

ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual



NETGEAR®

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

202-10521-01
v1.1
November, 2009

Technical Support

Please refer to the support information card that shipped with your product. By registering your product at <http://www.netgear.com/register>, we can provide you with faster expert technical support and timely notices of product and software upgrades.

NETGEAR, INC. Support Information

Phone: 1-888-NETGEAR, for US & Canada only. For other countries, see your Support information card.

E-mail: support@netgear.com

North American NETGEAR website: <http://www.netgear.com>

Trademarks

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

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Certificate of the Manufacturer/Importer

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

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

Bestätigung des Herstellers/Importeurs

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

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

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the Class B category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas. When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.

Model Number: FVS318G
Publication Date: November, 2009
Product Family: VPN Firewall Router
Product Name: ProSafe VPN Firewall
Home or Business Product: Business
Language: English
Publication Part Number: 202-10521-01
Publication Version Number: 1.1

Contents

About This Manual

Conventions, Formats, and Scope	xi
How to Print This Manual	xii
Revision History	xii

Chapter 1

Introduction

Key Features of the VPN Firewall	1-1
Advanced VPN Support for Both IPsec and SSL	1-2
A Powerful, True Firewall with Content Filtering	1-2
Autosensing Ethernet Connections with Auto Uplink	1-3
Extensive Protocol Support	1-3
Easy Installation and Management	1-4
Maintenance and Support	1-4
Package Contents	1-5
Front Panel Features	1-5
Rear Panel Features	1-7
Default IP Address, Login Name, and Password Location	1-8
Qualified Web Browsers	1-8

Chapter 2

Connecting the FVS318G to the Internet

Understanding the Connection Steps	2-1
Logging into the VPN Firewall Router Router	2-2
Navigating the Menus	2-3
Configuring the Internet Connections	2-4
Automatically Detecting and Connecting	2-5
Manually Configuring the Internet Connection	2-7
Configuring the WAN Mode	2-11
Network Address Translation	2-11

Classical Routing	2-12
Configuring Dynamic DNS (Optional)	2-13
Configuring the Advanced WAN Options (Optional)	2-15

Chapter 3

LAN Configuration

Choosing the Firewall DHCP Options	3-1
Configuring the LAN Setup Options	3-2
Managing Groups and Hosts (LAN Groups)	3-5
Viewing the LAN Groups Database	3-6
Changing Group Names in the LAN Groups Database	3-9
Configuring DHCP Address Reservation	3-9
Configuring Multi Home LAN IP Addresses	3-10
Configuring Static Routes	3-11
Configuring Routing Information Protocol (RIP)	3-13

Chapter 4

Firewall Protection and Content Filtering

About Firewall Protection and Content Filtering	4-1
Using Rules to Block or Allow Specific Kinds of Traffic	4-2
About Services-Based Rules	4-3
Viewing the Rules	4-8
Order of Precedence for Rules	4-8
Setting the Default Outbound Policy	4-9
Creating a LAN WAN Outbound Services Rule	4-9
Creating a LAN WAN Inbound Services Rule	4-10
Inbound Rules Examples	4-13
Outbound Rules Example	4-16
Adding Customized Services	4-16
Setting Quality of Service (QoS) Priorities	4-18
Attack Checks	4-19
Blocking Internet Sites (Content Filtering)	4-21
Configuring Source MAC Filtering	4-24
Configuring IP/MAC Address Binding Alerts	4-26
Configuring Port Triggering	4-27
Setting a Schedule to Block or Allow Specific Traffic	4-29

Configuring a Bandwidth Profile	4-30
Configuring Session Limits	4-31
E-Mail Notifications of Event Logs and Alerts	4-33
Administrator Tips	4-33

Chapter 5

Virtual Private Networking Using IPsec

Using the VPN Wizard for Client and Gateway Configurations	5-1
Creating Gateway to Gateway VPN Tunnels with the Wizard	5-2
Creating a Client to Gateway VPN Tunnel	5-5
Testing the Connections and Viewing Status Information	5-11
NETGEAR VPN Client Status and Log Information	5-11
FVS318G VPN Connection Status and Logs	5-13
Managing VPN Policies	5-14
Managing IKE Policies	5-14
Managing VPN Policies	5-16
Configuring Extended Authentication (XAUTH)	5-17
Configuring XAUTH for VPN Clients	5-18
User Database Configuration	5-19
RADIUS Client Configuration	5-19
Assigning IP Addresses to Remote Users (ModeConfig)	5-21
Mode Config Operation	5-22
Configuring the VPN Firewall Router	5-22
Configuring the ProSafe VPN Client for ModeConfig	5-25
Configuring Keepalives and Dead Peer Detection	5-27
Configuring Keepalive	5-27
Configuring NetBIOS Bridging with VPN	5-29

Chapter 6

Managing Users, Authentication, and Certificates

Managing Users	6-1
Changing the Administrator Login	6-2
Changing the Guest Login	6-3
Setting administrator timeout and domain display name	6-4
Changing Passwords and Settings	6-6

RADIUS Server External Authentication	6-7
Managing Certificates	6-8
Viewing and Loading CA Certificates	6-10
Viewing Active Self Certificates	6-11
Obtaining a Self Certificate from a Certificate Authority	6-11
Managing your Certificate Revocation List (CRL)	6-14

Chapter 7
Router and Network Management

Performance Management	7-1
Bandwidth Capacity	7-1
Features That Reduce Traffic	7-2
Features That Increase Traffic	7-5
Using QoS to Shift the Traffic Mix	7-7
Tools for Traffic Management	7-8
Changing Passwords and Administrator Settings	7-8
Enabling Remote Management Access	7-10
Using the Command Line Interface	7-13
Using an SNMP Manager	7-13
Configuration File Management	7-15
Upgrading the Firmware	7-17
Configuring Date and Time Service	7-18

Chapter 8
Troubleshooting

Basic Functions	8-1
Power LED Not On	8-2
LEDs Never Turn Off	8-2
LAN or WAN Port LEDs Not On	8-2
Troubleshooting the Web Configuration Interface	8-3
Troubleshooting the ISP Connection	8-4
Troubleshooting a TCP/IP Network Using a Ping Utility	8-5
Testing the LAN Path to Your VPN Firewall Router	8-5
Testing the Path from Your PC to a Remote Device	8-6
Restoring the Default Configuration and Password	8-7

Problems with Date and Time	8-8
Using the Diagnostics Utilities	8-9

Appendix A
Technical Specifications and Factory Default Settings

Appendix B
Related Documents

Appendix C
Two Factor Authentication

Why do I need Two-Factor Authentication?	C-1
What are the benefits of Two-Factor Authentication?	C-1
What is Two-Factor Authentication	C-2
NETGEAR Two-Factor Authentication Solutions	C-2

About This Manual

The *NETGEAR® FVS318G ProSafe™ Gigabit 8 Port VPN Firewall Reference Manual* describes how to install, configure and troubleshoot the ProSafe VPN Firewall. The information in this manual is intended for readers with intermediate computer and Internet skills.

Conventions, Formats, and Scope


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


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

<i>Italic</i>	Emphasis, books, CDs, file and server names, extensions
Bold	User input, IP addresses, GUI screen text
Fixed	Command prompt, CLI text, code
<i>italic</i>	URL links

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

	Note: This format is used to highlight information of importance or special interest.
---	--

	Tip: This format is used to highlight a procedure that will save time or resources.
---	--

	Warning: Ignoring this type of note may result in a malfunction or damage to the equipment.
---	--



Danger: This is a safety warning. Failure to take heed of this notice may result in personal injury or death.

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

Product Version	ProSafe VPN Firewall
Manual Publication Date	November, 2009

For more information about network, Internet, firewall, and VPN technologies, see the links to the NETGEAR website in [Appendix B, “Related Documents.”](#)



Note: Product updates are available on the NETGEAR, Inc. website at <http://kbserver.netgear.com/products/FVS318G.asp>.

How to Print This Manual

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



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

Revision History

Part Number	Version Number	Date	Description
202-10521-01	1.0	July 2009	Product update: New firmware and new user Interface
202-10521-01	1.1	November 2009	Update to LAN and Firewall configuration

Chapter 1

Introduction

The ProSafe VPN Firewall connects your local area network (LAN) to the Internet through an external access device such as a cable modem or DSL modem.

The FVS318G is a complete security solution that protects your network from attacks and intrusions. Unlike simple Internet sharing firewalls that rely on Network Address Translation (NAT) for security, the FVS318G uses stateful packet inspection for Denial of Service attack (DoS) protection and intrusion detection.

The FVS318G allows Internet access for up to 253 users. The use of Gigabit Ethernet LAN and WAN ports ensures extremely high data transfer speeds.

The VPN firewall provides you with multiple Web content filtering options, plus browsing activity reporting and instant alerts — both via e-mail. Parents and network administrators can establish restricted access policies based on time-of-day, web site addresses and address keywords, and share high-speed cable/DSL Internet access for up to 253 personal computers. In addition to NAT, the built-in firewall protects you from hackers.

With minimum setup, you can install and use the firewall within minutes.

This chapter contains the following sections:

- [“Key Features of the VPN Firewall Router” on page 1-1](#)
- [“Package Contents” on page 1-5](#)
- [“Front Panel Features” on page 1-5](#)
- [“Rear Panel Features” on page 1-7](#)
- [“Default IP Address, Login Name, and Password Location” on page 1-8](#)
- [“Qualified Web Browsers” on page 1-8](#)

Key Features of the VPN Firewall Router

The VPN firewall provides the following features:

- Easy, Web-based setup for installation and management.
- Content filtering and site blocking security.

- Built-in eight-port 10/100/1000 Mbps Gigabit Ethernet LAN switch for extremely fast data transfer between local network resources..
- 10/100/1000 Mbps Gigabit Ethernet WAN port for connection to a WAN device, such as a cable modem or DSL modem.
- Advanced IPsec VPN support.
- Advanced stateful packet inspection (SPI) firewall with multi-NAT support.Login capability.
- Front panel LEDs for easy monitoring of status and activity.
- Flash memory for firmware upgrade.

Advanced VPN Support for IPsec

The VPN firewall supports IPsec virtual private network (VPN) connections.

IPsec VPN delivers full network access between a central office and branch offices, or between a central office and telecommuters. Remote access by telecommuters requires the installation of VPN client software on the remote computer.

- IPsec VPN with broad protocol support for secure connection to other IPsec gateways and clients.
- Bundled with the single-user license of the NETGEAR ProSafe VPN Client software (VPN01L)
- Supports 5 concurrent IPsec VPN tunnels.

A Powerful, True Firewall with Content Filtering

Unlike simple Internet sharing NAT routers, the FVS318G is a true firewall, using stateful packet inspection (SPI) to defend against hacker attacks. Its firewall features include:

- Automatically detects and thwarts denial of service (DoS) attacks such as Ping of Death and SYN Flood.
- Blocks unwanted traffic from the Internet to your LAN.
- Blocks access from your LAN to Internet locations or services that you specify as off-limits.
- Prevents objectionable content from reaching your PCs. You can control access to Internet content by screening for Web services, Web addresses, and keywords within Web addresses. You can configure the firewall to log and report attempts to access objectionable Internet sites.
- Permits scheduling of firewall policies by day and time.

- Logs security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the firewall to email the log to you at specified intervals. You can also configure the firewall to send immediate alert messages to your email address or email pager whenever a significant event occurs.

Autosensing Ethernet Connections with Auto Uplink

With its internal 8-port 10/100/1000 Mbps switch and 10/100/1000 WAN port, the FVS318G can connect to either a 10 Mbps standard Ethernet network, a 100 Mbps Fast Ethernet network, or a 1000 Mbps Gigabit Ethernet network. The LAN and WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

The FVS318G incorporates Auto Uplink™ technology. Each Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a “normal” connection such as to a PC or an “uplink” connection such as to a switch or hub. That port will then configure itself to the correct configuration. This feature eliminates the need to worry about crossover cables, as Auto Uplink will accommodate 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). For further information about TCP/IP, refer to “[Internet Configuration Requirements](#)” on page C-3.

- **IP Address Sharing by NAT.** The VPN firewall allows many networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as NAT, allows the use of an inexpensive single-user ISP account.
- **Automatic Configuration of Attached PCs by DHCP.** The VPN firewall dynamically assigns network configuration information, including IP, gateway, and domain name server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of PCs on your local network.
- **DNS Proxy.** When DHCP is enabled and no DNS addresses are specified, the firewall provides its own address as a DNS server to the attached PCs. The firewall obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.
- **PPP over Ethernet (PPPoE).** PPPoE is a protocol for connecting remote hosts to the Internet over a DSL connection by simulating a dial-up connection. This feature eliminates the need to run a login program such as EnterNet or WinPOET on your PC.
- **Quality of Service (QoS)** support for traffic prioritization.

Easy Installation and Management

You can install, configure, and operate the ProSafe 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 your firewall from almost any type of personal computer, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided and online help documentation is built into the browser-based Web Management Interface.
- **Auto Detection of ISP.** The VPN firewall automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- **VPN Wizard.** The VPN firewall includes the NETGEAR VPN Wizard to easily configure IPsec VPN tunnels according to the recommendations of the Virtual Private Network Consortium (VPNC) to ensure the IPsec VPN tunnels are interoperable with other VPNC-compliant VPN routers and clients.
- **Diagnostic Functions.** The firewall incorporates built-in diagnostic functions such as Ping, Trace Route, DNS lookup, and remote reboot.
- **Remote Management.** The firewall allows you to login to the Web Management Interface from a remote location on the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses.
- **Visual monitoring.** The 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 upgrade.
- Free technical support seven days a week, 24 hours a day, according to the terms identified in the Warranty and Support information card provided with your product.

Package Contents

The product package should contain the following items:

- ProSafe VPN Firewall.
- One AC power adapter.
- Rubber feet.
- One Category 5e (Cat5e) Ethernet cable (yellow).
- *ProSafe Gigabit 8 Port VPN Firewall FVS318G Installation Guide*
- *Resource CD*, including:
 - Application Notes and other helpful information.
 - ProSafe VPN Client Software – one user license.
- *Warranty Information and Technical Support card*.

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the firewall for repair.

Front Panel Features

The ProSafe VPN Firewall front panel shown below includes four groups of status indicator light-emitting diodes (LEDs), including Power and Test, WAN, and LAN lights:

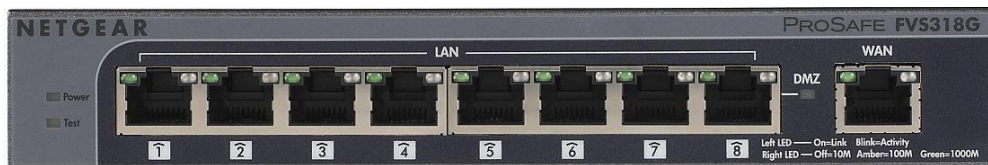


Figure 1-1

The function of each LED is described in the following table:

Table 1-1. LED Descriptions

Object	Activity	Description
Power	On (Green) Off	Power is supplied to the VPN firewall. Power is not supplied to the VPN firewall.
Test	On (Amber) Off	Test mode: The system is initializing or the initialization has failed. The system has booted successfully.
WAN Port		
Active (left side of port)	On (Green) Off)	The WAN port is connected. The Internet connection is down The WAN port is either not enabled or has no link.
Speed (right side of port)	On (Green) On (Amber) Off	The port is operating at 1,000 Mbps. The port is operating at 100 Mbps. The port is operating at 10 Mbps.
LAN Ports		
Link and Activity(left side of port)	On (Green) Blinking (Green) Off	The port has detected a link with a connected Ethernet device. Data is being transmitted or received by the port. The port has no link.
Speed (right side of port)	On (Green) On (Amber) Off	The LAN port is operating at 1,000 Mbps. The LAN port is operating at 100 Mbps. The LAN port is operating at 10 Mbps.
DMZ	On (Green) Off	LAN port 8 is enabled as a DMZ port. LAN port 8 is not enabled as a DMZ port.

Rear Panel Features

The rear panel of the ProSafe VPN Firewall includes a cable lock receptacle, and reset factory defaults switch, and a DC power connection.

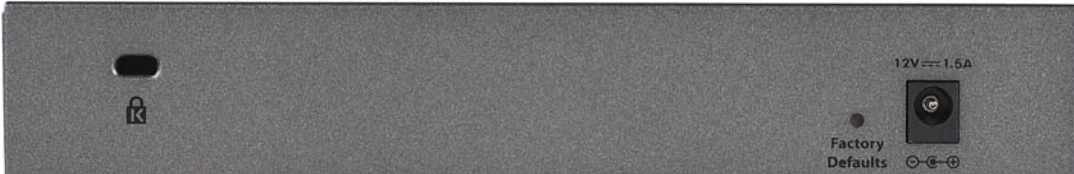


Figure 1-2

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

- Cable security lock receptacle.
- Factory Defaults button: Using a sharp object, press and hold this button for about ten seconds until the front panel TEST light flashes to reset the VPN firewall to factory default settings. All configuration settings will be lost and the default password will be restored.
- DC power receptacle: 12V @ 1.5A.

Default IP Address, Login Name, and Password Location

Check the label on the bottom of the FVS318G's enclosure if you need a reminder of the following factory default information:

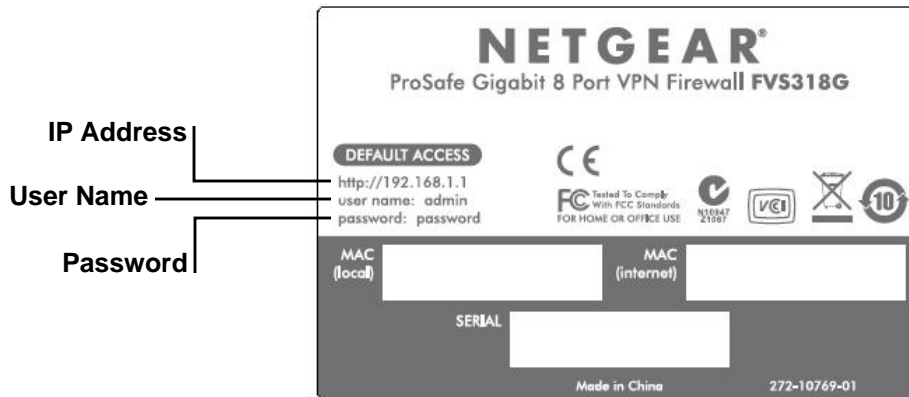


Figure 1-3

Qualified Web Browsers

To configure the ProSafe VPN Firewall, an administrator must use Internet Explorer 5.1 or higher, Apple Safari 1.2 or higher, or Mozilla Firefox 1.x Web browser with JavaScript, and cookies enabled.

Chapter 2

Connecting the FVS318G to the Internet

The initial Internet configuration of the ProSafe VPN Firewall is described in this chapter.

This chapter contains the following sections:

- “Understanding the Connection Steps” on page 2-1
- “Logging into the VPN Firewall Router Router” on page 2-2
- “Navigating the Menus” on page 2-3
- “Configuring the Internet Connections” on page 2-4
- “Configuring the WAN Mode” on page 2-11
- “Configuring Dynamic DNS (Optional)” on page 2-13
- “Configuring the Advanced WAN Options (Optional)” on page 2-15

Understanding the Connection Steps

Typically, six steps are required to complete the basic Internet connection of your VPN firewall.

1. **Connect the firewall physically to your network.** Connect the cables and restart your network according to the instructions in the installation guide. See the installation guide for complete steps. A PDF of the *Installation Guide* is on the NETGEAR website at: <http://kbserver.netgear.com>.
2. **Log in to the VPN Firewall Router.** After logging in, you are ready to set up and configure your VPN firewall. You can also change your password and enable remote management at this time. See “Logging into the VPN Firewall Router Router” on page 2-2.
3. **Configure the Internet connections to your ISP(s).** During this phase, you will connect to your ISPs. You can also program the WAN traffic meters at this time if desired. See “Configuring the Internet Connections” on page 2-4.
4. **Configure the WAN mode.** Select NAT or classical Routing. See “Configuring the WAN Mode” on page 2-11.
5. **Configure dynamic DNS on the WAN port (optional).** Configure your fully qualified domain names during this phase (if required). See “Configuring Dynamic DNS (Optional)” on page 2-13.

6. **Configure the WAN options (optional).** Optionally, you can enable each WAN port to respond to a ping, and you can change the factory default MTU size and port speed. However, these are advanced features and changing them is not usually required. See “[Configuring the Advanced WAN Options \(Optional\)](#)” on page 2-15.

Each of these tasks is detailed separately in this chapter. The configuration of firewall and VPN features is described in later chapters.

Logging into the VPN Firewall Router Router

To connect to the VPN firewall, your computer needs to be configured to obtain an IP address automatically from the VPN firewall by DHCP. For instructions on how to configure your computer for DHCP, refer to the link in [Appendix B, “Related Documents](#).”

To connect and log in to the VPN firewall follow these steps:

1. Start any of the qualified browsers, as detailed in “[Qualified Web Browsers](#)” on page 1-8.
2. Enter **http://192.168.1.1** in the address field. The Manager login features appear in the browser.



The screenshot shows a web browser window titled "NETGEAR Configuration Manager Login". The window contains a login form with the following elements:

- A title bar with the text "NETGEAR Configuration Manager Login" and a "help" icon.
- A "User Name:" label followed by a text input field.
- A "Password / Passcode:" label followed by a text input field.
- A "Domain:" label followed by a dropdown menu showing "LOCALDOMAIN".
- Two yellow buttons at the bottom: "Login" and "Reset".

Figure 2-1

3. In the User field, type **admin**
4. In the Password field, type **password**

Note that both entries are in lower case letters.

5. Click **Login**. The Web Configuration Manager appears, displaying the Router Status menu:

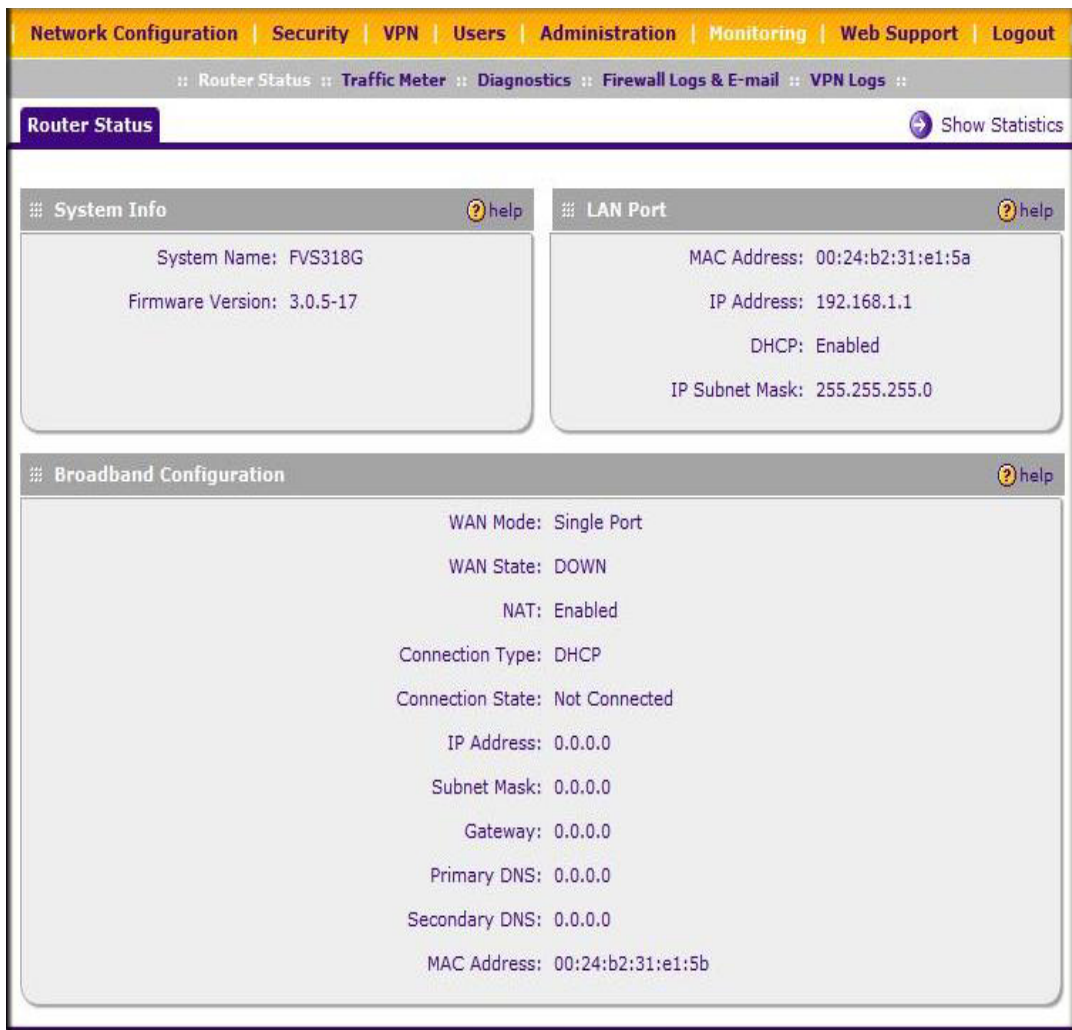
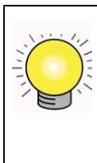


Figure 2-2

Navigating the Menus

The Web Configuration Manager menus are organized in a layered structure of main categories and submenus:

- **Main menu.** The horizontal orange bar near the top of the page is the main menu, containing the primary configuration categories. Clicking on a primary category changes the contents of the submenu bar.
- **Submenu.** The horizontal grey bar immediately below the main menu is the submenu, containing subcategories of the currently selected primary category.
- **Tab.** Immediately below the submenu bar, at the top of the menu active window, are one or more tabs, further subdividing the currently selected subcategory if necessary.
- **Option arrow.** To the right of the tabs on some menus are one or more blue dots with an arrow in the center. Clicking an option arrow brings up either a popup window or an advanced option menu.



Tip: In the instructions in this guide, we may refer to a menu using the notation primary | subcategory, such as Network Configuration | WAN Settings. In this example, Network is the selected primary category (in the main menu) and WAN Settings is the selected subcategory (in the submenu).

You can now proceed to the first configuration task, configuring the VPN firewall's Internet connections.

Configuring the Internet Connections

To set up your VPN firewall for secure Internet connections, you configure the WAN port. The Web Configuration Manager offers two connection configuration options:

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

Each option is detailed in the sections following.

Automatically Detecting and Connecting

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

The screenshot shows the 'Broadband ISP Settings' configuration page. The page is divided into several sections:

- ISP Login:** A section titled 'Does Your Internet Connection Require a Login?' with radio buttons for 'Yes' and 'No' (selected). It includes input fields for 'Login:' and 'Password:'.
- ISP Type:** A section titled 'Which type of ISP connection do you use?' with radio buttons for 'Austria (PPTP)' and 'Other (PPPoE)' (selected). It includes input fields for 'Account Name:', 'Domain Name:', 'My IP Address:', and 'Server IP Address:'. There are also radio buttons for 'Idle Timeout:' with options 'Keep Connected' and 'Idle Time: 5 Minutes' (selected).
- Internet (IP) Address (Current IP Address):** A section with radio buttons for 'Get Dynamically from ISP' (selected) and 'Use Static IP Address'. It includes input fields for 'IP Address:', 'IP Subnet Mask:', and 'Gateway IP Address:'.
- Domain Name Server (DNS) Servers:** A section with radio buttons for 'Get Automatically from ISP' (selected) and 'Use These DNS Servers'. It includes input fields for 'Primary DNS Server:' and 'Secondary DNS Server:'.

At the bottom of the page, there are four buttons: 'Apply', 'Reset', 'Test', and 'Auto Detect'.

Figure 2-3

1. Select **Network Configuration > WAN Settings** from the menu. The Broadband ISP Settings tab appears.

2. Click **Auto Detect** at the bottom of the menu. Auto Detect will probe the WAN port for a range of connection methods and suggest one that your ISP appears to support.

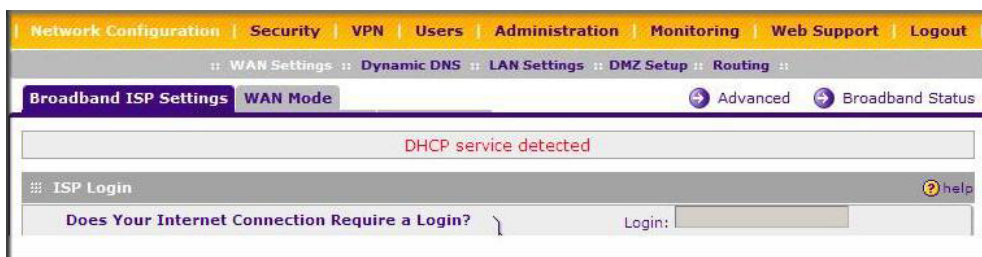


Figure 2-4

- a. If Auto Detect is successful, a status bar at the top of the menu will display the results:.
- b. If Auto Detect senses a connection method that requires input from you, it will prompt you for the information. All methods with their required settings are detailed in the following table.

Table 2-1. Internet connection methods

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

- c. If Auto Detect does not find a connection, you will be prompted to (1) check the physical connection between your VPN firewall and the cable or DSL line, or to (2) check your VPN firewall’s MAC address (For more information, see [“Configuring the WAN Mode”](#) on page 2-11 and [“Troubleshooting the ISP Connection”](#) on page 8-4).

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



Figure 2-5

The Connection Status window should show a valid IP address and gateway. If the configuration was not successful, skip ahead to [“Manually Configuring the Internet Connection”](#) following this section, or see [“Troubleshooting the ISP Connection”](#) on page 8-4.



Note: If the configuration process was successful, you are connected to the Internet through the WAN port.

If your WAN ISP configuration was successful, you can skip ahead to [“Configuring the WAN Mode”](#) on page 2-11.

If the automatic WAN ISP configuration failed, you can attempt a manual configuration as described in the following section, or see [“Troubleshooting the ISP Connection”](#) on page 8-4.

Manually Configuring the Internet Connection

Unless your ISP automatically assigns your configuration automatically via DHCP, you will need to obtain configuration parameters from your ISP in order to manually establish an Internet connection. The necessary parameters for various connection types are listed in [Table 2-1](#).

To manually configure your **Broadband ISP Settings**:

1. Select Network **Configuration** > **WAN Settings** > **Broadband ISP Settings** and enter the following:
2. In the **ISP Login** options, choose one of these options:



Figure 2-6

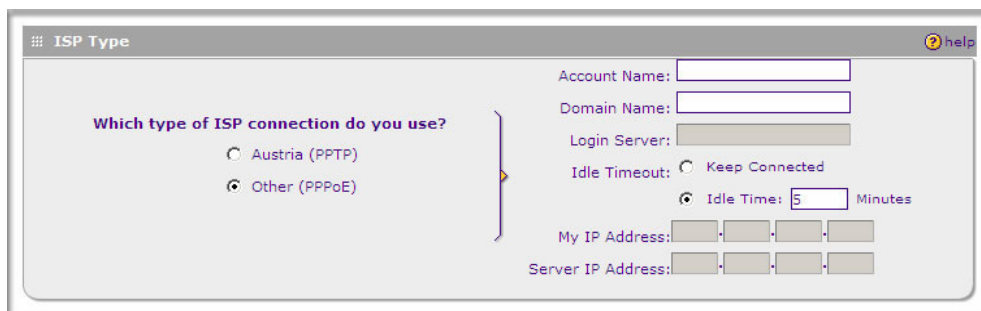
- If your ISP requires an initial login to establish an Internet connection, click **Yes** (this is the default).
 - If a login is not required, click **No** and ignore the Login and Password fields.
3. If you clicked **Yes**, enter the ISP-provided Login and Password information.
 4. In the ISP Type options, select the type of ISP connection you use from the three listed options. (By default, “Other (PPPoE)” is selected, as shown below.



Figure 2-7

(If your connection is PPPoE or PPTP, your ISP will require an initial login.)

5. If you have installed login software such as WinPoET or Enternet, then your connection type is PPPoE. If your ISP uses PPPoE as a login protocol:



The screenshot shows a configuration window titled "ISP Type". On the left, under the heading "Which type of ISP connection do you use?", there are two radio button options: "Austria (PPTP)" and "Other (PPPoE)". The "Other (PPPoE)" option is selected. To the right of this section are several input fields: "Account Name", "Domain Name", "Login Server", "Idle Timeout" (with radio buttons for "Keep Connected" and "Idle Time"), "My IP Address", and "Server IP Address". The "Idle Time" field is set to 5 minutes.

