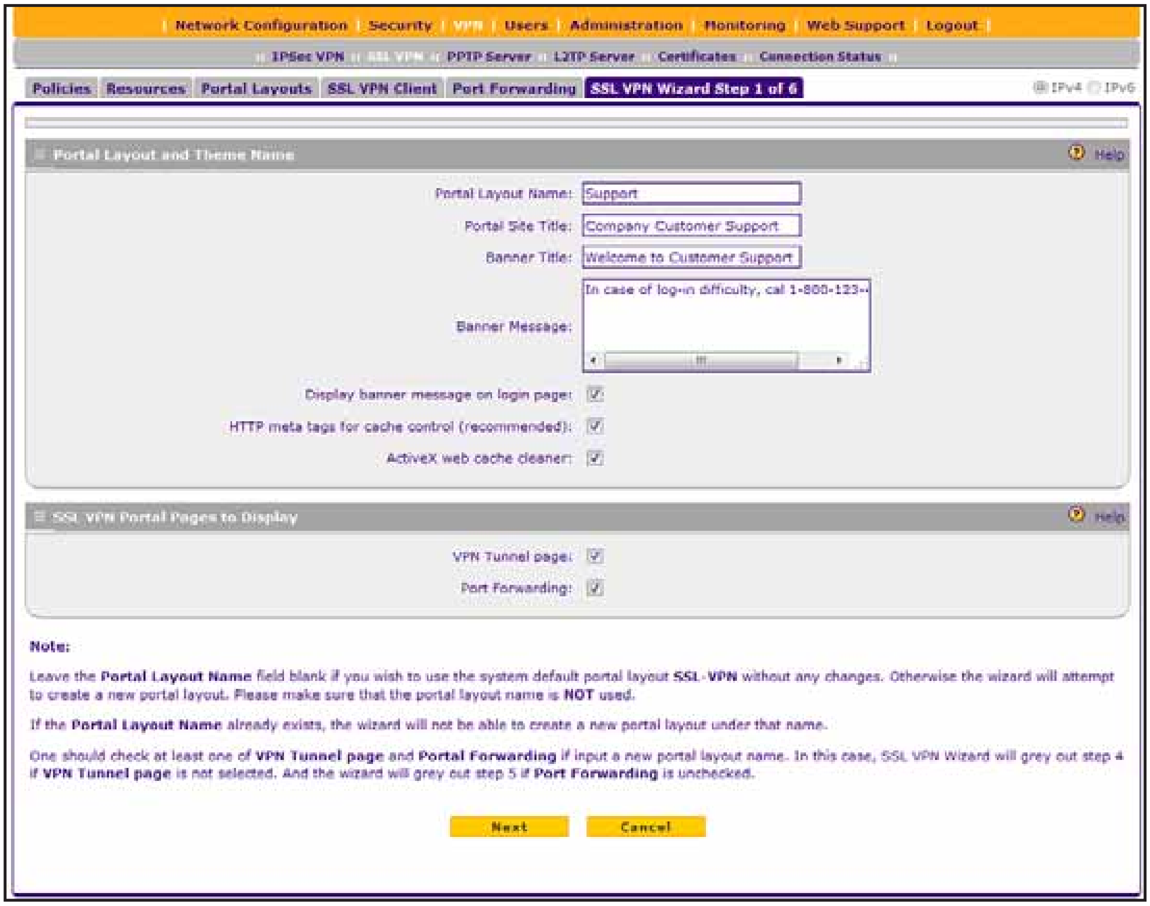
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > IPSec VPN > SSL VPN Wizard**.

   The SSL VPN Wizard Step 1 of 6 screen displays.



Portal Layout and Theme Name

Portal Layout Name:	Support
Portal Site Title:	Company Customer Support
Banner Title:	Welcome to Customer Support
Banner Message:	In case of log-in difficulty, call 1-800-123--
Display banner message on login page:	☑
HTTP meta tags for cache control (recommended):	☑
ActiveX web cache cleaner:	☑

SSL VPN Portal Pages to Display

VPN Tunnel page:	☑
Port Forwarding:	☑

Note:

Leave the **Portal Layout Name** field blank if you wish to use the system default portal layout **SSL-VPN** without any changes. Otherwise the wizard will attempt to create a new portal layout. Please make sure that the portal layout name is **NOT** used.

If the **Portal Layout Name** already exists, the wizard will not be able to create a new portal layout under that name.

One should check at least one of **VPN Tunnel page** and **Portal Forwarding** if input a new portal layout name. In this case, SSL VPN Wizard will grey out step 4 if **VPN Tunnel page** is not selected. And the wizard will grey out step 5 if **Port Forwarding** is unchecked.

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

WARNING:

Do not enter an existing portal layout name in the Portal Layout Name field; otherwise, the SSL VPN Wizard fails when you attempt to apply the settings.

Setting	Description
Portal Layout and Theme Name	
Portal Layout Name	A descriptive name for the portal layout. This name is part of the path of the SSL VPN portal URL. Use only alphanumeric characters, hyphens (-), and underscores (_) in the **Portal Layout Name** field. If you enter other types of characters or spaces, the layout name is truncated before the first nonalphanumeric character, hyphen, or underscore. Unlike most other names in URLs, this name is case-sensitive. **Note:** If you leave the **Portal Layout Name** field blank, the SSL VPN Wizard uses the default portal layout. (The name of the default portal is SSL-VPN). To enable the SSL VPN Wizard to create a portal layout, you must enter a name other than SSL-VPN in the **Portal Layout Name** field.
Portal Site Title	The title that displays at the top of the user's web browser window, for example, *Company Customer Support*.
Banner Title	**Note:** The banner title of a banner message that users see before they log in to the portal, for example, *Welcome to Customer Support*. **Note:** For an example, see *Access a Custom SSL VPN Portal* on page 440. The banner title is displayed in the orange header bar of the login screen that is shown in the procedure.
Banner Message	The text of a banner message that users see before they log in to the portal, for example, *In case of login difficulty, call 123-456-7890*. Enter a plain text message, or include HTML and JavaScript tags. The maximum length of the login screen message is 4096 characters. **Note:** You can enlarge the field (that is, the text box) by manipulating the lower right corner of the field. **Note:** For an example, see *Access a Custom SSL VPN Portal* on page 440. The banner message text is displayed in the gray header bar of the login screen that is shown in the procedure.
Display banner message on login page	Select this check box to show the banner title and banner message text on the login screen.

HTTP meta tags for cache control (recommended)	Select this check box to apply HTTP meta tag cache control directives to this portal layout. Cache control directives include the following:
	`<meta http-equiv="pragma" content="no-cache">`
	`<meta http-equiv="cache-control" content="no-cache">`
	`<meta http-equiv="cache-control" content="must-revalidate">`
	Note: NETGEAR strongly recommends enabling HTTP meta tags for security reasons and to prevent out-of-date web pages, themes, and data being stored in a user's web browser cache.

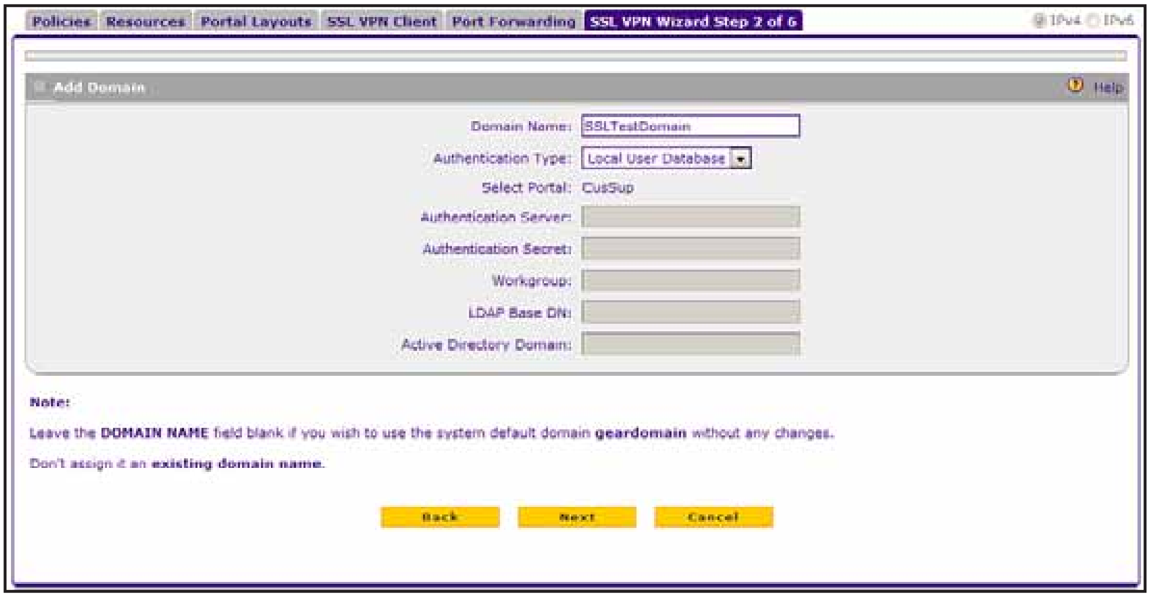
ActiveX web cache cleaner	Select this check box to enable ActiveX cache control to be loaded when users log in to the SSL VPN portal. The web cache cleaner prompts the user to remove all temporary Internet files, cookies, and browser history when the user logs out or closes the web browser window. Web browsers that do not support ActiveX ignore ActiveX web cache control.

Setting	Description
SSL VPN Portal Pages to Display **Note:** Although you can select both, you typically select either the **VPN Tunnel page** check box or the **Port Forwarding** check box.	
VPN Tunnel page	To provide full network connectivity, select this check box. **Note:** *Step 13* describes how to assign IP addresses and routes to clients for full network connectivity.
Port Forwarding	To provide access to specific network services, select this check box. **Note:** *Step 15* describes how to select the specific network services.

Note: For more information about portal settings, see *Manage the Portal Layout* on page 448.

8. Click the **Next** button.

   The SSL VPN Wizard Step 2 of 6 screen displays.



Domain Name: SSLTestDomain

Authentication Type: Local User Database

Select Portal: CusSup

Authentication Server:

Authentication Secret:

Workgroup:

LDAP Base DN:

Active Directory Domain:

Note:

Leave the **DOMAIN NAME** field blank if you wish to use the system default domain **geardomain** without any changes.

Don't assign it an **existing domain name**.

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

WARNING:

Do not enter an existing domain name in the Domain Name field; otherwise, the SSL VPN Wizard fails when you attempt to apply the settings.

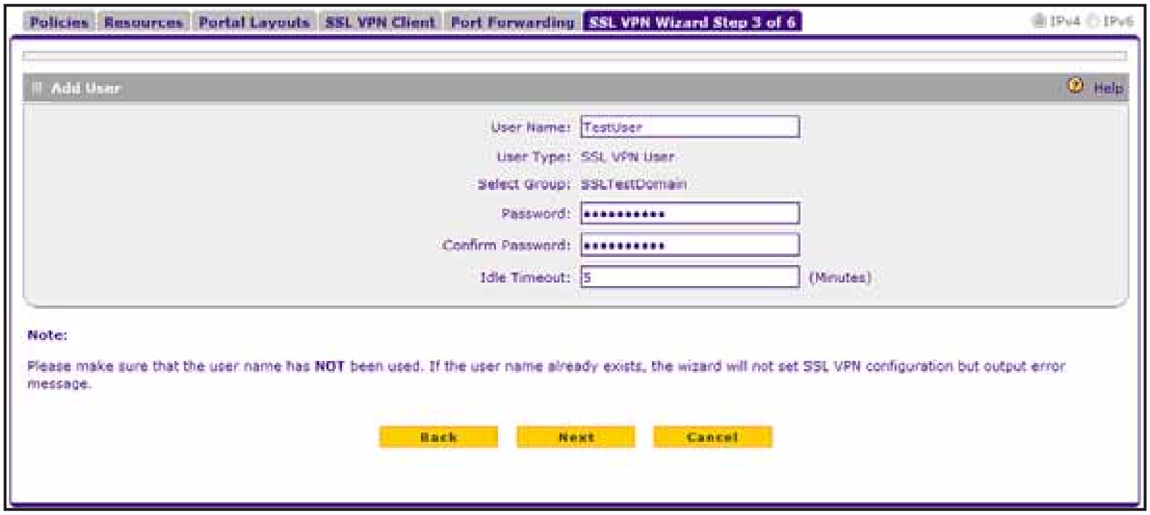
Setting	Description
Domain Name	A descriptive (alphanumeric) name of the domain for identification and management purposes. **Note:** If you leave the **Domain Name** field blank, the SSL VPN Wizard uses the default domain name geardomain. To enable the SSL VPN Wizard to create a domain, you must enter a name other than geardomain in the **Domain Name** field.
Authentication Type **Note:** If you select any type of RADIUS authentication, make sure that you configure one or more RADIUS servers (see *Configure the RADIUS Servers for the VPN Firewall's RADIUS Client* on page 392).	From the menu, 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 **Authentication Server** and **Authentication Secret** fields. • **Radius-CHAP**. RADIUS Challenge Handshake Authentication Protocol (CHAP). Complete the **Authentication Server** and **Authentication Secret** fields. • **Radius-MSCHAP**. RADIUS Microsoft CHAP. Complete the **Authentication Server** and **Authentication Secret** fields. • **Radius-MSCHAPv2**. RADIUS Microsoft CHAP version 2. Complete the **Authentication Server** and **Authentication Secret** fields. • **WIKID-PAP**. WiKID Systems PAP. Complete the **Authentication Server** and **Authentication Secret** fields. • **WIKID-CHAP**. WiKID Systems CHAP. Complete the **Authentication Server** and **Authentication Secret** fields. • **MIAS-PAP**. Microsoft Internet Authentication Service (MIAS) PAP. Complete the **Authentication Server** and **Authentication Secret** fields. • **MIAS-CHAP**. Microsoft Internet Authentication Service (MIAS) CHAP. Complete the **Authentication Server** and **Authentication Secret** fields. • **NT Domain**. Microsoft Windows NT Domain. Complete the **Authentication Server** and **Workgroup** fields. • **Active Directory**. Microsoft Active Directory. Complete the **Authentication Server** and **Active Directory Domain** fields. • **LDAP**. Lightweight Directory Access Protocol (LDAP). Complete the **Authentication Server** and **LDAP Base DN** fields.
Portal	The portal that you selected on the SSL VPN Wizard 1 of 6 screen in *Step 7*. You cannot change the portal on this screen; the portal displays for information only.
Authentication Server	The server IP address or server name of the authentication server for any type of authentication other than authentication through the local user database.
Authentication Secret	The authentication secret or password that is required to access the authentication server for RADIUS, WiKID, or MIAS authentication.
Workgroup	The workgroup that is required for Microsoft NT Domain authentication.

Setting	Description
LDAP Base DN	The LDAP distinguished name (DN) that is required to access the LDAP authentication server. This must be a user in the LDAP directory who has read access to all the users that you want to import into the VPN firewall. The **LDAP Base DN** field accepts two formats: • **A display name in the DN format**. For example: cn=Jamie Hanson,cn=users,dc=test,dc=com. • **A Windows login account name in email format**. For example: jhanson@testAD.com. This last type of bind DN can be used only for a Windows LDAP server.
Active Directory Domain	The Active Directory domain name that is required for Microsoft Active Directory authentication.

Note: For more information about domains, see *Manage Authentication Domains* on page 488.

10. Click the **Next** button.

    The SSL VPN Wizard Step 3 of 6 screen displays.



Add User

User Name: TestUser

User Type: SSL VPN User

Select Group: SSLTestDomain

Password: ••••••••••

Confirm Password: ••••••••••

Idle Timeout: 5 (Minutes)

Note:

Please make sure that the user name has **NOT** been used. If the user name already exists, the wizard will not set SSL VPN configuration but output error message.

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

WARNING:

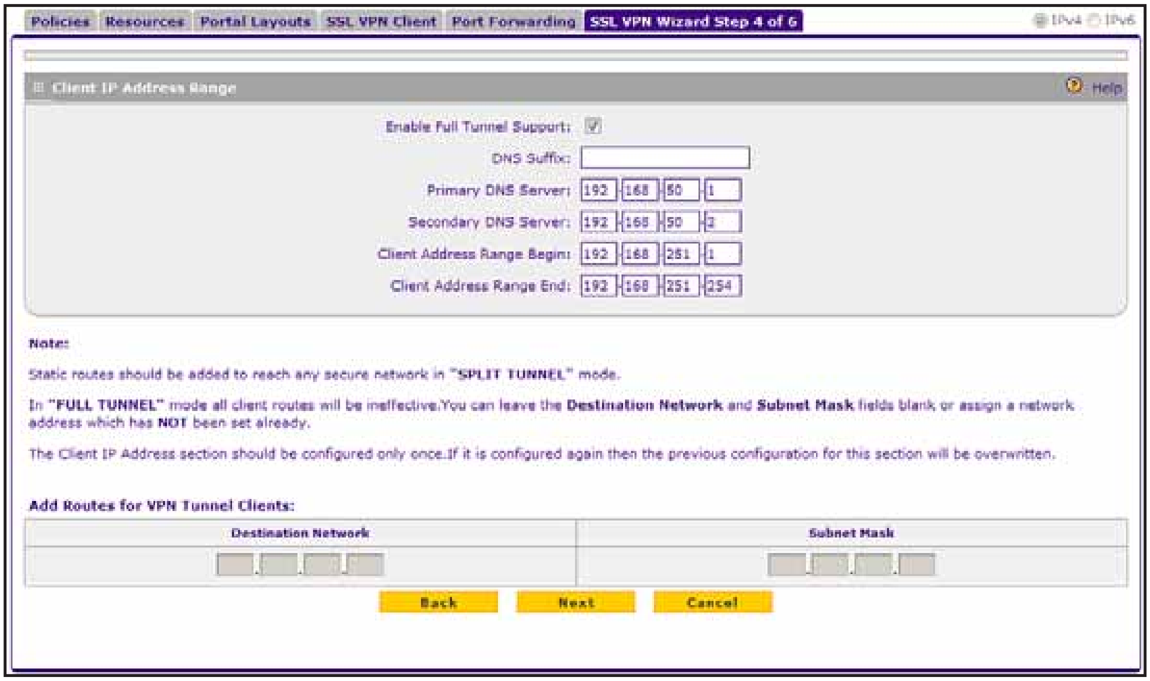
Do not enter an existing user name in the User Name field; otherwise, the SSL VPN Wizard fails when you attempt to apply the settings.

Setting	Description
User Name	A descriptive (alphanumeric) name of the user for identification and management purposes.
User Type	When you use the SSL VPN Wizard, the user type is always SSL VPN User. You cannot change the user type on this screen; the user type is displayed for information only.
Group	When you create a domain on the SSL VPN Wizard 2 of 6 screen in *Step 9*, a group with the same name is automatically created. (A user belongs to a group, and a group belongs to a domain.) You cannot change the group on this screen; the group is displayed for information only.
Password	The password that a user must enter to gain access to the VPN firewall. The password must contain alphanumeric, hyphen (-), or underscore (_) characters.
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.

Note: For more information about user accounts and about adding user accounts, see *Manage User Accounts* on page 498.

12. Click the **Next** button.

The SSL VPN Wizard Step 4 of 6 screen displays. If you did not select the **VPN Tunnel** check box on the SSL VPN Wizard Step 1 of 6 screen in *Step 7*, the fields on the SSL VPN Wizard Step 4 of 6 screen are masked out because they do not apply to a port forwarding portal.



Client IP Address Range

Enable Full Tunnel Support: ☑

DNS Suffix:

Primary DNS Server: 192 . 168 . 50 . 1

Secondary DNS Server: 192 . 168 . 50 . 2

Client Address Range Begin: 192 . 168 . 251 . 1

Client Address Range End: 192 . 168 . 251 . 254

Note:

Static routes should be added to reach any secure network in **"SPLIT TUNNEL"** mode.

In **"FULL TUNNEL"** mode all client routes will be ineffective.You can leave the **Destination Network** and **Subnet Mask** fields blank or assign a network address which has **NOT** been set already.

The Client IP Address section should be configured only once.If it is configured again then the previous configuration for this section will be overwritten.

Add Routes for VPN Tunnel Clients:

Destination Network	Subnet Mask
. . .	. . .

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

WARNING:

Do not enter an existing route for a VPN tunnel client in the Destination Network and Subnet Mask fields; otherwise, the SSL VPN Wizard fails when you attempt to apply the settings.

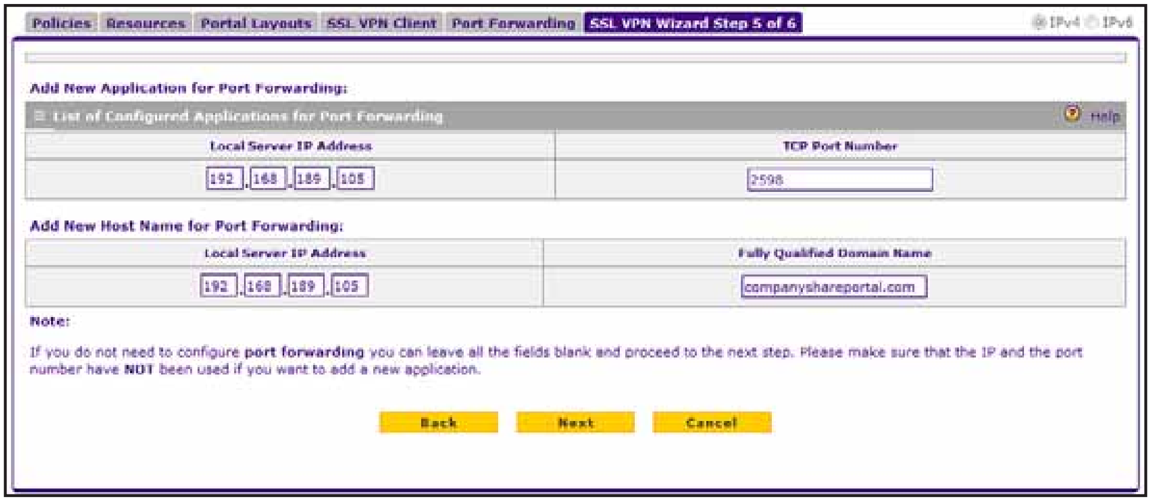
Setting	Description
Client IP Address Range	
Enable Full Tunnel Support	Select this check box to enable full-tunnel support. Full tunnel support provides clients access to the entire LAN network. If you leave this check box cleared (which is the default setting), full-tunnel support is disabled but split-tunnel support is enabled and you must add a client route by completing the **Destination Network** and **Subnet Mask** fields. Split-tunnel support provides clients access to specific networks. **Note:** When full-tunnel support is enabled, client routes are not operable.
DNS Suffix	A DNS suffix to be appended to incomplete DNS search strings. This setting is optional.
Primary DNS Server	The IP address of the primary DNS server that is assigned to the VPN tunnel clients. This setting is optional. **Note:** If you do not assign a DNS server, the DNS settings remain unchanged in the VPN client after a VPN tunnel is established.

Setting	Description
Secondary DNS Server	The IP address of the secondary DNS server that is assigned to the VPN tunnel clients. This setting is optional.
Client Address Range Begin	The first IP address of the IP address range that you want to assign to the VPN tunnel clients.
Client Address Range End	The last IP address of the IP address range that you want to assign to the VPN tunnel clients.
Add Routes for VPN Tunnel Clients	
Destination Network	Leave this field blank or specify a destination network IP address of a local network or subnet that is not used. This setting applies only when full-tunnel support is disabled.
Subnet Mask	Leave this field blank or specify the address of the appropriate subnet mask. This setting applies only when full-tunnel support is disabled.

Note: For more information about client IP address ranges and route settings, see *Configure the SSL VPN Client* on page 459.

14. Click the **Next** button.

    The SSL VPN Wizard Step 5 of 6 screen displays. If you did not select the **Port Forwarding** check box on the SSL VPN Wizard Step 1 of 6 screen in *Step 7*, the fields on the SSL VPN Wizard Step 5 of 6 screen are masked out because they do not apply to a VPN tunnel portal.



Add New Application for Port Forwarding:

List of Configured Applications for Port Forwarding

Local Server IP Address	TCP Port Number
192.168.189.105	2598

Add New Host Name for Port Forwarding:

Local Server IP Address	Fully Qualified Domain Name
192.168.189.105	companyshareportal.com

Note:

If you do not need to configure **port forwarding** you can leave all the fields blank and proceed to the next step. Please make sure that the IP and the port number have **NOT** been used if you want to add a new application.

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

⚠ **WARNING:**

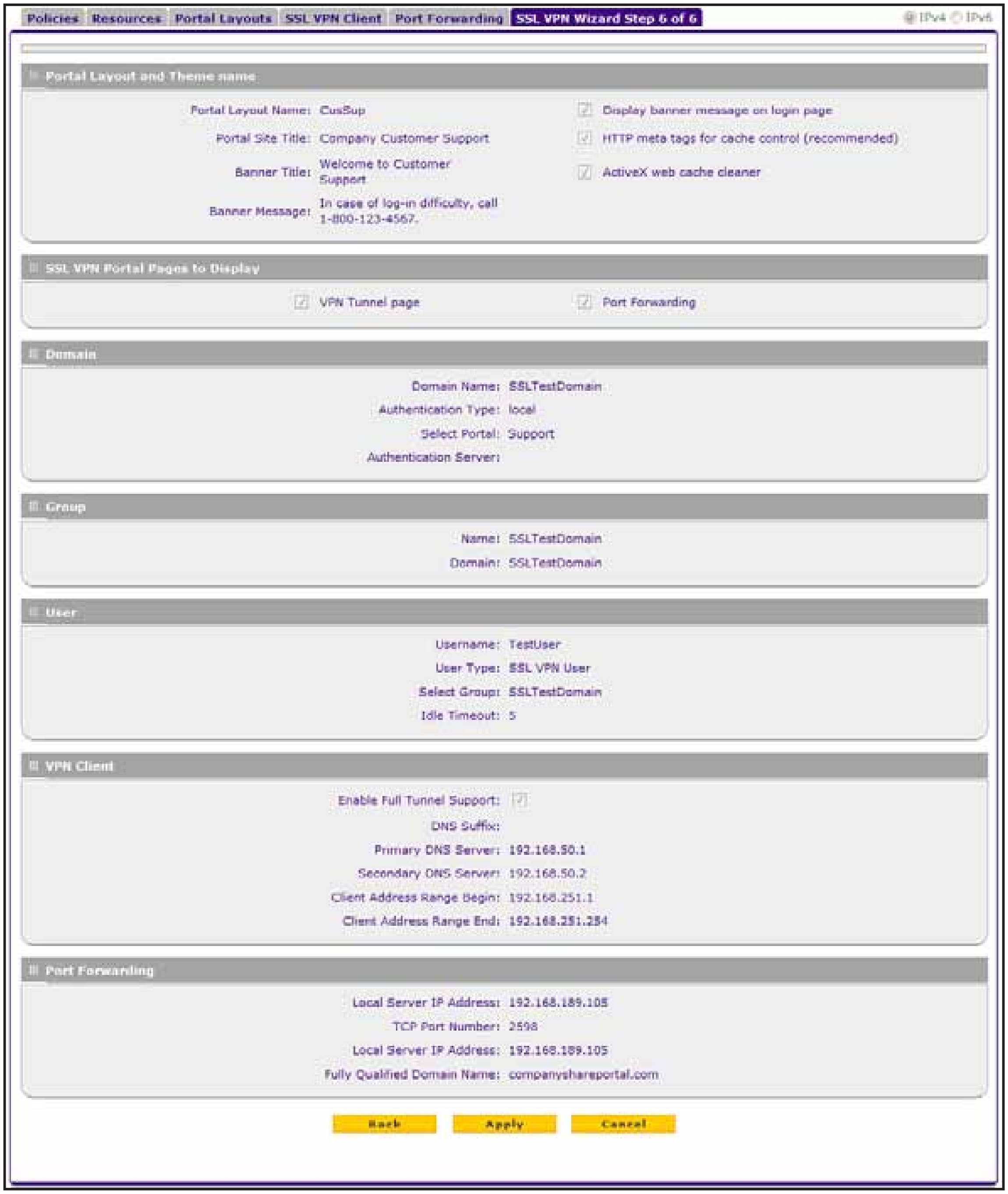
In the upper Local Server IP Address field, do not enter an IP address that is already in use or in the TCP Port Number field do not enter a port number that is already in use; otherwise, the SSL VPN Wizard fails when you attempt to apply the settings.

Setting	Description
Add New Application for Port Forwarding	
Local Server IP Address	The IP address of an internal server or host computer that remote users have access to.
TCP Port Number	The TCP port number of the application that users are allowed to access through the SSL VPN tunnel.
Add New Host Name for Port Forwarding	
Local Server IP Address	The IP address of an internal server or host computer that you want to name. **Note:** Both the upper and lower **Local Server IP Address** fields on this screen (that is, the field in the Add New Application for Port Forwarding section and the field in the Add New Host Name for Port Forwarding section) must contain the same IP address.
Fully Qualified Domain Name	The full server name, that is, the host name–to–IP address resolution for the network server as a convenience for remote users.

Note: After you create the SSL portal, you can add more network services. For more information about port-forwarding settings, see *Configure Applications for SSL VPN Port Forwarding* on page 453.

16. Click the **Next** button.

The SSL VPN Wizard Step 6 of 6 screen displays.



Portal Layout and Theme name

Portal Layout Name: CusSup

Portal Site Title: Company Customer Support

Banner Title: Welcome to Customer Support

Banner Message: In case of log-in difficulty, call 1-800-123-4567.

☑ Display banner message on login page

☑ HTTP meta tags for cache control (recommended)

☑ ActiveX web cache cleaner

SSL VPN Portal Pages to Display

☑ VPN Tunnel page

☑ Port Forwarding

Domain

Domain Name: SSLTestDomain

Authentication Type: local

Select Portal: Support

Authentication Server:

Group

Name: SSLTestDomain

Domain: SSLTestDomain

User

Username: TestUser

User Type: SSL VPN User

Select Group: SSLTestDomain

Idle Timeout: 5

VPN Client

Enable Full Tunnel Support: ☑

DNS Suffix:

Primary DNS Server: 192.168.50.1

Secondary DNS Server: 192.168.50.2

Client Address Range Begin: 192.168.251.1

Client Address Range End: 192.168.251.254

Port Forwarding

Local Server IP Address: 192.168.189.105

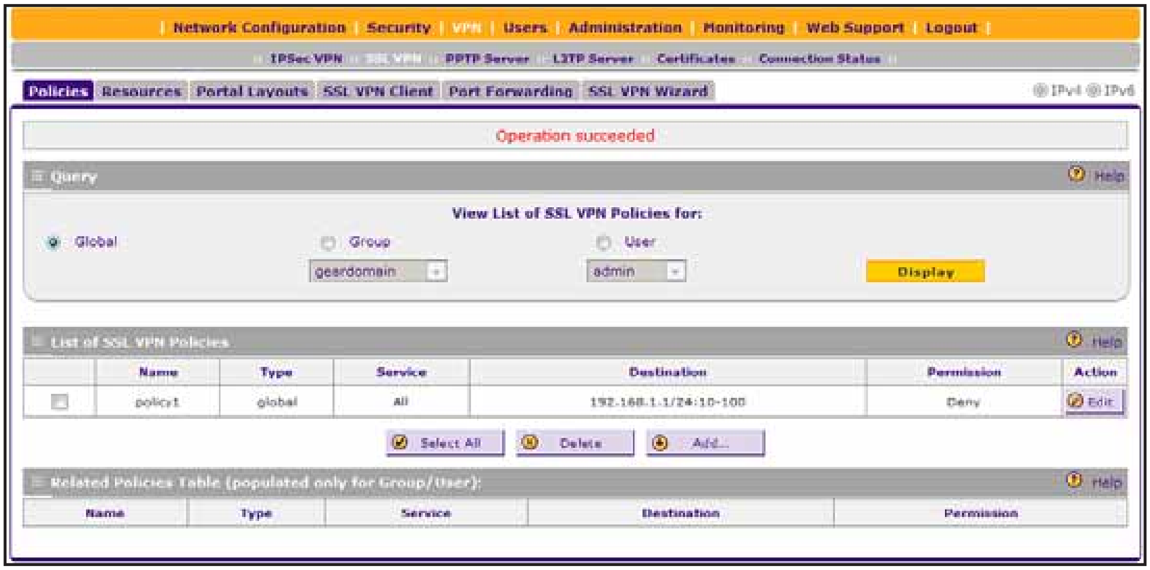
TCP Port Number: 2598

Local Server IP Address: 192.168.189.105

Fully Qualified Domain Name: companyshareportal.com

17. Verify the settings. To make changes to the settings:
    a. Click the **Back** button to navigate to the screen on which you want to change the settings.
    b. Change the settings.
    c. Click the **Next** button to navigate back to the SSL VPN Wizard Step 6 of 6 screen.
18. Click the **Apply** button.

Your settings are saved. If the VPN firewall accepts the settings, the Policies screen displays with a message *Operation succeeded* at the top of the screen.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
IPSec VPN | SSL VPN | PPTP Server | L2TP Server | Certificates | Connection Status
Policies | Resources | Portal Layouts | SSL VPN Client | Port Forwarding | SSL VPN Wizard
IPv4 IPv6
Query
Help
List of SSL VPN Policies
Help
Select All
Delete
Add...
Related Policies Table (populated only for Group/User):
Help

Operation succeeded

View List of SSL VPN Policies for:

● Global ○ Group ○ User

geardomain admin Display

	Name	Type	Service	Destination	Permission	Action
□	policy1	global	All	192.168.1.1/24:10-100	Deny	Edit

Name	Type	Service	Destination	Permission

If the VPN firewall rejects the settings, review the settings that you entered and try again. Most failures occur because of a misconfiguration.

For information about how to access the new portal, see *Access a Custom SSL VPN Portal* on page 440.

Access a Custom SSL VPN Portal

After you build a custom SSL portal, either with the SSL VPN Wizard or manually, access the portal to verify that it functions correctly before you provide the portal link to users who must access the portal.

Note: The first time that you attempt to connect through the VPN tunnel, the SSL VPN tunnel adapter is installed; the first time that you attempt to connect through the port-forwarding tunnel, the port-forwarding engine is installed.

➢ **To access a custom SSL portal:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

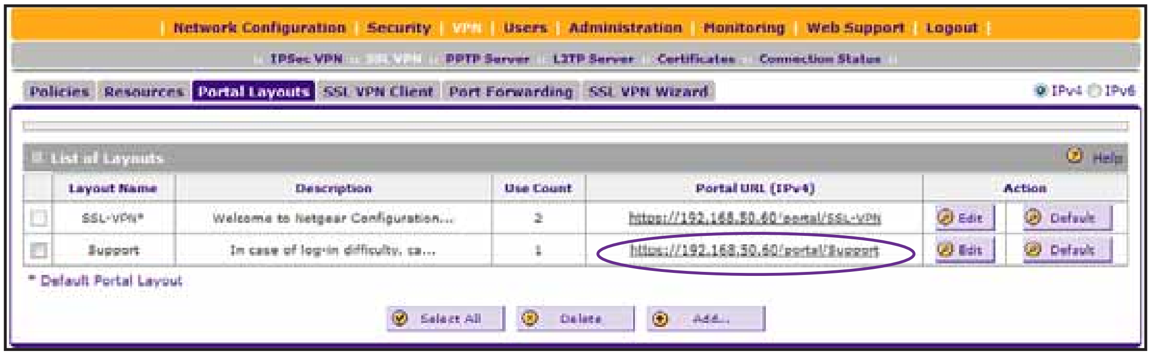
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **VPN > SSL VPN > Portal Layouts**.

   The Portal Layouts screen displays the IPv4 portals.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
IPSec VPN | SSL VPN | PPTP Server | L2TP Server | Certificates | Connection Status
Policies | Resources | Portal Layouts | SSL VPN Client | Port Forwarding | SSL VPN Wizard
● IPv4 ○ IPv6
Help
Select All
Delete
Add...

List of Layouts

	Layout Name	Description	Use Count	Portal URL (IPv4)	Action	
□	SSL-VPN*	Welcome to Netgear Configuration...	2	https://192.168.50.60/portal/SSL-VPN	Edit	Default
□	Support	In case of log-in difficulty, ca...	1	https://192.168.50.60/portal/Support	Edit	Default

* Default Portal Layout

7. To access an IPv6 portal instead of an IPv4 portal, in the upper right select the **IPv6** radio button.

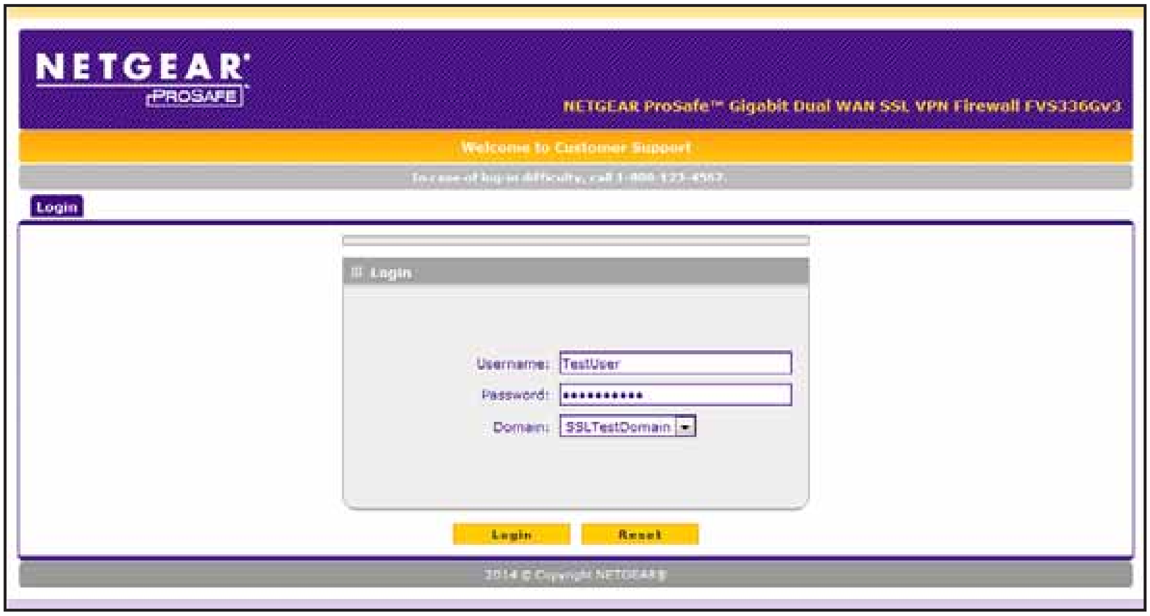
   The Portal Layouts screen displays the IPv6 portals.

8. In the Portal URL column of the List of Layouts table, click the URL for a portal.

   You can recognize a portal through the portal layout name with which a URL ends.

Note: This URL is the link that you must provide to a user who needs access to the portal. The user must enter this URL in the navigation toolbar of a browser. For you to enable a user outside the VPN firewall's local network to access the portal, the URL must have a public IP address.

The login screen displays.


NETGEAR
PROSAFE
NETGEAR ProSafe™ Gigabit Dual WAN SSL VPN Firewall FVS336Gv3
Welcome to Customer Support
In case of log-in difficulty, call 1-800-123-4567.
Login
Login
Login
Reset
2014 © Copyright NETGEAR®

Username: TestUser

Password: ●●●●●●●●●●●

Domain: SSLTestDomain

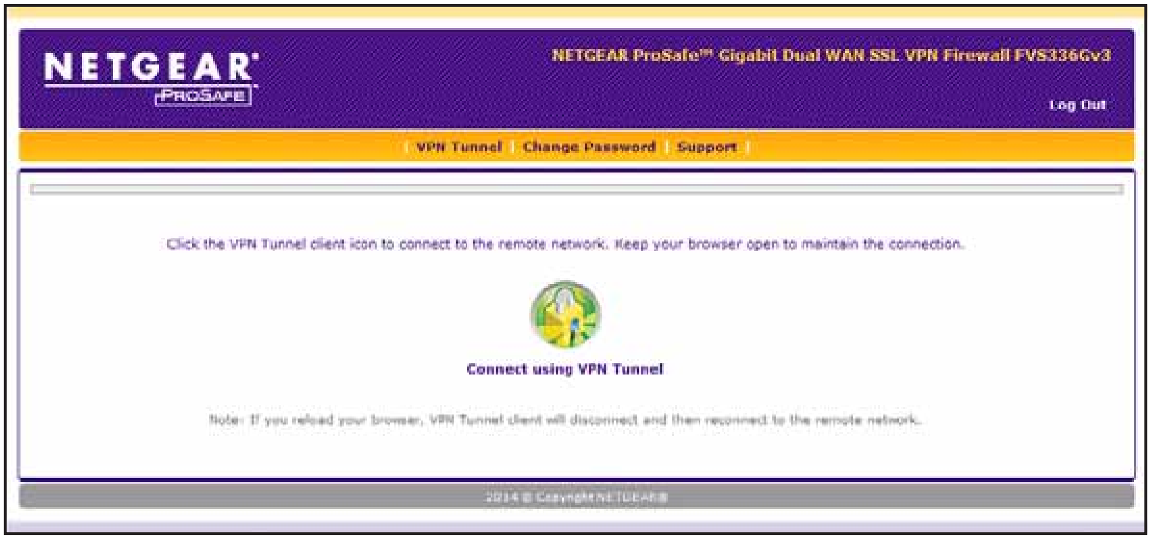
9. In the **Username** field, type the name that you associated with the portal and in the **Password / Passcode** field, type the password that you associated with the portal.
10. From the **Domain** menu, select the domain that you associated with the portal.

    Note: Any user for whom you have set up a user account that is linked to the domain for the portal and who has knowledge of the portal URL can access the portal. For information about setting up user accounts, see *Manage User Accounts* on page 498.

11. Click the **Login** button.

    A portal screen displays. The format of the portal screen depends on how you set up the portal.

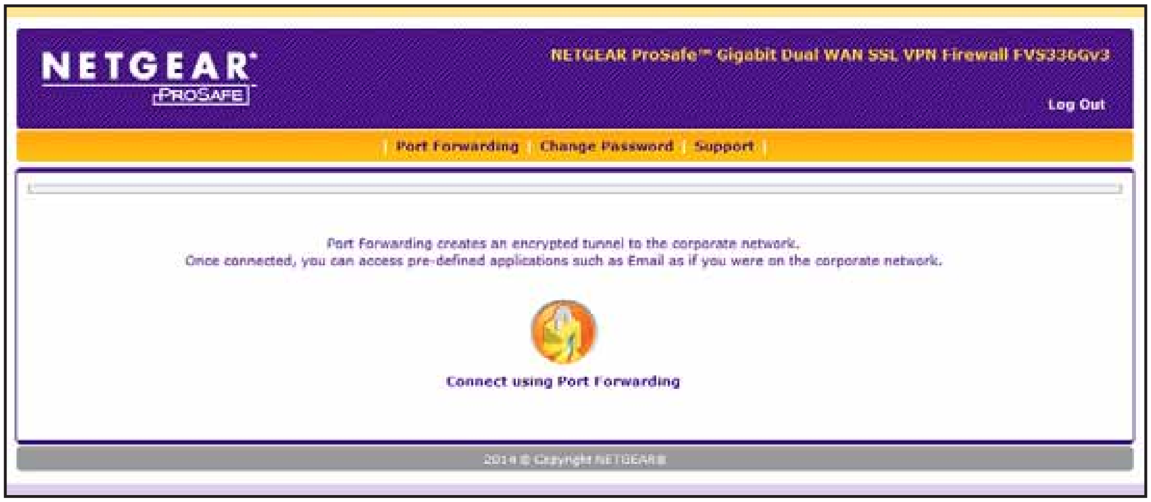
    The following figure shows a portal screen with a VPN Tunnel menu option only.


NETGEAR ProSAFE
NETGEAR ProSafe™ Gigabit Dual WAN SSL VPN Firewall FVS336Gv3
Log Out
| VPN Tunnel | Change Password | Support |
Connect using VPN Tunnel
2014 © Copyright NETGEAR®

Click the VPN Tunnel client icon to connect to the remote network. Keep your browser open to maintain the connection.

Note: If you reload your browser, VPN Tunnel client will disconnect and then reconnect to the remote network.

The following figure shows a portal screen with a Port Forwarding menu option only.


NETGEAR ProSAFE
NETGEAR ProSafe™ Gigabit Dual WAN SSL VPN Firewall FVS336Gv3
Log Out
| Port Forwarding | Change Password | Support |
Connect using Port Forwarding
2014 © Copyright NETGEAR®

Port Forwarding creates an encrypted tunnel to the corporate network.
Once connected, you can access pre-defined applications such as Email as if you were on the corporate network.

A portal screen displays a simple menu that provides the SSL user with the following menu selections:

- **VPN Tunnel**. Provides full network connectivity.
- **Port Forwarding**. Provides access to the network services that you defined (see *Build an SSL Portal with the SSL VPN Wizard* on page 429 or *Configure Applications for SSL VPN Port Forwarding* on page 453).
- **Change Password**. Allows the user to change the password.
- **Support**. Provides access to the NETGEAR website.

View SSL VPN Connection and Status Information

The following sections provide information about viewing the SSL VPN tunnel connections and log:

- *View the VPN Firewall SSL VPN Connection Status and Disconnect Active Users*
- *View the VPN Firewall SSL VPN Log*

View the VPN Firewall SSL VPN Connection Status and Disconnect Active Users

The following procedure describes how to view the connection status of all users who are logged in to an SSL portal on the VPN firewall and disconnect active users.

➢ **To view the status of all active SSL VPN users on the VPN firewall and disconnect active users:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

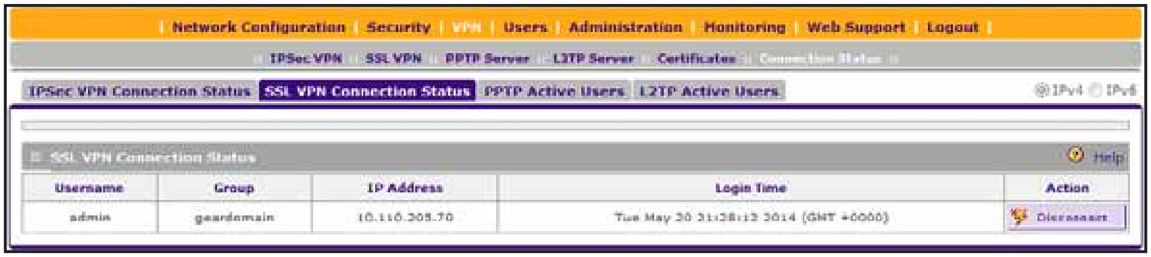
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > Connection Status > SSL VPN Connection Status**.

   The SSL VPN Connection Status screen displays.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
IPSec VPN | SSL VPN | PPTP Server | L2TP Server | Certificates | Connection Status
IPSec VPN Connection Status | SSL VPN Connection Status | PPTP Active Users | L2TP Active Users
IPv4 IPv6
Help

SSL VPN Connection Status

Username	Group	IP Address	Login Time	Action
admin	geardomain	10.116.205.70	Tue May 20 21:38:13 2014 (GMT +0000)	Disconnect

The SSL VPN Connection Status table lists each active connection with the information that is described in the following table.

Item	Description
Username	The user name that is associated with the SSL session.
Group	The group to which the user is assigned.
IP address	The IP address from the user is logged in.
Login Time	The time that the user logged in.
Action	The **Disconnect** button lets you terminate the SSL VPN tunnel connection. (This button displays only if an active SSL connection exists.)

7. To disable an active SSL user, in the SSL VPN Connection Status table, click the corresponding **Disconnect** button.

   The user is disconnected.

8. To disable another active L2TP user, repeat *Step 7*.

View the VPN Firewall SSL VPN Log

The SSL VPN log on the VPN firewall displays notifications and, if errors occur, error messages that are detected on the VPN firewall side. If problems occur during the SSL portal establishment process, these error messages can help you to determine what the problem is. (Misconfigration is the most common problem.)

➢ **To display the SSL VPN log on the VPN firewall:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

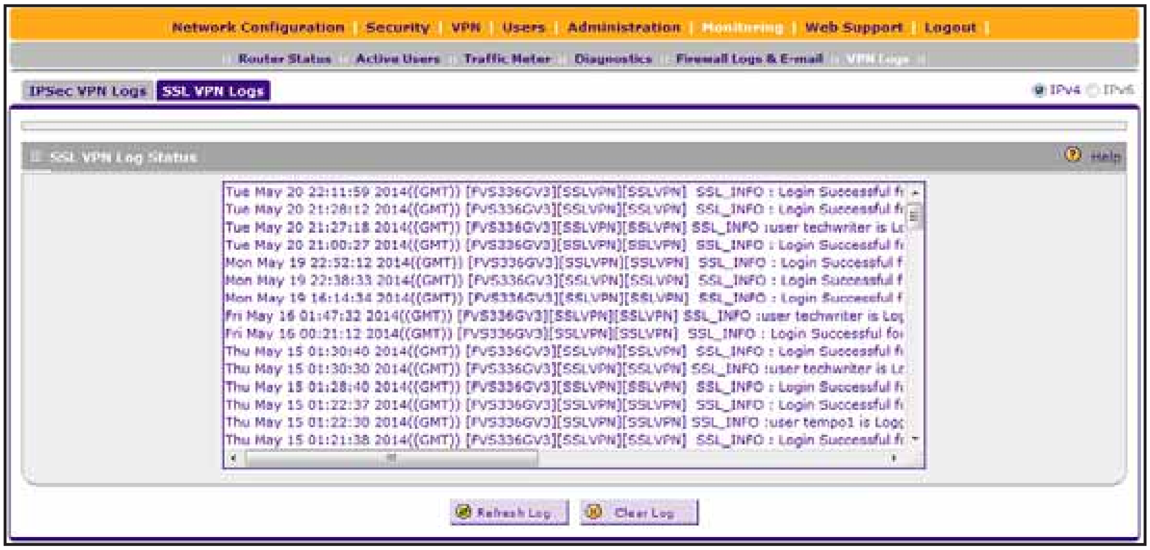
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Monitoring > VPN Logs > SSL VPN Logs**.

   The SSL VPN Logs screen displays.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
Router Status | Active Users | Traffic Meter | Diagnostics | Firewall Logs & E-mail | VPN Logs
IPSec VPN Logs
SSL VPN Logs
● IPv4 ○ IPv6
SSL VPN Log Status
Help
Refresh Log
Clear Log

```
Tue May 20 22:11:59 2014((GMT)) [FVS336GV3][SSLVPN][SSLVPN]  SSL_INFO : Login Successful fr
Tue May 20 21:28:12 2014((GMT)) [FVS336GV3][SSLVPN][SSLVPN]  SSL_INFO : Login Successful fr
Tue May 20 21:27:18 2014((GMT)) [FVS336GV3][SSLVPN][SSLVPN] SSL_INFO :user techwriter is Lo
Tue May 20 21:00:27 2014((GMT)) [FVS336GV3][SSLVPN][SSLVPN]  SSL_INFO : Login Successful fr
Mon May 19 22:52:12 2014((GMT)) [FVS336GV3][SSLVPN][SSLVPN]  SSL_INFO : Login Successful f
Mon May 19 22:38:33 2014((GMT)) [FVS336GV3][SSLVPN][SSLVPN]  SSL_INFO : Login Successful f
Mon May 19 14:14:34 2014((GMT)) [FVS336GV3][SSLVPN][SSLVPN]  SSL_INFO : Login Successful f
Fri May 16 01:47:32 2014((GMT)) [FVS336GV3][SSLVPN][SSLVPN] SSL_INFO :user techwriter is Log
Fri May 16 00:21:12 2014((GMT)) [FVS336GV3][SSLVPN][SSLVPN]  SSL_INFO : Login Successful for
Thu May 15 01:30:40 2014((GMT)) [FVS336GV3][SSLVPN][SSLVPN]  SSL_INFO : Login Successful fr
Thu May 15 01:30:30 2014((GMT)) [FVS336GV3][SSLVPN][SSLVPN] SSL_INFO :user techwriter is Lo
Thu May 15 01:28:40 2014((GMT)) [FVS336GV3][SSLVPN][SSLVPN]  SSL_INFO : Login Successful fr
Thu May 15 01:22:37 2014((GMT)) [FVS336GV3][SSLVPN][SSLVPN]  SSL_INFO : Login Successful fr
Thu May 15 01:22:30 2014((GMT)) [FVS336GV3][SSLVPN][SSLVPN] SSL_INFO :user tempo1 is Logg
Thu May 15 01:21:38 2014((GMT)) [FVS336GV3][SSLVPN][SSLVPN]  SSL_INFO : Login Successful fr
```

Manually Set Up or Change an SSL Portal

The following sections provide information about manually setting up or changing an SSL portal:

- *Manual SSL Configuration Overview*
- *Manage the Portal Layout*
- *Configure Applications for SSL VPN Port Forwarding*
- *Configure the SSL VPN Client*
- *Manage Network Resource Objects to Simplify Policies*
- *Configure User, Group, and Global Policies*

Manual SSL Configuration Overview

To configure and activate SSL connections, perform the following six basic steps in the order that they are presented:

1. Create an SSL portal layout (see *Manage the Portal Layout* on page 448).

   When remote users log in to the VPN firewall, they see a portal screen that you can customize to present the resources and functions that you want to make available.

2. Create authentication domains, user groups, and user accounts.

   Remote users connecting to the VPN firewall through an SSL VPN portal must be authenticated before they are granted access to the network. The login screen that is presented to the user requires three items: a user name, a password, and a domain selection. The domain determines both the authentication method and the portal layout that are used.

   For an SSL portal, you must create authentication domains, user groups, and user accounts as follows:

   a. Create one or more authentication domains for authentication of SSL VPN users (see *Manage Authentication Domains* on page 488).

      When remote users log in to the VPN firewall, they must specify a domain to which their login account belongs. The domain determines the authentication method that is used and the portal layout that is presented, which in turn determines the network resources to which the users are granted access. Because you must assign a portal layout when creating a domain, you create the domain after you create the portal layout.

   b. Create one or more groups for your SSL VPN users (*Manage Authentication Groups* on page 494).

      When you define the SSL VPN policies that determine network resource access for your SSL VPN users, you can define global policies, group policies, or individual policies. Because you must assign an authentication domain when creating a group, you create the group after you create the domain.

   c. Create one or more SSL VPN user accounts (see *Manage User Accounts* on page 498).

      Because you must assign a group when creating an SSL VPN user account, you first must create a group and then a user account.

3. For port forwarding, define the servers and services (see *Configure Applications for SSL VPN Port Forwarding* on page 453).

   Create a list of servers and services that can be made available through user, group, or global policies. You can also associate fully qualified domain names (FQDNs) with these servers. The VPN firewall resolves the names to the servers using the list you create.

4. For SSL VPN tunnel service, configure the virtual network adapter (see *Configure the SSL VPN Client* on page 459).

   For the SSL VPN tunnel option, the VPN firewall creates a virtual network adapter on the remote computer that then functions as if it were on the local network. Configure the portal's SSL VPN client to define a pool of local IP addresses to be issued to remote clients, as well as DNS addresses. Declare static routes or grant full access to the local network, subject to additional policies.

5. To simplify policies, define network resource objects (see *Manage Network Resource Objects to Simplify Policies* on page 467).

   Network resource objects are groups of IP addresses, IP address ranges, and services. By defining resource objects, you can more quickly create and configure network policies.

6. Configure the SSL VPN policies (see *Configure User, Group, and Global Policies* on page 473).

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

Manage the Portal Layout

The following sections provide information about managing the portal layout:

- *Portal Layouts Overview*
- *Create a Portal Layout*
- *Change a Portal Layout*
- *Remove One or More Portal Layouts*

Portal Layouts Overview

You can create a custom screen that remote users see when they log in to the SSL portal. Because the login screen is customizable, it provides an ideal way to communicate remote access instructions, support information, technical contact information, or VPN-related news updates to remote users. The login screen is also suitable as a starting screen for restricted users; if mobile users or business partners are permitted to access only a few resources, the login screen that you create presents only the resources that are relevant to these users.

You apply portal layouts by selecting one from the available portal layouts in the configuration of a domain. When you have completed your portal layout, you can apply the portal layout to one or more authentication domains (see *Manage Authentication Domains* on page 488). You can also make the new portal the default portal for the SSL VPN gateway.

The VPN firewall’s default portal address is https://<IP_address>/portal/SSL-VPN, in which the IP address can be either an IPv4 or an IPv6 address. Both types of addresses are supported simultaneously. The default domain geardomain is assigned to the default SSL-VPN portal.

If you have enabled IPv6 (see *Manage the IPv6 Routing Mode* on page 88), when you create a portal with an IPv4 address, the same portal is automatically created with an IPv6 address, and the other way around; when you create a portal with an IPv6 address, the same portal is automatically created with an IPv4 address.

You can define individual layouts for the SSL VPN portal. The layout configuration includes the menu layout, theme, portal pages to display, and web cache control options. The default portal layout is the SSL-VPN portal. You can add additional portal layouts. You can also make any portal the default portal for the VPN firewall.

Create a Portal Layout

The portal layout specifies the login screen that you present to an SSL VPN user and determines the type of access that you grant.

➤ **To create a portal layout:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

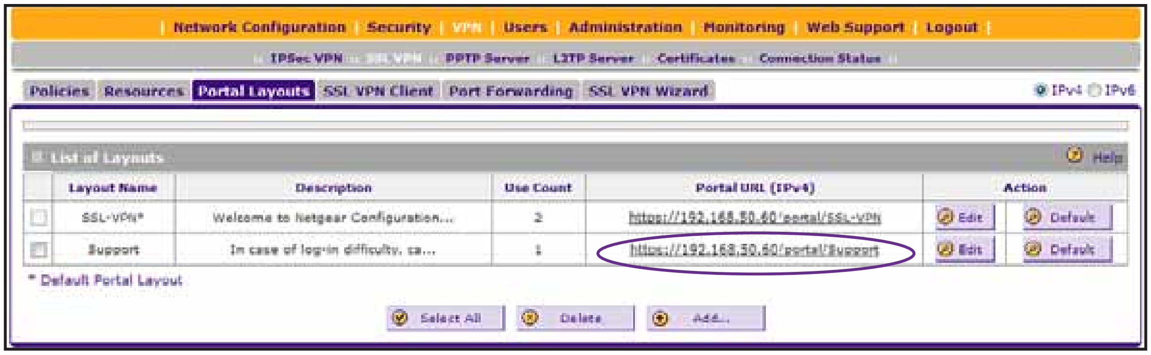
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > SSL VPN > Portal Layouts**.

   The Portal Layouts screen displays the IPv4 settings. The following figure shows the default IPv4 SSL portal (SSL-VPN) and a custom portal.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
IPSec VPN | SSL VPN | PPTP Server | L2TP Server | Certificates | Connection Status
Policies | Resources | Portal Layouts | SSL VPN Client | Port Forwarding | SSL VPN Wizard
● IPv4 ○ IPv6
List of Layouts
Help
Select All
Delete
Add...

