ProSafe 802.11g Wireless VPN Firewall FVG318 Reference Manual

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10318-01
September 2007

Trademarks

NETGEAR and the NETGEAR logo are registered trademarks and ProSafe is a trademark of NETGEAR, Inc. Microsoft, Windows, and Windows NT 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.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das ProSafe 802.11g Wireless 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.

Certificate of the Manufacturer/Importer

It is hereby certified that the ProSafe 802.11g Wireless 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.

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.

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

NOTE: This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

Europe – EU Declaration of Conformity CE (!)

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN300 328, EN301 489-17, EN60950

Europe – Declaration of Conformity in Languages of the European Community

Cesky [Czech]	*NETGEAR* Inc. tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES..
Dansk [Danish]	Undertegnede *NETGEAR Inc.* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *NETGEAR Inc.*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *NETGEAR Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *NETGEAR Inc.*, declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente *NETGEAR Inc.* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *NETGEAR Inc.* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *NETGEAR Inc.* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente *NETGEAR Inc.* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *NETGEAR Inc.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, *NETGEAR Inc.*, jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.

Português [Portuguese]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*NETGEAR Inc.* týmto vyhlasuje, _e Radiolan spĺňa základné po_iadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *NETGEAR Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Icelandic]	Hér með lýsir *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	*NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

FCC Requirements for Operation in the United States

FCC Information to User

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

FCC Guidelines for Human Exposure

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

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

FCC Declaration Of Conformity

We NETGEAR, Inc., 4500 Great America Parkway, Santa Clara, CA 95054, declare under our sole responsibility that the model FVG318 ProSafe 802.11g Wireless VPN Firewall complies with Part 15 of FCC Rules. Operation is subject to the following two conditions:

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

FCC Radio Frequency Interference Warnings & Instructions

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

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

ProSafe 802.11g Wireless VPN Firewall

Tested to Comply
with FCC Standards
FOR HOME OR OFFICE USE

Modifications made to the product, unless expressly approved by NETGEAR, Inc., could void the user's right to operate the equipment.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the second 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.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (ProSafe 802.11g Wireless VPN Firewall) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Product and Publication Details

Model Number:	FVG318
Publication Date:	September 2007
Product Family:	Wireless Router
Product Name:	ProSafe 802.11g Wireless VPN Firewall
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10318-01
Publication Version Number:	1.0

Contents

About This Manual

Chapter 1
Introduction

Chapter 2
Connecting the Firewall to the Internet

Chapter 3
Configuring Wireless Connectivity

Chapter 4
Firewall Protection and Content Filtering

Chapter 5
Basic Virtual Private Networking

Chapter 6
Advanced Virtual Private Networking

Chapter 7
Maintenance

Chapter 8
Advanced Configuration

About This Manual

The *NETGEAR® ProSafe™ 802.11g Wireless VPN Firewall FVG318 Reference Manual* describes how to install, configure and troubleshoot the ProSafe 802.11g Wireless 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:

Italic	Emphasis, books, CDs, file and server names, extensions
Bold	User input, IP addresses, GUI screen text
`Fixed`	Command prompt, CLI text, code
italic	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 802.11g Wireless VPN Firewall
Manual Publication Date	September 2007

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/FVG318.asp*.

How to Use This Manual

The HTML version of this manual includes the following:

- Buttons, > and <, for browsing forwards or backwards through the manual one page at a time
- A button that displays the table of contents and an button. Double-click on a link in the table of contents or index to navigate directly to where the topic is described in the manual.
- A button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

How to Print this Manual

To print this manual, you can choose one of the following options, according to your needs.

- **Printing a Page from HTML**. Each page in the HTML version of the manual is dedicated to a major topic. Select File > Print from the browser menu to print the page contents.

- **Printing from PDF**. 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*.
  - **Printing a PDF Chapter.** Use the *PDF of This Chapter* link at the top left of any page.
    - Click the *PDF of This Chapter* link at the top left of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.
    - Click the print icon in the upper left of your browser window.
  - **Printing a PDF version of the Complete Manual**. Use the *Complete PDF Manual* link at the top left of any page.
    - Click the *Complete PDF Manual* link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.
    - Click the print icon in the upper left of your browser window.

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
202-10318-01	1.0	August 2007	Product update: New firmware and new user Interface

Chapter 1
Introduction

This chapter describes the features of the NETGEAR® ProSafe 802.11g Wireless VPN Firewall, Model FVG318.

Key Features of the VPN Firewall Router

The ProSafe 802.11g Wireless VPN Firewall with eight-port switch connects your local area network (LAN) to the Internet through an external access device such as a cable modem or DSL modem and provides 802.11b/g wireless LAN connectivity.

The FVG318 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 FVG318 uses stateful packet inspection for Denial of Service attack (DoS) protection and intrusion detection. The FVG318 allows Internet access for up to 253 users. 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.

The VPN firewall provides the following features:

- 802.11g and 802.11b standards-based wireless networking.
- Wireless Multimedia (WMM) support.
- Easy, Web-based setup for installation and management.
- Front panel LEDs for easy monitoring of status and activity.
- Content filtering and site blocking security.
- Built-in eight-port 10/100 Mbps switch.
- Ethernet connection to a WAN device, such as a cable modem or DSL modem.
- Extensive protocol support.
- Flash memory for firmware upgrade.

802.11g and 802.11b Wireless Networking

The VPN firewall includes an 802.11g-compliant wireless access point. The access point provides:

- 802.11b standards-based wireless networking at up to 11 Mbps.
- 802.11g wireless networking at up to 54 Mbps, which conforms to the 802.11g standard.
- WPA and WPA2 enterprise class strong security with RADIUS and certificate authentication as well as dynamic encryption key generation.
- WPA-PSK and WPA2-PSK pre-shared key authentication without the overhead of RADIUS servers but with all of the strong security of WPA and WPA2.
- 64-bit and 128-bit WEP encryption security.
- WEP keys can be generated manually or by passphrase.
- Wireless access can be restricted by MAC Address.
- Wireless network name broadcast can be turned off so that only devices that have the network name (SSID) can connect.

Wireless Multimedia (WMM) Support

WMM is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the kind of data. Time-dependent information such as video or audio will have a higher priority than normal traffic. For WMM to function correctly, wireless clients must also support WMM.

A Powerful, True Firewall with Content Filtering

Unlike simple Internet sharing NAT firewalls, the FVG318 is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- DoS protection.

  Automatically detects and thwarts DoS attacks such as Ping of Death, SYN Flood, LAND Attack, and IP Spoofing.
- 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.
- Logs security incidents.