Figure 2-8

- a. Select **Other (PPPoE)**.
 - b. Configure the following fields:
 - **Account Name.** Valid account name for the PPPoE connection
 - **Domain Name.** Name of your ISP's domain or your domain name if your ISP has assigned one. In most cases, you may leave this field blank.
 - **Idle Timeout.** Select Keep Connected, to keep the connection always on. To logout after the connection is idle for a period of time, click Idle Time and in the timeout field enter the number of minutes to wait before disconnecting.
6. If your ISP is Austria Telecom or any other ISP that uses PPTP as a login protocol:
- a. Select **Austria (PPTP)**.
 - b. Configure the following fields:
 - **Account Name** (also known as Host Name or System Name). Enter the valid account name for the PPTP connection (usually your email name as assigned by your ISP). Some ISPs require entering your full email address here.
 - **Domain Name.** Your domain name or workgroup name assigned by your ISP, or your ISP's domain name. You may leave this field blank.
 - **Idle Timeout.** Check the Keep Connected radio button to keep the connection always on. To logout after the connection is idle for a period of time, click Idle Time and enter the number of minutes to wait before disconnecting in the timeout field. This is useful if your ISP charges you based on the amount of time you have logged in.
 - **My IP Address.** IP address assigned by the ISP to make the connection with the ISP server.

- **Server IP Address.** IP address of the PPTP server.

7. Review the Internet (IP) Address options.

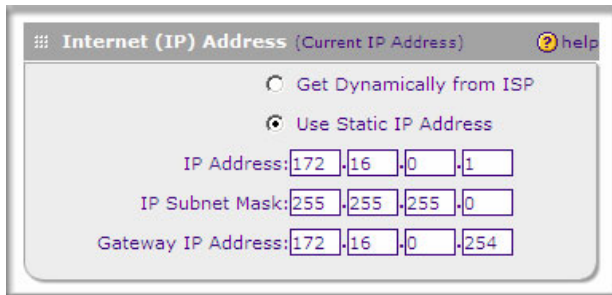


Figure 2-9

These options are inactive if BigPond Cable is selected.

8. If your ISP has assigned a fixed (static) IP address, select **Use Static IP Address**, and configure the following fields:
- **IP Address.** Enter the Static IP address assigned to you, that identifies the VPN firewall to your ISP.
 - **Subnet Mask.** Enter the mask provided by the ISP or your network administrator.
 - **Gateway IP Address.** Enter the IP address of the ISP's gateway, provided by the ISP or your network administrator.
9. If your ISP has not assigned a static IP address, click **Get dynamically from ISP**. The text fields will be inactivated.

The ISP will automatically assign an IP address to the VPN firewall using DHCP network protocol.

10. Review the Domain Name Server (DNS) Servers options.

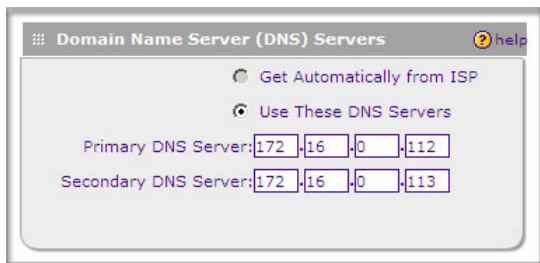


Figure 2-10

- If your ISP has not assigned any Domain Name Servers (DNS) addresses, click **Get dynamically from ISP**.
 - If your ISP (or your IT department) has assigned DNS addresses, click **Use these DNS Servers** and enter the DNS server IP addresses provided to you in the fields.
11. Click **Apply** to save any changes to the WAN ISP Settings. (Or click **Reset** to discard any changes and revert to the previous settings.)
12. Click **Test** to evaluate your entries.

The VPN firewall will attempt to connect to the NETGEAR Web site. If a successful connection is made, NETGEAR's Web site appears.

When you are finished, click Logout or proceed to additional setup and management tasks.

Configuring the WAN Mode

You must choose either NAT or classical routing, as explained in the following sections.

Network Address Translation

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

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

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

Classical Routing

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

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

To configure routing select **Network Configuration > WAN Settings > WAN Mode**. The WAN Mode screen displays. Click the setting you want and click **Apply**.

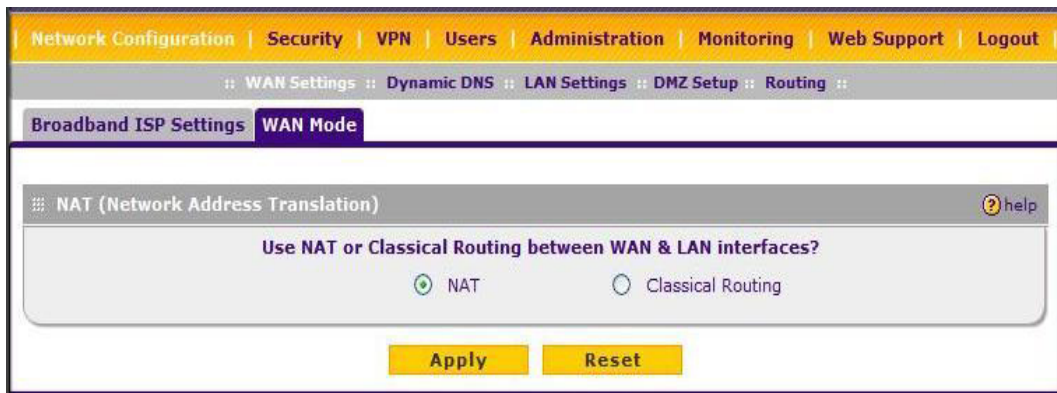


Figure 2-11

To learn the status of the WAN port, you can view the Router Status page (see “[Monitoring VPN Tunnel Connection Status](#)” on page 9-14) or look at the LEDs on the front panel (see “[Front Panel Features](#)” on page 1-5).

Configuring Dynamic DNS (Optional)

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

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

After you have configured your account information in the firewall, whenever your ISP-assigned IP address changes, your firewall will automatically contact your DDNS service provider, log in to your account, and register your new IP address.



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

To configure Dynamic DNS:

1. Select **Network Configuration > Dynamic DNS** from the main menu and click the **Dynamic DNS Configuration** tab. The Dynamic DNS Configuration screen is displayed.

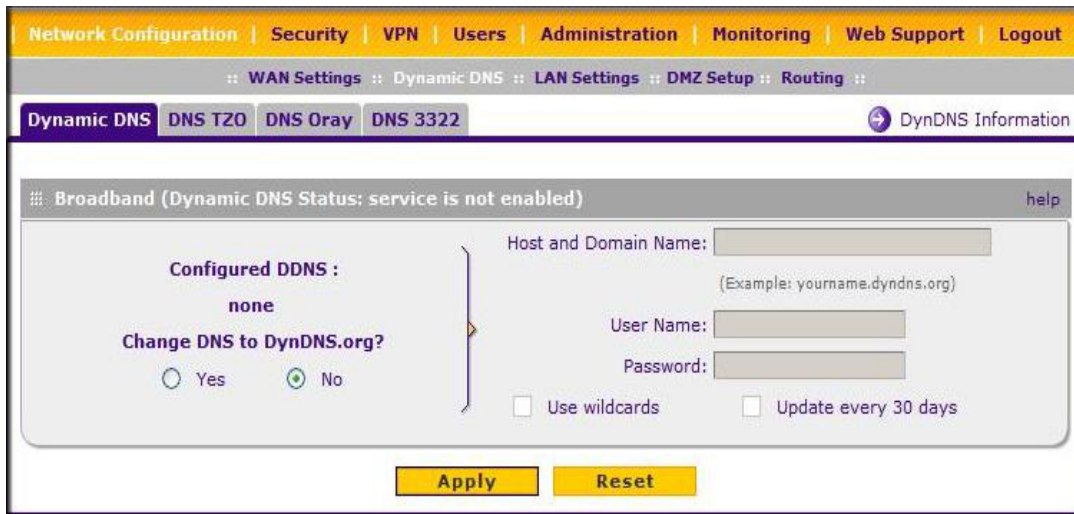


Figure 2-12

2. Select the tab for the DDNS service provider you will use.
3. Click the information or registration link in the upper right corner for registration information.



Figure 2-13:

4. Access the Web site of the DDNS service provider and register for an account (for example, for dyndns.org, go to <http://www.dyndns.org>).
5. Click the **Yes** radio button for **Change DNS to** <your desired DDNS service> and configure the active fields:

- a. Enter the account information for the service you have chosen (for example, user name, password, key, or domain).
 - b. If your DDNS provider allows the use of wild cards in resolving your URL, you may select the **Use wildcards** check box to activate this feature. For example, the wildcard feature will cause `*.yourhost.dyndns.org` to be aliased to the same IP address as `yourhost.dyndns.org`
 - c. If your WAN IP address does not change often, you may need to force a periodic update to the DDNS service to prevent your account from expiring. If it appears, you can select the **Update every 30 days** check box to enable a periodic update.
6. Click **Apply** to save your configuration.

Configuring the Advanced WAN Options (Optional)

To configure the Advanced WAN options:

1. Select **Network Configuration > WAN Settings** from the main menu. The Broadband ISP Settings screen will display.
2. Click the **Advanced** link to the right of the tabs. The **Broadband Options** tab is displayed.

The screenshot shows the 'Broadband Advanced Options' configuration window. It is divided into three main sections, each with a 'help' icon:

- MTU Size:** Features two radio buttons. 'Default' is selected. The 'Custom' option is accompanied by a text box containing '1500' and the unit 'Bytes'.
- Speed:** Features a 'Port Speed' dropdown menu currently set to 'AutoSense'.
- Router's MAC Address:** Features three radio buttons. 'Use Default Address' is selected. The other two options are 'Use this computer's MAC' and 'Use this MAC Address', the latter with a text box containing the MAC address '00:1b:2f:00:00:05'.

At the bottom of the window are two yellow buttons: 'Apply' and 'Reset'.

Figure 2-14

3. Edit the default information you want to change.

- a. **MTU Size.** The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 Bytes, or 1492 Bytes for PPPoE connections. For some ISPs, you may need to reduce the MTU. This is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- b. **Port Speed.** In most cases, your VPN firewall can automatically determine the connection speed of the WAN port. If you cannot establish an Internet connection and the WAN Link or Speed LED blinks continuously, you may need to manually select the port speed. AutoSense is the default.

If you know the Ethernet port speed that your broadband modem supports, select it; otherwise, select 10M. Use the half-duplex settings unless you are sure your broadband modem supports full duplex.

- c. **Router's MAC Address.** Each computer or router on your network has a unique 32-bit local Ethernet address. This is also referred to as the computer's MAC (Media Access Control) address. The default is **Use default address**. However, if your ISP requires MAC authentication, then select either of these options:
 - Use this Computer's MAC address to have the VPN firewall use the MAC address of the computer you are now using, or
 - Use This MAC Address to manually type in the MAC address that your ISP expects.

Chapter 3

LAN Configuration

This chapter describes how to configure the advanced LAN features of your ProSafe VPN Firewall.

This chapter contains the following sections

- “Choosing the Firewall DHCP Options” on page 3-1
- “Managing Groups and Hosts (LAN Groups)” on page 3-5
- “Configuring DHCP Address Reservation” on page 3-9
- “Configuring Multi Home LAN IP Addresses” on page 3-10
- “Configuring Static Routes” on page 3-11
- “Configuring Routing Information Protocol (RIP)” on page 3-13

Choosing the Firewall DHCP Options

By default, the firewall will function as a DHCP (Dynamic Host Configuration Protocol) server, allowing it to assign IP, DNS server, WINS Server, and default gateway addresses to all computers connected to the firewall LAN. The assigned default gateway address is the LAN address of the firewall. IP addresses will be assigned to the attached PCs from a pool of addresses specified in this menu. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN. The DHCP options are available for both the LAN and DMZ settings.

For most applications, the default DHCP and TCP/IP settings of the VPN firewall are satisfactory. See the link to “Preparing a Computer for Network Access” in [Appendix B, “Related Documents”](#) for an explanation of DHCP and information about how to assign IP addresses for your network.

If another device on your network will be the DHCP server, or if you will manually configure the network settings of all of your computers, clear the **Enable DHCP server** radio box by selecting the **Disable DHCP Server** radio box. Otherwise, leave it checked.

Specify the pool of IP addresses to be assigned by setting the Starting IP Address and Ending IP Address. These addresses should be part of the same IP address subnet as the firewall’s LAN IP address. Using the default addressing scheme, you should define a range between 192.168.1.2 and 192.168.1.100, although you may wish to save part of the range for devices with fixed addresses.

The firewall will deliver the following parameters to any LAN device that requests DHCP:

- An IP Address from the range you have defined.
- Subnet Mask.
- Gateway IP Address (the firewall's LAN IP address).
- Primary DNS Server (the firewall's LAN IP address).
- WINS Server (if you entered a WINS server address in the DHCP Setup menu).
- Lease Time (date obtained and duration of lease).

DHCP Relay options allow you to make the firewall a dhcp relay agent. 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, or which is not located on the local subnet. If you have no configured DHCP Relay Agent, your clients would only be able to obtain IP addresses from the DHCP server which is on the same subnet. To enable clients to obtain IP addresses from a DHCP server on a remote subnet, you have to configure the DHCP Relay Agent on the subnet that contains the remote clients, so that it can relay DHCP broadcast messages to your DHCP server.

When the **DNS Proxy** option is enabled, the router will act as a proxy for all DNS requests and communicate with the ISP's DNS servers (as configured in the WAN settings page). All DHCP clients will receive the Primary/Secondary DNS IP along with the IP where the DNS Proxy is running, i.e. the box's LAN IP. When disabled, all DHCP clients will receive the DNS IP addresses of the ISP excluding the DNS Proxy IP address.

Configuring the LAN Setup Options

The LAN Setup menu allows configuration of LAN IP services such as DHCP and allows you to configure a secondary or "multi-home" LAN IP setup in the LAN. The default values are suitable for most users and situations.



Note: If you enable the DHCP Relay feature, you will not use the FVS318G as a DHCP server but rather as a DHCP relay agent for a DHCP server somewhere else on your network.

1. Go to **Network Configuration > LAN Settings** to display the **LAN Setup** tab page.

The screenshot displays the LAN Setup configuration page. At the top, there is a navigation bar with tabs for Network Configuration, Security, VPN, Users, Administration, Monitoring, Web Support, and Logout. Below this, there are sub-tabs for WAN Settings, Dynamic DNS, LAN Settings, DMZ Setup, and Routing. The LAN Setup tab is active, with sub-tabs for LAN Setup, LAN Groups, and LAN Multi-homing. A DHCP Log icon is visible in the top right corner.

The LAN TCP/IP Setup section includes fields for IP Address (192.168.1.1) and Subnet Mask (255.255.255.0).

The DHCP section has two radio buttons: Disable DHCP Server and Enable DHCP Server. The Enable DHCP Server section includes:

- Domain Name: netgear.com
- Starting IP Address: 192.168.1.2
- Ending IP Address: 192.168.1.100
- Primary DNS Server: [][][][]
- Secondary DNS Server: [][][][]
- WINS Server: [][][][]
- Lease Time: 24 Hours

There is also an Enable LDAP information section with fields for LDAP Server, Search Base, and port (leave blank for default port).

The DHCP Relay section has a radio button DHCP Relay and a Relay Gateway field: [][][][]

The DNS Proxy section has a checkbox Enable DNS Proxy.

At the bottom, there are Apply and Reset buttons.

Figure 3-1

2. In the LAN TCP/IP Setup section, configure the following settings:

- **IP Address.** The LAN address of your VPN firewall (factory default: **192.168.1.1**).



Note: If you change the LAN IP address of the firewall while connected through the browser, you will be disconnected. You must then open a new connection to the new IP address and log in again. For example, if you change the default IP address 192.168.1.1 to 10.0.0.1, you must now enter **http://10.0.0.1** in your browser to reconnect to the Web Configuration Manager.

- **IP Subnet Mask.** The subnet mask specifies the network number portion of an IP address. Your VPN firewall will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use 255.255.255.0 as the subnet mask.

3. In the DHCP section, select **Enable** or **Disable DHCP Server**.

By default, the VPN firewall will function as a DHCP server, providing TCP/IP configuration settings for all computers connected to the VPN firewall's LAN. If another device on your network will be the DHCP server, or if you will manually configure all devices, click **Disable DHCP Server**. If the DHCP server is enabled, enter the following parameters:

- **Domain Name.** (Optional) The DHCP will assign the entered domain to DHCP clients.
- **Starting IP Address.** Specifies the first of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN will be assigned an IP address between this address and the Ending IP Address. The IP address 192.168.1.2 is the default start address.
- **Ending IP Address.** Specifies the last of the contiguous addresses in the IP address pool. The IP address 192.168.1.100 is the default ending address.



Note: The Starting and Ending DHCP addresses should be in the same subnet as the LAN IP address of the VPN firewall (the IP Address configured in the **LAN TCP/IP Setup** section).

- **Primary DNS Server.** (Optional) If an IP address is specified, the VPN firewall will provide this address as the primary DNS server IP address. If no address is specified, the VPN firewall will provide its own LAN IP address as the primary DNS server IP address.
- **Secondary DNS Server.** (Optional) If an IP address is specified, the VPN firewall will provide this address as the secondary DNS server IP address.
- **WINS Server.** (Optional) Specifies the IP address of a local Windows NetBios Server if one is present in your network.

- a. **Lease Time.** This specifies the duration for which IP addresses will be leased to clients.
 - b. **Enable LDAP Information.** This enables the DHCP server to provide LDAP server information.
 - **Enable DNS Proxy.** When DNS proxy is enabled (the default), the DHCP server will provide the VPN firewall's LAN IP address as the DNS server for address name resolution. If this box is unchecked, the DHCP server will provide the ISP's DNS server IP addresses. The VPN firewall will still service DNS requests sent to its LAN IP address unless you disable DNS Proxy in the firewall settings (see [“Attack Checks” on page 4-19](#)).
4. Click **Apply** to save your settings.



Note: Once you have completed the LAN setup, all outbound traffic is allowed and all inbound traffic is discarded. To change these default traffic rules, refer to [Chapter 4, “Firewall Protection and Content Filtering”](#).

Managing Groups and Hosts (LAN Groups)

The **Known PCs and Devices** table in the **LAN Groups** menu contains a list of all known PCs and network devices that are assigned dynamic IP addresses by the VPN firewall, or have been discovered by other means. Collectively, these entries make up the LAN Groups Database.

The LAN Groups Database is updated by these methods:

- **DHCP Client Requests.** By default, the DHCP server in this VPN firewall is enabled, and will accept and respond to DHCP client requests from PCs and other network devices. These requests also generate an entry in the LAN Groups Database. Because of this, leaving the DHCP server feature (on the LAN screen) enabled is strongly recommended.
- **Scanning the Network.** The local network is scanned using ARP requests. The ARP scan will detect active devices that are not DHCP clients. However, sometimes the name of the PC or device cannot be accurately determined, and will appear in the database as Unknown.
- **Manual Entry.** You can manually enter information about a network device.

Some advantages of the LAN Groups Database are:

- Generally, you do not need to enter either IP address or MAC addresses. Instead, you can just select the desired PC or device.
- No need to reserve an IP address for a PC in the DHCP server. All IP address assignments made by the DHCP server will be maintained until the PC or device is removed from the database, either by expiry (inactive for a long time) or by you.

- No need to use a fixed IP on PCs. Because the address allocated by the DHCP server will never change, you don't need to assign a fixed IP to a PC to ensure it always has the same IP address.
- MAC level control over PCs. The LAN Groups Database uses the MAC address to identify each PC or device. So changing a PC's IP address does not affect any restrictions on that PC.
- Group and individual control over PCs.
 - You can assign PCs to Groups and apply restrictions to each Group using the Firewall Rules screen (see “Using Rules to Block or Allow Specific Kinds of Traffic” on page 4-2).
 - You can also select the Groups to be covered by the Block Sites feature (see “Blocking Internet Sites (Content Filtering)” on page 4-21).
 - If necessary, you can also create Firewall Rules to apply to a single PC (see “Configuring Source MAC Filtering” on page 4-24). Because the MAC address is used to identify each PC, users cannot avoid these restrictions by changing their IP address.
- A computer is identified by its MAC address—not its IP address. Hence, changing a computer's IP address does not affect any restrictions applied to that PC.

Viewing the LAN Groups Database

To view the LAN Groups Database, do the following:

1. Select **Network Configuration > LAN Settings > LAN Groups** from the main menu. The LAN Groups tab displays.



Figure 3-2

The **Known PCs and Devices** table lists the entries in the LAN Groups Database. For each computer or device, the following fields are displayed:

- **Name.** The name of the PC or device. For computers that do not support the NetBIOS protocol, this will be listed as “Unknown” (you can edit the entry manually to add a meaningful name). If the computer was assigned an IP address by the DHCP server, then the Name will be appended by an asterisk.
- **IP Address.** The current IP address of the computer. For DHCP clients of the VPN firewall, this IP address will not change. If a computer is assigned a static IP addresses, you will need to update this entry manually if the IP address on the computer has been changed.
- **MAC Address.** The MAC address of the PC’s network interface.
- **Group.** Each PC or device can be assigned to a single group. By default, a computer is assigned to Group 1, unless a different group is chosen from the Group pull-down menu.
- **Action.** Allows modification of the selected entry by clicking **Edit**.

Adding Devices to the LAN Groups Database

To add devices manually to the LAN Groups Database, follow these steps:

1. In the **Add Known PCs and Devices** section, make the following entries:

- **Name.** Enter the name of the PC or device.
- **IP Address Type.** From the pull-down menu, choose how this device receives its IP address. The choices are:
 - **Fixed (Set on PC).** The IP address is statically assigned on the computer.
 - **Reserved (DHCP Client).** Directs the VPN firewall's DHCP server to always assign the specified IP address to this client during the DHCP negotiation (see [“Configuring DHCP Address Reservation”](#) on page 3-9).



Note: When assigning a Reserved IP address to a client, the IP address selected must be outside the range of addresses allocated to the DHCP server pool.

- **IP Address.** Enter the IP address that this computer or device is assigned in the IP Address field. If the IP Address Type is Reserved (DHCP Client), the VPN firewall will reserve the IP address for the associated MAC address.
 - **MAC Address.** Enter the MAC address of the computer's network interface in the MAC Address field. The MAC address format is six colon-separated pairs of hexadecimal characters (0-9 and A-F), such as 01:23:45:67:89:AB.
 - **Group.** From the pull-down menu, select the LAN Group to which the computer will be assigned. (Group 1 is the default group.)
2. Click **Add**. The device will be added to the **Known PCs and Devices** table.
3. (Optional) To enable DHCP Address Reservation after the entry is in the table, select the check box for the new table entry and click **Save Binding** to bind the IP address to the MAC address for DHCP assignment.

Changing Group Names in the LAN Groups Database

By default, the LAN Groups are named Group1 through Group8. You can rename these group names to be more descriptive, such as Engineering or Marketing.

To edit the names of any of the eight available groups:

1. From the **LAN Groups** tab, click the **Edit Group Names** link to the right of the tabs. The **Network Database Group Names** tab appears.

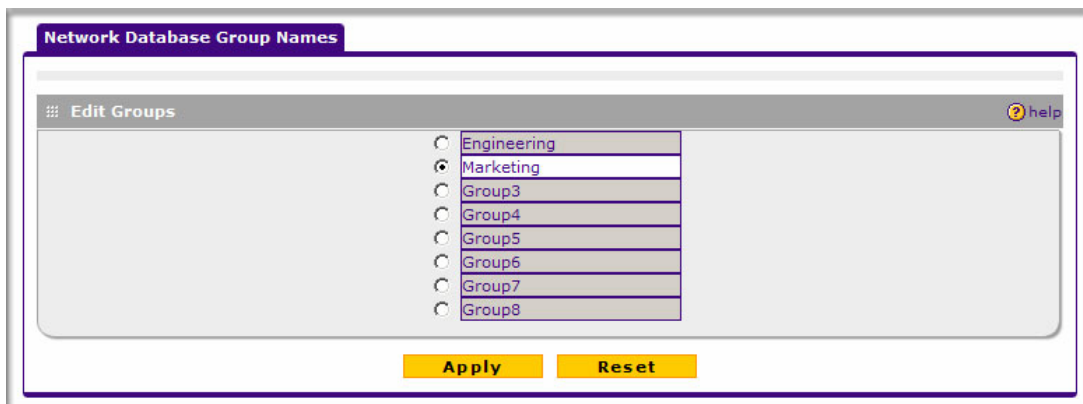


Figure 3-3

2. Select the radio button next to any group name to make that name active for editing.
3. Type a new name in the field.
4. Select and edit other group names if desired.
5. Click **Apply** to save your settings.

Configuring DHCP Address Reservation

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

To reserve an IP address, manually enter the device in the **LAN Groups** tab, specifying **Reserved (DHCP Client)**.



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

Configuring Multi Home LAN IP Addresses

If you have computers on your LAN using different IP address ranges (for example, 172.16.2.0 or 10.0.0.0), you can add “aliases” to the LAN port, giving computers on those networks access to the Internet through the VPN firewall. This allows the VPN firewall to act as a gateway to additional logical subnets on your LAN. You can assign the VPN firewall an IP address on each additional logical subnet.

To add a secondary LAN IP address, follow these steps:

1. Select **Network Configuration > LAN Settings** from the main menu, and click the LAN Multi-homing tab. The LAN Multi-homing screen displays.

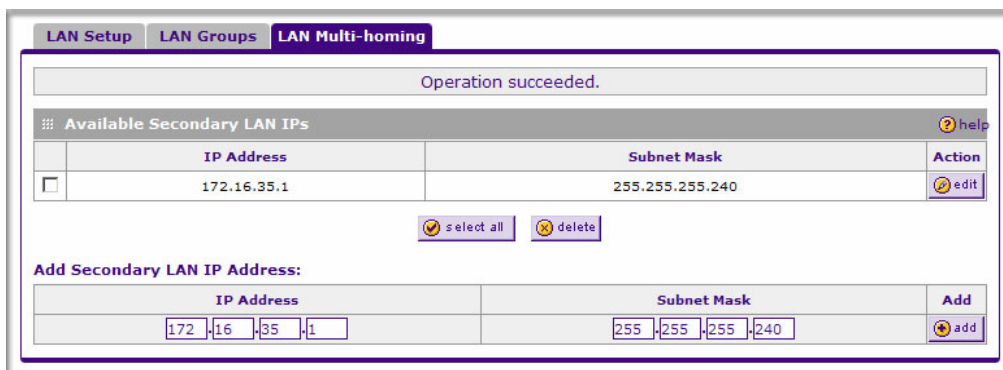




Figure 3-4

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

- **IP Address.** The “alias,” an additional IP address hosted by the LAN port of the VPN firewall. This address will be the gateway for computers on the secondary subnet.
- **Subnet Mask.** The IPv4 subnet mask that defines the range of the secondary subnet.

2. In the **Add Secondary LAN IP Address** section, enter the additional IP address and subnet mask to be assigned to the LAN port of the VPN firewall.
3. Click **Add**. The new Secondary LAN IP address will appear in the **Available Secondary LAN IPs** table.

	Note: IP addresses on these secondary subnets cannot be configured in the DHCP server. The hosts on the secondary subnets must be manually configured with IP addresses, gateway IP addresses, and DNS server IP addresses.
---	--

	Tip: The secondary LAN IP address will be assigned to the LAN interface of the VPN firewall and can be used as a gateway by computers on the secondary subnet.
---	---

Configuring Static Routes

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

To add or edit a static route:

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

Figure 3-5

2. Click **Add**. The **Add Static Route** tab is displayed.

The screenshot shows a web-based configuration interface for adding a static route. At the top, a purple header bar contains the text "Add Static Route". Below this is a light gray banner with the message "Operation succeeded.". The main content area is titled "Static Route" and contains several input fields and checkboxes. The "Route Name" field is empty. The "Active" checkbox is checked, and the "Private" checkbox is unchecked. The "Destination IP Address" and "IP Subnet Mask" fields are empty. The "Interface" dropdown menu is set to "Broadband". The "Gateway IP Address" and "Metric" fields are empty. At the bottom of the form are two yellow buttons: "Apply" and "Reset".

Figure 3-6

3. Enter a route name for this static route in the **Route Name** field (for identification and management).
4. Select **Active** to make this route effective.
5. Select **Private** if you want to limit access to the LAN only. The static route will not be advertised in RIP.
6. Enter the **Destination IP Address** to the host or network to which the route leads.
7. Enter the **IP Subnet Mask** for this destination. If the destination is a single host, enter 255.255.255.255.
8. Enter the **Interface** which is the physical network interface (WAN or LAN) through which this route is accessible.
9. Enter the **Gateway IP Address** through which the destination host or network can be reached (must be a firewall on the same LAN segment as the firewall).
10. Enter the **Metric** priority for this route. If multiple routes to the same destination exist, the route with the lowest metric is chosen (value must be between 1 and 15).
11. Click **Apply** to save your settings.

The new static route will be added to the Static Route table.

Configuring Routing Information Protocol (RIP)

RIP (Routing Information Protocol, RFC 2453) is an Interior Gateway Protocol (IGP) that is commonly used in internal networks (LANs). It allows a router to exchange its routing information automatically with other routers, and allows it to dynamically adjust its routing tables and adapt to changes in the network. RIP is disabled by default.

To configure RIP parameters:

1. Select **Network Configuration > Routing** from the main menu.
2. Click the **RIP Configuration** link to the right of the tab. The **RIP Configuration** menu is displayed.

Figure 3-7

3. From the **RIP Direction** pull-down menu, choose the direction in which the VPN firewall will send and receive RIP packets. The choices are:
 - **None.** The VPN firewall neither broadcasts its route table nor does it accept any RIP packets from other routers. This effectively disables RIP.

- **Both.** The VPN firewall broadcasts its routing table and also processes RIP information received from other routers.
 - **Out Only.** The VPN firewall broadcasts its routing table periodically but does not accept RIP information from other routers.
 - **In Only.** The VPN firewall accepts RIP information from other routers, but does not broadcast its routing table.
4. From the **RIP Version** pull-down menu, choose the version from the following options:
- **RIP-1.** A classful routing that does not include subnet information. This is the most commonly supported version.
 - **RIP-2.** 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.
5. **Authentication for RIP2B/2M required?** If you selected RIP-2B or RIP-2M, check **YES** the feature, and input the **First Key Parameters** and **Second Key Parameters**, MD-5 keys to authenticate between routers.
6. Click **Apply** to save your settings.

Chapter 4

Firewall Protection and Content Filtering

This chapter describes how to use the content filtering features of the ProSafe VPN Firewall to protect your network.

This chapter contains the following sections:

- [“About Firewall Protection and Content Filtering”](#) on page 4-1
- [“Using Rules to Block or Allow Specific Kinds of Traffic”](#) on page 4-2
- [“Attack Checks”](#) on page 4-19
- [“Blocking Internet Sites \(Content Filtering\)”](#) on page 4-21
- [“Configuring Source MAC Filtering”](#) on page 4-24
- [“Configuring IP/MAC Address Binding Alerts”](#) on page 4-26
- [“Configuring Port Triggering”](#) on page 4-27
- [“Setting a Schedule to Block or Allow Specific Traffic”](#) on page 4-29
- [“Configuring a Bandwidth Profile”](#) on page 4-30
- [“Configuring Session Limits”](#) on page 4-31
- [“E-Mail Notifications of Event Logs and Alerts”](#) on page 4-33
- [“Administrator Tips”](#) on page 4-33

About Firewall Protection and Content Filtering

The ProSafe VPN Firewall provides you with Web content filtering options, plus browsing activity reporting and instant alerts via e-mail. Network administrators can establish restricted access policies based on time-of-day, Web addresses and Web address keywords. You can also block Internet access by applications and services, such as chat or games.

A firewall is a special category of router that 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 (see [“Managing Groups and Hosts \(LAN Groups\)”](#) on page 3-5 to set up LAN Groups).