	Layout Name	Description	Use Count	Portal URL (IPv4)	Action	
□	SSL-VPN*	Welcome to Netgear Configuration...	2	https://192.168.50.60/portal/SSL-VPN	Edit	Default
□	Support	In case of log-in difficulty, ca...	1	https://192.168.50.60/portal/Support	Edit	Default

* Default Portal Layout

Note: If you have enabled IPv6 (see *Manage the IPv6 Routing Mode* on page 88), when you create a portal with an IPv4 address, the same portal is automatically created with an IPv6 address.

The List of Layouts table displays the following fields:

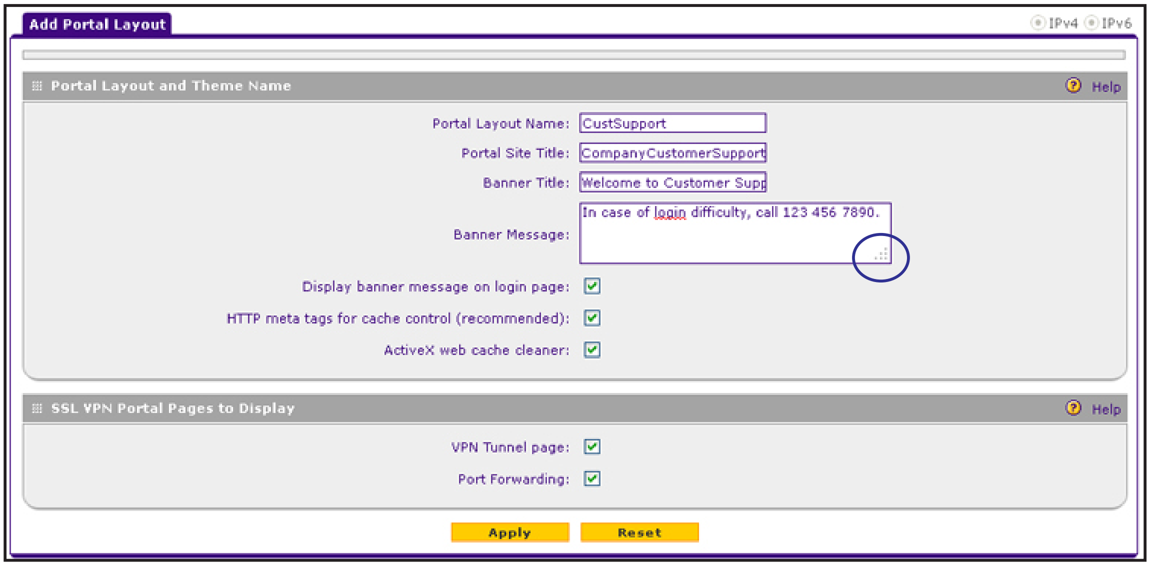
- **Layout Name**. The descriptive name of the portal.

- **Description**. The banner message that is displayed at the top of the portal.
- **Use Count**. The number of authentication domains that use the portal.
- **Portal URL (IPv4)**. The IPv4 URL at which the portal can be accessed. The IPv4 address in the URL is the public WAN address of the VPN firewall (see *Configure the IPv4 Internet Connection and WAN Settings* on page 30).

  If you have enabled IPv6, you can see the IPv6 URL by selecting the **IPv6** radio button.
- **Action**. The buttons, which allow you to change the portal layout or set it as the default.

7. Under the List of Layouts table, click the **Add** button.

   The Add Portal Layout screen displays. The following figure shows an example.



Portal Layout and Theme Name

Portal Layout Name: CustSupport

Portal Site Title: CompanyCustomerSupport

Banner Title: Welcome to Customer Supp

Banner Message: In case of login difficulty, call 123 456 7890.

Display banner message on login page: ☑

HTTP meta tags for cache control (recommended): ☑

ActiveX web cache cleaner: ☑

SSL VPN Portal Pages to Display

VPN Tunnel page: ☑

Port Forwarding: ☑

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

Setting	Description
Portal Layout and Theme Name	
Portal Layout Name	A descriptive name for the portal layout. This name is part of the path of the SSL VPN portal URL. Use only alphanumeric characters, hyphens (-), and underscores (_) in the **Portal Layout Name** field. If you enter other types of characters or spaces, the layout name is truncated before the first nonalphanumeric character, hyphen, or underscore. Unlike most other names in URLs, this name is case-sensitive. **Note:** To create a portal layout, you must enter a name other than SSL-VPN (the default portal name) in the **Portal Layout Name** field.
Portal Site Title	The title that displays at the top of the user's web browser window, for example, *Company Customer Support*.

Setting	Description
Banner Title	The banner title of a banner message that users see before they log in to the portal, for example, *Welcome to Customer Support*. **Note:** For an example, see *Access a Custom SSL VPN Portal* on page 440. The banner title is displayed in the orange header bar of the login screen that is shown in the procedure.
Banner Message	The text of a banner message that users see before they log in to the portal, for example, *In case of log-in difficulty, call 123-456-7890*. Enter a plain text message, or include HTML and JavaScript tags. The maximum length of the login screen message is 4096 characters. **Note:** You can enlarge the field (that is, the text box) by manipulating the lower right corner of the field (see the blue circle in the previous figure). **Note:** For an example, see *Access a Custom SSL VPN Portal* on page 440. The banner message text is displayed in the gray header bar of the login screen that is shown in the procedure.
Display banner message on login page	Select this check box to show the banner title and banner message text on the login screen.

HTTP meta tags for cache control (recommended)	Select this check box to apply HTTP meta tag cache control directives to this portal layout. Cache control directives include the following:
	`<meta http-equiv=”pragma” content=”no-cache”>`
	`<meta http-equiv=”cache-control” content=”no-cache”>`
	`<meta http-equiv=”cache-control” content=”must-revalidate”>`
	Note: NETGEAR strongly recommends enabling HTTP meta tags for security reasons and to prevent out-of-date web pages, themes, and data being stored in a user’s web browser cache.

ActiveX web cache cleaner	Select this check box to enable ActiveX cache control to be loaded when users log in to the SSL VPN portal. The web cache cleaner prompts the user to remove all temporary Internet files, cookies, and browser history when the user logs out or closes the web browser window. The ActiveX web cache control is ignored by web browsers that do not support ActiveX.
SSL VPN Portal Pages to Display **Note:** Although you can select both, you typically select either the **VPN Tunnel page** check box or the **Port Forwarding** check box.	
VPN Tunnel page	To provide full network connectivity, select this check box.
Port Forwarding	To provide access to specific defined network services, select this check box. For information about specifying network services, see *Configure Applications for SSL VPN Port Forwarding* on page 453.

9. Click the **Apply** button.

   Your settings are saved. The new portal layout is added to the List of Layouts table.

   For information about how to display the new portal layout, see *Access a Custom SSL VPN Portal* on page 440.

Change a Portal Layout

The following procedure describes how to change an existing portal layout. If you enabled IPv6 (see *Manage the IPv6 Routing Mode* on page 88), changes that you make to an IPv4 portal layout are automatically applied to the corresponding IPv6 portal layout, or the other way around. For this reason, the following procedure describes how to change an IPv4 portal layout only.

➢ **To change a portal layout:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > SSL VPN > Portal Layouts**.

   The Portal Layouts screen displays the IPv4 settings.
7. In the List of Layouts table, click the **Edit** button for the portal layout that you want to change.

   The Edit Portal Layout screen displays.
8. Change the settings.

   For more information about the settings, see *Create a Portal Layout* on page 449.
9. Click the **Apply** button.

   Your settings are saved to the IPV4 portal layout and the corresponding IPv6 portal layout. The modified portal layout displays in the List of Layouts table on the Portal Layouts screen.

Remove One or More Portal Layouts

The following procedure describes how to remove existing portal layouts. You cannot remove the default portal layout (SSL-VPN). If you enabled IPv6 (see *Manage the IPv6 Routing Mode* on page 88), if you remove an IPv4 portal layout, the corresponding IPv6 portal layout is removed automatically, and the other way around. If you remove an IPv6 portal layout, the corresponding IPv4 portal is removed automatically. For this reason, the following procedure describes the removal of IPv4 portal layouts only.

➢ **To remove one or more portal layouts:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > SSL VPN > Portal Layouts**.

   The Portal Layouts screen displays the IPv4 settings.
7. In the List of Layouts table, select the check box to the left of each portal layout that you want to remove or click the **Select All** button to select all layouts.
8. Click the **Delete** button.

   The selected IPv4 portal layouts and the corresponding IPv6 portal layouts are removed from the List of Layouts table.

Configure Applications for SSL VPN Port Forwarding

The following sections provide information about managing SSL port forwarding:

- *SSL VPN Port Forwarding Overview*
- *Add a Server and Port Number for SSL Port Forwarding*
- *Add a Host Name for SSL Port Forwarding*
- *Remove a Server and Port Number Configuration for SSL Port Forwarding*
- *Remove a Host Name for SSL Port Forwarding*

SSL VPN Port Forwarding Overview

Note: SSL port forwarding does not apply if you configure full VPN tunnel capability for an SSL portal. SSL VPN port forwarding is supported for IPv4 connections only.

Port forwarding provides access to specific defined network services. To define these services, you must specify the internal server addresses and port numbers for TCP applications that are intercepted by the port forwarding client on the user's computer. This client reroutes the traffic to the VPN firewall.

After you have configured port forwarding by defining the IP addresses of internal servers or host computers and the port number for TCP applications or services that are available to remote users, you can also specify host name-to-IP address resolution for the network servers as a convenience for users. Host name resolution allows users to access TCP applications at familiar addresses such as mail.*example*.com or ftp.*customer*.com, that is, fully qualified domain names (FQDNs), rather than by IP addresses.

Any applications and services that you do not select for SSL port forwarding are not visible from the SSL VPN portal. However, if users know the IP address of an application or service, they can still access it unless you create SSL VPN access policies to prevent access to the application or service.

The following table lists some commonly used TCP applications and port numbers that you could use for port forwarding.

Table 8. Port forwarding applications and TCP port numbers

TCP Application	Port Number
FTP data (usually not needed)	20
FTP Control Protocol	21
SSH	22[a]
Telnet	23[a]
SMTP (send mail)	25
HTTP (web)	80
POP3 (receive mail)	110
NTP (Network Time Protocol)	123
Citrix	1494
Terminal Services	3389
VNC (virtual network computing)	5900 or 5800

[a] *Users can specify the port number together with the host name or IP address.*

Add a Server and Port Number for SSL Port Forwarding

To configure port forwarding, you must define the IP addresses of the internal servers and the port number for TCP applications and services that are available to remote users.

➤ **To add a server and port number for an SSL port forwarding application or service:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

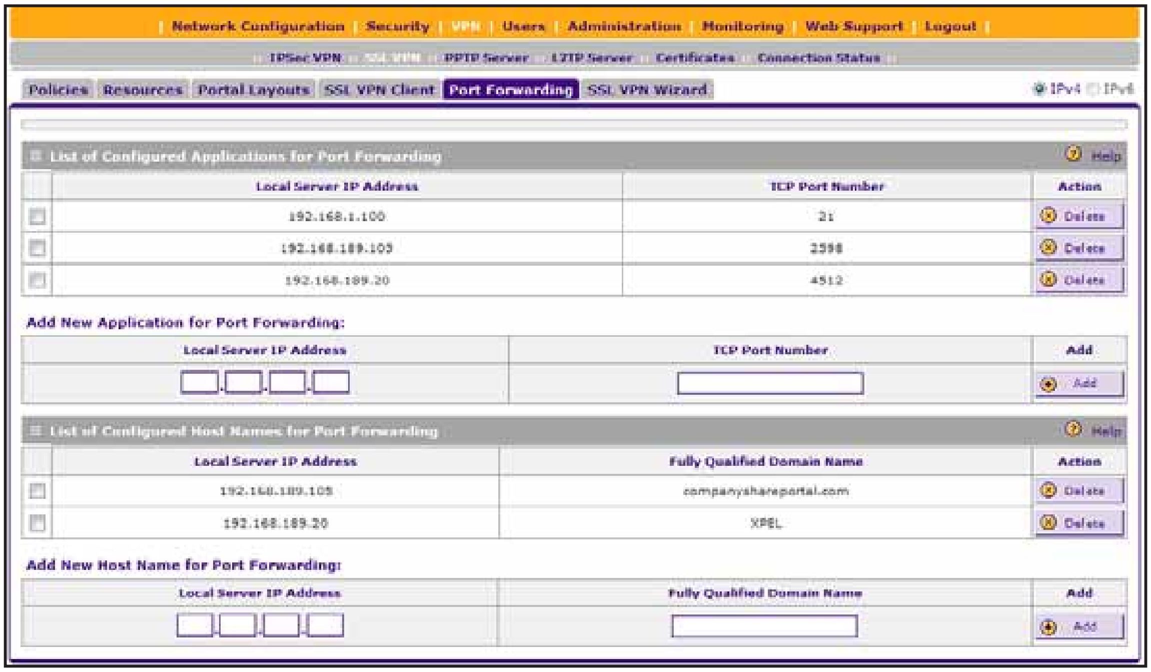
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > SSL VPN > Port Forwarding**.

   The Port Forwarding screen displays. The following figure shows examples.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
IPSec VPN | SSL VPN | PPTP Server | L2TP Server | Certificates | Connection Status
Policies | Resources | Portal Layouts | SSL VPN Client | Port Forwarding | SSL VPN Wizard
● IPv4 ○ IPv6
Help

List of Configured Applications for Port Forwarding

	Local Server IP Address	TCP Port Number	Action
□	192.168.1.100	21	Delete
□	192.168.189.105	2598	Delete
□	192.168.189.20	4512	Delete

Add New Application for Port Forwarding:

Local Server IP Address	TCP Port Number	Add
. . .		Add

List of Configured Host Names for Port Forwarding

	Local Server IP Address	Fully Qualified Domain Name	Action
□	192.168.189.105	companysharepotal.com	Delete
□	192.168.189.20	XPEL	Delete

Add New Host Name for Port Forwarding:

Local Server IP Address	Fully Qualified Domain Name	Add
. . .		Add

7. In the Add New Application for Port Forwarding section, complete the following fields:
   - **IP Address**. The IP address of an internal server or host computer on which a service or application runs to which you want to grant a remote user access.
   - **TCP Port**. The TCP port number of the service or application that is accessed through the SSL VPN tunnel.
8. In the Add New Application for Port Forwarding section, click the **Add** button.

   The application or service entry is added to the List of Configured Applications for Port Forwarding table. After logging in to the SSL VPN portal and launching port forwarding, remote users can securely access the network application or service.

Add a Host Name for SSL Port Forwarding

If a server or host computer that you want to name does not display in the List of Configured Applications for Port Forwarding table, you first must add it before you can name it (see *Add a Server and Port Number for SSL Port Forwarding* on page 455).

➢ **To add a host name for client name resolution:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

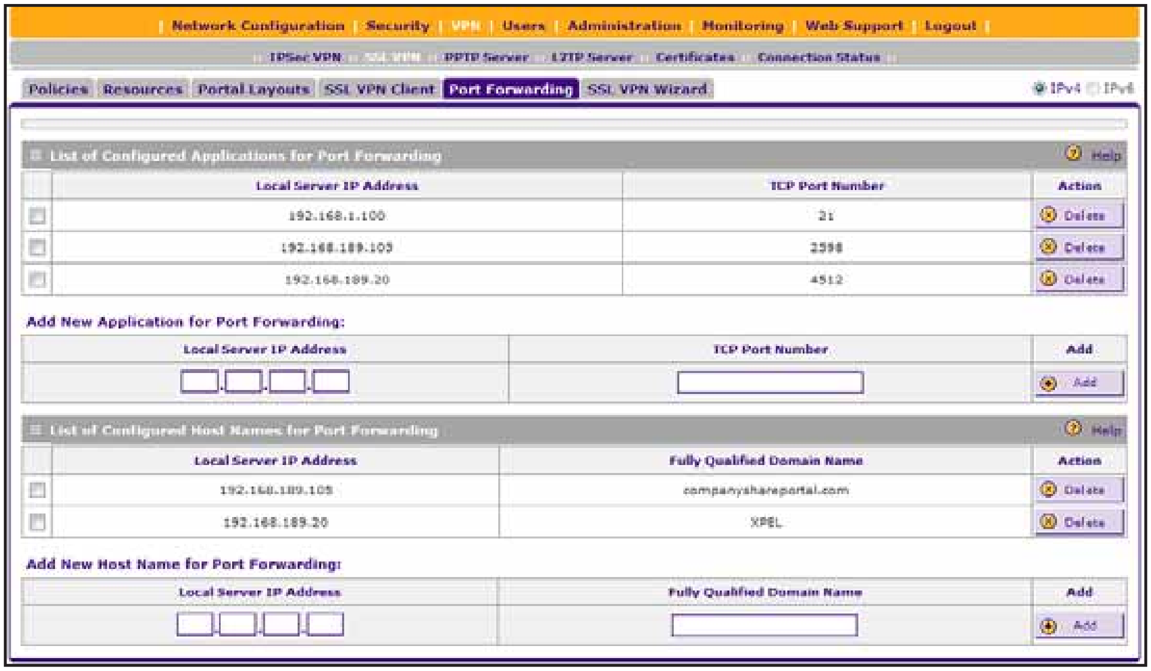
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > SSL VPN > Port Forwarding**.

   The Port Forwarding screen displays. The following figure shows examples.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
Policies
Resources
Portal Layouts
SSL VPN Client
Port Forwarding
SSL VPN Wizard
Help
Delete
Add

● IPv4 ○ IPv6

List of Configured Applications for Port Forwarding

	Local Server IP Address	TCP Port Number	Action
□	192.168.1.100	21	Delete
□	192.168.189.105	2598	Delete
□	192.168.189.20	4512	Delete

Add New Application for Port Forwarding:

Local Server IP Address	TCP Port Number	Add
☐.☐.☐.☐	☐	Add

List of Configured Host Names for Port Forwarding

	Local Server IP Address	Fully Qualified Domain Name	Action
□	192.168.189.105	companysharepoint.com	Delete
□	192.168.189.20	XPEL	Delete

Add New Host Name for Port Forwarding:

Local Server IP Address	Fully Qualified Domain Name	Add
☐.☐.☐.☐	☐	Add

7. In the Add New Host Name for Port Forwarding section, specify information in the following fields:
   - **Local Server IP Address**. The IP address of the internal server or host computer that you want to name. You can name only IP addresses that are listed in the List of Configured Applications for Port Forwarding table.
   - **Fully Qualified Domain Name**. The full name of the internal server or host computer.
8. In the Add New Host Name for Port Forwarding section, click the **Add** button.

   The IP address and FQDN are added to the List of Configured Host Names for Port Forwarding table.

Remove a Server and Port Number Configuration for SSL Port Forwarding

The following procedure describes how to remove a server and port number configuration that you no longer need for an SSL port forwarding application or service.

➢ **To remove a server and port number configuration:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **VPN > SSL VPN > Port Forwarding**.

   The Port Forwarding screen displays.

7. In the List of Configured Applications for Port Forwarding table, to the right of the application or service that you want to remove, click the corresponding **Delete** button.

   The IP address and port number are removed from the List of Configured Applications for Port Forwarding table.

Remove a Host Name for SSL Port Forwarding

The following procedure describes how to remove a host name that you no longer need.

➢ **To remove a host name for SSL port forwarding:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **VPN > SSL VPN > Port Forwarding**.

   The Port Forwarding screen displays.

7. In the List of Configured Applications for Port Forwarding table, to the right of the host name that you want to remove, click the corresponding **Delete** button.

   The IP address and port number are removed from the List of Configured Applications for Port Forwarding table.

Configure the SSL VPN Client

The following sections provide information about configuring SSL VPN clients:

- *SSL VPN Clients Overview*
- *Configure the Client IPv4 Address Range*
- *Add an IPv4 Route for VPN Tunnel Clients*
- *Configure the Client IPv6 Address Range*
- *Add an IPv6 Route for VPN Tunnel Clients*
- *Remove an IPv4 or IPv6 Client Route*

SSL VPN Clients Overview

Note: The SSL VPN client does not apply if you configure port forwarding capability for an SSL portal. The SSL VPN client applies only for VPN tunnel capability.

The SSL VPN client on the VPN firewall assigns IP addresses to remote VPN tunnel clients. Because the VPN tunnel connection is a point-to-point connection, you can assign IP addresses from the local subnet to the remote VPN tunnel clients.

The following are some additional considerations for the SSL VPN client:

- To prevent the virtual (PPP) interface address of a VPN tunnel client from conflicting with addresses on the local network, configure an IP address range that does not directly overlap with addresses on your local network. For example, if 192.168.1.1 through 192.168.1.100 are assigned to devices on the local network, start the client address range at 192.168.1.101, or choose an entirely different subnet altogether.
- The VPN tunnel client cannot contact a server on the local network if the VPN tunnel client’s Ethernet interface shares the same IP address as the server or the VPN firewall. (For example, if your computer has a network interface IP address of 10.0.0.45, you cannot contact a server on the remote network that also has the IP address 10.0.0.45.)
- Select whether you want to enable full-tunnel or split-tunnel support based on your bandwidth:
  - A full tunnel sends all of the client’s traffic across the VPN tunnel.
  - A split tunnel sends only traffic that is destined for the local network based on the specified client routes. All other traffic is sent to the Internet. A split tunnel allows you to manage bandwidth by reserving the VPN tunnel for local traffic only.

- If you enable split-tunnel support and you assign an entirely different subnet to the VPN tunnel clients from the subnet that is used by the local network, you must add a client route to ensure that a VPN tunnel client connects to the local network over the VPN tunnel.

Configure the Client IPv4 Address Range

The following procedure describes how to define the client IPv4 address range.

➢ **To define the client IPv4 address range:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

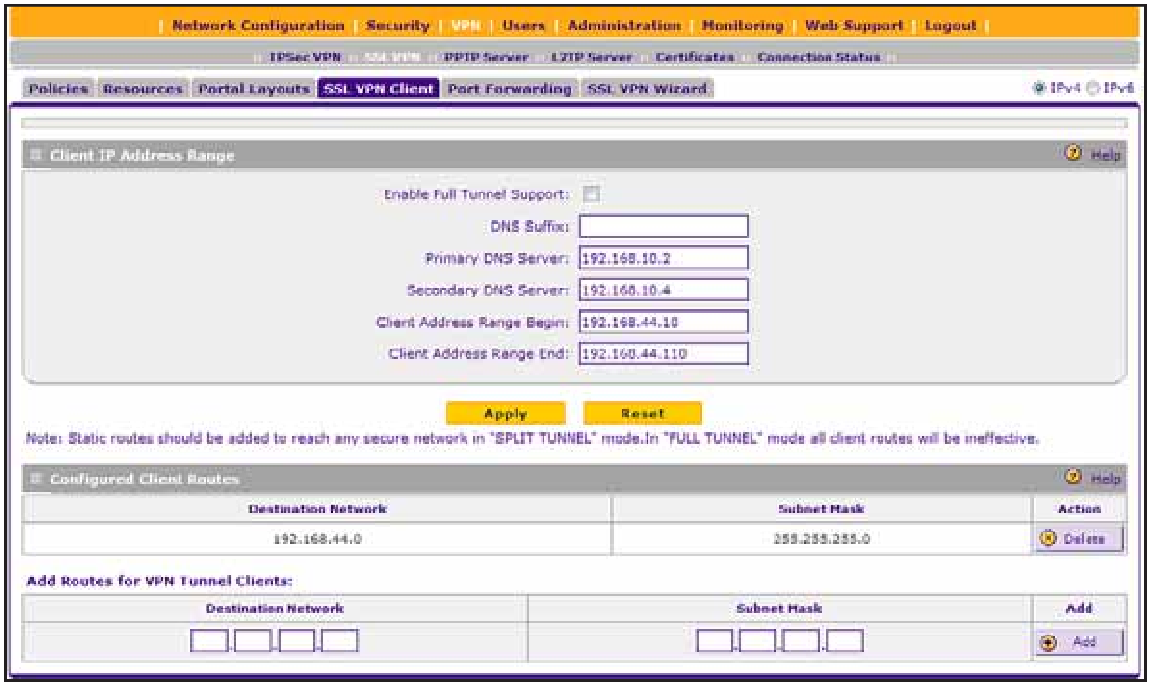
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > SSL VPN > SSL VPN Client**.

   The SSL VPN Client screen displays the IPv4 settings. The following figure shows an example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
|| IPSec VPN || SSL VPN || PPTP Server || L2TP Server || Certificates || Connection Status ||
Policies
Resources
Portal Layouts
SSL VPN Client
Port Forwarding
SSL VPN Wizard
● IPv4 ○ IPv6
Help
Apply
Reset
Help
Delete
Add

Client IP Address Range

Enable Full Tunnel Support: □

DNS Suffix:

Primary DNS Server: 192.168.10.2

Secondary DNS Server: 192.168.10.4

Client Address Range Begin: 192.168.44.10

Client Address Range End: 192.168.44.110

Note: Static routes should be added to reach any secure network in "SPLIT TUNNEL" mode.In "FULL TUNNEL" mode all client routes will be ineffective.

Configured Client Routes

Destination Network	Subnet Mask	Action
192.168.44.0	255.255.255.0	Delete

Add Routes for VPN Tunnel Clients:

Destination Network	Subnet Mask	Add
□.□.□.□	□.□.□.□	Add

7. In the Client IP Address Range section, enter the settings as described in the following table.

Setting	Description
Enable Full Tunnel Support	Select this check box to enable full-tunnel support. Full tunnel support provides clients access to the entire LAN network. If you leave this check box cleared (which is the default setting), full-tunnel support is disabled but split-tunnel support is enabled. You must add one or more IPv4 client routes to provide clients access to specific networks (see *Add an IPv4 Route for VPN Tunnel Clients* on page 462). **Note:** When full-tunnel support is enabled, client routes are not operable.
DNS Suffix	A DNS suffix to be appended to incomplete DNS search strings. This setting is optional.
Primary DNS Server	The IP address of the primary DNS server that is assigned to the VPN tunnel clients. This setting is optional. **Note:** If you do not assign a DNS server, the DNS settings remain unchanged in the SSL VPN client after a VPN tunnel is established.
Secondary DNS Server	The IP address of the secondary DNS server that is assigned to the VPN tunnel clients. This setting is optional.
Client Address Range Begin	The first IP address of the IPv4 address range that you want to assign to the VPN tunnel clients. By default, the first IPv4 address is 192.168.251.1.
Client Address Range End	The last IP address of the IPv4 address range that you want to assign to the VPN tunnel clients. By default, the last IPv4 address is 192.168.251.254.

8. Click the **Apply** button.

Your settings are saved. VPN tunnel clients are now able to connect to the VPN firewall and receive a virtual IPv4 address in the client address range.

Add an IPv4 Route for VPN Tunnel Clients

If the assigned client IPv4 address range is in a different subnet from the local network, or if the local network has multiple subnets, or if you select split-tunnel operation, you must define client routes.

➢ **To add an IPv4 route for SSL VPN tunnel clients:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

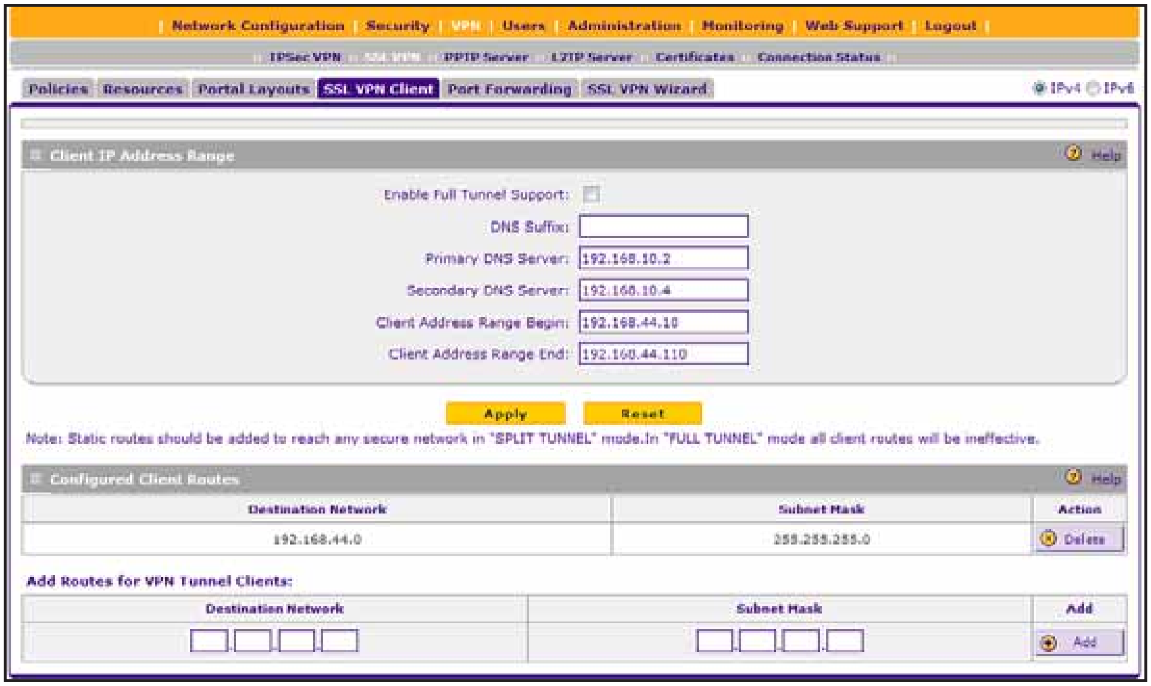
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > SSL VPN > SSL VPN Client**.

   The SSL VPN Client screen displays the IPv4 settings. The following figure shows an example.



● IPv4 ○ IPv6

Client IP Address Range

Enable Full Tunnel Support: □
DNS Suffix:
Primary DNS Server: 192.168.10.2
Secondary DNS Server: 192.168.10.4
Client Address Range Begin: 192.168.44.10
Client Address Range End: 192.168.44.110

Apply Reset

Note: Static routes should be added to reach any secure network in "SPLIT TUNNEL" mode.In "FULL TUNNEL" mode all client routes will be ineffective.

Configured Client Routes

Destination Network	Subnet Mask	Action
192.168.44.0	255.255.255.0	Delete

Add Routes for VPN Tunnel Clients:

Destination Network	Subnet Mask	Add
___.___.___.___	___.___.___.___	Add

7. In the Add Routes for VPN Tunnel Clients section, complete the following fields:
   - **Destination Network**. The IPv4 address of the local destination network or subnet that provides access to one or more port forwarding applications and services.
   - **Subnet Mask**. The subnet mask for the local destination or subnet.
8. Click the **Add** button.

   The new client route is added to the Configured Client Routes table.

Note: If VPN tunnel clients are already connected, you can disconnect the clients (see *View the VPN Firewall SSL VPN Connection Status and Disconnect Active Users* on page 444) to allow them to receive new addresses and routes when they reconnect.

Configure the Client IPv6 Address Range

If you enabled IPv6 (see *Manage the IPv6 Routing Mode* on page 88), you can define the IPv6 address range to be assigned to VPN tunnel clients.

➢ **To define the client IPv6 address range:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

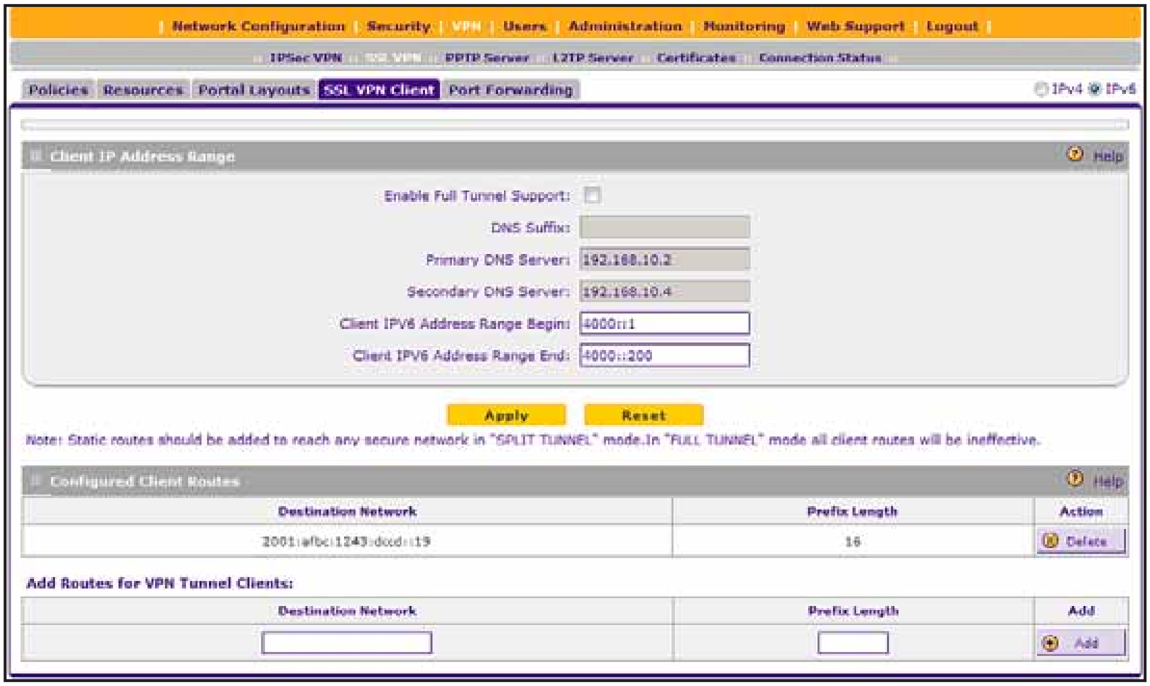
   The Router Status screen displays.

6. Select **VPN > SSL VPN > SSL VPN Client**.

   The SSL VPN Client screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The SSL VPN Client screen displays the IPv6 settings. The following figure shows an example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
Policies
Resources
Portal Layouts
SSL VPN Client
Port Forwarding
○ IPv4 ● IPv6
Client IP Address Range
Help
Apply
Reset
Configured Client Routes
Help
Delete
Add

Enable Full Tunnel Support: □

DNS Suffix:

Primary DNS Server: 192.168.10.2

Secondary DNS Server: 192.168.10.4

Client IPV6 Address Range Begin: 4000::1

Client IPV6 Address Range End: 4000::200

Note: Static routes should be added to reach any secure network in "SPLIT TUNNEL" mode.In "FULL TUNNEL" mode all client routes will be ineffective.

Destination Network	Prefix Length	Action
2001:afbc:1243:dccd::19	16	Delete

Add Routes for VPN Tunnel Clients:

Destination Network	Prefix Length	Add
		Add

8. In the Client IP Address Range section, enter the settings as described in the following table.

Setting	Description
Enable Full Tunnel Support	Select this check box to enable full-tunnel support. If you leave this check box cleared (which is the default setting), full-tunnel support is disabled but split-tunnel support is enabled and you must add an IPv6 client route (see *Add an IPv6 Route for VPN Tunnel Clients* on page 465). **Note:** When full-tunnel support is enabled, client routes are not operable.
Client IPv6 Address Range Begin	The first IP address of the IPv6 address range that you want to assign to the VPN tunnel clients. By default, the first IPv6 address is 4000::1.
Client IPv6 Address Range End	The last IP address of the IPv6 address range that you want to assign to the VPN tunnel clients. By default, the last IPv6 address is 4000::200.

9. Click the **Apply** button.

   Your settings are saved. VPN tunnel clients are now able to connect to the VPN firewall and receive a virtual IPv6 address in the client address range.

Add an IPv6 Route for VPN Tunnel Clients

If the assigned client IPv6 address range is different from the local network address range, or if the local network uses multiple address ranges, or if you select split-tunnel operation, you must define IPv6 client routes.

- **To add an IPv6 route for SSL VPN tunnel clients:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

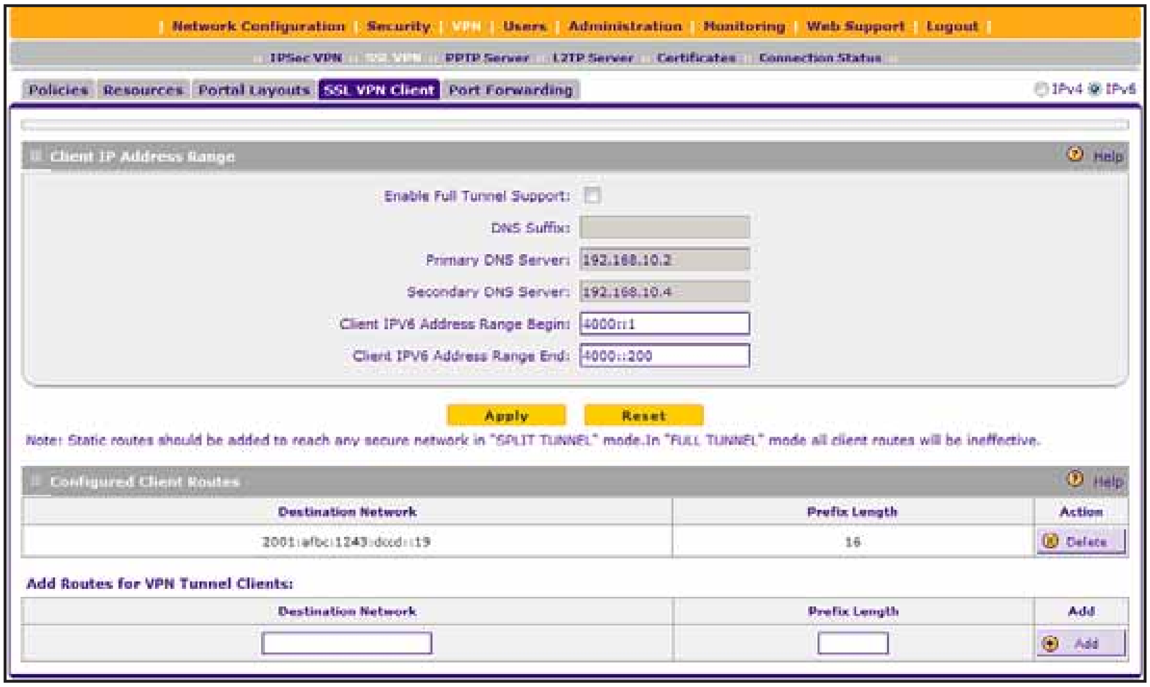
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > SSL VPN > SSL VPN Client**.

   The SSL VPN Client screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The SSL VPN Client screen displays the IPv6 settings. The following figure shows examples.



Client IP Address Range

Enable Full Tunnel Support: □

DNS Suffix:

Primary DNS Server: 192.168.10.2

Secondary DNS Server: 192.168.10.4

Client IPV6 Address Range Begin: 4000::1

Client IPV6 Address Range End: 4000::200

Note: Static routes should be added to reach any secure network in "SPLIT TUNNEL" mode.In "FULL TUNNEL" mode all client routes will be ineffective.

Configured Client Routes

Destination Network	Prefix Length	Action
2001:afbc:1243:dccd::19	16	Delete

Add Routes for VPN Tunnel Clients:

Destination Network	Prefix Length	Add
		Add

8. In the Add Routes for VPN Tunnel Clients section, complete the following fields:
   - **Destination Network**. The IPv6 address of the local destination network that provides access to one or more port forwarding applications and services.
   - **Prefix Length**. The prefix length for the local destination network.
9. Click the **Add** button.

   The new client route is added to the Configured Client Routes table.

Note: If VPN tunnel clients are already connected, you can disconnect the clients (see *View the VPN Firewall SSL VPN Connection Status and Disconnect Active Users* on page 444) to allow them to receive new addresses and routes when they reconnect.

Remove an IPv4 or IPv6 Client Route

The following procedure describes how to remove a client route that you no longer need.

➤ **To remove an IPv4 or IPv6 client route:**

1. On your computer, launch an Internet browser.

2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **VPN > SSL VPN > SSL VPN Client**.

   The SSL VPN Client screen displays the IPv4 settings.

7. To remove an IPv6 client route instead of an IPv4 client route, in the upper right, select the **IPv6** radio button.

   The SSL VPN Client screen displays the IPv6 settings.

8. In the Configured Client Routes table, to the right of the route that you want to remove, click the corresponding **Delete** button.

   The route is removed from the Configured Client Routes table.

Manage Network Resource Objects to Simplify Policies

The following sections provide information about managing network resource objects for SSL port forwarding:

- *Network Objects Overview*
- *Add an SSL Network Resource*
- *Define or Change an IPv4 or IPv6 Network Resource and Resource Address*
- *Remove One or More SSL Network Resources*
- *Remove an IPv4 or IPv6 SSL Resource Address Configuration*

Network Objects Overview

Network resources are groups of IP addresses, IP address ranges, and applications and services. By defining resource objects, you can more quickly create and configure network policies. You do not need to redefine the same set of IP addresses or address ranges when you configure the same access policies for multiple users.

Defining network resources is optional; smaller organizations can choose to create access policies using individual IP addresses or IP networks rather than predefined network resources. But for most organizations, NETGEAR recommends that you use network resources. If your server or network configuration changes, you can perform an update quickly by using network resources instead of individually updating all of the user and group policies.

Add an SSL Network Resource

The resource name and service are independent of the IP version. However, the resource definition (see *Define or Change an IPv4 or IPv6 Network Resource and Resource Address* on page 469) depends on the IP version because you can assign either an IPv4 or an IPv6 address or network.

➢ **To add an IPv4 or IPv6 SSL network resource:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

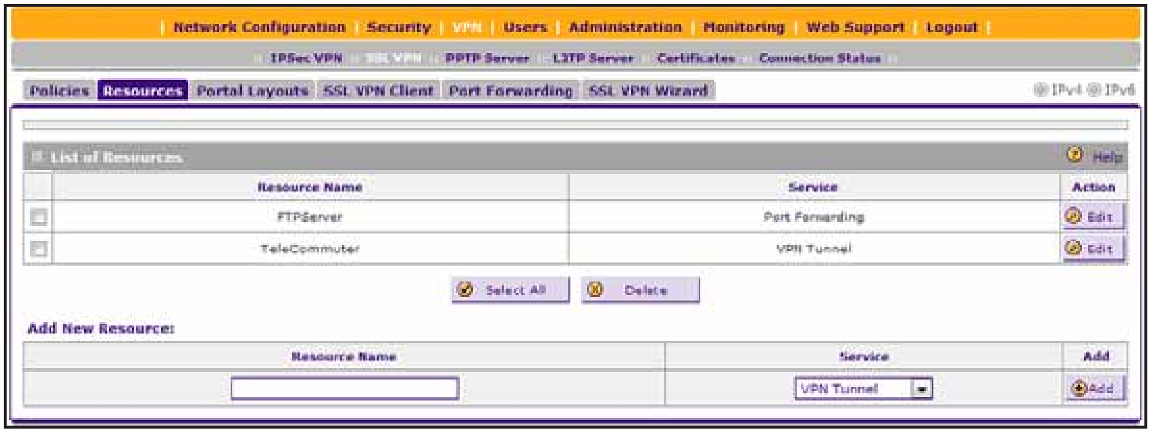
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > SSL VPN > Resources**.

   The Resources screen displays. The following figure shows some resources in the List of Resources table as an example.



List of Resources

	Resource Name	Service	Action
□	FTPServer	Port Forwarding	Edit
□	TeleCommuter	VPN Tunnel	Edit

Add New Resource:

Resource Name	Service	Add
	VPN Tunnel	Add

7. In the Add New Resource section, specify the following information:
   - **Resource Name**. A descriptive name of the resource for identification and management purposes.
   - **Service**. From the **Service** menu, select the type of service to which the resource applies:
     - **VPN Tunnel**. The resource applies only to a VPN tunnel.
     - **Port Forwarding**. The resource applies only to port forwarding.
     - **All**. The resource applies both to a VPN tunnel and to port forwarding.
8. Click the **Add** button.

   The new resource is added to the List of Resources table.

Define or Change an IPv4 or IPv6 Network Resource and Resource Address

After you add a network resource (see *Add an SSL Network Resource* on page 468), you must define an IP address, or FQDN, or IP network IP and services (port numbers) for the resource.

➢ **To define or change a network resources and resource address:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

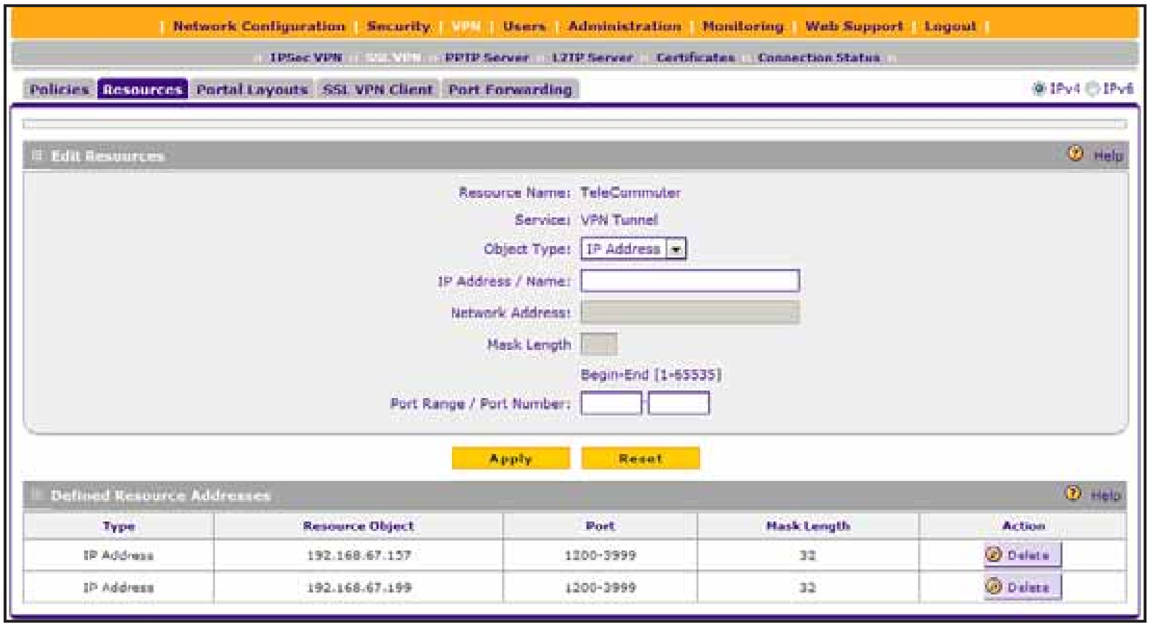
   The Router Status screen displays.

6. Select **VPN > SSL VPN > Resources**.

   The Resources screen displays.

7. In the List of Resources table, click the **Edit** button for the new resource.

   The Edit Resources screen displays the IPv4 settings. The following figure shows some examples.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
IPSec VPN | SSL VPN | PPTP Server | L2TP Server | Certificates | Connection Status
Policies | Resources | Portal Layouts | SSL VPN Client | Port Forwarding
● IPv4 ○ IPv6
Help
Apply
Reset
Help

Edit Resources

Resource Name: TeleCommuter

Service: VPN Tunnel

Object Type: IP Address

IP Address / Name:

Network Address:

Mask Length

Begin-End [1-65535]

Port Range / Port Number:

Defined Resource Addresses

Type	Resource Object	Port	Mask Length	Action
IP Address	192.168.67.157	1200-3999	32	Delete
IP Address	192.168.67.199	1200-3999	32	Delete

8. To configure the settings for an IPv6 resource instead of an IPv4 resource, in the upper right, select the **IPv6** radio button.

   The Edit Resources screen displays the IPv6 settings. Except for the **Prefix Length** field, which is the **Mask Length** field on the screen for IPv4, the IPv6 screen is identical to the IPv4 screen.

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

Setting	Description
Add Resource Addresses	
Resource Name	The unique identifier for the resource. This is the resource name that you created on the Resources screen.
Service	The SSL service that you assigned to the resource on the Resources screen.

Setting	Description
Object Type	From the menu, select an option: • **IP Address**. The object is an IPv4 or IPv6 address. In the **IP Address / Name** field, enter the IP address or FQDN for the object (that is, application or service) that you assign to this resource. • **IP Network**. The object is an IPv4 or IPv6 network. Configure the following settings: - In the **Network Address** field, enter the network IP address for the objects (that is, applications or services) that you assign to this resource. - For IPv4, in the **Mask Length** field, enter the associated network mask length from 0 to 31. For IPv6, in the **Prefix Length** field, enter the associated prefix length.
Port Range / Port Number	Enter the port or a range of ports (0–65535) to apply the policy to. The VPN firewall applies the policy to all TCP and UDP traffic that passes on those ports. To apply the policy to all traffic, leave the fields blank.

10. Click the **Apply** button.

    Your settings are saved. The new configuration is added to the Defined Resource Addresses table.

Remove One or More SSL Network Resources

The following procedure describes how you can remove an SSL network resource that you no longer need.

➢ **To remove an SSL network resource:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > SSL VPN > Resources**.

The Resources screen displays.

7. In the List of Resources table, select the check box to the left of each network resource that you want to remove or click the **Select All** button to select all network resources.
8. Click the **Delete** button.

   The selected network resources are removed from the List of Resources table.

Remove an IPv4 or IPv6 SSL Resource Address Configuration

The following procedure describes how to remove an SSL resource address configuration that you no longer need.

Note: If you remove all SSL resource address configurations for a corresponding SSL policy, the policy becomes ineffective.

➢ **To remove an SSL resource address configuration:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > SSL VPN > Resources**.

   The Resources screen displays.
7. In the List of Resources table, click the **Edit** button for the resource for which you want to remove a network resource address.

   The Edit Resources screen displays the IPv4 settings.
8. To remove an IPv6 resource address configuration instead of an IPv4 resource address configuration, in the upper right, select the **IPv6** radio button.

The Edit Resources screen displays the IPv6 settings.

9. In the Defined Resource Addresses table, click the **Delete** button to the right of the resource address configuration that you want to remove.

   The resource address configuration is removed from the Defined Resource Addresses table.

Configure User, Group, and Global Policies

The following sections provide information about configuring user, group, and global policies for SSL port forwarding:

- *SSL Policies Overview*
- *View SSL VPN Policies*
- *Add an IPv4 or IPv6 SSL VPN Policy for a Network Resource*
- *Add an IPv4 or IPv6 SSL VPN Policy for a Single IP Address*
- *Add an IPv4 or IPv6 SSL VPN Policy for an IP Network*
- *Add an IPv4 or IPv6 SSL VPN Policy for All Addresses*
- *Change an IPv4 or IPv6 SSL VPN Policy*
- *Remove One or More IPv4 or IPV6 SSL VPN Policies*

SSL Policies Overview

You can define and apply user, group, and global policies to predefined network resource objects, IP addresses, address ranges, or all IP addresses, and to different SSL VPN services (VPN tunnels and port forwarding configurations). A specific hierarchy is invoked over which policies take precedence. The VPN firewall SSL policy hierarchy is as follows:

- User policies take precedence over group policies.
- Group policies take precedence over global policies.
- If two or more user, group, or global policies are configured, the *most specific* policy takes precedence.

For example, a policy that is configured for a single IP address takes precedence over a policy that is configured for a range of addresses. And a policy that applies to a range of IP addresses takes precedence over a policy that applies to all IP addresses. If two or more IP address ranges are configured, the smallest address range takes precedence. Host names are treated the same as individual IP addresses.

Network resources are prioritized just like other address ranges. However, the prioritization is based on the individual address or address range, not the entire network resource.

For example, assume the following global policy configuration:

- **Policy 1**. A Deny rule blocks all services to the IP address range 10.0.0.0–10.0.0.255.
- **Policy 2**. A Deny rule blocks FTP access to 10.0.1.2–10.0.1.10.

- **Policy 3**. A Permit rule allows FTP access to the predefined network resource with the name FTP Servers. The FTP Servers network resource includes the following addresses: 10.0.0.5–10.0.0.20 and the FQDN ftp.*company*.com, which resolves to 10.0.1.3.

Assuming that no conflicting user or group policies are configured, if a user attempts to access FTP servers at the following addresses, the following actions occur:

- **10.0.0.1**. The user is blocked by Policy 1.
- **10.0.1.5**. The user is blocked by Policy 2.
- **10.0.0.10**. The user is granted access by Policy 3. The IP address range 10.0.0.5–10.0.0.20 is more specific than the IP address range that is defined in Policy 1.
- **ftp.*company*.com**. The user is granted access by Policy 3. A single host name is more specific than the IP address range that is configured in Policy 2.

Note: In this scenario, the user cannot access ftp.*company*.com using its IP address 10.0.1.3. The VPN firewall’s policy engine does not perform reverse DNS lookups.

View SSL VPN Policies

The following procedure describes how to view global, group, and user policies.

➢ **To view SSL VPN policies:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

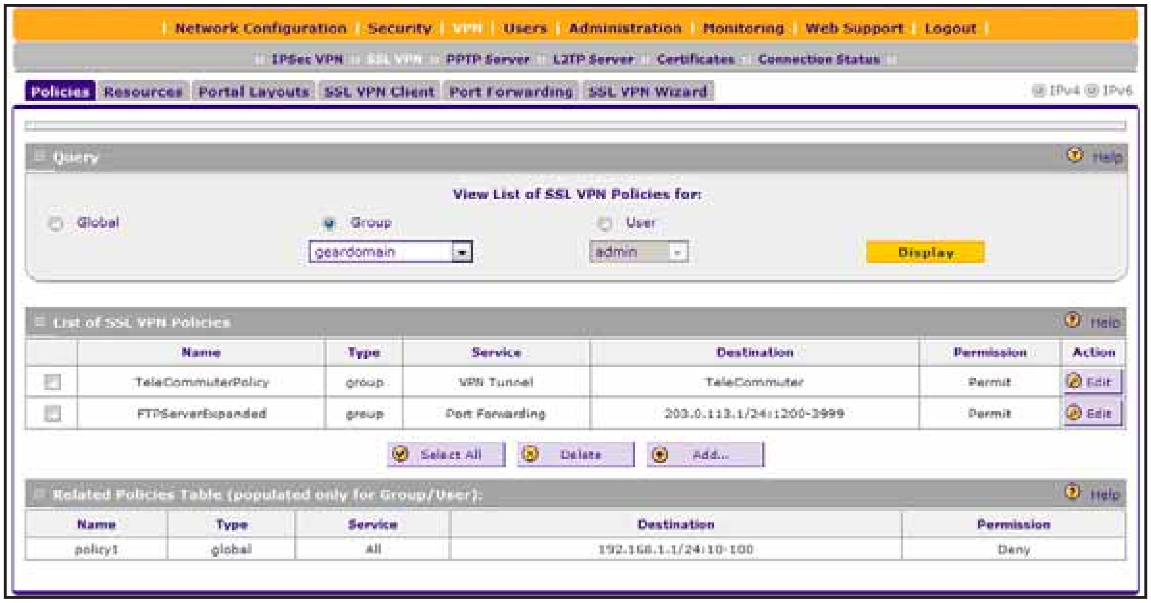
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > SSL VPN**.

The SSL VPN submenu tabs display with the Policies screen in view. The following figure shows examples.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
IPSec VPN | SSL VPN | PPTP Server | L2TP Server | Certificates | Connection Status
Policies | Resources | Portal Layouts | SSL VPN Client | Port Forwarding | SSL VPN Wizard
IPv4 IPv6
Query
Help
View List of SSL VPN Policies for:
Display
List of SSL VPN Policies
Select All
Delete
Add...
Related Policies Table (populated only for Group/User):

○ Global ● Group ○ User

geardomain admin

List of SSL VPN Policies

	Name	Type	Service	Destination	Permission	Action
□	TeleCommuterPolicy	group	VPN Tunnel	TeleCommuter	Permit	Edit
□	FTPServerExpanded	group	Port Forwarding	203.0.113.1/24:1200-3999	Permit	Edit

Related Policies Table (populated only for Group/User):

Name	Type	Service	Destination	Permission
policy1	global	All	192.168.1.1/24:10-100	Deny

7. In the Query section, select a radio button:
   - **Global**. View all global policies.
   - **Group**. To view group policies:
     a. Select the **Group** radio button.
     b. From the menu, select a user group.
   - **User**. To view user policies:
     a. Select the **User** radio button.
     b. From the menu, select a user.
8. Click the **Display** button.

   The List of SSL VPN Policies table displays the list for your selected query option.

   The Related Policies Table displays global policies that might affect group and user policies.

Add an IPv4 or IPv6 SSL VPN Policy for a Network Resource

The following procedure describes how to add an SSL policy for an existing network resource.

Note: Before you can add an SSL policy for a network resource, you must create the network resource (see *Manage Network Resource Objects to Simplify Policies* on page 467).

➢ To add an SSL policy for an existing network resource:

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

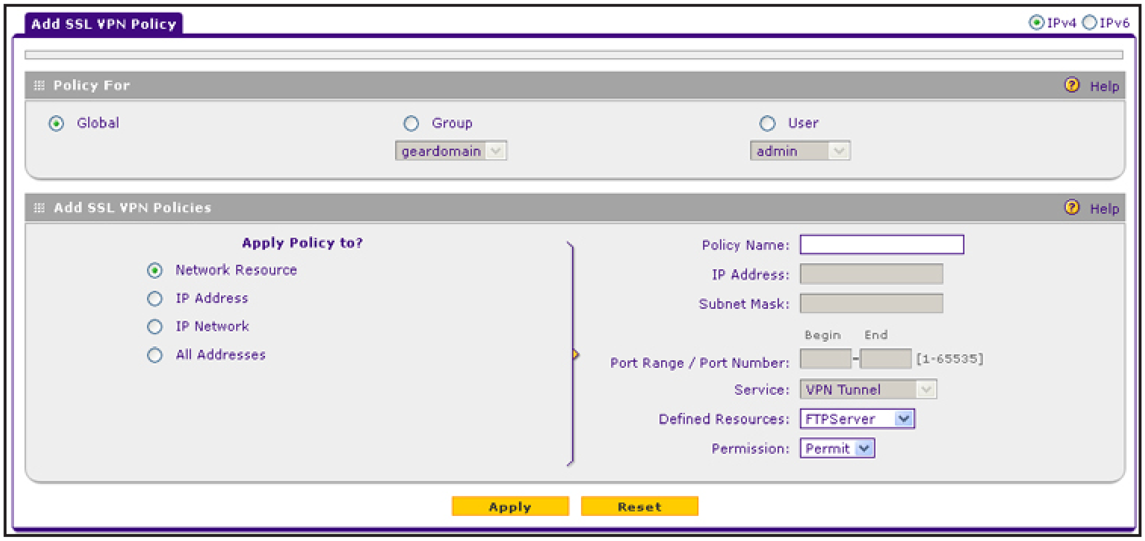
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > SSL VPN**.

   The SSL VPN submenu tabs display with the Policies screen in view.
7. Under the List of SSL VPN Policies table, click the **Add** button.

   The Add SSL VPN Policy screen displays the IPv4 settings.