The FVG318 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 e-mail address or email pager whenever a significant event occurs.

- With its content filtering feature, the FVG318 prevents objectionable content from reaching your PCs. The firewall allows you to control access to Internet content by screening for keywords within Web addresses. You can configure the firewall to log and report attempts to access objectionable Internet sites.

Security

The VPN firewall is equipped with several features designed to maintain security, as described in this section.

- **PCs Hidden by NAT.** NAT opens a temporary path to the Internet for requests originating from the local network. Requests originating from outside the LAN are discarded, preventing users outside the LAN from finding and directly accessing the PCs on the LAN.
- **Port Forwarding with NAT.** Although NAT prevents Internet locations from directly accessing the PCs on the LAN, the firewall allows you to direct incoming traffic to specific PCs based on the service port number of the incoming request, or to one designated DNS host computer. You can specify forwarding of single ports or ranges of ports.

Autosensing Ethernet Connections with Auto Uplink

With its internal eight-port 10/100 switch, the FVG318 can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. Both the LAN and WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

The firewall incorporates Auto Uplink™ technology. Each Ethernet port automatically senses whether the Ethernet cable plugged into the port should have a normal connection such as to a PC or an uplink connection such as to a switch or hub. That port then configures itself to the correct configuration. This feature also 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 Appendix B, “Related Documents.”

- **IP Address Sharing by NAT.** The VPN firewall allows several 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.
- **Point-to-Point Protocol 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 Entersys or WinPOET on your PC.

Easy Installation and Management

You can install, configure, and operate the ProSafe 802.11g Wireless VPN Firewall within minutes after connecting it to the network. The following features simplify installation and management tasks:

- **Browser-based management.** Browser-based configuration allows you to easily configure 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.
- **Smart Wizard.** The VPN firewall automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- **Diagnostic functions.** The firewall incorporates built-in diagnostic functions such as Ping, 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, and you can choose a nonstandard port number.
- **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.

Note: The FVS318v3 firmware is not backward compatible with earlier versions of the FVS318 firewall.

Package Contents

The product package should contain the following items:

- ProSafe 802.11g Wireless VPN Firewall.
- AC power adapter.
- Category 5 (Cat 5) Ethernet cable.
- Installation Guide.
- *Resource CD*, including:
  - This guide.
  - Application Notes and other helpful information.
- Registration and Warranty 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.

The FVG318 Front Panel

The front panel of the VPN firewall contains the status LEDs described below.

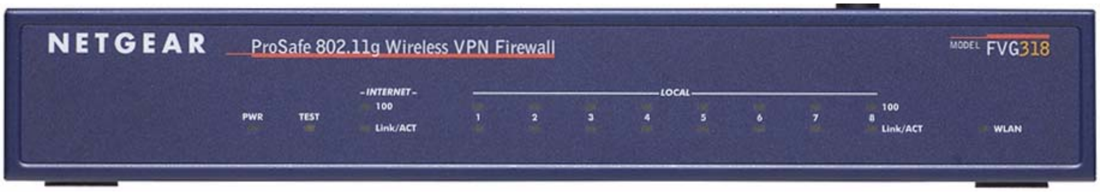


Figure 1-1

You can use some of the LEDs to verify connections. Viewed from left to right, Table 1-1 describes the LEDs on the front panel of the firewall. These LEDs are green when lit.

Table 1-1. LED Descriptions

LED Label		Activity	Description
PWR		On	Power is supplied to the firewall.
TEST		On Off	The system is initializing. The system is ready and running.
INTERNET			
	100 (100 Mbps)	On Off	The Internet (WAN) port is operating at 100 Mbps. The Internet (WAN) port is operating at 10 Mbps.
	LINK/ACT (Link/Activity)	On Blinking	The Internet port has detected a link with an attached device. Data is being transmitted or received by the Internet port.
LOCAL			
	100 (100 Mbps)	On Off	The Local port is operating at 100 Mbps. The Local port is operating at 10 Mbps.
	LINK/ACT (Link/Activity)	On Blinking	The Local port has detected a link with an attached device. Data is being transmitted or received by the Local port.
WLAN		On Off	The wireless interface is on. The wireless interface is off.

The FVG318 Rear Panel

The rear panel of the VPN firewall contains the port connections listed below.

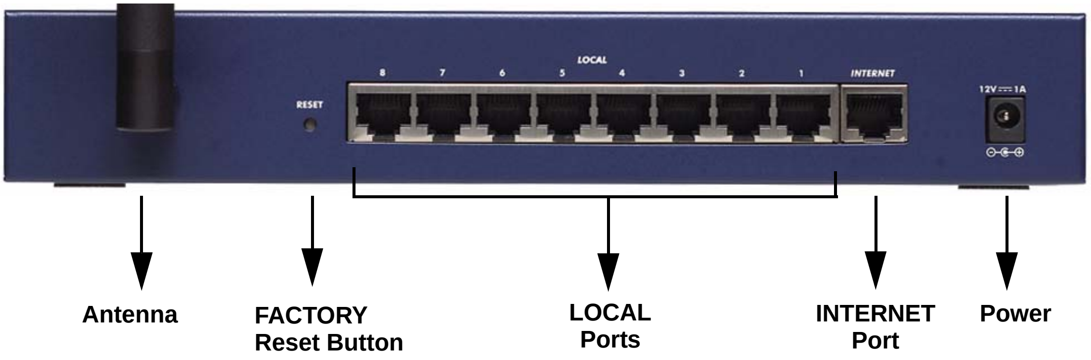


Figure 1-2

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

- Detachable wireless antenna
- Factory default reset push button
- Eight Ethernet LAN ports
- Internet Ethernet WAN port for connecting the firewall to a cable or DSL modem
- DC power input

Chapter 2
Connecting the Firewall to the Internet

This chapter describes how to set up the firewall on your LAN, connect to the Internet, perform basic configuration of your ProSafe 802.11g Wireless VPN Firewall using the Setup Wizard, or how to manually configure your Internet connection.

Follow these instructions to set up your firewall.

Installing Your FVG318

- **For Cable Modem Service**: When you set up the VPN firewall router, be sure to use the computer you first registered with your cable modem service provider.
- **For DSL Service:** You may need information such as the DSL login name and password in order to complete the VPN firewall router setup.

To connect the FVG318:

1. Connect the VPN firewall router to your computer and modem

   a. Turn off *and* unplug your cable or DSL modem.

   b. Turn off your computer

   c. At the computer end only, disconnect the Ethernet cable (point **A** in the illustration) that connects your computer to the cable or DSL modem.