A firewall incorporates the functions of a NAT (Network Address Translation) router, while adding features for dealing with a hacker intrusion or attack, and for controlling the types of traffic that can flow between the two networks. Unlike simple Internet sharing NAT routers, a firewall uses a process called stateful packet inspection to protect your network from attacks and intrusions. NAT performs a very limited stateful inspection in that it considers whether the incoming packet is in response to an outgoing request, but true Stateful Packet Inspection goes far beyond NAT.

Using Rules to Block or Allow Specific Kinds of Traffic

This section includes the following topics:

- [“About Services-Based Rules” on page 4-3](#)
- [“Viewing the Rules” on page 4-8](#)
- [“Order of Precedence for Rules” on page 4-8](#)
- [“Setting the Default Outbound Policy” on page 4-9](#)
- [“Creating a LAN WAN Outbound Services Rule” on page 4-9](#)
- [“Creating a LAN WAN Inbound Services Rule” on page 4-10](#)
- [“Inbound Rules Examples” on page 4-13](#)
- [“Outbound Rules Example” on page 4-16](#)
- [“Adding Customized Services” on page 4-16](#)
- [“Setting Quality of Service \(QoS\) Priorities” on page 4-18](#)

Firewall rules are used to block or allow specific traffic passing through from one side to the other. Inbound rules (WAN to LAN) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Outbound rules (LAN to WAN) determine what outside resources local users can have access to.

A firewall has two default rules, one for inbound traffic and one for outbound traffic. The default rules of the FVS318G are:

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

User-defined firewall rules for blocking or allowing traffic on the VPN firewall can be applied to inbound or outbound traffic.

About Services-Based Rules

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

- **Outbound Rules (service blocking).** Outbound traffic is normally allowed unless the firewall is configured to disallow it.
- **Inbound Rules (port forwarding).** Inbound traffic is normally blocked by the firewall unless the traffic is in response to a request from the LAN side. The firewall can be configured to allow this otherwise blocked traffic.
- **Customized Services.** Additional services can be added to the list of services in the factory default list. These added services can then have rules defined for them to either allow or block that traffic (see [“Adding Customized Services”](#) on page 4-16).
- **Quality of Service (QoS) priorities.** Each service at its own native priority that impacts its quality of performance and tolerance for jitter or delays. You can change this QoS priority if desired to change the traffic mix through the system (see [“Setting Quality of Service \(QoS\) Priorities”](#) on page 4-18).

Outbound Rules (Service Blocking)

The FVS318G allows you to block the use of certain Internet services by PCs on your network. This is called service blocking or port filtering.

The default policy can be changed to block all outbound traffic and enable only specific services to pass through the router. The following **Outbound Rules** table lists the configured rules for outgoing traffic. An outbound rule is defined by the following fields:

Table 4-1. Outbound Rules

Item	Description
Service Name	Select the desired Service or application to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see “Adding Customized Services” on page 4-16).
Action (Filter)	Select the desired action for outgoing connections covered by this rule: <ul style="list-style-type: none"> • BLOCK always • BLOCK by schedule, otherwise Allow • ALLOW always • ALLOW by schedule, otherwise Block <p>Note: Any outbound traffic which is not blocked by rules you create will be allowed by the Default rule.</p> <p>ALLOW rules are only useful if the traffic is already covered by a BLOCK rule. That is, you wish to allow a subset of traffic that is currently blocked by another rule.</p>

Table 4-1. Outbound Rules (continued)

Item	Description
Action (Select Schedule)	<p>Select the desired time schedule (Schedule1, Schedule2, or Schedule3) that will be used by this rule.</p> <ul style="list-style-type: none"> • This drop down menu gets activated only when “BLOCK by schedule, otherwise Allow” or “ALLOW by schedule, otherwise Block” is selected as Action. • Use schedule page to configure the time schedules (see “Setting a Schedule to Block or Allow Specific Traffic” on page 4-29).
LAN Users	<p>Specifies which computers on your network are affected by this rule. Select the desired options:</p> <ul style="list-style-type: none"> • Any – All PCs and devices on your LAN. • Single address – Enter the required address and the rule will be applied to that particular PC. • Address range – If this option is selected, you must enter the start and finish fields. • Groups – Select the Group to which this rule will apply. Use the LAN Groups screen (under Network Configuration) to assign PCs to Groups. See “Managing Groups and Hosts (LAN Groups)” on page 3-5.
WAN Users	<p>Specifies which Internet locations are covered by the rule, based on their IP address. Select the desired option:</p> <ul style="list-style-type: none"> • Any – All Internet IP address are covered by this rule. • Single address – Enter the required address in the start field. • Address range – If this option is selected, you must enter the start and end fields.
QoS Priority	<p>Specifies the priority of a service which, in turn, determines the quality of that service for the traffic passing through the firewall. By default, the priority shown is that of the selected service. The user can change it accordingly. If the user does not make a selection (leaves it as Normal-Service), then the native priority of the service will be applied to the policy. See “Setting Quality of Service (QoS) Priorities” on page 4-18.</p>
Log	<p>This determines whether packets covered by this rule are logged. Select the desired action:</p> <ul style="list-style-type: none"> • Always – always log traffic considered by this rule, whether it matches or not. This is useful when debugging your rules. • Never – never log traffic considered by this rule, whether it matches or not.
Bandwidth Profile	<p>Specifies the name of a bandwidth limiting profile. Using a bandwidth profile, bandwidth consumed by different connections can be limited. If multiple connections correspond to the same firewall rule, they will share the same bandwidth limiting. See “Configuring a Bandwidth Profile” on page 4-30.</p>
NAT IP	<p>Specifies whether the source IP address of the outgoing packets should be the WAN interface address or a specified address. If WAN Interface Address is selected, all outgoing packets on WAN will be assigned the WAN interface address. If Single Address is selected, the address entered next to the NAT IP field will be used. This address should belong to the WAN subnet. The WAN Mode must be set to NAT to enable the NAT IP setting.</p>



Note: See “[Configuring Source MAC Filtering](#)” on page 4-24 for yet another way to block outbound traffic from selected PCs that would otherwise be allowed by the firewall.

Inbound Rules (Port Forwarding)

When the FVS318G uses Network Address Translation (NAT), your network presents only one IP address to the Internet and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a Web server or game server) visible and available to the Internet. The rule tells the firewall to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as port forwarding.

Whether or not DHCP is enabled, how the PCs will access 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 may change periodically as the DHCP lease expires. Consider using **Dynamic DNS** (under Network Configuration) so that external users can always find your network (see “[Configuring Dynamic DNS \(Optional\)](#)” on page 2-13).
- If the IP address of the local server PC is assigned by DHCP, it may change when the PC is rebooted. To avoid this, use the Reserved IP address feature in the **LAN Groups** menu (under Network Configuration) to keep the PC’s IP address constant (see “[Configuring DHCP Address Reservation](#)” on page 3-9).
- Local PCs must access the local server using the server’s local LAN address. Attempts by local PCs to access the server using the external WAN IP address will fail.



Note: See “[Configuring Port Triggering](#)” on page 4-27 for yet another way to allow certain types of inbound traffic that would otherwise be blocked by the firewall.

Table 4-2. Inbound Rules

Item	Description
Service	Select the desired Service or application to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see “Adding Customized Services” on page 4-16).
Action (Filter)	Select the desired action for packets covered by this rule: <ul style="list-style-type: none"> • BLOCK always • BLOCK by schedule, otherwise Allow • ALLOW always • ALLOW by schedule, otherwise Block Note: Any inbound traffic which is not allowed by rules you create will be blocked by the Default rule.
Schedule	Select the desired time schedule (Schedule1, Schedule2, or Schedule3) that will be used by this rule (see “Setting a Schedule to Block or Allow Specific Traffic” on page 4-29). <ul style="list-style-type: none"> • This drop down menu gets activated only when “BLOCK by schedule, otherwise Allow” or “ALLOW by schedule, otherwise Block” is selected as Action. • Use schedule page to configure the time schedules.
Send to LAN Server	This field appears only with NAT Routing (not Classical). This LAN address determines which computer on your network is hosting this service rule. (You can also translate this address to a port number.)
Translate to Port Number	Check this box and enter a port number to assign the LAN Server to a different service port number. Inbound traffic to the service port will have the destination port number modified to the port number configured here.
WAN Destination IP Address	Specifies the destination IP address applicable to incoming traffic. This is the public IP address that will map to the internal LAN server; it can either be the address of the WAN port or another public IP address.
LAN users	This field appears only with Classical Routing (not NAT). Specifies which computers on your network are affected by this rule. Select the desired options: <ul style="list-style-type: none"> • Any – All PCs and devices on your LAN. • Single address – Enter the required address and the rule will be applied to that particular PC. • Address range – If this option is selected, you must enter the start and finish fields. • Groups – Select the Group to which this rule will apply. Use the LAN Groups screen (under Network Configuration) to assign PCs to Groups. See “Managing Groups and Hosts (LAN Groups)” on page 3-5.
WAN Users	Specifies which Internet locations are covered by the rule, based on their IP addresses. Select the desired option: <ul style="list-style-type: none"> • Any – All Internet IP address are covered by this rule. • Single address – Enter the required address in the start field. • Address range – If this option is selected, you must enter the start and end fields.

Table 4-2. Inbound Rules (continued)

Item	Description
Log	Specifies whether packets covered by this rule are logged. Select the desired action: <ul style="list-style-type: none">• Always – Always log traffic considered by this rule, whether it matches or not. This is useful when debugging your rules.• Never – Never log traffic considered by this rule, whether it matches or not.
Bandwidth Profile	Specifies the name of a bandwidth limiting profile. Using a bandwidth profile, bandwidth consumed by different connections can be limited. If multiple connections correspond to the same firewall rule, they will share the same bandwidth limiting. See “Configuring a Bandwidth Profile” on page 4-30.



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 may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to the Acceptable Use Policy of your ISP.

Remember that allowing inbound services opens holes in your VPN firewall. Enable only those ports that are necessary for your network. We also recommend enabling the server's application security and configuring user password or privilege levels, if provided.

Viewing the Rules

To view the firewall rules: Select **Security > Firewall** from the main menu. The LAN WAN Rules tab appears:

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout

Services :: Schedule :: Block Sites :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile ::

LAN WAN Rules | DMZ WAN Rules | LAN DMZ Rules | Attack Checks | Session Limit

Default Outbound Policy: Allow Always

Operation succeeded.

Outbound Services

	!	Service Name	Filter	LAN Users	WAN Users	Priority	Bandwidth Profile	Log	Action
<input type="checkbox"/>	<input checked="" type="radio"/>	AIM	Block by schedule 1 else allow	ANY	ANY	Normal-Service	NONE	Never	<input type="button" value="up"/> <input type="button" value="down"/> <input type="button" value="edit"/>

enable disable

Inbound Services

	!	Service Name	Filter	LAN Server IP Address	LAN Users	WAN Users	Destination	Bandwidth Profile	Log	Action
<input type="checkbox"/>	<input checked="" type="radio"/>	FTP	Allow Always	192.168.1.21		ANY	WAN1	NONE	Never	<input type="button" value="up"/> <input type="button" value="down"/> <input type="button" value="edit"/>
<input type="checkbox"/>	<input checked="" type="radio"/>	HTTP	Allow by schedule 2 else block	192.168.1.11:8080		ANY	172.16.30.57	NONE	Never	<input type="button" value="up"/> <input type="button" value="down"/> <input type="button" value="edit"/>

enable disable

Figure 4-1

Order of Precedence for Rules

As you define new rules, they are added to the tables in the Rules menu as the last item in the list, as shown in [Figure 4-1](#). For any traffic attempting to pass through the firewall, the packet information is subjected to the rules in the order shown in the Rules Table, beginning at the top

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

Setting the Default Outbound Policy

The Default Outbound Policy is to allow all traffic to the Internet to pass through. Firewall rules can then be applied to block specific types of traffic from going out from the LAN to the Internet (Outbound). The default policy of Allow Always can be changed to block all outbound traffic which then allows you to enable only specific services to pass through the VPN firewall.

To change the Default Outbound Policy, follow these steps:

1. Click the LAN WAN Rules tab, shown in [Figure 4-1](#).
2. Change the **Default Outbound Policy** by choosing Block Always from the drop-down menu.
3. Click **Apply**.

Creating a LAN WAN Outbound Services Rule

An outbound rule will block or allow the selected application from an internal IP LAN address to an external WAN IP address according to the schedule created in the Schedule menu.

You can also tailor these rules to your specific needs (see [“Administrator Tips” on page 4-33](#)).



Note: This feature is for Advanced Administrators only! Incorrect configuration will cause serious problems.

To create a new outbound service rule in the LAN WAN Rules tab:

1. Click **Add** under the Outbound Services Table. The **Add LAN WAN Outbound Service** screen is displayed..

The screenshot displays the 'Add LAN WAN Outbound Service' configuration window. At the top, a message indicates 'Operation succeeded.' Below this is the 'Outbound Service' configuration area. The 'Service' dropdown is set to 'ANY', 'Action' is 'BLOCK always', and 'Select Schedule' is 'Schedule 1'. The 'LAN Users' and 'WAN Users' dropdowns are both set to 'Any'. The 'QoS Priority' is set to 'Normal-Service', 'Log' is 'Never', and 'Bandwidth Profile' is 'NONE'. The 'NAT IP' is set to 'WAN Interface Address'. There are two sets of 'Start' and 'Finish' time pickers, each consisting of four input boxes. At the bottom, there are 'Apply' and 'Reset' buttons.

Figure 4-2

2. Configure the parameters based on the descriptions in [Table 4-1 on page 4-3](#).
3. Click **Apply** to save your changes and reset the fields on this screen. The new rule will be listed on the **Outbound Services** table.

Creating a LAN WAN Inbound Services Rule

This Inbound Services Rules table lists all existing rules for inbound traffic. If you have not defined any rules, no rules will be listed. By default, all inbound traffic is blocked. Remember that allowing inbound services opens holes in your firewall. Only enable those ports that are necessary for your network.

To create a new inbound service rule in the LAN WAN Rules tab:

1. Click **Add** under the Inbound Services Table. The **Add LAN WAN Inbound Service** screen is displayed.

Figure 4-3


2. Configure the parameters based on the descriptions in [Table 4-2 on page 4-6](#).
3. Click **Apply** to save your changes and reset the fields on this screen. The new rule will be listed on the **Inbound Services** table.

Modifying Rules

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

1. In the **Action** column adjacent to the rule, do the following:
 - Click **Edit** to make any changes to the rule definition of an existing rule. The Outbound Service or Inbound Service screen is displayed containing the data for the selected rule.
 - Click **Up** to move the rule up one position in the table rank.

- Click **Down** to move the rule down one position in the table rank.

	Note: Since rules are applied in the order listed (from top to bottom), the order of the rules may make a difference in how traffic is handled.
---	--

2. Check the box adjacent to the rule, then do any of the following:

- Click **Enable** to enable the rule. The “!” Status icon will turn green.
- Click **Disable** to disable the policy. A rule can be disabled if not in use and enabled as needed. Disabling a rule does not delete the configuration, but merely de-activates the rule. The status circle will change from green to grey, indicating that the rule is disabled. (By default, when a rule is added to the table it is automatically enabled.)
- Click **Delete** to delete the rule.

Inbound Rules Examples

LAN WAN Inbound Rule: Hosting A Local Public Web Server

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

The screenshot shows the 'Add LAN WAN Inbound Service' configuration window. At the top, a message box says 'Operation succeeded.'. Below that, the 'Inbound Service' configuration is shown. The 'Service' is set to 'HTTP'. The 'Action' is 'ALLOW always'. The 'Select Schedule' is 'Schedule 1'. The 'Send to LAN Server' is '192.168.1.99'. The 'Translate to Port Number' checkbox is unchecked. The 'WAN Destination IP Address' is 'Broadband'. The 'LAN Users' is 'Any'. The 'WAN Users' is 'Any'. The 'Log' is 'Never'. The 'Bandwidth Profile' is 'NONE'. There are also empty fields for 'Start' and 'Finish' times on the right side. At the bottom, there are 'Apply' and 'Reset' buttons.

Figure 4-4

In the example shown in [Figure 4-4](#), unrestricted access is provided from the Internet to the local Web server at LAN IP address 192.168.1.99.

LAN WAN Inbound Rule: Allowing Videoconference from Restricted Addresses

If you want to allow incoming videoconferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office, you can create an inbound rule.

In the example shown in [Figure 4-5](#), CU-SeeMe connections are allowed to a local host only from a specified range of external IP addresses. Connections are blocked during the period specified by Schedule 1.

Operation succeeded.

Add LAN WAN Inbound Service

Service: CU-SEEME:UDP
Action: BLOCK by schedule, otherwise allow
Select Schedule: Schedule 1
Send to LAN Server: 192.168.1.11
Translate to Port Number :
WAN Destination IP Address: Broadband
LAN Users: Any
WAN Users: Address Range
Log: Never
Bandwidth Profile: NONE

Start:
Finish:
Start: 172.16.88.1
Finish: 172.16.88.254

Apply Reset

Figure 4-5

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

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. One of these public IP addresses will be used as the primary IP address of the VPN firewall. This address will be used to provide Internet access to your LAN PCs through NAT. The other addresses are available to map to your servers.

In the example shown in [Figure 4-6](#), we have configured multi-NAT to support multiple public IP addresses on one WAN interface. The inbound rule instructs the VPN firewall to host an additional public IP address (10.1.0.5) and to associate this address with the Web server on the LAN (at 192.168.1.2). We also instruct the VPN firewall to translate the incoming HTTP port number (port 80) to a different port number (port 8080).

The screenshot shows the 'Add LAN WAN Inbound Service' configuration window. At the top, a message states 'Operation succeeded.' Below this, the configuration is as follows:

- Service:** HTTP
- Action:** ALLOW always
- Select Schedule:** Schedule 1
- Send to LAN Server:** 192.168.1.11
- Translate to Port Number:** 8080
- WAN Destination IP Address:** Other Public IP Address (10.1.0.5)
- LAN Users:** Any
- WAN Users:** Any
- Log:** Never
- Bandwidth Profile:** NONE

Buttons for 'Apply' and 'Reset' are located at the bottom of the configuration area.

Figure 4-6

The following addressing scheme is used in this example:

- VPN firewall FVS318G
 - WAN1 primary public IP address: 10.1.0.1
 - WAN1 additional public IP address: 10.1.0.5
 - LAN IP address 192.168.1.1
- Web server PC on the VPN firewall's LAN
 - LAN IP address: 192.168.1.11
 - Port number for Web service: 8080

To test the connection from a PC on the WAN side, type **http://10.1.0.5**. The home page of the Web server should appear.

LAN WAN Inbound Rule: Specifying an Exposed Host

Specifying an exposed host allows you to set up a computer or server that is available to anyone on the Internet for services that you have not yet defined.

To expose one of the PCs on your LAN as this host:

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



Note: For security, NETGEAR strongly recommends that you avoid creating an exposed host. When a computer on your LAN 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.

Outbound Rules Example

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

LAN WAN Outbound Rule: Blocking Instant Messenger

To block Instant Messenger usage by employees during working hours, you can create an outbound rule to block that application from any internal IP address to any external address according to the schedule that you have created in the Schedule menu. You can also have the firewall log any attempt to use Instant Messenger during that blocked period.

Adding Customized Services

Services are functions performed by server computers at the request of client computers. For example, Web servers serve Web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server computer, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (Web server) request.

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application.

Although the FVS318G already holds a list of many service port numbers, you are not limited to these choices. Use the Services screen to add additional services and applications to the list for use in defining firewall rules. The Services menu shows a list of services that you have defined, as shown in Figure 4-7.

To define a new service, you must first determine which port number or range of numbers is used by the application. This information can usually be determined by contacting the publisher of the application or from user groups or newsgroups. When you have the port number information, you can enter it on the **Services** screen. You can configure up to 125 custom services.

To add a custom service:

1. Select **Security > Services** from the main menu. The **Services** screen is displayed.

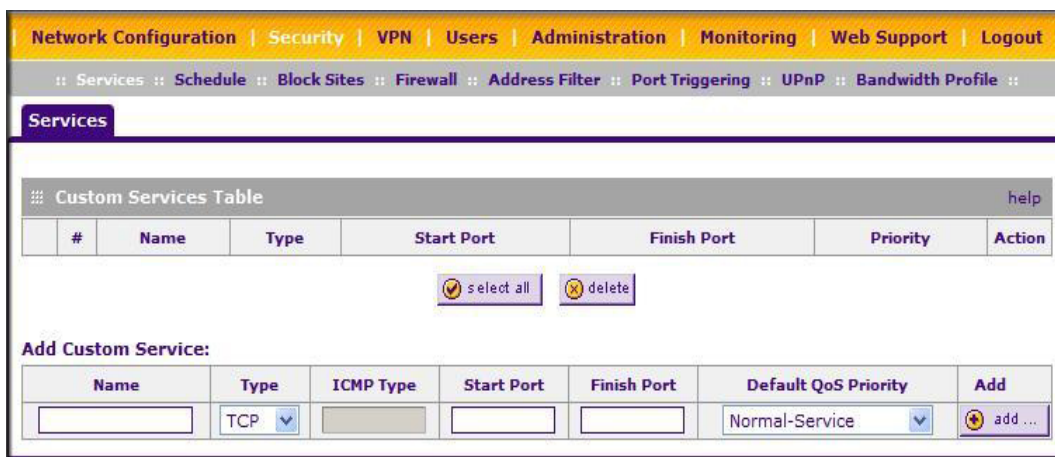


Figure 4-7

2. In the **Add Custom Services** section, enter a descriptive name for the service (this name is for your convenience).
3. Select the Layer 3 transport protocol of the service: TCP, UDP, or ICMP.
4. For TCP or UDP services, enter the first port of the range that the service uses. For ICMP services, enter the ICMP Type number.
5. For TCP or UDP services, enter the last port of the range that the service uses. If the service only uses a single port number, enter the same number in both fields.
6. Click **Add**. The new custom service will be added to the Custom Services Table.

Modifying a Service

To edit the parameters of an existing service:

1. In the Custom Services Table, click the **Edit** button adjacent to the service you want to edit. The **Edit Service** screen is displayed.
2. Modify the parameters you wish to change.
3. Click **Apply** to confirm your changes. The modified service is displayed in the Custom Services Table.

Setting Quality of Service (QoS) Priorities

The QoS setting determines the priority of a service, which in turn determines the quality of that service for the traffic passing through the firewall. You can change the QoS Priority:

- On the **Services** screen in the Custom Services Table for customized services (see [Figure 4-7](#)).
- On the **Add LAN WAN Outbound Services** screen:

The screenshot shows the 'Add LAN WAN Outbound Service' configuration window. At the top, a message box indicates 'Operation succeeded.' Below this, the configuration area is titled '# Outbound Service' and includes a help icon. The settings are as follows:

- Service: ANY
- Action: BLOCK always
- Select Schedule: Schedule 1
- LAN Users: Any
- WAN Users: Any
- QoS Priority: Normal-Service (indicated by a black arrow)
- Log: Never
- Bandwidth Profile: NONE
- NAT IP: WAN Interface Address

There are also four empty IP address input fields on the right side of the configuration area. At the bottom, there are 'Apply' and 'Reset' buttons.

Figure 4-8

The QoS priority definition for a service determines the queue that is used for the traffic passing through the VPN firewall. A priority is assigned to IP packets using this service. Priorities are defined by the “Type of Service (ToS) in the Internet Protocol Suite” standards, RFC 1349. A ToS priority for traffic passing through the VPN firewall is one of the following:

- **Normal-Service.** No special priority given to the traffic. The IP packets for services with this priority are marked with a ToS value of 0.
- **Minimize-Cost.** Used when the data must be transferred over a link that has a low transmission cost. The IP packets for this service priority are marked with a ToS value of 1.
- **Maximize-Reliability.** Used when data needs to travel to the destination over a reliable link with little or no retransmission. The IP packets for this service priority are marked with a ToS value of 2.
- **Maximize-Throughput.** Used when the volume of data transferred during an interval is important even if the latency over the link is high. The IP packets for services with this priority are marked with a ToS value of 4.
- **Minimize-Delay.** Used when the time required for the packet to reach the destination must be short (low link latency). The IP packets for this service priority are marked with a ToS value of 8.

Attack Checks

The Attack Checks menu allows you to specify whether or not the VPN firewall should be protected against common attacks in the LAN and WAN networks. To enable the appropriate Attack Checks for your environment:

1. Select **Security > Firewall** from the main menu and click **Attack Checks** to display the **Attack Checks** tab page.

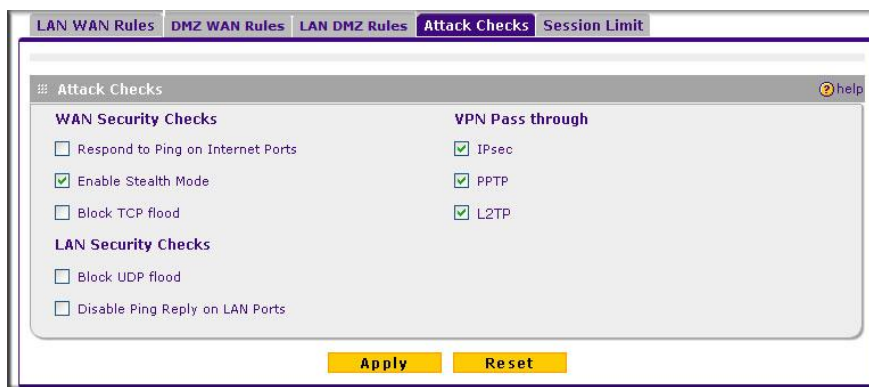


Figure 4-9

2. Check the boxes for the Attack Checks you wish to monitor. The various types of attack checks are listed and defined below.
3. Click **Apply** to save your settings.

The various types of attack checks listed on the **Attack Checks** screen are:

- **WAN Security Checks**

- **Respond To Ping On Internet Ports**—By default, the VPN firewall does not respond to an ICMP Echo (ping) packet coming from the Internet or WAN side. We recommend that you leave this option disabled to prevent hackers from easily discovering the VPN firewall via a ping, but it can be enabled as a diagnostic tool for connectivity problems.
- **Enable Stealth Mode**—In stealth mode, the VPN firewall will not respond to port scans from the WAN or Internet, which makes it less susceptible to discovery and attacks.
- **Block TCP Flood**. A SYN flood is a form of denial of service attack in which an attacker sends a succession of SYN requests to a target system. When the system responds, the attacker doesn't complete the connection, thus saturating the server with half-open connections. No legitimate connections can then be made.

When blocking is enabled, the VPN firewall will limit the lifetime of partial connections and will be protected from a SYN flood attack.

- **LAN Security Checks**

- **Block UDP flood**—A UDP flood is a form of denial of service attack in which the attacking machine sends a large number of UDP packets to random ports to the victim host. As a result, the victim host will check for the application listening at that port, see that no application is listening at that port, and reply with an ICMP Destination Unreachable packet.

When the victimized system is flooded, it is forced to send many ICMP packets, eventually making it unreachable by other clients. The attacker may also spoof the IP address of the UDP packets, ensuring that the excessive ICMP return packets do not reach him, making the attacker's network location anonymous.

If flood checking is enabled, the VPN firewall will not accept more than 20 simultaneous, active UDP connections from a single computer on the LAN.

- **Disable Ping Reply on LAN Ports**. To prevent the VPN firewall from responding to Ping requests from the LAN, click this checkbox.

- **VPN Pass through**—When the FVS318G is in NAT mode, all packets going to the Remote VPN Gateway are first filtered through NAT and then encrypted per the VPN policy.

If a VPN client or gateway on the LAN side of the VPN firewall wants to connect to another VPN endpoint on the WAN, with the FVS318G between the two VPN end points, all encrypted packets will be sent to the FVS318G. Since the FVS318G filters the encrypted packets through NAT, the packets become invalid.

IPSec, PPTP, and L2TP represent different types of VPN tunnels that can pass through the FVS318G. To allow the VPN traffic to pass through without filtering, enable those options for the type of tunnel(s) that will pass through the FVS318G.

Blocking Internet Sites (Content Filtering)

To restrict internal LAN users from access to certain sites on the Internet, you can use the VPN firewall router's Content Filtering and Web Components filtering. By default, these features are disabled; all requested traffic from any Web site is allowed. If you enable one or more of these features and users try to access a blocked site, they will see a "Blocked by NETGEAR" message.

Several types of blocking are available:

- **Web Components blocking.** You can filter the following Web Component types: Proxy, Java, ActiveX, and Cookies. For example, by enabling Java filtering, "Java" files will be blocked. Certain commonly used web components can be blocked for increased security. Some of these components are can be used by malicious websites to infect computers that access them.
 - **Proxy.** A proxy server (or simply, proxy) allows computers to route connections to other computers through the proxy, thus circumventing certain firewall rules. For example, if connections to a specific IP address are blocked by a firewall rule, the requests can be routed through a proxy that is not blocked by the rule, rendering the restriction ineffective. Enabling this feature blocks proxy servers.
 - **Java.** Blocks java applets from being downloaded from pages that contain them. Java applets are small programs embedded in web pages that enable dynamic functionality of the page. A malicious applet can be used to compromise or infect computers. Enabling this setting blocks Java applets from being downloaded.
 - **ActiveX.** Similar to Java applets, ActiveX controls install on a Windows computer running Internet Explorer. A malicious ActiveX control can be used to compromise or infect computers. Enabling this setting blocks ActiveX applets from being downloaded.

- **Cookies.** Cookies are used to store session information by websites that usually require login. However, several websites use cookies to store tracking information and browsing habits. Enabling this option filters out cookies from being created by a website..



Note: Many websites require that cookies be accepted in order for the site to be accessed properly. Blocking cookies may interfere with useful functions provided by these websites.

- **Keyword Blocking (Domain Name Blocking).** You can specify up to 32 words that, should they appear in the Web site name (URL) or in a newsgroup name, will cause that site or newsgroup to be blocked by the VPN firewall router.

You can apply the keywords to one or more groups. Requests from the PCs in the groups for which keyword blocking has been enabled will be blocked. Blocking does not occur for the PCs that are in the groups for which keyword blocking has not been enabled.

You can bypass Keyword blocking for trusted domains by adding the exact matching domain to the list of Trusted Domains. Access to the domains or keywords on this list by PCs, even those in the groups for which keyword blocking has been enabled, will still be allowed without any blocking.

Keyword application examples:

- If the keyword “XXX” is specified, the URL <http://www.badstuff.com/xxx.html> is blocked, as is the newsgroup alt.pictures.XXX.
- If the keyword “.com” is specified, only Web sites with other domain suffixes (such as .edu or .gov) can be viewed.
- To block all Internet browsing access, enter the keyword “.”.

To enable Content Filtering:

1. Select **Security > Block Sites** to display the **Block Sites** screen.

The screenshot shows the 'Block Sites' configuration page. It is divided into several sections:

- Content Filtering:** A section with a 'Turn Content Filtering On?' prompt and two radio buttons: 'Yes' (unselected) and 'No' (selected).
- Web Components:** A section with four checkboxes: 'Proxy', 'Java', 'ActiveX', and 'Cookies', all of which are currently unchecked.
- Buttons:** Two yellow buttons labeled 'Apply' and 'Reset' are positioned below the Web Components section.
- Apply Keyword Blocking to:** A table with a header 'Group Name' and eight rows labeled 'Group1' through 'Group8'. Each row has a checkbox on the left, all of which are checked. Below the table are three buttons: 'select all' (checked), 'enable' (green), and 'disable' (radio button).
- Blocked Keywords:** A section with a table header 'Blocked Keyword' and 'Action'. Below the table are 'select all' and 'delete' buttons. There is an 'Add Blocked Keyword:' section with a text input field and an 'Add' button.
- Trusted Domains:** A section with a table header 'Trusted Domains' and 'Action'. Below the table are 'select all' and 'delete' buttons. There is an 'Add Trusted Domain:' section with a text input field and an 'Add' button.