Add SSL VPN Policy ● IPv4 ○ IPv6

Policy For

● Global ○ Group: geardomain ○ User: admin

Add SSL VPN Policies

Apply Policy to?
● Network Resource
○ IP Address
○ IP Network
○ All Addresses

Policy Name:
IP Address:
Subnet Mask:
Port Range / Port Number: Begin – End [1-65535]
Service: VPN Tunnel
Defined Resources: FTPServer
Permission: Permit

8. To add an IPv6 SSL policy instead of an IPv4 SSL policy, in the upper right select the **IPv6** radio button.

The Add SSL VPN Policy screen displays the IPv6 settings. Except for the **IPv6 Prefix Length** field, which is the **Subnet Mask** field on the screen for IPv4, the IPv6 screen is identical to the IPv4 screen.

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

Setting	Description
Policy For	
Select type of SSL VPN policy: • **Global**. The new policy is global and includes all groups and users. • **Group**. The new policy must be limited to a single group. From the menu, select a group name. For information about how to create groups, see *Manage Authentication Groups* on page 494. • **User**. The new policy must be limited to a single user. From the menu, select a user name. For information about how to create user accounts, see *Manage User Accounts* on page 498.	
Add SSL VPN Policies	
Apply Policy to?	Select the **Network Resource** radio button. The policy applies to a network resource. The screen adjusts to make the associated fields and menus available fields; and menus that do not apply are masked out.
Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.
Defined Resources	From the menu, select a network resource that you must have defined on the Resources screen (see *Manage Network Resource Objects to Simplify Policies* on page 467).
Permission	From the menu, select **Permit** or **Deny** to specify whether the policy permits or denies access.

10. Click the **Apply** button.

Your settings are saved. The policy is added to the List of SSL VPN Policies table on the Policies screen. The new policy goes into effect immediately.

Note: If you have configured SSL VPN user policies, make sure that secure HTTP remote management is enabled (see *Set Up Remote Management Access* on page 534). If secure HTTP remote management is not enabled, all SSL VPN user connections are disabled.

Add an IPv4 or IPv6 SSL VPN Policy for a Single IP Address

The following procedure describes how to add an SSL policy for a single IP address.

➢ **To add an SSL policy for a single IP address:**

1. On your computer, launch an Internet browser.

2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

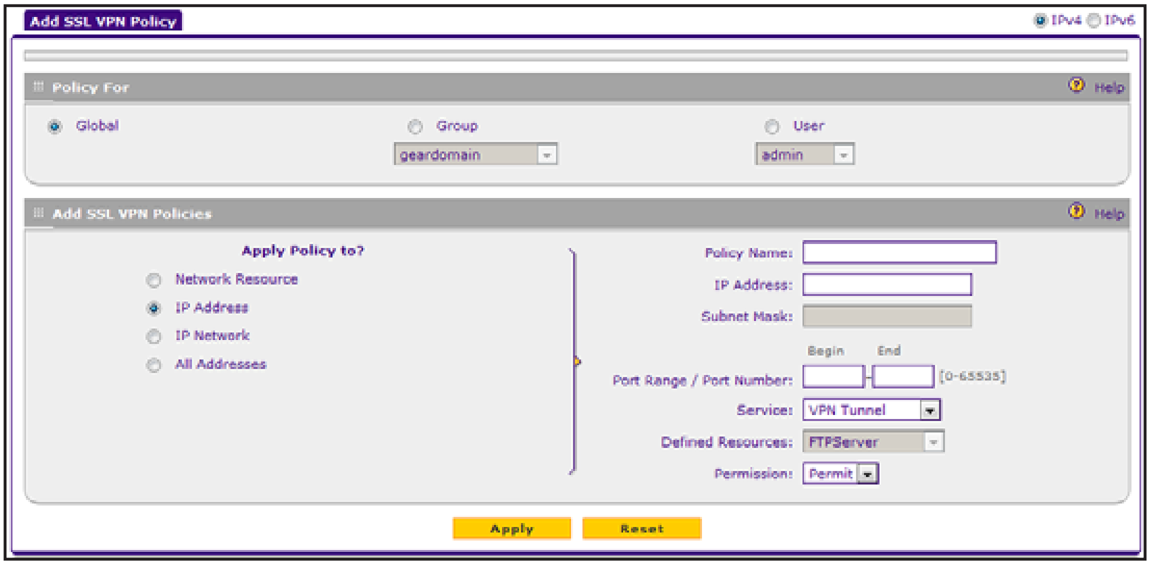
   The Router Status screen displays.

6. Select **VPN > SSL VPN**.

   The SSL VPN submenu tabs display with the Policies screen in view.

7. Under the List of SSL VPN Policies table, click the **Add** button.

   The Add SSL VPN Policy screen displays the IPv4 settings.



Add SSL VPN Policy ● IPv4 ○ IPv6

Policy For

● Global ○ Group geardomain ○ User admin

Add SSL VPN Policies

Apply Policy to?

○ Network Resource
● IP Address
○ IP Network
○ All Addresses

Policy Name:
IP Address:
Subnet Mask:
Port Range / Port Number: Begin End [0-65535]
Service: VPN Tunnel
Defined Resources: FTPServer
Permission: Permit

8. To add an IPv6 SSL policy instead of an IPv4 SSL policy, in the upper right select the **IPv6** radio button.

   The Add SSL VPN Policy screen displays the IPv6 settings. Except for the **IPv6 Prefix Length** field, which is the **Subnet Mask** field on the screen for IPv4, the IPv6 screen is identical to the IPv4 screen.

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

Setting	Description
Policy For	
Select the type of SSL VPN policy: • **Global**. The new policy is global and includes all groups and users. • **Group**. The new policy must be limited to a single group. From the menu, select a group name. For information about how to create groups, see *Manage Authentication Groups* on page 494. • **User**. The new policy must be limited to a single user. From the menu, select a user name. For information about how to create user accounts, see *Manage User Accounts* on page 498.	
Add SSL VPN Policies	
Apply Policy to?	Select the **IP Address** radio button. The policy applies to a single IP address. The screen adjusts to make the associated fields and menus available; fields and menus that do not apply are masked out.
Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.
IP Address	The IPv4 or IPv6 address to which the SSL VPN policy applies.
Port Range / Port Number	A port (complete the **Begin** field) or a range of ports (complete the **Begin** and **End** fields) to which the SSL VPN policy applies. Ports can be 0 through 65535. The policy applies to all TCP and UDP traffic that passes on those ports. Leave the fields blank to apply the policy to all traffic.
Service	From the menu, select the service to which the SSL VPN policy applies: • **VPN Tunnel**. The policy applies only to a VPN tunnel. • **Port Forwarding**. The policy applies only to port forwarding. • **All**. The policy applies both to a VPN tunnel and to port forwarding.
Permission	From the menu, select **Permit** or **Deny** to specify whether the policy permits or denies access.

10. Click the **Apply** button.

    Your settings are saved. The policy is added to the List of SSL VPN Policies table on the Policies screen. The new policy goes into effect immediately.

Add an IPv4 or IPv6 SSL VPN Policy for an IP Network

The following procedure describes how to add an SSL policy for an IP network.

➢ To add an SSL policy for an IP network:

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

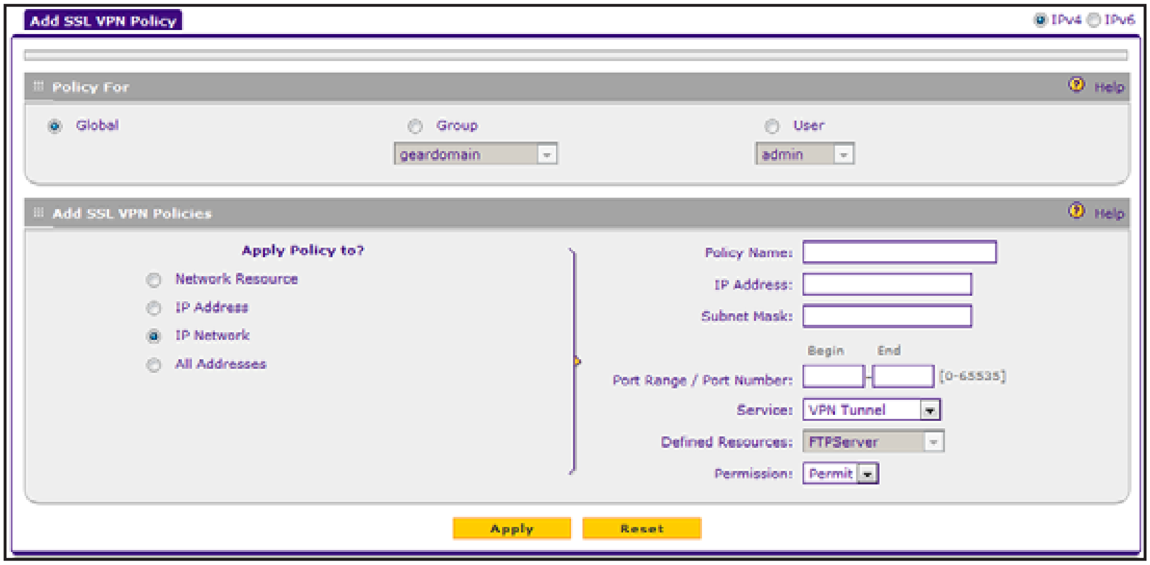
   The Router Status screen displays.

6. Select **VPN > SSL VPN**.

   The SSL VPN submenu tabs display with the Policies screen in view.

7. Under the List of SSL VPN Policies table, click the **Add** button.

   The Add SSL VPN Policy screen displays the IPv4 settings.



Add SSL VPN Policy

● IPv4 ○ IPv6

Policy For

● Global ○ Group ○ User

geardomain

admin

Add SSL VPN Policies

Apply Policy to?

○ Network Resource
○ IP Address
● IP Network
○ All Addresses

Policy Name:

IP Address:

Subnet Mask:

Port Range / Port Number: Begin End [0-65535]

Service: VPN Tunnel

Defined Resources: FTPServer

Permission: Permit

8. To add an IPv6 SSL policy instead of an IPv4 SSL policy, in the upper rights select the **IPv6** radio button.

   The Add SSL VPN Policy screen displays the IPv6 settings. Except for the **IPv6 Prefix Length** field, which is the **Subnet Mask** field on the screen for IPv4, the IPv6 screen is identical to the IPv4 screen.

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

Setting	Description
Policy For	
Select the type of SSL VPN policy: • **Global**. The new policy is global and includes all groups and users. • **Group**. The new policy must be limited to a single group. From the menu, select a group name. For information about how to create groups, see *Manage Authentication Groups* on page 494. • **User**. The new policy must be limited to a single user. From the menu, select a user name. For information about how to create user accounts, see *Manage User Accounts* on page 498.	
Add SSL VPN Policies	
Apply Policy to?	Select the **IP Network** radio button.The policy applies to a network address. The screen adjusts to make the associated fields and menus available; fields and menus that do not apply are masked out.
Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.
IP Address	The network IPv4 or IPv6 network address to which the SSL VPN policy applies.
Subnet Mask (IPv4 screen) or IPv6 Prefix Length (IPv6 screen)	The IPv4 subnet mask that apples to the network to which the SSL VPN policy applies.
	The IPv6 prefix length that apples to the network to which the SSL VPN policy applies.
Port Range / Port Number	A port (complete the **Begin** field) or a range of ports (complete the **Begin** and **End** fields) to which the SSL VPN policy applies. Ports can be 0 through 65535. The policy applies to all TCP and UDP traffic that passes on those ports. Leave the fields blank to apply the policy to all traffic.
Service	From the menu, select the service to which the SSL VPN policy applies: • **VPN Tunnel**. The policy applies only to a VPN tunnel. • **Port Forwarding**. The policy applies only to port forwarding. • **All**. The policy applies both to a VPN tunnel and to port forwarding.
Permission	From the menu, select **Permit** or **Deny** to specify whether the policy permits or denies access.

10. Click the **Apply** button.

    Your settings are saved. The policy is added to the List of SSL VPN Policies table on the Policies screen. The new policy goes into effect immediately.

Add an IPv4 or IPv6 SSL VPN Policy for All Addresses

The following procedure describes how to add an SSL policy for all IP addresses.

➢ **To add an SSL policy for all IP addresses:**

1. On your computer, launch an Internet browser.

2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

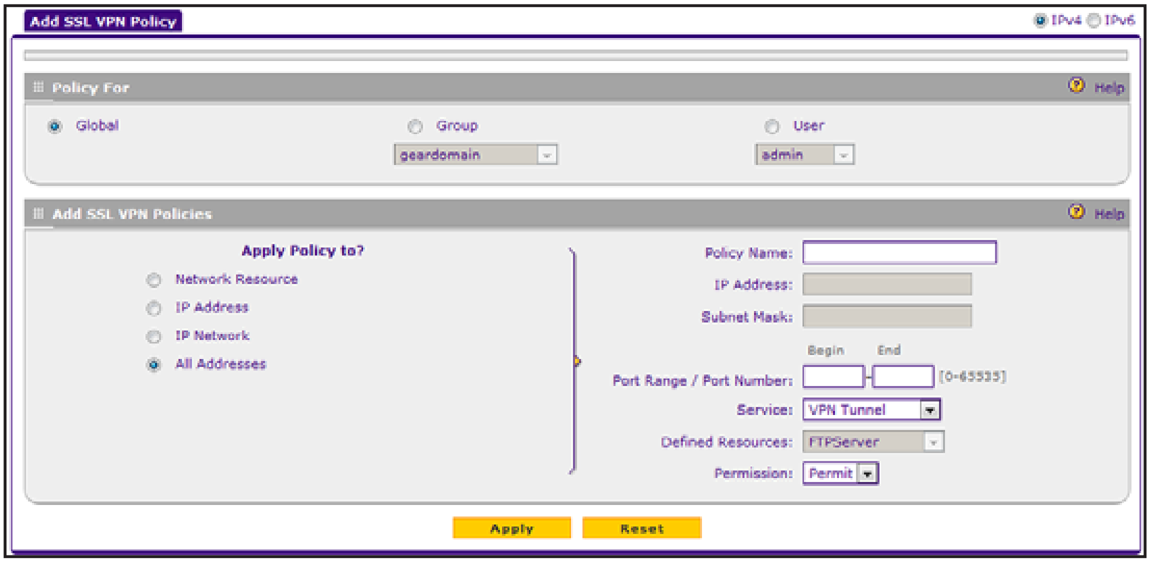
   The Router Status screen displays.

6. Select **VPN > SSL VPN**.

   The SSL VPN submenu tabs display with the Policies screen in view.

7. Under the List of SSL VPN Policies table, click the **Add** button.

   The Add SSL VPN Policy screen displays the IPv4 settings.



Add SSL VPN Policy

● IPv4 ○ IPv6

Policy For

● Global ○ Group ○ User

geardomain admin

Add SSL VPN Policies

Apply Policy to?

○ Network Resource
○ IP Address
○ IP Network
● All Addresses

Policy Name:

IP Address:

Subnet Mask:

Port Range / Port Number: Begin End [0-65535]

Service: VPN Tunnel

Defined Resources: FTPServer

Permission: Permit

8. To add an IPv6 SSL policy instead of an IPv4 SSL policy, in the upper right, select the **IPv6** radio button.

   The Add SSL VPN Policy screen displays the IPv6 settings. Except for the **IPv6 Prefix Length** field, which is the **Subnet Mask** field on the screen for IPv4, the IPv6 screen is identical to the IPv4 screen.

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

Setting	Description
Policy For	
Select the type of SSL VPN policy: • **Global**. The new policy is global and includes all groups and users. • **Group**. The new policy must be limited to a single group. From the menu, select a group name. For information about how to create groups, see *Manage Authentication Groups* on page 494. • **User**. The new policy must be limited to a single user. From the menu, select a user name. For information about how to create user accounts, see *Manage User Accounts* on page 498.	
Add SSL VPN Policies	
Apply Policy to?	Select the **All Addresses** radio button. The policy applies to all addresses. The screen adjusts to make the associated fields and menus available; fields and menus that do not apply are masked out.
Policy Name	A descriptive name of the SSL VPN policy for identification and management purposes.
Port Range / Port Number	A port (complete the **Begin** field) or a range of ports (complete the **Begin** and **End** fields) to which the SSL VPN policy applies. Ports can be 0 through 65535. The policy applies to all TCP and UDP traffic that passes on those ports. Leave the fields blank to apply the policy to all traffic.
Service	From the menu, select the service to which the SSL VPN policy applies: • **VPN Tunnel**. The policy applies only to a VPN tunnel. • **Port Forwarding**. The policy applies only to port forwarding. • **All**. The policy applies both to a VPN tunnel and to port forwarding.
Permission	From the menu, select **Permit** or **Deny** to specify whether the policy permits or denies access.

10. Click the **Apply** button.

    Your settings are saved. The policy is added to the List of SSL VPN Policies table on the Policies screen. The new policy goes into effect immediately.

Change an IPv4 or IPv6 SSL VPN Policy

The following procedure describes how to change an existing SSL policy.

➢ **To change an SSL VPN policy:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **VPN > SSL VPN**.

   The SSL VPN submenu tabs display with the Policies screen in view.

7. In the Query section, select a radio button:
   - **Global**. View all global policies.
   - **Group**. To view group policies:
     a. Select the **Group** radio button.
     b. From the menu, select a user group.
   - **User**. To view user policies:
     a. Select the **User** radio button.
     b. From the menu, select a user.

8. Click the **Display** action button.

   The List of SSL VPN Policies table displays the list for your selected Query option.

9. In the List of SSL VPN Policies table, click the **Edit** button for the SSL policy that you want to change.

   The Edit SSL VPN Policy screen displays the IPv4 settings.

10. To change an IPv6 SSL policy instead of an IPv4 SSL policy, in the upper right, select the **IPv6** radio button.

    The Edit SSL VPN Policy screen displays the IPv6 settings.

11. Change the settings.

    For more information about the settings, see one of the following sections that relates to the type of SSL policy that you are changing:

    - *Add an IPv4 or IPv6 SSL VPN Policy for a Network Resource* on page 475
    - *Add an IPv4 or IPv6 SSL VPN Policy for a Single IP Address* on page 477
    - *Add an IPv4 or IPv6 SSL VPN Policy for an IP Network* on page 479
    - *Add an IPv4 or IPv6 SSL VPN Policy for All Addresses* on page 481

12. Click the **Apply** button.

    Your settings are saved. The modified policy displays in the List of SSL VPN Policies table on the Policies screen.

Remove One or More IPv4 or IPV6 SSL VPN Policies

The following procedure describes how to remove an SSL policy that you no longer need.

➢ **To remove one or more VPN policies:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > SSL VPN**.

   The SSL VPN submenu tabs display with the Policies screen in view.
7. In the Query section, select a radio button:
   - **Global**. View all global policies.
   - **Group**. To view group policies:
     a. Select the **Group** radio button.
     b. From the menu, select a user group.
   - **User**. To view user policies:
     a. Select the **User** radio button.
     b. From the menu, select a user.
8. Click the **Display** action button.

   The List of SSL VPN Policies table displays the list for your selected Query option.
9. In the List of SSL VPN Policies table, select the check box to the left of each SSL policy that you want to remove or click the **Select All** button to select all policies.
10. Click the **Delete** button.

    The selected policies are removed from the List of SSL VPN Policies table.

10. Manage Users, Authentication, and VPN Certificates

10

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

- *VPN Firewall’s Authentication*
- *Configure Authentication Domains, Groups, and User Accounts*
- *Manage Digital Certificates for VPN Connections*

VPN Firewall's Authentication

Users are assigned to a group, and a group is assigned to a domain. Therefore, first create any domains, then groups, then user accounts.

Note: Do not confuse the authentication groups with the LAN groups that are described in *Manage IPv4 LAN Groups and Hosts* on page 132.

You must create name and password accounts for all users who must be able to connect to the VPN firewall. This includes administrators, guests, and SSL VPN clients. Accounts for IPSec VPN clients are required only if you have enabled extended authentication (XAUTH) in your IPSec VPN configuration.

Users connecting to the VPN firewall 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 and, for SSL connections, the portal layout that is presented.

Note: IPSec VPN, L2TP, and PPTP users do not belong to a domain and are not assigned to a group.

Except in the case of IPSec VPN users, when you create a user account, you must specify a group. When you create a group, you must specify a domain.

The following table summarizes the external authentication protocols and methods that the VPN firewall supports.

Table 9. 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, which 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.

Table 9. External authentication protocols and methods (continued)

Authentication Protocol or Method	Description
WiKID	WiKID Systems is a PAP or CHAP key-based two-factor authentication method that functions with public key cryptography. The client sends an encrypted PIN to the WiKID server and receives a one-time passcode with a short expiration period. The client logs in with the passcode. See *Appendix C, Two-Factor Authentication*, for more information about WiKID authentication.
NT Domain	A network-validated domain-based authentication method that functions with a Microsoft Windows NT Domain authentication server. This authentication method is superseded by Microsoft Active Directory authentication but is supported to authenticate legacy Windows clients.
Active Directory	A network-validated domain-based authentication method that functions with a Microsoft Active Directory authentication server. Microsoft Active Directory authentication servers support a group and user structure. Because the Active Directory supports a multilevel hierarchy (for example, groups or organizational units), this information can be queried to provide specific group policies or bookmarks based on Active Directory attributes. **Note:** A Microsoft Active Directory database uses an LDAP organization schema.
LDAP	A network-validated domain-based authentication method that functions with a Lightweight Directory Access Protocol (LDAP) authentication server. LDAP is a standard for querying and updating a directory. Because LDAP supports a multilevel hierarchy (for example, groups or organizational units), this information can be queried to provide specific group policies or bookmarks based on LDAP attributes.

Configure Authentication Domains, Groups, and User Accounts

The following sections provide information about configuring authentication domains, groups, and user accounts:

- *Manage Authentication Domains*
- *Manage Authentication Groups*
- *Manage User Accounts*
- *Manage User Login Policies*
- *Change Passwords and Automatic Logout Period*

Manage Authentication Domains

The following sections provide information about managing authentication domains:

- *Authentication Domains Overview*
- *Add an Authentication Domain*
- *Change an Authentication Domain*

- *Remove One or More Authentication Domains*

Authentication Domains Overview

An authentication domain specifies the authentication method for users that are assigned to the domain. For SSL connections, the domain also determines the portal layout that is presented, which in turn determines the network resources to which the associated users have access. The default domain of the VPN firewall is named geardomain. You cannot change or remove the default domain.

Add an Authentication Domain

The following procedure describes how to add a new authentication domain.

➢ **To add an authentication domain:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

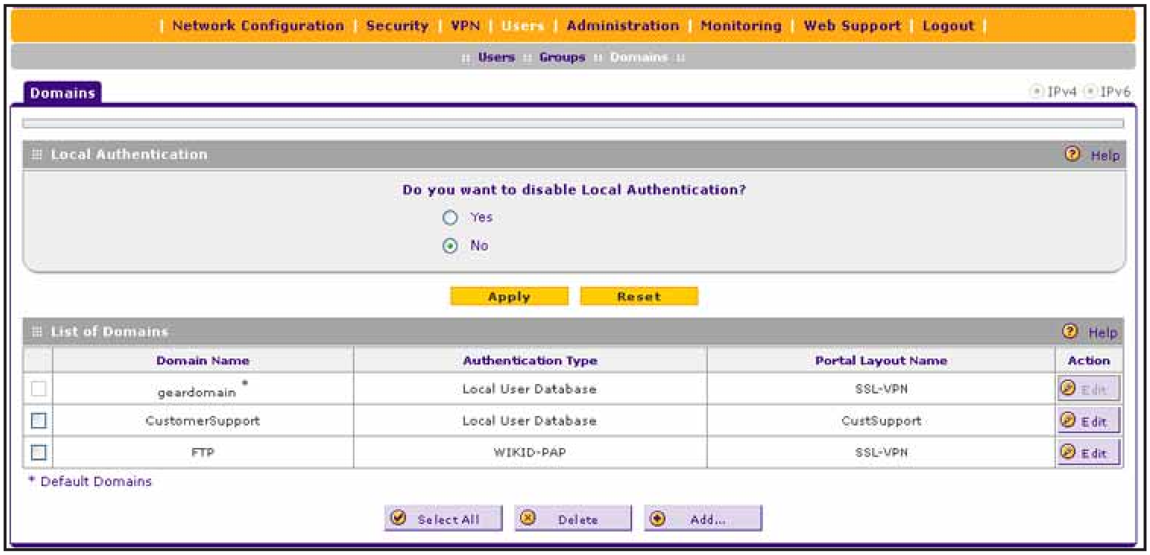
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Users > Domains**.

   The Domains screen displays. The following figure shows the VPN firewall’s default domain—geardomain—and, as an example, other domains in the List of Domains table.


| 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	Portal Layout Name	Action
□	geardomain *	Local User Database	SSL-VPN	Edit
□	CustomerSupport	Local User Database	CustSupport	Edit
□	FTP	WIKID-PAP	SSL-VPN	Edit

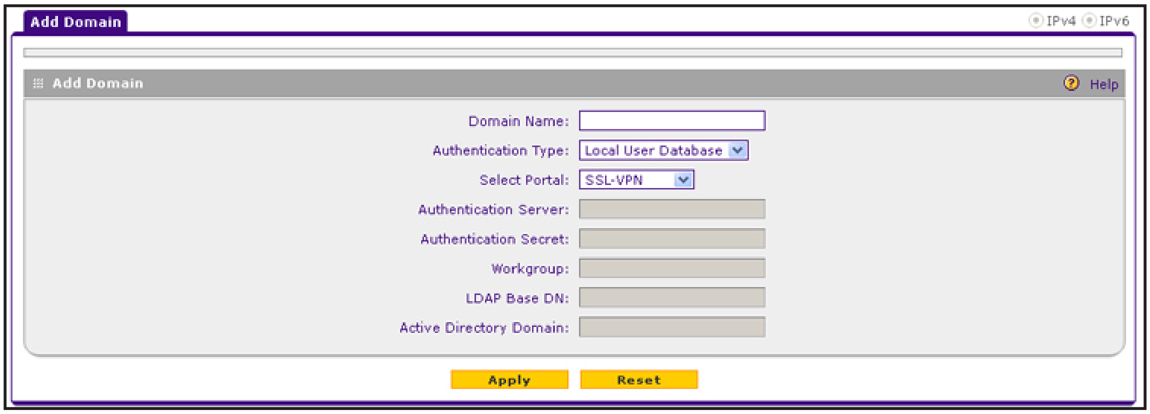
* Default Domains

The List of Domains table lists the following information:

- **Check box**. Allows you to select the domain in the table.
- **Domain Name**. The name of the domain. The name of the default domain (geardomain) to which the default SSL-VPN portal is assigned is appended by an asterisk.
- **Authentication Type**. The authentication method that is assigned to the domain.
- **Portal Layout Name**. The SSL portal layout that is assigned to the domain.
- **Action**. The **Edit** button, which provides access to the Edit Domain screen.

7. Under the List of Domains table, click the **Add** button.

   The Add Domain screen displays.



Add Domain

Domain Name:	
Authentication Type:	Local User Database
Select Portal:	SSL-VPN
Authentication Server:	
Authentication Secret:	
Workgroup:	
LDAP Base DN:	
Active Directory Domain:	

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

Setting	Description
Domain Name	A descriptive (alphanumeric) name of the domain for identification and management purposes. **Note:** If you leave the **Domain Name** field blank, the SSL VPN Wizard uses the default domain name geardomain. To enable the SSL VPN Wizard to create a domain, you must enter a name other than geardomain in the **Domain Name** field.
Authentication Type **Note:** If you select any type of RADIUS authentication, make sure that you configure one or more RADIUS servers (see *Configure the RADIUS Servers for the VPN Firewall's RADIUS Client* on page 392).	From the menu, 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 **Authentication Server** and **Authentication Secret** fields. • **Radius-CHAP**. RADIUS Challenge Handshake Authentication Protocol (CHAP). Complete the **Authentication Server** and **Authentication Secret** fields. • **Radius-MSCHAP**. RADIUS Microsoft CHAP. Complete the **Authentication Server** and **Authentication Secret** fields. • **Radius-MSCHAPv2**. RADIUS Microsoft CHAP version 2. Complete the **Authentication Server** and **Authentication Secret** fields. • **WIKID-PAP**. WiKID Systems PAP. Complete the **Authentication Server** and **Authentication Secret** fields. • **WIKID-CHAP**. WiKID Systems CHAP. Complete the **Authentication Server** and **Authentication Secret** fields. • **MIAS-PAP**. Microsoft Internet Authentication Service (MIAS) PAP. Complete the **Authentication Server** and **Authentication Secret** fields. • **MIAS-CHAP**. Microsoft Internet Authentication Service (MIAS) CHAP. Complete the **Authentication Server** and **Authentication Secret** fields. • **NT Domain**. Microsoft Windows NT Domain. Complete the **Authentication Server** and **Workgroup** fields. • **Active Directory**. Microsoft Active Directory. Complete the **Authentication Server** and **Active Directory Domain** fields. • **LDAP**. Lightweight Directory Access Protocol (LDAP). Complete the **Authentication Server** and **LDAP Base DN** fields.
Portal	The portal that is assigned to this domain and that is presented to the user to enter credentials. The default portal is SSL-VPN.
Authentication Server	The server IP address or server name of the authentication server for any type of authentication other than authentication through the local user database.
Authentication Secret	The authentication secret or password that is required to access the authentication server for RADIUS, WiKID, or MIAS authentication.
Workgroup	The workgroup that is required for Microsoft NT Domain authentication.

Setting	Description
LDAP Base DN	The LDAP distinguished name (DN) that is required to access the LDAP authentication server. This must be a user in the LDAP directory who has read access to all the users that you want to import into the VPN firewall. The **LDAP Base DN** field accepts two formats: • **A display name in the DN format**. For example: cn=Jamie Hanson,cn=users,dc=test,dc=com. • **A Windows login account name in email format**. For example: jhanson@testAD.com. This last type of bind DN can be used only for a Windows LDAP server.
Active Directory Domain	The Active Directory domain name that is required for Microsoft Active Directory authentication.

9. Click the **Apply** button.

   Your settings are saved. The domain is added to the List of Domains table.

10. 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.

Note: The VPN firewall supports a combination of local and external authentication.

WARNING:

If you disable local authentication, make sure that there is at least one external administrative user; otherwise, access to the VPN firewall is blocked.

11. If you do change local authentication, click the **Apply** button.

    Your settings are saved.

Change an Authentication Domain

The following procedure describes how to change an authentication domain. However, you cannot change the domain name and type of authentication.

Note: You cannot change the default domain geardomain.

- **To change an authentication domain:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

The VPN firewall factory default IP address is 192.168.1.1.

The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Users > Domains**.

   The Domains screen displays.

7. In the List of Domains table, click the **Edit** button for the domain that you want to change.

   The Edit Domains screen displays.

8. Change the settings.

   For more information about the settings, see *Add an Authentication Domain* on page 489.

9. Click the **Apply** button.

   Your settings are saved. The modified domain displays in the List of Domains table on the Domains screen.

Remove One or More Authentication Domains

The following procedure describes how to remove one or more domains that you no longer need. However, if a domain has users assigned to it, you first must assign the users to another domain; otherwise, you cannot remove the domain (see *Change a User Account* on page 502).

Note: You cannot remove the default domain geardomain.

➢ **To remove one or more authentication domains:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Users > Domains**.

   The Domains screen displays.

7. In the List of Domains table, select the check box to the left of each domain that you want to remove or click the **Select All** button to select all domains.
8. Click the **Delete** button.

   The selected domains are removed from the List of Domains table.

Manage Authentication Groups

The following sections provide information about managing authentication groups:

- *Authentication Groups Overview*
- *Add an Authentication Group*
- *Change an Authentication Group*
- *Remove One or More Authentication Groups*

Authentication Groups Overview

The use of groups simplifies the configuration of VPN policies when different sets of users have different restrictions and access controls. It also simplifies the configuration of web access exception rules. Like the default domain of the VPN firewall, the default group is also named geardomain. The default group geardomain is assigned to the default domain geardomain. You cannot remove the default domain geardomain, nor its associated default group geardomain.

IPSec VPN, L2TP, and PPTP users do not belong to a domain and are not assigned to a group.

IMPORTANT:

When you add a domain, the VPN firewall creates a group with the same name as the new domain automatically. You cannot remove such a group. However, when you remove the domain with which the group is associated, the group is removed automatically.

Note: Authentication groups are different from LAN groups that you use to simplify firewall policies. For information about LAN groups, see *Manage IPv4 LAN Groups and Hosts* on page 132.

Add an Authentication Group

The following procedure describes how to manually add an authentication group.

➢ **To add a group:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

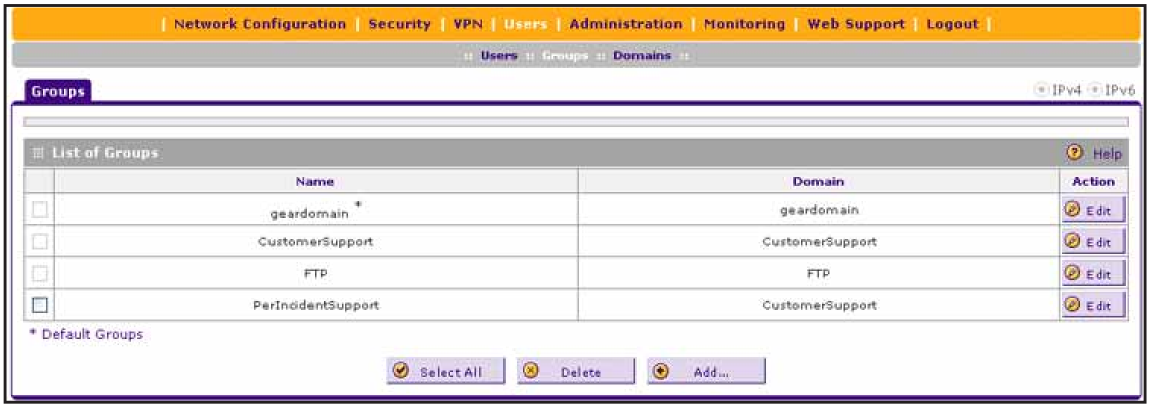
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Users > Groups**.

   The Groups screen displays. The following figure shows the VPN firewall's default group—geardomain—and, as an example, several other groups in the List of Groups table.



	Name	Domain	Action
□	geardomain *	geardomain	Edit
□	CustomerSupport	CustomerSupport	Edit
□	FTP	FTP	Edit
□	PerIncidentSupport	CustomerSupport	Edit

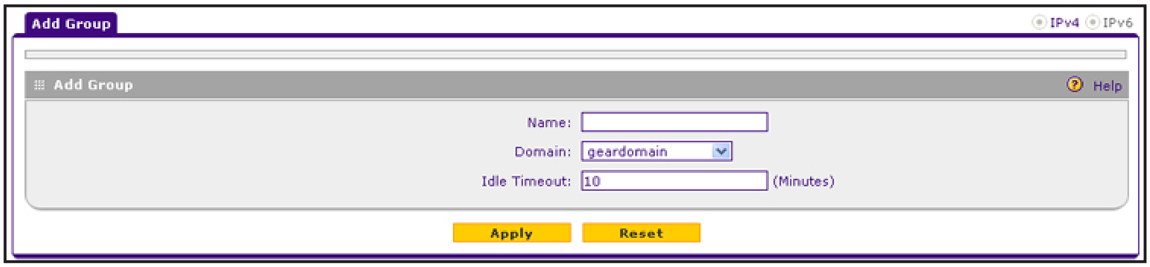
* Default Groups

The List of Groups table lists the following information:

- **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** button, which provides access to the Edit Group screen.

7. Under the List of Groups table, click the **Add** button.

   The Add Group screen displays.



Name:

Domain: geardomain

Idle Timeout: 10 (Minutes)

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

Setting	Description
Name	A descriptive (alphanumeric) name of the group for identification and management purposes.
Domain	The menu shows the domains that are listed on the Domain screen. From the menu, select the domain with which you want to associate the group. For information about how to configure domains, see *Manage Authentication Domains* on page 488.
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.

9. Click the **Apply** button.

   Your settings are saved. The new group is added to the List of Groups table.

Change an Authentication Group

For a group that was automatically created when you added an authentication domain, you can modify only the idle time-out settings but not the group name or associated domain.

For groups that you created manually, you can modify the domain and the idle time-out settings but not the group name.

➢ **To change an authentication group:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Users > Groups**.

   The Groups screen displays.
7. In the List of Groups table, click the **Edit** button for the group that you want to change.

   The Edit Groups screen displays.
8. Change the settings.

   For more information about the settings, see *Add an Authentication Group* on page 495.
9. Click the **Apply** button.

   Your settings are saved. The modified group displays in the List of Groups table on the Groups screen.

Remove One or More Authentication Groups

You can remove only an authentication group that you created manually. You cannot remove a group that was automatically created when you added an authentication domain. However, when you remove the domain with which the group is associated, the group is removed automatically.

For a group that you created manually, if the group has users assigned to it, you first must assign the users to another group; otherwise, you cannot remove the group (see *Change a User Account* on page 502).

Note: You cannot remove the default group geardomain.

➢ **To remove one or more authentication groups:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Users > Groups**.

   The Groups screen displays.
7. In the List of Groups table, select the check box to the left of each group that you want to remove or click the **Select All** button to select all groups.
8. Click the **Delete** button.

   The selected groups are removed from the List of Groups table.

Manage User Accounts

The following sections provide information about managing user accounts:

- *User Accounts Overview*
- *Add a User Account*
- *Change a User Account*
- *Remove One or More User Accounts*

User Accounts Overview

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, first create any domains, then groups, and then user accounts.

Note: IPSec VPN, L2TP, and PPTP users do not belong to a domain and are not assigned to a group.

The VPN firewall provides two default (preconfigured) user accounts:

- A user with the name **admin** and the password **password**. This is a user who has read/write access, is associated with the domain geardomain, and is denied login from the WAN interface by default. The user name is appended by an asterisk. You cannot remove this user account.
- A user with the name **guest** and the password **password**. This is a user who has read-only access, is associated with the domain geardomain, and is denied login from the WAN interface by default. The user name is appended by an asterisk. You cannot remove this user account.

Note: For information about allowing user access from the WAN interface, see *Configure Login Policies* on page 504.

You can create different types of user accounts by applying one of the predefined user types:

- **SSL VPN user**. A user who can log in only to the SSL VPN portal.
- **Administrator**. A user who has full access and the capacity to change the VPN firewall configuration (that is, read/write access).
- **Guest user**. A user who can only view the VPN firewall configuration (that is, read-only access).
- **IPSec VPN user**. A user who can make an IPSec VPN connection only through a NETGEAR ProSAFE VPN Client, and only when the XAUTH feature is enabled (see *Configure Extended Authentication (XAUTH)* on page 388).
- **L2TP user**. A user who can connect over an L2TP connection to an L2TP client that is located behind the VPN firewall.
- **PPTP user**. A user who can connect over a PPTP connection to a PPTP client that is located behind the VPN firewall.

Add a User Account

The following procedure describes how to manually add a user account.

➢ **To add a user account:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

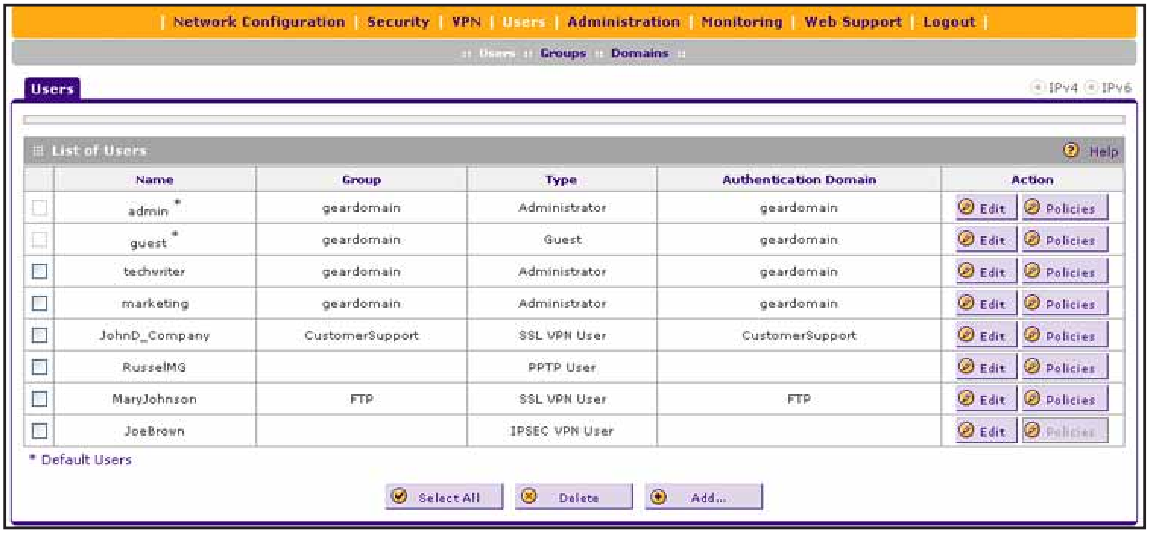
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Users > Users**.

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


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Users :: Groups :: Domains ::
Users
○ IPv4 ○ IPv6
List of Users
Help

	Name	Group	Type	Authentication Domain	Action
□	admin *	geardomain	Administrator	geardomain	Edit Policies
□	guest *	geardomain	Guest	geardomain	Edit Policies
□	techwriter	geardomain	Administrator	geardomain	Edit Policies
□	marketing	geardomain	Administrator	geardomain	Edit Policies
□	JohnD_Company	CustomerSupport	SSL VPN User	CustomerSupport	Edit Policies
□	RusselMG		PPTP User		Edit Policies
□	MaryJohnson	FTP	SSL VPN User	FTP	Edit Policies
□	JoeBrown		IPSEC VPN User		Edit Policies

* Default Users

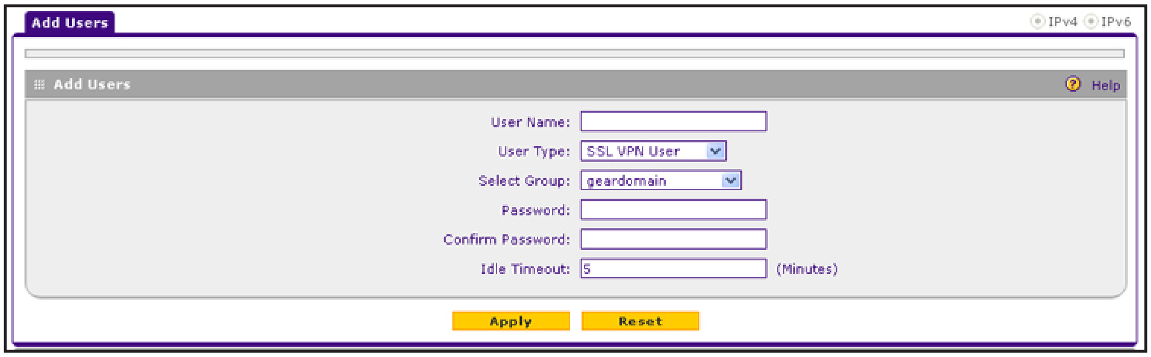
The List of Users table lists the following information:

- **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 you cannot remove the user.
- **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** button, which provides access to the Edit User screen, and the Policies button, which provides access to the policy screens.

7. Under the List of Users table, click the **Add** button.

   The Add Users screen displays.



User Name:
User Type: SSL VPN User
Select Group: geardomain
Password:
Confirm Password:
Idle Timeout: 5 (Minutes)

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

Setting	Description
User Name	A descriptive (alphanumeric) name of the user for identification and management purposes.
User Type	From the menu, select a predefined user type, which determines the access credentials: • **SSL VPN User**. A user who can log in only to the SSL VPN portal. • **Administrator**. A user who has full access and the capacity to change the VPN firewall configuration (that is, read/write access). • **Guest (readonly)**. A user who can only view the VPN firewall configuration (that is, read-only access). • **IPSEC VPN User**. A user who can make an IPSec VPN connection only through a NETGEAR ProSAFE VPN Client, and only when the XAUTH feature is enabled (see *Configure Extended Authentication (XAUTH)* on page 388). • **L2TP User**. A user who can connect over an L2TP connection to an L2TP client that is located behind the VPN firewall. • **PPTP User**. A user who can connect over a PPTP connection to a PPTP client that is located behind the VPN firewall.
Select Group	The menu shows the groups that are listed on the Groups screen. From the menu, select the group to which you want to assign the user. For information about how to configure groups, see *Manage Authentication Groups* on page 494. **Note:** The user is assigned automatically to the domain that is associated with the selected group.

Setting	Description
Password	The password that the user must enter to gain access to the VPN firewall.
Confirm Password	The password that you enter in this field must be identical to the password that you enter 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.

9. Click the **Apply** button.

   Your settings are saved. The user is added to the List of Users table.

Change a User Account

The following procedure describes how to change an existing user account. However, you cannot change the user name or the group to which the user is assigned.

➢ **To change a user account:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Users > Users**.

   The Users screen displays.

7. In the List of Users table, click the **Edit** button for the user that you want to change.

   The Edit Users screen displays.

8. Change the settings.

   For more information about the settings, see *Add a User Account* on page 500.

9. To change the password, select the **Check to Edit Password** check box.

The password fields become accessible.

10. Change the password.
11. Click the **Apply** button.

    Your settings are saved. The modified user account displays in the List of Users table on the Users screen.

Remove One or More User Accounts

The following procedure describes how to remove one or more user accounts that you no longer need.

Note: You cannot remove the default admin or guest user account.

➢ **To remove one or more user accounts:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Users > Groups**.

   The Groups screen displays.
7. In the List of Users table, select the check box to the left of each user that you want to remove or click the **Select All** button to select all users.
8. Click the **Delete** button.

   The selected users are removed from the List of Users table.

Manage 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.

The following sections provide information about managing user login policies:

- *Configure Login Policies*
- *Configure Login Restrictions Based on IP Addresses*
- *Remove One or More IP Addresses for Login Restrictions*
- *Configure Login Restrictions Based on Web Browsers*
- *Remove One or More Web Browsers for Login Restrictions*

Configure Login Policies

The following procedure describes how to configure a user login procedure.

➢ **To configure user login policies:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

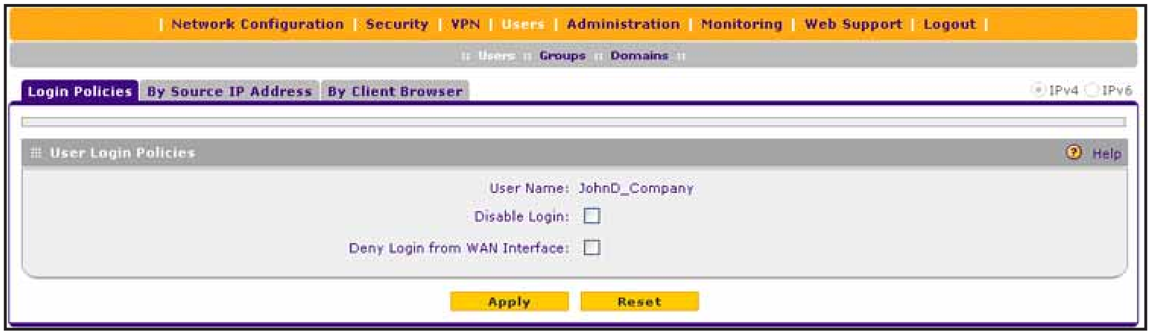
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Users > Users**.

   The Users screen displays.
7. In the List of Users table, to the right of the user for which you want to set login policies, click the corresponding **Policies** button.

   The policies submenu tabs display, with the Login Policies screen in view.


| 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: JohnD_Company

Disable Login: □

Deny Login from WAN Interface: □

8. Select one or both check boxes:
   - **Disable Login**. Prohibits the user from logging in to the VPN firewall.
   - **Deny Login from WAN Interface**. Prohibits the user from logging in from the WAN interface. In this case, the user can log in only from the LAN interface.

Note: For security reasons, the **Deny Login from WAN Interface** check box is selected by default for guests and administrators. The **Disable Login** check box is disabled (masked out) for administrators.

9. Click the **Apply** button.

   Your settings are saved.

Configure Login Restrictions Based on IP Addresses

The following procedure describes how to restrict logging in based on IP addresses.

➤ **To restrict logging in based on IP addresses:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

The Router Status screen displays.

6. Select **Users > Users**.

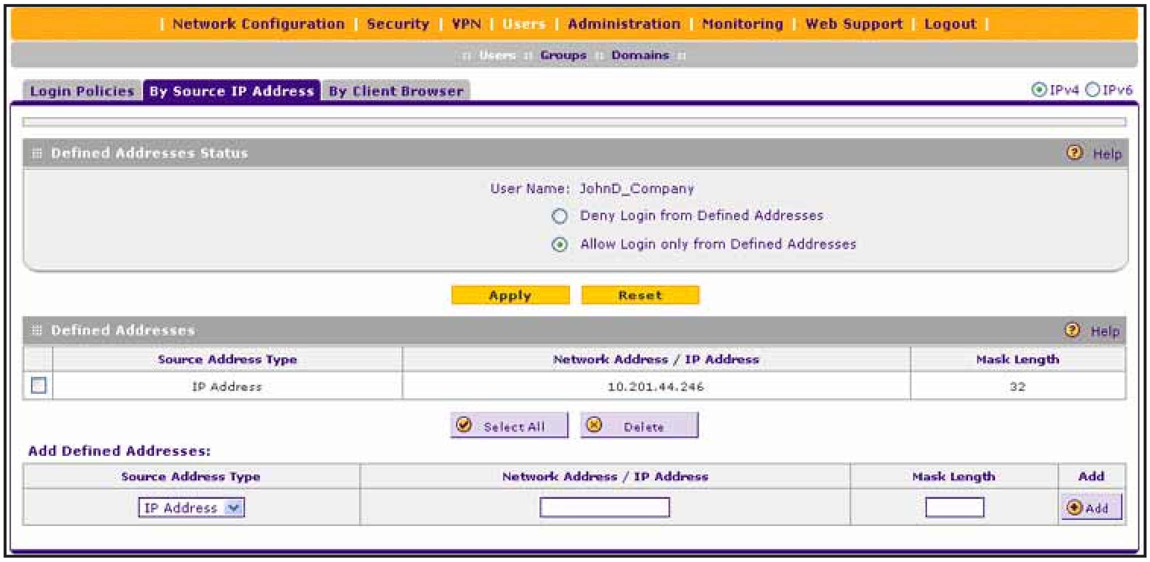
   The Users screen displays.

7. In the List of Users table, to the right of the user for which you want to set login policies, click the corresponding **Policies** button.

   The policies submenu tabs display, with the Login Policies screen in view.

8. Click the **By Source IP Address** submenu tab.

   The By Source IP Address screen displays the IPv4 settings. The following figure shows an IP address in the Defined Addresses table as an example.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Users :: Groups :: Domains ::
Login Policies
By Source IP Address
By Client Browser
Defined Addresses Status
Help
Apply
Reset
Defined Addresses
Help
Select All
Delete

● IPv4 ○ IPv6

User Name: JohnD_Company

○ Deny Login from Defined Addresses

● Allow Login only from Defined Addresses

	Source Address Type	Network Address / IP Address	Mask Length
□	IP Address	10.201.44.246	32

Add Defined Addresses:

Source Address Type	Network Address / IP Address	Mask Length	Add
IP Address ▾			Add

9. To restrict logging in based on IPv6 addresses, in the upper right, select the **IPv6** radio button.

   The By Source IP Address screen displays the IPv6 settings. Except for the **Prefix Length** field, which is the **Subnet Mask** field on the screen for IPv4, the IPv6 screen is identical to the IPv4 screen.

10. In the Defined Addresses Status section, select a radio button:

    - **Deny Login from Defined Addresses**. Denies logging in from the IP addresses in the Defined Addresses table.
    - **Allow Login only from Defined Addresses**. Allows logging in from the IP addresses in the Defined Addresses table.

11. Click the **Apply** button.

    Your settings are saved.

12. In the Add Defined Addresses section, add an address to the Defined Addresses table by entering the settings as described in the following table.

WARNING:

If you allow login only from the defined IP addresses, add your own IP address to the Defined Addresses table; otherwise, you are locked out.

Setting	Description
Source Address Type	Select the type of address from the menu: • **IP Address**. A single IPv4 or IPv6 address. • **IP Network**. A network of IPv4 or IPv6 addresses. For IPv4, you must enter a netmask length in the **Mask Length** field. For IPv6, you must enter a prefix length in the **Prefix Length** field.
Network Address / IP Address	Depending on your selection from the **Source Address Type** menu, enter the IP address or the network address.
Subnet Mask (IPv4 screen) or Prefix Length (IPv6 screen)	For IPv4, and only for a network address, enter the netmask length (0–32). By default, a single IPv4 address is assigned a netmask length of 32.
	For IPv6, and only for a network address, enter the prefix length (0–64). By default, a single IPv6 address is assigned a prefix length of 64.

13. Click the **Add** button.

    The address is added to the Defined Addresses table.

14. Repeat *Step 12* and *Step 13* for any other addresses that you want to add to the Defined Addresses table.

Remove One or More IP Addresses for Login Restrictions

The following procedure describes how to remove one or more IP addresses that you no longer need for login restrictions.

➢ **To remove one or more IP addresses for login restrictions:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Users > Users**.

   The Users screen displays.

7. In the List of Users table, to the right of the user for which you want to change login policies, click the corresponding **Policies** button.

   The policies submenu tabs display, with the Login Policies screen in view.

8. Click the **By Source IP Address** submenu tab.

   The By Source IP Address screen displays the IPv4 settings.

9. To remove IPv6 addresses, in the upper right, select the **IPv6** radio button.

   The By Source IP Address screen displays the IPv6 settings.

10. In the Defined Addresses table, select the check box to the left of each address that you want to remove or click the **Select All** button to select all addresses.
11. Click the **Delete** button.

    The selected addresses are removed from the Defined Addresses table.

Configure Login Restrictions Based on Web Browsers

The following procedure describes how to restrict login restrictions based on web browsers.

➢ **To restrict logging in based on the user’s browsers:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

The Router Status screen displays.

6. Select **Users > Users**.

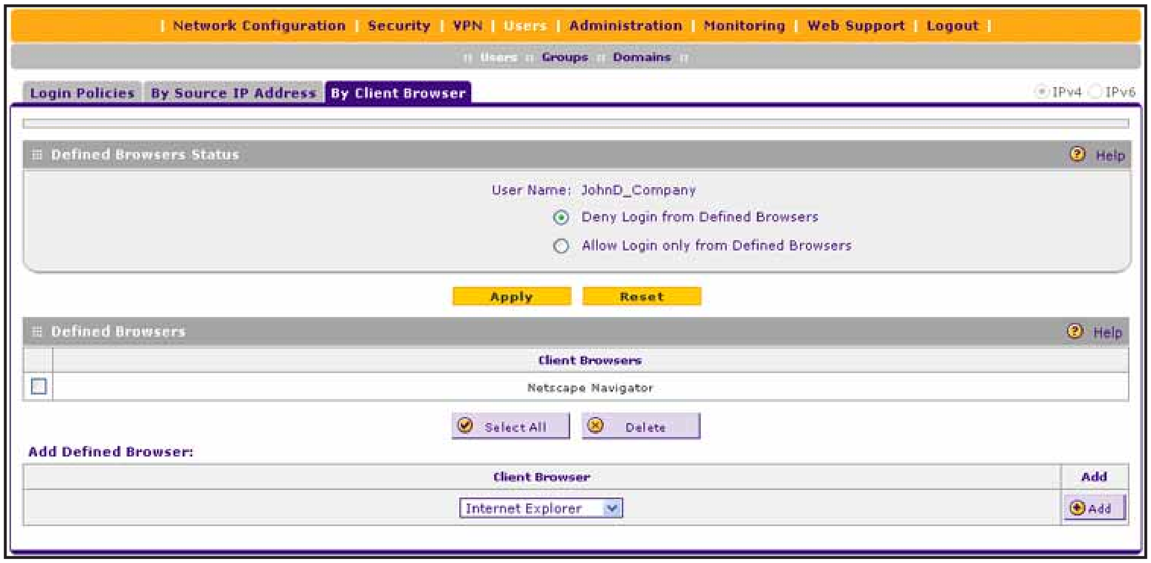
   The Users screen displays.

7. In the List of Users table, to the right of the user for which you want to set login policies, click the corresponding **Policies** button.

   The policies submenu tabs display, with the Login Policies screen in view.

8. Click the **By Client Browser** submenu tab.

   The By Client Browser screen displays. The following figure shows a browser in the Defined Browsers table as an example.



User Name: JohnD_Company

● Deny Login from Defined Browsers

○ Allow Login only from Defined Browsers

	Client Browsers
□	Netscape Navigator

Add Defined Browser:

Client Browser	Add
Internet Explorer	Add

9. In the Defined Browsers Status section, select a radio button:
   - **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.

10. Click the **Apply** button.

    Your settings are saved.

11. In the Add Defined Browser section, add a browser to the Defined Browsers table by selecting one of the following browsers from the menu:
    - **Internet Explorer**.
    - **Opera**.
    - **Netscape Navigator**.
    - **Firefox**. Mozilla Firefox.
    - **Mozilla**. Other Mozilla browsers.

12. Click the **Add** button.

    The browser is added to the Defined Browsers table.

13. Repeat *Step 11* and *Step 12* for any other browsers that you want to add to the Defined Browsers table.

Remove One or More Web Browsers for Login Restrictions

The following procedure describes how to remove one or more web browsers that you no longer need for login restrictions.

➢ **To remove one or more web browsers for login restrictions:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Users > Users**.

   The Users screen displays.

7. In the List of Users table, to the right of the user for which you want to change login policies, click the corresponding **Policies** button.

   The policies submenu tabs display, with the Login Policies screen in view.

8. Click the **By Client Browser** submenu tab.

   The By Client Browser screen displays.

9. In the Defined Browsers table, select the check box to the left of each browser that you want to remove or click the **Select All** button to select all browsers.
10. Click the **Delete** button.

    The selected browsers are removed from the Defined Browsers table.

Change Passwords and Automatic Logout Period

For any user, you can change the password and automatic logout period. Only administrators have read/write access and can change these settings. All other users have read-only access.

> IMPORTANT:
>
> **The default administrator 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 does not contain dictionary words from any language and is a mixture of letters (both uppercase and lowercase), numbers, and selected special characters. The password can be up to 32 characters in length. However, the password cannot contain a space nor any of the following special characters:

```
` ~ ! # $ & * ( ) - + | \ ; : ' " < >
```

After a factory defaults reset, the password and time-out value are changed back to **password** and 5 minutes, respectively.