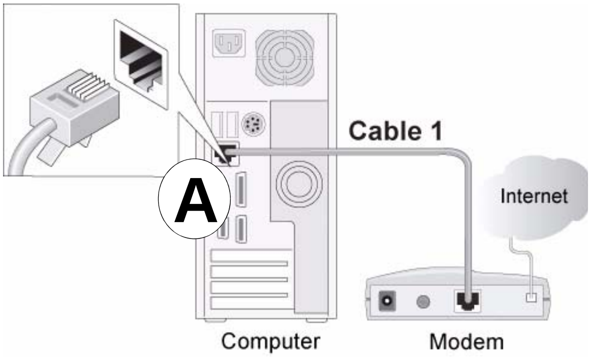


Figure 2-1

d. Securely insert the Ethernet cable from your modem into the FVG318 Internet port (point **B** in the illustration).

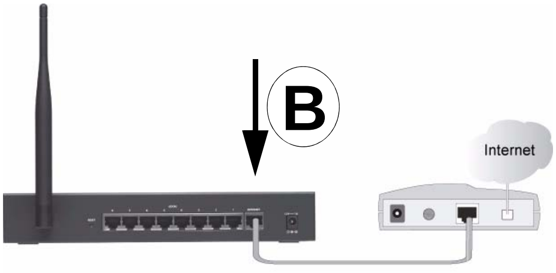


Figure 2-2

e. Securely insert one end of the NETGEAR cable that came with your FVG318 into a Local port on the router such as port 4 (point **C** in the illustration), and the other end into the Ethernet port of your computer (point **D** in the illustration).

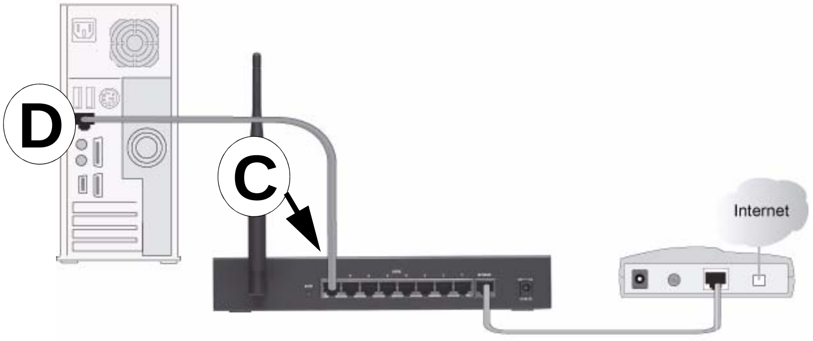


Figure 2-3

2. Restart your network in the correct sequence

⚠ **Warning:** Failure to restart your network in the correct sequence could prevent you from connecting to the Internet.

a. First, plug in and turn on the cable or DSL modem.Wait about 2 minutes.

b. Now, plug in the power cord to your FVG318 and wait about 30 seconds.

c. Last, turn on your computer.

➡ **Note:** For DSL customers, if ISP-provided software logs you in to the Internet, *do not* run that software. You may need to go to the Internet Explorer® Tools menu, Internet Options, Connections tab page where you can select the “Never dial a connection” radio button and click Apply.

d. Check the status lights and verify the following:

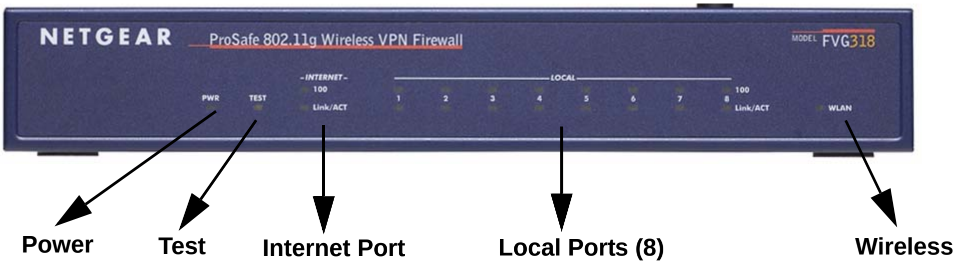


Figure 2-4

- **Power:** The power light should be lit. If after 2 minutes the power light turns solid amber, see the Troubleshooting Tips in this guide.
- **Test**: The test light blinks when the FVG318 is first turned on. If after 2 minutes it is still on, see the Troubleshooting Tips in this guide.
- **Internet**: The Internet light on the FVG318 should be lit. If not, make sure the Ethernet cable is securely attached to the VPN firewall router Internet port and the powered on modem.
- **Wireless***:* The WLAN light should be lit. If the Wireless light is not lit, see the Troubleshooting Tips in this guide.
- **LOCAL***:* A LOCAL light should be lit.

Configuring the FVG318 for Internet Access with Auto Detect

To connect to the firewall, your computer needs to be configured to obtain an IP address automatically via DHCP, which is usually the case for most computers. However, if you need instructions on how to configure your TCP/IP settings to obtain an IP address automatically, see “Internet Networking and TCP/IP Processing” at Appendix B, “Related Documents.

Before you begin, be sure you have the configuration parameters from your ISP handy.

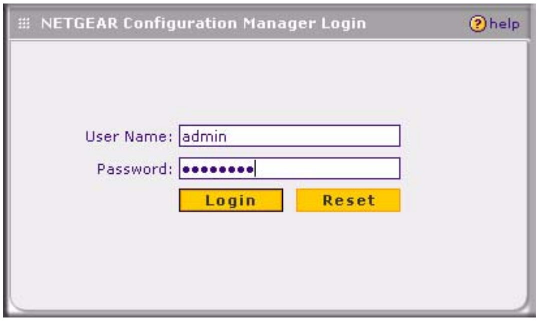
To log in the router:

1. 0pen a browser such as Internet Explorer, Netscape Navigator or Firefox and enter the default IP address of the router in the browser address field: **http://192.168.0.1**.

http://192.168.0.1

Figure 2-5

2. When prompted, enter **admin** for the firewall User Name and **password** for the firewall Password. Both fields are case-sensitive. (For security reasons, the firewall has its own User Name and Password.)