Figure 4-10

2. Select **Yes** to enable Content Filtering.

3. Click **Apply** to activate the menu controls.
4. Select any **Web Components** you wish to block and click **Apply**.
5. Select the groups to which Keyword Blocking will apply, then click **Enable** to activate Keyword blocking (or disable to deactivate Keyword Blocking).
6. Enter your list of blocked Keywords or Domain Names in the **Blocked Keyword** fields. After each entry, click **Add**. The Keyword or Domain name will be added to the **Blocked Keywords** table. (You can also edit an entry by clicking **Edit** in the Action column adjacent to the entry.)
7. In the **Add Trusted Domain** table, enter the name(s) of any domain for which the keyword filtering will be bypassed and click **Add**. The Trusted Domain will appear in the **Trusted Domains** table and will be exempt from filtering.

Configuring Source MAC Filtering

Source MAC Filter will drop or allow the Internet-bound traffic received from PCs with specified MAC addresses.

- By default, the source MAC address filter is disabled. Traffic received from any MAC address is allowed.
- When the source MAC address filter is enabled, outbound Internet traffic will be filtered using the **MAC Addresses** list in this menu. You can choose to block MAC addresses in the list or to allow only those addresses in the list.



Note: For additional ways of restricting outbound traffic, see “[Outbound Rules \(Service Blocking\)](#)” on page 4-3

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

1. Select **Security > Address Filter > Source MAC Filter** to display the **Source MAC Filter** tab page.

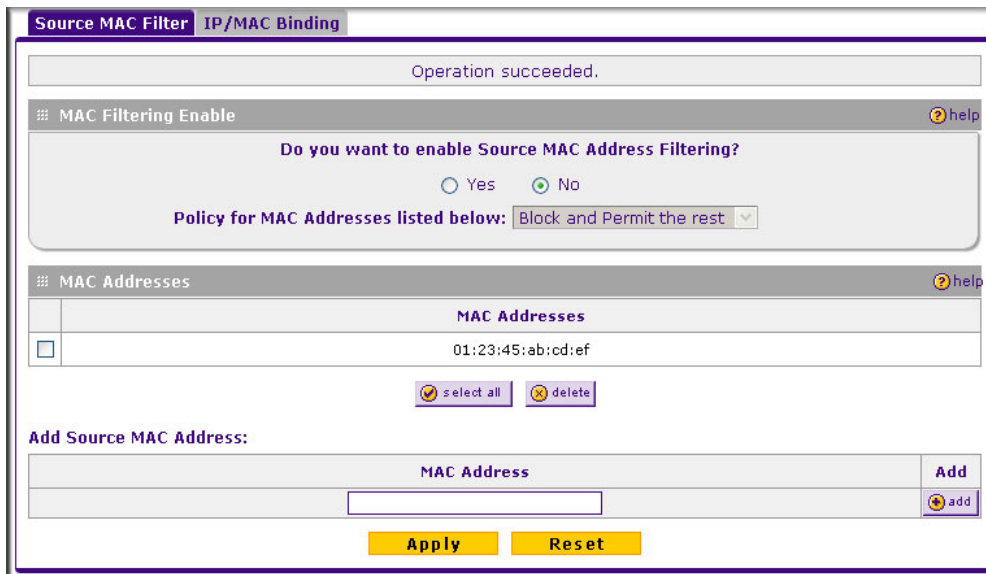


Figure 4-11

2. Click **Yes** to enable **Source MAC Filtering**.
3. Select the action to be taken on outbound traffic from the listed MAC addresses:
 - Block this list and permit all other MAC addresses
 - Permit this list and block all other MAC addresses
4. Enter a MAC Address in the **Add Source MAC Address** box and click **Add**. The MAC address will appear in the **MAC Addresses** table. Repeat this process to add additional MAC addresses.

A valid MAC address is six colon-separated pairs of hexadecimal digits (0 to 9 and a to f). For example: 01:23:45:ab:cd:ef.

5. Click **Add**. The MAC address will be added to the **MAC Addresses** table.
6. Click **Apply** to save your settings.

To remove an entry from the table, select the MAC address entry and click **Delete**.

Configuring IP/MAC Address Binding Alerts

You can configure the FVS318G to drop packets and generate an alert when a device appears to have hijacked or spoofed another device's IP address. An IP address can be bound to a specific MAC address either by using a DHCP reserved address (see [“Configuring DHCP Address Reservation”](#) on page 3-9) or by manually binding in the IP/MAC Binding menu.

To enable IP/MAC address binding enforcement and alerts:

1. Select **Security > Address Filter > IP/MAC Binding** to display the **Source MAC Filter** tab page.

The screenshot shows the 'IP/MAC Binding' configuration page. At the top, there is a message 'Operation succeeded.' Below that is a section titled 'Email IP/MAC Violations' with a question: 'Do you want to enable E-mail Logs for IP/MAC Binding Violation?'. There are two radio buttons: 'Yes' (selected) and 'No'. A note below says '* For this option e-mailing of logs must be enabled in [Firewall Logs & E-mail page](#)'. There are 'Apply' and 'Reset' buttons. Below this is a table titled 'IP/MAC Bindings' with columns: Name, MAC Addresses, IP Addresses, Log Dropped Packets, and Action. The table contains one entry: 'fileserver' with MAC '01:23:45:67:89:ab' and IP '192.168.1.25'. There are 'select all' and 'delete' buttons below the table. At the bottom is a form titled 'Add IP/MAC Binding:' with fields for Name, MAC Address, IP Address (split into four boxes), Log Dropped Packets (set to 'Disable'), and an 'add' button.

Figure 4-12

2. In the Email IP/MAC Violations frame, check the **Yes** radio button to enable IP/MAC address binding enforcement and alerts. Email alerts must be enabled (see [“E-Mail Notifications of Event Logs and Alerts”](#) on page 4-33).
3. Click **Apply**.

4. To add a manual binding entry, enter the following data in the **Add IP/MAC Bindings** section:
 - a. Enter a **Name** for the bound host device.
 - b. Enter the **MAC Address** and **IP Address** to be bound. A valid MAC address is six colon-separated pairs of hexadecimal digits (0 to 9 and a to f). For example: 01:23:45:ab:cd:ef.
 - c. From the pull-down list, select whether dropped packets should be logged to a special counter. To view the counter, click the **Set Poll Interval** link at the top of the menu.
5. Click **Apply**. The specified binding will be added to the list.

Configuring Port Triggering

Port triggering allows some applications to function correctly that would otherwise be partially blocked by the firewall when the router is in NAT mode. Some applications require that when external devices connect to them, they receive data on a specific port or range of ports. The router must send all incoming data for that application only on the required port or range of ports. Using this feature requires that you know the port numbers used by the application.

Port triggering allows computers on the private network (LAN) to request that one or more ports be forwarded to them. Unlike basic port forwarding which forwards ports to only one preconfigured IP address, port triggering waits for an outbound request from the private network on one of the defined outgoing ports. It then automatically sets up forwarding to the IP address that sent the request. When the application ceases to transmit data over the port, the router waits for a timeout interval and then closes the port or range of ports, making them available to other computers on the private network.


Once configured, port triggering operates as follows:

1. A PC makes an outgoing connection using a port number defined in the Port Triggering table.
2. The VPN firewall records this connection, opens the additional incoming port or ports associated with this entry in the Port Triggering table, and associates them with the PC.
3. The remote system receives the PC's request and responds using the different port numbers that you have now opened.
4. The VPN firewall router matches the response to the previous request, and forwards the response to the PC.

Without Port Triggering, this response would be treated as a new connection request rather than a response. As such, it would be handled in accordance with the inbound service rules.

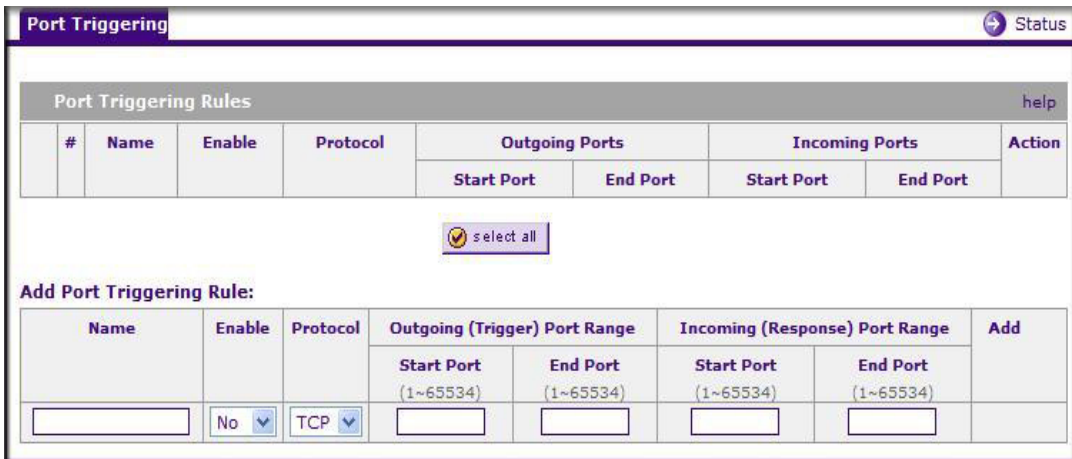
Note these restrictions with Port Triggering:

- Only one PC can use a port triggering application at any time.
- After a PC has finished using a port triggering application, there is a time-out period before the application can be used by another PC. This is required because the VPN firewall router cannot be sure when the application has terminated.

	Note: For additional ways of allowing inbound traffic, see “ Inbound Rules (Port Forwarding) ” on page 4-5.
---	--

To add a port triggering rule:

1. Select **Security > Port Triggering** to display the **Port Triggering** tab page.



Port Triggering Rules								help
#	Name	Enable	Protocol	Outgoing Ports		Incoming Ports		Action
				Start Port	End Port	Start Port	End Port	
<input checked="" type="checkbox"/> select all								
Add Port Triggering Rule:								
Name	Enable	Protocol	Outgoing (Trigger) Port Range		Incoming (Response) Port Range		Add	
<input type="text"/>	No	TCP	Start Port (1~65534)	End Port (1~65534)	Start Port (1~65534)	End Port (1~65534)	<input type="button" value="Add"/>	

Figure 4-13

2. Enter a user-defined name for this rule in the **Name** field.
3. From the **Enable** pull-down menu, indicate if the rule is enabled or disabled.
4. From the **Protocol** pull-down menu, choose either TCP or UDP transport protocol.
5. In the **Outgoing (Trigger) Port Range** fields:
 - a. Enter the **Start Port** range (1 - 65534).
 - b. Enter the **End Port** range (1 - 65534).

6. In the **Incoming (Response) Port Range** fields:
 - a. Enter the **Start Port** range (1 - 65534).
 - b. Enter the **End Port** range (1 - 65534).
7. Click **Add**. The port triggering rule will be added to the **Port Triggering Rules** table.

To check the status of the port triggering rules, click the **Status** option arrow to the right of the tab on the **Port Triggering** screen. The following data is displayed:

- Rule – The name of the port triggering rule.
- LAN IP Address – The IP address of the PC currently using this rule.
- Open Ports – The incoming ports associated with this rule. Incoming traffic using these ports will be sent to the LAN IP address above.
- Time Remaining – The time remaining before this rule is released, and thus available for other PCs. The timer is reset whenever incoming or outgoing traffic is received.

Setting a Schedule to Block or Allow Specific Traffic

Schedules define the timeframes under which firewall rules may be applied.

The screenshot shows the 'Schedule 1' configuration page. It has three tabs: 'Schedule 1', 'Schedule 2', and 'Schedule 3'. The 'Scheduled Days' section has a question: 'Do you want this schedule to be active on all days or specific days?'. Below this, 'All Days' is selected with a radio button, and 'Specific Days' is unselected. To the right, there are checkboxes for Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday, all of which are currently unchecked. The 'Scheduled Time of Day' section has a question: 'Do you want this schedule to be active all day or at specific times during the day?'. Below this, 'All Day' is selected with a radio button, and 'Specific Times' is unselected. To the right, there are 'Start Time' and 'End Time' fields, each with a dropdown for 'Hour' (set to 12), a dropdown for 'Minute' (set to 00), and a dropdown for 'AM/PM' (set to AM for start and PM for end). At the bottom of the form are two yellow buttons: 'Apply' and 'Reset'.

Figure 4-14

Three schedules, Schedule 1, Schedule 2 and Schedule3 can be defined, and any one of these can be selected when defining firewall rules.

To invoke rules based on a schedule, follow these steps:

1. Select **Security > Schedule** to display the **Schedule 1** tab page.
2. Check the radio button for All Days or Specific Days. If you chose Specific Days, check the radio button for each day you want the schedule to be in effect.
3. Check the radio button to schedule the time of day: All Day, or Specific Times. If you chose Specific Times, enter the Start Time and End Time fields (Hour, Minute, AM/PM), which will limit access during certain times for the selected days.
4. Click **Apply** to save your settings to **Schedule 1**.

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

Configuring a Bandwidth Profile

To prevent one user or group from using excessive inbound or outbound bandwidth, you can define a bandwidth profile to set a minimum and maximum bandwidth for an individual or group. You can apply a defined profile in a firewall rule to limit specific protocols or all traffic (see “Using Rules to Block or Allow Specific Kinds of Traffic” on page 4-2).

To create a bandwidth profile:

1. Select **Security > Bandwidth Profile** from the submenu. The **Bandwidth Profile** menu will display showing a list of existing profiles.

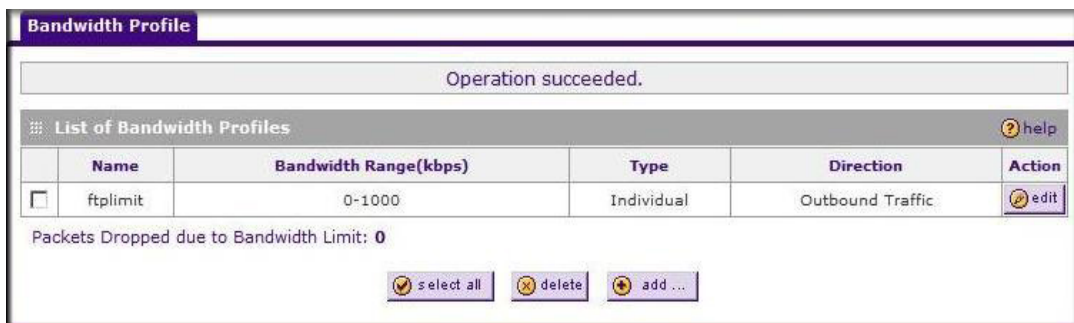


Figure 4-15

- To create a new bandwidth profile, click **add**. The **Add Bandwidth Profile** menu will display.

The screenshot shows the 'Add Bandwidth Profile' configuration page. The navigation bar includes 'Network Configuration', 'Security', 'VPN', 'Users', 'Administration', 'Monitoring', 'Web Support', and 'Logout'. The breadcrumb trail is 'Services :: Schedule :: Block Sites :: Firewall :: Address Filter :: Port Triggering :: UPnP :: Bandwidth Profile ::'. The main form area is titled 'Add Bandwidth Profile' and contains the following fields:

- Profile Name:
- Minimum Bandwidth: (0 - Max. Bandwidth Kbps)
- Maximum Bandwidth: (100 - 100000 Kbps)
- Type:
- Direction:

At the bottom of the form are two buttons: **Apply** and **Reset**.

Figure 4-16

- Enter the following data in the **Bandwidth Profile** section:
 - Enter a **Profile Name**. This name will become available in the firewall rules definition menus.
 - Enter the **Minimum Bandwidth** and **Maximum Bandwidth** to be allowed.
 - From the **Type** pull-down box, select whether the profile will apply to a group or individual.
 - From the **Direction** pull-down box, select whether the profile will apply to outbound or inbound traffic.
- Click **Apply**. The new bandwidth profile will be added to the list.

Configuring Session Limits

To prevent one user or group from using excessive system resources, you can limit the total number of IP sessions allowed through the FVS318G for an individual or group. You can specify the maximum number of sessions by either a percentage of maximum sessions or an absolute number of maximum sessions. Session limiting is disabled by default.

To configure session limits:

1. Select **Security > Firewall > Session Limit** to display the Session Limit tab page.

The screenshot shows the 'Session Limit' configuration page. At the top, there are tabs for 'LAN WAN Rules', 'DMZ WAN Rules', 'LAN DMZ Rules', 'Attack Checks', and 'Session Limit'. The 'Session Limit' tab is active. Below the tabs, there is a section titled 'Session Limit' with a 'help' icon. The main content area contains a question: 'Do you want to enable Session Limit?'. There are two radio buttons: 'Yes' (unselected) and 'No' (selected). Below this, there is a 'User Limit Parameter' dropdown menu set to 'Percentage of Max Sessions'. A 'User Limit' input field is set to '0'. Below that, it says 'Total Number of Packets Dropped due to Session Limit: 0'. Below this section is another section titled 'Session Timeout' with a 'help' icon. It contains three input fields: 'TCP Timeout: 1200 (Seconds)', 'UDP Timeout: 180 (Seconds)', and 'ICMP Timeout: 30 (Seconds)'. At the bottom of the page, there are two yellow buttons: 'Apply' and 'Reset'.

Figure 4-17

2. Click **Yes** to enable Session Limits.
3. In the pull-down menu, select whether you will limit sessions by percentage or by absolute number. The percentage is computed based on the total connection capacity of the device. When setting a limit based on absolute number, note that some protocols (for example, FTP and RSTP) create two sessions per connection.
4. Click **Apply**.

To monitor session limiting, return to this menu periodically and check the display of **Total Number of Packets Dropped due to Session Limit**, which indicates that session limits have been reached.

E-Mail Notifications of Event Logs and Alerts

The Firewall Logs can be configured to log and then e-mail denial of access, general attack information, and other information to a specified e-mail address. For example, your VPN firewall router will log security-related events such as: accepted and dropped packets on different segments of your LAN; denied incoming and outgoing service requests; hacker probes and login attempts; and other general information based on the settings you input on the **Firewall Logs & E-mail** menu. In addition, if you have set up Content Filtering on the Block Sites screen (see [“Blocking Internet Sites \(Content Filtering\)” on page 4-21](#)), a log will be generated when someone on your network tries to access a blocked site.

To configure e-mail or syslog notification, or to view the logs, see [“Activating Notification of Events and Alerts” on page 9-4](#).

Administrator Tips

Consider the following operational items:

1. As an option, you can enable remote management if you have to manage distant sites from a central location (see [“Enabling Remote Management Access” on page 7-10](#)).
2. Although rules (see [“Using Rules to Block or Allow Specific Kinds of Traffic” on page 4-2](#)) are the basic way of managing the traffic through your system, you can further refine your control with the following optional features of the VPN firewall:
 - Groups and hosts (see [“Managing Groups and Hosts \(LAN Groups\)” on page 3-5](#))
 - Services (see [“About Services-Based Rules” on page 4-3](#))
 - Schedules (see [“Setting a Schedule to Block or Allow Specific Traffic” on page 4-29](#))
 - Block sites (see [“Blocking Internet Sites \(Content Filtering\)” on page 4-21](#))
 - Source MAC filtering (see [“Configuring Source MAC Filtering” on page 4-24](#))
 - Port triggering (see [“Configuring Port Triggering” on page 4-27](#))

Chapter 5

Virtual Private Networking Using IPsec

This chapter describes how to use the IPsec virtual private networking (VPN) features of the ProSafe VPN Firewall to provide secure, encrypted communications between your local network and a remote network or computer.

This chapter contains the following sections:

- “Using the VPN Wizard for Client and Gateway Configurations” on page 5-1
- “Testing the Connections and Viewing Status Information” on page 5-11
- “Managing VPN Policies” on page 5-14
- “Configuring Extended Authentication (XAUTH)” on page 5-17
- “Assigning IP Addresses to Remote Users (ModeConfig)” on page 5-21
- “Configuring Keepalives and Dead Peer Detection” on page 5-27
- “Configuring NetBIOS Bridging with VPN” on page 5-29

Using the VPN Wizard for Client and Gateway Configurations

You use the VPN Wizard to configure multiple gateway or client VPN tunnel policies.

The section below provides wizard and NETGEAR *VPN Client* configuration procedures for the following scenarios:

- Using the wizard to configure a VPN tunnel between 2 VPN gateways
- Using the wizard to configure a VPN tunnel between a VPN gateway and a VPN client

Configuring a VPN tunnel connection requires that all settings and parameters on both sides of the VPN tunnel match or mirror each other precisely, which can be a daunting task. The VPN Wizard efficiently guides you through the setup procedure with a series of questions that will determine the IPsec keys and VPN policies it sets up. The VPN Wizard will also set the parameters for the network connection: Security Association, traffic selectors, authentication algorithm, and encryption. The parameters used by the VPN wizard are based on the recommendations of the VPN Consortium (VPNC), an organization that promotes multi-vendor VPN interoperability.

Creating Gateway to Gateway VPN Tunnels with the Wizard

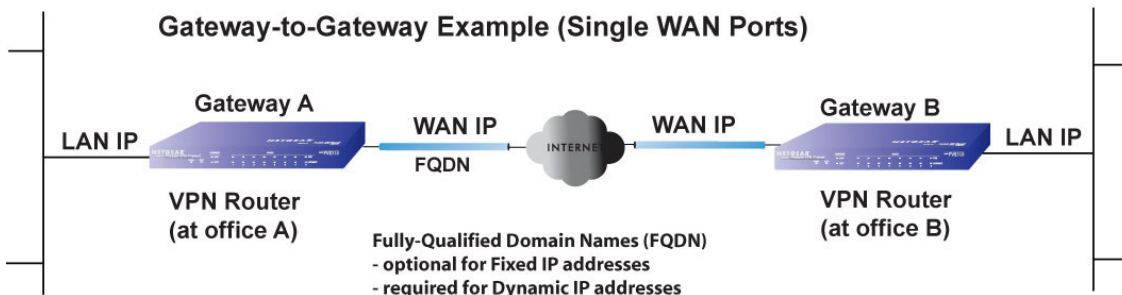


Figure 5-1

Follow these steps to set up a gateway VPN tunnel using the VPN Wizard.

1. Select **VPN > VPN Wizard** to display the VPN Wizard tab page.
To view the wizard default settings, click the VPN Default values link. You can modify these settings after completing the wizard.

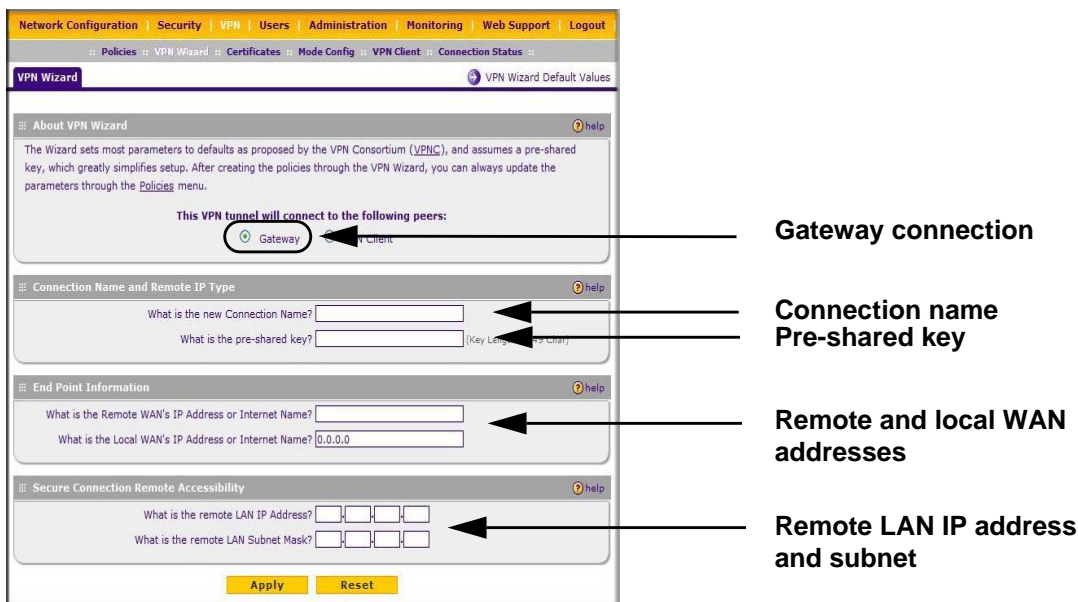


Figure 5-2

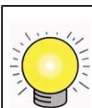
2. Select **Gateway** as your connection type.

3. Create a **Connection Name**. Enter a descriptive name for the connection. This name used to help you manage the VPN settings; is not supplied to the remote VPN endpoint.
4. Enter a **Pre-shared Key**. The key must be entered both here and on the remote VPN gateway, or the remote VPN client. This key must be a minimum of 8 characters and should not exceed 49 characters.
5. Enter the **Remote and Local WAN IP Addresses or Internet Names** of the gateways which will connect.
 - Both the remote WAN address and your local WAN address are required.



Tip: To assure tunnels stay active, after completing the wizard, manually edit the VPN policy to enable keepalive which periodically sends ping packets to the host on the peer side of the network to keep the tunnel alive.

- The remote WAN IP address must be a public address or the Internet name of the remote gateway. The *Internet name* is the Fully Qualified Domain Name (FQDN) as registered in a Dynamic DNS service. Both local and remote endpoints should be defined as either FQDN or IP addresses. A combination of IP address and FQDN is not allowed.



Tip: For DHCP WAN configurations, first, set up the tunnel with IP addresses. Once you validate the connection, use the wizard to create new policies using FQDN for the WAN addresses.

6. Enter the local LAN IP and Subnet Mask of the remote gateway in the **Remote LAN IP Address and Subnet Mask** fields.



Note: The Remote LAN IP address *must* be in a different subnet than the Local LAN IP address. For example, if the local subnet is 192.168.1.x, then the remote subnet could be 192.168.10.x. but *could not* be 192.168.1.x. If this information is incorrect, the tunnel will fail to connect.

- Click **Apply** to save your settings: the VPN Policies page shows the policy is now enabled.



Figure 5-3

- If you are connecting to another NETGEAR VPN firewall, use the VPN Wizard to configure the second VPN firewall to connect to the one you just configured.

After both firewalls are configured, go to **VPN > Connection Status** to display the status of your VPN connections.

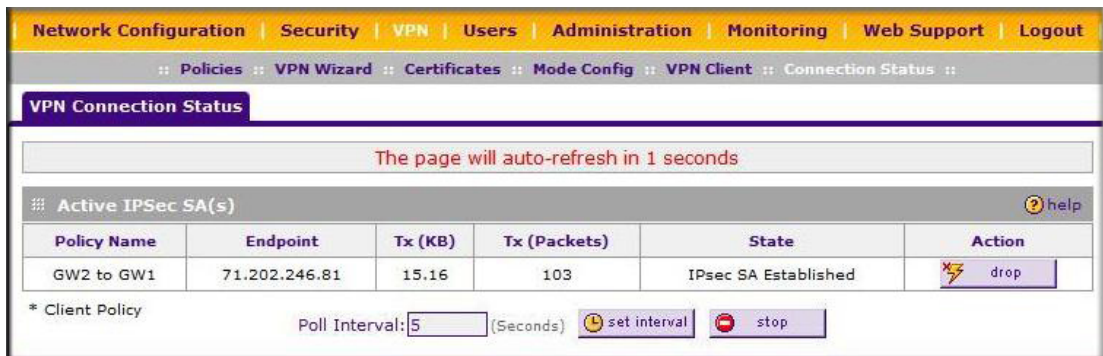


Figure 5-4

The tunnel will automatically establish when both the local and target gateway policies are appropriately configured and enabled,



Note: When using FQDN, if the dynamic DNS service is slow to update their servers when your DHCP WAN address changes, the VPN tunnel will fail because the FQDN does not resolve to your new address. If you have the option to configure the update interval, set it to an appropriately short time.

Creating a Client to Gateway VPN Tunnel

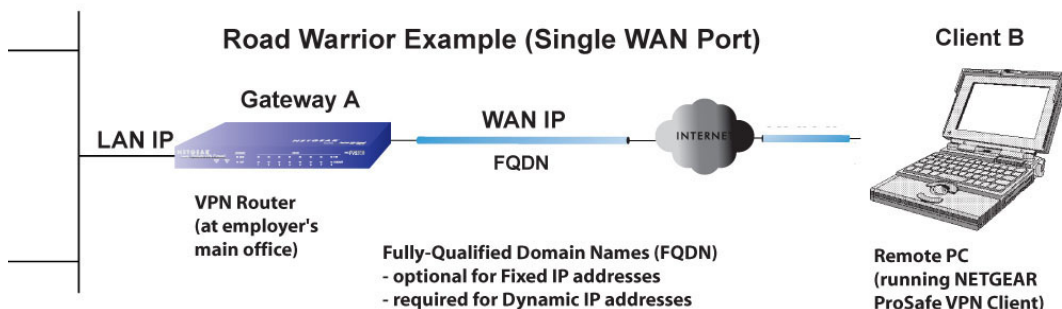


Figure 5-5

Follow these steps to configure the a VPN client tunnel:

- Configure the client policies on the gateway.
- Configure the VPN client to connect to the gateway.

Use the VPN Wizard Configure the Gateway for a Client Tunnel

1. From the main menu, go to **VPN > VPN Wizard**. The VPN Wizard displays.

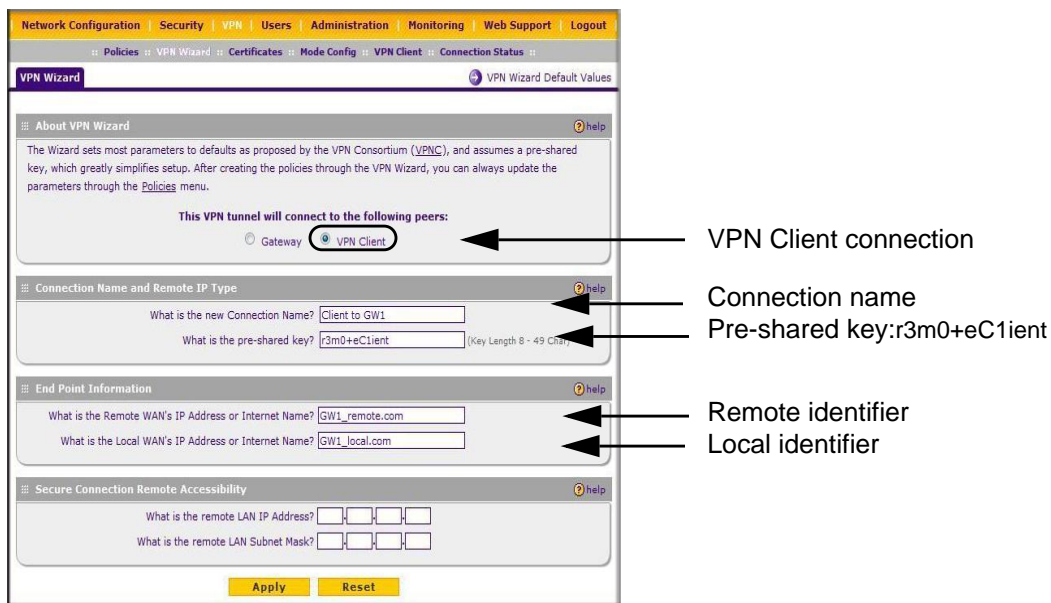
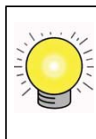


Figure 5-6

2. Select **VPN Client** as your VPN tunnel connection.
3. Create a **Connection Name** like “Client to GW1”.

This descriptive name is not supplied to the remote VPN client; it is only for your reference.

4. Enter a **Pre-shared Key**; in this example, we are using **r3m0+eC1ient**, which must also be entered in the VPN client software. The key length must be 8 characters minimum and cannot exceed 49 characters.
5. The public **Remote and Local Identifier** are automatically filled in by pre-pending the first several letters of the model number of your gateway to form FQDNs used in the VPN policies. In this example, we are using GW1_remote.com, and GW1_local.com.



Tip: To assure tunnels stay active, after completing the wizard, manually edit the VPN policy to enable keepalive which periodically sends ping packets to the host on the peer side of the network to keep the tunnel alive.

- Click **Apply** to save your settings: the VPN Policies page shows the policy is now enabled.