➢ **To change a password:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

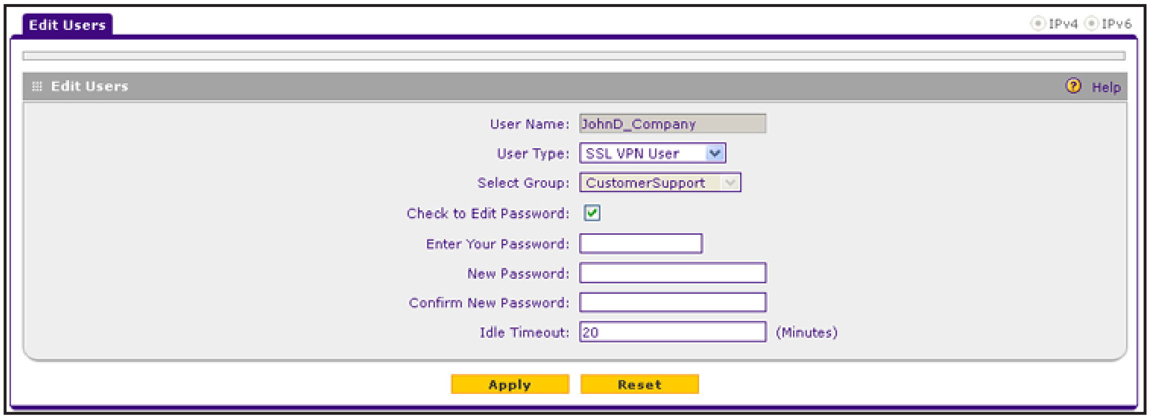
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Users > Users**.

   The Users screen displays.

7. In the List of Users table, to the right of the user for which you want to change the settings, click the corresponding **Edit** button.

   The Edit Users screen displays.



User Name: JohnD_Company
User Type: SSL VPN User
Select Group: CustomerSupport
Check to Edit Password: ☑
Enter Your Password:
New Password:
Confirm New Password:
Idle Timeout: 20 (Minutes)

8. Change the password and logout period settings as described in the following table.

Setting	Description
Check to Edit Password	Select this check box to make the password fields accessible.
Enter Your Password	Enter the password with which you have logged in.
New Password	Enter the new password.
Confirm New Password	Reenter the new password for confirmation. The password that you enter in this field must be identical to the password that you enter 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.

9. Click the **Apply** button.

   Your settings are saved.

Manage Digital Certificates for VPN Connections

The following sections provide information about managing digital certificates:

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

VPN Certificates Overview

The VPN firewall uses digital certificates (also known as X509 certificates) during the Internet Key Exchange (IKE) authentication phase to authenticate connecting IPSec VPN gateways or clients, or to be authenticated by remote entities:

- On the VPN firewall, you can enter a digital certificate when you manually configure an IKE policy. For an IKE policy, the digital certificate is referred to as an RSA signature (see *Authentication Method* on page 372).
- On the VPN client, you can enter a digital certificate when you configure authentication.

Digital certificates are extended for secure web access connections over HTTPS (that is, SSL connections). Digital certificates either can be self-signed or can be issued by certification authorities (CAs) such as an internal Windows server or an external organization such as Verisign or Thawte.

However, if the digital certificate contains the extKeyUsage extension, the certificate 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.

When you upload a digital certificate, the VPN firewall checks the validity and purpose of the certificate. If the certificate passes the validity test and the purpose matches its use, the VPN firewall accepts the certificate. The check for the purpose must correspond to its use for IPSec VPN, SSL VPN, or both. If the defined purpose is for IPSec VPN and SSL VPN, the digital certificate is uploaded to both the IPSec VPN certificate repository and the SSL VPN certificate repository. However, if the defined purpose is for IPSec VPN only, the certificate is uploaded only to the IPSec VPN certificate repository.

The 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. 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.

You can view loaded digital certificates, upload a new digital certificate, and generate a certificate signing request (CSR). The VPN firewall typically holds two types of digital certificates:

- **CA certificates**. Each CA issues its own digital certificate to validate communication with the CA and to verify the validity of digital certificates that are signed by the CA.
- **Self-signed certificates**. The digital certificates that are issued to you by a CA to identify your device.

On the VPN firewall, you can manage certificates through four tables:

- **Trusted Certificates (CA Certificate) table**. Contains the trusted digital certificates that were issued by CAs and that you uploaded (see *Manage VPN CA Certificates* on page 514).
- **Active Self Certificates table**. Contains the self-signed certificates that were issued by CAs and that you uploaded (see *Manage VPN Self-Signed Certificates* on page 516).
- **Self Certificate Requests table**. Contains the self-signed certificate requests that you generated. You might or might not have submitted these requests to CAs, and CAs might or might not have issued digital certificates for these requests. Only the self-signed certificates in the Active Self Certificates table are active on the VPN firewall (see *Manage VPN Self-Signed Certificates* on page 516).
- **Certificate Revocation Lists (CRL) table**. Contains the lists with digital certificates that are revoked and no longer valid, that were issued by CAs, and that you uploaded. Note, however, that the table displays only the active CAs and their critical release dates (see *Manage the VPN Certificate Revocation List* on page 522).

Manage VPN CA Certificates

The following sections provide information about managing VPN certification authority (CA) certificates:

- *Upload a CA Certificate*
- *Remove a CA Certificate*

Upload a CA Certificate

The following procedure describes how to upload a CA certificate of a trusted CA on the VPN firewall.

➢ **To upload a CA certificate of a trusted CA on the VPN firewall:**

1. Download a digital certificate file from a trusted CA and store it on your computer.
2. On your computer, launch an Internet browser.
3. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

4. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

5. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

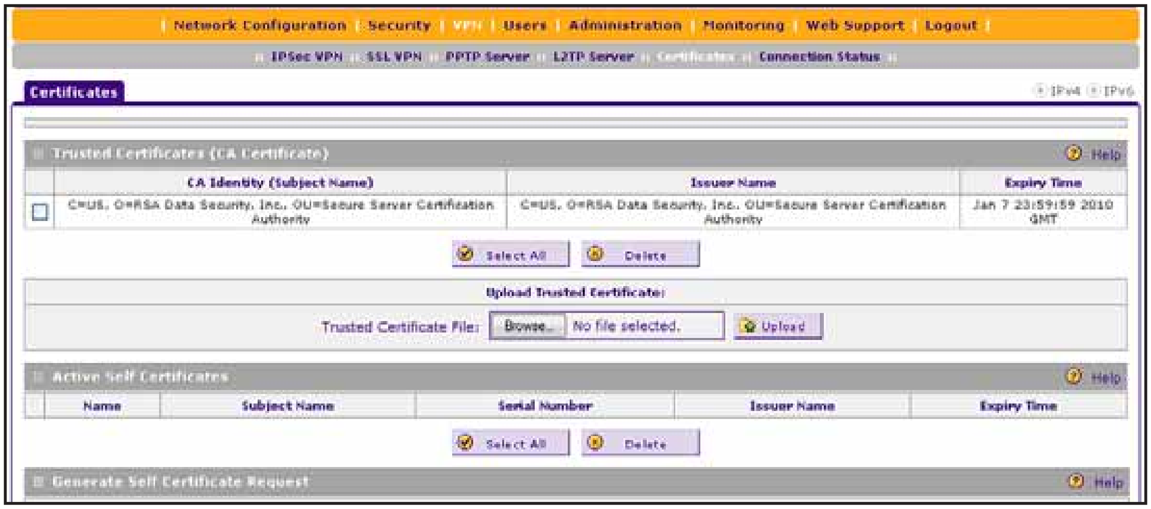
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

6. Click the **Login** button.

   The Router Status screen displays.

7. Select **VPN > Certificates**.

   The Certificates screen displays. The following figure shows the top section with the trusted certificate information and a sample certificate in the Trusted Certificates (CA Certificate) table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
Certificates
○ IPv4 ○ IPv6
Help
Select All
Delete
Browse...
Upload
Help
Select All
Delete
Help

Trusted Certificates (CA Certificate)

	CA Identity (Subject Name)	Issuer Name	Expiry Time
□	C=US, O=RSA Data Security, Inc., OU=Secure Server Certification Authority	C=US, O=RSA Data Security, Inc., OU=Secure Server Certification Authority	Jan 7 23:59:59 2010 GMT

Upload Trusted Certificate:

Trusted Certificate File: No file selected.

Active Self Certificates

	Name	Subject Name	Serial Number	Issuer Name	Expiry Time

Generate Self Certificate Request

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.

8. In the Upload Trusted Certificates section, click the **Browse** button and navigate to the trusted digital certificate file that you downloaded on your computer.

9. Click the **Upload** button.

   The VPN firewall verifies the certificate for validity and purpose. If the VPN firewall approves the certificate, it is added to the Trusted Certificates (CA Certificates) table.

Remove a CA Certificate

The following procedure describes how to remove one or more CA certificates that you no longer need.

➢ **To remove one or more CA certificates:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > Certificates**.

   The Certificates screen displays.
7. In the Trusted Certificates (CA Certificate) table, select the check box to the left of each digital certificate that you want to remove or click the **Select All** button to select all digital certificates.
8. Click the **Delete** button.

   The selected certificates are removed from the Trusted Certificates (CA Certificate) table.

Manage VPN Self-Signed Certificates

Instead of obtaining a digital certificate from a CA, you can generate and sign your own digital certificate. The following sections provide information about managing VPN self-signed certificates:

- *Generate a Certificate Signing Request and Obtain a Self-Signed Certificate from a CA*
- *View Self-Signed Certificates*
- *Remove One or More Self-Signed Certificates*
- *Remove One or More Certificate Signing Requests*

Generate a Certificate Signing Request 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 then 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, obtain a digital certificate from a CA, and upload the digital certificate to the VPN firewall:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

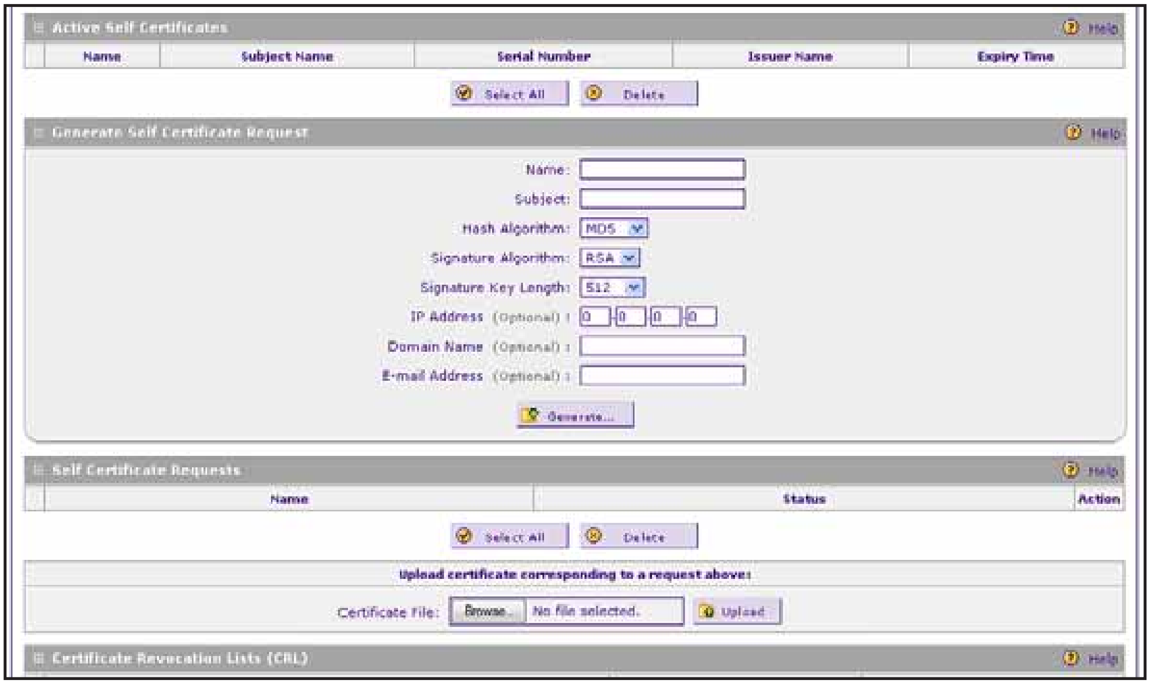
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > Certificates**.

   The Certificates screen displays. The following figure shows the middle section with the Active Self Certificates section, Generate Self Certificate Request section, and Self Certificate Requests section. The Self Certificate Requests table shows a sample certificate.



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) :

7. In the Generate Self Certificate Request section, enter the settings as described in the following table.

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 must have the same value in the **Subject** field.
Hash Algorithm	From the menu, select a 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 menu, the only possible selection is RSA. That is, RSA is the default setting for generating a CSR.
Signature Key Length	From the menu, select one of the following signature key lengths in bits: • **512** • **1024** • **2048** **Note:** Larger key sizes might improve security but might also decrease performance.
IP Address (Optional)	Enter your fixed (static) IP address. If your IP address is dynamic, leave this field blank.

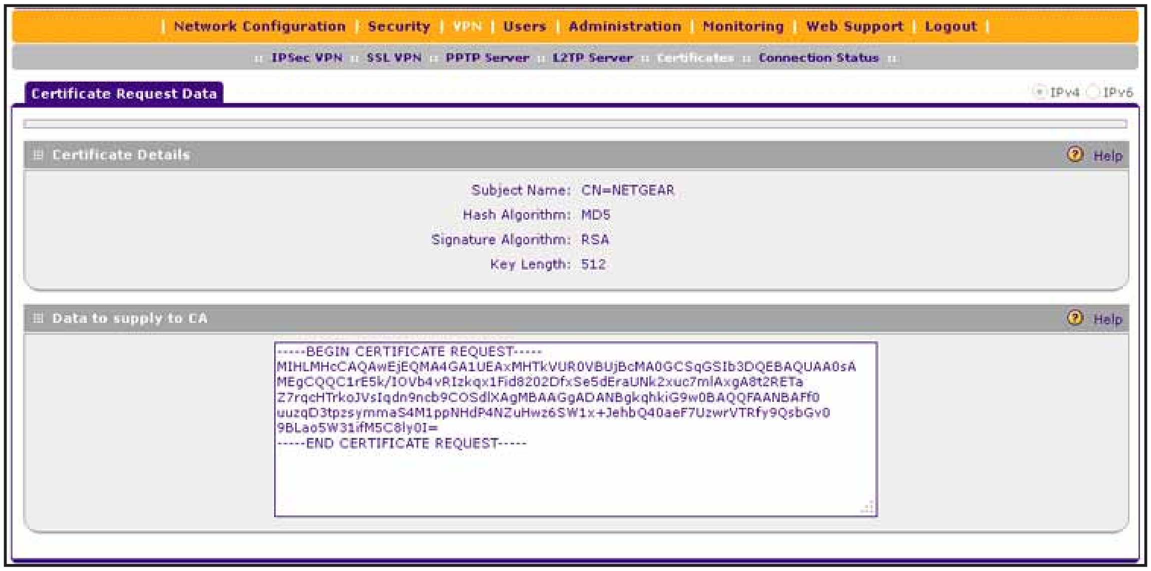
Setting	Description
Domain Name (Optional)	Enter your Internet domain name or leave this field blank.
E-mail Address (Optional)	Enter the email address of a technical contact in your company.

8. Click the **Generate** button.

   A new SCR is created and added to the Self Certificate Requests table.

9. To view the new SCR, in the Self Certificate Requests table, click the **View** button.

   The Certificate Request Data screen displays.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: IPSec VPN :: SSL VPN :: PPTP Server :: L2TP Server :: Certificates :: Connection Status ::
Certificate Request Data
● IPv4 ○ IPv6
Certificate Details
Help
Data to supply to CA
Help

Subject Name: CN=NETGEAR
Hash Algorithm: MD5
Signature Algorithm: RSA
Key Length: 512

```
-----BEGIN CERTIFICATE REQUEST-----
MIHLMHcCAQAwEjEQMA4GA1UEAxMHTkVUR0VBUjBcMA0GCSqGSIb3DQEBAQUAA0sA
MEgCQQC1rE5k/IOVb4vRIzkqx1Fid8202DfxSe5dEraUNk2xuc7mlAxgA8t2RETa
Z7rqcHTrkoJVsIqdn9ncb9COSdlXAgMBAAGgADANBgkqhkiG9w0BAQQFAANBAFf0
uuzqD3tpzsymmaS4M1ppNHdP4NZuHwz6SW1x+JehbQ40aeF7UzwrVTRfy9QsbGv0
9BLao5W31ifM5C8ly0I=
-----END CERTIFICATE REQUEST-----
```

10. 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-----.”
11. 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.
12. Download the digital certificate file from the CA and store it on your computer.
13. Return to the Certificates screen and locate the Self Certificate Requests section.
14. Select the check box next to the self-signed certificate request.
15. Click the **Browse** button and navigate to the digital certificate file from the CA that you just stored on your computer.

16. Click the **Upload** button.

    The VPN firewall verifies the certificate for validity and purpose. If the VPN firewall approves the certificate, it is added to the Active Self Certificates table.

View Self-Signed Certificates

The following procedure describes how to view active self-signed certificates.

➢ **To view active self-signed certificates:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > Certificates**.

   The Certificates screen displays.

   The Active Self Certificates table shows the digital certificates that are 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**. A serial number maintained by the CA. The number is used to identify the digital certificate with the CA.
   - **Issuer Name**. The name of the CA that issued the digital certificate.
   - **Expiry Time**. The date on which the digital certificate expires. You must renew the digital certificate before it expires.

Remove One or More Self-Signed Certificates

The following procedure describes how to remove one or more self-signed certificates that you no longer need.

➤ **To remove one or more self-signed certificates:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > Certificates**.

   The Certificates screen displays.
7. In the Active Self Certificates table, select the check box to the left of each self-signed certificate that you want to remove or click the **Select All** button to select all self-signed certificates.
8. Click the **Delete** button.

   The selected certificates are removed from the Active Self Certificates table.

Remove One or More Certificate Signing Requests

The following procedure describes how to remove one or more certificate signing requests (CSRs) that you no longer need.

➤ **To remove one or more CSRs:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **VPN > Certificates**.

   The Certificates screen displays.

7. In the Self Certificate Requests table, select the check box to the left of each certificate signing request that you want to remove or click the **Select All** button to select all certificate signing requests.
8. Click the **Delete** button.

   The selected requests are removed from the Self Certificate Requests table.

Manage the VPN Certificate Revocation List

A Certificate Revocation List (CRL) shows digital certificates that are revoked and no longer valid. Each CA issues its own CRLs. It is important that you keep your CRLs up-to-date. You must obtain the CRL for each CA regularly.

The following sections provide information about managing CRLs:

- *View Certificate Revocation Lists and Upload a Certificate Revocation List*
- *Remove One or More Certificate Revocation Lists*
- *Self-Signed Certificates and Security Alerts*

View Certificate Revocation Lists and Upload a Certificate Revocation List

The following procedure describes how to view the loaded Certificate Revocation Lists (CRLs) and upload a new CRL.

➤ **To view the CRLs and upload a new CRL:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

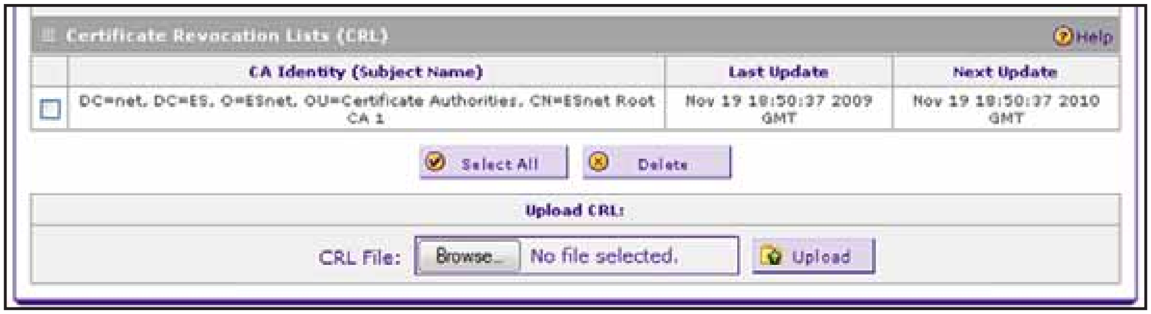
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **VPN > Certificates**.

   The Certificates screen displays. The following figure shows the bottom section with the Certificate Revocation Lists (CRL) table. The table shows a certificate as an example.



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

   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.

7. In the Upload CRL section, click the **Browse** button and navigate to the CLR file that you previously downloaded from a CA.

8. Click the **Upload** button.

   The VPN firewall verifies the CRL. If the VPN firewall approves the CRL, it is added to the Certificate Revocation Lists (CRL) table.

Note: If the table already contains a CRL from the same CA, the old CRL is removed when you upload the new CRL.

Remove One or More Certificate Revocation Lists

The following procedure describes how to remove one or more Certificate Revocation Lists (CRLs) that you no longer need.

- **To remove one or more CRLs:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

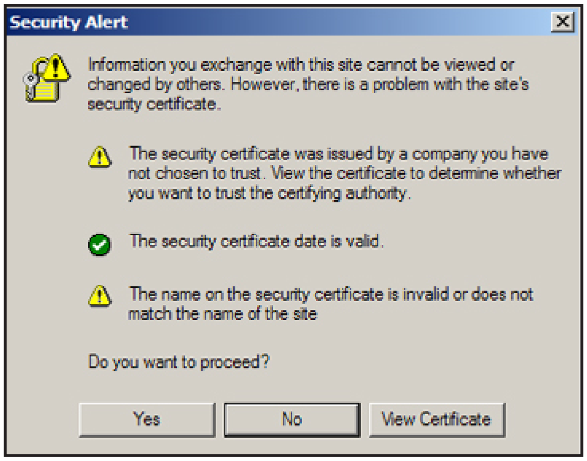
   The Router Status screen displays.
6. Select **VPN > Certificates**.

   The Certificates screen displays.
7. In the Certificate Revocation Lists (CRL) table, select the check box to the left of each CRL that you want to remove or click the **Select All** button to select all CRLs.
8. Click the **Delete** button.

   The selected CRLs are removed from the Certificate Revocation Lists (CRL) table.

Self-Signed Certificates and Security Alerts

A self-signed digital certificate triggers a warning from most browsers because the certificate provides no protection against identity theft of a server. The following figure shows an image of a browser security alert.



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?

Figure 12. Security alert

A security alert can be generated for a security certificate for three reasons:

- The security certificate was issued by a company you have not chosen to trust.
- The date of the security certificate is invalid.
- The name on the security certificate is invalid or does not match the name of the site.

When a security alert is generated, the user can decide whether to trust the host.

11 Optimize Performance and Manage Your System

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 if a bottleneck occurs. To prevent bottlenecks from occurring in the first place, you can either reduce unnecessary traffic or reschedule some traffic to low-peak times. The VPN firewall has the necessary features and tools to help the network manager accomplish these goals.

The following sections provide information about performance management:

- *Bandwidth Capacity Overview*
- *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 Overview

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

- **LAN side**. 4000 Mbps (four LAN ports at 1000 Mbps each)
- **WAN side**
  - **Load balancing mode**. 2000 Mbps (two WAN ports at 1000 Mbps each)
  - **Auto-rollover mode**. 1000 Mbps (one active WAN port at 1000 Mbps)
  - **Single WAN port mode**. 1000 Mbps (one active WAN port at 1000 Mbps)

In practice, the WAN-side bandwidth capacity is much lower when you use a DSL or cable modem to connect to the Internet. At 1.5 Mbps, the WAN ports support the following traffic rates:

- **Load balancing mode**. 3 Mbps (two WAN ports at 1.5 Mbps each)
- **Auto-rollover mode**. 1.5 Mbps (one active WAN port at 1.5 Mbps)
- **Single WAN port mode**. 1.5 Mbps (one active WAN port at 1.5 Mbps)

As a result, and depending on the traffic that is being carried, the WAN side of the VPN firewall is the limiting factor to throughput for most installations.

Using two WAN ports in load balancing mode increases the bandwidth capacity of the WAN side of the VPN firewall, but no backup is present if one of the WAN ports fails. When such a failure occurs, the traffic that would be sent on the failed WAN port is diverted to another WAN port that is still working, thus increasing its load. However, one exception exists: Traffic that is bound by protocol to the WAN port that failed is not diverted.

Features That Reduce Traffic

The following sections provide information about features of the VPN firewall that you can change in such a way that the traffic load on the WAN side decreases:

- *LAN WAN Outbound Rules and DMZ WAN Outbound Rules — Service Blocking*
- *Content Filtering*
- *Source MAC Filtering*

LAN WAN Outbound Rules and DMZ WAN Outbound Rules — Service Blocking

You can control specific outbound traffic (from LAN to WAN and from the DMZ to WAN). Any outbound rule that you create restricts outgoing traffic and therefore decreases the traffic load on the WAN side.

If you have not defined any LAN WAN outbound rules, only the default rule applies, which allows all outgoing traffic.

WARNING:

Incorrect configuration of outbound firewall rules can cause serious connection problems.

Each of the following rules 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

This section summarizes the various criteria that you can apply to outbound rules in order to reduce traffic. For more information about outbound rules, see *Outbound Rules — Service Blocking* on page 212. For detailed information about how to configure outbound rules, see *Add LAN WAN Rules* on page 223 and *Add DMZ WAN Rules* on page 233.

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 (see *Outbound Rules — Service Blocking* on page 212 and *Manage Customized Services* on page 280).
- **LAN users (or DMZ users)**. You can specify which computers on your network are affected by an outbound rule. You have several options:
  - **Any**. The rule applies to all computers and devices on your LAN or DMZ.
  - **Single address**. The rule applies to the address of a particular computer.

  - **Address range**. The rule applies to a range of addresses.
  - **Groups**. The rule applies to a group of computers. (You can configure groups for LAN WAN outbound rules but not for DMZ WAN outbound rules.) The Known PCs and Devices table is an automatically maintained list of all known computers and network devices and is generally referred to as the network database, (see *Manage the Network Database* on page 133). Computers and network devices are entered into the network database by various methods, (see *Manage IPv4 LAN Groups and Hosts* on page 132).
  - **IP Groups**. The rule applies to a group of individual LAN IP addresses. For information about assigning IP addresses to groups, see *Manage IP Address Groups* on page 288. (LAN IP groups do not apply to DMZ WAN outbound rules.)
- **WAN users**. You can specify which Internet locations are covered by an outbound rule, based on their IP address:
  - **Any**. The rule applies to all Internet IP address.
  - **Single address**. The rule applies to a single Internet IP address.
  - **Address range**. The rule applies to a range of Internet IP addresses.
  - **IP Groups**. The rule applies to a group of individual WAN IP addresses. For information about assigning IP addresses to groups, see *Manage IP Address Groups* on page 288.
- **Schedule**. You can configure three different schedules to specify when a rule is applied. After 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 *Define a Schedule* on page 292.
- **QoS profile**. You can apply QoS profiles to outbound rules to regulate the priority of traffic. For information about QoS profiles, see *Manage Quality of Service Profiles for IPv4 Firewall Rules* on page 293.
- **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 *Manage Bandwidth Profiles for IPv4 Traffic* on page 299.

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 information about how to use this feature, see *Enable Source MAC Filtering* on page 312.

Features That Increase Traffic

The following sections provide information about features of the VPN firewall that might cause the traffic load on the WAN side to increase:

- *LAN WAN Inbound Rules and DMZ WAN Inbound Rules — Port Forwarding*
- *Port Triggering*
- *DMZ Port*
- *Exposed Hosts*
- *VPN, L2TP, and PPTP Tunnels*

LAN WAN Inbound Rules and DMZ WAN Inbound Rules — Port Forwarding

Any inbound rule that you create allows additional incoming traffic (from WAN to LAN and from WAN to the DMZ) and therefore increases the traffic load on the WAN side.

If you have not defined any LAN WAN inbound rules, only the default rule applies, which 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 of the following rules 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

This section summarizes the various criteria that you can apply to inbound rules and that might increase traffic. For more information about inbound rules, see *Inbound Rules — Port Forwarding* on page 215. For detailed information about how to configure inbound rules, see

Add LAN WAN Rules on page 223 and *Add DMZ WAN Rules* on page 233.

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 (see *Inbound Rules — Port Forwarding* on page 215 and *Manage Customized Services* on page 280).
- **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)**. You specify which computers on your network are affected by an inbound rule only when the IPv4 routing mode is Classical Routing. When Classical Routing is enabled, you have several options:
  - **Any**. The rule applies to all computers and devices on your LAN or DMZ.
  - **Single address**. The rule applies to the address of a particular computer.
  - **Address range**. The rule applies to a range of addresses.
  - **Groups**. The rule is applied to a group of computers. (You can configure groups for LAN WAN outbound rules but not for DMZ WAN outbound rules.) The Known PCs and Devices table is an automatically maintained list of all known computers and network devices and is generally referred to as the network database (see *Manage the Network Database* on page 133). Computers and network devices are entered into the network database by various methods (see *Manage IPv4 LAN Groups and Hosts* on page 132).
  - **IP Groups**. The rule applies to a group of individual LAN IP addresses. For information about assigning IP addresses to groups, see *Manage IP Address Groups* on page 288. (LAN IP groups do not apply to DMZ WAN inbound rules.)
- **WAN users**. You can specify which Internet locations are covered by an inbound rule, based on their IP address:
  - **Any**. The rule applies to all Internet IP address.
  - **Single address**. The rule applies to a single Internet IP address.
  - **Address range**. The rule applies to a range of Internet IP addresses.
  - **IP Groups**. The rule applies to a group of individual WAN IP addresses. For information about assigning IP addresses to groups, see *Manage IP Address Groups* on page 288.
- **Schedule**. You can configure three different schedules to specify when a rule is applied. After 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 *Define a Schedule* on page 292.
- **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 *Manage Bandwidth Profiles for IPv4 Traffic* on page 299.

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 *Manage Port Triggering* on page 325.

DMZ Port

The demilitarized zone (DMZ) is a network that, by default, has fewer firewall restrictions when compared to the LAN. The DMZ can be used to host servers (such as a web server, FTP server, or email server) and provide public access to them. The fourth LAN port on the VPN firewall (the rightmost LAN port) can be dedicated as a hardware DMZ port to safely provide services to the Internet without compromising security on your LAN. By default, the DMZ port and both inbound and outbound DMZ traffic are disabled. Enabling the DMZ port and allowing traffic to and from the DMZ increases the traffic through the WAN ports.

For information about how to enable the DMZ port, see *Manage the DMZ Port for IPv4 Traffic* on page 140. For information about how to configure DMZ traffic rules, see *Add DMZ WAN Rules* on page 233.

Exposed Hosts

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

WARNING:

For security, NETGEAR strongly recommends that you do not set up 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.

VPN, L2TP, and PPTP Tunnels

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

For information about IPSec VPN, L2TP, and PPTP tunnels, see *Chapter 8, Set Up Virtual Private Networking With IPSec Connections*. For information about SSL VPN tunnels, see *Chapter 9, Set Up Virtual Private Networking with SSL Connections*.

Use QoS and Bandwidth Assignment to Shift the Traffic Mix

By setting the Quality of Service (QoS) priority and assigning bandwidth profiles to firewall rules, you can shift the traffic mix to aim for optimum performance of the VPN firewall.

The following sections provide information about using QoS and bandwidth assignment to shift the traffic mix:

- *Setting QoS Priorities*
- *Assigning Bandwidth Profiles*

Setting QoS Priorities

The QoS priority settings determine the Quality of Service for the traffic passing through the VPN firewall.

You can create and assign QoS profiles to WAN interfaces. For more information about QoS profiles for WAN interfaces, see *Manage WAN QoS and WAN QoS Profiles* on page 74.

You can also create and assign a QoS profile (IPv4) or QoS priority (IPv6) to LAN WAN and DMZ WAN outbound firewall rules. 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 in the following ways:

- You can accept the default priority defined by the service itself by not changing its QoS priority.
- You can change the priority to a higher or lower value than its default setting to give the service higher or lower priority than it otherwise would have.

For more information about QoS profiles, see *Manage Quality of Service Profiles for IPv4 Firewall Rules* on page 293 and *Default Quality of Service Priorities for IPv6 Firewall Rules* on page 298.

Assigning 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 sufficient bandwidth to LAN users while preventing them from consuming all the bandwidth on your WAN links.

For more information about bandwidth profiles, see *Manage Bandwidth Profiles for IPv4 Traffic* on page 299.

Monitoring Tools for Traffic Management

The VPN firewall includes several tools that can be used to monitor the traffic conditions of the firewall and content-filtering engine and to monitor the users’ access to the Internet and the types of traffic that they are allowed to have. For a description of these tools, see *Chapter 12, Monitor System Access and Performance*.

System Management

The following sections provide information about system management:

- *Set Up Remote Management Access*
- *Use the Command-Line Interface*
- *Use a Simple Network Management Protocol Manager*
- *Manage the Configuration File*
- *Revert to Factory Default Settings*
- *Configure Date and Time Service*

Set Up Remote Management Access

An administrator can configure, upgrade, and check the status of the VPN firewall over the Internet through an SSL VPN connection.

The following sections provide information about setting up remote management access:

- *Remote Access*
- *Configure Remote Access*

Remote Access

When you enable remote management, you must use an SSL connection to access the VPN firewall from the Internet. You must enter **https://** (*not* http://) and type the VPN firewall’s WAN IP address and port number in your browser. For example, if the VPN firewall’s WAN IP address is 192.168.15.175 and the port number is 443, type the following in your browser: **https://192.168.15.175:443**.

The VPN firewall’s remote login URL is as follows:

https://<*IP_address*>:<*port_number*> or
https://<*FullyQualifiedDomainName*>:<*port_number*>

The IP address can be an IPv4 or IPv6 address.

Concerning security, note the following:

- For enhanced security, restrict access to as few external IP addresses as practical. See *Manage User Login Policies* on page 504 for information about restricting administrator access by IP address.
- To maintain security, the VPN firewall rejects a login that uses http://*address* rather than the SSL https://*address*.
- The first time that you remotely connect to the VPN firewall with a browser through an SSL connection, you might get a warning message regarding the SSL certificate. If you are using a Windows computer with Internet Explorer, click the **Yes** button to accept the certificate.

Tip: If you are using a Dynamic DNS service such as TZO, you can identify the WAN IP address of your VPN firewall by running **`tracert`** from the Windows Run menu option. Trace the route to your registered FQDN. For example, enter **`tracert VPN firewall.mynetgear.net`** and the WAN IP address that your ISP assigned to the VPN firewall is displayed.

Configure Remote Access

The following procedure describes how to configure remote management access on the VPN firewall.

WARNING:

When you enable remote management and grant administrative access through a WAN interface (see *Configure Login Policies* on page 504), 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 default admin and guest passwords before continuing (see *Change Passwords and Automatic Logout Period* on page 511).

➤ **To configure remote management on the VPN firewall:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

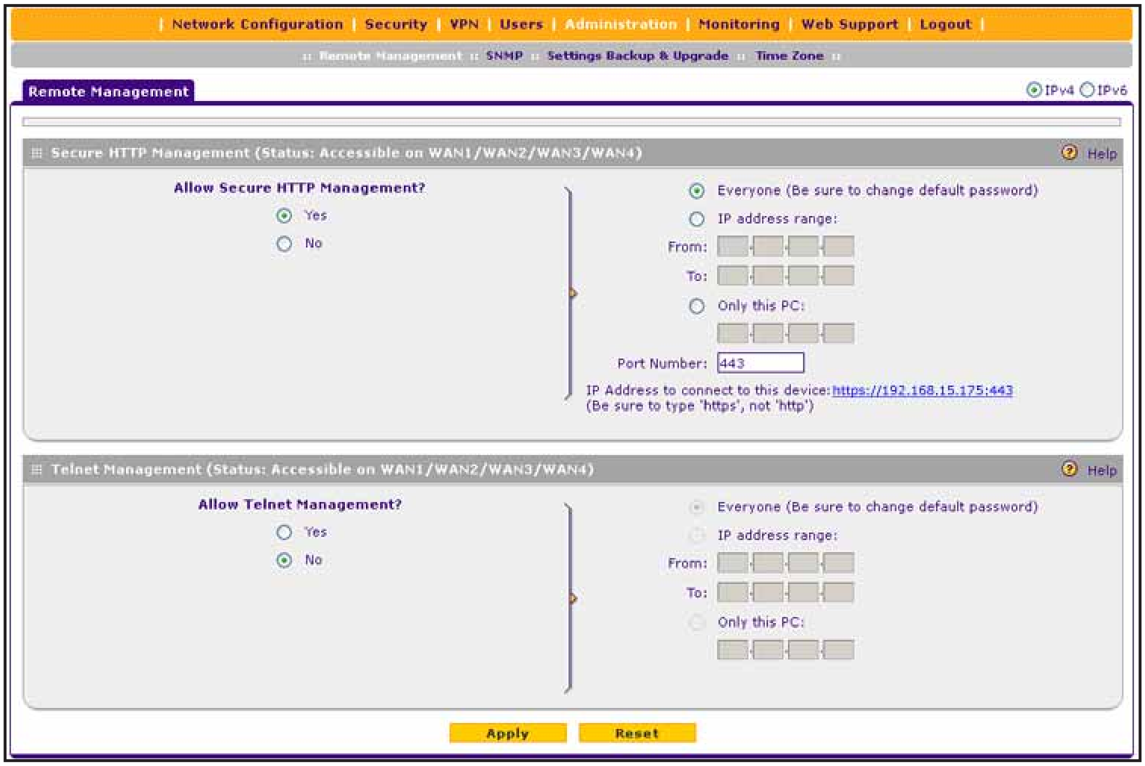
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Administration > Remote Management**.

   The Remote Management screen displays the IPv4 settings.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone ::
Remote Management
Help
Help
Apply
Reset

● IPv4 ○ IPv6

Secure HTTP Management (Status: Accessible on WAN1/WAN2/WAN3/WAN4)

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 WAN1/WAN2/WAN3/WAN4)

Allow Telnet Management?

○ Yes

● No

● Everyone (Be sure to change default password)

○ IP address range:

From:

To:

○ Only this PC:

7. To configure remote management for IPv6, in the upper right, select the **IPv6** radio button.

   The Remote Management screen displays the IPv6 settings.

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

Setting	Description
Secure HTTP Management	
Allow Secure HTTP Management?	To enable secure HTTP management, select the **Yes** radio button, which is the default setting. Selecting the **No** radio button disables secure HTTP management. **Note:** The selected setting applies to both WAN interfaces.
	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 first IP address of the range; in the **To** fields, type the last 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.
	In the **Port Number** field, 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.

Setting	Description
Telnet Management	
Allow Telnet Management?	To enable Telnet management, select the **Yes** radio button. By default, the **No** radio button is selected and Telnet management is disabled.
	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 first IP address of the range; in the **To** fields, type the last IP address of the range. • **Only this PC**. Only a user who uses the device with the specified IP address can manage over a Telnet connection. Type the IP address in the fields.

WARNING:

If you are remotely connected to the VPN firewall and you select the No radio button to disable secure HTTP management, you and all other SSL VPN users are disconnected when you click the Apply button.

9. Click the **Apply** button.

   Your settings are saved.

Use the Command-Line Interface

You can access the command-line interface (CLI) using the console port on the back panel of the VPN firewall (see *Back Panel* on page 20).

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.

   You are prompted for the login and password information.

2. Enter **admin** and **password** (or enter **guest** and **password** to log in as a read-only guest).

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.

To end a CLI session, issue the **exit** command.

Use a Simple Network Management Protocol Manager

Simple Network Management Protocol (SNMP) lets you monitor and manage the VPN firewall from an SNMP manager. The following sections provide information about using an SNMP manager:

- *SNMP Overview*
- *Set Up an SNMP Configuration and Specify the Trap Events*
- *Change an SNMP Configuration*
- *Remove One or More SNMP Configurations*
- *View SNMPv3 Default Users and Change the Security for an SNMPv3 User*
- *Configure the SNMP System Information*

SNMP Overview

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 (NMS300) 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 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.

Set Up an SNMP Configuration and Specify the Trap Events

The following procedure describes how to set up an SNMP configuration and specify the trap events.

➢ **To set up an SNMP configuration and specify the trap events:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

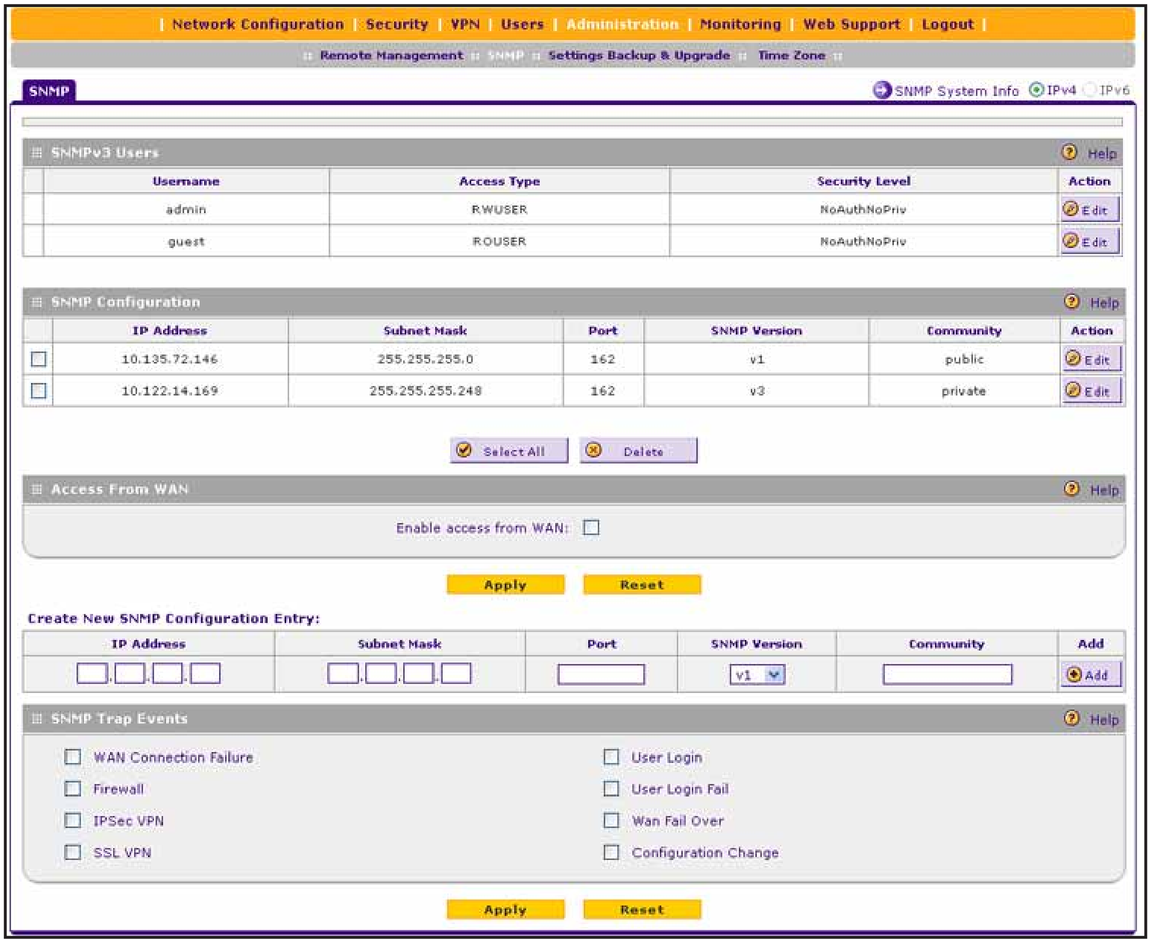
If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Administration > SNMP**.

   The SNMP screen displays. The following figure shows examples in the SNMP Configuration table.


| 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
Edit
Select All
Delete
Apply
Reset
Add

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
□	10.135.72.146	255.255.255.0	162	v1	public	Edit
□	10.122.14.169	255.255.255.248	162	v3	private	Edit

Access From WAN

Enable access from WAN: □

Create New SNMP Configuration Entry:

IP Address	Subnet Mask	Port	SNMP Version	Community	Add
. . .	. . .		v1		Add

SNMP Trap Events

□ WAN Connection Failure

□ Firewall

□ IPSec VPN

□ SSL VPN

□ User Login

□ User Login Fail

□ Wan Fail Over

□ Configuration Change

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.

7. In the Create New SNMP Configuration Entry section, enter the settings as described in the following table.

Setting	Description
Access From WAN	
Enable access from WAN	To enable SNMP access by an SNMP manager through the WAN interface, select the **Enable access from WAN** check box. By default, this check box is cleared and access is disabled.
Create New SNMP Configuration Entry	
IP Address	Enter the IP address of the new SNMP manager.
Subnet Mask	Enter the subnet mask of the new SNMP manager. Note the following: • If you want to narrow down the number of devices that can access the VPN firewall through the host IP address and receive traps, enter an IP address with a subnet mask of 255.255.255.252. • If you want to allow a subnet to access the VPN firewall through the host IP address and receive traps, enter an IP address with a subnet mask of 255.0.0.0. The traps are received at the IP address but almost the entire subnet has access through the community string.
Port	Enter the port number of the new SNMP manager. The default port number is 162.
SNMP Version	From the menu, select the SNMP version: • **v1**. SNMPv1. • **v2c**. SNMPv2c. • **v3**. SNMPv3.
Community	Enter the community string that allows the SNMP manager access to the MIB objects of the VPN firewall for the purpose of reading only.
SNMP Trap Events	
Select the check boxes to specify which SNMP trap events are sent to an SNMP manager: • **WAN Connection Failure**. Sent when the WAN connection fails. • **Firewall**. Sent when a new connection is initiated through the addition of a custom firewall rule. • **IPSec VPN**. Sent when an IPSec VPN tunnel is established or disconnected. • **SSL VPN**. Sent when an SSL VPN tunnel is established or disconnected. • **User Login**. Sent when a user logs in to the VPN firewall. • **User Login Fail**. Sent when a user attempts to log in to the VPN firewall but fails to do so. • **Wan Fail Over**. Sent when an auto-rollover occurs from one WAN interface to another. • **Configuration Change**. Sent when the configuration of the VPN firewall changes.	

8. Click the **Add** button.

   Your settings are saved and the new SNMP configuration is added to the SNMP Configuration table.

Change an SNMP Configuration

The following procedure describes how to change an existing SNMP configuration.

➢ To change an SNMP configuration:

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

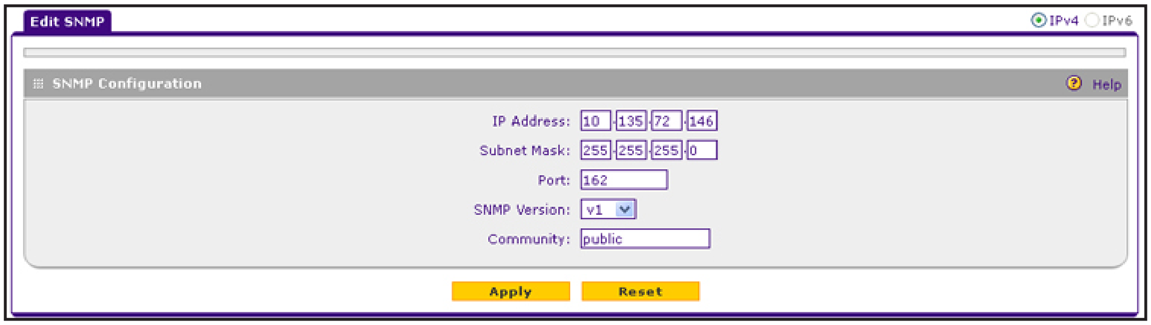
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Administration > SNMP**.

   The SNMP screen displays.
7. In the SNMP Configuration table, click the **Edit** button for the SNMP configuration that you want to change.

   The Edit SNMP screen displays.



IP Address: 10.135.72.146

Subnet Mask: 255.255.255.0

Port: 162

SNMP Version: v1

Community: public

8. Change the settings.

   For information about the settings, see *Set Up an SNMP Configuration and Specify the Trap Events* on page 538.
9. Click the **Apply** button.

   Your settings are saved. The modified SNMP configuration displays in the SNMP Configuration table on the SNMP screen.

Remove One or More SNMP Configurations

The following procedure describes how to remove one or more SNMP configurations that you no longer need.

- **To remove one or more SNMP configurations:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Administration > SNMP**.

   The SNMP screen displays.
7. In the SNMP Configuration table, select the check box to the left of each SNMP configuration that you want to remove or click the **Select All** button to select all SNMP configurations.
8. Click the **Delete** button.

   The selected SNMP configurations are removed from the SNMP Configuration table.

View SNMPv3 Default Users and Change the Security for an SNMPv3 User

The following procedure describes how to view the SNMPv3 default users and change the security for an SNMPv3 user.

- **To view the SNMPv3 default users and change the security for an SNMPv3 user:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

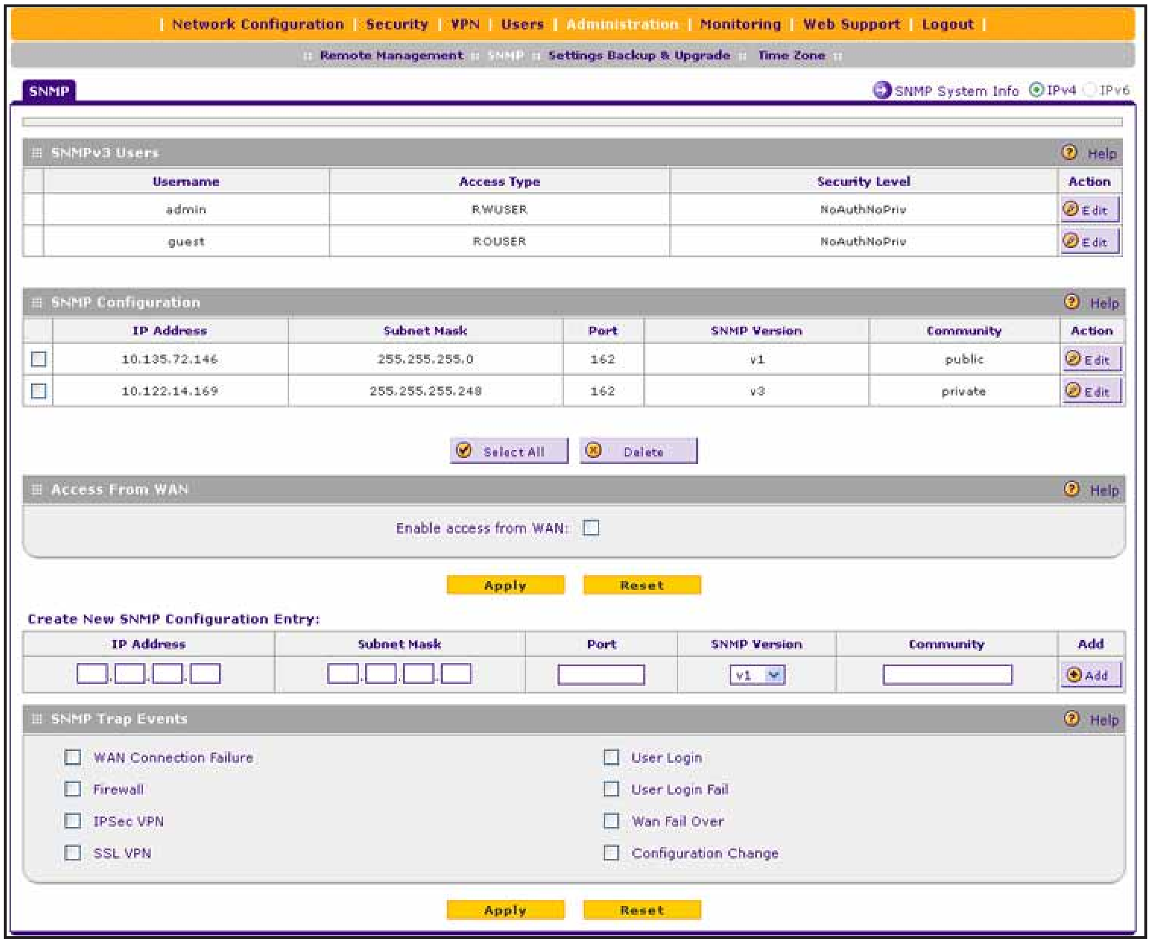
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Administration > SNMP**.

   The SNMP screen displays.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone ::
SNMP
SNMP System Info
● IPv4 ○ IPv6

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
□	10.135.72.146	255.255.255.0	162	v1	public	Edit
□	10.122.14.169	255.255.255.248	162	v3	private	Edit

Access From WAN

Enable access from WAN: □

Create New SNMP Configuration Entry:

IP Address	Subnet Mask	Port	SNMP Version	Community	Add
□.□.□.□	□.□.□.□		v1		Add

SNMP Trap Events

□ WAN Connection Failure

□ Firewall

□ IPSec VPN

□ SSL VPN

□ User Login

□ User Login Fail

□ Wan Fail Over

□ Configuration Change

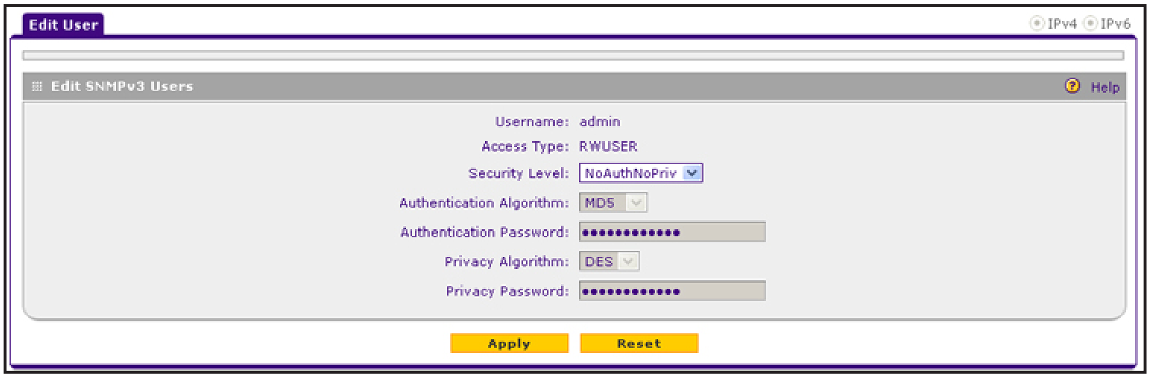
The SNMPv3 Users table lists the default SNMPv3 users that are preconfigured on the VPN firewall. The SNMPv3 Users table shows the following columns:

- **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.

7. In the SNMPv3 User table, to the right of the SNMPv3 user for which you want to change the settings, click the corresponding **Edit** button.

   The Edit User screen displays.



Username: admin
Access Type: RWUSER
Security Level: NoAuthNoPriv
Authentication Algorithm: MD5
Authentication Password: ●●●●●●●●●●●●
Privacy Algorithm: DES
Privacy Password: ●●●●●●●●●●●●

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

Setting	Description
Username	The default user name (admin or guest) for information only.
Access Type	The default access type (RWUSER or ROUSER) for information only.
Security Level	From the menu, 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** menu and enter an authentication password. • **AuthPriv**. Authentication and privacy are enabled. Make a selection from the **Authentication Algorithm** menu and enter an authentication password. In addition, make a selection from the **Privacy Algorithm** menu and enter a privacy password.
Authentication Algorithm	From the menu, 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.

Setting	Description
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 menu, 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.

9. Click the **Apply** button.

   Your settings are saved. If you changed the security level, the new level displays in the SNMPv3 User table on the SNMP screen.

Configure the SNMP System Information

The following procedure describes how to configure the SNMP system information.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

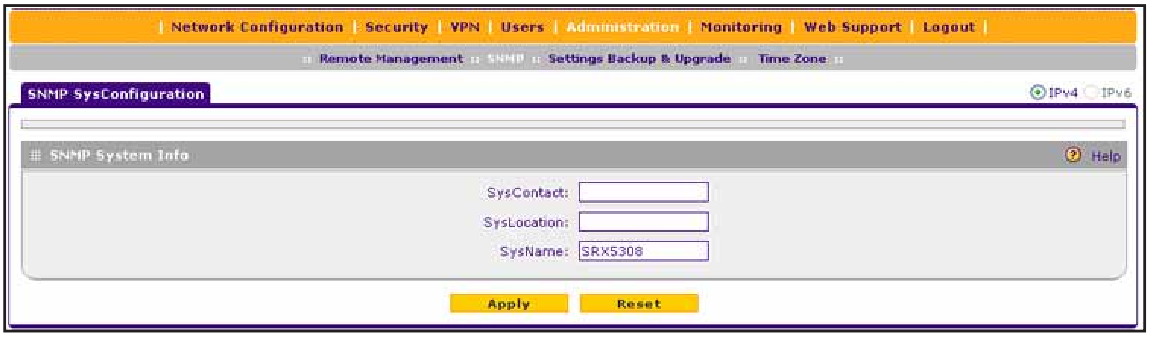
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Administration > SNMP**.

   The SNMP screen displays.
7. Click the **SNMP System Info** option arrow in the upper right.

   The SNMP SysConfiguration screen displays.


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: SRX5308

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

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 FVS336GV2.

9. Click the **Apply** button.

   Your settings are saved.

Manage the Configuration File

The configuration settings of the VPN firewall are stored in a configuration file on the VPN firewall. You can save (back up) the configuration file to a computer, retrieve (restore) it from the computer, or upgrade it 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 following sections provide information about managing the configuration file:

- *Back Up Settings*
- *Restore Settings*
- *Upgrade the Firmware*

Note: For information about how to return the configuration settings of theVPN firewall to the factory default settings, see *Revert to Factory Default Settings* on page 551.

Back Up Settings

The backup feature saves all VPN firewall settings to a file. Back up your settings periodically and store the backup file in a safe place.

> **Tip:** You can use a backup file to export all settings to another VPN firewall that has the same language and management software versions. Remember to change the IP address of the second VPN firewall before deploying it to eliminate IP address conflicts on the network.

➢ **To back up settings:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

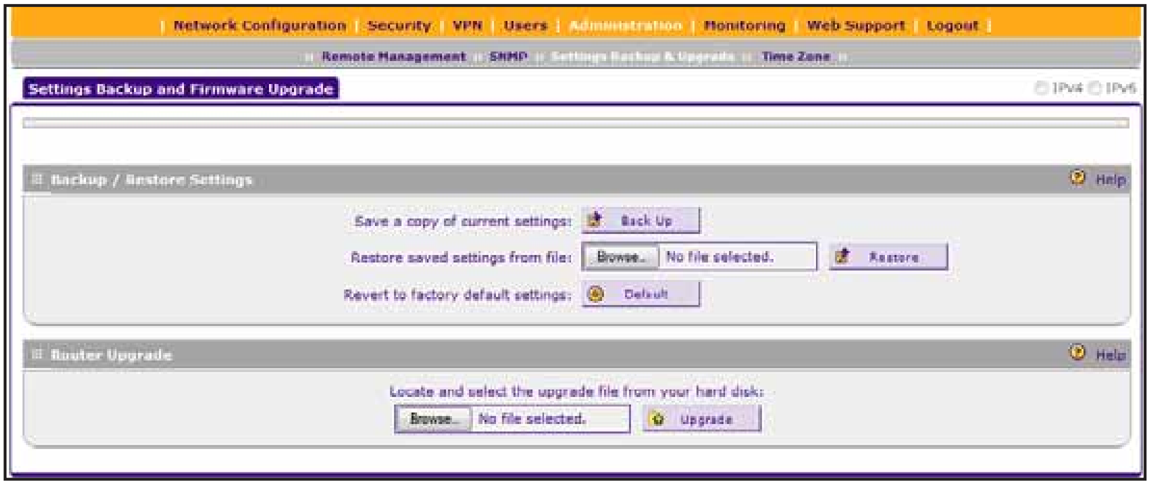
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Administration > Settings Backup & Upgrade**.