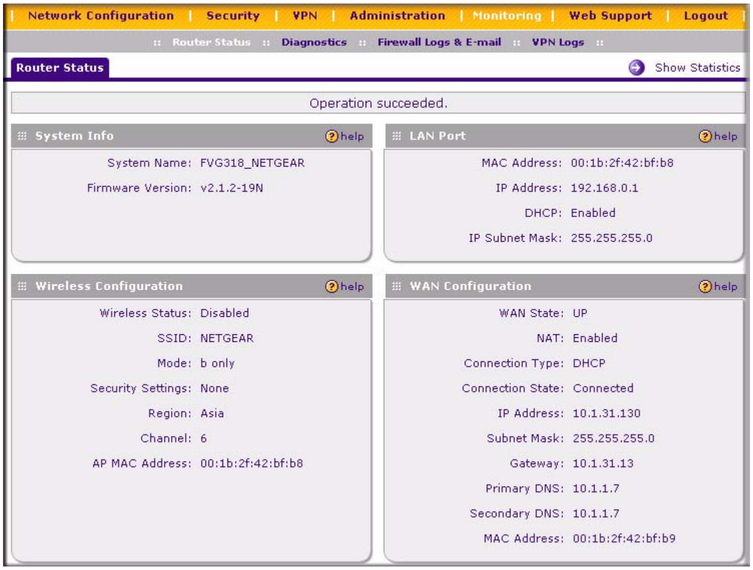


User Name: admin

Password: ●●●●●●●●

Figure 2-6

3. Click **Login.** You will be connected to the firewall Router Status screen which will give you status of your router configuration and current firmware version.


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
:: Router Status :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Router Status
Show Statistics
help
help
help
help

Operation succeeded.

System Info

System Name: FVG318_NETGEAR
Firmware Version: v2.1.2-19N

LAN Port

MAC Address: 00:1b:2f:42:bf:b8
IP Address: 192.168.0.1
DHCP: Enabled
IP Subnet Mask: 255.255.255.0

Wireless Configuration

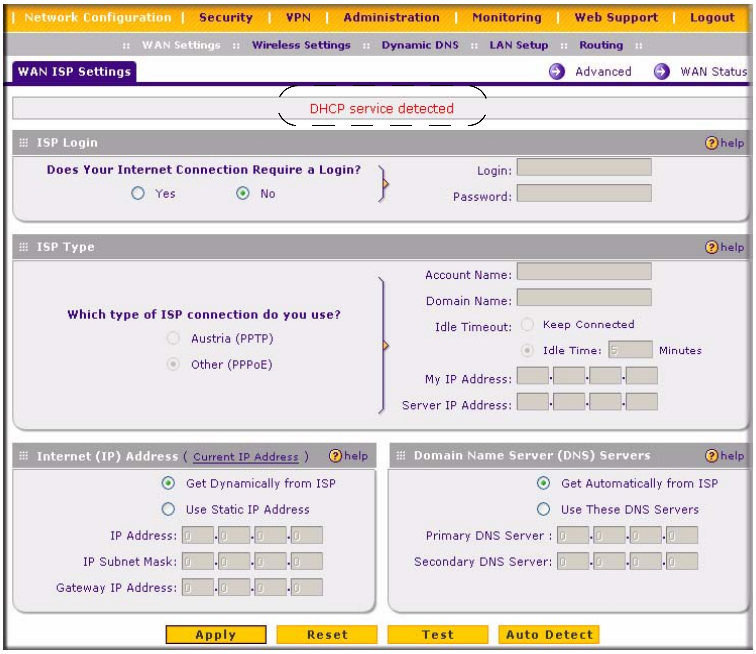
Wireless Status: Disabled
SSID: NETGEAR
Mode: b only
Security Settings: None
Region: Asia
Channel: 6
AP MAC Address: 00:1b:2f:42:bf:b8

WAN Configuration

WAN State: UP
NAT: Enabled
Connection Type: DHCP
Connection State: Connected
IP Address: 10.1.31.130
Subnet Mask: 255.255.255.0
Gateway: 10.1.31.13
Primary DNS: 10.1.1.7
Secondary DNS: 10.1.1.7
MAC Address: 00:1b:2f:42:bf:b9

Figure 2-7

4. Select Network Configuration. The WAN ISP Settings screen will display. Click **Auto Detect** at the bottom of the WAN ISP Settings screen. The router will automatically attempt to detect your connection type. A message will display indicating if the service connection was detected.


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
WAN Settings :: Wireless Settings :: Dynamic DNS :: LAN Setup :: Routing
WAN ISP Settings
Advanced
WAN Status
help
Apply
Reset
Test
Auto Detect

DHCP service detected

ISP Login

Does Your Internet Connection Require a Login? ○ Yes ● No

Login:

Password:

ISP Type

Which type of ISP connection do you use?

○ Austria (PPTP)

● Other (PPPoE)

Account Name:

Domain Name:

Idle Timeout: ○ Keep Connected

● Idle Time: 5 Minutes

My IP Address: . . .

Server IP Address: . . .

Internet (IP) Address (Current IP Address)

● Get Dynamically from ISP

○ Use Static IP Address

IP Address: 0.0.0.0

IP Subnet Mask: 0.0.0.0

Gateway IP Address: 0.0.0.0

Domain Name Server (DNS) Servers

● Get Automatically from ISP

○ Use These DNS Servers

Primary DNS Server : 0.0.0.0

Secondary DNS Server: 0.0.0.0

Figure 2-8

If you know your ISP connection type or if want to bypass the auto configuration, you can manually configure the router settings on the WAN ISP screen. See the "Manually Configuring your Internet Connection" on page 2-7 to connect your router manually.

5. Click **Test** to verify that the Internet connection is active.

➡	**Note:** You might want to enable remote management at this time so that you can log in remotely in the future to manage the gateway. See "Enabling Remote Management Access" on page 8-8 for more information. Remote management enable is cleared with a factory default reset.

> **Note:** When you enable remote management, we strongly advise that you change your password. See "Changing the Administrator Password" on page 7-6 for the procedure on how to do this.

Manually Configuring your Internet Connection

Unless your ISP assigns your configuration automatically via DHCP, you will need the configuration parameters from your ISP. For example, if your router detected a PPPoE or PPPoA service, you must provide a Login sequence in order to obtain an Internet connection from your ISP. If your ISP requires a Static IP address, then you must provide the fixed addresses for Static IP. The types of data you will need are highlighted in Table 2-1 by connection method, and explained in more detail below.

The information required by each of the connection types is described in the following table.

Table 2-1. Internet Service Connections

Connection Method	Data Required
PPPoE	Login (Username, Password).
PPPoA	Login (Username, Password).
DHCP (Dynamic IP)	No data is required.
Static (Fixed) IP	Internet IP address, Subnet Mask and Gateway IP Address supplied by your ISP; and the Router's DNS Address (also supplied by your ISP).
IPoA	Internet IP Address and Subnet Mask; Gateway IP Address

To configure your Internet connection:

1. Enter your ISP Login information. Select the **Does Your Internet Connection require a Login?** option based on the type of account your have with your ISP. If you need to enter login information every time you connect to the Internet, select **Yes**. Otherwise, select **No**.