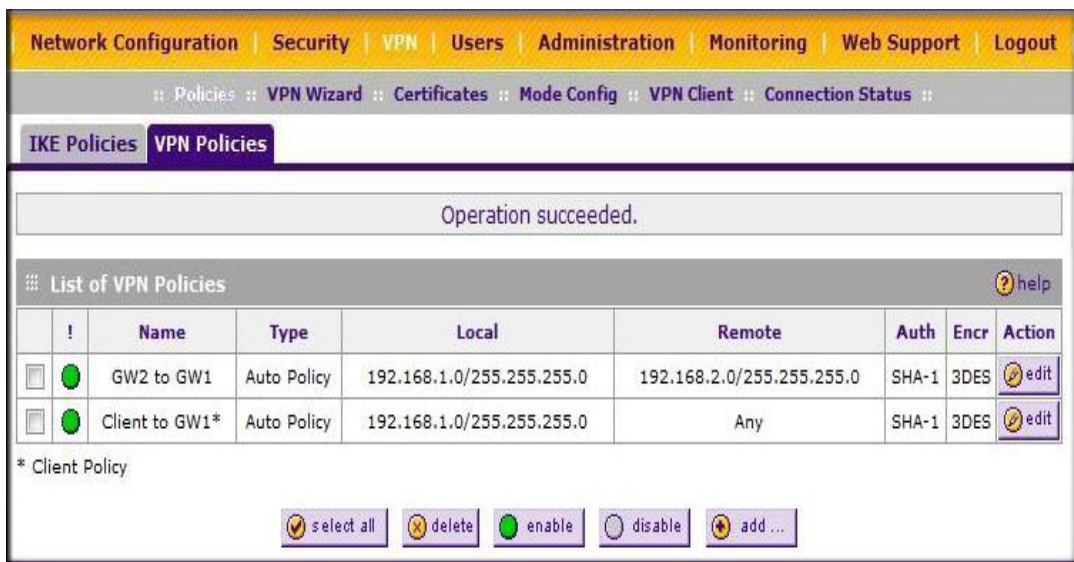


Figure 5-7

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

From a PC with the NETGEAR Prosafe VPN Client installed, configure a VPN client policy to connect to the FVS318G. Follow these steps to configure your VPN client.

- Right-click on the VPN client icon in your Windows toolbar, choose **Security Policy Editor**, and verify that the **Options > Secure > Specified Connections** selection is enabled.

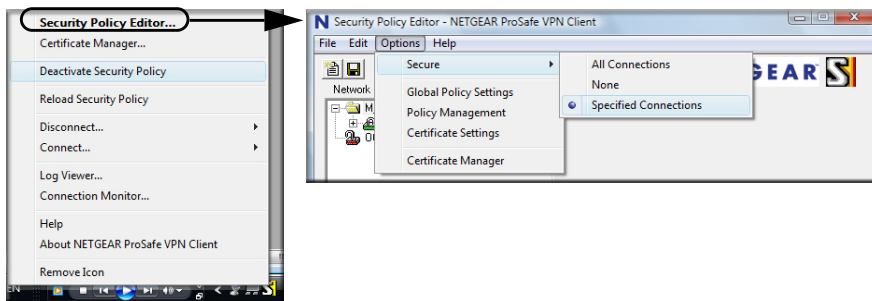


Figure 5-8

2. In the upper left of the Policy Editor window, click the New Document icon (the first on the left) to open a New Connection. Give the New Connection a name; in this example, we are using **gw1**.

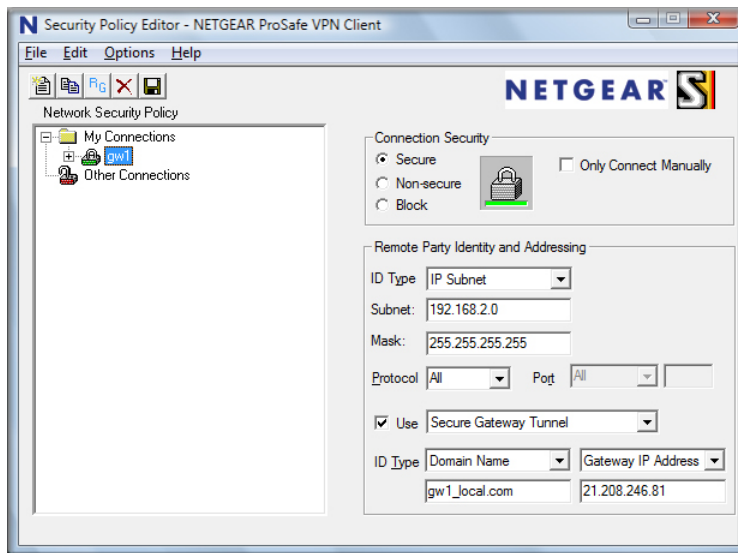


Figure 5-9

Fill in the other options according to the instructions below.

- Under Connection Security, verify that the Secure radio button is selected.
- From the **ID Type** pull-down menu, choose **IP Subnet**.
- Enter the LAN IP **Subnet Address** and **Subnet Mask** of the FVS318G LAN; in this example, we are using 192.168.2.0.
- Check the **Use** checkbox and choose **Secure Gateway Tunnel** from the pull-down menu.
- From the first **ID Type** pull-down menus, choose **Domain Name**. Enter the FQDN address which the FVS318G VPN Wizard provided; in this example, we are using gw1_local.com.
- From the second **ID Type** pull-down menu, choose **Gateway IP Address** and enter the WAN IP Gateway address of the FVS318G; in this example, we are using 21.208.216.81.

3. In the left frame, click **My Identity**. Fill in the options according to the instructions below.

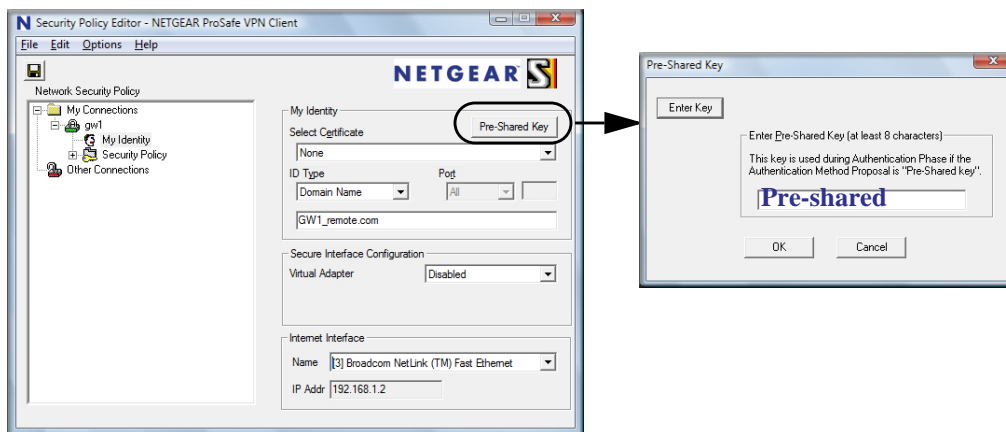


Figure 5-10

- From the **Select Certificate** pull-down menu, choose **None**.
- Click **Pre-Shared Key** to enter the key you provided in the VPN Wizard; in this example, we are using **Pre-shared key:r3m0+eC1ient**.
- From the **ID Type** pull-down menu, choose **Domain Name**.
- Leave **Virtual Adapter** disabled.
- In **Network Adapter** select the adapter you will use; the IP address of the selected adapter will display.

4. Verify the Security Policy settings.

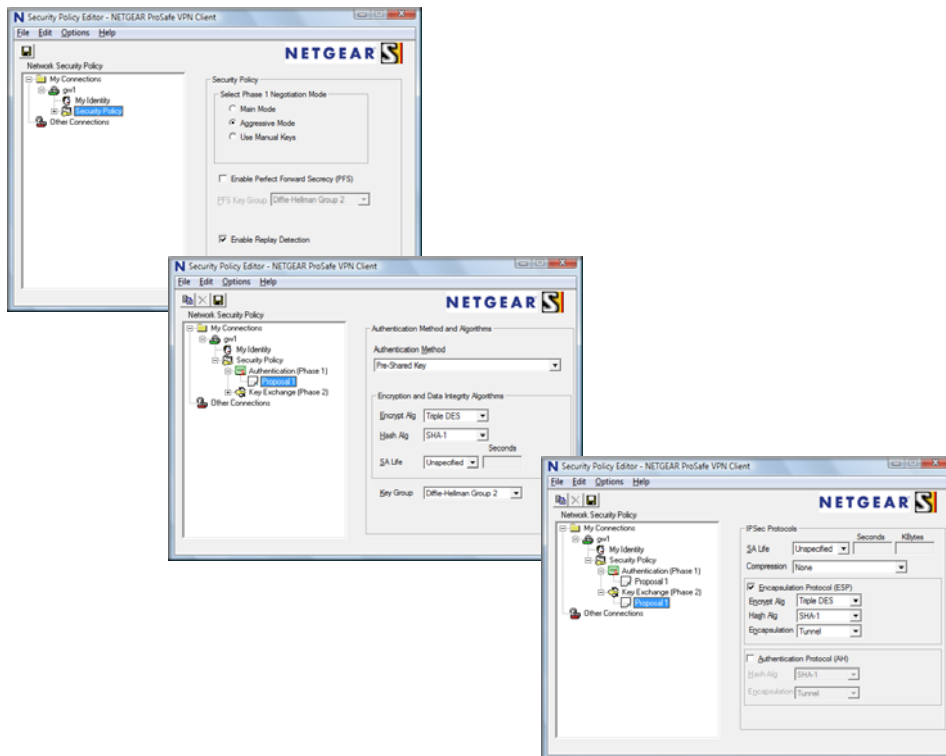


Figure 5-11

- By default TF1 routers use PFS with Group 2, so we need to click on **Security Policy** to make this change on the Client software to match the policy on the router.
 - On the left, expand **Authentication (Phase 1)** and click **Proposal 1**: no changes are needed.
 - On the left, expand **Key Exchange (Phase 2)** and click **Proposal 1**. No changes are needed.
5. In the upper left of the window, click the disk icon to save the policy.

Testing the Connections and Viewing Status Information

Both the NETGEAR VPN Client and the FVS318G provide VPN connection and status information. This information is useful for verifying the status of a connection and troubleshooting problems with a connection.

NETGEAR VPN Client Status and Log Information

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

1. To test the client connection, from your PC, right-click on the VPN client icon in your Windows toolbar and choose **Connect...**, then **My Connections\gw1**.

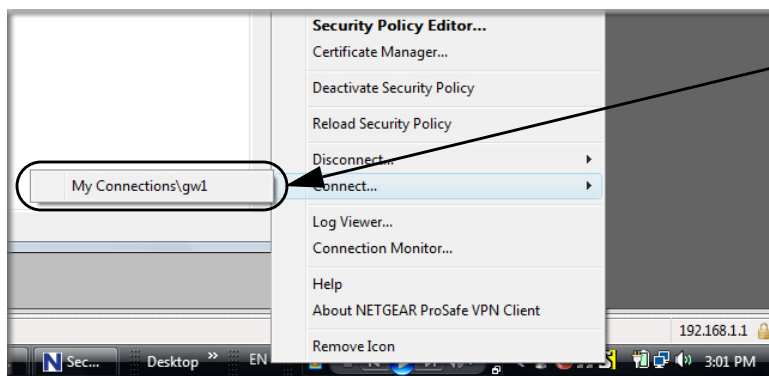


Figure 5-12

Within 30 seconds you should receive the message “Successfully connected to My Connections\gw1”.

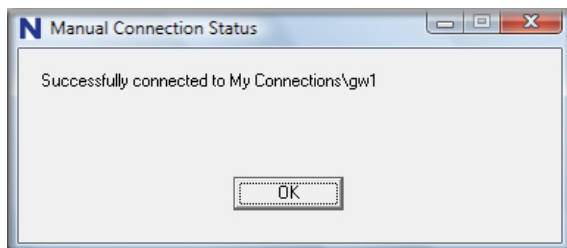


Figure 5-13

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



2. To view more detailed additional status and troubleshooting information from the NETGEAR VPN client, follow these steps.
 - Right-click the VPN Client icon in the system tray and select Log Viewer.

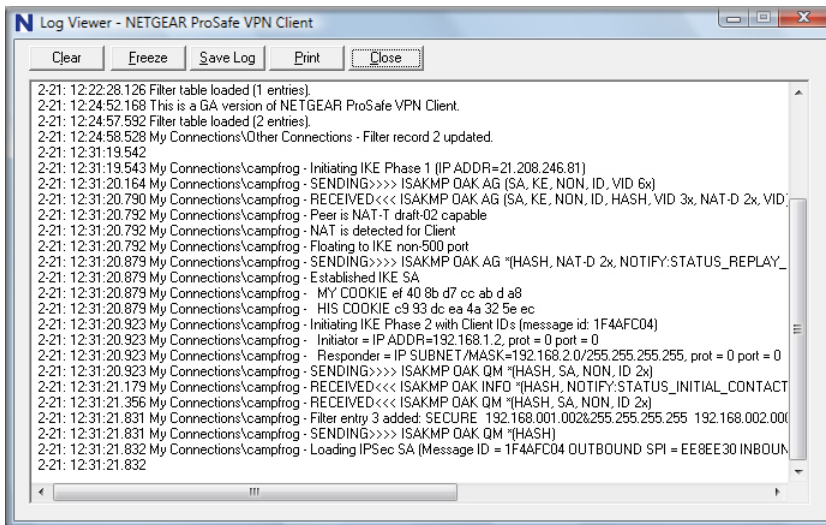


Figure 5-14

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

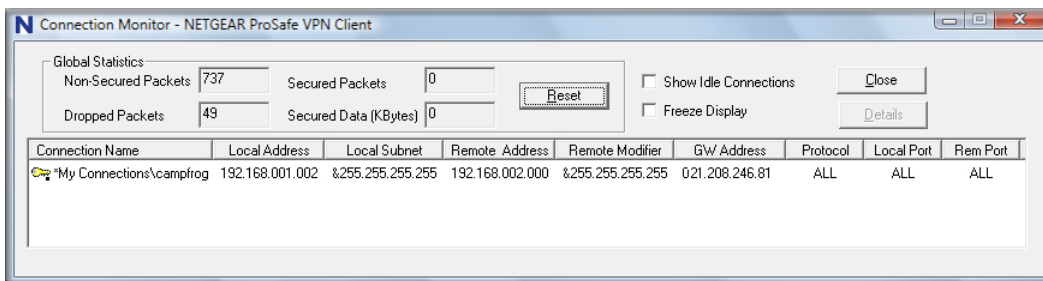





Figure 5-15

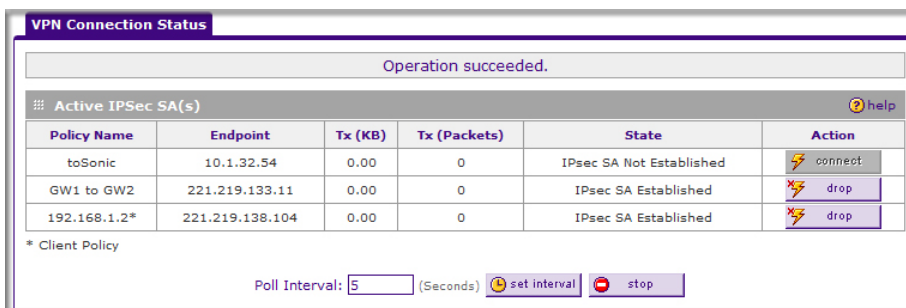
The VPN client system tray icon provides a variety of status indications, which are listed below.

Table 5-1.

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

FVS318G VPN Connection Status and Logs




To view FVS318G VPN connection status, go to **VPN > Connection Status**.



VPN Connection Status

Operation succeeded.

Active IPsec SA(s) help

Policy Name	Endpoint	Tx (KB)	Tx (Packets)	State	Action
toSonic	10.1.32.54	0.00	0	IPsec SA Not Established	
GW1 to GW2	221.219.133.11	0.00	0	IPsec SA Established	
192.168.1.2*	221.219.138.104	0.00	0	IPsec SA Established	

* Client Policy

Poll Interval: (Seconds) set interval stop

Figure 5-16

To view FVS318G VPN logs, go to **Monitoring > VPNLogs**.

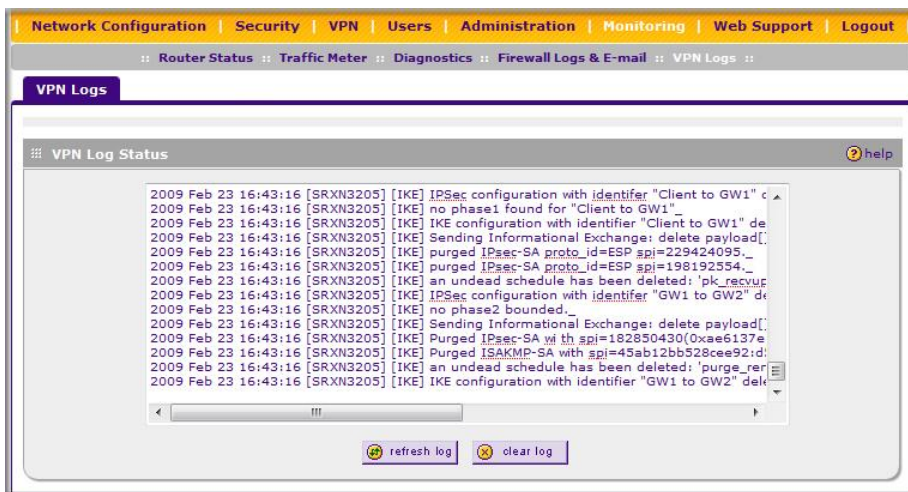


Figure 5-17

Managing VPN Policies

After you use the VPN Wizard to set up a VPN tunnel, a VPN policy and an IKE policy are stored in separate policy tables. The name you selected as the VPN tunnel connection name during Wizard setup identifies both the VPN policy and IKE policy. You can edit existing policies, or add new VPN and IKE policies directly in the policy tables.

Managing IKE Policies

The IKE (Internet Key Exchange) protocol performs negotiations between the two VPN gateways, and provides automatic management of the keys used in IPsec. It is important to remember that:

- “Auto” generated VPN policies must use the IKE negotiation protocol.
- “Manual” generated VPN policies cannot use the IKE negotiation protocol.

IKE Policies are activated when the following occur:

1. The VPN policy selector determines that some traffic matches an existing VPN policy. If the VPN policy is of type “Auto”, then the **Auto Policy Parameters** defined in the VPN policy are accessed which specify which IKE Policy to use.

2. If the VPN Policy is a “Manual” policy, then the **Manual Policy Parameters** defined in the VPN policy are accessed and the first matching IKE policy is used to start negotiations with the remote VPN gateway.
 - If negotiations fail, the next matching IKE policy is used.
 - If none of the matching IKE policies are acceptable to the remote VPN gateway, then a VPN tunnel cannot be established.
3. An IKE session is established, using the SA (Security Association) parameters specified in a matching IKE Policy:
 - Keys and other parameters are exchanged.
 - An IPsec SA (Security Association) is established, using the parameters in the VPN policy.

The VPN tunnel is then available for data transfer.

The IKE Policies Tab Page

When you use the VPN Wizard to set up a VPN tunnel, an IKE policy is established and populated in the List of IKE Policies and is given the same name as the new VPN connection name. You can also edit exiting policies or add new IKE policies directly on the List of IKE Policies. Each policy contains the following data:

- **Name.** Uniquely identifies each IKE policy. The name is chosen by you and used for managing your policies; it is not supplied to the remote VPN endpoint.
- **Mode.** Two modes are available: either Main or Aggressive.
 - Main Mode is slower but more secure.
 - Aggressive mode is faster but less secure. (If specifying either a FQDN or a User FQDN name as the Local ID/Remote ID, aggressive mode is automatically selected.)
- **Local ID.** The IKE/ISAKMP identify of this device. (The remote VPN must have this value as their Remote ID.)
- **Remote ID.** The IKE/ISAKMP identify of the remote VPN gateway. (The remote VPN must have this value as its Local ID.)
- **Encr.** Encryption algorithm used for the IKE SA. The default setting using the VPN Wizard is 3DES. (This setting must match the Remote VPN.)
- **Auth.** Authentication Algorithm used for the IKE SA. The default setting using the VPN Wizard is SHA1. (This setting must match the Remote VPN.)

- **DH.** The Diffie-Hellman (DH) group used when exchanging keys. The DH group sets the number of bits. The VPN Wizard default setting is Group 2. (This setting must match the remote VPN.)

To gain a more complete understanding of the encryption, authentication and DH algorithm technologies, see [Appendix B, “Related Documents”](#) for a link to the NETGEAR website.

Managing VPN Policies

You can create two types of VPN policies. When using the VPN Wizard to create a VPN policy, only the Auto method is available.

- **Manual.** All settings (including the keys) for the VPN tunnel are manually input at each end (both VPN Endpoints). No third party server or organization is involved.
- **Auto.** Some parameters for the VPN tunnel are generated automatically by using the IKE (Internet Key Exchange) protocol to perform negotiations between the two VPN Endpoints (the Local ID Endpoint and the Remote ID Endpoint).

In addition, a Certificate Authority (CA) can also be used to perform authentication (see [“Managing Certificates” on page 6-7](#)). To use a CA, each VPN gateway must have a certificate from the CA. For each certificate, there is both a public key and a private key. The public key is freely distributed, and is used by any sender to encrypt data intended for the receiver (the key owner). The receiver then uses its private key to decrypt the data (without the private key, decryption is impossible). The use of certificates for authentication reduces the amount of data entry required on each VPN endpoint.

The VPN Policies Tab Page

The VPN Policies screen allows you to add additional policies—either Auto or Manual—and to manage the VPN policies already created. You can edit policies, enable or disable policies, or delete them entirely. The rules for VPN policy use are:

1. Traffic covered by a policy will automatically be sent via a VPN tunnel.
2. When traffic is covered by two or more policies, the first matching policy will be used. (In this situation, the order of the policies is important. However, if you have only one policy for each remote VPN Endpoint, then the policy order is not important.)
3. The VPN tunnel is created according to the parameters in the SA (Security Association).
4. The remote VPN Endpoint must have a matching SA, or it will refuse the connection.

Only one Client Policy may be configured at a time (noted by an “*” next to the policy name). The Policy Table contains the following fields:

- **! (Status).** Indicates whether the policy is enabled (green circle) or disabled (grey circle). To Enable or Disable a Policy, check the box adjacent to the circle and click **Enable** or **Disable**, as required.
- **Name.** Each policy is given a unique name (the Connection Name when using the VPN Wizard).
- **Type.** The Type is “Auto” or “Manual” as described previously (Auto is used during VPN Wizard configuration).
- **Local.** IP address (either a single address, range of address or subnet address) on your local LAN. Traffic must be from (or to) these addresses to be covered by this policy. (The Subnet address is supplied as the default IP address when using the VPN Wizard).
- **Remote.** IP address or address range of the remote network. Traffic must be to (or from) these addresses to be covered by this policy. (The VPN Wizard default requires the remote LAN IP address and subnet mask).
- **Auth.** Authentication Algorithm used for the VPN tunnel. The default setting using the VPN Wizard is SHA1. (This setting must match the Remote VPN.)
- **Encr.** Encryption algorithm used for the VPN tunnel. The default setting using the VPN Wizard is 3DES. (This setting must match the Remote VPN.)
- **Action.** Allows you to access individual policies to make any changes or modifications.

Configuring Extended Authentication (XAUTH)

When connecting many VPN clients to a VPN firewall, an administrator may want a unique user authentication method beyond relying on a single common preshared key for all clients. Although the administrator could configure a unique VPN policy for each user, it is more convenient for the VPN firewall to authenticate users from a stored list of user accounts. XAUTH provides the mechanism for requesting individual authentication information from the user, and a local User Database or an external authentication server, such as a RADIUS server, provides a method for storing the authentication information centrally in the local network.

XAUTH can be enabled when adding or editing an IKE Policy. Two types of XAUTH are available:

- **Edge Device.** If this is selected, the VPN firewall is used as a VPN concentrator where one or more gateway tunnels terminate. If this option is chosen, you must specify the authentication type to be used in verifying credentials of the remote VPN gateways: User Database, RADIUS-PAP, or RADIUS-CHAP.

- **IPsec Host.** If you want authentication by the remote gateway, enter a User Name and Password to be associated with this IKE policy. If this option is chosen, the remote gateway must specify the user name and password used for authenticating this gateway.



Note: If a RADIUS-PAP server is enabled for authentication, XAUTH will first check the local User Database for the user credentials. If the user account is not present, the VPN firewall will then connect to a RADIUS server.

Configuring XAUTH for VPN Clients

Once the XAUTH has been enabled, you must establish user accounts on the User Database to be authenticated against XAUTH, or you must enable a RADIUS-CHAP or RADIUS-PAP server.



Note: You cannot modify an existing IKE policy to add **XAUTH** while the IKE policy is in use by a VPN policy. The VPN policy must be disabled before you can modify the IKE policy.

To enable and configure XAUTH:

1. Select VPN > IPsec VPN from the main menu.
2. Click the **IKE Policies** tab. The IKE Policies screen is displayed.

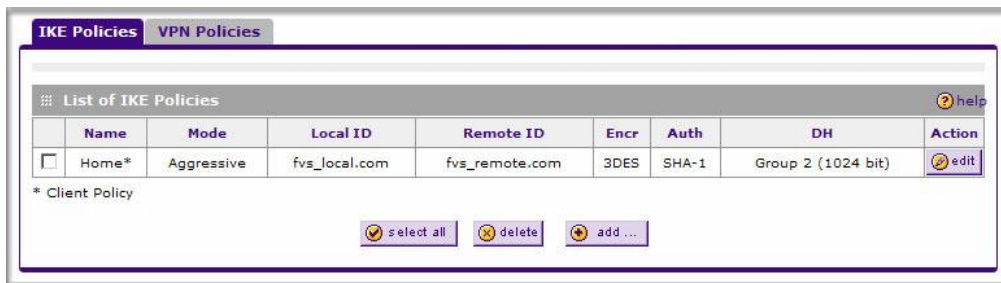


Figure 5-18

3. You can add **XAUTH** to an existing IKE Policy by clicking **Edit** adjacent to the policy to be modified or you can create a new IKE Policy incorporating **XAUTH** by clicking **Add**.
4. In the **Extended Authentication** section, choose the **Authentication Type** from the pull-down menu which will be used to verify user account information. Select

- **Edge Device** to use this VPN firewall as a VPN concentrator where one or more gateway tunnels terminate. When this option is chosen, you will need to specify the authentication type to be used in verifying credentials of the remote VPN gateways.
 - **User Database** to verify against the VPN firewall’s user database. Users must be added through the User Database screen (see [“User Database Configuration” on page 5-19](#)).
 - **RADIUS–CHAP** or **RADIUS–PAP** (depending on the authentication mode accepted by the RADIUS server) to add a RADIUS server. If RADIUS–PAP is selected, the VPN firewall will first check in the user database to see if the user credentials are available. If the user account is not present, the VPN firewall will then connect to the RADIUS server (see [“RADIUS Client Configuration” on page 5-19](#)).
- **IPsec Host** if you want to be authenticated by the remote gateway. In the adjacent **Username** and **Password** fields, type in the information user name and password associated with the IKE policy for authenticating this gateway (by the remote gateway).

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

User Database Configuration

When XAUTH is enabled as an Edge Device, users must be authenticated either by a local User Database account or by an external RADIUS server. Whether or not you use a RADIUS server, you may want some users to be authenticated locally. These users must be added to the List of Users table, as described in [“Changing the Administrator Login” on page 6-2](#).

RADIUS Client Configuration

RADIUS (Remote Authentication Dial In User Service, RFC 2865) is a protocol for managing Authentication, Authorization and Accounting (AAA) of multiple users in a network. A RADIUS server will store 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 username/password or some encrypted response using his username/password information. The gateway will try to verify this information first against a local User Database (if RADIUS-PAP is enabled) and then by relaying the information to a central authentication server such as a RADIUS server.

To configure the Primary RADIUS Server:

1. Select **VPN > VPN Client** from the main menu.

- Click the **RADIUS Client** tab. The RADIUS Client screen is displayed.

The screenshot shows the 'RADIUS Client' configuration page. It features three main sections:

- Primary RADIUS Server:** Includes a question 'Do you want to enable a Primary RADIUS Server?' with 'Yes' and 'No' radio buttons. To the right are input fields for 'Primary Server IP Address', 'Secret Phrase', and 'Primary Server NAS Identifier' (pre-filled with 'FVS336G').
- Backup RADIUS Server:** Includes a question 'Do you want to enable a Backup RADIUS Server?' with 'Yes' and 'No' radio buttons. To the right are input fields for 'Backup Server IP Address', 'Secret Phrase', and 'Backup Server NAS Identifier' (pre-filled with 'FVS336G').
- Connection Configuration:** Includes input fields for 'Time out period: 30 (Sec)' and 'Maximum Retry Count: 4'.

At the bottom of the form are two yellow buttons: 'Apply' and 'Reset'.

Figure 5-19

- To activate (enable) the Primary RADIUS server, click the **Yes** radio button. The primary server options become active.
- Configure the following entries:
 - Primary RADIUS Server IP address.** The IP address of the RADIUS server.
 - Secret Phrase.** Transactions between the client and the RADIUS server are authenticated using a shared secret phrase, so the same Secret Phrase must be configured on both client and server.
 - Primary Server NAS Identifier** (Network Access Server). This Identifier **MUST** be present in a RADIUS request. Ensure that NAS Identifier is configured identically on both client and server.

The FVS318G is acting as a NAS (Network Access Server), allowing network access to external users after verifying 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 FVS318G's IP address may be sufficient as an identifier, or the server may require a name, which you would enter here. This name would also be configured on the RADIUS server, although in some cases it should be left blank on the RADIUS server.

5. Enable a Backup RADIUS Server (if required).
6. Set the **Time Out Period**, in seconds, that the VPN firewall should wait for a response from the RADIUS server.
7. Set the **Maximum Retry Count**. This is the number of tries the VPN firewall will make to the RADIUS server before giving up.
8. Click **Apply** to save the settings.



Note: Selection of the Authentication Protocol, usually PAP or CHAP, is configured on the individual IKE policy screens.

Assigning IP Addresses to Remote Users (ModeConfig)

To simplify the process of connecting remote VPN clients to the FVS318G, the ModeConfig module can be used to assign IP addresses to remote users, including a network access IP address, subnet mask, and name server addresses from the VPN firewall. Remote users are given IP addresses available in secured network space so that remote users appear as seamless extensions of the network.

In the following example, we configured the VPN firewall using ModeConfig, and then configured a PC running ProSafe VPN Client software using these IP addresses.

- NETGEAR FVS318G ProSafe VPN Firewall
 - WAN IP address: 172.21.4.1
 - LAN IP address/subnet: 192.168.2.1/255.255.255.0
- NETGEAR ProSafe VPN Client software IP address: 192.168.1.2

Mode Config Operation

After IKE Phase 1 is complete, the VPN connection initiator (remote user/client) asks for IP configuration parameters such as IP address, subnet mask and name server addresses. The Mode Config module will allocate an IP address from the configured IP address pool and will activate a temporary IPsec policy using the template security proposal information configured in the Mode Config record.



Note: After configuring a Mode Config record, you must go to the IKE Policies menu and configure an IKE policy using the newly-created Mode Config record as the Remote Host Configuration Record. The VPN Policies menu does not need to be edited.

Configuring the VPN Firewall Router

Two menus must be configured—the Mode Config menu and the IKE Policies menu.

To configure the Mode Config menu:

1. Click **VPN** in the main menu.
2. Click **Mode Config** in the submenu. The Mode Config tab is displayed.



Figure 5-20

3. Click **Add**. The **Add Mode Config Record** screen is displayed

Figure 5-21

4. Enter a descriptive **Record Name** such as “Sales”.
5. Assign at least one range of IP Pool addresses in the First IP Pool field to give to remote VPN clients.



Note: The IP Pool should not be within your local network IP addresses. Use a different range of private IP addresses such as 172.20.xx.xx.

6. If you have a WINS Server on your local network, enter its IP address.
7. Enter one or two DNS Server IP addresses to be used by remote VPN clients.
8. If you enable Perfect Forward Secrecy (PFS), choose DH Group 1 or 2. This setting must match exactly the configuration of the remote VPN client,
9. Specify the Local IP Subnet to which the remote client will have access. Typically, this is your VPN firewall’s LAN subnet, such as 192.168.2.1/255.255.255.0. (If not specified, it will default to the LAN subnet of the VPN firewall.)