   The Settings Backup and Firmware Upgrade screen displays.


| 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

7. Click the **Back Up** button.

   A screen displays, showing the file name of the backup file (`FVS336GV2.cfg`).

8. Follow the directions of your browser to save the file.
9. Open the folder in which you saved the backup file and verify that it is saved successfully.

Restore Settings

The following procedure describes how to restore the configuration settings of the VPN firewall from a backup file.

WARNING:

Restore only settings that were backed up from the same software version. Restoring settings from a different software version can corrupt your backup file or the VPN firewall system software.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

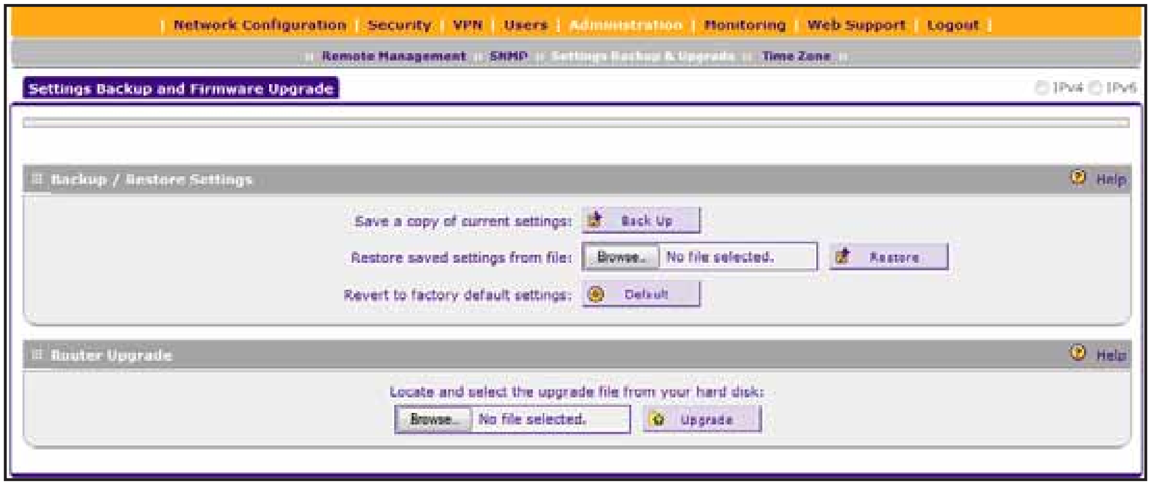
If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Administration > Settings Backup & Upgrade**.

   The Settings Backup and Firmware Upgrade screen displays.


| 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

7. To the left of the **Restore** button, click the **Browse** button.
8. Locate and select the previously saved backup file (by default, `FVS336GV2.cfg`).

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.

9. Click the **Restore** button.

   A warning message might display and you might need to confirm that you want to restore the configuration.

   The VPN firewall reboots. During the reboot process, the Settings Backup and Firmware Upgrade screen might remain visible or a status message with a counter might show the number of seconds left until the reboot process is complete. The reboot process takes about 160 seconds. (If you can see the unit: The reboot process is complete when the Test LED on the front panel goes off.)

Upgrade the Firmware

You can install a different version of the VPN firewall firmware. For information about how to view the current version of the firmware that the VPN firewall is running, see *Display an Overview of the VPN Firewall Addresses and Firmware Version* on page 582.

Note: In some cases, such as a major upgrade, it might be necessary to erase the configuration and manually reconfigure your VPN firewall after upgrading it. See the firmware release notes that NETGEAR makes available.

➤ **To download a firmware version and upgrade the firmware:**

1. Visit the NETGEAR website at *http://support.netgear.com*.
2. Navigate to the FVS336GV2 support page and click the **Downloads** tab.
3. Click the desired firmware version to reach the download page.

   Be sure to read the release notes on the download page before upgrading the VPN firewall's software.
4. On your computer, launch an Internet browser.
5. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

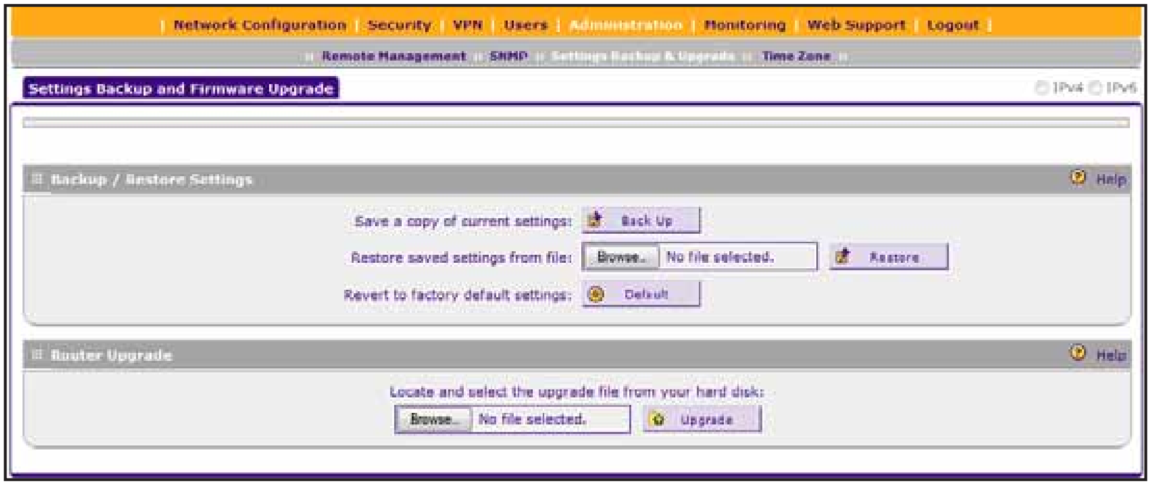
   The NETGEAR Configuration Manager Login screen displays.
6. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
7. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
8. Click the **Login** button.

   The Router Status screen displays.
9. Select **Administration > Settings Backup & Upgrade**.

   The Settings Backup and Firmware Upgrade screen displays.


| 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

10. To the left of the **Upgrade** button, click the **Browse** button.
11. Follow the directions of your browser to locate and select the downloaded firmware file.

WARNING:

After you have started the firmware installation process, do *not* interrupt the process. Do not try to go online, turn off the VPN firewall, or do anything else to the VPN firewall until the VPN firewall has fully rebooted.

12. Click the **Upload** button.

    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.

    (If you can see the unit: The reboot process is complete when the Test LED on the front panel goes off.)

13. When the reboot process is complete, log in to the VPN firewall again (see *Step 4* through *Step 8*).
14. To verify the firmware version, select **Monitoring**.

    The Router Status screen displays, showing the new firmware version in the System Info section.

Revert to Factory Default Settings

To restore the factory default settings you can either use the **Factory Defaults** reset button or the web management interface. If you have lost the administration password, you must use the **Factory Default** reset button.

WARNING:

When you press the hardware Factory Defaults reset button or use the web management interface to reset the VPN firewall to factory default settings, all custom 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 IP address is **192.168.1.1**.

The following sections provide information about reverting to factory default settings:

- *Revert to Factory Default Settings by Using the Factory Defaults Reset Button*
- *Revert to Factory Default Settings by Using the Web Management Interface*

Revert to Factory Default Settings by Using the Factory Defaults Reset Button

The following procedure describes how to use the Factory Defaults reset button on the back panel (see *Back Panel* on page 20) to reset the VPN firewall to the original factory defaults settings.

➢ **To use the Factory Defaults reset button to reset the VPN firewall to the original factory defaults settings:**

1. Using a sharp object, press and hold the **Factory Defaults** reset button on the back panel for about 8 seconds or until the Test LED lights and begins to blink.

   Note: Pressing the **Factory Defaults** reset button for a shorter period might cause the VPN firewall to reboot instead of resetting to factory defaults.

2. Release the **Factory Defaults** reset button.

   The VPN firewall reboots. The reboot process takes about 160 seconds. The reboot process is complete when the Test LED on the front panel turns off.

Revert to Factory Default Settings by Using the Web Management Interface

The following procedure describes how to use the web management interface to reset the VPN firewall to the original factory defaults settings.

➢ **To use the web management interface to reset the VPN firewall to factory defaults settings:**

1. On your computer, launch an Internet browser.

2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

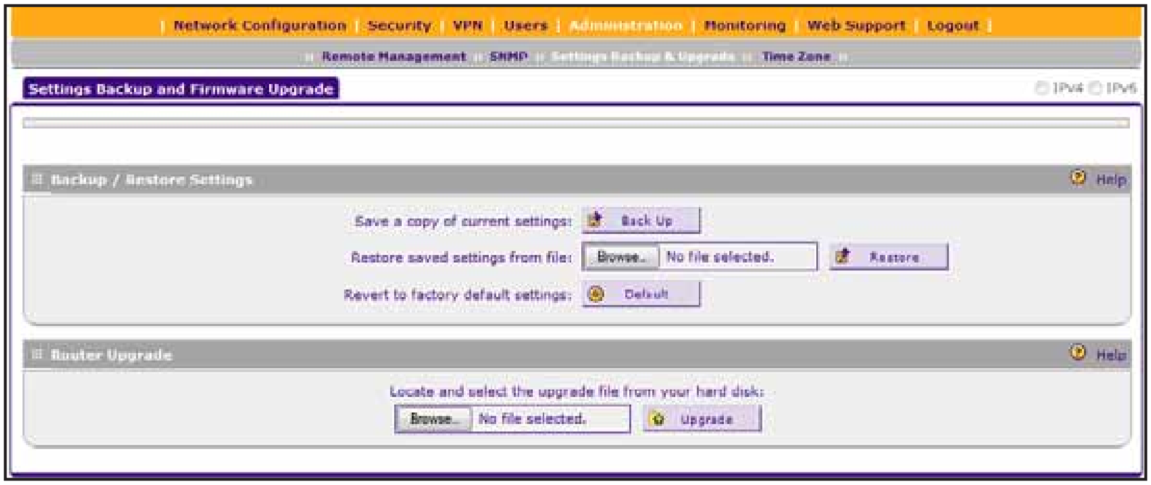
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Administration > Settings Backup & Upgrade**.

   The Settings Backup and Firmware Upgrade screen displays.


| 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

WARNING:

Once you start restoring the default 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 default settings are fully restored.

7. Click the **Default** button.

   The VPN firewall reboots. During the reboot process, the Settings Backup and Firmware Upgrade screen might remain visible or a status message with a counter might show the number of seconds left until the reboot process is complete. The reboot process takes about 160 seconds. (If you can see the unit: The reboot process is complete when the Test LED on the front panel turns off.)

Configure Date and Time Service

You can configure date, time, and NTP server designations. 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.

Note: If you select the default NTP servers or if you enter a custom server FQDN, the VPN firewall determines the IP address of the NTP server by performing a DNS lookup. Before the VPN firewall can perform this lookup, you must configure a DNS server address (see *Configure the IPv4 Internet Connection and WAN Settings* on page 30).

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

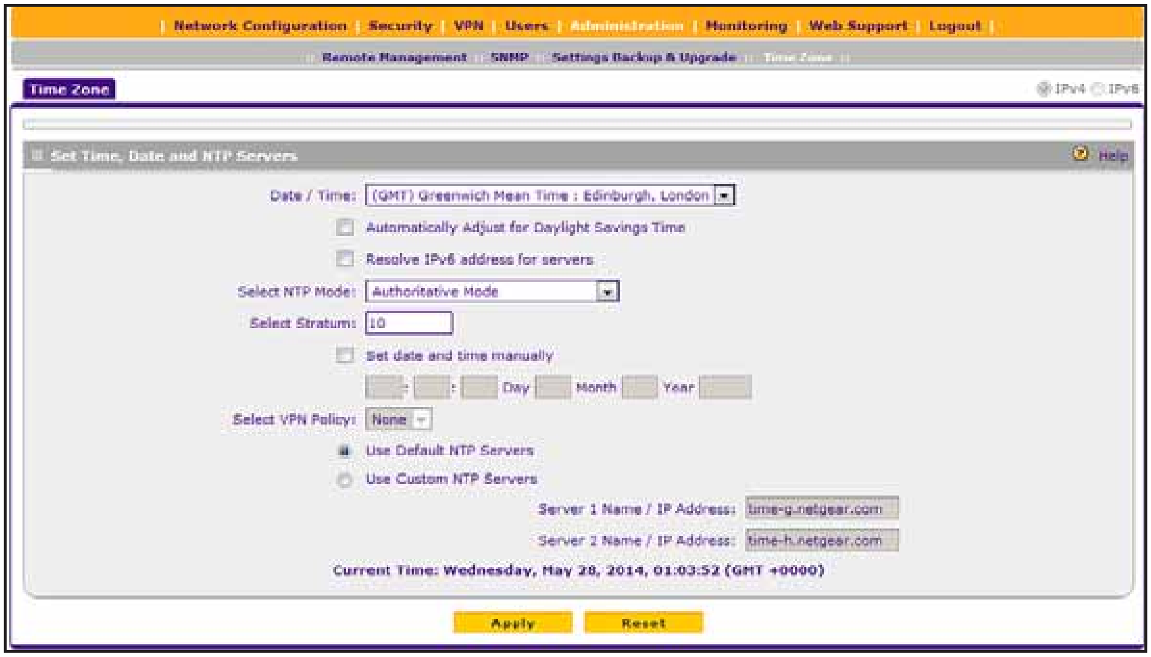
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Administration > Time Zone**.

   The Time Zone screen displays.


| 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) Greenwich Mean Time : Edinburgh, London

□ Automatically Adjust for Daylight Savings Time

□ Resolve IPv6 address for servers

Select NTP Mode: Authoritative Mode

Select Stratum: 10

□ Set date and time manually

: : Day Month Year

Select VPN Policy: None

● Use Default NTP Servers

○ Use Custom NTP Servers

Server 1 Name / IP Address: time-g.netgear.com

Server 2 Name / IP Address: time-h.netgear.com

Current Time: Wednesday, May 28, 2014, 01:03:52 (GMT +0000)

The bottom of the screen displays the current weekday, date, time, time zone, and year. In the example in the previous figure, the following displays: Current Time: Wednesday, May 28, 2014, 01:03:52 (GMT +0000).

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

Setting	Description
Date/Time	From the menu, 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 you live in a region that observes daylight savings time, select the **Automatically Adjust for Daylight Savings Time** check box. By default, the check box is cleared.
Resolve IPv6 address for servers	Select this check box to force the use of IPv6 addresses and FQDN (domain name) resolution in the **Server 1 Name / IP Address** and **Server 2 Name / IP Address** fields when you select the **Use Custom NTP Servers** radio button.

Setting	Description
Select NTP Mode	In all three NTP modes, the VPN firewall functions both as a client and a server. The VPN firewall synchronizes its clock with the specified NTP server or servers and provides time service to clients. From the menu, select the NTP mode: • **Authoritative Mode**. The VPN firewall synchronizes its clock with the specified NTP server or servers on the Internet. If external servers are unreachable, the VPN firewall’s RTC provides time service to clients. In authoritative mode, you can enter a stratum value and set the date and time manually. • **Sync to NTP Servers on Internet**. The VPN firewall synchronizes its clock with the specified NTP server or servers on the Internet. If external servers are unreachable, the VPN firewall does *not* use its RTC. • **Sync to NTP Servers on VPN**. The VPN firewall synchronizes its clock with the specified NTP server on the VPN. If the server is unreachable, the VPN firewall does *not* use its RTC. You must select a VPN policy that enables the VPN firewall to contact the NTP server on the VPN.
Select Stratum	In authoritative mode, enter a stratum value, which indicates the distance from a reference clock. The default value is 10, which specifies an unsynchronized local clock and causes NTP to use the VPN firewall’s RTC when the specified NTP server is not available.
Set date and time manually	This is an optional setting that is available in authoritative mode. Select the **Set date and time manually** check box to unmask the time (hour, minute, second), **Day**, **Month**, and **Year** fields. Enter the date and time.
Select VPN Policy	When the VPN firewall is configured to synchronize to an NTP server on the VPN, select the VPN policy from the menu. For information about configuring VPN policies, see *Manage VPN Policies* on page 378.
NTP Servers (default or custom)	Select an 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 Name / IP Address** or **Server 2 Name / IP Address** field blank, both fields are set to the default NETGEAR NTP servers. **Note:** A list of public NTP servers is available at *http://support.ntp.org/bin/view/Servers/WebHome*.
NTP Servers (custom)	In the **Server 1 Name / IP Address** field, enter the IP address or host name of the primary NTP server. In the **Server 2 Name / IP Address** field, enter the IP address or host name of the backup NTP server.

8. Click the **Apply** button.

   Your settings are saved.

12. Monitor System Access and Performance

12

This chapter describes the system-monitoring features of the VPN firewall. You can be alerted to important events such WAN traffic limits reached, login failures, and attacks. You can also view status information about the firewall, WAN ports, LAN ports, active VPN users and tunnels, and more. In addition, the diagnostics utilities are described. The chapter contains the following sections:

- *Configure and Enable the WAN IPv4 Traffic Meter*
- *Manage the LAN IPv4 Traffic Meter*
- *Manage Logging, Alerts, and Event Notifications*
- *View the Status and Statistics of the VPN Firewall and Its Traffic*

Note: All log and report functions and some diagnostic functions require that you configure the email notification server. See *Manage Logging, Alerts, and Event Notifications* on page 567.

Configure and Enable the WAN IPv4 Traffic Meter

If your ISP charges by traffic volume over a given period, or if you want to study traffic types over a period, you can activate the traffic meter for IPV4 traffic on a WAN interface.

For information about displaying the Internet traffic that is measured by the WAN IPv4 traffic meter, see *Display Internet Traffic by Type of Traffic*.

Note: When you enable the WAN IPv4 traffic meter, the performance of the VPN firewall might be affected slightly.

➢ **To configure and monitor traffic limits for a WAN IPv4 interface:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

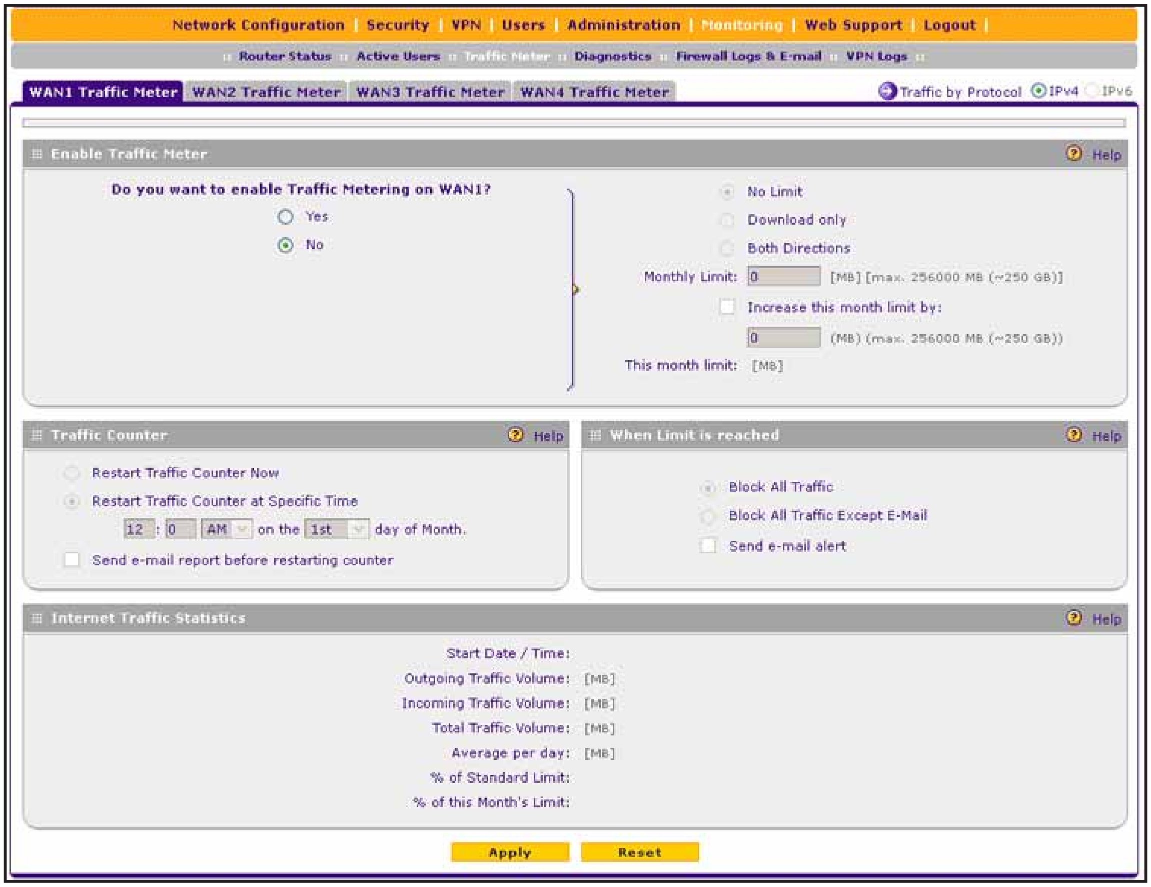
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Monitoring > Traffic Meter**.

   The WAN Traffic Meter tabs display, with the WAN1 Traffic Meter screen in view.

   Note: The Internet Traffic Statistics section in the lower part displays statistics on Internet traffic through the WAN port. If you did not enable the traffic meter, these statistics are not available.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs
WAN1 Traffic Meter
WAN2 Traffic Meter
WAN3 Traffic Meter
WAN4 Traffic Meter
Traffic by Protocol
Help
Apply
Reset

● IPv4 ○ IPv6

Enable Traffic Meter

Do you want to enable Traffic Metering on WAN1?

○ 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 1st 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:

7. If you want to configure the settings for the WAN2 interface, click the **WAN2 Traffic Meter** tab.

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

Setting	Description
Enable Traffic Meter	
In the Do you want to enable Traffic Metering on WAN1? section, select a radio button: • **Yes**. Traffic metering is enabled and the traffic meter records the volume of Internet traffic passing through the WAN interface. Complete the fields on the right (see explanations later in this table). • **No**. Traffic metering is disabled. This is the default setting.	
Select a radio button to specify if or how the VPN firewall applies restrictions when the traffic limit is reached: • **No Limit**. No restrictions are applied when the traffic limit is reached. • **Download only**. Restrictions are applied to incoming traffic when the traffic limit is reached. 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.

Setting	Description
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 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 the meridiem and the day of the month from the menus.
Send e-mail report before restarting counter	An email report is sent immediately before the counter restarts. Ensure that emailing of logs is enabled (see *Enable and Schedule Emailing of Logs* on page 569).
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 (see *Enable and Schedule Emailing of Logs* on page 569).

9. Click the **Apply** button.

   Your settings are saved.

Manage the LAN IPv4 Traffic Meter

The following sections provide information about managing the LAN IPv4 traffic meter:

- *Configure and Enable the Traffic Meter for a LAN IPv4 Address Account*
- *View Traffic Meter Statistics for a LAN Account*
- *Change the Traffic Meter for a LAN Account*
- *Remove One or More LAN Traffic Meter Accounts*

Configure and Enable the Traffic Meter for a LAN IPv4 Address Account

If your ISP charges by traffic volume over a period and you must charge the costs to individual accounts, or if you want to study the traffic volume that is requested or sent over LAN IPv4 addresses over a period, add and configure individual LAN IPv4 address accounts (profiles) for the LAN traffic meter.

Note: When you add a profile for the LAN traffic meter, the performance of the VPN firewall might be affected slightly.

➢ **To add and configure a LAN IPv4 address account (profile) for the LAN traffic meter:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

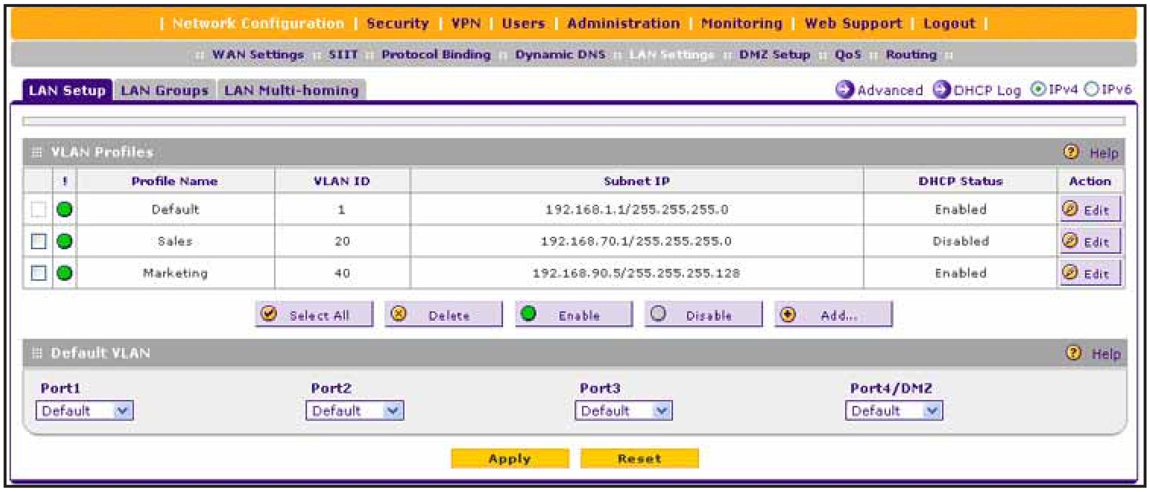
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > LAN Settings**.

   The LAN submenu tabs display with the LAN Setup screen in view.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: 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	192.168.1.1/255.255.255.0	Enabled	Edit
□	●	Sales	20	192.168.70.1/255.255.255.0	Disabled	Edit
□	●	Marketing	40	192.168.90.5/255.255.255.128	Enabled	Edit

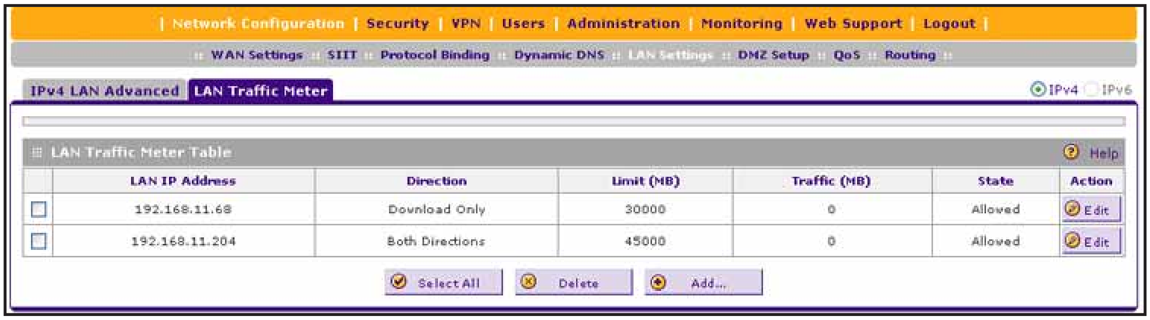
Port1	Port2	Port3	Port4/DMZ
Default	Default	Default	Default

7. Click the **Advanced** option arrow in the upper right.

   The IPv4 LAN Advanced screen displays.

8. Click the **LAN Traffic Meter** tab.

   The LAN Traffic Meter screen displays. The following figure shows some examples in the LAN Traffic Meter Table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
IPv4 LAN Advanced
LAN Traffic Meter
IPv4
IPv6
LAN Traffic Meter Table
Help
Select All
Delete
Add...

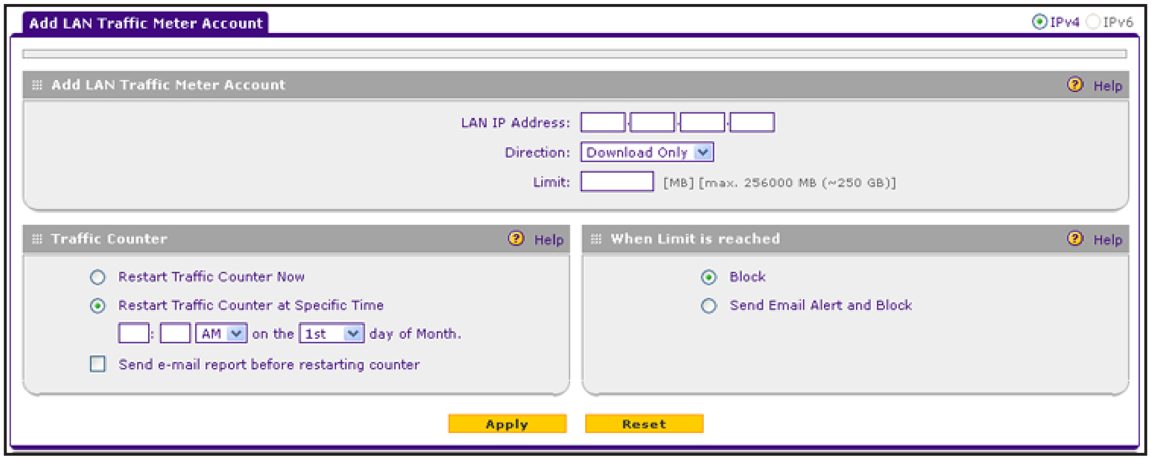
	LAN IP Address	Direction	Limit (MB)	Traffic (MB)	State	Action
□	192.168.11.68	Download Only	30000	0	Allowed	Edit
□	192.168.11.204	Both Directions	45000	0	Allowed	Edit

The LAN Traffic Meter Table shows the following columns, which are described in the table that follows the next figure:

- **LAN IP Address**. The LAN IP address that is subject to the traffic meter.
- **Direction**. The direction for which traffic is measured.
- **Limit (MB)**. The traffic limit in MB.
- **Traffic (MB)**. The traffic usage in MB.
- **State**. The state that indicates whether traffic to and from the IP address is allowed or blocked.
- **Action**. The **Edit** button provides access to the Edit LAN Traffic Meter screen for the corresponding IP address.

9. On the LAN Traffic Meter screen, click the **Add** button.

   The Add LAN Traffic Meter screen displays.



Add LAN Traffic Meter Account ● IPv4 ○ IPv6

Add LAN Traffic Meter Account

LAN IP Address: [ ] . [ ] . [ ] . [ ]

Direction: Download Only

Limit: [ ] [MB] [max. 256000 MB (~250 GB)]

Traffic Counter

○ Restart Traffic Counter Now

● Restart Traffic Counter at Specific Time

[ ] : [ ] AM on the 1st day of Month.

□ Send e-mail report before restarting counter

When Limit is reached

● Block

○ Send Email Alert and Block

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

Setting	Description
Add LAN Traffic Meter Account	
LAN IP Address	The LAN IP address for the account.
Direction	From the **Direction** menu, select the direction of the traffic that is measured: • **Inbound traffic**. Restrictions are applied to incoming traffic when the traffic limit is reached. • **Both directions**. Restrictions are applied to both incoming and outgoing traffic when the traffic limit is reached.
Limit	Enter the monthly traffic volume limit in MB. The default setting is 0 MB. The maximum limit that you can enter is 256,000 MB.
Traffic Counter	
Restart Traffic Counter	Select when the traffic counter restarts: • **Restart Traffic Counter Now**. The traffic counter restarts immediately after you click the **Apply** button. • **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 the meridiem and day of the month from the menu.
Send e-mail report before restarting counter	An email report is sent immediately before the counter restarts. Ensure that emailing of logs is enabled (see *Enable and Schedule Emailing of Logs* on page 569).
When Limit is reached	
Block Traffic	Select what action the VPN firewall performs when the traffic limit is reached: • **Block**. All incoming and outgoing Internet and email traffic is blocked. • **Send Email Alert and Block**. An email alert is sent when all incoming and outgoing Internet and email traffic is blocked. Ensure that emailing of logs is enabled (see *Enable and Schedule Emailing of Logs* on page 569).

11. Click the **Apply** button.

Your settings are saved. The new account is added to the LAN Traffic Meter Table on the LAN Traffic Meter screen.

View Traffic Meter Statistics for a LAN Account

The following procedure describes how to view the traffic meter statistics for a LAN IPv4 address account.

➢ **To view the traffic meter statistics for a LAN IPv4 address account:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

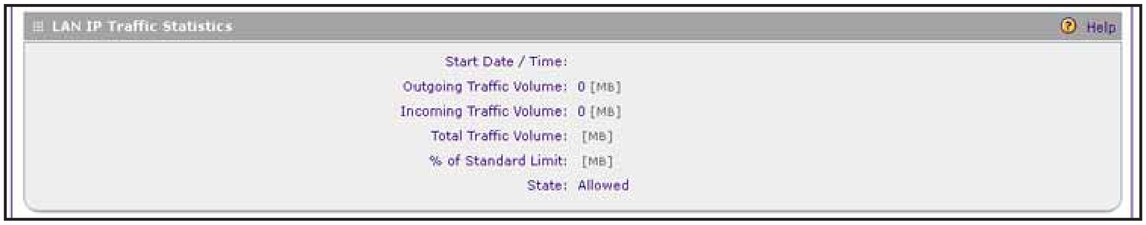
   The Router Status screen displays.
6. Select **Network Configuration > LAN Settings**.

   The LAN submenu tabs display with the LAN Setup screen in view.
7. Click the **Advanced** option arrow in the upper right.

   The IPv4 LAN Advanced screen displays.
8. Click the **LAN Traffic Meter** tab.

   The LAN Traffic Meter screen displays.
9. In the LAN Traffic Meter Table, click the **Edit** button for the account for which you want to view the statistics.

   The Edit LAN Traffic Meter Account screen displays that traffic statistics.



Start Date / Time:
Outgoing Traffic Volume: 0 [MB]
Incoming Traffic Volume: 0 [MB]
Total Traffic Volume: [MB]
% of Standard Limit: [MB]
State: Allowed

Change the Traffic Meter for a LAN Account

The following procedure describes how to change the traffic meter for an existing LAN IPv4 address account.

➢ **To change the traffic meter for an existing LAN IPv4 address account:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > LAN Settings**.

   The LAN submenu tabs display with the LAN Setup screen in view.
7. Click the **Advanced** option arrow in the upper right.

   The IPv4 LAN Advanced screen displays.
8. Click the **LAN Traffic Meter** tab.

   The LAN Traffic Meter screen displays.
9. In the LAN Traffic Meter Table, click the **Edit** button for the account that you want to change.

   The Edit LAN Traffic Meter Account screen displays.
10. Change the settings.

For more information about the settings, see *Configure and Enable the Traffic Meter for a LAN IPv4 Address Account* on page 561.

11. Click the **Apply** button.

    Your settings are saved. The modified account displays in the LAN Traffic Meter Table on the LAN Traffic Meter screen.

Remove One or More LAN Traffic Meter Accounts

The following procedure describes how to remove one or more LAN IPv4 address accounts that you no longer need for the LAN traffic meter.

➢ **To remove one or more LAN IPv4 address accounts:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > LAN Settings**.

   The LAN submenu tabs display, with the LAN Setup screen in view.
7. Click the **Advanced** option arrow in the upper right.

   The IPv4 LAN Advanced screen displays.
8. Click the **LAN Traffic Meter** tab.

   The LAN Traffic Meter screen displays.
9. In the LAN Traffic Meter Table, select the check box to the left of the accounts that you want to remove or click the **Select All** button to select all accounts.
10. Click the **Delete** button.

    The selected accounts are removed from the LAN Traffic Meter Table.

Manage Logging, Alerts, and Event Notifications

The following sections provide information about managing logging, alerts, and event notifications:

- *Logging, Alert, and Event Notification*
- *Configure and Activate Logs*
- *Enable and Schedule Emailing of Logs*
- *Enable the Syslogs*
- *View the Routing Logs, System Logs, and Other Event Logs*
- *View the DNS Logs*
- *View the NTP Logs*
- *Send Syslogs over a VPN Tunnel Between Sites*

Note: This release does not support sending the NTP and DNS logs to the syslog server or the mail server.

Logging, Alert, and Event Notification

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.

Note: Enabling routing and other event logs might generate a significant volume of log messages. NETGEAR recommends that you enable firewall logs for debugging purposes only.

Configure and Activate Logs

➢ **To configure and activate logs:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

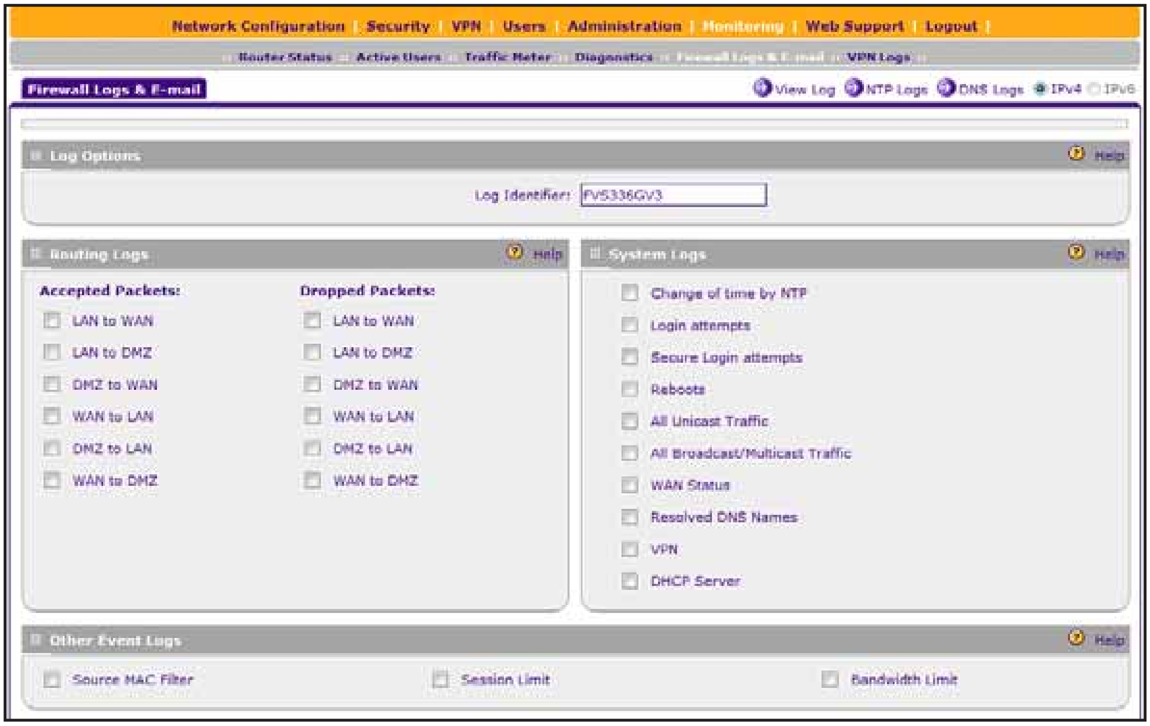
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Monitoring > Firewall Logs & E-mail**.

   The Firewall Logs & E-mail screen displays. The following figure shows the top section only.


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
NTP Logs
DNS Logs
Help

● IPv4 ○ IPv6

Log Options

Log Identifier: FVS336GV3

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

Other Event Logs

□ Source MAC Filter □ Session Limit □ Bandwidth Limit

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

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 FVS336GV2.
Routing Logs	
In the Accepted Packets and Dropped Packets columns, select which traffic is logged.	

Setting	Description
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 you press the **Factory Defaults** reset button.) • **All Unicast Traffic**. Logs all incoming unicast packets. • **All Broadcast/Multicast Traffic**. Logs all incoming broadcast and multicast packets. • **WAN Status**. Logs WAN link status–related events. • **Resolved DNS Names**. Logs all resolved DNS names. • **VPN**. Logs all VPN negotiation messages. • **DHCP Server**. Logs all DHCP server messages.	
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 is exceeded.
Bandwidth Limit	Select this check box to log packets that are dropped because the bandwidth limit is exceeded.

8. Click the **Apply** button.

   Your settings are saved.

Enable and Schedule Emailing of Logs

Although you can view the logs onscreen, the VPN firewall provides the convenience of emailing the logs to a specific email address.

➢ **To enable and schedule emailing of logs:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

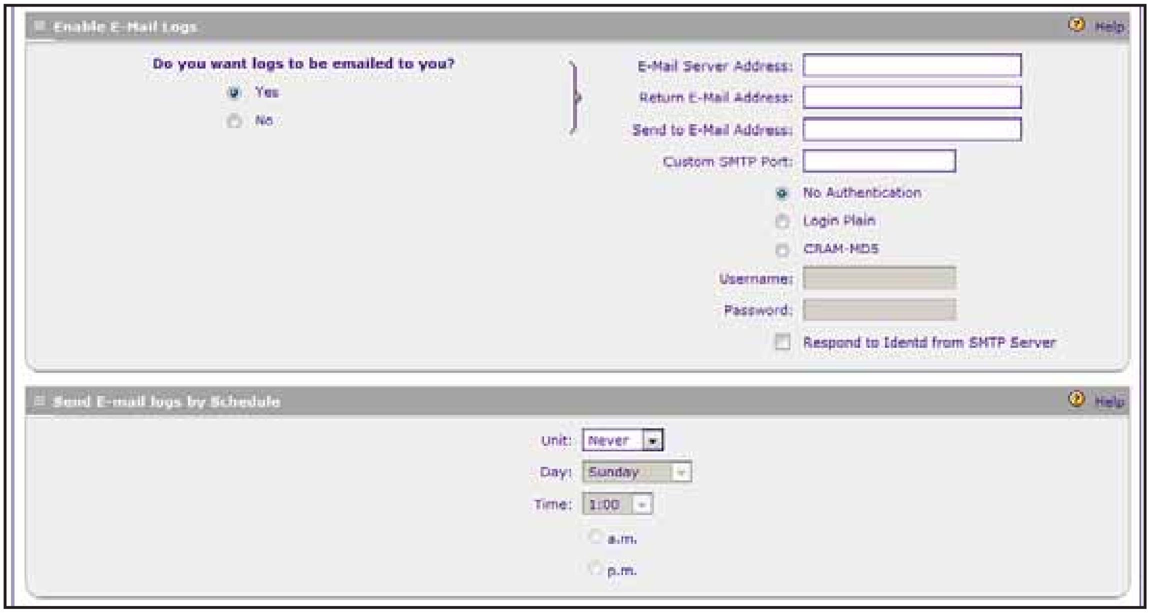
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Monitoring > Firewall Logs & E-mail**.

   The Firewall Logs & E-mail screen displays. The following figure shows the middle section only.



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:
Password:
□ Respond to Identd from SMTP Server

Send E-mail logs by Schedule

Unit: Never
Day: Sunday
Time: 1:00
○ a.m.
○ p.m.

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

Setting	Description
Enable E-mail Logs	
In the Do you want logs to be emailed to you? section, select the **Yes** radio button to enable the VPN firewall to email logs to a specified email address. Complete the fields on the right. By default, the **No** radio button is selected to prevent the logs from being emailed.	
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.

Setting	Description
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	The port number of the SMTP server for the outgoing email.
Select the SMTP server authentication for the outgoing email: • **No Authentication**. The SMTP server does not require authentication. • **Login Plain**. The SMTP server requires authentication with regular login. Specify the user name and password to be used for authentication. • **CRAM-MD5**. The SMTP server requires authentication with CRAM-MD5 login. Specify the user name and password to be used for authentication.	
Username	The user name for SMTP server authentication.
Password	The password for SMTP server authentication.
Respond to Identd from SMTP Server	To respond to Ident protocol messages, select the **Respond to Identd from SMTP Server** check box. The Ident protocol is a relatively weak scheme to verify the sender of an email. (A common daemon program for providing the Ident service is Identd.)
Send e-mail logs by Schedule	
Unit	Enter a schedule for sending the logs. From the **Unit** menu, select one of the following: • **Hourly**. The VPN firewall sends logs every hour. • **Daily**. The VPN firewall sends logs daily. Specify the time and meridiem. • **Weekly**. The VPN firewall sends logs weekly. Specify the day, time, and meridiem. By default, the menu selection is **Never** and the VPN firewall does not send logs.
Day	From the **Day** menu, select the day on which the VPN firewall sends logs.
Time	From the **Time** menu, select the hour on which the VPN firewall sends logs and select either the **a.m.** or **p.m.** radio button.

8. Click the **Apply** button.

   Your settings are saved.

Enable the Syslogs

If you have a syslog server, you can enable the syslog of the VPN firewall. For information about sending syslogs from one site to another over a gateway-to-gateway VPN tunnel, see *Send Syslogs over a VPN Tunnel Between Sites* on page 576.

➤ **To enable the syslogs:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

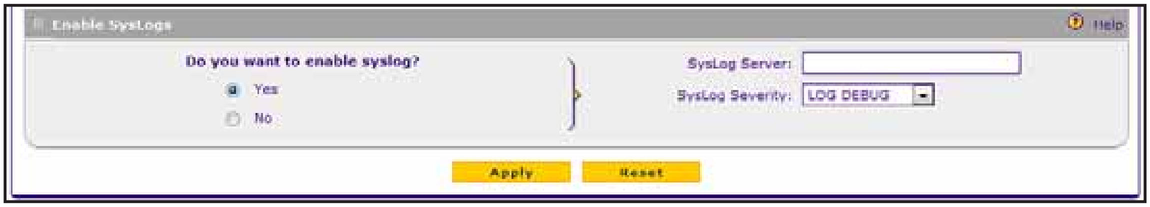
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Monitoring > Firewall Logs & E-mail**.

   The Firewall Logs & E-mail screen displays. The following figure shows the bottom section only.



Enable SysLogs

Do you want to enable syslog?
● Yes
○ No

SysLog Server:
SysLog Severity: LOG DEBUG

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

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 on the right. To prevent the logs from being sent, select the **No** radio button, which is the default setting.	

Setting	Description
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 a syslog severity from the menu: • **LOG DEBUG**. Debug-level messages. • **LOG INFO**. Informational messages. • **LOG NOTICE**. Normal but significant conditions. • **LOG WARNING**. Warning conditions. • **LOG ERROR**. Error conditions. • **LOG CRITICAL**. Critical conditions. • **LOG ALERT**. An action must be taken immediately. • **LOG EMERG**. The VPN firewall is unusable.

8. Click the **Apply** button.

   Your settings are saved.

View the Routing Logs, System Logs, and Other Event Logs

You can view the routing logs, system logs, and other event logs onscreen. You can manually send the logs to an email address and clear the logs.

➢ **To view the routing logs, system logs, and other event logs and send the logs to an email address or clear the logs:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

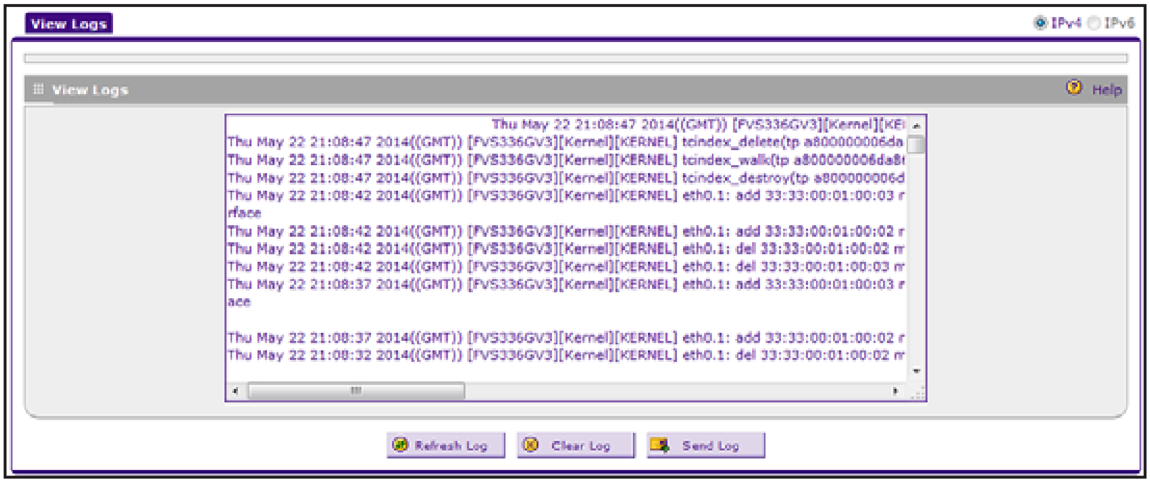
   The Router Status screen displays.

6. Select **Monitoring > Firewall Logs & E-mail**.

   The Firewall Logs & E-mail screen displays.

7. Click the **View Log** option arrow in the upper right.

   The View Log screen displays the logs.



```
                          Thu May 22 21:08:47 2014((GMT)) [FVS336GV3][Kernel][KE
Thu May 22 21:08:47 2014((GMT)) [FVS336GV3][Kernel][KERNEL] tcindex_delete(tp a800000006da
Thu May 22 21:08:47 2014((GMT)) [FVS336GV3][Kernel][KERNEL] tcindex_walk(tp a800000006da8
Thu May 22 21:08:47 2014((GMT)) [FVS336GV3][Kernel][KERNEL] tcindex_destroy(tp a800000006d
Thu May 22 21:08:42 2014((GMT)) [FVS336GV3][Kernel][KERNEL] eth0.1: add 33:33:00:01:00:03 r
rface
Thu May 22 21:08:42 2014((GMT)) [FVS336GV3][Kernel][KERNEL] eth0.1: add 33:33:00:01:00:02 r
Thu May 22 21:08:42 2014((GMT)) [FVS336GV3][Kernel][KERNEL] eth0.1: del 33:33:00:01:00:02 m
Thu May 22 21:08:42 2014((GMT)) [FVS336GV3][Kernel][KERNEL] eth0.1: del 33:33:00:01:00:03 m
Thu May 22 21:08:37 2014((GMT)) [FVS336GV3][Kernel][KERNEL] eth0.1: add 33:33:00:01:00:03 r
ace

Thu May 22 21:08:37 2014((GMT)) [FVS336GV3][Kernel][KERNEL] eth0.1: add 33:33:00:01:00:02 r
Thu May 22 21:08:32 2014((GMT)) [FVS336GV3][Kernel][KERNEL] eth0.1: del 33:33:00:01:00:02 m
```

8. To send the logs to the email address that is specified on the Firewall Logs & E-mail screen, click the **Send Log** button.
9. To clear the logs, click the **Clear Log** button.
10. To refresh the information onscreen, click the **Refresh Log** button.

View the DNS Logs

The VPN firewall logs a message when a DNS address is resolved for a LAN host. You can view the DNS logs onscreen.

➢ **To view the DNS logs or clear the DNS logs:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

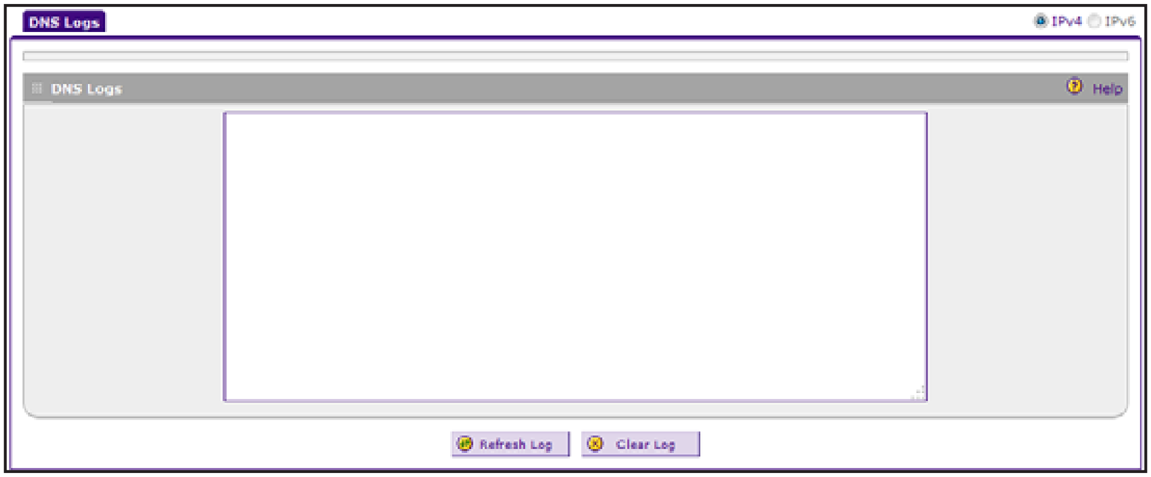
   The Router Status screen displays.

6. Select **Monitoring > Firewall Logs & E-mail**.

   The Firewall Logs & E-mail screen displays.

7. Click the **DNS Logs** option arrow in the upper right.

   The DNS Logs screen displays.



8. To clear the logs, click the **Clear Log** button.
9. To refresh the information onscreen, click the **Refresh Log** button.

View the NTP Logs

The VPN firewall logs a message when an NTP event occurs. You can view the NTP logs onscreen.

➤ **To view the NTP logs or clear the NTP logs:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

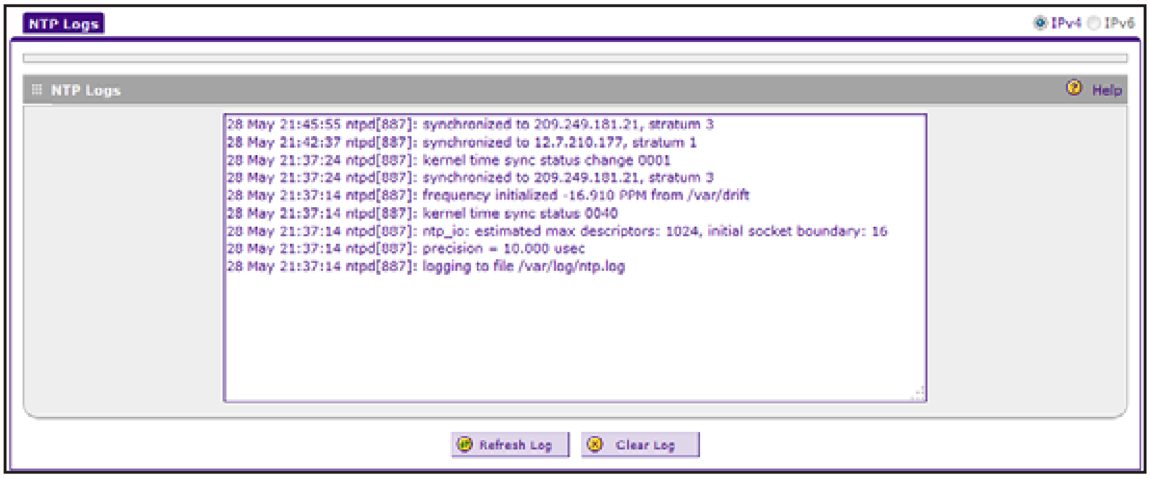
   The Router Status screen displays.

6. Select **Monitoring > Firewall Logs & E-mail**.

   The Firewall Logs & E-mail screen displays.

7. Click the **NTP Logs** option arrow in the upper right.

   The NTP Logs screen displays.



```
28 May 21:45:55 ntpd[887]: synchronized to 209.249.181.21, stratum 3
28 May 21:42:37 ntpd[887]: synchronized to 12.7.210.177, stratum 1
28 May 21:37:24 ntpd[887]: kernel time sync status change 0001
28 May 21:37:24 ntpd[887]: synchronized to 209.249.181.21, stratum 3
28 May 21:37:14 ntpd[887]: frequency initialized -16.910 PPM from /var/drift
28 May 21:37:14 ntpd[887]: kernel time sync status 0040
28 May 21:37:14 ntpd[887]: ntp_io: estimated max descriptors: 1024, initial socket boundary: 16
28 May 21:37:14 ntpd[887]: precision = 10.000 usec
28 May 21:37:14 ntpd[887]: logging to file /var/log/ntp.log
```

8. To clear the logs, click the **Clear Log** button.
9. To refresh the information onscreen, click the **Refresh Log** button.

Send Syslogs over a VPN Tunnel Between Sites

This section describes how to send syslogs from one site to another over a gateway-to-gateway VPN tunnel.

The high-level steps that describe the actions that you must take to send syslogs from one site to another over a gateway-to-gateway VPN tunnel, that is, a VPN tunnel between two VPN firewalls:

1. At Site 1, set up a syslog server that is connected to Gateway 1.
2. At Site 1, set up a VPN tunnel between Gateway 1 and Gateway 2 at Site 2 (see *Configure the VPN Tunnel on Gateway 1 at Site 1* on page 577).
3. At Site 1, change the remote IP address in the VPN policy on Gateway 1 to the WAN IP address of Gateway 2 at Site 2 (see *Change the Remote IP Address in the VPN Policy on Gateway 1 at Site 1* on page 578).

4. At Site 2, set up a VPN tunnel between Gateway 2 and Gateway 1 at Site 1 (see *Configure the VPN Tunnel on Gateway 2 at Site 2* on page 579)
5. At Site 2, change the local IP address in the VPN policy on Gateway 2 to the WAN IP address of Gateway 2 (see *Change the Remote IP Address in the VPN Policy on Gateway 2 at Site 2* on page 580).
6. At Site 2, specify that Gateway 2 must send the syslogs to the syslog server at Site 1 (see *On the Gateway at Site 2, Specify the Syslog Server on Site 1* on page 581).

The sections listed describe Steps 2 through 6, using the topology that is described in the following table.

Type of Address	Gateway 1 at Site 1	Gateway 2 at Site 2
WAN IP address	10.0.0.1	10.0.0.2
LAN IP address	192.168.10.0	192.168.20.0
LAN subnet mask	255.255.255.0	255.255.255.0
LAN IP address syslog server	192.168.10.2	Not applicable

After you have completed the steps, the VPN tunnel is established automatically and the syslogs are sent to the syslog server at Site 1. For information about verifying the VPN connection, see *View the VPN Connection Status, L2TP Users, and PPTP Users* on page 592.

Configure the VPN Tunnel on Gateway 1 at Site 1

The following procedure describes how to set up a VPN tunnel at Site 1 between Gateway 1 at Site 1 and Gateway 2 at Site 2.

➢ **To create a gateway-to-gateway VPN tunnel on Gateway 1 at Site 1 to Gateway 2 at Site 2, using the IPSec VPN wizard:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter **10.0.0.1** if you log in from the WAN or enter **192.168.10.0** if you log in from the LAN.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

The Router Status screen displays.

6. Select **VPN > IPSec VPN > VPN Wizard**.

   The VPN Wizard screen displays.

7. 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
8. Click the **Apply** button.

   Your settings are saved.

Change the Remote IP Address in the VPN Policy on Gateway 1 at Site 1

The following procedure describes how to change the remote IP address in the VPN policy on Gateway 1 at Site 1 to the WAN IP address of Gateway 2 at Site 2.

➢ **To change the remote IP address in the VPN policy on Gateway 1 at Site 1:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter **10.0.0.1** if you log in from the WAN or enter **192.168.10.0** if you log in from the LAN.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

   Select **VPN > IPSec VPN > VPN Policies**.

   The VPN Policy screen displays.