   If your connection is PPTP or PPPoE, then you need to login. Choose Yes and enter:

   – **Login.** This is often the name that you use in your e-mail address (for example, if your main mail account is jdoe@aol.com, enter jdoe).

   > **Note:** Some ISPs (for example, Earthlink) require that you use your full e-mail address when you log in.

  - **Password**. Enter the password you use to log in to your ISP.

- Enter your **ISP Type** information:
  - **Austria (PPTP)**: If your ISP is Austria Telecom or any other ISP that uses PPTP to log in, fill in the following fields:
    - **Account Name** (also known as Host Name or System Name): Valid account name for the PPTP connection. This is usually your email "ID" assigned by your ISP, the name before the "@" symbol in your email address. Some ISPs require that you enter your full email address here.
    - **Domain Name:** Domain name or workgroup name assigned by your ISP, or your ISPs domain name (optional).
    - **Idle Timeout:** Select Keep Connected, to Keep the Connection Always On. To logout after the connection is idle for a period of time, select 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 a connection with the ISP server.
    - **Server IP Address**: IP address of the PPTP server.
  - **Other (PPPoE):** If you have installed log in software such as WinPoET or Enternet, then your connection type is PPPoE. Select this option and configure the following fields:
    - **Account Name**: Valid account name for the PPPoE connection
    - **Domain Name**: Name of your ISPs domain or your domain name if your ISP has assigned one (optional).
    - **Idle Timeout**: Select Keep Connected, to keep the connection always on. To logout after the connection is idle for a period of time, select Idle Time and enter the number of minutes to wait before disconnecting, in the Timeout field.

2. Enter your **Internet (IP) Address**.

  - Select the **Get dynamically from ISP** radio box if you have not been assigned any static IP address. The ISP will automatically assign an IP address to the router using DHCP network protocol.
  - If your ISP has assigned a fixed (static) IP address, select **Use Static IP Address** and fill in the following fields:
    - **IP Address**: Static IP address assigned to you. This will identify the router to your ISP.

- **IP Subnet Mask**: This is usually provided by the ISP or your network administrator.
- **Gateway IP Address**: IP address of your ISP's gateway. This is usually provided by the ISP or your network administrator.

3. Select your **Domain Name Servers** (DNS). Domain name servers (DNS) convert Internet names such as www.google.com, www.netgear.com, etc. to Internet addresses called IP addresses.
   – Select the **Get Automatically from ISP** radio box if you have not been assigned a static DNS IP address.
   – If the **Use these DNS Servers** radio box is selected, enter valid DNS server IP addresses in the Primary DNS Server and Secondary DNS Server fields.
4. Click **Apply** to save your settings. Click **Test** to verify that the connection is active.

> ➡ **Note:** At this point in the configuration process, you should now be connected to the Internet.

Configuring Dynamic DNS (If Needed)

> ➡ **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.

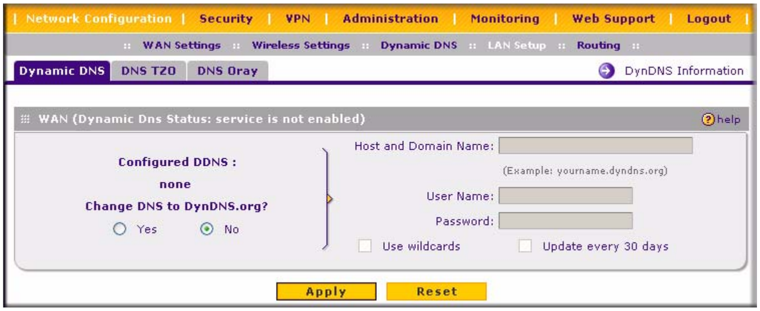
If your network has a permanently assigned (static or fixed) IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will not know in advance what your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

For rollover mode, you will need a fully qualified domain name (FQDN) to implement features such as exposed hosts and virtual private networks regardless of whether you have a fixed or dynamic IP address.

The gateway contains a client that can connect to a dynamic DNS service provider. To use this feature, you must select a service provider and obtain an account with them. After you have configured your account information in the gateway, whenever your ISP-assigned IP address changes, your gateway will automatically contact your dynamic DNS service provider, log in to your account, and register your new IP address.

To configure Dynamic DNS:

1. Select **Network Configuration** > **Dynamic DNS**. The **Dynamic DNS** screen will display with the default Dynamic DNS selected as None.



WAN (Dynamic Dns Status: service is not enabled)

Configured DDNS :
none

Change DNS to DynDNS.org?
○ Yes ● No

Host and Domain Name:
(Example: yourname.dyndns.org)
User Name:
Password:
□ Use wildcards □ Update every 30 days

Figure 2-9

2. Each DNS service provider—Dynamic DNS, DNS TZO or DNS Oray—requires its own parameters (Figure 2-9). Select the tab for the DNS service provider you want to use and then select the Yes radio box. Click **Apply.**

3. Access the Web site of the Dynamic DNS service provider you have chosen and register for an account (for example, for dyndns.org, go to *http://www.dyndns.org*).

4. Complete entering the Dynamic DNS screen for the service you have chosen:

   a. Select the Use a dynamic DNS service check box of the name of your dynamic DNS Service Provider.

   b. Enter the entire FQDN that your dynamic DNS service provider gave you, (for example, **myName.dyndns.org**).

   c. Enter the User Name and Password (or key) for logging into your dynamic DNS account.

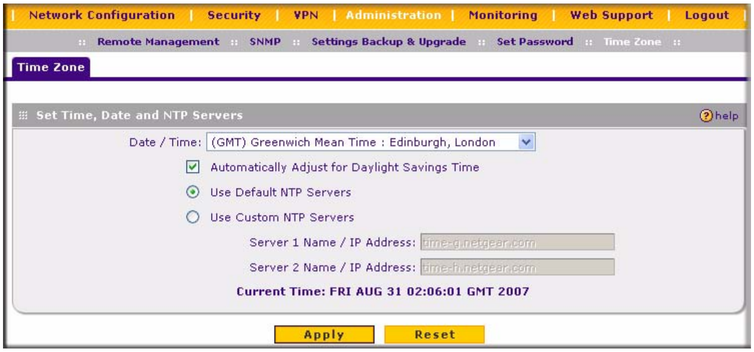
   d. If your dynamic DNS provider allows the use of wild cards in resolving your URL, you may select the Use wild cards check box to activate this feature.