10. Specify the VPN policy settings. These settings must match the configuration of the remote VPN client. Recommended settings are:

- SA Lifetime: 3600 seconds
- Authentication Algorithm: SHA-1
- Encryption Algorithm: 3DES

11. Click **Apply**.

The new record should appear in the VPN Remote Host Mode Config Table.

Next, you must configure an IKE Policy:

1. Click VPN > IPsec VPN in the main menu. The **IKE Policies** screen is displayed showing the current policies in the **List of IKE Policies** Table.
2. Click **Add** to configure a new IKE Policy. The **Add IKE Policy** screen is displayed.
3. Enable **Mode Config** by checking the **Yes** radio button and selecting the Mode Config record you just created from the pull-down menu. (You can view the parameters of the selected record by clicking the **View selected** radio button.)

Mode Config works only in Aggressive Mode, and Aggressive Mode requires that both ends of the tunnel be defined by an FQDN.

4. In the **General** section:
 - a. Enter a descriptive name in the Policy Name Field such as “salesperson”. This name will be used as part of the remote identifier in the VPN client configuration.
 - b. Set Direction/Type to Responder.
 - c. The Exchange Mode will automatically be set to Aggressive.
5. For Local information:
 - a. Select Fully Qualified Domain Name for the Local Identity Type.
 - b. Enter an identifier in the Remote Identity Data field that is not used by any other IKE policies. This identifier will be used as part of the local identifier in the VPN client configuration.
6. Specify the IKE SA parameters. These settings must be matched in the configuration of the remote VPN client. Recommended settings are:
 - Encryption Algorithm: 3DES
 - Authentication Algorithm: SHA-1
 - Diffie-Hellman: Group 2
 - SA Lifetime: 3600 seconds

7. Enter a Pre-Shared Key that will also be configured in the VPN client.
8. XAUTH is disabled by default. To enable XAUTH, choose one of the following:
 - **Edge Device** to use this VPN firewall as a VPN concentrator where one or more gateway tunnels terminate. (If selected, you must specify the **Authentication Type** to be used in verifying credentials of the remote VPN gateways.)
 - **IPsec Host** if you want this gateway to be authenticated by the remote gateway. Enter a Username and Password to be associated with the IKE policy. When this option is chosen, you will need to specify the user name and password to be used in authenticating this gateway (by the remote gateway).

For more information on XAUTH, see [“Configuring XAUTH for VPN Clients”](#) on page 5-18.

9. If Edge Device was enabled, choose the **Authentication Type** from the pull down menu which will be used to verify account information: User Database, RADIUS-CHAP or RADIUS-PAP. Users must be added through the User Database screen (see [“Changing the Administrator Login”](#) on page 6-2 or [“RADIUS Client Configuration”](#) on page 5-19).



Note: If RADIUS-PAP is selected, the VPN firewall will first check the User Database to see if the user credentials are available. If the user account is not present, the VPN firewall will then connect to the RADIUS server.

10. Click **Apply**. The new policy will appear in the IKE Policies Table.


Configuring the ProSafe VPN Client for ModeConfig

From a client PC running NETGEAR ProSafe VPN Client software, configure the remote VPN client connection.

To configure the client PC:

1. Right-click the VPN client icon in the Windows toolbar. In the upper left of the Policy Editor window, click the New Policy editor icon.
 - a. Give the connection a descriptive name such as “modecfg_test”. (This name will only be used internally).
 - b. From the ID Type pull-down menu, choose IP Subnet.
 - c. Enter the IP Subnet and Mask of the VPN firewall (this is the LAN network IP address of the gateway).
 - d. Check the Connect using radio button and choose Secure Gateway Tunnel from the pull-down menu.

- e. From the ID Type pull-down menu, choose Domain name and enter the FQDN of the VPN firewall; in this example it is “local_id.com”.
 - f. Choose Gateway IP Address from the second pull-down menu and enter the WAN IP address of the VPN firewall; in this example it is “172.21.4.1”.
2. From the left side of the menu, click My Identity and enter the following information:
- a. Click **Pre-Shared Key** and enter the key you configured in the FVS318G IKE menu.
 - b. From the Select Certificate pull-down menu, choose None.
 - c. From the ID Type pull-down menu, choose Domain Name and create an identifier based on the name of the IKE policy you created; for example “salesperson11.remote_id.com”.
 - d. Under Virtual Adapter pull-down menu, choose Preferred. The Internal Network IP Address should be 0.0.0.0.

	Note: If no box is displayed for Internal Network IP Address, go to Options/Global Policy Settings, and check the box for “Allow to Specify Internal Network Address.”
---	---

- e. Select your Internet Interface adapter from the Name pull-down menu.
3. On the left-side of the menu, choose Security Policy.
- a. Under Security Policy, Phase 1 Negotiation Mode, check the Aggressive Mode radio button.
 - b. Check the Enable Perfect Forward Secrecy (PFS) box, and choose the Diffie-Hellman Group 2 from the PFS Key Group pull-down menu.
 - c. Enable Replay Detection should be checked.
4. Click on Authentication (Phase 1) on the left-side of the menu and choose Proposal 1. Enter the Authentication values to match those in the VPN firewall ModeConfig Record menu.
5. Click on Key Exchange (Phase 2) on the left-side of the menu and choose Proposal 1. Enter the values to match your configuration of the VPN firewall ModeConfig Record menu. (The SA Lifetime can be longer, such as 8 hours [28800 seconds]).
6. Click the Save icon to save the Security Policy and close the VPN ProSafe VPN client.

To test the connection:

1. Right-click on the VPN client icon in the Windows toolbar and click Connect. The connection policy you configured will appear; in this case “My Connections\modecfg_test”.

2. Click on the connection. Within 30 seconds the message “Successfully connected to MyConnections/modectfg_test is displayed and the VPN client icon in the toolbar will read “On”.
3. From the client PC, ping a computer on the VPN firewall LAN.

Configuring Keepalives and Dead Peer Detection

In some cases, it may not be desirable to have a VPN tunnel drop when traffic is idle; for example, when client-server applications over the tunnel cannot tolerate the tunnel establishment time. If you require your VPN tunnel to remain connected, you can use the Keepalive and Dead Peer Detection features to prevent the tunnel from dropping and to force a reconnection if the tunnel drops for any reason.

For Dead Peer Detection to function, the peer VPN device on the other end of the tunnel must also support Dead Peer Detection. Keepalive, though less reliable than Dead Peer Detection, does not require any support from the peer device.

Configuring Keepalive

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

1. Select **VPN > Policies** from the main menu.
2. Click the **VPN Policies** tab, then click the **edit** button next to the desired VPN policy.

3. In the **General** menu frame of the **Edit VPN Policy** menu, locate the keepalive configuration settings, as shown in [Figure 5-22](#):

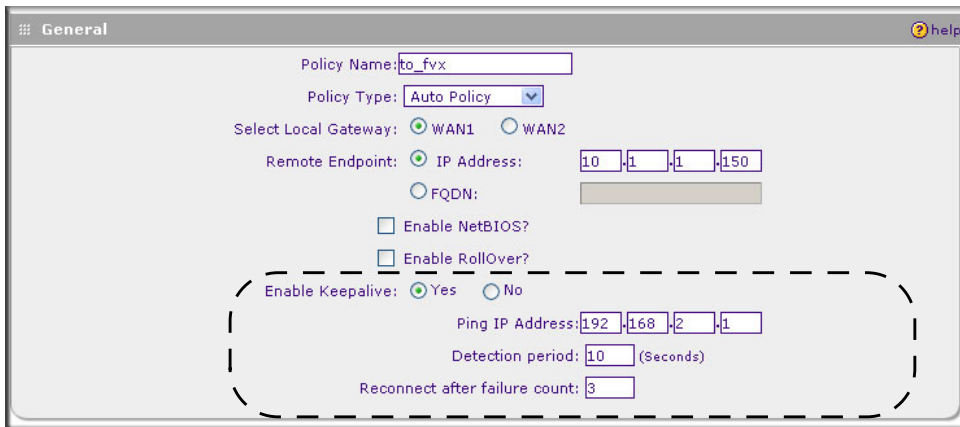


Figure 5-22

4. Click the **Yes** radio button to enable keepalive.
5. In the **Ping IP Address** boxes, enter an IP address on the remote LAN. This must be the address of a host that can respond to ICMP ping requests.
6. Enter the **Detection Period** to set the time between ICMP ping requests. The default is 10 seconds.
7. In **Reconnect after failure count**, set the number of consecutive missed responses that will be considered a tunnel connection failure. The default is 3 missed responses. When the FVS318G senses a tunnel connection failure, it forces a reestablishment of the tunnel.
8. Click **Apply** at the bottom of the menu.

The Dead Peer Detection feature maintains the IKE SA by exchanging periodic messages with the remote VPN peer. To configure Dead Peer Detection on a configured IKE policy, follow these steps:

1. Select **VPN** from the main menu and **Policies** from the submenu.
2. Click the **IKE Policies** tab, then click the **edit** button next to the desired VPN policy.

- In the **IKE SA Parameters** menu frame of the **Edit IKE Policy** menu, locate the Dead Peer Detection configuration settings, as shown in [Figure 5-23](#).

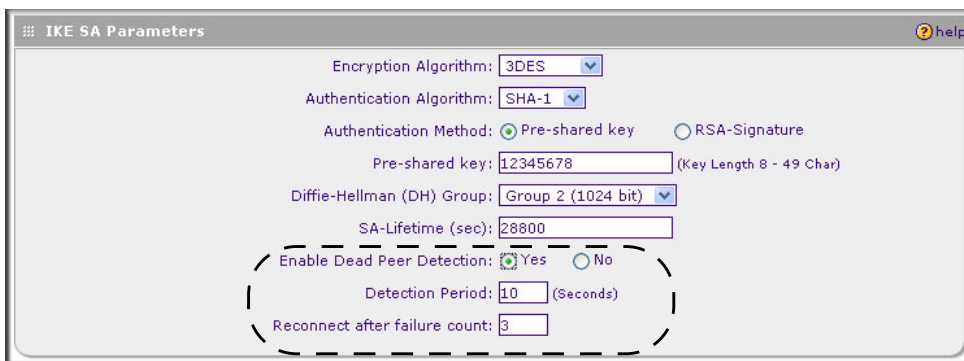


Figure 5-23

- Click the **Yes** radio button to **Enable Dead Peer Detection**.
- Enter the **Detection Period** to set the interval between consecutive DPD R-U-THERE messages. DPD R-U-THERE messages are sent only when the IPsec traffic is idle. The default is 10 seconds.
- In **Reconnect after failure count**, set the number of DPD failures allowed before tearing down the connection. The default is 3 failures. When the FVS318G senses an IKE connection failure, it deletes the IPsec and IKE Security Association and forces a reestablishment of the connection.
- Click **Apply** at the bottom of the menu.

Configuring NetBIOS Bridging with VPN

Windows networks use the Network Basic Input/Output System (NetBIOS) for several basic network services such as naming and neighborhood device discovery. Because VPN routers do not normally pass NetBIOS traffic, these network services do not work for hosts on opposite ends of a VPN connection. To solve this problem, you can configure the FVS318G to bridge NetBIOS traffic over the VPN tunnel. To enable NetBIOS bridging on a configured VPN tunnel, follow these steps:

- Select **VPN > Policies** from the main menu.
- Click the **VPN Policies** tab, then click the **edit** button next to the desired VPN policy.

3. In the **General** menu frame of the **Edit VPN Policy** menu, click the **Enable NetBIOS** check box, as shown in [Figure 5-24](#).

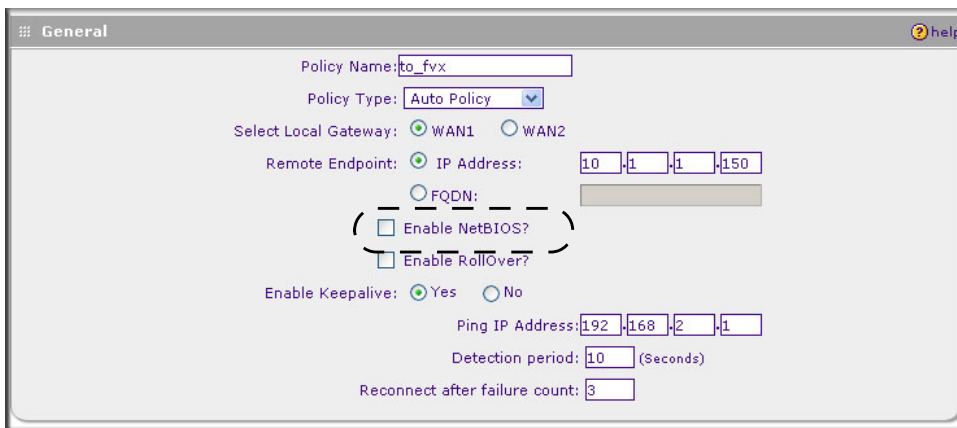


Figure 5-24

4. Click **Apply** at the bottom of the menu.

Chapter 6

Managing Users, Authentication, and Certificates

This chapter contains the following sections:

- “Managing Users” on page 6-1
- “Managing Certificates” on page 6-7

Managing Users

The VPN Firewall has one administrator account and one guest account. The administrator can login and reconfigure the VPN firewall. The guest can login and display information but cannot change settings. The default name and password for the administrator is admin and password. The default name and password for the guest is guest and password. VPN firewall. IPsec VPN clients are only needed 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 window presented to the user requires a User Name and a Password.



Note: IPsec VPN users will always belong to the default domain (geardomain).

Changing the Administrator Login

To change the administrator name or password:

1. Select **Users**. The Users screen will display.
2. Select **Edit Admin Settings** in the User Selection window.



The screenshot shows a web interface titled "User Selection" with a "help" icon. Below the title bar are two radio buttons: "Edit Admin Settings" (selected) and "Edit Guest Settings". The main area is divided into two panels: "Admin Settings" and "Guest Settings", each with its own "help" icon. The "Admin Settings" panel contains four input fields: "New User Name" (containing "admin"), "Old Password", "New Password", and "Retype New Password". The "Guest Settings" panel contains four input fields: "New User Name" (containing "guest"), "Old Password", "New Password", and "Retype New Password". At the bottom of the interface are two yellow buttons: "Apply" and "Reset".

Figure 6-1

3. If you are changing the administrator name, enter the new name and the old administrator password (default is **password**).
4. If you want to change the password, enter and reenter the new password.
5. Click **Apply**.

Changing the Guest Login

To change the guest login name or password::

1. Select **Users**. The Users screen will display.
2. Select **Edit Guest Settings** in the User Selection window.



The screenshot shows a web configuration interface titled "User Selection". At the top, there are two radio buttons: "Edit Admin Settings" (selected) and "Edit Guest Settings". Below this, there are two side-by-side panels. The left panel is titled "Admin Settings" and contains four input fields: "New User Name:", "Old Password:", "New Password:", and "Retype New Password:". The right panel is titled "Guest Settings" and contains four input fields: "New User Name:", "Old Password:", "New Password:", and "Retype New Password:". At the bottom of the interface are two yellow buttons: "Apply" and "Reset".

Figure 6-2

3. If you are changing the guest name, enter the new name and the old password (default is **password**).
4. If you want to change the password, enter and reenter the new password.
5. Click **Apply**.
 - a. **Password/Confirm Password.** The password can contain alphanumeric characters, dash, and underscore.
 - b. **Idle Timeout.** For an Administrator, this is the period at which an idle user will be automatically logged out of the Web Configuration Manager.

Setting administrator timeout and domain display name

You can set the timeout for the administrator. After a period of no activity in the user interface, the administrator will automatically be logged out. You can also enter a domain name to be displayed in the login window.

To configure the administrator timeout:

1. Select **Users**. The Users screen displays.
2. Enter a new timeout value in the Local Authentication Settings window.



Figure 6-3

3. If you want, enter a domain name to be displayed at login.
4. Click **Apply** to save your settings.

Changing Passwords and Settings


You can change the administrator and guest passwords and settings. Administrator access is read/write and guest access is read-only. The default passwords for the firewall's Web Configuration Manager is **password**.

To modify User or Admin settings:


1. Select **Users** from the main menu and **Local Authentication** from the submenu.

Figure 6-4

2. Select the Settings you wish to edit by checking either the **Edit Admin Settings** or **Edit Guest Settings** radio box.
3. Change the password by first entering the old password, and then entering the new password twice.
4. Click **Apply** to save your settings or **Cancel** to return to your previous settings.
5. Change the **Idle Logout Time** field to the number of minutes you require. The default is 5 minutes.

	<p>Note: If you make the administrator login time-out value too large, you will have to wait a long time before you are able to log back into the router if your previous login was disrupted (i.e., you did not click Logout on the Main Menu bar to log out).</p>
---	---

6. Click **Apply** to save this setting.

 **Note:** The password and time-out value you enter will be changed back to **password** and **5** minutes, respectively, after a factory defaults reset.

RADIUS Server External Authentication

For authentication to RADIUS or WIKID, you can define the authentication type.

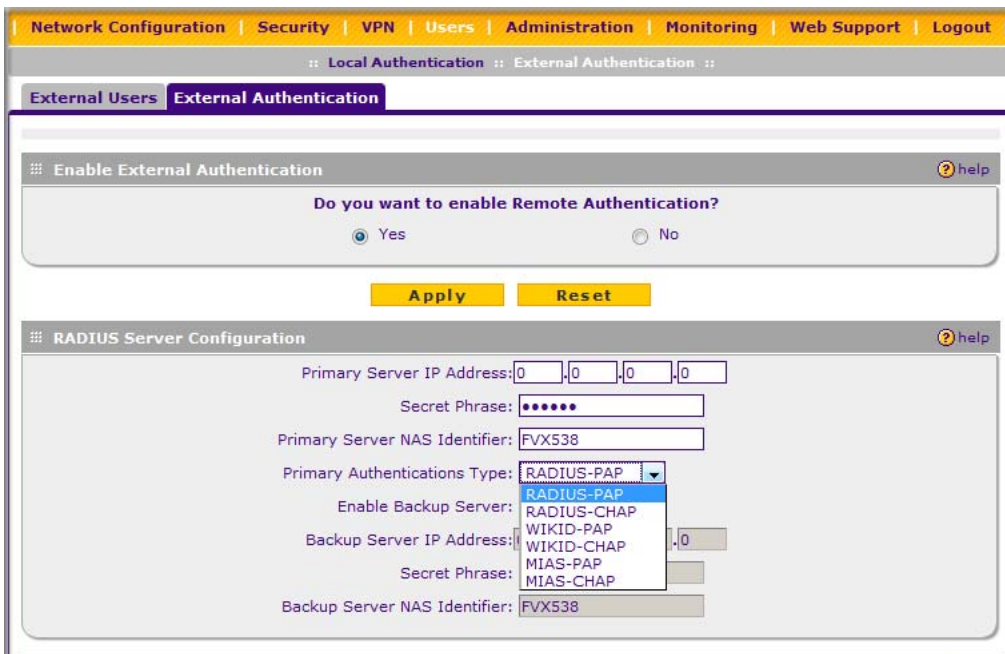


Figure 6-5

When a user logs in, the VPN firewall will validate with the appropriate RADIUS or WIKID server that the user is authorized to log in.

When specifying RADIUS domain authentication, you are presented with several authentication protocol choices, as summarized in the following table:

Table 6-1.

Authentication Protocol	Description
PAP	Password Authentication Protocol (PAP) is a simple protocol in which the client sends a password in clear text.
CHAP	Challenge Handshake Authentication Protocol (CHAP) executes a three-way handshake in which the client and server trade challenge messages, each responding with a hash of the other's challenge message that is calculated using a shared secret value.
MIAS	Network validated PAP or CHAP password based authentication scheme.
WiKID	WiKID is a PAP or CHAP key-based two-factor authentication method using 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 on WiKID authentication.

The chosen authentication protocol must be configured on the RADIUS server and on the authenticating client devices.

Managing Certificates

The FVS318G uses Digital Certificates (also known as X509 Certificates) during the Internet Key Exchange (IKE) authentication phase to authenticate connecting VPN gateways or clients, or to be authenticated by remote entities. The same Digital Certificates are extended for secure web access connections over HTTPS.

Digital Certificates can be either self signed or can be issued by Certification Authorities (CA) such as via an in-house Windows server, or by an external organization such as Verisign or Thawte.

However, if the Digital Certificates contain the extKeyUsage extension then the certificate must be used for one of the purposes defined by the extension. For example, if the Digital Certificate contains the extKeyUsage extension defined to SNMPV2 then the same certificate cannot be used for secure web management.

The extKeyUsage would govern the certificate acceptance criteria in the FVS318G when the same digital certificate is being used for secure web management.

In the FVS318G, the uploaded digital certificate is checked for validity and also the purpose of the certificate is verified. Upon passing the validity test and the purpose matches its use (has to be SSL and VPN) the digital certificate is accepted. The additional check for the purpose of the uploaded digital certificate must correspond to use for VPN and secure web remote management via HTTPS. If the purpose defined is for VPN & HTTPS then the certificate is uploaded to the HTTPS certificate repository and as well in the VPN certificate repository. If the purpose defined is ONLY for VPN then the certificate is only uploaded to the VPN certificate repository. Thus, certificates used by HTTPS and IPSec will be different if their purpose is not defined to be VPN and HTTPS.

The VPN firewall uses digital certificates to authenticate connecting VPN gateways or clients, and to be authenticated by remote entities. A certificate that authenticates a server, for example, is a file that contains:

- 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 absolutely.

You can obtain a certificate from a well-known commercial Certificate Authority (CA) such as Verisign or Thawte, or you can generate and sign your own certificate. Because a commercial CA takes steps to verify the identity of an applicant, a certificate from a commercial CA provides a strong assurance of the server's identity. A self-signed certificate will trigger a warning from most browsers as it provides no protection against identity theft of the server.

Your VPN firewall contains a self-signed certificate from NETGEAR. We recommend that you replace this certificate prior to deploying the VPN firewall in your network.

From the VPN > Certificates menu, you can view the currently loaded certificates, upload a new certificate and generate a Certificate Signing Request (CSR). Your VPN firewall will typically hold two types of certificates:

- CA certificate. Each CA issues its own CA identity certificate in order to validate communication with the CA and to verify the validity of certificates signed by the CA.
- Self certificate. The certificate issued to you by a CA identifying your device.

Viewing and Loading CA Certificates

The Trusted Certificates (CA Certificates) table lists the certificates of CAs and contains the following data:

- **CA Identity (Subject Name).** The organization or person to whom the certificate is issued.
- **Issuer Name.** The name of the CA that issued the certificate.
- **Expiry Time.** The date after which the certificate becomes invalid.

To view the VPN Certificates:

Select **VPN > Certificates** from the main menu. The Certificates screen displays. The top section of the Certificates screen displays the **Trusted Certificates (CA Certificates)**.

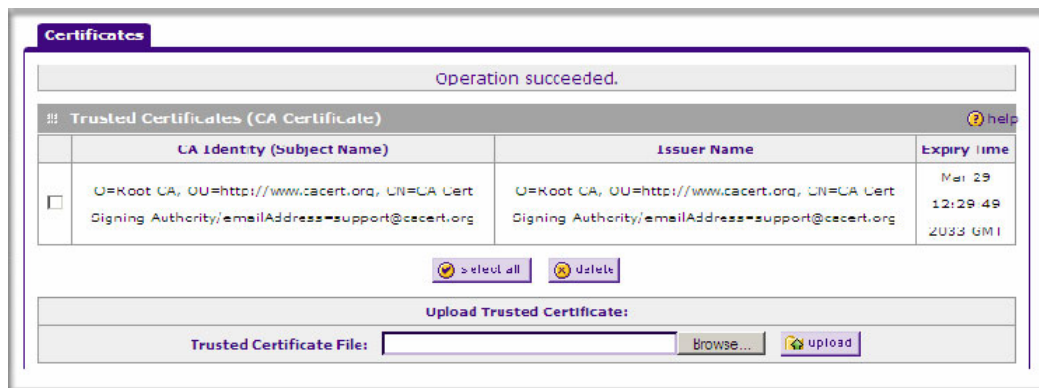


Figure 6-6

When you obtain a self certificate from a CA, you will also receive the CA certificate. In addition, many CAs make their certificates available on their websites.

To load a CA certificate into your VPN firewall:

1. Store the CA certificate file on your computer.
2. Under **Upload Trusted Certificates** in the Certificates menu, click **Browse** and locate the CA certificate file.
3. Click **Upload**. The CA Certificate will appear in the **Trusted Certificates (CA Certificates) table**.

Viewing Active Self Certificates

The Active Self Certificates table in the Certificates screen shows the certificates issued to you by a CA and available for use.

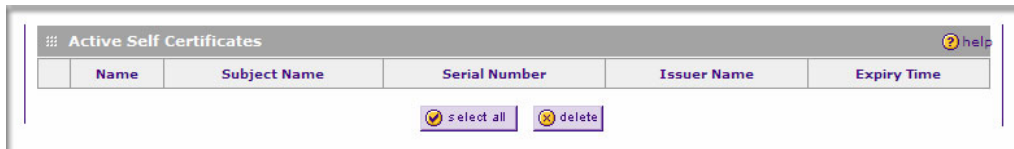


Figure 6-7

For each self certificate, the following data is listed:

- **Name.** The name you used to identify this certificate.
- **Subject Name.** This is the name that other organizations will see as the holder (owner) of this certificate. This should be your registered business name or official company name. Generally, all of your certificates should have the same value in the Subject field.
- **Serial Number.** This is a serial number maintained by the CA. It is used to identify the certificate with in the CA.
- **Issuer Name.** The name of the CA that issued the certificate.
- **Expiry Time.** The date on which the certificate expires. You should renew the certificate before it expires.

Obtaining a Self Certificate from a Certificate Authority

To use a self certificate, you must first request the certificate from the CA, then download and activate the certificate on your system. To request a self certificate from a CA, you must generate a Certificate Signing Request (CSR) for your VPN firewall. The CSR is a file containing information about your company and about the device that will hold the certificate. Refer to the CA for guidelines on the information you include in your CSR.

To generate a new Certificate Signing Request (CSR) file:

1. Locate the **Generate Self Certificate Request** section of the Certificates screen.
2. Configure the following fields:
 - **Name** – Enter a descriptive name that will identify this certificate.

- **Subject** – This is the name which other organizations will see as the holder (owner) of the certificate. Since this name will be seen by other organizations, you should use your registered business name or official company name. (Using the same name, or a derivation of the name, in the Title field would be useful.)

The screenshot shows a web interface for generating a self-certificate request. The top section is titled "Generate Self Certificate Request" and contains several input fields and dropdown menus. The fields are: Name, Subject, Hash Algorithm (set to MD5), Signature Algorithm (set to RSA), Signature Key Length (set to 512), IP Address (Optional), Domain Name (Optional), and E-mail Address (Optional). A "generate..." button is located below these fields. Below the form is a table titled "Self Certificate Requests" with columns for Name, Status, and Action. Below the table are "select all" and "delete" buttons. At the bottom, there is a section for uploading a certificate, with a "Certificate File:" field, a "Browse..." button, and an "upload" button.

Figure 6-8

- From the pull-down menus, choose the following values:
 - Hash Algorithm: MD5 or SHA2.
 - Signature Algorithm: RSA.
 - Signature Key Length: 512, 1024, 2048. (Larger key sizes may improve security, but may also decrease performance.)
- 3. Complete the **Optional** fields, if desired, with the following information:
 - **IP Address** – If you have a fixed IP address, you may enter it here. Otherwise, you should leave this field blank.
 - **Domain Name** – If you have an Internet domain name, you can enter it here. Otherwise, you should leave this field blank.
 - **E-mail Address** – Enter the e-mail address of a technical contact in your organization.

4. Click **Generate**. A new certificate request is created and added to the **Self Certificate Requests** table.

Self Certificate Requests			help
	Name	Status	Action
<input type="checkbox"/>	ExampleFVS336G	Active Self Certificate Not Uploaded	view

Figure 6-9

5. In the **Self Certificate Requests** table, click **View** under the Action column to view the request.

Operation succeeded.

Certificate Details

Subject Name: CN=SSL VPN Router
 Hash Algorithm: MD5
 signature Algorithm: RSA
 Key Length: 512

Data to supply to CA

```

-----BEGIN CERTIFICATE REQUEST-----
MIHSMH4CAQAuSTEXMBUGA1UEAxMOU1NMFZQTIBSb3V0ZXIwIw
AQEFAANLADBIaKEAjdZVQHmp/+HuZRGFZ8+cWki2gGSb0oK7H
eIVbplLg5TeVJaTYZLgvoUCR+6YuRbzkGFSX+wIDAQABoAAyDQY
EQADQQBAGiHy+hEe98FVo+R6tzddfvpFEycCBWMoi1G2EaoxGT
K3p4yzSxNvgzknh+Z/7gU1kZk212
-----END CERTIFICATE REQUEST-----

```

Figure 6-10

6. Copy the contents of the **Data to supply to CA** text box into a text file, including all of the data contained from “-----BEGIN CERTIFICATE REQUEST---” to “---END CERTIFICATE REQUEST---”.
7. Submit your certificate request to a CA:
 - a. Connect to the website of the CA.
 - b. Start the Self Certificate request 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 certificate will be issued.
8. Store the certificate file from the CA on your computer.
9. Return to the Certificates screen and locate the **Self Certificate Requests** section.

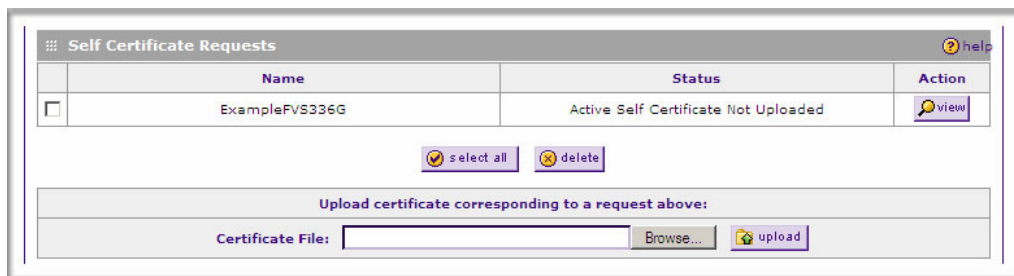


Figure 6-11

10. Select the checkbox next to the certificate request, then click **Browse** and locate the certificate file on your PC.
11. Click **Upload**. The certificate file will be uploaded to this device and will appear in the **Active Self Certificates** list.

If you have not already uploaded the CA certificate, do so now, as described in “[Select VPN > Certificates](#) from the main menu. The Certificates screen displays. The top section of the Certificates screen displays the Trusted Certificates (CA Certificates).” on page 6-9. You should also periodically check your CA’s Certificate Revocation List, as described in “[Managing your Certificate Revocation List \(CRL\)](#)” on page 6-13.

Managing your Certificate Revocation List (CRL)

A CRL (Certificate Revocation List) file shows certificates that have been revoked and are no longer valid. Each CA issues their own CRLs. It is important that you keep your CRLs up-to-date. You should obtain the CRL for each CA regularly.

In the Certificates menu, you can view your currently-loaded CRLs and upload a new CRL.

To view your currently-loaded CRLs and upload a new CRL, follow these steps:

1. Select **VPN > Certificates** from the main menu.

The Certificates menu will display showing the **Certificate Revocation Lists (CRL)** table at the bottom of the screen.

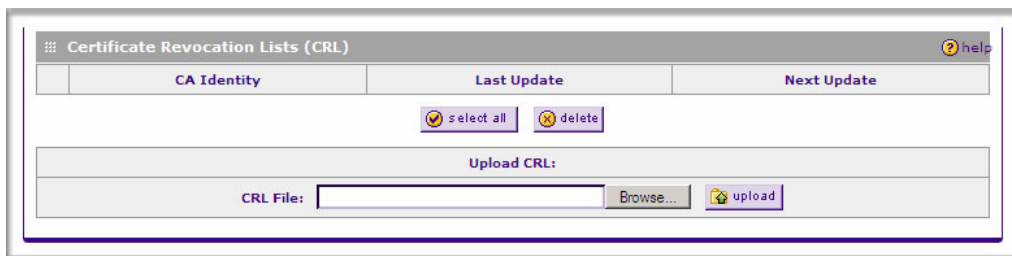


Figure 6-12

The CRL table lists your active CAs and their critical release dates:

- **CA Identify** – The official name of the CA which issued this CRL.
 - **Last Update** – The date when this CRL was released.
 - **Next Update** – The date when the next CRL will be released.
2. Click **Browse** and locate the CRL file you previously downloaded from a CA.
 3. Click **Upload**. The CRL file will be uploaded and the CA Identity will appear in the **Certificate Revocation Lists (CRL)** table. If you had a previous CA Identity from the same CA, it will be deleted.