6. Next to the policy name for the Gateway 1–to–Gateway 2 autopolicy, click the **Edit** button.

   The Edit VPN Policy screen displays.

7. In the General section, clear the **Enable NetBIOS** check box.
8. In the Traffic Selector section, make the following changes:
   - From the **Remote IP** menu, select **Single**.
   - In the **Start IP** field, type **10.0.0.2.**

     This IP address is the WAN IP address of Gateway 2.
9. Click the **Apply** button.

   Your settings are saved.

Configure the VPN Tunnel on Gateway 2 at Site 2

The following procedure describes how you can set up a VPN tunnel at Site 2 between Gateway 2 at Site 2 and Gateway 1 at Site 1.

➢ **To create a gateway-to-gateway VPN tunnel on Gateway 2 at Site 2 to Gateway 1 at Site 1, using the IPSec VPN wizard:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter **10.0.0.2** if you log in from the WAN or enter **192.168.20.0** if you log in from the LAN.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > IPSec VPN > VPN Wizard**.

   The VPN Wizard screen displays.
7. 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

8. Click the **Apply** button.

   Your settings are saved.

Change the Remote IP Address in the VPN Policy on Gateway 2 at Site 2

The following procedure describes how to change the local IP address in the VPN policy on Gateway 2 at Site 2 to the WAN IP address of the same Gateway 2.

➢ **To change the local IP address in the VPN policy on Gateway 2 at Site 2:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter **10.0.0.2** if you log in from the WAN or enter **192.168.20.0** if you log in from the LAN.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **VPN > IPSec VPN > VPN Policies**.

   The VPN Policy screen displays.
7. Next to the policy name for the Gateway 2–to–Gateway 1 autopolicy, click the **Edit** button.

   The Edit VPN Policy screen displays.
8. In the General section, clear the **Enable NetBIOS** check box.
9. In the Traffic Selector section, make the following changes:
   - From the **Local IP** menu, select **Single**.
   - In the **Start IP** fields, type **10.0.0.2**.

     This IP address is the WAN IP address of Gateway 2.
10. Click the **Apply** button.

    Your settings are saved.

On the Gateway at Site 2, Specify the Syslog Server on Site 1

The following procedure describes how to specify that Gateway 2 at Site 2 must send the syslogs to the syslog server that is connected to Gateway 1 at Site 1.

➢ **To specify that Gateway 2 at Site 2 must send the syslogs to the syslog server that is connected to Gateway 1 on Site 1:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter **10.0.0.2** if you log in from the WAN or enter **192.168.20.0** if you log in from the LAN.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Monitoring > Firewall Logs & E-mail**.

   The Firewall Logs & E-mail screen displays.
7. In the Enable SysLogs section, select the **Yes** radio button.
8. In the **SysLog Server** field, enter **192.168.10.2**.

   This IP address is the LAN IP address of the syslog server at Site 1.
9. From the **SysLog Severity** menu, select a severity level.

   For more information severity levels, see *Enable the Syslogs* on page 571.
10. Click the **Apply** button.

    Your settings are saved.

View the Status and Statistics of the VPN Firewall and Its Traffic

The following sections provide information about the status and statistics of the VPN firewall and its traffic:

- *View the System Status*

- *View the VPN Connection Status, L2TP Users, and PPTP Users*
- *View the VPN Logs*
- *View the Port Triggering Status*
- *View the WAN Port Status and Terminate or Establish the Internet Connection*
- *Display Internet Traffic by Type of Traffic*
- *View the Attached Devices*
- *View the DHCP Log*

View the System Status

You can view 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
- IPv6 tunnels

The following sections provide information about viewing the system status:

- *Display an Overview of the VPN Firewall Addresses and Firmware Version*
- *View the Traffic Statistics for the Interfaces and Change the Polling Interval*
- *View Detailed Status Information About the VPN Firewall*
- *View the VLAN Status*
- *View the IPv6 Tunnel Status*

Display an Overview of the VPN Firewall Addresses and Firmware Version

The following procedure describes how to display an overview of the LAN and WAN IPv4 and IPv6 addresses and firmware version.

➢ **To view the addresses and firmware version:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter **10.0.0.2** if you log in from the WAN or enter **192.168.20.0** if you log in from the LAN.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

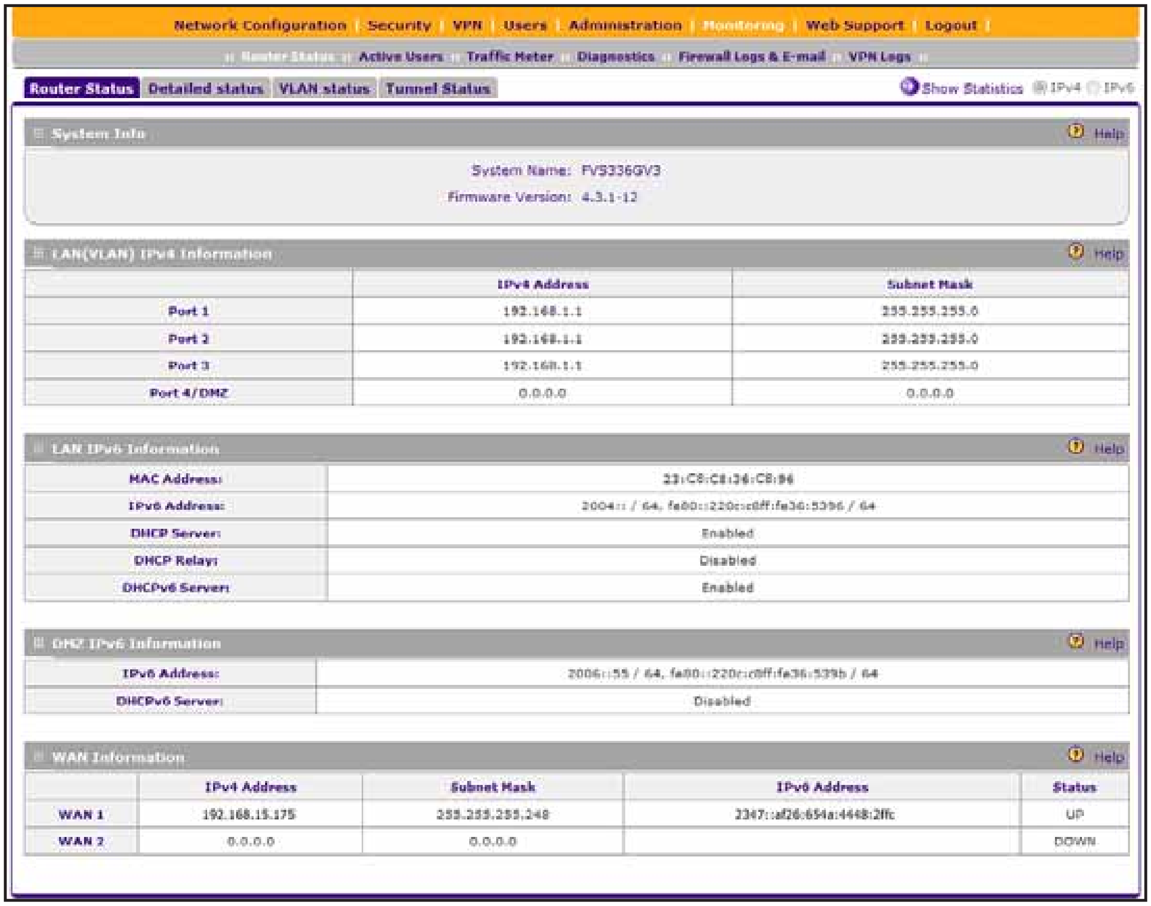
   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.


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

System Info

System Name: FVS336GV3

Firmware Version: 4.3.1-12

LAN(VLAN) IPv4 Information

	IPv4 Address	Subnet Mask
Port 1	192.168.1.1	255.255.255.0
Port 2	192.168.1.1	255.255.255.0
Port 3	192.168.1.1	255.255.255.0
Port 4/DMZ	0.0.0.0	0.0.0.0

LAN IPv6 Information

MAC Address:	23:C8:C8:36:C8:96
IPv6 Address:	2004:: / 64, fe80::220c:c0ff:fe36:5396 / 64
DHCP Server:	Enabled
DHCP Relay:	Disabled
DHCPv6 Server:	Enabled

DMZ IPv6 Information

IPv6 Address:	2006::55 / 64, fe80::220c:c0ff:fe36:539b / 64
DHCPv6 Server:	Disabled

WAN Information

	IPv4 Address	Subnet Mask	IPv6 Address	Status
WAN 1	192.168.15.175	255.255.255.248	2347::af26:654a:4448:2ffc	UP
WAN 2	0.0.0.0	0.0.0.0		DOWN

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

Item	Description
System Info	
System Name	The NETGEAR system name.
Firmware Version	The installed firmware version.
LAN (VLAN) IPv4 Information	
For each of the four LAN ports, the screen shows the IPv4 LAN address and subnet mask. For more detailed information, see *View Detailed Status Information About the VPN Firewall* on page 586.	

Item	Description
LAN IPv6 Information	
MAC Address	The MAC address of the VPN firewall.
IPv6 Address	The IPv6 LAN address that is assigned to the VPN firewall. For information about configuring the IPv6 address, see *Configure the IPv6 Internet Connection and WAN Settings* on page 87.
DHCP Server	The status of the IPv4 DHCP server (Enabled or Disabled). For information about configuring the IPv4 DHCP server, see *Manage VLAN Profiles* on page 119.
DHCP Relay	The status of the IPv4 DHCP relay (Enabled or Disabled). For information about configuring the IPv4 DHCP relay, see *Manage VLAN Profiles* on page 119.
DHCPv6 Server	The status of the DHCPv6 server for the LAN (Enabled or Disabled). For information about configuring the DHCPv6 server, see *Manage the IPv6 LAN* on page 153.
DMZ IPv6 Information	
IPv6 Address	The IPv6 DMZ address that is assigned to the VPN firewall. For information about configuring the IPv6 address, see *Manage the DMZ Port for IPv4 Traffic* on page 140.
DHCPv6 Server	The status of the DHCPv6 server for the DMZ (Enabled or Disabled). For information about configuring the DHCPv6 server, see *Manage the DMZ Port for IPv4 Traffic* on page 140.
WAN Information	
WAN 1	For each WAN interface, the screen shows the IPv4 address, subnet mask, IPv6 address, and status of the port (UP or DOWN). For more detailed information, see *View Detailed Status Information About the VPN Firewall* on page 586.
WAN 2	

View the Traffic Statistics for the Interfaces and Change the Polling Interval

The following procedure describes how to view the traffic statistics for the interfaces of the VPN firewall and change the polling interval.

➤ **To view the traffic statistics for the interfaces and change the polling interval:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter **10.0.0.2** if you log in from the WAN or enter **192.168.20.0** if you log in from the LAN.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

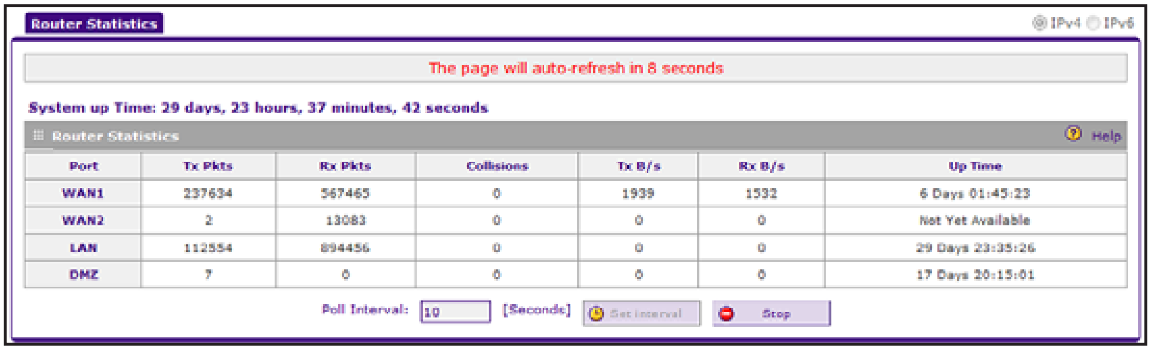
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Click the **Show Statistics** option arrow in the upper right.

   The Router Statistics screen displays.



The page will auto-refresh in 8 seconds

System up Time: 29 days, 23 hours, 37 minutes, 42 seconds

Router Statistics

Port	Tx Pkts	Rx Pkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN1	237634	567465	0	1939	1532	6 Days 01:45:23
WAN2	2	13083	0	0	0	Not Yet Available
LAN	112554	894456	0	0	0	29 Days 23:35:26
DMZ	7	0	0	0	0	17 Days 20:15:01

Poll Interval: 10 [Seconds]

The following table explains the fields of the Router Statistics screen.

Item	Description
System up Time. The period since the last time that the VPN firewall was started up.	
Router Statistics	
The following statistics are displayed for each of the two WAN interfaces, for all LAN interfaces combined, and for the DMZ interface:	
Tx Pkts	The number of packets transmitted on the port in bytes.
Rx Pxts	The number of packets received on the port in bytes.
Collisions	The number of signal collisions that have occurred on the port. A collision occurs when the port attempts to send data at the same time as a port on the other router or computer that is connected to this port.
Tx B/s	The number of bytes transmitted per second on the port.
Rx B/s	The number of bytes received per second on the port.
Up Time	The period that the port is active since it was restarted.

7. To change the polling interval period:

   a. Click the **Stop** button.

Wait for the counter to stop.

b. In the **Poll Interval** field, enter a new value in seconds.

c. Click the **Set interval** button.

View Detailed Status Information About the VPN Firewall

The following procedure describes how to view detailed status information about the IP addresses and MAC addresses on the VPN firewall, as well as other information.

➢ **To view detailed status information about the VPN firewall:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter **10.0.0.2** if you log in from the WAN or enter **192.168.20.0** if you log in from the LAN.

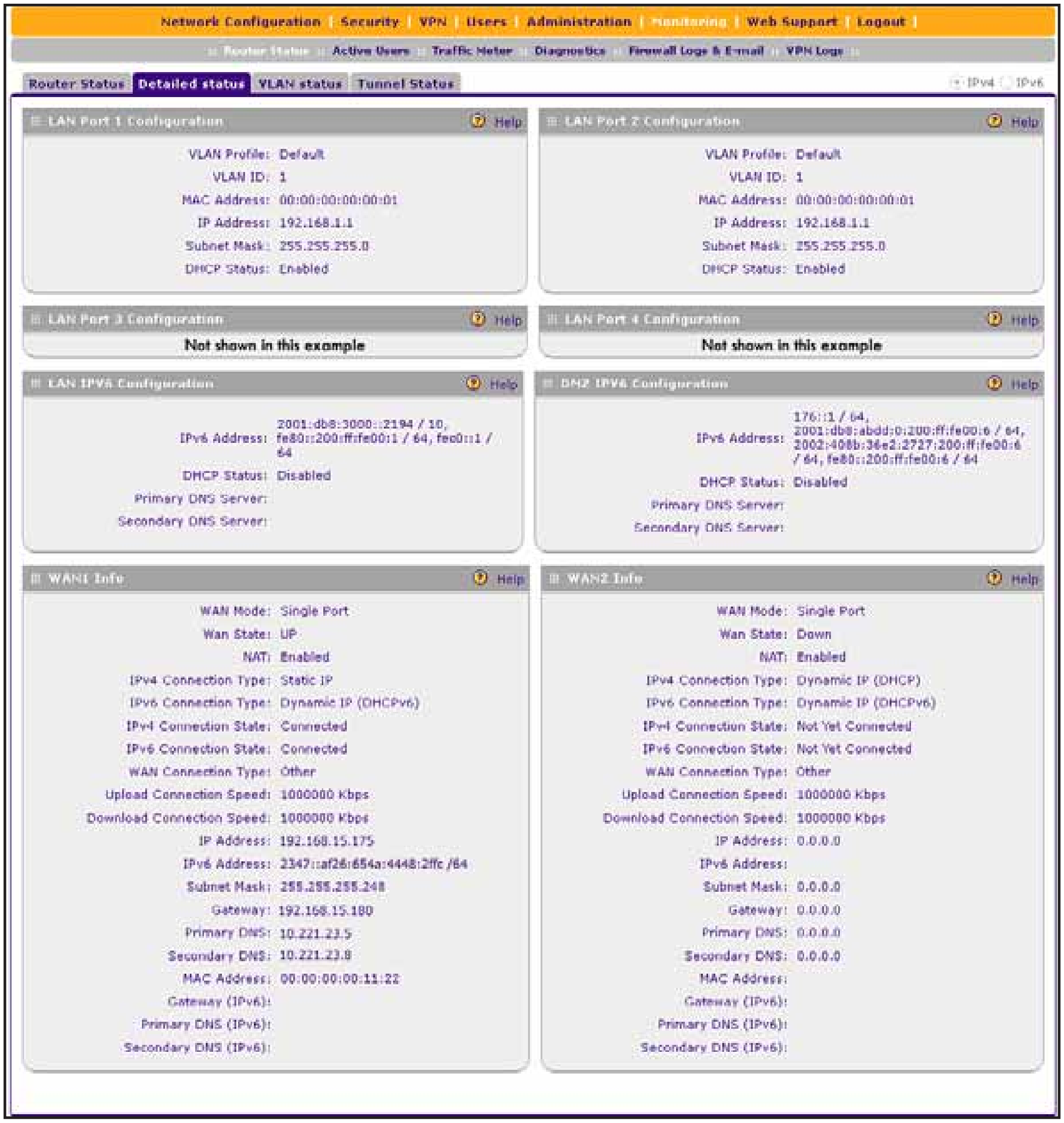
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Monitoring > Router Status > Detailed Status**.

   The Detailed Status screen displays.


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

LAN Port 1 Configuration

VLAN Profile: Default
VLAN ID: 1
MAC Address: 00:00:00:00:00:01
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHCP Status: Enabled

LAN Port 2 Configuration

VLAN Profile: Default
VLAN ID: 1
MAC Address: 00:00:00:00:00:01
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHCP Status: Enabled

LAN Port 3 Configuration

Not shown in this example

LAN Port 4 Configuration

Not shown in this example

LAN IPV6 Configuration

IPv6 Address: 2001:db8:3000::2194 / 10, fe80::200:ff:fe00:1 / 64, fec0::1 / 64
DHCP Status: Disabled
Primary DNS Server:
Secondary DNS Server:

DMZ IPV6 Configuration

IPv6 Address: 176::1 / 64, 2001:db8:abdd:0:200:ff:fe00:6 / 64, 2002:408b:36e2:2727:200:ff:fe00:6 / 64, fe80::200:ff:fe00:6 / 64
DHCP Status: Disabled
Primary DNS Server:
Secondary DNS Server:

WAN1 Info

WAN Mode: Single Port
Wan State: UP
NAT: Enabled
IPv4 Connection Type: Static IP
IPv6 Connection Type: Dynamic IP (DHCPv6)
IPv4 Connection State: Connected
IPv6 Connection State: Connected
WAN Connection Type: Other
Upload Connection Speed: 1000000 Kbps
Download Connection Speed: 1000000 Kbps
IP Address: 192.168.15.175
IPv6 Address: 2347::af26:654a:4448:2ffc /64
Subnet Mask: 255.255.255.248
Gateway: 192.168.15.180
Primary DNS: 10.221.23.5
Secondary DNS: 10.221.23.8
MAC Address: 00:00:00:00:11:22
Gateway (IPv6):
Primary DNS (IPv6):
Secondary DNS (IPv6):

WAN2 Info

WAN Mode: Single Port
Wan State: Down
NAT: Enabled
IPv4 Connection Type: Dynamic IP (DHCP)
IPv6 Connection Type: Dynamic IP (DHCPv6)
IPv4 Connection State: Not Yet Connected
IPv6 Connection State: Not Yet Connected
WAN Connection Type: Other
Upload Connection Speed: 1000000 Kbps
Download Connection Speed: 1000000 Kbps
IP Address: 0.0.0.0
IPv6 Address:
Subnet Mask: 0.0.0.0
Gateway: 0.0.0.0
Primary DNS: 0.0.0.0
Secondary DNS: 0.0.0.0
MAC Address:
Gateway (IPv6):
Primary DNS (IPv6):
Secondary DNS (IPv6):

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

Item	Description
LAN Port Configuration The following fields are shown for each of the LAN ports.	
VLAN Profile	The name of the VLAN profile that you assigned to the LAN port (see *Assign VLAN Profiles* on page 116). If the VLAN is not enabled on this port, the default profile (with VLAN ID 1) is assigned automatically.

Item	Description
VLAN ID	The VLAN ID that you assigned to the LAN port (see *Manage VLAN Profiles* on page 119). If the default VLAN profile is used, the VLAN ID is 1, which means that all tagged and untagged traffic can pass on the LAN port.
MAC Address	The MAC address for this port. Note the following about the LAN MAC address: • All LAN ports that are part of the default VLAN share the same default MAC address (00:00:00:00:00:01) unless you specified that each VLAN must be assigned a unique MAC address (see *Configure Unique VLAN MAC Addresses* on page 126). • LAN ports with an IPv4 address that differs from the default VLAN can still share the same MAC address as the default VLAN. • LAN port 4 can be assigned as the DMZ port, in which case its default MAC address is 00:00:00:00:00:06. For information about configuring the DMZ port, see *Manage the DMZ Port for IPv4 Traffic* on page 140.
IP Address	The IPv4 address for the LAN port. If the port is part of the default VLAN, the IP address is the default LAN IP address (192.168.1.1). For information about configuring VLAN profiles, see *Manage VLAN Profiles* on page 119.
Subnet Mask	The subnet mask for the LAN port. If the port is part of the default VLAN, the subnet mask is the default LAN IP subnet mask (255.255.255.0). For information about configuring VLAN profiles, see *Manage VLAN Profiles* on page 119.
DHCP Status	The status of the IPv4 DHCP server for the VLAN (Enabled or Disabled). For information about enabling DHCP for VLANs, see *Manage VLAN Profiles* on page 119.
LAN IPv6 Configuration For information about configuring the IPv6 LAN, see *DHCPv6 LAN Server Concepts and Configuration Roadmap* on page 153 and *Configure a Stateless DHCPv6 Server Without Prefix Delegation for the LAN* on page 155.	
IPv6 Address	The IPv6 address and prefix length for the LAN.
DHCP Status	The status of the DHCPv6 server for the LAN (Enabled or Disabled).
Primary DNS Server	The IPv6 address of the primary DNS server for the LAN.
Secondary DNS Server	The IP address of the secondary DNS server for the LAN.
DMZ IPv6 Configuration For information about configuring the IPv6 DMZ, see *Manage a Stateless DHCPv6 Server with Prefix Delegation for the DMZ* on page 185.	
IPv6 Address	The IPv6 address and prefix length for the DMZ.
DHCP Status	The status of the DHCPv6 server for the DMZ (Enabled or Disabled).
Primary DNS Server	The IPv6 address of the primary DNS server for the DMZ.
Secondary DNS Server	The IP address of the secondary DNS server for the DMZ.

Item	Description
WAN Configuration	
WAN Mode	The WAN mode can be Single Port, Load Balancing, or Auto Rollover. For information about configuring the WAN mode, see *Manage the IPv4 WAN Routing Mode* on page 30.
WAN State	The WAN state can be either UP or DOWN, depending on whether the port is connected to the Internet.
NAT	The NAT state for IPv4 can be either Enabled or Disabled, depending on whether NAT is enabled (see *Network Address Translation Overview* on page 30) or classical routing is enabled (see *Classical Routing* on page 31).
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 30.
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 87.
IPv4 Connection State	The IPv4 connection state can be either Connected or Not Yet Connected, depending on whether the WAN interface is connected to the Internet over an IPv4 address. For information about configuring the IPv4 address of the WAN port, see *Configure the IPv4 Internet Connection and WAN Settings* on page 30.
IPv6 Connection State	The IPv6 connection state can be either Connected or Not Yet Connected, depending on whether the WAN interface is connected to the Internet over an IPv6 address. For information about configuring the IPv6 address of the WAN port, see *Configure the IPv6 Internet Connection and WAN Settings* on page 87.
WAN Connection Type	The detected type of Internet connection that is used on this port. The WAN connection type can be DSL, ADSL, T1, T3, or Other. For information about configuring the WAN connection type, upload speed, and download speed, see *Managing Advanced WAN Options* on page 66.
Upload Connection Speed	The maximum upload speed that is provided by your ISP.
Download Connection Speed	The maximum download speed that is provided by your ISP.
IP Address	The IPv4 address of the WAN port. For information about configuring the IPv4 address of the WAN port, see *Configure the IPv4 Internet Connection and WAN Settings* on page 30.

Item	Description
IPv6 Address	The IPv6 address and prefix length of the WAN port. For information about configuring the IPv6 address and prefix length of the WAN port, see *Configure the IPv6 Internet Connection and WAN Settings* on page 87.
Subnet Mask	The IPv4 subnet mask of the WAN port. For information about configuring the subnet mask of the WAN port, see *Configure the IPv4 Internet Connection and WAN Settings* on page 30.
Gateway	The IPv4 address of the gateway. The gateway and DNS IPv4 settings are either obtained dynamically from your ISP or specified by you (see *Configure the IPv4 Internet Connection and WAN Settings* on page 30).
Primary DNS	The IPv4 address of the primary DNS server.
Secondary DNS	The IPv4 address of the secondary DNS server.
MAC Address	The default MAC address for the port or the MAC address that you specified (see *Managing Advanced WAN Options* on page 66).
Gateway (IPv6)	The IPv6 address of the gateway. The gateway and DNS IPv6 settings are either obtained dynamically from your ISP or specified by you (see *Manually Configure a Static IPv6 Internet Connection* on page 94 or *Manually Configure a PPPoE IPv6 Internet Connection* on page 97).
Primary DNS (IPv6)	The IPv6 address of the primary DNS server.
Secondary DNS (IPv6)	The IPv6 address of the secondary DNS server.

View the VLAN Status

You can view information about the VLANs that are enabled. Disabled VLANs are not displayed. For information about enabling and disabling VLANs, see *Assign VLAN Profiles* on page 116.

➢ **To view the status of the IPv4 VLANs:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter **10.0.0.2** if you log in from the WAN or enter **192.168.20.0** if you log in from the LAN.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

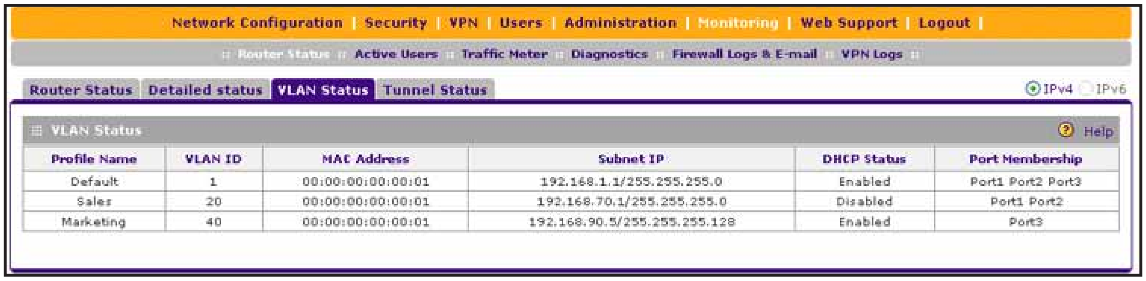
If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Monitoring > Router Status > VLAN Status**.

   The VLAN Status screen displays.


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

VLAN Status

Profile Name	VLAN ID	MAC Address	Subnet IP	DHCP Status	Port Membership
Default	1	00:00:00:00:00:01	192.168.1.1/255.255.255.0	Enabled	Port1 Port2 Port3
Sales	20	00:00:00:00:00:01	192.168.70.1/255.255.255.0	Disabled	Port1 Port2
Marketing	40	00:00:00:00:00:01	192.168.90.5/255.255.255.128	Enabled	Port3

Note: For information about configuring VLANs, see *Manage VLAN Profiles* on page 119

The following table explains the fields of the VLAN Status screen.

Item	Description
Profile Name	The unique name that you assigned for the VLAN.
VLAN ID	The identifier that you assigned for the VLAN.
MAC Address	VLANs can have the same MAC address as the associated LAN port or can be assigned a unique MAC address, depending on the VLAN MAC settings that you specified (see *Configure Unique VLAN MAC Addresses* on page 126).
Subnet IP	The IP address and subnet mask that you assigned.
DHCP Status	The DHCP status for the VLAN, which can be either DHCP Enabled or DHCP Disabled, depending on the DHCP configuration that you specified.
Port Membership	The ports that you have associated with the VLAN.

View the IPv6 Tunnel Status

The following procedure describes how to view the status of all active 6to4 and ISATAP tunnels and their IPv6 addresses.

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

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter **10.0.0.2** if you log in from the WAN or enter **192.168.20.0** if you log in from the LAN.

   The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

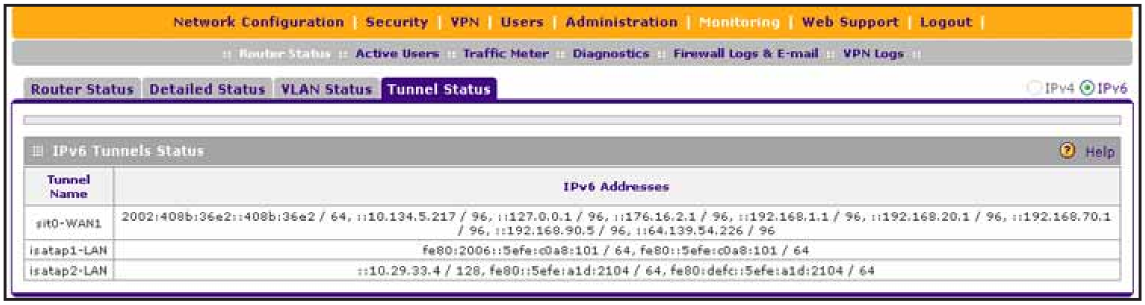
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

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

   The Tunnel Status screen displays.


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

IPv6 Tunnels Status

Tunnel Name	IPv6 Addresses
sit0-WAN1	2002:408b:36e2::408b:36e2 / 64, ::10.134.5.217 / 96, ::127.0.0.1 / 96, ::176.16.2.1 / 96, ::192.168.1.1 / 96, ::192.168.20.1 / 96, ::192.168.70.1 / 96, ::192.168.90.5 / 96, ::64.139.54.226 / 96
isatap1-LAN	fe80:2006::5efe:c0a8:101 / 64, fe80::5efe:c0a8:101 / 64
isatap2-LAN	::10.29.33.4 / 128, fe80::5efe:a1d:2104 / 64, fe80:defc::5efe:a1d:2104 / 64

Note: For information about configuring IPv6 tunnels, see *Manage Tunneling for IPv6 Traffic* on page 101.

The IPv6 Tunnel Status table shows the following fields:

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

View the VPN Connection Status, L2TP Users, and PPTP Users

The following sections provide information about viewing the status of IPSec VPN and SSL VPN connections and PPTP and L2TP users:

- *View the VPN Firewall IPSec VPN Connection Status and Terminate or Establish Tunnels* on page 363
- *View the VPN Firewall SSL VPN Connection Status and Disconnect Active Users* on page 444
- *View the Active PPTP Users and Disconnect Active Users* on page 420
- *View the Active L2TP Users and Disconnect Active Users* on page 423

View the VPN Logs

The following sections provide information about viewing the IPSec VPN and SSL VPN logs:

- *View the VPN Firewall IPSec VPN Log* on page 364
- *View the VPN Firewall SSL VPN Log* on page 445

View the Port Triggering Status

The following procedure describes how to view the status of the ports that were triggered by the port triggering feature.

➢ **To view the status of the ports that were triggered by the port triggering feature:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

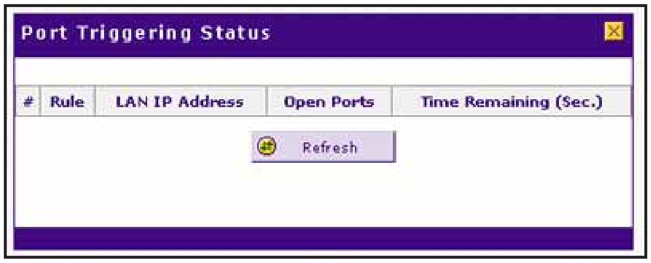
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Security > Port Triggering**.

   The Port Triggering screen displays.
7. Click the **Status** option arrow in the upper right.

   The Port Triggering Status pop-up screen displays.



Port Triggering Status

#	Rule	LAN IP Address	Open Ports	Time Remaining (Sec.)

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

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 and Terminate or Establish the Internet Connection

You can view the status of the IPv4 and IPv6 WAN connections, the DNS servers, and the DHCP servers, and you can terminate or establish the Internet connection.

The following sections provide information about viewing the WAN port status and terminating or establishing the Internet connection:

- *View the Status of an IPv4 WAN Port and Terminate or Establish the Internet Connection*
- *View the Status of an IPv6 WAN Port and Terminate or Establish the Connection*

View the Status of an IPv4 WAN Port and Terminate or Establish the Internet Connection

If a WAN port is active, you can terminate the Internet connection. If a WAN port is not active, you can establish the Internet connection.

➢ **To view the IPv4 status of a WAN port and terminate or establish the Internet connection:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

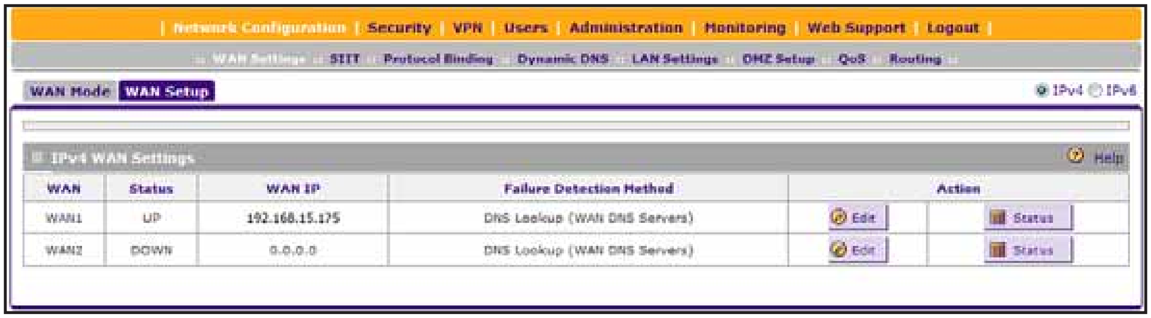
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Network Configuration > WAN Settings > WAN Setup**.

   The WAN Setup screen displays the IPv4 settings.

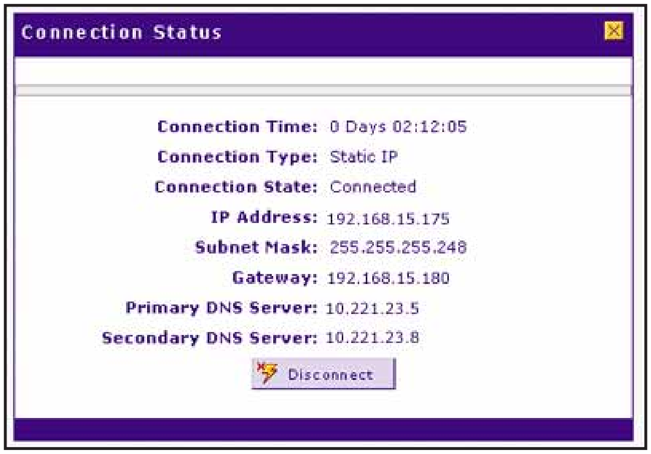

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
WAN Mode
WAN Setup
● IPv4 ○ IPv6
Help

IPv4 WAN Settings

WAN	Status	WAN IP	Failure Detection Method	Action	
WAN1	UP	192.168.15.175	DNS Lookup (WAN DNS Servers)	Edit	Status
WAN2	DOWN	0.0.0.0	DNS Lookup (WAN DNS Servers)	Edit	Status

7. Click the **Status** button that corresponds to the WAN interface for which you want to view the status.

   The following figure shows a static IP address configuration as an example.



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.

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.

Item	Description
Connection Status	The connection status can be either Connected or Disconnected.
IP Address	The addresses that were automatically detected or that you configured (see *Configure the IPv4 Internet Connection and WAN Settings* on page 30).
Subnet Mask	
Gateway	
DNS Server	
DHCP Server	The DHCP server that was automatically detected. This field displays only if your ISP does not require a login and the IP address is acquired dynamically from your ISP (see *Configure the IPv4 Internet Connection and WAN Settings* on page 30).
Lease Obtained	The time when the DHCP lease was obtained.
Lease Duration	The period that the DHCP lease remains in effect.

8. To terminate an active connection, click the **Disconnect** button.
9. To establish a connection, click **Connect** button.

View the Status of an IPv6 WAN Port and Terminate or Establish the Connection

If a WAN port is active, you can terminate the connection. If a WAN port is not active, you can establish the connection.

➢ **To view the IPv6 status of a WAN port and terminate or establish the Internet connection:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

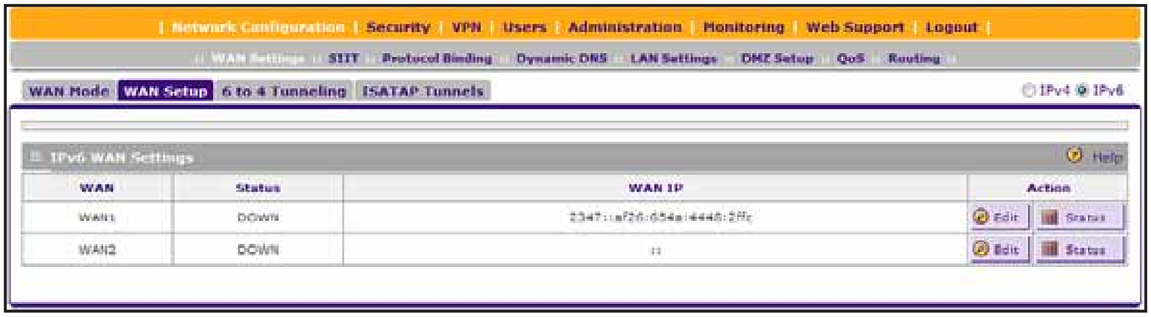
   The Router Status screen displays.

6. Select **Network Configuration > WAN Settings > WAN Setup**.

   The WAN Setup screen displays the IPv4 settings.

7. In the upper right, select the **IPv6** radio button.

   The WAN Setup screen displays the IPv6 settings:

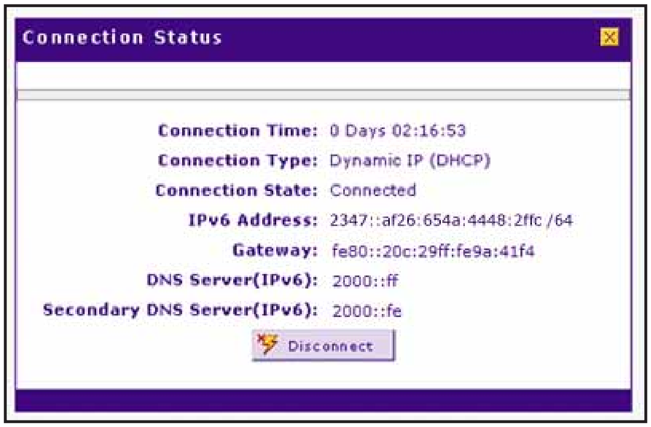

| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: QoS :: Routing ::
WAN Mode
WAN Setup
6 to 4 Tunneling
ISATAP Tunnels
○ IPv4 ● IPv6
Help

IPv6 WAN Settings

WAN	Status	WAN IP	Action
WAN1	DOWN	2347::af26:654a:4448:2ffc	Edit Status
WAN2	DOWN	::	Edit Status

8. Click the **Status** button that corresponds to the WAN interface for which you want to view the status.

   The following figure shows a static IP address configuration as an example.



Connection Status

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

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.

Item	Description
IPv6 Address	The IPv6 addresses that were automatically detected or that you configured (see *Use a DHCPv6 Server to Configure an IPv6 Internet Connection Automatically* on page 90 and *Manually Configure a Static IPv6 Internet Connection* on page 94). **Note:** The **Gateway**, **Primary DNS Server (IPv6)**, and **Secondary DNS Server (IPv6)** fields apply only to static IPv6 and PPPoE IPv6 connections.
Gateway	
Primary DNS Server (IPv6)	
Secondary DNS Server (IPv6)	

9. To terminate an active connection, click the **Disconnect** button.
10. To establish a connection, click the **Connect** button.

Display Internet Traffic by Type of Traffic

If you enabled the WAN traffic meter for an interface (see *Configure and Enable the WAN IPv4 Traffic Meter* on page 558), you can display the Internet traffic by protocol.

➤ **To display a report of the Internet traffic by protocol type for a WAN interface:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

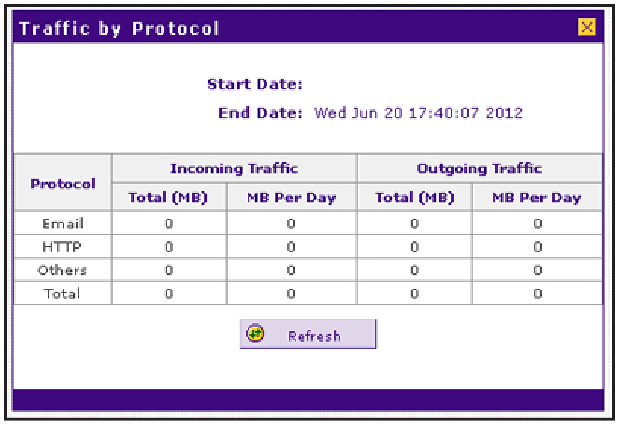
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Monitoring > Traffic Meter**.

   The WAN Traffic Meter tabs display with the WAN1 Traffic Meter screen in view.
7. If you want to display traffic for the WAN2 interface, click the **WAN2 Traffic Meter** tab.
8. Click the **Traffic by Protocol** option arrow in the upper right.

   The Traffic by Protocol pop-up screen displays.



Start Date:

End Date: Wed Jun 20 17:40:07 2012

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.

View the Attached Devices

You can view the network database (which is also referred to as the Known PCs and Devices table), which contains all IP devices that VPN firewall has discovered on the local network.

Note: If you reboot the VPN firewall, the data in the Known PCs and Devices table is lost until the VPN firewall rediscovers the devices.

➢ **To view the attached devices:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

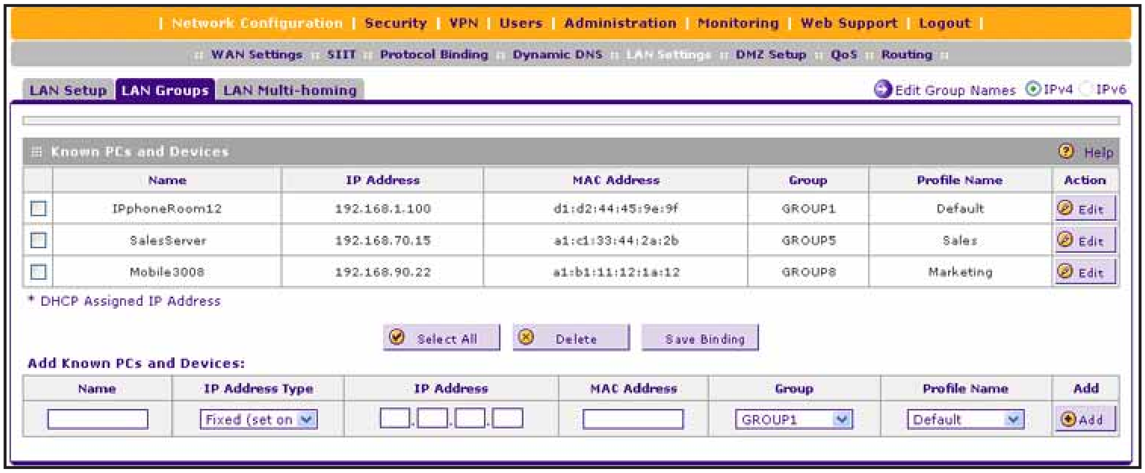
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

The Router Status screen displays.

6. Select **Network Configuration > LAN Settings > LAN Groups**.

   The LAN Groups screen displays. The following figure shows some examples in the Known PCs and Devices table.


| Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: SIIT :: Protocol Binding :: Dynamic DNS :: LAN Settings :: 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
□	IPphoneRoom12	192.168.1.100	d1:d2:44:45:9e:9f	GROUP1	Default	Edit
□	SalesServer	192.168.70.15	a1:c1:33:44:2a:2b	GROUP5	Sales	Edit
□	Mobile3008	192.168.90.22	a1:b1:11:12:1a:12	GROUP8	Marketing	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

The Known PCs and Devices table contains lists 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.

The following table describes the information that displays for each device.

Item	Description
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 change 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	You can assign each computer or device to a single LAN group. By default, a computer or device is assigned to Group 1. However, you can manually select a different LAN group (see *Manage the Network Database* on page 133).
Action	The **Edit** button, which provides access to the Edit Groups and Hosts screen. For information about how to change information for a device or manually add a device to the table, see *Manage the Network Database* on page 133.

View the DHCP Log

The following procedure describes how to view and clear the DHCP log.

Note: For information about how to change the DHCP settings, see *Manage VLAN Profiles* on page 119.

➢ **To view the most recent entries in the DHCP log or clear the log:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

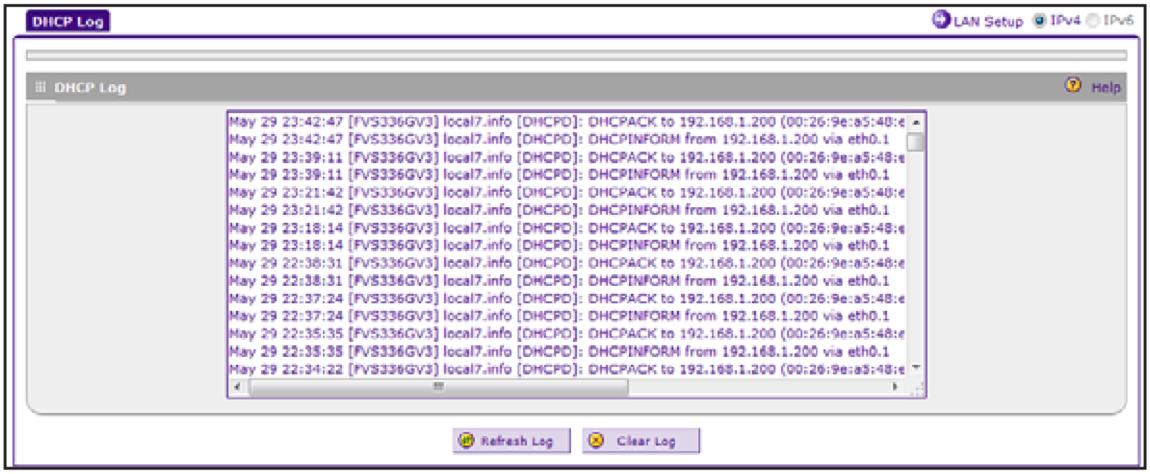
   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > LAN Settings**.

   The LAN Setup screen displays the IPv4 settings.
7. Click the **DHCP Log** option arrow in the upper right.

   The DHCP Log screen displays.



```
May 29 23:42:47 [FVS336GV3] local7.info [DHCPD]: DHCPACK to 192.168.1.200 (00:26:9e:a5:48:e
May 29 23:42:47 [FVS336GV3] local7.info [DHCPD]: DHCPINFORM from 192.168.1.200 via eth0.1
May 29 23:39:11 [FVS336GV3] local7.info [DHCPD]: DHCPACK to 192.168.1.200 (00:26:9e:a5:48:e
May 29 23:39:11 [FVS336GV3] local7.info [DHCPD]: DHCPINFORM from 192.168.1.200 via eth0.1
May 29 23:21:42 [FVS336GV3] local7.info [DHCPD]: DHCPACK to 192.168.1.200 (00:26:9e:a5:48:e
May 29 23:21:42 [FVS336GV3] local7.info [DHCPD]: DHCPINFORM from 192.168.1.200 via eth0.1
May 29 23:18:14 [FVS336GV3] local7.info [DHCPD]: DHCPACK to 192.168.1.200 (00:26:9e:a5:48:e
May 29 23:18:14 [FVS336GV3] local7.info [DHCPD]: DHCPINFORM from 192.168.1.200 via eth0.1
May 29 22:38:31 [FVS336GV3] local7.info [DHCPD]: DHCPACK to 192.168.1.200 (00:26:9e:a5:48:e
May 29 22:38:31 [FVS336GV3] local7.info [DHCPD]: DHCPINFORM from 192.168.1.200 via eth0.1
May 29 22:37:24 [FVS336GV3] local7.info [DHCPD]: DHCPACK to 192.168.1.200 (00:26:9e:a5:48:e
May 29 22:37:24 [FVS336GV3] local7.info [DHCPD]: DHCPINFORM from 192.168.1.200 via eth0.1
May 29 22:35:35 [FVS336GV3] local7.info [DHCPD]: DHCPACK to 192.168.1.200 (00:26:9e:a5:48:e
May 29 22:35:35 [FVS336GV3] local7.info [DHCPD]: DHCPINFORM from 192.168.1.200 via eth0.1
May 29 22:34:22 [FVS336GV3] local7.info [DHCPD]: DHCPACK to 192.168.1.200 (00:26:9e:a5:48:e
```

8. To view the most recent entries, click the **Refresh Log** button.

   The information onscreen is updated.

9. To remove all existing log entries, click the **Clear Log** button.

   All log entries are removed.

13. Diagnostics and Troubleshooting

13

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.

The chapter contains the following sections:

- *Use the Diagnostics Utilities*
- *Troubleshoot Basic Functioning*
- *Troubleshoot the Web Management Interface*
- *When You Enter a URL or IP Address, a Time-Out Error Occurs*
- *Troubleshoot the ISP Connection*
- *Troubleshoot the IPv6 Connection*
- *Troubleshoot a TCP/IP Network Using a Ping Utility*
- *Troubleshoot Problems with Date and Time*
- *Access Documentation from the Web Management Interface*

Note: For information about restoring the VPN firewall to factory default settings, see *Revert to Factory Default Settings* on page 551.

Use the Diagnostics Utilities

The following sections provide information about using the diagnostic utilities:

- *Diagnostic Utility*
- *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*
- *Schedule the VPN Firewall to Reboot*

Diagnostic Utility

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 for each interface in real time for a short period and download the packet information.

Note: For normal operation, diagnostic tools are not required.

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.

➢ **To send a ping:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

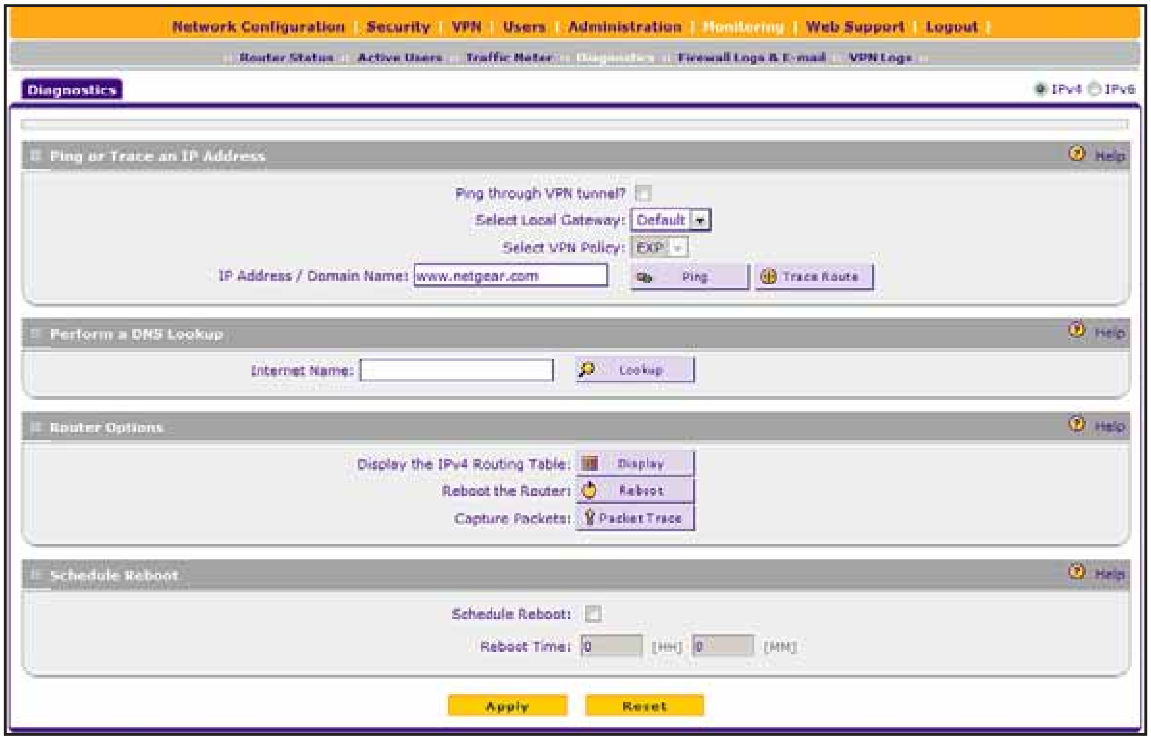
   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Monitoring > Diagnostics**.

   The Diagnostics screen displays the IPv4 settings.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Active Users :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Diagnostics
Ping or Trace an IP Address
Help
Ping
Trace Route
Perform a DNS Lookup
Help
Lookup
Router Options
Help
Display
Reboot
Packet Trace
Schedule Reboot
Help
Apply
Reset

● IPv4 ○ IPv6

Ping through VPN tunnel? □
Select Local Gateway: Default
Select VPN Policy: EXP
IP Address / Domain Name: www.netgear.com

Internet Name:

Display the IPv4 Routing Table:
Reboot the Router:
Capture Packets:

Schedule Reboot: □
Reboot Time: 0 [HH] 0 [MM]

7. To send a ping to an IPv6 location instead of an IPv4 location, in the upper right, select the **IPv6** radio button.

   The Diagnostics screen displays the IPv6 settings. Except for the **Domain Name** field, which is the **IP Address / Domain Name** field on the screen for IPv4, the IPv6 screen is identical to the IPv4 screen.

8. In the Ping or Trace an IP Address section, in the **IP Address / Domain Name** field, enter the IP address or domain name that you want to ping.

   Note: On the Diagnostics screen for IPv6, you cannot enter an IP address. You must enter a domain name in the **Domain Name** field.

9. Select either a gateway or a VPN policy:
   - Clear the **Ping through VPN tunnel?** check box and select a gateway from the **Select Local Gateway** menu.

     The **Select VPN Policy** menu is masked out.
   - Select the **Ping through VPN tunnel?** check box and select a VPN policy from the **Select VPN Policy** menu.

     The **Select Local Gateway** menu is masked out.
10. Click the **Ping** button.

    The results of the ping display in a new screen.
11. To return to the Diagnostics screen, click the **Back** button on the browser menu bar.

    The Diagnostics screen displays.

Trace a Route

A traceroute lists all routers between the source (the VPN firewall) and the destination IP address.

➢ **To send a traceroute:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

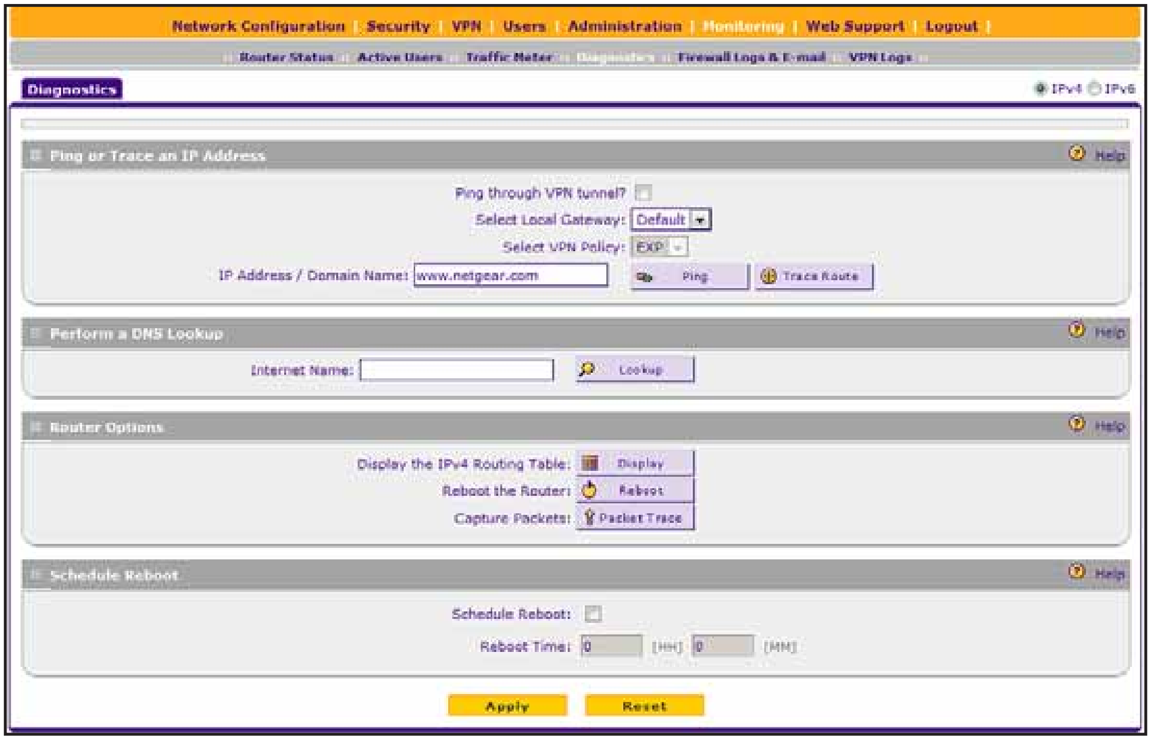
   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Monitoring > Diagnostics**.

   The Diagnostics screen displays the IPv4 settings.


Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Router Status | Active Users | Traffic Meter | Diagnostics | Firewall Logs & E-mail | VPN Logs
Diagnostics
IPv4 IPv6
Ping or Trace an IP Address
Help
Ping
Trace Route
Perform a DNS Lookup
Lookup
Router Options
Display
Reboot
Packet Trace
Schedule Reboot
Apply
Reset

● IPv4 ○ IPv6

Ping through VPN tunnel? □

Select Local Gateway: Default

Select VPN Policy: EXP

IP Address / Domain Name: www.netgear.com

Internet Name:

Display the IPv4 Routing Table:

Reboot the Router:

Capture Packets:

Schedule Reboot: □

Reboot Time: 0 [HH] 0 [MM]

7. To trace the route to an IPv6 location instead of an IPv4 location, in the upper right, select the **IPv6** radio button.

   The Diagnostics screen displays the IPv6 settings. Except for the **Domain Name** field, which is the **IP Address / Domain Name** field on the screen for IPv4, the IPv6 screen is identical to the IPv4 screen.