   For example, the wildcard feature will cause `*.yourhost.dyndns.org` to be aliased to the same IP address as `yourhost.dyndns.org`

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

Configuring Your Time Zone

The VPN firewall uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet. In order to localize the time for your log entries, you must specify your Time Zone.



Date / Time: (GMT) Greenwich Mean Time : Edinburgh, London

☑ Automatically Adjust for Daylight Savings Time

● Use Default NTP Servers

○ Use Custom NTP Servers

Server 1 Name / IP Address: time-g.netgear.com

Server 2 Name / IP Address: time-h.netgear.com

Current Time: FRI AUG 31 02:06:01 GMT 2007

Figure 2-10

To specify your time zone:

1. Select Administration > Time Zone from the menu. The Time Zone screen will display.
2. From the **Date/Time** pull-down menu, select your local time zone. This setting will be used for the blocking schedule and for time-stamping log entries.
3. **Automatically Adjust for Daylight Savings Time**. Check this box for enable daylight savings time.

Note: If your region uses Daylight Savings Time, you must manually select Adjust for Daylight Savings Time on the first day of Daylight Savings Time, and deselect it at the end. Enabling Daylight Savings Time will add one hour to the standard time.

4. Select an NTP Server.
   - The **Use Default NTP Servers** is selected by default. If this is enabled, then the RTC (Real-Time Clock) is updated regularly by contacting a NETGEAR NTP Server on the Internet.

- Select the **Use Custom NTP Servers** if you prefer to use a particular NTP server.
  - Enter the name or IP address of an NTP Server in the **Server 1 Name/IP Address** field.
  - If required, you can also enter the address of another 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, then they will be set to the default NETGEAR NTP servers (time-a.netgear.com, time-b.netgear.com, etc.).

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

Troubleshooting Tips

Here are some tips for correcting simple problems you may have.

Be sure to restart your network in the correct sequence.

Always follow this sequence: 1) Unplug and turn off the modem, FVG318, and computer; 2) plug in and turn on the modem, wait two minutes; 3) plug in the FVG318 and wait 30 seconds; 4) turn on the computer.

Make sure the Ethernet cables are securely plugged in.

- For each powered on computer connected to the VPN firewall router with a securely plugged in Ethernet cable, the corresponding VPN firewall router LAN port status light will be lit. The label on the bottom of the VPN firewall router identifies the number of each LAN port.
- The Internet port status light on the VPN firewall router will be lit if the Ethernet cable from the FVG318 to the modem is plugged in securely and the modem and VPN firewall router are turned on.

Make sure the computer & router wireless settings match exactly.

The Wireless Network Name (SSID) and security settings (WEP/WPA, MAC access control list) of the FVG318 and wireless computer must match exactly.

Make sure the network settings of the computer are correct.

- LAN and wirelessly connected computers *must* be configured to obtain an IP address automatically via DHCP.

- Some cable modem ISPs require you to use the MAC address of the computer registered on the account. If so, in the Router MAC Address section of the Basic Settings menu, select, “Use this Computer’s MAC Address.” The router will then capture and use the MAC address of the computer that you are now using. You must be using the computer that is registered with the ISP. Click **Apply** to save your settings. Restart the network in the correct sequence.

Check the router status lights to verify correct router operation.

- If the Power light does not turn solid green within 2 minutes after turning the router on, reset the router according to the instructions in the *Reference Manual* on the CD.
- If the Wireless light does not come on, verify that the wireless feature is turned on according to the instructions in the *Reference Manual* on the CD.

Tips for Accessing the VPN firewall

The table below describes how you access the VPN firewall router, depending on the state of the VPN firewall router.

Table 2-2. Accessing the firewall router

Firewall State	Access Options	Description
Factory Default **Note**: The VPN firewall router is supplied in the factory default state. Also, the factory default state is restored when you use the factory reset button. See “To backup and restore your configuration:” on page 7-5 for more information on this feature.	Automatic Access via the Smart Wizard Configuration Assistant	Any time a browser is opened on any computer connected to the VPN firewall router, the VPN firewall router will automatically connect to that browser and display the Configuration Assistant welcome page. There is no need to enter the VPN firewall router URL in the browser, or provide the login user name and password.
	Manually enter a URL to bypass the Smart Wizard Configuration Assistant	You can bypass the Smart Wizard Configuration Assistant feature by typing **http://192.168.0.1/basicsetting.htm** in the browser address bar and pressing **Enter**. You will not be prompted for a user name or password. This will enable you to manually configure the VPN firewall router even when it is in the factory default state. When manually configuring the firewall, you must complete the configuration by clicking **Apply** when you finish entering your settings. If you do not do so, a browser on any PC connected to the firewall will automatically display the firewall Configuration Assistant welcome page rather than the browser’s home page.

Table 2-2. Accessing the firewall router (continued)

Firewall State	Access Options	Description
Configuration Settings Have Been Applied	Enter the standard URL to access the VPN firewall router	Connect to the VPN firewall router by typing the default router IP address in the address field of your browser, then press **Enter**: **http://192.168.0.1** The VPN firewall router will prompt you to enter the user name of **admin** and the **password**. The default password is password.
	Enter the IP address of the VPN firewall router	Connect to the VPN firewall router by typing the IP address of the VPN firewall router in the address field of your browser, then press **Enter**. 192.168.0.1 is the default IP address of the VPN firewall router. The VPN firewall router will prompt you to enter the user name of **admin** and the **password**. The default password is password.

Chapter 3
Configuring Wireless Connectivity

This chapter describes how to configure the wireless features of your FVG318 VPN firewall.

Observing Performance, Placement, and Range Guidelines

In planning your wireless network, you should consider the level of security required. You should also select the physical placement of your FVG318 in order to maximize the network speed. For further information on wireless networking, refer to in "Wireless Communications" in Appendix B.

> **Note:** Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the VPN firewall router. For complete range and performance specifications, please see "Default Settings and Technical Specifications" in Appendix A."

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the VPN firewall. The latency, data throughput performance, and notebook power consumption also vary depending on your configuration choices. For best results, place your VPN firewall router:

- Near the center of the area in which your PCs will operate.
- In an elevated location, such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls). The best location is elevated, such as wall mounted or on the top of a cubicle, and at the center of your wireless coverage area for all the mobile devices.
- Away from sources of interference, such as PCs, microwaves, and 2.4 GHz cordless phones.
- Away from large metal surfaces.