Chapter 7

Router and Network Management

This chapter describes how to use the network management features of your ProSafe VPN Firewall. These features can be found by clicking on the appropriate heading in the Main Menu of the browser interface.

The ProSafe VPN Firewall offers many tools for managing the network traffic to optimize its performance. You can also control administrator access, be alerted to important events requiring prompt action, monitor the firewall status, perform diagnostics, and manage the firewall configuration file.

This chapter contains the following sections:

- [“Performance Management” on page 7-1](#)
- [“Changing Passwords and Administrator Settings” on page 7-8](#)
- [“Enabling Remote Management Access” on page 7-10](#)
- [“Using the Command Line Interface” on page 7-13](#)
- [“Using an SNMP Manager” on page 7-13](#)
- [“Configuration File Management” on page 7-15](#)
- [“Upgrading the Firmware” on page 7-17](#)
- [“Configuring Date and Time Service” on page 7-18](#)

Performance Management

Performance management consists of controlling the traffic through the VPN firewall so that the necessary traffic gets through when there is a bottleneck and either reducing unnecessary traffic or rescheduling some traffic to low-peak times to prevent bottlenecks from occurring in the first place. The VPN firewall has the necessary features and tools to help the network manager accomplish these goals.

Bandwidth Capacity

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

- LAN side: 8000 Mbps (eight LAN ports at 1000 Mbps each)

- WAN side: 1000 Mbps (one active WAN port at 1000 Mbps)

In practice, the WAN side bandwidth capacity will be much lower when DSL or cable modems are used to connect to the Internet. As a result and depending on the traffic being carried, the WAN side of the firewall will be the limiting factor to throughput for most installations.

Features That Reduce Traffic

Features of the VPN firewall router that can be called upon to decrease WAN-side loading are as follows:

- Service blocking
- Block sites
- Source MAC filtering

Service Blocking

You can control specific outbound traffic (from LAN to WAN). Outbound Services lists all existing rules for outbound traffic. If you have not defined any rules, only the default rule will be listed. The default rule allows all outgoing traffic.



Warning: This feature is for Advanced Administrators only! Incorrect configuration will cause serious problems.

Each rule lets you specify the desired action for the connections covered by the rule:

- BLOCK always
- BLOCK by schedule, otherwise Allow
- ALLOW always
- ALLOW by schedule, otherwise Block

As you define your firewall rules, you can further refine their application according to the following criteria:

- **LAN Users.** These settings determine which computers on your network are affected by this rule. Select the desired options:
 - Any. All PCs and devices on your LAN.
 - Single address. The rule will be applied to the address of a particular PC.
 - Address range. The rule is applied to a range of addresses.

- **Groups.** The rule is applied to a Group (see [“Managing Groups and Hosts \(LAN Groups\)”](#) on page 3-5 to assign PCs to a Group using the LAN Groups Database).
- **WAN Users.** These settings determine which Internet locations are covered by the rule, based on their IP address.
 - **Any.** The rule applies to all Internet IP address.
 - **Single address.** The rule applies to a single Internet IP address.
 - **Address range.** The rule is applied to a range of Internet IP addresses.
- **Services.** You can specify the desired Services or applications to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see [“About Services-Based Rules”](#) on page 4-3 and [“Adding Customized Services”](#) on page 4-16).
- **Schedule.** You can specify whether the rule is to be applied on the Schedule 1, Schedule 2, or Schedule 3 time schedule (see [“Setting a Schedule to Block or Allow Specific Traffic”](#) on page 4-29).

See [“Using Rules to Block or Allow Specific Kinds of Traffic”](#) on page 4-2 for the procedure on how to use this feature.

Services

The Rules menu contains a list of predefined Services for creating firewall rules. If a service does not appear in the predefined Services list, you can define the service. The new service will then appear in the Rules menu's Services list.

See [“About Services-Based Rules”](#) on page 4-3 for the procedure on how to use this feature.

Groups and Hosts

You can apply these rules selectively to groups of PCs to reduce the outbound or inbound traffic. The LAN Groups Database is an automatically-maintained list of all known PCs and network devices. PCs and devices become known by the following methods:

- **DHCP Client Request.** By default, the DHCP server in this VPN firewall is enabled, and will accept and respond to DHCP client requests from PCs and other network devices. These requests also generate an entry in the LAN Groups Database. Because of this, leaving the DHCP server feature (on the LAN screen) enabled is strongly recommended.
- **Scanning the Network.** The local network is scanned using ARP requests. The ARP scan will detect active devices that are not DHCP clients. However, sometimes the name of the PC or device cannot be accurately determined, and will appear in the database as Unknown.

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

See “[Managing Groups and Hosts \(LAN Groups\)](#)” on page 3-5 for the procedure on how to use this feature.

Schedule

If you have set firewall rules on the Rules screen, you can configure three different schedules (for example, schedule 1, schedule 2, and schedule 3) for when a rule is to be applied. Once a schedule is configured, it affects all Rules that use this schedule. You specify the days of the week and time of day for each schedule.

See “[Setting a Schedule to Block or Allow Specific Traffic](#)” on page 4-29 for the procedure on how to use this feature.

Block Sites

If you want to reduce traffic by preventing access to certain sites on the Internet, you can use the VPN firewall router’s filtering feature. By default, this feature is disabled; all requested traffic from any Web site is allowed.

- **Keyword (and Domain Name) Blocking.** You can specify up to 32 words that, should they appear in the Web site name (i.e., URL) or in a newsgroup name, will cause that site or newsgroup to be blocked by the VPN firewall router.

You can apply the keywords to one or more groups. Requests from the PCs in the groups for which keyword blocking has been enabled will be blocked. Blocking does not occur for the PCs that are in the groups for which keyword blocking has not been enabled.

You can bypass keyword blocking for trusted domains by adding the exact matching domain to the list of Trusted Domains. Access to the domains on this list by PCs even in the groups for which keyword blocking has been enabled will still be allowed without any blocking.

- **Web Component blocking.** You can block the following Web component types: Proxy, Java, ActiveX, and Cookies. Sites on the Trusted Domains list are still subject to Web component blocking when the blocking of a particular Web component has been enabled.

See “[Blocking Internet Sites \(Content Filtering\)](#)” on page 4-21 for the procedure on how to use this feature.

Source MAC Filtering

If you want to reduce outgoing traffic by preventing Internet access by certain PCs on the LAN, you can use the source MAC filtering feature to drop the traffic received from the PCs with the specified MAC addresses. By default, this feature is disabled; all traffic received from PCs with any MAC address is allowed.

See “[Configuring Source MAC Filtering](#)” on page 4-24 for the procedure on how to use this feature.

Features That Increase Traffic

Features that tend to increase WAN-side loading are as follows:

- Port forwarding
- Port triggering
- Exposed hosts
- VPN tunnels

Port Forwarding

The firewall always blocks DoS (Denial of Service) attacks. A DoS attack does not attempt to steal data or damage your PCs, but overloads your Internet connection so you can not use it (i.e., the service is unavailable). You can also create additional firewall rules that are customized to block or allow specific traffic.



Warning: This feature is for Advanced Administrators only! Incorrect configuration will cause serious problems.

You can control specific inbound traffic (from WAN to LAN). Inbound Services lists all existing rules for inbound traffic. If you have not defined any rules, only the default rule will be listed. The default rule blocks all inbound traffic.

Each rule lets you specify the desired action for the connections covered by the rule:

- BLOCK always
- BLOCK by schedule, otherwise Allow
- ALLOW always
- ALLOW by schedule, otherwise Block

You can also enable a check on special rules:

- **VPN Passthrough.** Passes the VPN traffic without any filtering, specially used when this firewall is between two VPN tunnel end points.
- **Drop fragmented IP packets.** Drops any fragmented IP packets.
- **UDP Flooding.** Limits the number of UDP sessions created from one LAN machine.
- **TCP Flooding.** Protects the VPN firewall from SYN flood attack.
- **Enable DNS Proxy.** Allows the VPN firewall to handle DNS queries from the LAN.
- **Enable Stealth Mode.** Prevents the VPN firewall from responding to incoming requests for unsupported services.

As you define your firewall rules, you can further refine their application according to the following criteria:

- **LAN Users.** These settings determine which computers on your network are affected by this rule. Select the desired IP Address in this field.
- **WAN Users.** These settings determine which Internet locations are covered by the rule, based on their IP address.
 - Any: The rule applies to all Internet IP address.
 - Single address: The rule applies to a single Internet IP address.
 - Address range: The rule is applied to a range of Internet IP addresses.
- **Destination Address.** These settings determine the destination IP address for this rule which will be applicable to incoming traffic This rule will be applied only when the destination IP address of the incoming packet matches the IP address of the selected WAN interface Selecting ANY enables the rule for any LAN IP destination. WAN1 and WAN2 corresponds to the respective WAN interface governed by this rule.
- **Services.** You can specify the desired Services or applications to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see [“Adding Customized Services”](#) on page 4-16).
- **Schedule.** You can specify whether the rule is to be applied on the Schedule 1, Schedule 2, or Schedule 3 time schedule (see [“Setting a Schedule to Block or Allow Specific Traffic”](#) on page 4-29).

See [“Using Rules to Block or Allow Specific Kinds of Traffic”](#) on page 4-2 for the procedure on how to use this feature.

Port Triggering

Port triggering allows some applications to function correctly that would otherwise be partially blocked by the firewall. Using this feature requires that you know the port numbers used by the application.

Once configured, port triggering operates as follows:

- A PC makes an outgoing connection using a port number defined in the Port Triggering table.
- This VPN firewall records this connection, opens the additional INCOMING port or ports associated with this entry in the Port Triggering table, and associates them with the PC.
- The remote system receives the PC's request and responds using the different port numbers that you have now opened.
- This VPN firewall matches the response to the previous request and forwards the response to the PC. Without port triggering, this response would be treated as a new connection request rather than a response. As such, it would be handled in accordance with the Port Forwarding rules.
 - Only one PC can use a port triggering application at any time.
 - After a PC has finished using a port triggering application, there is a time-out period before the application can be used by another PC. This is required because the firewall cannot be sure when the application has terminated.

See [“Configuring Port Triggering” on page 4-27](#) for the procedure on how to use this feature.

VPN Tunnels

The VPN firewall router permits up to 25 IPsec VPN tunnels and 10 SSL VPN tunnels at a time. Each tunnel requires extensive processing for encryption and authentication.

See [Chapter 5, “Virtual Private Networking Using IPsec”](#) for the procedure on how to use IPsec VPN.

Using QoS to Shift the Traffic Mix

The QoS priority settings determine the priority and, in turn, the quality of service for the traffic passing through the firewall. The QoS is set individually for each service.

- You can accept the default priority defined by the service itself by not changing its QoS setting.
- You can change the priority to a higher or lower value than its default setting to give the service higher or lower priority than it otherwise would have.

The QoS priority settings conform to the IEEE 802.1D-1998 (formerly 802.1p) standard for class of service tag.

You will not change the WAN bandwidth used by changing any QoS priority settings. But you will change the mix of traffic through the WAN ports by granting some services a higher priority than others. The quality of a service is impacted by its QoS setting, however.

See “[Setting Quality of Service \(QoS\) Priorities](#)” on page 4-18 for the procedure on how to use this feature.

Tools for Traffic Management

The ProSafe VPN Firewall includes several tools that can be used to monitor the traffic conditions of the firewall and control who has access to the Internet and the types of traffic they are allowed to have. See “[Monitoring System Performance](#)” on page 9-1 for a discussion of the tools.

Changing Passwords and Administrator Settings

The default administrator and guest password for the Web Configuration Manager is **password**. Netgear recommends that you change this password to a more secure password. You can also configure a separate password for the guest account.

To modify the Admin user account settings, including password:

1. Select Users > Users from the main menu. The Users screen will display.

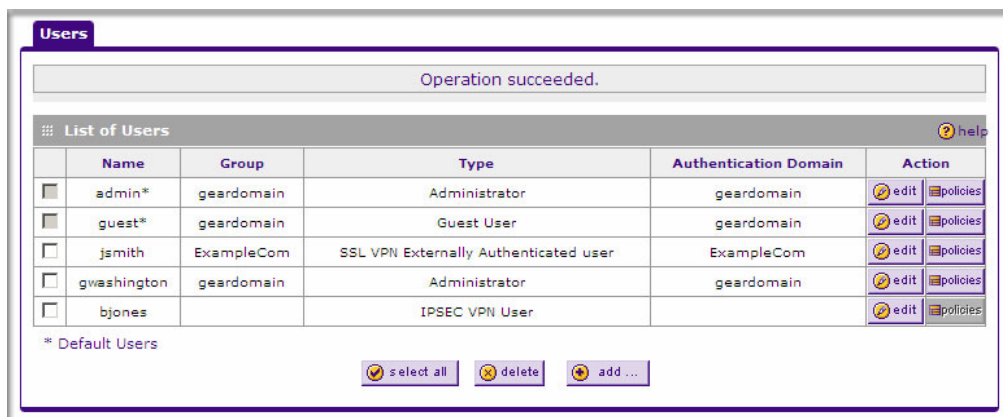



Figure 7-1


2. Select the checkbox adjacent to **admin** in the **Name** column, then click **Edit** in the **Action** column.

The Edit User screen is displayed, with the current settings for Administrator displayed in the **Select User Type** pull-down menu.

Figure 7-2

3. Select the **Check to Edit Password** checkbox. The password fields become active.
4. Enter the old password, then enter the new password twice.
5. (Optional) To change the idle timeout for an administrator login session, enter a new number of minutes in the **Idle Timeout** field.
6. Click **Apply** to save your settings or **Reset** to return to your previous settings.

	Note: If the administrator login timeout value is too large, you may have to wait a long time before you are able to log back into the VPN firewall if your previous login was disrupted (for example, if you did not click Logout on the Main Menu bar to log out).
---	--

	Note: After a factory default reset, the password and timeout value will be changed back to password and 5 minutes, respectively.
---	--

Enabling Remote Management Access

Using the Remote Management page, you can allow an administrator on the Internet to configure, upgrade, and check the status of your VPN firewall. You must be logged in locally to enable remote management (see [“Logging into the VPN Firewall Router Router”](#) on page 2-2).



Note: Be sure to change the default configuration password of the firewall to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both upper and lower case), numbers, and symbols. Your password can be up to 30 characters. See [“Changing Passwords and Administrator Settings”](#) on page 7-8 for the procedure on how to do this.

To configure your firewall for Remote Management:

1. Select **Administration > Remote Management** from the main menu. The **Remote Management** screen is displayed.

The screenshot displays the configuration interface for the ProSafe Gigabit 8 Port VPN Firewall FVS318G. The top navigation bar includes links for Network Configuration, Security, VPN, Users, Administration, Monitoring, Web Support, and Logout. Below this, a secondary navigation bar shows Remote Management, SNMP, Settings Backup & Upgrade, and Time Zone. The main content area is titled "Remote Management" and contains two sections: "Secure HTTP Management" and "Telnet Management".

Secure HTTP Management

Allow Secure HTTP Management?

Yes

No

Everyone (Be sure to change default password)

IP address range:

From:

To:

Only this PC:

Port Number:

Telnet Management

Allow Telnet Management?

Yes

No

Everyone (Be sure to change default password)

IP address range:

From:

To:


Only this PC:

At the bottom of the configuration area are two buttons: "Apply" and "Reset".

Figure 7-3

2. Click the **Yes** radio button to enable HTTPS remote management (enabled by default).
3. To enable remote management by the command line interface (CLI) over Telnet, click **Yes** to Allow Telnet Management, and configure the external IP addresses that will be allowed to connect.
 - a. To allow access from any IP address on the Internet, select Everyone.
 - b. To allow access from a range of IP addresses on the Internet, select IP address range. Enter a beginning and ending IP address to define the allowed range.

- c. To allow access from a single IP address on the Internet, select Only this PC.
Enter the IP address that will be allowed access.


	Note: For enhanced security, restrict access to as few external IP addresses as practical. See “Password/Confirm Password. The password can contain alphanumeric characters, dash, and underscore.” on page 6-3 for instructions on restricting administrator access. Be sure to use strong passwords.
---	---


4. Click **Apply** to have your changes take effect.


For accessing your VPN firewall from the Internet, the Secure Sockets Layer (SSL) will be enabled. You will enter `https://` (not `http://`) and type your firewall’s WAN IP address into your browser. For example, if your WAN IP address is 172.16.0.123, type the following in your browser:


`https://172.16.0.123`

The VPN firewall’s remote login URL is **`https://<IP_address>`** or **`https://<FullyQualifiedDomainName>`**.

	Note: To maintain security, the FVS318G will reject a login that uses <code>http://address</code> rather than the SSL <code>https://address</code> .
---	---

	Note: The first time you remotely connect to the FVS318G with a browser via SSL, you may get a warning message regarding the SSL certificate. If you are using a Windows computer with Internet Explorer 5.5 or higher, simply click Yes to accept the certificate.
---	--

	Note: If you are unable to remotely connect to the FVS318G after enabling HTTPS remote management, check whether other user policies, such as the default user policy, are preventing access.
---	--

	Tip: If you are using a dynamic DNS service such as TZO, you can identify the WAN IP address of your FVS318G by running <code>tracert</code> from the Windows Run menu option. Trace the route to your registered FQDN. For example, enter <code>tracert FVS318G.mynetgear.net</code> , and the WAN IP address that your ISP assigned to the FVS318G is displayed.
---	---

Using the Command Line Interface



Note: The command line interface is not supported at this time. Check the NETGEAR Web site for the latest status.

You can access the command line interface (CLI) using Telnet from the LAN or, if enabled in the Remote Management menu, from the WAN.

To access the CLI from a communications terminal when the VPN firewall is still set to its factory defaults (or use your own settings if you have changed them), do the following:

1. From your computer's command line prompt, enter the following command:

```
telnet 192.168.1.1
```

2. Enter **admin** and **password** when prompted for the login and password information (or enter **guest** and **password** to log in as a read-only guest).
3. Enter **exit** to end the CLI session.

Any configuration changes made via the CLI are not preserved after a reboot or power cycle unless the user issues the CLI **save** command after making the changes.

Using an SNMP Manager

Simple Network Management Protocol (SNMP) lets you monitor and manage your VPN firewall from an SNMP Manager. It provides a remote means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

The SNMP Configuration table lists the SNMP configurations by:

- **IP Address.** The IP address of the SNMP manager.
- **Port.** The trap port of the configuration.
- **Community.** The trap community string of the configuration.

To create a new SNMP configuration entry:

1. Select **Administration > SNMP** from the main menu. The **SNMP** screen is displayed.

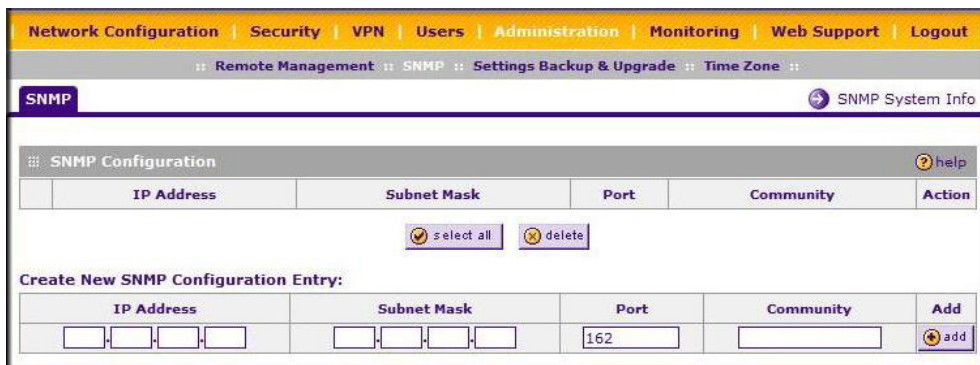


Figure 7-4

2. Configure the following fields in the **Create New SNMP Configuration Entry** section:
 - a. Enter the IP Address of the SNMP manager in the **IP Address** field and the Subnet Mask in the **Subnet Mask** field.
 - To allow only the host address to access the VPN firewall router and receive traps, enter an IP Address of, for example, 192.168.1.101 with a Subnet Mask of 255.255.255.255.
 - To allow a subnet access to the VPN firewall router through SNMP, enter an IP address of, for example, 192.168.1.101 with a Subnet Mask of 255.255.255.0. The traps will still be received on 192.168.1.101, but the entire subnet will have access through the community string.
 - To make the VPN firewall router globally accessible using the community string, but still receive traps on the host, enter 0.0.0.0 as the Subnet Mask and an IP Address for where the traps will be received.
 - b. Enter the trap port number of the configuration in the **Port** field. The default is 162.
 - c. Enter the trap community string of the configuration in the **Community** field.
3. Click **Add** to create the new configuration. The entry is displayed in the **SNMP Configuration** table.

The **SNMP System Info** option arrow at the top of the tab opens the **SNMP SysConfiguration** menu that displays the SNMP System contact information available to the SNMP manager:

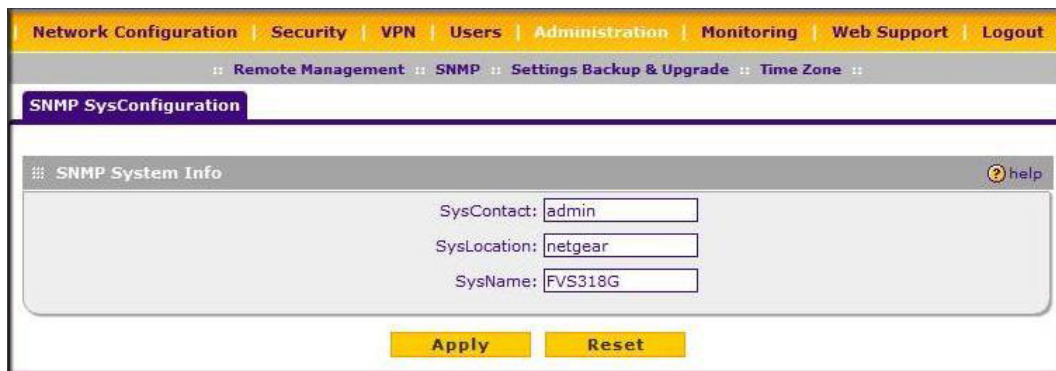


Figure 7-5

You can edit the System Contact, System Location, and System name.

Configuration File Management

The configuration settings of the VPN firewall are stored within the firewall in a configuration file. This file can be saved (backed up) to a user's PC, retrieved (restored) from the user's PC, or cleared to factory default settings.

Once you have installed the VPN firewall router and have it working properly, you should back up a copy of your settings to a file on your computer. If necessary, you can later restore the VPN firewall router settings from this file. The **Settings Backup and Firmware Upgrade** screen allows you to:

- Back up and save a copy of your current settings
- Restore saved settings from the backed-up file.
- Revert to the factory default settings.
- Upgrade the VPN firewall router firmware from a saved file on your hard disk to use a different firmware version.

Backup and Restore Settings

To backup settings:

1. Select Administration > Settings Backup and Firmware Upgrade from the main menu. The **Settings Backup and Firmware Upgrade** screen is displayed.

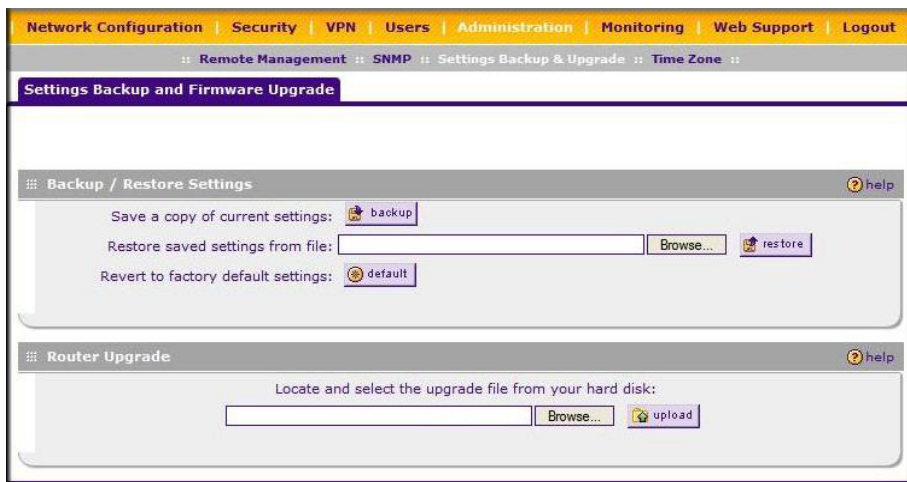



Figure 7-6

2. Click **Backup** to save a copy of your current settings.
 - If your browser isn't set up to save downloaded files automatically, locate where you want to save the file, specify file name, and click Save.
 - If you have your browser set up to save downloaded files automatically, the file will be saved to your browser's download location on the hard disk.

	<p>Warning: Once you start restoring settings or erasing the VPN firewall, 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 it finishes restarting!</p>
---	--

To restore settings from a backup file:

1. Next to **Restore save settings from file**, click **Browse**.
2. Locate and select the previously saved backup file (by default, netgear.cfg).
3. When you have located the file, click **restore**.

An Alert page will appear indicating the status of the restore operation. You must manually restart the VPN firewall router for the restored settings to take effect.

Revert to Factory Default Settings

To reset the VPN firewall to the original factory default settings:

1. Click **default**.
2. You must manually restart the VPN firewall router in order for the default settings to take effect. After rebooting, the VPN firewall's password will be **password** and the LAN IP address will be **192.168.1.1**. The VPN firewall router will act as a DHCP server on the LAN and act as a DHCP client to the Internet.



Warning: When you click **default**, your VPN firewall settings will be erased. All firewall rules, VPN policies, LAN/WAN settings and other settings will be lost. Backup your settings if you intend on using them!

Upgrading the Firmware

You can install a different version of the VPN firewall router firmware from the **Settings Backup and Firmware Upgrade** menu. To view the current version of the firmware that your VPN firewall router is running, choose **Monitoring** from the main menu. In the displayed **Router Status** screen, the **System Info** frame shows the firmware version. When you upgrade your firmware, this frame will change to reflect the new version.

To download a firmware version:

1. Go to the NETGEAR Web site at <http://www.netgear.com/support> and click **Downloads**.
2. From the **Product Selection** pull-down menu, choose the FVS318G.
3. Click on the desired firmware version to reach the download page. Be sure to read the release notes on the download page before continuing.
4. Follow the **To Upgrade** steps to download your firmware.

To upgrade the router software:

1. Select Administration > Settings Backup and Firmware Upgrade from the main menu.
2. Click **Browse** in the **Router Upgrade** section.

3. Locate the downloaded file and click **upload**. This will start the software upgrade to your VPN firewall router. This may take some time. At the conclusion of the upgrade, your VPN firewall will reboot.



Warning: Do not try to go online, turn off the VPN firewall, shutdown the computer or do anything else to the VPN firewall until the VPN firewall finishes the upgrade! When the Test light turns off, wait a few more seconds before continuing.

4. After the VPN firewall router has rebooted, check the firmware version in the **Router Status** screen to verify that your router now has the new firmware installed.



Note: In some cases, such as a major upgrade, it may be necessary to erase the configuration and manually reconfigure your VPN firewall after upgrading it. Refer to the notes on the firmware download page to find out if this is required.

Configuring Date and Time Service

Date, time and NTP server designations can be reset on the **Time Zone** screen. Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock times in a network of computers.

To set Time, Date and NTP servers:

1. Select Administration > Time Zone from the main menu. The **Time Zone** screen is displayed.



Figure 7-7

2. From the **Date/Time** pull-down menu, choose the Local Time Zone. This is required in order for scheduling to work correctly. The VPN firewall router includes a real-time clock (RTC), which it uses for scheduling.
3. If supported in your region, select **Automatically Adjust for Daylight Savings Time**.
4. Select an NTP Server option:
 - **Use Default NTP Servers.** The RTC is updated regularly by contacting a NETGEAR NTP server on the Internet. A primary and secondary (backup) server are preloaded.
 - **Use Custom NTP Servers.** To use a particular NTP server, enter the name or IP address of the NTP Server in the **Server 1 Name/IP Address** field. You can enter the address of a backup NTP server in the **Server 2 Name/IP Address** field. If you select this option and leave either the Server 1 or Server 2 fields empty, they will be set to the default Netgear NTP servers.



Note: If you select the default NTP servers or if you enter a custom server FQDN, the VPN firewall must determine the IP address of the NTP server by a DNS lookup. You must configure a DNS server address in the Network menu before the VPN firewall can perform this lookup.

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

Chapter 8

Troubleshooting

This chapter provides troubleshooting tips and information for your ProSafe VPN Firewall. After each problem description, instructions are provided to help you diagnose and solve the problem.

This chapter contains the following sections:

- “Basic Functions” on page 8-1
- “Troubleshooting the Web Configuration Interface” on page 8-3
- “Troubleshooting the ISP Connection” on page 8-4
- “Troubleshooting a TCP/IP Network Using a Ping Utility” on page 8-5
- “Restoring the Default Configuration and Password” on page 8-7
- “Problems with Date and Time” on page 8-8
- “Using the Diagnostics Utilities” on page 8-9

Basic Functions

After you turn on power to the VPN firewall, the following sequence of events should occur:

1. When power is first applied, verify that the PWR LED is on.
2. After approximately two minutes, verify that:
 - a. The Test LED is not lit.
 - b. The LAN port LINK/ACT LEDs are lit for any local ports that are connected.
 - c. The WAN port LINK/ACT LEDs are lit for any WAN ports that are connected.

If a port’s LINK/ACT LED is lit, a link has been established to the connected device. If a LAN port is connected to a 1000 Mbps device, verify that the port’s SPEED LED is green. If the port is 100 Mbps, the LED will be amber. If the port is 10 Mbps, the LED will be off.

If any of these conditions does not occur, refer to the appropriate following section.

Power LED Not On

If the Power and other LEDs are off when your VPN firewall is turned on:

- Make sure that the power cord is properly connected to your VPN firewall and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12 V DC power adapter supplied by NETGEAR for this product.

If the error persists, you have a hardware problem and should contact technical support.

LEDs Never Turn Off

When the VPN firewall is turned on, the LEDs turn on for about 10 seconds and then turn off. If all the LEDs stay on, there is a fault within the firewall.

If all LEDs are still on one minute after power up:

- Cycle the power to see if the VPN firewall recovers.
- Clear the VPN firewall's configuration to factory defaults. This will set the VPN firewall's IP address to 192.168.1.1. This procedure is explained in [“Restoring the Default Configuration and Password” on page 8-7](#).

If the error persists, you might have a hardware problem and should contact technical support.

LAN or WAN Port LEDs Not On

If either the LAN LEDs or WAN LEDs do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the VPN firewall and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.
- Be sure you are using the correct cable:

When connecting the VPN firewall's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

Troubleshooting the Web Configuration Interface

If you are unable to access the VPN firewall's Web Configuration interface from a PC on your local network, check the following:

- Check the Ethernet connection between the PC and the VPN firewall as described in the previous section.
- Make sure your PC's IP address is on the same subnet as the VPN firewall. If you are using the recommended addressing scheme, your PC's address should be in the range of 192.168.1.2 to 192.168.1.254.



Note: If your PC's IP address is shown as 169.254.x.x: Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the PC to the VPN firewall and reboot your PC.

- If your VPN firewall's IP address has been changed and you don't know the current IP address, clear the VPN firewall's configuration to factory defaults. This will set the VPN firewall's IP address to 192.168.1.1. This procedure is explained in [“Restoring the Default Configuration and Password”](#) on page 8-7.



Tip: If you don't want to revert to the factory default settings and lose your configuration settings, you can reboot the VPN firewall and use a sniffer to capture packets sent during the reboot. Look at the ARP packets to locate the VPN firewall's LAN interface address.

- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

If the VPN firewall does not save changes you have made in the Web Configuration Interface, check the following:

- When entering configuration settings, be sure to click the APPLY button before moving to another menu or tab, or your changes are lost.
- Click the Refresh or Reload button in the Web browser. The changes may have occurred, but the Web browser may be caching the old configuration.

Troubleshooting the ISP Connection

If your VPN firewall is unable to access the Internet, you should first determine whether the VPN firewall is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your VPN firewall must request an IP address from the ISP. You can determine whether the request was successful using the Web Configuration Manager.

To check the WAN IP address:

1. Launch your browser and navigate to an external site such as www.netgear.com
2. Access the Main Menu of the VPN firewall's configuration at <https://192.168.1.1>
3. Under the Monitoring menu, click Router Status.
4. Check that an IP address is shown for the WAN Port.
If 0.0.0.0 is shown, your VPN firewall has not obtained an IP address from your ISP.

If your VPN firewall is unable to obtain an IP address from the ISP, you may need to force your cable or DSL modem to recognize your new VPN firewall by performing the following procedure:

1. Turn off power to the cable or DSL modem.
2. Turn off power to your VPN firewall.
3. Wait five minutes and reapply power to the cable or DSL modem.
4. When the modem's LEDs indicate that it has reacquired sync with the ISP, reapply power to your VPN firewall.

If your VPN firewall is still unable to obtain an IP address from the ISP, the problem may be one of the following:

- Your ISP may require a login program.
Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, you may have incorrectly set the login name and password.

- Your ISP may check for your PC's host name. Assign the PC Host Name of your ISP account as the Account Name in the Basic Settings menu.
- Your ISP only allows one Ethernet MAC address to connect to the Internet, and may check for your PC's MAC address. In this case:
 - Inform your ISP that you have bought a new network device, and ask them to use the VPN firewall's MAC address; or
 - Configure your VPN firewall to spoof your PC's MAC address. This can be done in the Basic Settings menu. Refer to [“Manually Configuring the Internet Connection”](#) on page 2-7.

If your VPN firewall can obtain an IP address, but your PC is unable to load any Web pages from the Internet:

- Your PC may not recognize any DNS server addresses.

A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. You may configure your PC manually with DNS addresses, as explained in your operating system documentation.
- Your PC may not have the VPN firewall configured as its TCP/IP gateway.

Troubleshooting a TCP/IP Network Using a Ping Utility

Most TCP/IP terminal devices and firewalls contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. Troubleshooting a TCP/IP network is made very easy by using the Ping utility in your PC or workstation.

Testing the LAN Path to Your VPN Firewall Router

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

To ping the firewall from a PC running Windows 95 or later:

1. From the Windows toolbar, click **Start** and choose **Run**.
2. In the field provided, type “ping” followed by the IP address of the VPN firewall; for example:

```
ping 192.168.1.1
```

3. Click **Ok**. A message, similar to the following, should display:

```
Pinging <IP address> with 32 bytes of data
```

If the path is working, you will see this message:

```
Reply from <IP address>: bytes=32 time=NN ms TTL=xxx
```

If the path is not working, you will see this message:

```
Request timed out
```

If the path is not functioning correctly, you could have one of the following problems:

- Wrong physical connections
 - Make sure the LAN port LED is on. If the LED is off, follow the instructions in “[LAN or WAN Port LEDs Not On](#)” on page 8-2.
 - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and VPN firewall.
- Wrong network configuration
 - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC 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.

Testing the Path from Your PC to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device. From the Windows run menu, type:

```
PING -n 10 <IP address>
```

where <IP address> is the IP address of a remote device such as your ISP’s DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- Check that your PC has the IP address of your VPN firewall listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC’s Network Control Panel.
- Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.

- If your ISP assigned a host name to your PC, enter that host name as the Account Name in the Basic Settings menu.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your VPN firewall to “clone” or “spoof” the MAC address from the authorized PC. Refer to [“Manually Configuring the Internet Connection”](#) on page 2-7.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the VPN firewall’s administration password to **password** and the IP address to **192.168.1.1**. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the VPN firewall (see [“Configuration File Management”](#) on page 7-15).
- Use the reset button on the rear panel of the VPN firewall. Use this method for cases when the administration password or IP address is not known.

To restore the factory default configuration settings without knowing the administration password or IP address, you must use the reset button on the rear panel of the VPN firewall.

To restore the factory defaults:

1. Press and hold the reset button until the Test LED turns on and begins to blink (about 10 seconds).
2. Release the reset button and wait for the VPN firewall to reboot.

Problems with Date and Time

The Administration | Time Zone menu displays the current date and time of day. The VPN firewall uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day.

Problems with the date and time function can include:

- Date shown is January 1, 2000. Cause: The VPN firewall has not yet successfully reached a Network Time Server. Check that your Internet access settings are configured correctly. If you have just completed configuring the VPN firewall, wait at least five minutes and check the date and time again.
- Time is off by one hour. Cause: The VPN firewall does not automatically sense Daylight Savings Time. Check the Time Zone menu, and check or uncheck the box marked “Adjust for Daylight Savings Time”.

Using the Diagnostics Utilities

You can perform diagnostics such as pinging an IP address, performing a DNS lookup, displaying the routing table, rebooting the firewall, and capturing packets. Select **Monitoring > Diagnostics** from the main menu. The Diagnostics screen displays.



Note: For normal operation, diagnostics are not required.

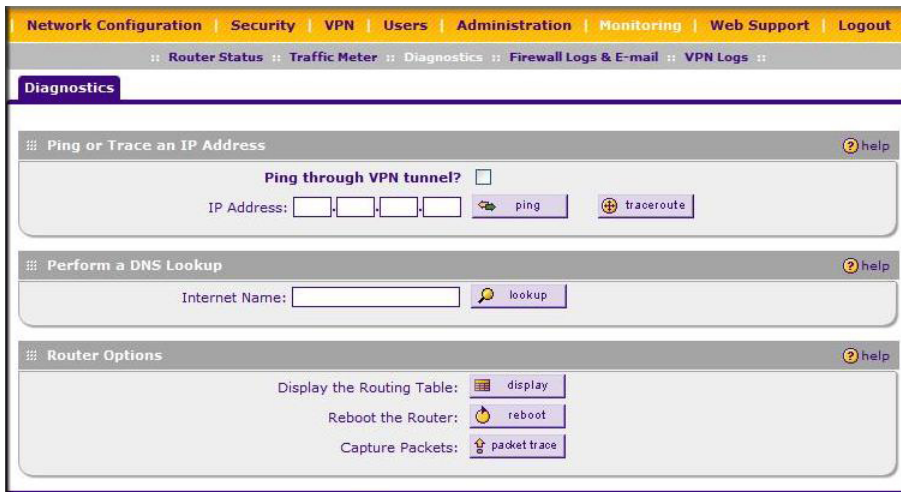


Figure 8-1

Table 8-1. Diagnostics

Item	Description
Ping or trace an IP address	Ping – Used to send a ping packet request to a specified IP address—most often, to test a connection. If the request times out (no reply is received), it usually means that the destination is unreachable. However, some network devices can be configured not to respond to a ping. The ping results will be displayed in a new screen; click “Back” on the Windows menu bar to return to the Diagnostics screen. If the specified address is intended to be reached through a VPN tunnel, check Ping through VPN tunnel .
	Traceroute – Lists all routers between the source (this device) and the destination IP address. The traceroute results will be displayed in a new screen; click “Back” on the Windows menu bar to return to the Diagnostics screen.
Perform a DNS lookup	A DNS (Domain Name Server) converts the Internet name (for example, www.netgear.com) to an IP address. If you need the IP address of a Web, FTP, Mail or other Server on the Internet, you can request a DNS lookup to find the IP address.
Display the routing table	This operation will display the internal routing table, which can be used by Technical Support to diagnose routing problems.
Reboot the VPN firewall	Used to perform a remote reboot (restart). You can use this if the VPN firewall seems to have become unstable or is not operating normally.
	Note: Rebooting will break 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 will automatically be re-established when possible.
Packet trace	Packet Trace selects the interface and starts the packet capture on that interface.

Appendix A

Technical Specifications and Factory Default Settings

You can use the reset button located on the front of your device to reset all settings to their factory defaults. This is called a hard reset.

- To perform a hard reset, push and hold the reset button for approximately 5 seconds (until the Test LED blinks rapidly). Your device will return to the factory configuration settings shown in [Table A-1](#) below.
- Pressing the reset button for a shorter period of time will simply cause your device to reboot.

Table A-1. Business Router Default Configuration Settings

Feature	Default Behavior
Router Login	
User Login URL	http://192.168.1.1/index.htm
User Name (case sensitive)	admin
Login Password (case sensitive)	password
Internet Connection	
WAN MAC Address	Use Default address
WAN MTU Size	1500
Port Speed	AutoSense
Local Network (LAN)	
Lan IP	192.168.1.1
Subnet Mask	255.255.255.0
RIP Direction	None
RIP Version	Disabled
RIP Authentication	None
DHCP Server	Enabled

Table A-1. Business Router Default Configuration Settings

Feature		Default Behavior
	DHCP Starting IP Address	192.168.1.2
	DHCP Ending IP Address	192.168.1.254
	DMZ	Disabled
	Time Zone	GMT
	Time Zone Adjusted for Daylight Saving Time	Disabled
	SNMP	Disabled
Firewall		
	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the http port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled

This appendix provides technical specifications for the ProSafe VPN Firewall.

Table A-2. Technical Specificaions

Specification		Description
Network Protocol and Standards Compatibility		
	Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP PPP over Ethernet (PPPoE)
Power Adapter		
	North America:	120V, 60 Hz, input
	United Kingdom, Australia:	240V, 50 Hz, input
	Europe:	230V, 50 Hz, input
	Japan:	100V, 50/60 Hz, input
	All regions (output):	12 V DC @ 1.5 A output, 18W maximum
Physical Specifications		
	Dimensions:	32 x 189 x 123 mm (1.6 x 10 x 7 in)
	Weight:	590 g (1.3 lb)
Environmental Specifications		
	Operating temperature:	0° to 40° C (32° to 104° F)
	Operating humidity:	90% maximum relative humidity, noncondensing
Electromagnetic Emissions		
	Meets requirements of:	FCC Part 15 Class B
		VCCI Class B
		EN 55 022 (CISPR 22), Class B
Interface Specifications		
	LAN:	Eight 10/100/1000BASE-Tx (Gb), RJ-45 ports
	WAN:	One 10/100/1000BASE-Tx (Gb), RJ-45 port

Appendix B

Related Documents

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
Internet Networking and TCP/IP Addressing	http://documentation.netgear.com/reference/enu/tcpip/index.htm
Wireless Communications	http://documentation.netgear.com/reference/enu/wireless/index.htm
Preparing a Computer for Network Access	http://documentation.netgear.com/reference/enu/wsdhcp/index.htm
Virtual Private Networking (VPN)	http://documentation.netgear.com/reference/enu/vpn/index.htm
Glossary	http://documentation.netgear.com/reference/enu/glossary/index.htm

Appendix C

Two Factor Authentication

This appendix provides an overview of two factor authentication, and an example of how to implement the WiKID solution.

This appendix contains the following sections:

- [“Why do I need Two-Factor Authentication?”](#) on page C-1
- [“NETGEAR Two-Factor Authentication Solutions”](#) on page C-2

Why do I need Two-Factor Authentication?

In today’s market, online identity theft and online fraud continue to be one of the fast-growing cyber crime activities used by many unethical hackers and cyber criminals to steal digital assets for financial gains. Many companies and corporations are losing millions of dollars and running into risks of revealing their trade secrets and other proprietary information as the results of these cyber crime activities. Security threats and hackers have becoming more sophisticated where user names, encrypted passwords and the presence of firewalls are no longer enough to protect the networks from being compromised. IT professionals and security experts have recognized the need to go beyond the traditional authentication process by introducing and requiring additional factors to the authentication process. NETGEAR has also recognized the need to provide more than just a firewall to protect the networks. As part the new maintenance firmware release, NETGEAR has implemented a more robust authentication system known as Two-Factor Authentication (2FA or T-FA) on its SSL and IPSec VPN firewall product line to help address the fast-growing network security issues.

What are the benefits of Two-Factor Authentication?

- **Stronger security.** Passwords cannot efficiently protect the corporate networks because attackers can easily guess simple passwords or users cannot remember complex and unique passwords. One-time passcode (OTP) strengthens and replaces the need to remember complex password.
- **No need to replace existing hardware.** Two-Factor Authentication can be added to existing NETGEAR products through via firmware upgrade.

- **Quick to deploy and manage.** The WiKID solution integrates seamlessly with the NETGEAR SSL and VPN firewall products.
- **Proven regulatory compliance.** Two-Factor Authentication has been used as a mandatory authentication process for many corporations and enterprises worldwide.

What is Two-Factor Authentication

Two-Factor Authentication is a new security solution that enhances and strengthens security by implementing multiple factors to the authentication process that challenge and confirm the users identities before they can gain access to the network. There are several factors that are used to validate the users to make that you are who you said you are. These factors are:

Something you know – for example, your password or your PIN

Something you have – for example, a token with generated passcode that is either 6 to 8 digits in length.

Something you are – for example, biometrics such as fingerprints or retinal.

We will only focus and discuss the first two factors – something you know and something you have. This new security method can be viewed as a two-tiered authentication approach because it typically relies on what you know and what you have. A common example of two-factor authentication is a bank (ATM) card that has been issued by a bank institute:

- The PIN to access your account is “*something you know*”
- The ATM card is “*something you have*”

You must have both of these factors to gain access to your bank account. Similar to the ATM card, access to the corporate networks and data can also be strengthen using combination of the multiple factors such as a PIN and a token (hardware or software) to validate the users and reduce the incidence of online identity theft.

NETGEAR Two-Factor Authentication Solutions

NETGEAR has implemented 2 Two-Factor Authentication solutions from WiKID. WiKID is the software-based token solution. So instead of using Windows Active Directory or LDAP as the authentication server, administrators now have the option to use WiKID to do Two-Factor Authentication on NETGEAR SSL and VPN firewall products.

The WiKID solution is based on a request-response architecture where a one-time passcode (OTP), that is time synchronized with the authentication server, is generated and sent to the user once the validity of a user credential has been confirmed by the server. The request-response architecture is capable of self-service initialization by end-users, dramatically reducing implementation and maintenance costs. Here is a quick example of how WiKID work.

1. The user launches the WiKID token software, enter the PIN that has been given to them (*something they know*) and then press “continue” to receive the one-time passcode (OTP) from the WiKID authentication server:



Figure C-1

2. A one-time passcode (*something they have*) is generated for this user.

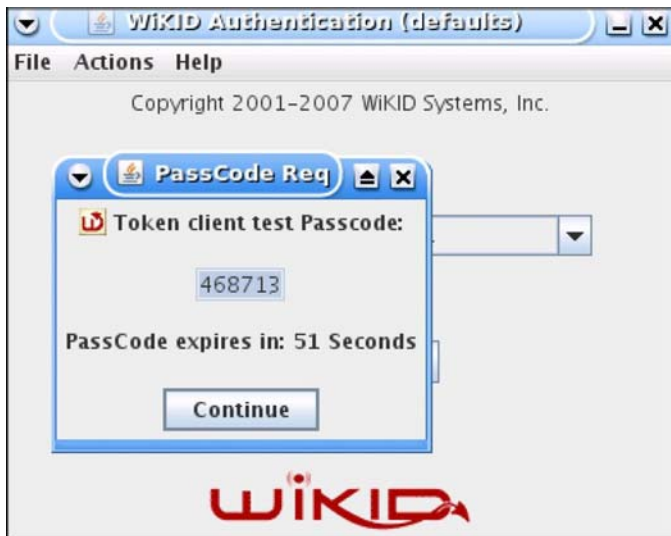



Figure C-2

	<p>Note: The one-time passcode is time synchronized to the authentication server so that the OTP can only be used once and must be used before the expiration time. If a user does not use this passcode before it is expired, the user will need to go through the request process again to generate a new OTP.</p>
--	---

3. The user then goes to the two factor login page and enters the generated one-time passcode as the login password.

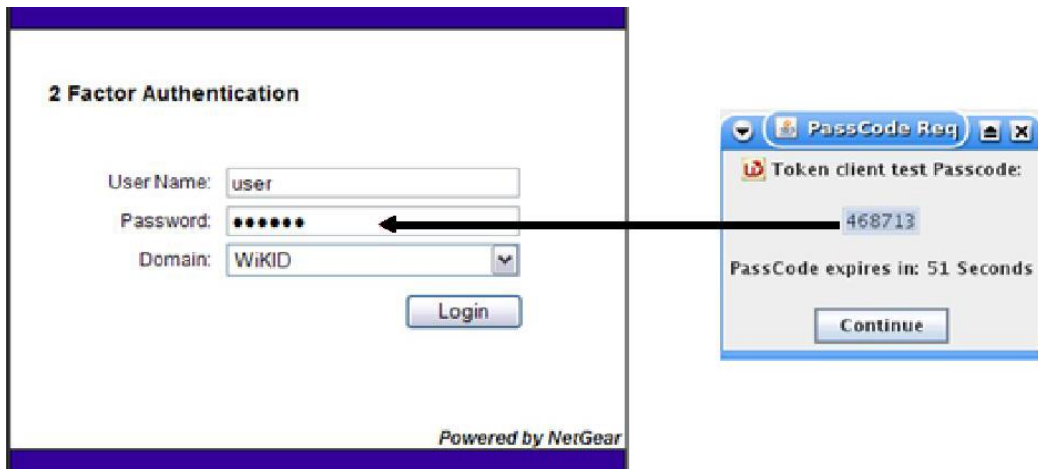


Figure C-3

Two-Factor Authentication is a new and easy way to enhance networking security products without having to replace the existing hardware. To obtain and try the new Two-Factor Authentication solution on your products, visit NETGEAR Support website at <http://kbserver.netgear.com>.

A

- access
 - remote management 7-10
- Add LAN WAN Inbound Service4-10
- Add LAN WAN Outbound Service4-10
- Adding4-16
- Add Mode Config Record screen 5-22
- address reservation 3-9
- administrator login timeout 7-9
- Advanced Options
 - MTU Size 2-15
 - Port Speed 2-16
 - Router's MAC Address 2-16
- Allowing Videoconference from Restricted Addresses
 - example of 4-13
- Attack Checks
 - about 4-19
- Attack Checks screen 4-19
- authentication
 - WiKID 6-8
- Authentication Algorithm
 - IKE Policy 5-15, 5-17
- Auto Detect 2-5
- Auto Uplink 1-3

B

- backup and restore settings 7-15
- bandwidth capacity 7-1
- Block Sites
 - Content Filtering4-21
- Block Sites
 - reducing traffic 7-4
- Block Sites screen4-23

- Block TCP Flood4-20
- block traffic
 - with schedule4-29
- Blocking Instant Messenger
 - example of4-16
- Content4-21
- Content Filtering4-1
 - about4-21
 - Block Sites4-21
 - enabling4-23
 - firewall protection, about4-1
- content filtering4-1
- customized service
 - adding4-3,4-17
 - editing4-18

C

- CA
 - about 6-9
- certificate
 - generate new CSR 6-11
- Certificate Signing Request, see CSR
- certificates
 - management of 6-11
- Certificate Authority. See CA
- Classical Routing definition of 2-11
- CLI management
 - by Telnet 7-11
- command line interface 7-13
- configuration
 - automatic by DHCP 1-3
- content filtering 1-2
- connecting the VPN firewall 2-1
- crossover cable 1-3

crossover cable 8-2

CSR 6-11

D

Date

troubleshooting 8-8

Date

setting 7-18

Daylight Savings Time

adjusting for 7-19

DNS proxy 7-6

DDNS

about 2-12

configuration of 2-14

providers of 2-12

default configuration

restoring 8-7

default password 2-2diagnostics

DNS lookup 8-9

packet capture 8-9

ping 8-9

rebooting 8-9

routing table 8-9

Denial of Service. See DoS.

Diagnostics screen 8-9

DHCP 2-6

denial of service attack4-20

DHCP

DNS server address 3-4

DHCP Address Pool 3-4

DHCP IP Address pool 3-1

DHCP server

about 3-1

address pool 3-4

configuring secondary IP addresses 3-11

enable 3-4

lease time 3-5

Diffie-Hellman Group

IKE Policy 5-16

Disable DHCP Server 3-1

DNS

server IP address 3-4

DNS proxy

enable 3-5

Disable DNS Proxy4-20

DMZ WAN Rule

example of4-14

DNS proxy

disable4-20

DNS

ISP server addresses 2-11

Domain Name Servers. See DNS.

Dynamic DNS

configuration of 2-13

Dynamic DNS Configuration screen 2-13, 2-14

Dynamic DNS. See DDNS

DynDNS.org 2-13

Domain Name Blocking4-22

Domain Name

router 3-4

E

e-mail logs

enabling notification4-33

Edge Device 5-19

XAUTH, with ModeConfig 5-25

Edit Group Names 3-9

Enable DHCP server 3-1

Enable DNS Proxy 3-5

Enable LDAP Information 3-5

Ending IP Address

DHCP Address Pool 3-4

Event Logs

emailing of 4-33

Extended Authentication. See XAUTH.

F

- factory default login 1-8
- factory default settings
 - revert to 7-15
- firmware
 - downloading 7-17
 - upgrade 7-17
- Flash memory, for firmware upgrade 1-2
- fragmented IP packets 7-6
- Firewall Logs
 - emailing of 4-33
- Firewall Logs & E-mail screen 4-33
- Firewall Protection
 - Content Filtering, about 4-1
- firewall protection 4-1
- firewall
 - connecting to the Internet 2-1
- fixed IP address 2-6
- fixed IP address 3-8

G

- Group Names
 - editing 3-9
- groups, managing 3-5

H

- hosts, managing 3-5
- Hosting A Local Public Web Server
 - example of 4-13

I

- Iego.net 2-12
- IGP 3-13
- IKE Policy
 - about 5-14
 - management of 5-14
 - ModeConfig, configuring with 5-24
 - XAUTH, adding to 5-18
- installation 1-4

- IPSec Host 5-19
- IPsec Host
 - XAUTH, with ModeConfig 5-25
- IPsec host 18
- Inbound Rules
 - default definition 4-2
 - field descriptions 4-6
 - order of precedence 4-8
 - Port Forwarding 4-3, 4-5
 - rules for use 4-5
- inbound rules 4-5
 - example 4-14
- Inbound Service Rule
 - modifying 4-11
- Inbound Services
 - field descriptions 4-6
- increasing traffic 7-5
 - Port Forwarding 7-5
 - Port Triggering 7-7
 - VPN Tunnels 7-7

Interior Gateway Protocol. See IGP.

Installation, instructions for 2-1

- Internet
 - configuring the connection manually 2-7
 - connecting to 2-1

Internet connection

- manual configuration 2-7

- IP addresses
 - auto-generated 8-3
 - DHCP address pool 3-1
 - how to assign 3-1
 - multi home LAN 3-5
 - reserved 3-9
 - router default 3-4

IP Subnet Mask

- router default 3-4

ISP connection

- troubleshooting 8-4

K

- keepalive, VPN 5-27
- Keep Connected
 - Idle Timeout 2-9
- Keyword Blocking4-22
 - applying4-24
- Known PCs and Devices
 - list of 3-7

L

- LAN
 - configuration 3-1
 - using LAN IP setup options 3-2
- LAN Groups Database
 - about 3-5
 - advantages of 3-5
 - fields 3-7
- LAN side
 - bandwidth capacity 7-1
 - Load balancing mode 7-2
- LAN Setup screen 3-3
- LAN Security Checks4-20
- LAN WAN Inbound Rule
 - example of4-13,4-16
- LAN WAN Inbound Services Rules
 - about4-10
 - add4-10
- LAN WAN Outbound Rule
 - example of4-16
- LAN WAN Rule
 - example of4-14
- LAN WAN Rules
 - default outbound 4-9
- lease time 3-5
- LEDs
 - explanation of 1-5, 1-6
- LEDs
 - troubleshooting 8-2
- Load Balancing
 - bandwidth capacity 7-2
- Load Balancing

definition of 2-11

- logging in
 - default login 2-2
- login policy
 - restrict by IP address 6-5
 - restrict by port 6-4

M

- MAC addresses
 - blocked, adding4-25
 - MAC address
 - in LAN groups database 3-8
 - MAC address 8-7
 - spoofing 8-5
 - MAC address
 - authentication by ISP 2-16
 - configuring 2-6
 - main menu 2-4
 - metric
 - in static routes 3-12
 - ModeConfig 5-21
 - about 5-22
 - assigning remote addresses, example 5-21
 - Client Configuration 5-25
 - IKE Policies menu, configuring 5-22
 - menu, configuring 5-22
 - testing Client 5-26
 - MTU Size 2-15
 - multi home LAN IPs 3-5
 - about 3-10
 - multi-NAT4-15
- ## N
- NAS
 - Identifier 5-20
 - NAT
 - firewall, use with4-2
 - multi-NAT4-15
 - one-to-one mapping example4-14
 - NAT
 - configuring 2-11
 - one-to-one mapping 2-11

NetBIOS bridging over VPN [5-29](#)

Network Access Server. See NAS.

Network Address Translation. See NAT.
Network Database table [3-7](#)

Network Database Group Names screen [3-9](#)

Network Time Protocol. See NTP.

newsgroup [4-22](#)

NTP [7-18](#)

NTP servers

 custom [7-19](#)

 default [7-19](#)

 setting [7-18](#)

NTP

 troubleshooting [8-8](#)

O

option arrow [2-4](#)

Outbound Rules

 default definition [4-2](#)

 field descriptions [4-3](#)

 order of precedence [4-8](#)

 service blocking [4-3](#)

outbound rules [4-3](#)

Outbound Service Rule

 adding [4-9](#)

 modifying [4-11](#)

Outbound Services

 field descriptions [4-3](#)

P

package contents [1-5](#)

packet capture [8-10](#)

passwords and login timeout
 changing [6-6](#)

passwords and login timeout
 changing [7-8](#)

passwords, restoring [8-7](#)

performance management [7-1](#)

Ping

 troubleshooting TCP/IP [8-5](#)

ping [8-10](#)

Ping On Internet Ports [4-20](#)

port filtering

 service blocking [4-3](#)

Port Forwarding

 Inbound Rules [4-3](#), [4-5](#)

 rules, about [4-5](#)

port numbers [4-16](#)

ports

 explanation of WAN and LAN [1-6](#)

Port Triggering

 about [4-27](#)

 adding a rule [4-28](#)

 rules of use [4-27](#)

Port Triggering screen [4-28](#)

Port Forwarding

 increasing traffic [7-5](#)

Port Speed [2-16](#)

Port Triggering

 increasing traffic [7-7](#)

PPPoE [2-6](#), [2-8](#)

 Internet connection [2-9](#)

PPTP [2-6](#), [2-8](#)

PPP over Ethernet. See PPPoE.

PPPoE [1-3](#)

protocols

 Routing Information Protocol [1-3](#)

protocol numbers

 assigned [4-16](#)

Q

QoS

 about [4-18](#)

 priority definitions [4-19](#)

 using in firewall rules [4-3](#)

QoS

 shifting traffic mix [7-7](#)

Quality of Service. See QoS.

R

RADIUS Server

configuring 5-19

RADIUS-CHAP 5-17, 5-19

AUTH, using with 5-18

RADIUS-PAP 5-17

XAUTH, using with 5-18

RADIUS

WiKID 6-8

reducing traffic 7-2

Block Sites 7-4

service blocking 7-2

Source MAC Filtering 7-5

remote management 6-7

remote management 7-10

access 7-10

configuration 7-10

remote users

assigning addresses 5-21

ModeConfig 5-21

restore saved settings 7-15

RIP

feature 1-3

upgrade software 7-17

Router Upgrade

about 7-17

Routing Information Protocol. See RIP.router

running tracert 7-12

reserved IP address

configuring 3-9

in LAN groups database 3-8

restrictions 3-8

RIP

about 3-13

advertising static routes 3-12

configuring parameters 3-13

versions of 3-14

RIP Configuration menu 3-13

Routing Information Protocol. See RIP.

routing menu 3-11

RFC4-13494-19

RFC1700

protocol numbers4-16

router administration

tips on4-33

Router Status 2-12

Router's MAC Address 2-16

rules

blocking traffic4-2

inbound 4-5

inbound example4-14

outbound4-3

service blocking4-3

services-based4-3

S

save binding button 3-8

schedule

blocking traffic4-29

Schedule4-1 screen4-30

secondary IP addresses

DHCP, use with 3-11

Secondary LAN IPs

see Multi Home LAN IPs 3-10

security 1-1

self certificate request 6-11

service4-17

Service Based Rules4-3

service blocking4-3

Outbound Rules4-3

port filtering4-3

service numbers

common protocols4-16

Services4-17

Services menu4-17

Session Limits4-31

service blocking

reducing traffic 7-2

Service

Add Protocol Binding 2-12

Settings Backup & Upgrade screen 7-15

Settings Backup and Firmware Upgrade [7-16](#)
Simple Network Management Protocol. See SNMP.
Setting Up One-to-One NAT Mapping
 example of [4-14](#)
sniffer [8-3](#)
SNMP
 about [7-13](#)
 configuring [7-13](#)
 global access [7-14](#)
 host only access [7-14](#)
 subnet access [7-14](#)
SNMP screen [7-13](#)
Source MAC Filtering
 reducing traffic [7-5](#)
Source MAC Filter screen [4-25](#)
Source MAC Filtering
 enabling [4-24](#)
Specifying an Exposed Host
 example of [4-16](#)
spoof MAC address [8-5](#)
Starting IP Address
 DHCP Address Pool [3-4](#)
stateful packet inspection. See SPI.
Stateful Packet Inspection
 firewall, use with [4-2](#)
Static [3-11](#)
static IP address
 configuring [2-10](#)
 detecting [2-6](#)
static routes
 about [3-11](#)
 configuring [3-11](#)
 metric [3-12](#)
stealth mode [4-20](#)
stealth mode [7-6](#)
submenu [2-4](#)
SYN flood [7-6](#)
SYN flood [4-20](#)

T

tab, menu [2-4](#)

TCP/IP
 network, troubleshooting [8-5](#)
Time
 troubleshooting [8-8](#)
time
 daylight savings, troubleshooting [8-8](#)
TCP flood
 special rule [7-6](#)
Time
 setting [7-18](#)
Time Zone
 setting of [7-18](#)
Time Zone screen [7-18](#)
timeout, administrator login [7-9](#)
ToS. See QoS
 use with DDNS [7-12](#)
traffic
 increasing [7-5](#)
 reducing [7-2](#)
traffic management [7-8](#)
traceroute [8-10](#)
troubleshooting [8-1](#)
 browsers [8-3](#)
 configuration settings, using sniffer [8-3](#)
 defaults [8-3](#)
 ISP connection [8-4](#)
 NTP [8-8](#)
 testing your setup [8-6](#)
 Web configuration [8-3](#)
Trusted Certificates [6-10](#)
two-factor authentication
 WiKID [6-8](#)
TZO.com [2-12](#)

U

UDP flood special rule [7-6](#)
UDP flood [4-20](#)
User Database [5-19](#)

V

VPN firewall

- connecting 2-1
- VPN Client
 - configuring 5-5
- VPN Policies screen 5-4, 5-7
- VPN Policy
 - Auto 5-16
 - Manual 5-16
- VPN tunnels
 - about 5-1
- VPN Wizard
 - Gateway tunnel 5-1
 - VPN Client, configuring 5-5
- VPNC 5-1
- VPN passthrough 4-21
- VPN passthrough 7-6
- VPN tunnels increasing traffic 7-7

X

- XAUTH
 - IPsec host 5-18
 - types of 5-17

W

- WAN
 - configuring Advanced options 2-15
 - configuring WAN Mode 2-11
- WAN Security Check
 - about 4-20
- WAN sidebandwidth capacity 7-2
- WAN ports
 - status of 2-12
- WAN Status 2-7
- WAN1 Advanced Options 2-15
- WAN1 ISP Settings
 - manual setup 2-7
- WinPoET 2-9
- Web Components 4-21
 - blocking 4-24
 - filtering, about 4-21
- Web configuration
 - troubleshooting 8-3
- WiKID 6-8
- WINS server 3-4