8. In the Ping or Trace an IP Address section, in the **IP Address / Domain Name** field, enter the IP address or domain name that you want to trace.

   Note: On the Diagnostics screen for IPv6, you cannot enter an IP address. You must enter a domain name in the **Domain Name** field.

9. Select either a gateway or a VPN policy:
   - Clear the **Ping through VPN tunnel?** check box and select a gateway from the **Select Local Gateway** menu.

     The **Select VPN Policy** menu is masked out.
   - Select the **Ping through VPN tunnel?** check box and select a VPN policy from the **Select VPN Policy** menu.

     The **Select Local Gateway** menu is masked out.

10. Click the **Traceroute** button.

    The results of the traceroute display in a new screen.

11. To return to the Diagnostics screen, click the **Back** button on the browser menu bar.

    The Diagnostics screen displays.

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. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Monitoring > Diagnostics**.

   The Diagnostics screen displays the IPv4 settings.
7. To look up an IPv6 address instead of an IPv4 address, in the upper right, select the **IPv6** radio button.

   The Diagnostics screen displays the IPv6 settings.
8. In the Perform a DNS Lookup section, in the **Internet Name** field, enter a domain name.
9. Click the **Lookup** button.

   The results of the lookup action display in a new screen.
10. To return to the Diagnostics screen, click the **Back** button on the browser menu bar.

    The Diagnostics screen displays.

Display the Routing Tables

Displaying the internal routing table can assist NETGEAR technical support in diagnosing routing problems.

➢ **To display the routing table:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Monitoring > Diagnostics**.

   The Diagnostics screen displays the IPv4 settings.
7. To display the IPv6 routing table instead of the IPv4 routing table, in the upper right, select the **IPv6** radio button.

   The Diagnostics screen displays the IPv6 settings.
8. In the Router Options section, click the **Display** button.

   The Route Display pop-up screen displays the routing table.

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 and download packets in real time:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Monitoring > Diagnostics**.

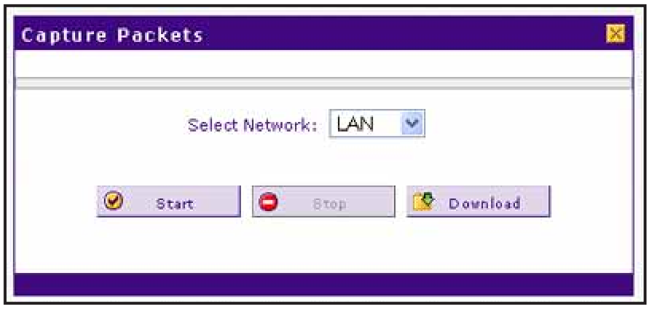
   The Diagnostics screen displays the IPv4 settings.

7. To capture IPv6 packets instead of the IPv4 packets, in the upper right, select the **IPv6** radio button.

   The Diagnostics screen displays the IPv6 settings.

8. In Router Options section, click the **Packet Trace** button.

   The Capture Packets pop-up screen displays.



9. From the **Select Network** menu, select the physical or virtual interface for which you want to capture packets.
10. Click the **Start** button.

    After a few seconds, the packet-tracing process starts, which is indicated by a message onscreen.

11. 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.

12. Click the **Download** button.
13. Select a location to save the captured packets.

    The file downloads to the location that you specify. The default file name is `pkt.cap`.

14. When the download is complete, browse to the download location you specified and verify that the file was downloaded successfully.

Reboot the VPN Firewall Remotely

You can perform a remote reboot, for example, when the VPN firewall seems to have become unstable or is not operating normally. For information about scheduling the VPN firewall to reboot, see *Schedule the VPN Firewall to Reboot* on page 611.

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 immediately:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Monitoring > Diagnostics**.

   The Diagnostics screen displays the IPv4 settings.
7. In Router Options section, click the **Reboot** button.

   The VPN firewall reboots. The Diagnostics screen might remain visible during the reboot process or a status message with a counter might show the number of seconds left until the reboot process is complete. The reboot process takes about 160 seconds.

Schedule the VPN Firewall to Reboot

You can schedule the VPN firewall to reboot at a time when a service disruption is minimal.

For information about rebooting the VPN firewall immediately, see *Reboot the VPN Firewall Remotely* on page 611.

➤ **To schedule the VPN firewall to reboot:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Monitoring > Diagnostics**.

   The Diagnostics screen displays the IPv4 settings.
7. In the Schedule Reboot section, select the **Schedule Reboot** check box.

   The **Reboot Time** fields become accessible.
8. In the **Reboot Time** fields, enter the hour in 24-hour format (1–23) and the minute (1–59) to specify the time that the VPN firewall must reboot.
9. Click the **Apply** button.

   The VPN firewall is scheduled to reboot.

Troubleshoot Basic Functioning

This section provides information about troubleshooting basic functioning of the VPN firewall.

➤ **After you turn on power to the VPN firewall, verify that the following sequence of events occurs:**

1. When power is first applied, verify that the Power LED lights.
2. After approximately two minutes, verify the following:
   a. The Test LED no longer lights (it turns off after approximately two minutes).
   b. The left LAN port LEDs light for any local ports that are connected.
   c. The left WAN port LEDs light for any WAN ports that are connected.

If a port’s left LED lights, a link is established to the connected device. The port’s right LED indicates the connection speed:

- If the port is connected to a 1000 Mbps device, the right LED lights green.
- If the port is connected to a 100 Mbps device, the right LED lights amber.
- If the port is connected to a 10 Mbps device, the right LED is off.

If any of these conditions do not occur, see the information in the following table.

Table 10. Troubleshooting basic functions

Problem	Solution
Power LED does not light.	If the Power and other LEDs are off when your VPN firewall is turned on, make sure that the power cord is correctly connected to your VPN firewall and that the power supply adapter is correctly connected to a functioning power outlet. If the error persists, you have a hardware problem. Contact NETGEAR technical support.
Test LED does not turn 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 has completed its initialization. If the Test LED remains on, there is a fault within the VPN firewall. If the Test LED is still on more than three minutes 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. For more information, see *Revert to Factory Default Settings* on page 551. If the error persists, you might have a hardware problem. Contact NETGEAR technical support.
LAN or WAN port LEDs do not light.	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 *Troubleshoot Basic Functioning* on page 612.
- If your computer’s IP address is shown as 169.254.x.x:
  Windows and Mac operating systems generate and assign an IP address if the computer

cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x.

If your IP address is in this range, check the connection from the computer to the VPN firewall and reboot your computer.

- If your VPN firewall’s IP address has changed and you do not know the current IP address, use an IP address scanner application on your network to discover the IP address. These applications are available on the Internet free of charge.

Tip: You can also reboot the VPN firewall and use a sniffer to capture packets sent during the reboot. Look at the ARP packets to locate the VPN firewall’s LAN interface address.

- Make sure that you are using the SSL https://*address* login rather than the http://*address* login.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click 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: For you 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 that you made in the web management interface, do the following:

- When entering configuration settings, be sure to click the **Apply** button before moving to another menu or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser. The changes might have occurred but the web browser might be caching the old configuration.

When You Enter a URL or IP Address, a Time-Out Error Occurs

A number of things could be causing a time-out error. 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 (see *Manually Configure a Static IPv4 Internet Connection* on page 36).

- 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 613.
- If the VPN firewall is configured correctly, check your Internet connection (for example, your modem or router) to make sure that it is working correctly.

Troubleshoot the ISP Connection

If your 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.

The following sections provide information about troubleshooting the ISP connection:

- *Check the WAN IP Address*
- *Force Your Modem or Router to Recognize the VPN Firewall*
- *Other ISP Troubleshooting Suggestions*

Check the WAN IP Address

If your VPN firewall is unable to access the Internet, check if the VPN firewall has a WAN IPv4 or IPv6 address.

➢ **To check the WAN IP address:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Network Configuration > WAN Settings > WAN Setup**.

The WAN Setup screen for IPv4 displays.

7. To check the WAN IPv6 address instead of the WAN IPv4 address, in the upper right, select the **IPv6** radio button.

   The WAN Setup screen for IPv6 displays.

8. Click the **Status** button that corresponds to the WAN interface for which you want to check the IP address.

   The Connection Status pop-up screen displays.

9. Check that an IP address is shown for the WAN port.

   If an IP address with zeros only is shown, or if no IP address is shown, the VPN firewall has not obtained an IP address from your ISP, or for IPv6, has not obtained or generated an IP address.

Force Your Modem or Router to Recognize the VPN Firewall

If the VPN firewall is unable to obtain an IP address from the ISP, you might need to force your modem or router to recognize your new VPN firewall.

➢ **To force your modem or router to recognize the VPN firewall:**

1. Turn off the power to the modem or router.
2. Turn off the power to your VPN firewall.
3. Wait five minutes and turn on the power to the modem or router.
4. When the LEDs of the modem or router indicate that synchronization with the ISP has occurred, turn on the power to the VPN firewall.

Other ISP Troubleshooting Suggestions

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.
  - If your ISP does require a login, make sure that you use the correct login name and password.
- For IPv4 PPPoE or PPTP connections, your ISP might check for your computer’s host name. For information about entering the host name, system name, or account name and the domain name or workgroup name that was assigned to you by your ISP, see *Manually Configure a PPPoE IPv4 Internet Connection* on page 39 or *Manually Configure a PPTP IPv4 Internet Connection* on page 44.

- If your ISP allows only one Ethernet MAC address to connect to the Internet and checks for your computer's MAC address, do one of the following:
  - Inform your ISP that you have a new network device and ask them to use the VPN firewall's MAC address.
  - Configure your VPN firewall to spoof your computer's MAC address. For more information, see *Managing Advanced WAN Options* on page 66.

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.
- Your computer might not have the VPN firewall configured as its TCP/IP gateway.

Troubleshoot the IPv6 Connection

If you have difficulty connecting over an IPv6 connection, the VPN firewall might be configured incorrectly or the computer from which you are trying to connect to the VPN firewall might be configured incorrectly.

Check the VPN firewall:

- By default, the VPN firewall is set to IPv4-only mode. Make sure that the VPN firewall is set to IPv4/IPv6 mode (see *Manage the IPv6 Routing Mode* on page 88).
- Make sure that the ISP settings are correct (see *Manually Configure a Static IPv6 Internet Connection* on page 94). The VPN firewall cannot receive a valid IPv6 address if the Internet connection is not correctly configured.
- Make sure that the VPN firewall can provide IPv6 addresses to the computers on the LAN (see *Manage the IPv6 LAN* on page 153). Make sure that the LAN settings and, if applicable for your type of configuration, the RADVD settings are correct.

Check the computer:

- Make sure that the operating system supports IPv6. Normally, the following operating systems support IPv6:
  - Windows 8, all 32- and 64-bit versions
  - Windows 7, all 32- and 64-bit versions
  - Windows Vista, all 32- and 64-bit versions
  - Windows XP Professional SP3, all 32- and 64-bit versions
  - Windows Server 2008, all versions
  - Windows Server 2008 R2, all versions
  - Windows Server 2003, all versions

- Windows Server 2003 R2, all versions
- Linux and other UNIX-based systems with a correctly configured kernel
- MAC OS X

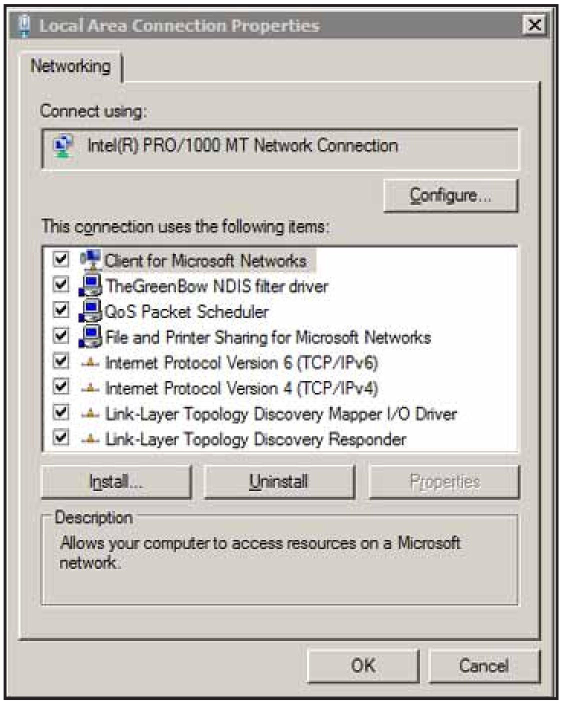
- Make sure that IPv6 is enabled on the computer. On a computer that runs a Windows-based operating system, do the following (note that the steps might differ on the various Windows operating systems):

  a. Open the Network Connections screen or the Network and Sharing Center screen.

     For example, on the Windows taskbar, click **Start**, select **Control Panel**, and select **Network Connections**.

  b. Click or double-click **Local Area Connection** for the connection to the VPN firewall.

     The Local Area Connection Properties screen displays.



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, as is shown in the previous figure.

- Make sure that the computer has an IPv6 address. If the computer has a link-local address only, it cannot reach the VPN firewall or the Internet.

  On a computer that runs a Windows-based operating system, do the following (note that the steps might differ on the various Windows operating systems):

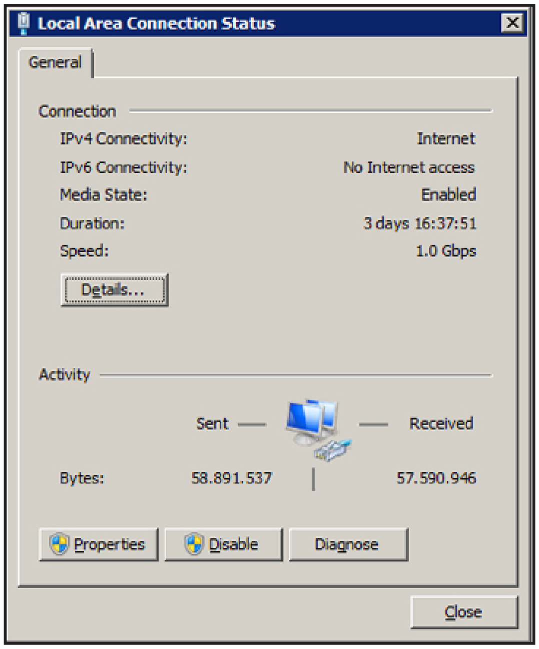
  a. Open the Network Connections screen or the Network and Sharing Center screen.

     For example, on the Windows taskbar, click **Start**, select **Control Panel**, and select **Network Connections**.

  b. Click or double-click **Local Area Connection** for the connection to the VPN firewall.

c. Click or double-click **View status of this connection**.

The Local Area Connection Status screen displays.



Local Area Connection Status

General

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

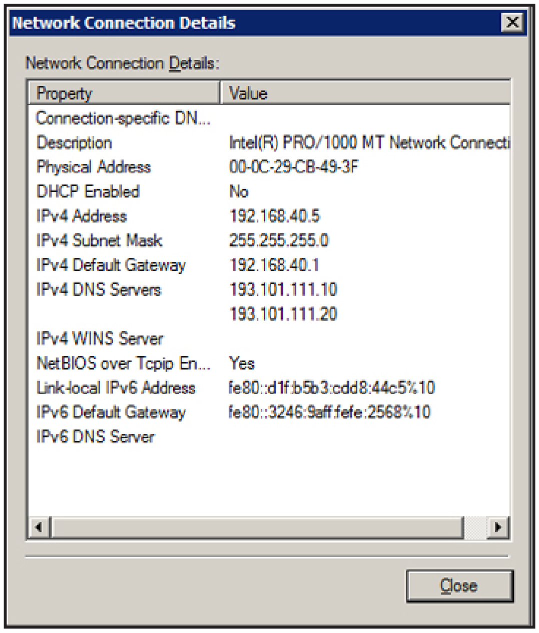
Bytes: 58.891.537 | 57.590.946

d. Make sure that Internet access shows for the IPv6 connection.

The previous figure shows that there is no Internet access.

e. Click the **Details** button.

The Network Connection Details screen displays.



Network Connection Details

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.

The following sections provide information about troubleshooting a TCP/IP network using a ping utility:

- *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, you might have one of the following problems:

   - Wrong physical connections
     - Make sure that the LAN port LED is lit. If the LED is off, see *Troubleshoot Basic Functioning* on page 612.
     - Check that the corresponding link LEDs are lit 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 620 are displayed. If you do not receive replies, check the following:

- Check that your computer has the IP address of your VPN firewall listed as the default gateway. If the IP configuration of your computer is assigned by DHCP, this information is not visible in your computer's Network Control Panel.
- Check to see that the network address of your computer (the portion of the IP address that is specified by the netmask) is different from the network address of the remote device.
- Check that the modem or router is connected and functioning.
- For IPv4 PPPoE or PPTP connections, your ISP might check for your computer's host name. For information about entering the host name, system name, or account name and the domain name or workgroup name that was assigned to you by your ISP, see *Manually Configure a PPPoE IPv4 Internet Connection* on page 39 or *Manually Configure a PPTP IPv4 Internet Connection* on page 44.
- 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 your ISP does this, you must configure your VPN firewall to *clone* or *spoof* the MAC address from the authorized computer. For more information, see *Managing Advanced WAN Options* on page 66.

Troubleshoot Problems with Date and Time

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. For information about displaying the current date and time of day, see *Configure Date and Time Service* on page 554.

Problems with the date and time function can include the following:

- Date shown is January 1, 2000. Cause: The VPN firewall has not yet successfully reached a network time server. Check that your Internet access settings are configured correctly. If you have just completed configuring the VPN firewall, wait at least five minutes, and check the date and time again.

- Time is off by one hour. Cause: The VPN firewall does not automatically detect daylight saving time.

➢ **To configure the VPN firewall to detect daylight saving time:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

   The NETGEAR Configuration Manager Login screen displays.
3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.
4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.
5. Click the **Login** button.

   The Router Status screen displays.
6. Select **Administration > Time Zone**.

   The Time Zone screen displays.
7. Select the **Automatically Adjust for Daylight Savings Time** check box.
8. Click the **Apply** button.

   Your settings are saved.

Access Documentation from the Web Management Interface

From the web management interface, you can access the online documentation library for your VPN firewall model.

➢ **To access NETGEAR's documentation library for your VPN firewall model:**

1. On your computer, launch an Internet browser.
2. In the address field of your browser, enter the IP address that was assigned to the VPN firewall during the installation process.

   The VPN firewall factory default IP address is 192.168.1.1.

The NETGEAR Configuration Manager Login screen displays.

3. In the **Username** field, type your user name and in the **Password / Passcode** field, type your password.

   For the default administrative account, the default user name is **admin** and the default password is **password**.

4. If you changed the default domain or were assigned a domain, from the **Domain** menu, select the domain.

   If you did not change the domain or were not assigned a domain, leave the menu selection at **geardomain**.

5. Click the **Login** button.

   The Router Status screen displays.

6. Select **Web Support > Documentation**.

   The download center at *downloadcenter.netgear.com* displays.

7. In the search field, enter **FVS336Gv2**.

   The support page for your product displays.

8. Click the **Get more Downloads...** link.

   All available documentation displays on the left side.

Network Planning for Multiple WAN Ports

A

This appendix describes the factors to consider when planning a network using a firewall that has more than one WAN port.

This appendix contains the following sections:

- *What to Consider Before You Begin*
- *Overview of the Planning Process*
- *Planning for Inbound Traffic*
- *Planning for Virtual Private Networks*

What to Consider Before You Begin

The following sections provide information about planning and requirements:

- *Planning Overview*
- *Cabling and Computer Hardware Requirements*
- *Computer Network Configuration Requirements*
- *Internet Configuration Requirements*

Planning Overview

The VPN firewall is a powerful and versatile solution for your networking needs. To make the configuration process easier and to understand all of the choices that are available to you, consider the following before you begin:

1. Plan your network.
   - **a.** Determine whether you will use one or several WAN ports. For one WAN port, you might need a fully qualified domain name either for convenience or to remotely access a dynamic WAN IP address.
   - **b.** If you intend to use several WAN ports, determine whether you will use them in auto-rollover mode for increased system reliability or load balancing mode for maximum bandwidth efficiency. See the topics in this appendix on page *624* for more information. Your decision has the following implications:
     - Fully qualified domain name (FQDN)
       - For auto-rollover mode, you need an FQDN to implement features such as exposed hosts and virtual private networks.
       - For load balancing mode, you might still need an FQDN either for convenience or to remotely access a dynamic WAN IP address.
     - Protocol binding
       - For auto-rollover mode, protocol binding does not apply.
       - For load balancing mode, decide which protocols will be bound to a specific WAN port.
       - You can also add your own service protocols to the list.
2. Set up your accounts.
   - **a.** Obtain active Internet services such as DSL broadband accounts and locate the Internet service provider (ISP) configuration information.
     - In this manual, the WAN side of the network is presumed to be provisioned as shown in the following figure, with two ISPs connected to the VPN firewall through separate physical facilities.
     - Each WAN port must be configured separately, whether you are using a separate ISP for each WAN port or you are using the same ISP to route the traffic of both WAN ports.

- If your ISP charges by the volume of data traffic each month, consider enabling the VPN firewall’s traffic meter to monitor or limit your traffic.

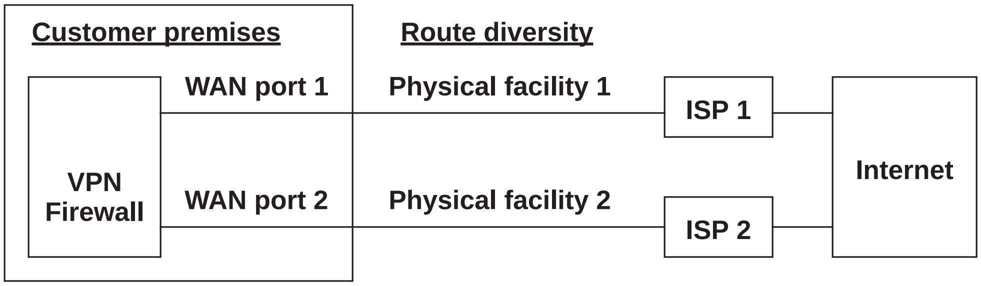


Figure 13. Planning for route diversity

b. Contact a Dynamic DNS service and register FQDNs for one or both WAN ports.

3. Plan your network management approach.
   - The VPN firewall can be managed remotely but you must enable remote management locally after each factory default reset.

     NETGEAR strongly advises you to change the default management password to a strong password before enabling remote management.
   - If the factory default settings are not suitable for your installation, you can choose various WAN options. These options include enabling a WAN port to respond to a ping, and setting MTU size, port speed, and upload bandwidth.
4. Prepare to physically connect the firewall to your cable or DSL modems and a computer. Instructions for connecting the VPN firewall are in the *ProSAFE Gigabit Quad WAN SSL VPN Firewall FVS336Gv2 Installation Guide*.

Cabling and Computer Hardware Requirements

For you to use the VPN firewall in your network, each computer must have an Ethernet network interface card (NIC) installed and must be equipped with an Ethernet cable. If the computer connects to your network at 100 Mbps or higher speeds, you must use a Category 5 (Cat 5) cable.

Computer Network Configuration Requirements

The VPN firewall integrates a web management interface. To access the configuration screens on the VPN firewall, you must use a Java-enabled web browser that supports HTTP uploads, such as the most recent version of Google Chrome, Microsoft Internet Explorer, Mozilla Firefox, or Apple Safari with JavaScript, cookies, and SSL enabled. Free browsers are readily available for Windows, Macintosh, and UNIX/Linux.

For the initial connection to the Internet and configuration of the VPN firewall, you must connect a computer to the VPN firewall and the computer must be configured to automatically get its TCP/IP configuration from the VPN firewall through DHCP.

The DSL broadband access device or router must provide a standard Ethernet interface.

Internet Configuration Requirements

Depending on how your ISP sets up your Internet accounts, you need the following Internet configuration information to connect VPN firewall to the Internet:

- Host and domain names
- One or more ISP login names and passwords
- ISP Domain Name Server (DNS) addresses
- One or more fixed IP addresses (also known as static IP addresses)

Where Do I Get the Internet Configuration Information?

You can gather the required Internet connection information in several ways.

Your ISPs provide all the information needed to connect to the Internet. If you cannot locate this information, you can ask your ISP to provide you with it, or, if you have a computer already connected using the active Internet access account, you can gather the configuration information from that computer.

- For Windows computers, open the Network and Sharing Center, select the TCP/IP entry for the Ethernet adapter, and click **Properties**. Record all the settings for each tab page.
- For Macintosh computers, open the TCP/IP or Network Control Panel. Record all the settings for each section.

After you have located your Internet configuration information, you might want to record the information in *Internet Connection Information* on page 627.

Internet Connection Information

Print the following Internet connection information. Write down the configuration settings that are provided to you by ISP.

- **ISP login information**. The login name and password are case-sensitive and must be entered exactly as given by your ISP. Some ISPs use your full email address as the login name. The service name is not required by all ISPs. If you connect using a login name and password, complete the following:

  WAN 1 login name: ______________________________

  WAN 1 password: ______________________________

  WAN 1 service name: ______________________________

  WAN 2 login name: ______________________________

  WAN 2 password: ______________________________

  WAN 2 service name: ______________________________

- **Fixed or static IP address**. If you have a static IP address, record the following information. For example, 169.254.141.148 could be a valid IP address.

  WAN 1 fixed or static Internet IP address: ______.______.______.______

WAN 1 gateway IP address: ______.______.______.______

WAN 1 subnet mask: ______.______.______.______

WAN 2 fixed or static Internet IP address: ______.______.______.______

WAN 2 gateway IP address: ______.______.______.______

WAN 2 subnet mask: ______.______.______.______

- **ISP DNS server addresses**. If you were given DNS server addresses, complete the following:

  WAN 1 primary DNS server IP address: ______.______.______.______

  WAN 1 secondary DNS server IP address: ______.______.______.______

  WAN 2 primary DNS server IP address: ______.______.______.______

  WAN 2 secondary DNS server IP address: ______.______.______.______

- **Host and domain names**. Some ISPs use a specific host or domain name such as CCA7324-A or home. If you were not given host or domain names, you can use the following examples as a guide:
  - If your main email account with your ISP is aaa@yyy.com, use **aaa** as your host name. Your ISP might call this your account, user, host, computer, or system name.
  - If your ISP’s mail server is mail.xxx.yyy.com, use **xxx.yyy.com** as the domain name.

  WAN 1 ISP host name: ________________________

  WAN 1 ISP domain name: ________________________

  WAN 2 ISP host name: ________________________

  WAN 2 ISP domain name: ________________________

- **Fully qualified domain name**. Some organizations use a fully qualified domain name (FQDN) from a Dynamic DNS service provider for their IP addresses.

  Dynamic DNS service provider: ________________________

  WAN 1 FQDN: ________________________

  WAN 2 FQDN: ________________________

Overview of the Planning Process

The areas that require planning when you use a firewall that has multiple WAN ports such as the VPN firewall include the following:

- Inbound traffic (port forwarding, port triggering)
- Outbound traffic (protocol binding)
- Virtual private networks (VPNs)

You can configure two WAN ports on a mutually exclusive basis to do either of the following:

- Auto-rollover for increased reliability
- Load balance for outgoing traffic

These various types of traffic and auto-rollover or load balancing, which are listed below, all interact to make the planning process more challenging:

- **Inbound traffic**. Unrequested incoming traffic can be directed to a computer on your LAN rather than being discarded. The mechanism for making the IP address public depends on whether the dual WAN ports are configured for auto-rollover or load balancing.
- **Virtual private networks**. A virtual private network (VPN) tunnel provides a secure communication channel either between two gateway VPN firewalls or between a remote computer client and gateway VPN firewall. As a result, the IP address of at least one of the tunnel endpoints must be known in advance for the other tunnel endpoint to establish (or reestablish) the VPN tunnel.

Note: When the VPN firewall's WAN port rolls over, the VPN tunnel closes and must be reestablished using the new WAN IP address. However, you can configure automatic IPSec VPN rollover to ensure that an IPSec VPN tunnel is reestablished.

- **Dual WAN ports in auto-rollover mode**. Rollover for a VPN firewall with dual WAN ports is different from a single WAN port gateway configuration when you specify the IP address. Only one WAN port is active at a time, and when it rolls over, the IP address of the active WAN port always changes. Therefore, the use of a fully qualified domain name (FQDN) is always required, even when the IP address of each WAN port is fixed.

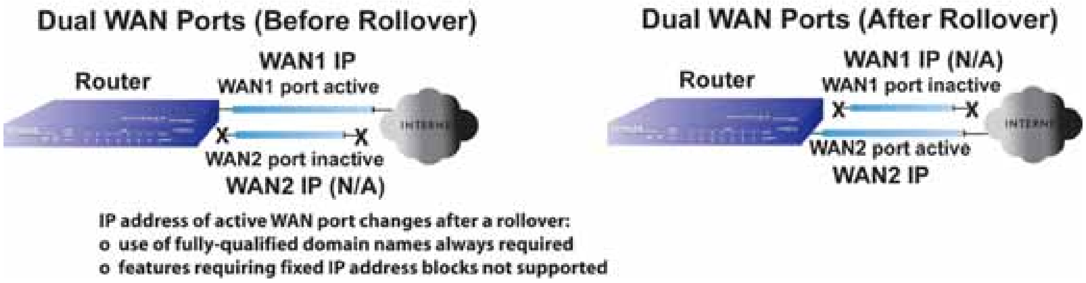

Dual WAN Ports (Before Rollover)
Router
WAN1 IP
WAN1 port active
INTERNET
WAN2 port inactive
WAN2 IP (N/A)
Dual WAN Ports (After Rollover)
Router
WAN1 IP (N/A)
WAN1 port inactive
INTERNET
WAN2 port active
WAN2 IP
IP address of active WAN port changes after a rollover:
o use of fully-qualified domain names always required
o features requiring fixed IP address blocks not supported

Figure 14. Dual WAN ports in auto-rollover mode

Features such as multiple exposed hosts are not supported in auto-rollover mode because the IP addresses of each WAN port must be in the identical range of fixed addresses.

- **Dual WAN ports in load balancing mode**. Load balancing for a VPN firewall with dual WAN ports is similar to a single WAN gateway configuration when you specify the IP address. Each IP address is either fixed or dynamic based on the ISP: You must use FQDNs when the IP address is dynamic, but FQDNs are optional when the IP address is static.

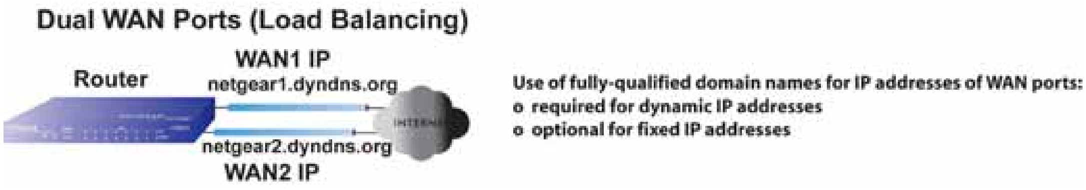

Dual WAN Ports (Load Balancing)
Router
WAN1 IP
netgear1.dyndns.org
INTERNET
netgear2.dyndns.org
WAN2 IP
Use of fully-qualified domain names for IP addresses of WAN ports:
o required for dynamic IP addresses
o optional for fixed IP addresses

Figure 15. Dual WAN ports in load balancing mode

Planning for Inbound Traffic

Incoming traffic from the Internet is normally discarded by the VPN firewall unless the traffic is a response to one of your local computers or a service for which you have configured an inbound rule. Instead of discarding this traffic, you can configure the VPN firewall to forward it to one or more LAN hosts on your network.

The addressing of the VPN firewall's dual WAN port depends on the configuration being implemented.

Table 11. IP addressing requirements for exposed hosts in a dual WAN port configuration

Configuration and WAN IP Address		**Single WAN Port (Reference Case)**	**Dual WAN Port Cases**	
			Rollover	**Load Balancing**
Inbound traffic • Port forwarding • Port triggering	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required

The following sections provide information about planning for inbound traffic:

- *Inbound Traffic to a Single WAN Port System*
- *Inbound Traffic to a Dual WAN Port System*

Inbound Traffic to a Single WAN Port System

The Internet IP address of the VPN firewall's WAN port must be known to the public so that the public can send incoming traffic to the exposed host when this feature is supported and enabled.

In the single WAN case, the WAN's Internet address is either a fixed IP address or an FQDN if the IP address is dynamic.

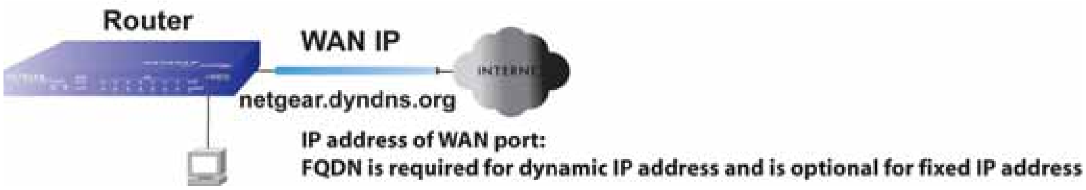

Router
WAN IP
INTERNET
netgear.dyndns.org
IP address of WAN port:
FQDN is required for dynamic IP address and is optional for fixed IP address

Figure 16. Inbound traffic to a single WAN port system

Inbound Traffic to a Dual WAN Port System

The IP address range of the VPN firewall's WAN port must be both fixed and public so that the public can send incoming traffic to the multiple exposed hosts when this feature is supported and enabled.

Inbound Traffic: Dual WAN Ports for Improved Reliability

In a dual WAN port auto-rollover configuration, the WAN port's IP address always changes when a rollover occurs. You must use an FQDN that toggles between the IP addresses of the WAN ports (that is, WAN1 or WAN2).

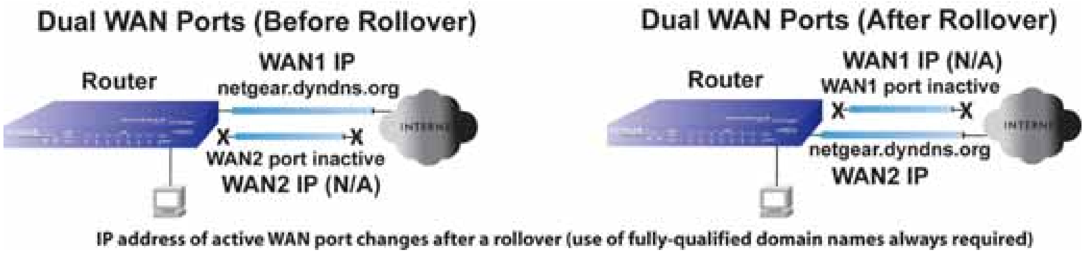
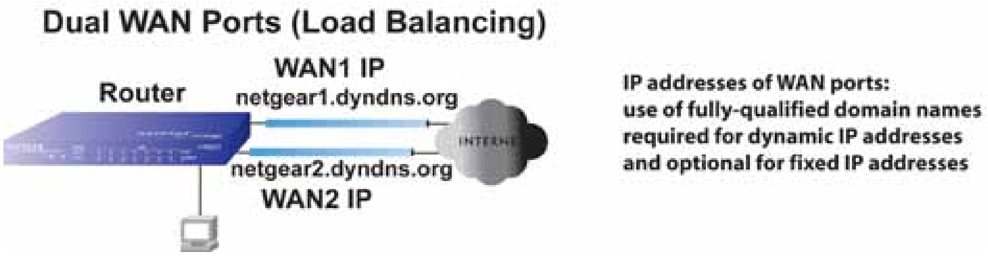

Dual WAN Ports (Before Rollover)
WAN1 IP
Router
netgear.dyndns.org
INTERNET
X
X
WAN2 port inactive
WAN2 IP (N/A)
Dual WAN Ports (After Rollover)
Router
WAN1 IP (N/A)
WAN1 port inactive
X
X
INTERNET
netgear.dyndns.org
WAN2 IP
IP address of active WAN port changes after a rollover (use of fully-qualified domain names always required)

Figure 17. Inbound traffic to a dual WAN port system in auto-rollover mode

Inbound Traffic: Dual WAN Ports for Load Balancing

In a dual WAN port load balancing configuration, the Internet address of each WAN port is either fixed if the IP address is fixed or an FQDN if the IP address is dynamic (see the following figure).

Note: Load balancing is implemented for outgoing traffic and not for incoming traffic. To maintain better control of WAN port traffic, consider making one of the WAN port Internet addresses public and to keep the other one private.



IP addresses of WAN ports:
use of fully-qualified domain names
required for dynamic IP addresses
and optional for fixed IP addresses

Figure 18. Inbound traffic to a dual WAN port system in load balancing mode

Planning for Virtual Private Networks

The following sections provide information about planning for VPN:

- *VPN Telecommuter - Client-to-Gateway*
- *VPN Gateway-to-Gateway*
- *VPN Telecommuter - Client-to-Gateway Through a NAT Router*

When implementing virtual private network (VPN) tunnels, you must use a mechanism for determining the IP addresses of the tunnel endpoints. The addressing of the firewall's WAN ports in a dual WAN port auto-rollover or load balancing configuration depends on the configuration being implemented.

Table 12. IP addressing requirements for VPNs in a dual WAN port configuration

Configuration and WAN IP Address		Single WAN Port Configurations (Reference Cases)	Dual WAN Port Configurations	
			Rollover Mode[a]	Load Balancing Mode
VPN Telecommuter - Client-to-Gateway	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required
VPN Gateway-to-Gateway	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required
VPN Telecommuter - Client-to-Gateway Through a NAT Router	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required

[a] *After a rollover, all tunnels must be reestablished using the new WAN IP address.*

For a single WAN gateway configuration, use an FQDN when the IP address is dynamic and either an FQDN or the IP address itself when the IP address is fixed. The situation is different in dual WAN port gateway configurations.

- **Dual WAN ports in auto-rollover mode**. A gateway configuration with dual WAN ports that function in auto-rollover mode is different from a gateway configuration with a single WAN port when you specify the IP address of the VPN tunnel endpoint. Only one WAN port is active at a time, and when it rolls over, the IP address of the active WAN port always changes. Therefore, the use of an FQDN is always required, even when the IP address of each WAN port is fixed.

Note: When the VPN firewall's WAN port rolls over, the VPN tunnel collapses and must be reestablished using the new WAN IP address. However, you can configure automatic IPSec VPN rollover to ensure that an IPSec VPN tunnel is reestablished.

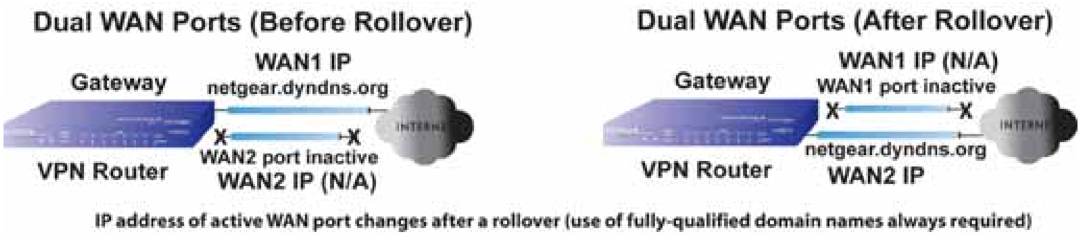

Dual WAN Ports (Before Rollover)
Gateway
WAN1 IP
netgear.dyndns.org
INTERNET
VPN Router
WAN2 port inactive
WAN2 IP (N/A)
Dual WAN Ports (After Rollover)
Gateway
WAN1 IP (N/A)
WAN1 port inactive
INTERNET
VPN Router
netgear.dyndns.org
WAN2 IP
IP address of active WAN port changes after a rollover (use of fully-qualified domain names always required)

Figure 19. Dual WAN ports in auto-rollover mode with VPN traffic

- **Dual WAN ports in load balancing mode**. A gateway configuration with dual WAN ports that function in load balancing mode is the same as a single WAN port configuration when you specify the IP address of the VPN tunnel endpoint. Each IP address is either fixed or dynamic based on the ISP: You must use FQDNs when the IP address is dynamic, and FQDNs are optional when the IP address is static.

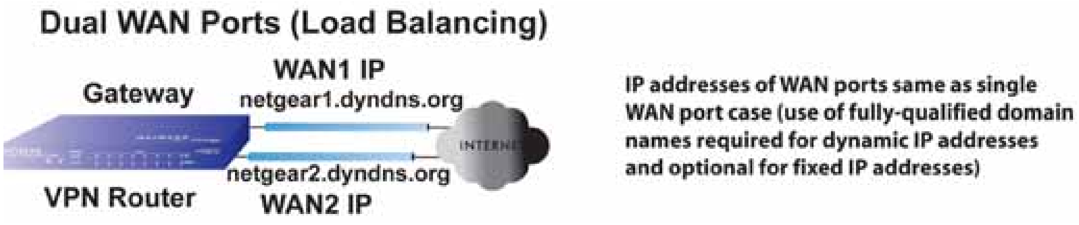

Dual WAN Ports (Load Balancing)
Gateway
WAN1 IP
netgear1.dyndns.org
INTERNET
netgear2.dyndns.org
VPN Router
WAN2 IP
IP addresses of WAN ports same as single WAN port case (use of fully-qualified domain names required for dynamic IP addresses and optional for fixed IP addresses)

Figure 20. Dual WAN ports in load balancing mode with VPN traffic

VPN Telecommuter - Client-to-Gateway

The following situations exemplify the requirements for a remote computer client with no firewall to establish a VPN tunnel with a gateway VPN firewall:

- Single-gateway WAN port
- Redundant dual-gateway WAN ports for increased reliability (before and after rollover)
- Dual-gateway WAN ports for load balancing

VPN Telecommuter: Single-Gateway WAN Port - Reference Case

In a single WAN port gateway configuration, the remote computer client initiates the VPN tunnel because the IP address of the remote computer client is not known in advance. The gateway WAN port must act as the responder.

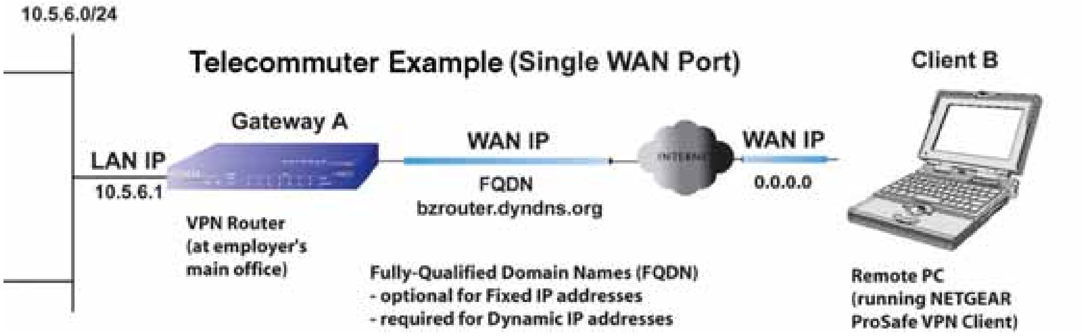


Figure 21. Telecommuter example in a single WAN port configuration

The IP address of the gateway WAN port can be either fixed or dynamic. If the IP address is dynamic, an FQDN must be used. If the IP address is fixed, an FQDN is optional.

VPN Telecommuter: Dual-Gateway WAN Ports for Improved Reliability

In a gateway configuration with dual WAN ports that function in auto-rollover mode, the remote computer client initiates the VPN tunnel with the active WAN port (port WAN1 in the following figure) because the IP address of the remote computer client is not known in advance. The gateway WAN port must act as a responder.

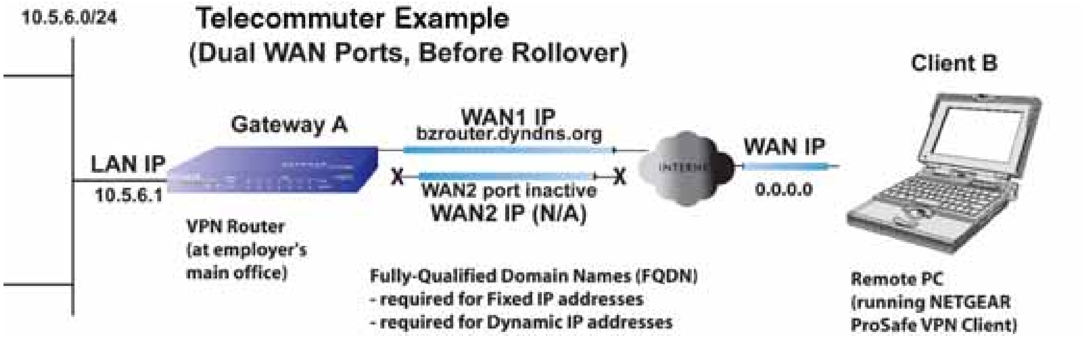


Figure 22. Telecommuter example in a dual WAN port configuration before auto-rollover

The IP addresses of the WAN ports can be either fixed or dynamic, but you always must use an FQDN because the active WAN port could be either WAN1 or WAN2 (that is, the IP address of the active WAN port is not known in advance).

After a rollover of the WAN port occurs, the previously inactive gateway WAN port becomes the active port (port WAN2 in the following figure) and the remote computer client must reestablish the VPN tunnel. The gateway WAN port must act as the responder.

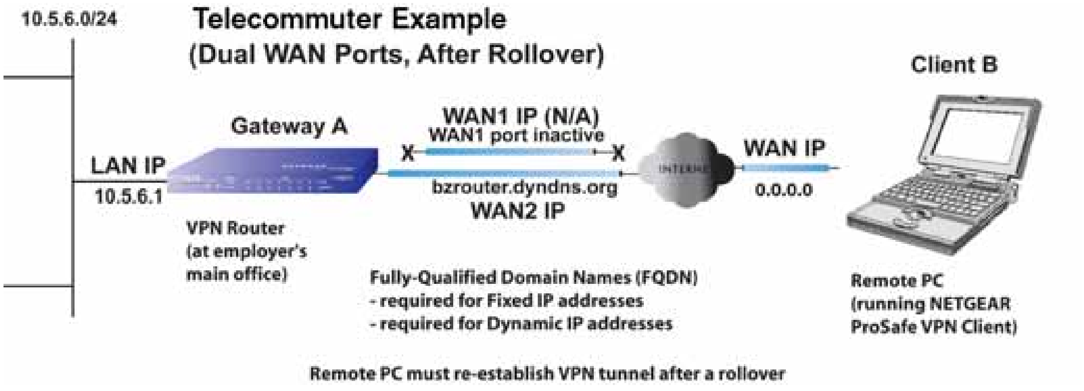


Figure 23. Telecommuter example in a dual WAN port configuration after auto-rollover

The purpose of the FQDN in this case is to toggle the domain name of the gateway firewall between the IP addresses of the active WAN port (that is, WAN1 and WAN2) so that the remote computer client can determine the gateway IP address to establish or reestablish a VPN tunnel.

VPN Telecommuter: Dual-Gateway WAN Ports for Load Balancing

In a gateway configuration with dual WAN ports that function in load balancing mode, the remote computer initiates the VPN tunnel with the appropriate gateway WAN port (that is, port WAN1 or WAN2 as necessary to balance the loads of the two gateway WAN ports) because the IP address of the active WAN port is not known in advance. The selected gateway WAN port must act as the responder.

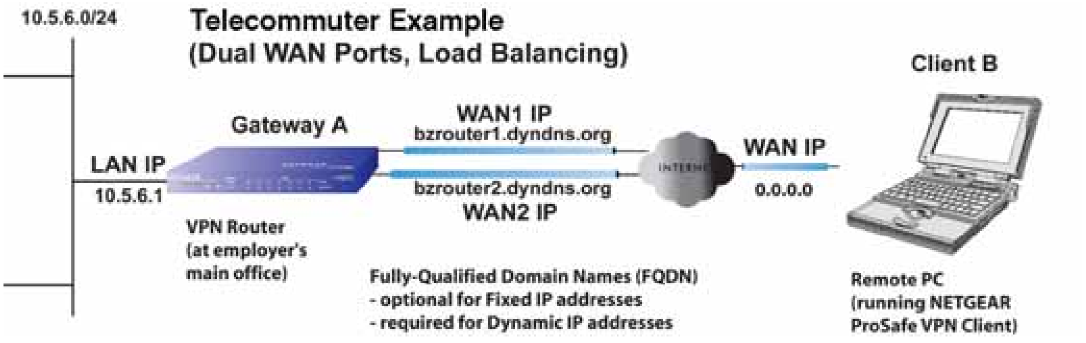


Figure 24. Telecommuter example in a dual WAN port configuration with load balancing

The IP addresses of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, you must use an FQDN. If an IP address is fixed, an FQDN is optional.

VPN Gateway-to-Gateway

The following situations exemplify the requirements for a gateway VPN firewall to establish a VPN tunnel with another gateway VPN firewall:

- Single-gateway WAN ports
- Redundant dual-gateway WAN ports for increased reliability (before and after rollover)
- Dual-gateway WAN ports for load balancing

VPN Gateway-to-Gateway: Single-Gateway WAN Ports - Reference Case

In a configuration with two single WAN port gateways, either gateway WAN port can initiate the VPN tunnel with the other gateway WAN port because the IP addresses are known in advance.

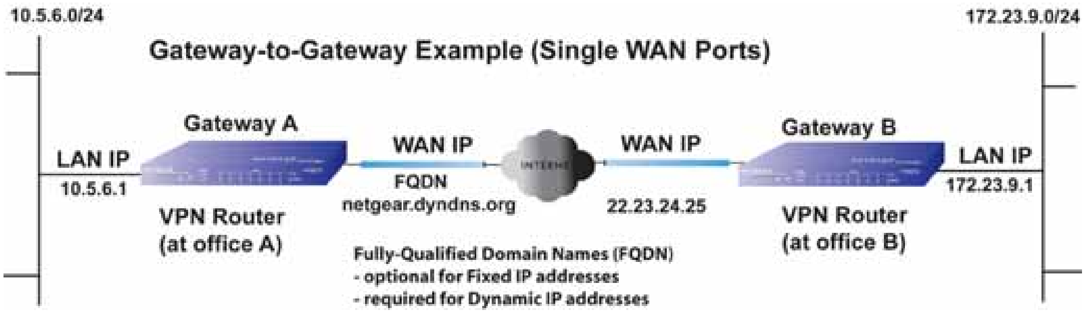


Figure 25. Gateway-to-gateway example in a single WAN port configuration

The IP address of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, you must use an FQDN. If an IP address is fixed, an FQDN is optional.

VPN Gateway-to-Gateway: Dual-Gateway WAN Ports for Improved Reliability

In a configuration with two dual WAN port VPN gateways that function in auto-rollover mode, either of the gateway WAN ports at one end can initiate the VPN tunnel with the appropriate gateway WAN port at the other end as necessary to balance the loads of the gateway WAN ports because the IP addresses of the WAN ports are known in advance. In this example (see the following figure), port WAN_A1 is active and port WAN_A2 is inactive at Gateway A; port WAN_B1 is active and port WAN_B2 is inactive at Gateway B.

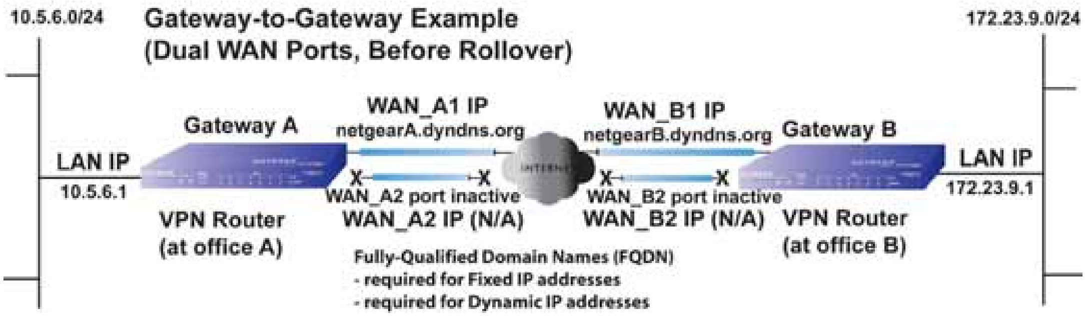


Figure 26. Gateway-to-gateway example in a dual WAN port configuration before auto-rollover

The IP addresses of the gateway WAN ports can be either fixed or dynamic, but you must always use an FQDN because the active WAN ports could be either WAN_A1, WAN_A2, WAN_B1, or WAN_B2 (that is, the IP address of the active WAN ports is not known in advance).

After a rollover of a gateway WAN port, the previously inactive gateway WAN port becomes the active port (port WAN_A2 in the following figure) and one of the gateways must reestablish the VPN tunnel.

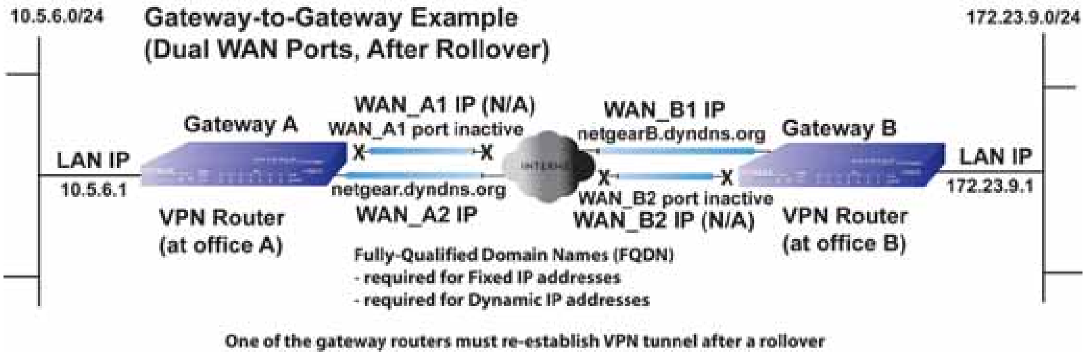


Figure 27. Gateway-to-gateway example in a dual WAN port configuration after auto-rollover

The purpose of the FQDNs is to toggle the domain name of the rolled-over gateway between the IP addresses of the active WAN port (that is, WAN_A1 and WAN_A2 in the previous figure) so that the other end of the tunnel has a known gateway IP address to establish or reestablish a VPN tunnel.

VPN Gateway-to-Gateway: Dual-Gateway WAN Ports for Load Balancing

In a configuration with two dual-WAN port VPN gateways that function in load balancing mode, either of the gateway WAN ports at one end can be programmed in advance to initiate the VPN tunnel with the appropriate gateway WAN port at the other end as necessary to manage the loads of the gateway WAN ports because the IP addresses of the WAN ports are known in advance.

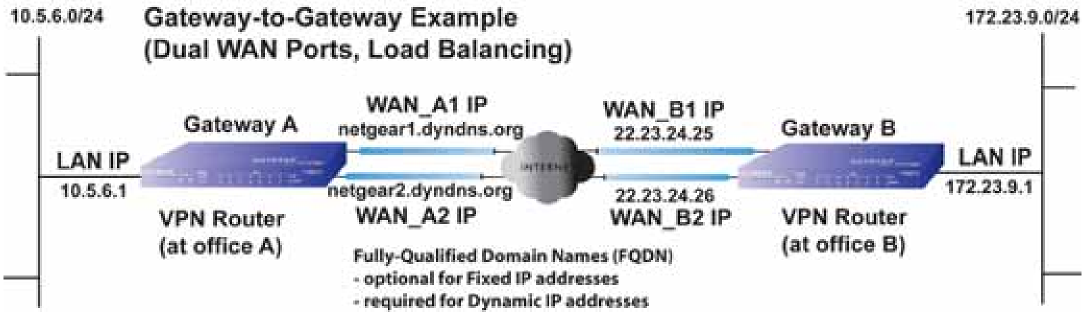


Figure 28. Gateway-to-gateway example in a dual WAN port configuration with load balancing

The IP addresses of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, you must use an FQDN. If an IP address is fixed, an FQDN is optional.

VPN Telecommuter - Client-to-Gateway Through a NAT Router

Note: The telecommuter case presumes that the home office has a dynamic IP address and NAT router.

The following situations exemplify the requirements for a remote computer client connected to the Internet with a dynamic IP address through a NAT router to establish a VPN tunnel with a gateway VPN firewall at the company office:

- Single-gateway WAN port
- Redundant dual-gateway WAN ports for increased reliability (before and after rollover)
- Dual-gateway WAN ports for load balancing

VPN Telecommuter: Single-Gateway WAN Port - Reference Case

In a single WAN port gateway configuration, the remote computer client at the NAT router initiates the VPN tunnel because the IP address of the remote NAT router is not known in advance. The gateway WAN port must act as the responder.

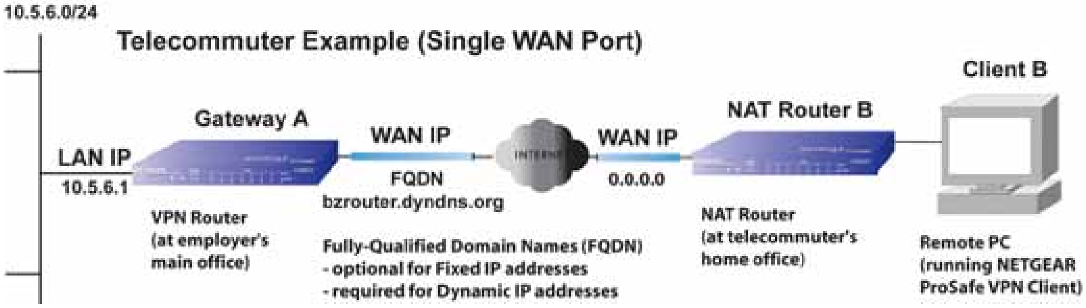


Figure 29. Telecommuter example in a single WAN port configuration with NAT

The IP address of the gateway WAN port can be either fixed or dynamic. If the IP address is dynamic, you must use an FQDN. If the IP address is fixed, an FQDN is optional.

VPN Telecommuter: Dual-Gateway WAN Ports for Improved Reliability

In a gateway configuration with dual WAN ports that function in auto-rollover mode, the remote computer client initiates the VPN tunnel with the active gateway WAN port (port WAN1 in the following figure) because the IP address of the remote NAT router is not known in advance. The gateway WAN port must act as the responder.

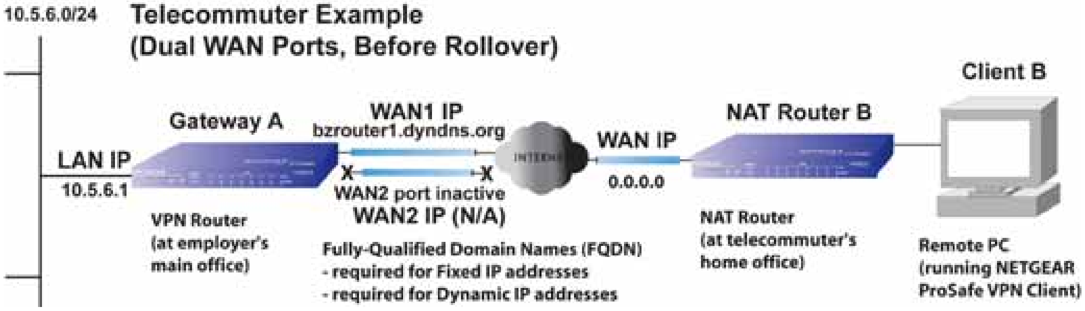


Figure 30. Telecommuter example in a dual WAN port configuration with NAT before auto-rollover

The IP addresses of the gateway WAN ports can be either fixed or dynamic, but you must always use an FQDN because the active WAN port could be either WAN1 or WAN2 (that is, the IP address of the active WAN port is not known in advance).