Be aware that the time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

Implementing Appropriate Wireless Security

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

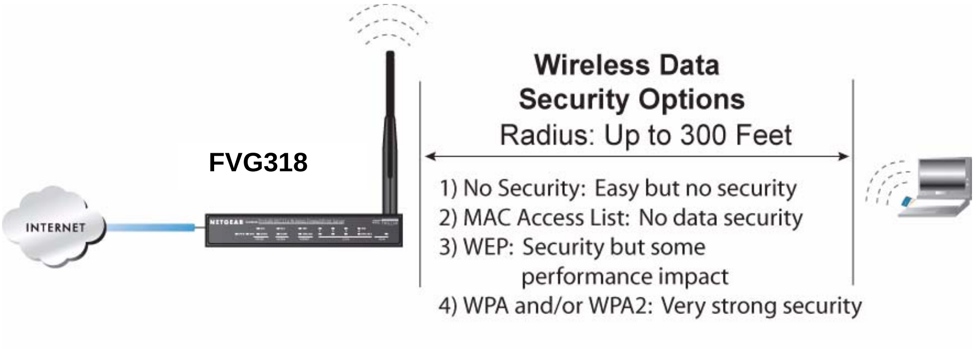

FVG318
INTERNET
Wireless Data
Security Options
Radius: Up to 300 Feet
1) No Security: Easy but no security
2) MAC Access List: No data security
3) WEP: Security but some performance impact
4) WPA and/or WPA2: Very strong security

Figure 3-1

Note: Indoors, computers can connect to wireless networks at ranges of 300 feet or more. Such distances allow others outside of your area to access your network.

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

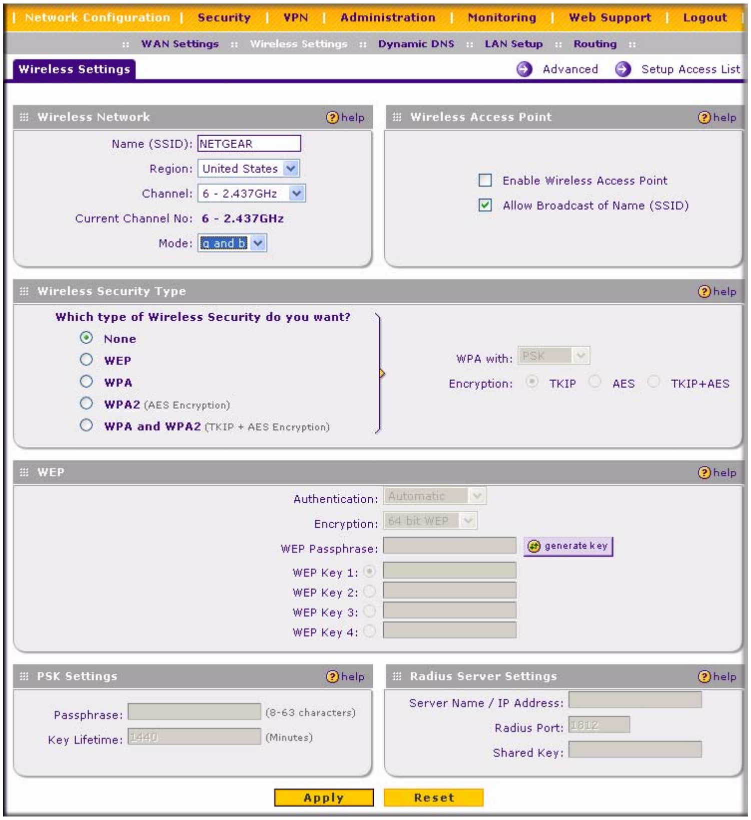
- **Restrict Access Based on MAC Address.** You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the FVG318. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn Off the Broadcast of the Wireless Network Name SSID.** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies wireless network “discovery” feature of some products, such as Windows XP, but the data is still exposed.
- **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption will block all but the most determined eavesdropper.

- **Wi-Fi Protected Access (WPA and WPA2)**. The very strong authentication along with dynamic per frame rekeying of WPA and WPA2 make it virtually impossible to compromise. Because this is a new standard, wireless device driver and software availability may be limited.
  - **WPA with PSK** (Wi-Fi Protected Access Pre-Shared Key). WPA-PSK uses TKIP standard encryption.
  - **WPA2 with PSK**. WPA2 is a later version of WPA. Only select this if all clients support WPA2. If selected, you must use AES encryption, and enter the WPA passphrase (Network key).
  - **WPA-PSK and WPA2-PSK**. This selection allows clients to use either WPA (with TKIP encryption) or WPA2 (with AES encryption). If selected, encryption must be TKIP + AES.
  - **WPA with Radius**. This version of WPA requires the use of a Radius server for authentication. Each user (Wireless Client) must have a “user” login on the Radius Server—normally done via a digital certificate. Also, this device must have a “client” login on the Radius server. Data transmissions are encrypted using a key which is automatically generated.
  - **WPA2 with RADIUS**. WPA2 is a later version of WPA. Only select this if all clients support WPA2. If selected, you must use AES encryption, and configure the RADIUS Server Settings. Each user (Wireless Client) must have a “user” login on the Radius Server—normally done via a digital certificate. Also, this device must have a “client” login on the RADIUS server. Data transmissions are encrypted using a key which is automatically generated.
  - **WPA and WPA2 with RADIUS**. This selection allows clients to use either WPA (with AES encryption) or WPA2 (with TKIP encryption). If selected, encryption must be TKIP+AES. You must also configure the RADIUS Server Settings

Understanding Wireless Settings

To configure the wireless settings of your FVG318:

1. Select Network Configuration > Wireless Settings from the main menu. The Wireless Settings screen will display.


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Wireless Settings :: Dynamic DNS :: LAN Setup :: Routing ::
Wireless Settings
Advanced
Setup Access List
help
Apply
Reset
generate key

Wireless Network

Name (SSID): NETGEAR

Region: United States

Channel: 6 - 2.437GHz

Current Channel No: 6 - 2.437GHz

Mode: g and b

Wireless Access Point

□ Enable Wireless Access Point

☑ Allow Broadcast of Name (SSID)

Wireless Security Type

Which type of Wireless Security do you want?