After a rollover of the WAN port occurs, the previously inactive gateway WAN port becomes the active port (port WAN2 in the following figure) and the remote computer must reestablish the VPN tunnel. The gateway WAN port must act as the responder.

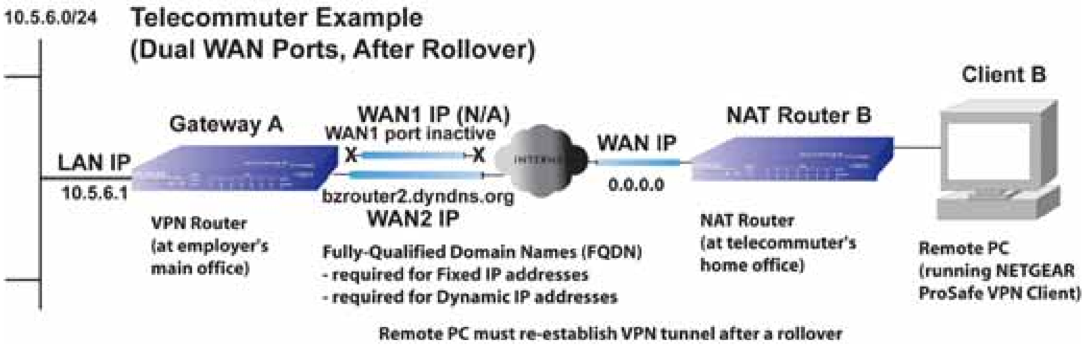


Figure 31. Telecommuter example in a dual WAN port configuration with NAT after auto-rollover

The purpose of the FQDN is to toggle the domain name of the gateway between the IP addresses of the active WAN port (that is, WAN1 and WAN2) so that the remote computer client can determine the gateway IP address to establish or reestablish a VPN tunnel.

VPN Telecommuter: Dual-Gateway WAN Ports for Load Balancing

In a gateway configuration with dual WAN ports that function in load balancing mode, the remote computer client initiates the VPN tunnel with the appropriate gateway WAN port (that is, port WAN1 or WAN2 as necessary to balance the loads of the two gateway WAN ports) because the IP address of the remote NAT router is not known in advance. The selected gateway WAN port must act as the responder.

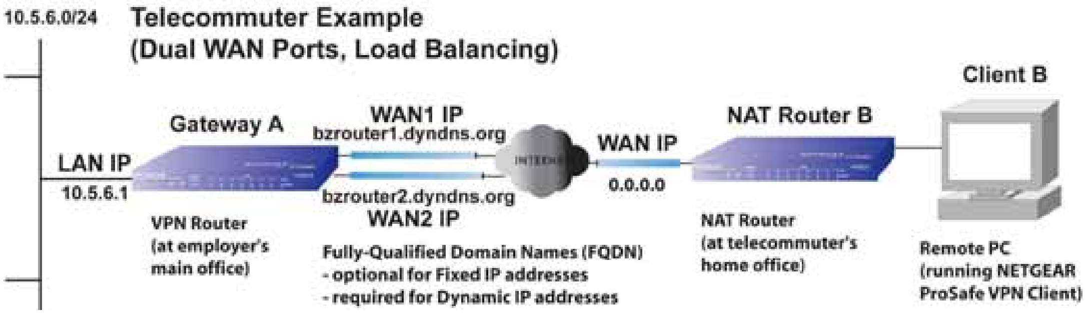


Figure 32. Telecommuter example in a dual WAN port configuration with NAT and load balancing

The IP addresses of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, you must use an FQDN. If an IP address is fixed, an FQDN is optional.

B. System Logs and Error Messages

B

This appendix provides examples and explanations of system logs and error message. When applicable, a recommended action is provided.

This appendix contains the following sections:

Log Message Terms

This appendix uses the following log message terms.

Table 13. Log message terms

Term	Description
[FVS336Gv2]	System identifier.
[kernel]	Message from the kernel.
CODE	Protocol code (for example, protocol is ICMP, type 8) and CODE=0 means successful reply.
DEST	Destination IP address of the machine to which the packet is destined.
DPT	Destination port.
IN	Incoming interface for packet.
OUT	Outgoing interface for packet.
PROTO	Protocol used.
SELF	Packet coming from the system only.
SPT	Source port.
SRC	Source IP address of machine from which the packet is coming.
TYPE	Protocol type.

System Log Messages

The following sections provide information about system log messages:

- *NTP*
- *Login and Logout*
- *System Startup*
- *Reboot*
- *Firewall Restart*
- *IPSec Restart*
- *Unicast, Multicast, and Broadcast Logs*
- *WAN Status*
- *Resolved DNS Names*
- *VPN Log Messages*
- *Traffic Meter Logs*

These sections describe log messages that belong to one of the following categories:

- Logs generated by traffic that is meant for the VPN firewall.
- Logs generated by traffic that is routed or forwarded through the VPN firewall.
- Logs generated by system daemons, the NTP daemon, the WAN daemon, and other daemons.

For information about how to select many of these logs, see *Manage Logging, Alerts, and Event Notifications* on page 567.

NTP

This section describes log messages generated by the NTP daemon during synchronization with the NTP server.

Table 14. System logs: NTP

Message	Nov 28 12:31:13 [FVS336Gv2] [ntpdate] Looking Up time-f.netgear.com Nov 28 12:31:13 [FVS336Gv2] [ntpdate] Requesting time from time-f.netgear.com Nov 28 12:31:14 [FVS336Gv2] [ntpdate] Adjust time server 69.25.106.19 offset 0.140254 sec Nov 28 12:31:14 [FVS336Gv2] [ntpdate] Synchronized time with time-f.netgear.com Nov 28 12:31:16 [FVS336Gv2] [ntpdate] Date and Time Before Synchronization: Tue Nov 28 12:31:13 GMT+0530 2006 Nov 28 12:31:16 [FVS336Gv2] [ntpdate] Date and Time After Synchronization: Tue Nov 28 12:31:16 GMT+0530 2006 Nov 28 12:31:16 [FVS336Gv2] [ntpdate] Next Synchronization after 2 Hours
Explanation	Message 1: DNS resolution for the NTP server (time-f.netgear.com). Message 2: Request for NTP update from the time server. Message 3: Adjust time by resetting system time. Message 4: Display date and time before synchronization, that is, when resynchronization started. Message 5: Display the new updated date and time. Message 6: Next synchronization will be after the specified time. Example: In these logs the next synchronization will be after two hours. The synchronization time interval is configurable through the CLI.
Recommended action	None

Login and Logout

This section describes logs generated by the administrative interfaces of the device.

Table 15. System logs: login and logout

Message	Nov 28 14:45:42 [FVS336Gv2] [login] Login succeeded: user admin from 192.168.10.10
Explanation	Login of user admin from host with IP address 192.168.10.10.

Table 15. System logs: login and logout (continued)

Recommended action	None
Message	Nov 28 14:55:09 [FVS336Gv2] [seclogin] Logout succeeded for user admin Nov 28 14:55:13 [FVS336Gv2] [seclogin] Login succeeded: user admin from 192.168.1.214
Explanation	Secure login or logout of user admin from host with IP address 192.168.1.214.
Recommended action	None

System Startup

This section describes the log message generated during system startup.

Table 16. System logs: system startup

Message	Jan 1 15:22:28 [FVS336Gv2] [ledTog] [SYSTEM START-UP] System Started
Explanation	Log generated when the system is started.
Recommended action	None

Reboot

This section describes the log message generated during system reboot.

Table 17. System logs: reboot

Message	Nov 25 19:42:57 [FVS336Gv2] [reboot] Rebooting in 3 seconds
Explanation	Log generated when the system is rebooted from the web management interface.
Recommended action	None

Firewall Restart

This section describes logs that are generated when the VPN firewall restarts.

Table 18. System logs: VPN firewall restart

Message	Jan 23 16:20:44 [FVS336Gv2] [wand] [FW] Firewall Restarted
Explanation	Log generated when the VPN firewall is restarted. This message is logged when the VPN firewall restarts after any changes in the configuration are applied.
Recommended action	None

IPSec Restart

This section describes logs that are generated when IPSec restarts.

Table 19. System logs: IPSec restart

Message	Jan 23 16:20:44 [FVS336Gv2] [wand] [IPSEC] IPSEC Restarted
Explanation	Log generated when the IPSec is restarted. This message is logged when IPSec restarts after any changes in the configuration are applied.
Recommended action	None

Unicast, Multicast, and Broadcast Logs

Table 20. System logs: unicast

Message	Nov 24 11:52:55 [FVS336Gv2] [kernel] UCAST IN=SELF OUT=WAN SRC= 192.168.10.1 DST=192.168.10.10 PROTO=UDP SPT=800 DPT=2049
Explanation	• This packet (unicast) is sent to the device from the WAN network. • For other settings, see *Table 13* on page 642.
Recommended action	None

ICMP Redirect Logs

Table 21. System logs: unicast, redirect

Message	Feb 2007 22 14:36:07 [FVS336Gv2] [kernel] [LOG_PACKET] SRC=192.168.1.49 DST=192.168.1.124 PROTO=ICMP TYPE=5 CODE=1
Explanation	This packet is an ICMP redirect message sent to the device by another device. For other settings, see *Table 13* on page 642.

Recommended action	To enable these logs, from the CLI command prompt of the VPN firewall, enter this command:
	`monitor/firewallLogs/logger/loggerConfig logIcmpRedirect 1`
	And to disable it enter:
	`monitor/firewallLogs/logger/loggerConfig logIcmpRedirect 0`

Multicast and Broadcast Logs

Table 22. System logs: multicast and broadcast

Message	Jan 1 07:24:13 [FVS336Gv2] [kernel] MCAST-BCAST IN=WAN OUT=SELF SRC= 192.168.1.73 DST=192.168.1.255 PROTO=UDP SPT=138 DPT=138
Explanation	• This multicast or broadcast packet is sent to the device from the WAN network. • For other settings, see *Table 13* on page 642.
Recommended action	None

WAN Status

This section describes the logs generated by the WAN component. If you have several ISP links for Internet connectivity, you can configure the VPN firewall either in auto-rollover or load balancing mode.

- *Load Balancing*
- *Auto-Rollover*

Load Balancing

When the WAN mode is configured for load balancing, all the WAN ports are active simultaneously and the traffic is balanced between them. If one WAN link goes down, all the traffic is diverted to the other WAN links that are active.

This section describes the logs generated when the WAN mode is set to load balancing.

Table 23. System logs: WAN status, load balancing

Message	Dec 1 12:11:27 [FVS336Gv2] [wand] [LBFO] Restarting WAN1_ Dec 1 12:11:31 [FVS336Gv2] [wand] [LBFO] Restarting WAN2_ Dec 1 12:11:35 [FVS336Gv2] [wand] [LBFO] WAN1(UP), WAN2(UP)_ Dec 1 12:24:12 [FVS336Gv2] [wand] [LBFO] WAN1(UP), WAN2(DOWN)_ Dec 1 12:29:43 [FVS336Gv2] [wand] [LBFO] Restarting WAN2_ Dec 1 12:29:47 [FVS336Gv2] [wand] [LBFO] WAN1(UP), WAN2(DOWN)_
Explanation	Message 1 and Message 2 indicate that both the WANs are restarted. Message 3: This message shows that both the WANs are up and the traffic is balanced between the two WAN interfaces. Messages 4, 5, and 6: These messages show that one of the WAN links is down and that restarting the WAN link does not resolve the situation. At this point, all the traffic is directed through the WAN that is up.
Recommended action	None

Auto-Rollover

When the WAN mode is configured for auto-rollover, the primary link is active and the secondary link acts only as a backup. When the primary link goes down, the secondary link becomes active only until the primary link comes back up. The VPN firewall monitors the status of the primary link using the configured WAN failure detection method.

This section describes the logs generated when the WAN mode is set to auto-rollover.

Table 24. System logs: WAN status, auto-rollover

Message	Nov 17 09:59:09 [FVS336Gv2] [wand] [LBFO] WAN1 Test Failed 1 of 3 times_ Nov 17 09:59:39 [FVS336Gv2] [wand] [LBFO] WAN1 Test Failed 2 of 3 times_ Nov 17 10:00:09 [FVS336Gv2] [wand] [LBFO] WAN1 Test Failed 3 of 3 times_ Nov 17 10:01:01 [FVS336Gv2] [wand] [LBFO] WAN1 Test Failed 4 of 3 times_ Nov 17 10:01:35 [FVS336Gv2] [wand] [LBFO] WAN1 Test Failed 5 of 3 times_ Nov 17 10:01:35 [FVS336Gv2] [wand] [LBFO] WAN1(DOWN), WAN2(UP), ACTIVE(WAN2)_ Nov 17 10:02:25 [FVS336Gv2] [wand] [LBFO] WAN1 Test Failed 6 of 3 times_ Nov 17 10:02:25 [FVS336Gv2] [wand] [LBFO] Restarting WAN1_ Nov 17 10:02:57 [FVS336Gv2] [wand] [LBFO] WAN1 Test Failed 7 of 3 times_ Nov 17 10:03:27 [FVS336Gv2] [wand] [LBFO] WAN1 Test Failed 8 of 3 times_ Nov 17 10:03:57 [FVS336Gv2] [wand] [LBFO] WAN1 Test Failed 9 of 3 times_ Nov 17 10:03:57 [FVS336Gv2] [wand] [LBFO] Restarting WAN1_
Explanation	The logs suggest that the failover was detected after 5 attempts instead of 3. However, the reason that the messages appear in the log is because of the WAN state transition logic, which is part of the failover algorithm. These logs can be interpreted as follows: The primary link failure is correctly detected after the third attempt. Thereafter, the algorithm attempts to restart the WAN connection and checks once again to determine if WAN1 is still down. This results in the fourth failure detection message. If it is still down, then it starts a secondary link, and once the secondary link is up, the secondary link is marked as active. Meanwhile, the primary link has failed once more, and that results in the fifth failure detection message. Note that the fifth failure detection message and the message suggesting that the secondary link is active have the same time stamp, and so they happen in the same algorithm state–machine cycle. So although it appears that the failover did not happen immediately after 3 failures, internally, the failover process is triggered after the third failure, and transition to the secondary link is completed by the fifth failure. The primary link is also restarted every 3 failures till it is functional again. In these logs, the primary link was restarted after the sixth failure, that is, 3 failures after the failover process was triggered.
Recommended action	Check the WAN settings and WAN failure detection method configured for the primary link.

PPP Logs

This section describes the WAN PPP connection logs. The PPP type can be configured from the web management interface (see *Manually Configure a PPPoE IPv4 Internet Connection* on page 39).

- PPPoE idle time-out logs

Table 25. System logs: WAN status, PPPoE idle time-out

Message	Nov 29 13:12:46 [FVS336Gv2] [pppd] Starting connection Nov 29 13:12:49 [FVS336Gv2] [pppd] Remote message: Success Nov 29 13:12:49 [FVS336Gv2] [pppd] PAP authentication succeeded Nov 29 13:12:49 [FVS336Gv2] [pppd] local IP address 50.0.0.62 Nov 29 13:12:49 [FVS336Gv2] [pppd] remote IP address 50.0.0.1 Nov 29 13:12:49 [FVS336Gv2] [pppd] primary DNS address 202.153.32.3 Nov 29 13:12:49 [FVS336Gv2] [pppd] secondary DNS address 202.153.32.3 Nov 29 11:29:26 [FVS336Gv2] [pppd] Terminating connection due to lack of activity. Nov 29 11:29:28 [FVS336Gv2] [pppd] Connect time 8.2 minutes. Nov 29 11:29:28 [FVS336Gv2] [pppd] Sent 1408 bytes, received 0 bytes. Nov 29 11:29:29 [FVS336Gv2] [pppd] Connection terminated.
Explanation	Message 1: PPPoE connection started. Message 2: Message from PPPoE server for correct login. Message 3: Authentication for PPP succeeded. Message 4: Local IP address assigned by the server. Message 5: Server side IP address. Message 6: The primary DNS server that is configured on the WAN ISP Settings screen. Message 7: The secondary DNS server that is configured on the WAN ISP Settings screen. Message 8: The PPP link has transitioned to idle mode. This event occurs if there is no traffic from the LAN network. Message 9: The time in minutes for which the link is up. Message 10: Data sent and received at the LAN side while the link was up. Message 11: PPP connection terminated after idle time-out.
Recommended action	To reconnect during idle mode, initiate traffic from the LAN side.

- PPTP idle time-out logs

Table 26. System logs: WAN status, PPTP idle time-out

Message	Nov 29 11:19:02 [FVS336Gv2] [pppd] Starting connection Nov 29 11:19:05 [FVS336Gv2] [pppd] CHAP authentication succeeded Nov 29 11:19:05 [FVS336Gv2] [pppd] local IP address 192.168.200.214 Nov 29 11:19:05 [FVS336Gv2] [pppd] remote IP address 192.168.200.1 Nov 29 11:19:05 [FVS336Gv2] [pppd] primary DNS address 202.153.32.2 Nov 29 11:19:05 [FVS336Gv2] [pppd] secondary DNS address 202.153.32.2 Nov 29 11:20:45 [FVS336Gv2] [pppd] No response to 10 echo-requests Nov 29 11:20:45 [FVS336Gv2] [pppd] Serial link appears to be disconnected. Nov 29 11:20:45 [FVS336Gv2] [pppd] Connect time 1.7 minutes. Nov 29 11:20:45 [FVS336Gv2] [pppd] Sent 520 bytes, received 80 bytes. Nov 29 11:20:51 [FVS336Gv2] [pppd] Connection terminated.
Explanation	Message 1: Starting PPP connection process. Message 2: Message from the server for authentication success. Message 3: Local IP address assigned by the server. Message 4: Server side IP address. Message 6: The primary DNS server that is configured on the WAN ISP Settings screen. Message 7: The secondary DNS server that is configured on the WAN ISP Settings screen. Message 7: Sensing idle link. Message 8: Idle link sensed. Message 9: Data sent and received at the LAN side while the link was up. Message 10: PPP connection terminated after idle time-out.
Recommended action	To reconnect during idle mode, initiate traffic from the LAN side.

- PPP authentication logs

Table 27. System logs: WAN status, PPP authentication

Message	Nov 29 11:29:26 [FVS336Gv2] [pppd] Starting link Nov 29 11:29:29 [FVS336Gv2] [pppd] Remote message: Login incorrect Nov 29 11:29:29 [FVS336Gv2] [pppd] PAP authentication failed Nov 29 11:29:29 [FVS336Gv2] [pppd] Connection terminated.WAN2(DOWN)_
Explanation	Starting link: Starting PPPoE connection process. Remote message: Login incorrect: Message from PPPoE server for incorrect login. PAP authentication failed: PPP authentication failed due to incorrect login. Connection terminated: PPP connection terminated.
Recommended action	If authentication fails, then check the login and password and enter the correct one.

Resolved DNS Names

This section describes the logs of DNS name resolution messages.

Table 28. System logs: DNS name resolution messages

Message	2000 Jan 1 05:12:00 [FVS336Gv2] [dnsmasq] [DNSRESOLV]:teamf1.com from 192.168.11.2
Explanation	This log is generated when the DNS name (that is, teamf1) is resolved.
Recommended action	None

VPN Log Messages

This section explains logs that are generated by IPSec VPN and SSL VPN policies. These logs are generated automatically and do not need to be enabled.

- *IPSec VPN Logs*
- *SSL VPN Logs*

IPSec VPN Logs

This section describes the log messages generated by IPSec VPN policies.

Note: The same IPSec VPN log messages can appear in the logs that are accessible when you select the **VPN** check box on the Firewall Logs & E-mail screen (see *Manage Logging, Alerts, and Event Notifications* on page 567) and in the logs on the IPSec VPN Logs screen (see *View the VPN Logs* on page 593).

Table 29. System logs: IPSec VPN tunnel, tunnel establishment

Messages 1 through 5	2000 Jan 1 04:01:39 [FVS336Gv2] [wand] [IPSEC] IPSEC Restarted 2000 Jan 1 04:02:09 [FVS336Gv2] [wand] [FW] Firewall Restarted 2000 Jan 1 04:02:29 [FVS336Gv2] [IKE] IKE stopped_ 2000 Jan 1 04:02:31 [FVS336Gv2] [IKE] IKE started_ 2000 Jan 1 04:02:31 [FVS336Gv2] [wand] [IPSEC] IPSEC Restarted
Messages 6 and 7	2000 Jan 1 04:07:04 [FVS336Gv2] [IKE] Adding IPSec configuration with identifier "pol1"_ 2000 Jan 1 04:07:04 [FVS336Gv2] [IKE] Adding IKE configuration with identifier "pol1"_
Messages 8 through 19	2000 Jan 1 04:13:39 [FVS336Gv2] [IKE] Configuration found for 20.0.0.1[500]._ 2000 Jan 1 04:13:39 [FVS336Gv2] [IKE] Received request for new phase 1 negotiation: 20.0.0.2[500]<=>20.0.0.1[500]_ 2000 Jan 1 04:13:39 [FVS336Gv2] [IKE] Beginning Identity Protection mode._ 2000 Jan 1 04:13:39 [FVS336Gv2] [IKE] Received Vendor ID: RFC XXXX_ 2000 Jan 1 04:13:39 [FVS336Gv2] [IKE] Received Vendor ID: DPD_ 2000 Jan 1 04:13:39 [FVS336Gv2] [IKE] DPD is Enabled_ 2000 Jan 1 04:13:39 [FVS336Gv2] [IKE] For 20.0.0.1[500], Selected NAT-T version: RFC XXXX_ 2000 Jan 1 04:13:39 [FVS336Gv2] [IKE] Setting DPD Vendor ID_ 2000 Jan 1 04:13:39 [FVS336Gv2] [IKE] Received Vendor ID: KAME/racoon_ 2000 Jan 1 04:13:39 [FVS336Gv2] [IKE] NAT-D payload matches for 20.0.0.2[500]_ 2000 Jan 1 04:13:39 [FVS336Gv2] [IKE] NAT-D payload matches for 20.0.0.1[500]_
Messages 20 and 21	2000 Jan 1 04:13:39 [FVS336Gv2] [IKE] NAT not detected _ 2000 Jan 1 04:13:39 [FVS336Gv2] [IKE] ISAKMP-SA established for 20.0.0.2[500]-20.0.0.1[500] with spi:c56f7a1d42baf28a:68fcf85e3c148bd8_ 2000 Jan 1 04:13:39 [FVS336Gv2] [IKE] Sending Informational Exchange: notify payload[INITIAL-CONTACT]_
Messages 22 and 23	2000 Jan 1 04:13:40 [FVS336Gv2] [IKE] Responding to new phase 2 negotiation: 20.0.0.2[0]<=>20.0.0.1[0]_ 2000 Jan 1 04:13:40 [FVS336Gv2] [IKE] Using IPSec SA configuration: 192.168.11.0/24<->192.168.10.0/24_
Messages 24 and 25	2000 Jan 1 04:13:41 [FVS336Gv2] [IKE] IPSec-SA established: ESP/Tunnel 20.0.0.1->20.0.0.2 with spi=34046092(0x207808c)_ 2000 Jan 1 04:13:41 [FVS336Gv2] [IKE] IPSec-SA established: ESP/Tunnel 20.0.0.2->20.0.0.1 with spi=87179451(0x53240bb)_
Explanation	Message 1–5: IPSec, IKE, and VPN firewall restart. Message 6–7: IPSec and IKE configurations are added with the identifier “pol1.” Message 8–19: New phase 1 negotiation starts by determining the configuration for the WAN host. Dead Peer Detection (DPD) is enabled and set. NAT payload matching and NAT detection are done. Message 20–21: ISAKMP-SA is established between the two WANs and information is exchanged. Message 22–23: New phase 2 negotiation starts by using IPSec SA configuration pertaining to the LAN hosts. Message 24–25: IPSec-SA VPN tunnel is established.

Table 29. System logs: IPSec VPN tunnel, tunnel establishment (continued)

Recommended action	None

Table 30. System logs: IPSec VPN tunnel, SA lifetime (150 sec in phase 1; 300 sec in phase 2), VPN tunnel is reestablished

Message 1	2000 Jan 1 04:32:25 [FVS336Gv2] [IKE] Sending Informational Exchange: delete payload[]_
Messages 2 through 6	2000 Jan 1 04:32:25 [FVS336Gv2] [IKE] purged IPSec-SA proto_id=ESP spi= 181708762._ 2000 Jan 1 04:32:25 [FVS336Gv2] [IKE] purged IPSec-SA proto_id=ESP spi= 153677140._ 2000 Jan 1 04:32:25 [FVS336Gv2] [IKE] an undead schedule has been deleted: 'pk_recvupdate'._ 2000 Jan 1 04:32:25 [FVS336Gv2] [IKE] IPSec configuration with identifier "pol1" deleted successfully_ 2000 Jan 1 04:32:25 [FVS336Gv2] [IKE] no phase 2 bounded._
Message 7	2000 Jan 1 04:32:25 [FVS336Gv2] [IKE] Sending Informational Exchange: delete payload[]_
Messages 8 through 11	2000 Jan 1 04:32:25 [FVS336Gv2] [IKE] Purged ISAKMP-SA with spi= d67f2be9ca0cb241:8a094623c6811286._ 2000 Jan 1 04:32:25 [FVS336Gv2] [IKE] an undead schedule has been deleted: 'purge_remote'._ 2000 Jan 1 04:32:25 [FVS336Gv2] [IKE] IKE configuration with identifier "pol1" deleted successfully_ 2000 Jan 1 04:32:25 [FVS336Gv2] [IKE] Could not find configuration for 20.0.0.1[500]_
Explanation	Message 1: Informational exchange for deleting the payload. Message 2–6: Phase 2 configuration is purged and confirms that no phase 2 is bounded. Message 7: Informational exchange for deleting the payload. Message 8–11: Phase 1 configuration. The VPN tunnel is reestablished.
Recommended action	None

Table 31. System logs: IPSec VPN tunnel, SA lifetime (150 sec in phase 1; 300 sec in phase 2), VPN tunnel not reestablished

Message	2000 Jan 1 04:52:33 [FVS336Gv2] [IKE] Using IPSec SA configuration: 192.168.11.0/24<->192.168.10.0/24_ 2000 Jan 1 04:52:33 [FVS336Gv2] [IKE] Configuration found for 20.0.0.1._ 2000 Jan 1 04:52:59 [FVS336Gv2] [IKE] Phase 1 negotiation failed due to time up for 20.0.0.1[500]. b73efd188399b7f2:0000000000000000_ 2000 Jan 1 04:53:04 [FVS336Gv2] [IKE] Phase 2 negotiation failed due to time up waiting for phase 1. ESP 20.0.0.1->20.0.0.2 _ 2000 Jan 1 04:53:05 [FVS336Gv2] [IKE] Using IPSec SA configuration: 192.168.11.0/24<->192.168.10.0/24_ 2000 Jan 1 04:53:05 [FVS336Gv2] [IKE] Configuration found for 20.0.0.1._ 2000 Jan 1 04:53:05 [FVS336Gv2] [IKE] Initiating new phase 1 negotiation: 20.0.0.2[500]<=>20.0.0.1[500]_ 2000 Jan 1 04:53:05 [FVS336Gv2] [IKE] Beginning Identity Protection mode._ 2000 Jan 1 04:53:05 [FVS336Gv2] [IKE] Setting DPD Vendor ID_ 2000 Jan 1 04:53:36 [FVS336Gv2] [IKE] Phase 2 negotiation failed due to time up waiting for phase 1. ESP 20.0.0.1->20.0.0.2 _
Explanation	Phase 1 and phase 2 negotiations failed because of a mismatch of the WAN IP address in the IPSec VPN policy and the WAN IP address of the remote host attempting to establish the IPSec VPN tunnel.
Recommended action	None

Table 32. System logs: IPSec VPN tunnel, Dead Peer Detection and keep-alive (default 30 sec)

Messages 1 through 4	2000 Jan 1 04:13:39 [FVS336Gv2] [IKE] Received request for new phase 1 negotiation: 20.0.0.2[500]<=>20.0.0.1[500]_ 2000 Jan 1 04:13:39 [FVS336Gv2] [IKE] Beginning Identity Protection mode._ 2000 Jan 1 04:13:39 [FVS336Gv2] [IKE] Received Vendor ID: RFC XXXX_ 2000 Jan 1 04:13:39 [FVS336Gv2] [IKE] Received Vendor ID: DPD_
Message 5	2000 Jan 1 04:13:39 [FVS336Gv2] [IKE] DPD is Enabled_
Message 6	2000 Jan 1 04:13:39 [FVS336Gv2] [IKE] For 20.0.0.1[500], Selected NAT-T version: RFC XXXX_
Message 7	2000 Jan 1 04:13:39 [FVS336Gv2] [IKE] Setting DPD Vendor ID_
Explanation	Message 1–4: After receiving a request for phase 1 negotiation, a Dead Peer Detection vendor ID is received. Message 5: DPD is enabled. Message 7: The DPD vendor ID is set.
Recommended action	None

Table 33. System logs: IPSec VPN tunnel, Dead Peer Detection and keep-alive (default 30 sec), VPN tunnel torn down

Message 1	2000 Jan 1 06:01:18 [FVS336Gv2] [VPNKA] Keep alive to peer 192.168.10.2 failed 3 consecutive times and 5 times cumulative_
Message 2	2000 Jan 1 06:01:19 [FVS336Gv2] [IKE] DPD R-U-THERE sent to "20.0.0.1[500]"_
Message 3	2000 Jan 1 06:01:19 [FVS336Gv2] [IKE] DPD R-U-THERE-ACK received from "20.0.0.1[500]"_
Explanation	Message 1: When the remote host connection is removed and when there are no packets from the remote host, the VPN firewall sends packets to keep the remote host alive. As the connection itself is removed, keep-alive fails. Message 2: The VPN firewall sends packets to check whether the peer is dead. Message 3: The VPN firewall receives an acknowledgment that the peer is dead. The connection is removed.
Recommended action	None

Table 34. System logs: IPSec VPN tunnel, client policy, disconnection from the client side

Message	2000 Jan 1 02:34:45 [FVS336Gv2] [IKE] Deleting generated policy for 20.0.0.1[0]_ 2000 Jan 1 02:34:45 [FVS336Gv2] [IKE] an undead schedule has been deleted: 'pk_recvupdate'._ 2000 Jan 1 02:34:45 [FVS336Gv2] [IKE] Purged IPSec-SA with proto_id=ESP and spi=3000608295(0xb2d9a627)._ 2000 Jan 1 02:34:45 [FVS336Gv2] [IKE] Purged IPSec-SA with proto_id=ESP and spi=248146076(0xeca689c)._ 2000 Jan 1 02:34:45 [FVS336Gv2] [IKE] Purged ISAKMP-SA with proto_id= ISAKMP and spi=da1f2efbf0635943:4eb6fae677b2e4f4._ 2000 Jan 1 02:34:46 [FVS336Gv2] [IKE] ISAKMP-SA deleted for 20.0.0.2[500]-20.0.0.1[500] with spi:da1f2efbf0635943:4eb6fae677b2e4f4_
Explanation	Phase 2 and phase 1 policies are deleted when the client is disconnected.
Recommended action	None

Table 35. System logs: IPSec VPN tunnel, client policy behind a NAT device

Message 3	2000 Jan 1 01:54:21 [FVS336Gv2] [IKE] Floating ports for NAT-T with peer 20.0.0.1[4500]_ 2000 Jan 1 01:54:21 [FVS336Gv2] [IKE] NAT-D payload matches for 20.0.0.2[4500]_ 2000 Jan 1 01:54:21 [FVS336Gv2] [IKE] NAT-D payload does not match for 20.0.0.1[4500]_ 2000 Jan 1 01:54:21 [FVS336Gv2] [IKE] Ignore REPLAY-STATUS notification from 20.0.0.1[4500]._ 2000 Jan 1 01:54:21 [FVS336Gv2] [IKE] Ignore INITIAL-CONTACT notification from 20.0.0.1[4500] because it is only accepted after phase 1._
Message 6	2000 Jan 1 01:54:21 [FVS336Gv2] [IKE] NAT detected: Peer is behind a NAT device_
Explanation	These logs are generated when the remote WAN host is connected through a device such as the VPN firewall. NAT is detected before phase 1 is established. Message 3: NAT-D does not match the remote host. Message 6: The VPN firewall confirms that the remote host or the peer is behind a NAT device.
Recommended action	None

SSL VPN Logs

This section describes the log messages that are generated by SSL VPN policies.

Table 36. System logs: SSL VPN tunnel, WAN host and interface

Message	2000 Jan 1 03:44:55 [FVS336Gv2] [sslvpntunnel] id=FVS336Gv2 time="2000-1-1 3:44:55" fw=20.0.0.2 pri=6 rule=access-policy proto="SSL VPN Tunnel" src=20.0.0.1 user=sai dst=20.0.0.2 arg="" op="" result="" rcvd="" msg="SSL VPN Tunnel"
Explanation	An SSL VPN tunnel is established for ID FVS336Gv2 with the WAN host 20.0.0.1 through WAN interface 20.0.0.2 and logged in with the user name “sai.”
Recommended action	None

Table 37. System logs: VPN log messages, port forwarding, WAN host and interface

Message	2000 Jan 1 01:30:08 [FVS336Gv2] [portforwarding] id=FVS336Gv2 time="2000-1-1 1:30: 8" fw=20.0.0.2 pri=6 rule=access-policy proto="Port Forwarding" src=20.0.0.1 user=sai dst=20.0.0.2 arg="" op="" result="" rcvd="" msg="Port Forwarding"
Explanation	An SSL VPN tunnel through port forwarding is established for ID FVS336Gv2 with the WAN host 20.0.0.1 through WAN interface 20.0.0.2 and logged in with the user name “sai.”
Recommended action	None

Table 38. System logs: VPN log messages, port forwarding, LAN host and interface

Message	2000 Jan 1 01:35:41 [FVS336Gv2] [portforwarding] id=FVS336Gv2 time="2000-1-1 1:35:41" fw=192.168.11.1 pri=6 rule=access-policy proto="Virtual Transport (Java)" src=192.168.11.2 user=sai dst=192.168.11.1 arg= "" op="" result="" rcvd="" msg="Virtual Transport (Java)"
Explanation	An SSL VPN tunnel through port forwarding is established for ID FVS336Gv2 from the LAN host 192.168.11.2 with interface 192.168.11.1 and logged in with the user name “sai.”
Recommended action	None

Traffic Meter Logs

Table 39. System logs: traffic meter

Message	Jan 23 19:03:44 [TRAFFIC_METER] TRAFFIC_METER: Monthly Limit of 10 MB has reached for WAN1._
Explanation	Traffic limit to WAN1 that was set as 10 Mb is reached. This stops all the incoming and outgoing traffic, that is, if you selected the **Block All Traffic** radio button in the When Limit is Reached section on the WAN TrafficMeter screen.
Recommended action	To start the traffic, restart the traffic limit counter.

Routing Logs

The following sections provide information about routing log messages:

- *LAN to WAN Logs*
- *LAN to DMZ Logs*
- *DMZ to WAN Logs*
- *WAN to LAN Logs*
- *DMZ to LAN Logs*
- *WAN to DMZ Logs*

These sections explain the logging messages for the various network segments (such as LAN to WAN) for debugging purposes. These logs might generate a significant volume of messages.

LAN to WAN Logs

Table 40. Routing logs: LAN to WAN

Message	Nov 29 09:19:43 [FVS336Gv2] [kernel] LAN2WAN[ACCEPT] IN=LAN OUT=WAN SRC=192.168.10.10 DST=72.14.207.99 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from LAN to WAN is allowed by the firewall. • For other settings, see *Table 13* on page 642.
Recommended action	None

LAN to DMZ Logs

Table 41. Routing logs: LAN to DMZ

Message	Nov 29 09:44:06 [FVS336Gv2] [kernel] LAN2DMZ[ACCEPT] IN=LAN OUT=DMZ SRC=192.168.10.10 DST=192.168.20.10 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from LAN to DMZ is allowed by the firewall. • For other settings, see *Table 13* on page 642.
Recommended action	None

DMZ to WAN Logs

Table 42. Routing logs: DMZ to WAN

Message	Nov 29 09:19:43 [FVS336Gv2] [kernel] DMZ2WAN[DROP] IN=DMZ OUT=WAN SRC=192.168.20.10 DST=72.14.207.99 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from DMZ to WAN is dropped by the firewall. • For other settings, see *Table 13* on page 642.
Recommended action	None

WAN to LAN Logs

Table 43. Routing logs: WAN to LAN

Message	Nov 29 10:05:15 [FVS336Gv2] [kernel] WAN2LAN[ACCEPT] IN=WAN OUT=LAN SRC=192.168.1.214 DST=192.168.10.10 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from LAN to WAN is allowed by the firewall. • For other settings, see *Table 13* on page 642.
Recommended action	None

DMZ to LAN Logs

Table 44. Routing logs: DMZ to WAN

Message	Nov 29 09:44:06 [FVS336Gv2] [kernel] DMZ2LAN[DROP] IN=DMZ OUT=LAN SRC=192.168.20.10 DST=192.168.10.10 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from DMZ to LAN is dropped by the firewall. • For other settings, see *Table 13* on page 642.
Recommended action	None

WAN to DMZ Logs

Table 45. Routing logs: WAN to DMZ

Message	Nov 29 09:19:43 [FVS336Gv2] [kernel] WAN2DMZ[ACCEPT] IN=WAN OUT=DMZ SRC=192.168.1.214 DST=192.168.20.10 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from WAN to DMZ is allowed by the firewall. • For other settings, see *Table 13* on page 642.
Recommended action	None

Other Event Logs

The following sections provide information about other event messages:

- *Session Limit Logs*
- *Source MAC Filter Logs*
- *Bandwidth Limit Logs*

These sections describe the log messages generated by other events such source MAC filtering, session limiting, and bandwidth limiting. For information about how to select these logs, see *Manage Logging, Alerts, and Event Notifications* on page 567.

Session Limit Logs

Table 46. Other event logs: session limit logs

Message	2000 Jan 1 06:53:33 [FVS336Gv2] [kernel] SESS_LIMIT[DROP] IN=LAN OUT= WAN SRC=192.168.11.2 DST=20.0.0.1 PROTO=TCP SPT=50709 DPT=21
Explanation	When two FTP sessions are established from the same LAN host at IP address 192.168.11.2 and a session limit (SESS_LIMIT) is set as 1, the FTP packets from the second session are dropped.
Recommended action	Change the session limit to 2 to prevent packets from being dropped.

Source MAC Filter Logs

Table 47. Other event logs: source MAC filter logs

Message	2000 Jan 1 06:40:10 [FVS336Gv2] [kernel] SRC_MAC_MATCH[DROP] SRC MAC = 00:12:3f:34:41:14 IN=LAN OUT=WAN SRC=192.168.11.3 DST=209.85.153.103 PROTO=ICMP TYPE=8 CODE=0
Explanation	Because MAC address 00:12:3f:34:41:14 of LAN host with IP address 192.168.11.3 is filtered so that it cannot access the Internet, the packets sent by this MAC address to the Google server at address 09.85.153.103 are dropped.
Recommended action	Disable source MAC filtering.

Bandwidth Limit Logs

Table 48. Other event logs: bandwidth limit, outbound bandwidth profile

Message	2000 Jan 1 00:10:36 [FVS336Gv2] [kernel] [BW_LIMIT_DROP] IN=LAN OUT= WAN SRC=192.168.100.2 DST=22.0.0.2 PROTO=ICMP TYPE=144 CODE=145 TC_INDEX=10 CLASSID=10:5
Explanation	This log is generated when an outbound packet is dropped because the packet size exceeds the specified bandwidth limit.
Recommended action	Ensure that the packet size is within the specified bandwidth limit.

Table 49. Other event logs: bandwidth limit, inbound bandwidth profile

Message	2000 Jan 1 00:08:21 [FVS336Gv2] [kernel] [BW_LIMIT_DROP] IN=LAN OUT= WAN SRC=22.0.0.2 DST=192.168.100.2 PROTO=ICMP TYPE=112 CODE=113 TC_INDEX=10 CLASSID=10:2
Explanation	This log is generated when an inbound packet is dropped because the packet size exceeds the specified bandwidth limit.
Recommended action	Ensure that the packet size is within the specified bandwidth limit.

DHCP Logs

This section explains the log messages that are generated when a host is assigned a dynamic IP address. These messages are displayed on the DHCP Log screen (see *View the DHCP Log* on page 601).

Table 50. DHCP logs

Message 1	2000 Jan 1 07:27:28 [FVS336Gv2] [dhcpd] Listening on LPF/eth0.1/00:11:22:78:89:90/192.168.11/24
Message 2	2000 Jan 1 07:27:37 [FVS336Gv2] [dhcpd] DHCPRELEASE of 192.168.10.2 from 00:0f:1f:8f:7c:4a via eth0.1 (not found)
Message 3	2000 Jan 1 07:27:47 [FVS336Gv2] [dhcpd] DHCPDISCOVER from 00:0f:1f:8f:7c:4a via eth0.1
Message 4	2000 Jan 1 07:27:48 [FVS336Gv2] [dhcpd] DHCPOFFER on 192.168.11.2 to 00:0f:1f:8f:7c:4a via eth0.1
Message 5	2000 Jan 1 07:27:48 [FVS336Gv2] [dhcpd] Wrote 2 leases to leases file.
Message 6	2000 Jan 1 07:27:48 [FVS336Gv2] [dhcpd] DHCPREQUEST for 192.168.11.2 (192.168.11.1) from 00:0f:1f:8f:7c:4a via eth0.1
Message 7	2000 Jan 1 07:27:48 [FVS336Gv2] [dhcpd] DHCPACK on 192.168.11.2 to 00:0f:1f:8f:7c:4a via eth0.1
Explanation	Message 1: The DHCP server is listening on eth0.1. Message 2: Release of the currently assigned IP address from the host by the DHCP server. Message 3: DHCP broadcast by the host is discovered by the DHCP server. Message 4: The DHCP server offers a new IP address to the host’s current network interface. Message 5: Two new leases are written to the lease file. Message 6: DHCP is requested to assign the new IP address by the host. Message 7: DHCP acknowledgment to the current network interface from the server on assignment of the new IP address.
Recommended action	None

C. Two-Factor Authentication

C

This appendix provides an overview of two-factor authentication and an example of how to implement the WiKID solution. The appendix contains the following sections:

- *Why Do I Need Two-Factor Authentication?*
- *NETGEAR Two-Factor Authentication Solutions*

Why Do I Need Two-Factor Authentication?

This section includes the following topics:

- *What Are the Benefits of Two-Factor Authentication?*
- *What Is Two-Factor Authentication?*

In today’s market, online identity theft and online fraud continue to be among the fast-growing cybercrime activities used by many unethical hackers and cybercriminals to steal digital assets for financial gains. Many companies and corporations are losing millions of dollars and running into risks of revealing their trade secrets and other proprietary information as a result of these cybercrime activities. Security threats and hackers have become more sophisticated, and user names, encrypted passwords, and the presence of firewalls are no longer enough to protect the networks from being compromised. IT professionals and security experts have recognized the need to go beyond the traditional authentication process by introducing and requiring additional factors in the authentication process. NETGEAR has also recognized the need to provide more than just a firewall to protect the networks. NETGEAR has implemented a more robust authentication system known as two-factor authentication (2FA or T-FA) to help address the fast-growing network security issues.

What Are the Benefits of Two-Factor Authentication?

The following are the benefits of two-factor authentication:

- **Stronger security**. Passwords cannot efficiently protect the corporate networks because attackers can easily guess simple passwords or users cannot remember complex and unique passwords. One-time passcode (OTP) strengthens and replaces the need to remember complex password.
- **No need to replace existing hardware**. Two-factor authentication can be added to existing NETGEAR products through a firmware upgrade.
- **Quick to deploy and manage**. The WiKID solution integrates seamlessly with the NETGEAR SSL and VPN firewall products.
- **Proven regulatory compliance**. Two-factor authentication 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 can validate a user:

- Something the user knows—for example, a password or PIN.
- Something the user possesses—for example, a token with generated passcode that is six to eight digits in length.

- Something the user is—for example, biometrics such as a fingerprint or retinal print.

This appendix focuses on and discusses only the first two factors, something you know and something you have. This security method can be viewed as a two-tiered authentication approach because it typically relies on what you know and what you have. A common example of two-factor authentication is a bank (ATM) card that is issued by a bank institute:

- The PIN to access your account is *something the user knows.*
- The ATM card is *something the user has.*

You must have both of these factors to gain access to your bank account. Similar to the way ATM cards work, access to the corporate networks and data can also be strengthened using a combination of multiple factors such as a PIN and a token (hardware or software) to validate the users and reduce the incidence of online identity theft.

NETGEAR Two-Factor Authentication Solutions

NETGEAR has implemented 2 two-factor authentication solutions from WiKID. WiKID is the software-based token solution. So instead of using only Windows Active Directory or LDAP as the authentication server, administrators now can use WiKID to perform two-factor authentication on NETGEAR SSL and VPN firewall products.

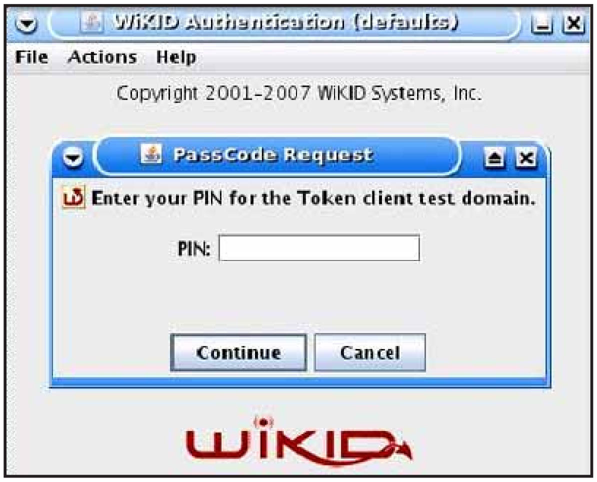
The WiKID solution is based on a request-response architecture where a one-time passcode (OTP), which is time-synchronized with the authentication server, is generated and sent to the user after the validity of a user credential is confirmed by the server.

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. On your computer, launch the WiKID token software.
2. Enter the PIN (“*something the user know*s”).
3. Click the **Continue** button.



WiKID Authentication (defaults)

File Actions Help

Copyright 2001-2007 WiKID Systems, Inc.

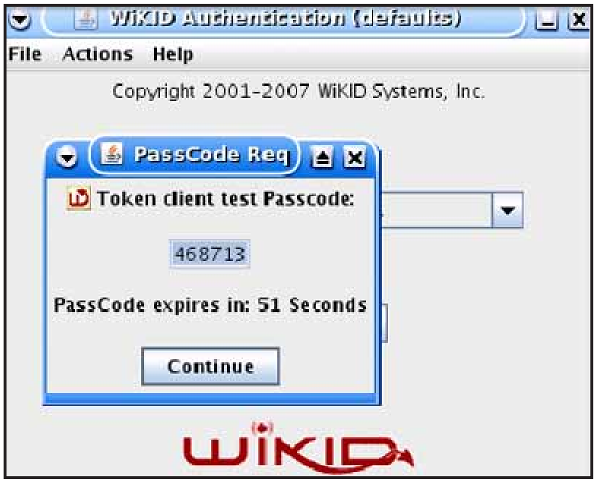
PassCode Request

Enter your PIN for the Token client test domain.

PIN:

The WiKID authentication server generates the one-time passcode (“*something the user has”*).

The one-time passcode (OTP) is time-synchronized to the authentication server so that you can use the OTP only once and you must the OTP before the expiration time. If you do not use this passcode before it expires, you must go through the request process again to generate a new OTP.



WiKID Authentication (defaults)

File Actions Help

Copyright 2001-2007 WiKID Systems, Inc.

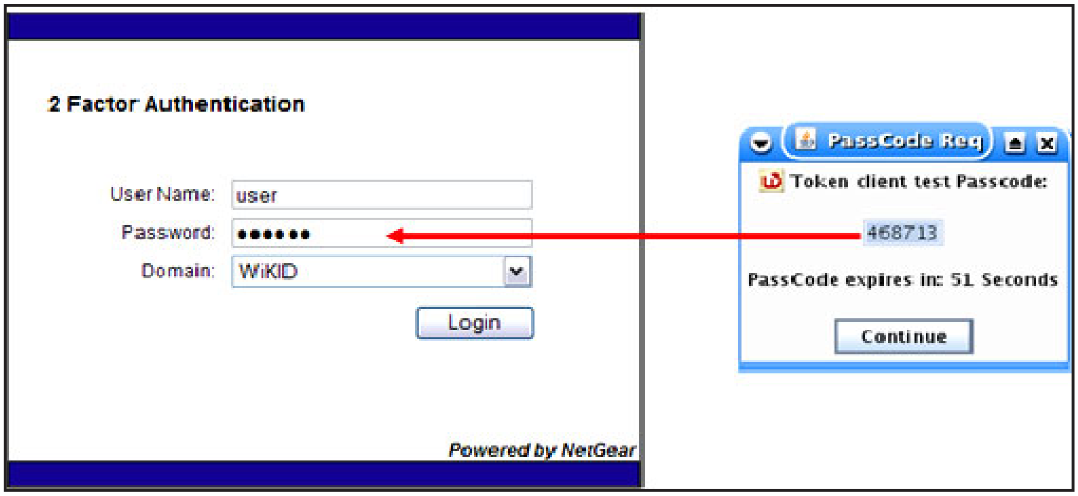
PassCode Req

Token client test Passcode:

468713

PassCode expires in: 51 Seconds

4. Click the **Continue** button.
5. The 2 Factor Authentication login screen displays.



2 Factor Authentication

User Name: user

Password: ●●●●●●

Domain: WiKID

Token client test Passcode:

468713

PassCode expires in: 51 Seconds

6. Enter the OTP as the login password.
7. Click the **Login** button.

   You are logged in.

D. Default Settings and Technical Specifications

D

This appendix provides the default settings and the physical and technical specifications of the VPN firewall in the following sections:

Factory Default Settings

For information about restoring the VPN firewall to factory default settings, see *Revert to Factory Default Settings* on page 551.

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

Table 51. VPN firewall factory default configuration settings

Feature	Default Behavior
Login settings	
User login URL	https://192.168.1.1
Administrator user name (case-sensitive)	admin
Administrator login password (case-sensitive)	password
Guest user name (case-sensitive)	guest
Guest login password (case-sensitive)	password
WAN settings	
WAN IPv4 mode (all WAN interfaces)	NAT
WAN IPv4 load balancing settings (all WAN interfaces)	Primary WAN mode
WAN IPv6 mode (all WAN interfaces)	IPv4 only mode
Stateless IP/ICMP Translation (SIIT)	Disabled
WAN MAC address (all WAN interfaces)	Use default MAC addresses of the VPN firewall.
WAN MTU size (all WAN interfaces)	1500 bytes 1492 bytes for PPPoE connections
Port speed (all WAN interfaces)	AutoSense
Secondary IPv4 WAN addresses	None
Dynamic DNS for IPv4	Disabled
WAN QoS profiles for IPv4	None

Table 51. VPN firewall factory default configuration settings (continued)

Feature		**Default Behavior**
IPv4 LAN, DMZ, and routing settings		
	LAN IPv4 address for the default VLAN	192.168.1.1
	LAN IPv4 subnet mask for the default VLAN	255.255.255.0
	VLAN 1 membership	All ports
	LAN DHCP server for the default VLAN	Enabled
	LAN DHCP IPv4 starting address for the default VLAN	192.168.1.100
	LAN DHCP IPv4 ending address for the default VLAN	192.168.1.254
	VLAN MAC addresses	All LAN ports share the same MAC address.
	Broadcast of ARP packets	Enabled for the default VLAN
	DMZ port for IPv4	Disabled
	DMZ IPv4 address (Port 4)	172.16.2.1
	DMZ IPv4 subnet mask (Port 4)	255.255.255.0
	DMZ DHCP server	Disabled
	DMZ DHCP IPv4 starting address	176.16.2.100
	DMZ DHCP IPv4 ending address	176.16.2.254
	RIP direction	None
	RIP version	Disabled
	RIP authentication	Disabled
IPv6 LAN and DMZ settings		
	LAN IPv6 address	fec0::1
	LAN IPv6 prefix length	64
	LAN DHCPv6 server	Disabled
	DMZ port for IPv6	Disabled
	DMZ IPv6 address (Port 4)	176::1
	DMZ IPv6 prefix length (Port 4)	64
	DMZ DHCPv6 server	Disabled

Table 51. VPN firewall factory default configuration settings (continued)

Feature		Default Behavior
Firewall and security settings		
	Inbound LAN WAN rules (communications coming in from the Internet)	All traffic is blocked, except for traffic in response to requests from the LAN.
	Outbound LAN WAN rules (communications from the LAN to the Internet)	All traffic is allowed.
	Inbound and outbound DMZ WAN rules	None
	Inbound and outbound LAN DMZ rules	None
	Respond to ping on WAN (Internet) ports	Disabled
	Stealth mode	Enabled
	TCP flood	Enabled
	UDP flood	Enabled
	Respond to ping on LAN ports	Disabled
	IPv4 VPN pass-through for IPSec in NAT mode	Enabled
	IPv4 VPN pass-through for PPTP in NAT mode	Enabled
	IPv4 VPN pass-through for L2TP in NAT mode	Enabled
	IPv6 VPN pass-through for IPSec	Enabled
	Multicast pass-through for IGMP	Disabled
	Session limits	Disabled
	TCP time-out	1200 seconds
	UDP time-out	180 seconds
	ICMP time-out	Eight seconds
	SIP ALG	Disabled
	Source MAC filtering	Disabled
	IP/MAC bindings	Disabled
	Port triggering rules	None
	UPnP	Disabled
	Bandwidth profiles	None
	QoS profiles (for IPv4 firewall rules)	None

Table 51. VPN firewall factory default configuration settings (continued)

Feature		Default Behavior
	QoS priorities (for IPv6 firewall rules)	Normal-Service Minimize-Cost Maximize-Reliability Maximize-Throughput Minimize-Delay
	Content filtering	Disabled
	Proxy server blocking	Disabled
	Java applets blocking	Disabled
	ActiveX controls blocking	Disabled
	Cookies blocking	Disabled
	Blocked keywords	None
	Trusted domains	All
VPN IPsec Wizard: IKE policy settings for IPv4 and IPv6 gateway-to-gateway tunnels		
	Exchange mode	Main
	ID type	Local WAN IP address
	Local WAN ID	Local WAN IP address
	Remote WAN ID	Not applicable
	Encryption algorithm	3DES
	Authentication algorithm	SHA-1
	Authentication method	Pre-shared Key
	Key group	DH-Group 2 (1024 bit)
	Lifetime	Eight hours
VPN IPsec Wizard: VPN policy settings for IPv4 and IPv6 gateway-to-gateway tunnels		
	Encryption algorithm	3DES
	Authentication algorithm	SHA-1
	Lifetime	One hour
	Key group	DH-Group 2 (1024 bit)
	NetBIOS	Enabled

Table 51. 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
	Lifetime	One hour
	Key group	DH-Group 2 (1024 bit)
	NetBIOS	Disabled
RADIUS settings		
	Primary RADIUS server	Disabled and none configured
	Secondary RADIUS server	Disabled and none configured
	RADIUS time-out period	30 seconds
	RADIUS maximum retry count	Four
SSL VPN settings		
	SSL VPN IPv4 client address range	192.168.251.1–192.168.251.254
	SSL VPN IPv6 client address range	4000::1–4000::200
User, group, and domain settings		
	Default domain	geardomain
	Default group	geardomain
	Default users, default passwords	admin, password
		guest, password

Table 51. VPN firewall factory default configuration settings (continued)

Feature		Default Behavior
Administrative and monitoring settings		
	Secure HTTP management	Enabled
	Telnet management	Disabled
	Traffic meter	Disabled
	SNMP	Disabled
	Time zone	GMT
	Time zone adjusted for daylight saving time	Disabled
	Routing logs	Disabled
	System logs	Disabled
	Other event logs	Disabled
	Email logs	Disabled
	Syslogs	Disabled
	IPSec VPN logs	Enabled
	SSL VPN logs	Enabled

Physical and Technical Specifications

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

Table 52. VPN firewall physical and technical specifications

Feature		Specification
Network protocol and standards compatibility		
	Data and routing protocols	TCP/IP, RIP-1, RIP-2, PPP over Ethernet (PPPoE), DHCP, DHCPv6
Power adaptor		
	Universal input	100–240V, AC/50–60 Hz, 1.2 Amp maximum
Dimensions and weight		
	Dimensions (W x H x D)	33 x 4.3 x 20.9 cm (13 x 1.7 x 8.2 in.)
	Weight	2.1 kg (4.8 lb)

Table 52. VPN firewall physical and technical specifications (continued)

Feature		Specification
Environmental specifications		
	Operating temperatures	0º to 45ºC
		32º to 113ºF
	Storage temperatures	–20º to 70ºC
		–4º to 158ºF
	Operating humidity	90% maximum relative humidity, noncondensing
	Storage humidity	95% maximum relative humidity, noncondensing
Electromagnetic emissions		
	Meets requirements of	FCC Class A
		CE
		WEEE
		RoHS
Interface specifications		
	4 LAN, one of which is a configurable DMZ interface	AutoSense 10/100/1000BASE-T, RJ-45
	2 WAN	AutoSense 10/100/1000BASE-T, RJ-45
	1 administrative console port	RS-232

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

Table 53. VPN firewall IPSec VPN specifications

Setting	Specification
Network management	Web-based configuration and status monitoring
Number of concurrent users supported	25
IPSec authentication algorithm	SHA-1, MD5
IPSec encryption algorithm	DES, 3DES, AES-128, AES-192, AES-256
IPSec key exchange	IKE, manual key, pre-shared key, X.509 certificate
IPSec authentication types	Local user database, RADIUS PAP, RADIUS CHAP
IPSec certificates supported	CA certificates, self-signed certificate

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

Table 54. VPN firewall SSL VPN specifications

Setting	Specification
Network management	Web-based configuration and status monitoring
Number of concurrent users supported	10
SSL versions	SSLv3, TLS1.0
SSL encryption algorithm	DES, 3DES, ARC4, AES-128, AES-192, AES-256
SSL message integrity	MD5, SHA-1, MAC-MD5/SHA-1, HMAC-MD5/SHA-1
SSL authentication types	Local user database, RADIUS-PAP, RADIUS-CHAP, RADIUS-MSCHAP, RADIUS-MSCHAPv2, WiKID-PAP, WiKID-CHAP, MIAS-PAP, MIAS-CHAP, NT domain, Active Directory, LDAP
SSL certificates supported	CA certificates, self-signed certificate

Index