● None
○ WEP
○ WPA
○ WPA2 (AES Encryption)
○ WPA and WPA2 (TKIP + AES Encryption)

WPA with: PSK

Encryption: ● TKIP ○ AES ○ TKIP+AES

WEP

Authentication: Automatic

Encryption: 64 bit WEP

WEP Passphrase:

WEP Key 1: ●

WEP Key 2: ○

WEP Key 3: ○

WEP Key 4: ○

PSK Settings

Passphrase: (8-63 characters)

Key Lifetime: 1440 (Minutes)

Radius Server Settings

Server Name / IP Address:

Radius Port: 1812

Shared Key:

Figure 3-2

	Note: The 802.11b and 802.11g wireless networking protocols are configured in exactly the same fashion. The FVG318 will automatically adjust to the 802.11g or 802.11b protocol as the device requires without compromising the speed of the other devices.

- **Wireless Network.** The station name of the FVG318.
  - **Wireless Network Name (SSID).** The SSID is also known as the wireless network name. Enter a value of up to 32 alphanumeric characters. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device you want to participate in the 802.11b/g wireless network will need to use this SSID for that network. The FVG318 default SSID is: **NETGEAR**.

- **Region.** This field identifies the region where the FVG318 can be used. It may not be legal to operate the wireless features of the VPN firewall router in a region other than one of those identified in this field. Unless you select a region, you will only be able to use Channel 11.
- **Channel.** This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby access point. For more information on the wireless channel frequencies, please refer to "Wireless Communications" in Appendix B.
- **Mode**. Select the desired wireless mode. The options are:
  - g & b - Both 802.11g and 802.11b wireless stations can be used.
  - g only - Only 802.11g wireless stations can be used.
  - b only - All 802.11b wireless stations can be used. 802.11g wireless stations can still be used if they can operate in 802.11b mode.

  The default is "g & b" which allows both 802.11g and 802.11b wireless stations to access this device.

- **Wireless Access Point**
  - **Enable Wireless Access Point**. Enables the wireless radio. When disabled, there are no wireless communications through the FVG318.
  - **Allow Broadcast of Name (SSID).** The default setting is to enable SSID broadcast. If you disable broadcast of the SSID, only devices that have the correct SSID can connect. Disabling SSID broadcast somewhat hampers the wireless network "discovery" feature of some products.
- **Wireless Card Access List**

  Lets you restrict wireless connections according to a list of Trusted PCs MAC addresses. When the Trusted PCs Only radio button is selected, the FVG318 checks the MAC address of the wireless station and only allows connections to PCs identified on the trusted PCs list.

  To restrict access based on MAC addresses, click the Set up Access List button and update the MAC access control list**.**
- **Security Options**
  - **Disable**: No data encryption is used.
  - **WEP (Wired Equivalent Privacy)**: Use WEP 64 or 128 bit data encryption.
  - **WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)**: Use TKIP standard encryption

- **WPA2-PSK**: WPA2 is a later version of WPA. Only select this if all clients support WPA2. If selected, you must use AES encryption
- **WPA-PSK and WPA2-PSK**: This selection allows clients to use either WPA (with TKIP encryption) or WPA2 (with AES encryption). If selected, encryption must be TKIP + AES.
- **WPA with Radius**: This version of WPA requires the use of a Radius server for authentication. Each user (Wireless Client) must have a “user” login on the Radius Server—normally done via a digital certificate. Also, this device must have a “client” login on the Radius server. Data transmissions are encrypted using a key which is automatically generated.
- **WPA2 with Radius**: WPA2 is a later version of WPA. Only select this if all clients support WPA2. If selected, you must use AES encryption, and configure the Radius Server Settings.
- **WPA and WPA2 with Radius**: This selection allows clients to use either WPA (with AES encryption) or WPA2 (with TKIP encryption). If selected, encryption must be TKIP + AES. If selected, you must configure the Radius Server Settings.

Security Check List for SSID and WEP Settings

For a new wireless network, print or copy this form and fill in the configuration parameters. For an existing wireless network, the person who set up or is responsible for the network will be able to provide this information. Be sure to set the Regulatory Domain correctly as the first step.

- **SSID***:* The Service Set Identification (SSID) identifies the wireless local area network. **Wireless** is the default FVG318 SSID. However, you may customize it by using up to 32 alphanumeric characters. Write your customized SSID on the line below.

  Note: The SSID in the VPN firewall router is the SSID you configure in the wireless adapter card. All wireless nodes in the same network must be configured with the same SSID:

- **Authentication**

  Circle one: Open System or Shared Key. Choose “Shared Key” for more security.

  Note: If you select shared key, the other devices in the network will not connect unless they are set to Shared Key as well and have the same keys in the same positions as those in the FVG318.

- **WEP Encryption Keys**

  For all four 802.11b keys, choose the Key Size. Circle one: 64 or 128 bits

  Key 1: ______________________________

  Key 2: ______________________________

  Key 3: ______________________________

  Key 4: ______________________________

- **WPA-PSK or WPA2-PSK (Pre-Shared Key)**

  Record the WPA-PSK or WPA2-PSK key:

  Key: ______________________________

- **WPA or WPA2 RADIUS Settings**

  For WPA or WPA2, record the following RADIUS settings:

  Server Name/IP Address: Primary _______________ Secondary ________________

  Port: ______________________________

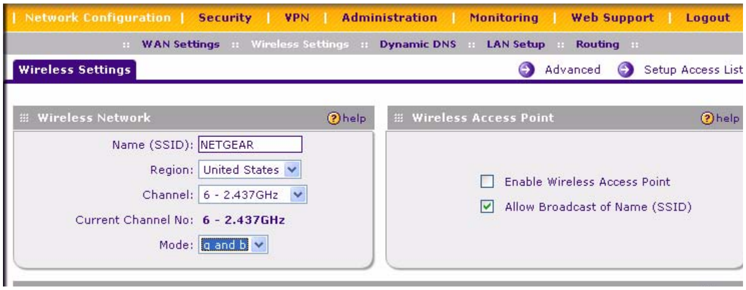
  Shared Key: ______________________________

Use the procedures described in the following sections to configure the FVG318. Store this information in a safe place.

Setting Up and Testing Basic Wireless Connectivity

Follow the instructions below to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs.

1. Log in using the default LAN address of **http://192.168.0.1** with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Select Network Configuration > Wireless Settings to display the Wireless Settings screen.


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
:: WAN Settings :: Wireless Settings :: Dynamic DNS :: LAN Setup :: Routing ::
Wireless Settings
Advanced
Setup Access List
Wireless Network
help
Wireless Access Point
help

Name (SSID): NETGEAR
Region: United States
Channel: 6 - 2.437GHz
Current Channel No: 6 - 2.437GHz
Mode: g and b

□ Enable Wireless Access Point
☑ Allow Broadcast of Name (SSID)

Figure 3-3

3. Set the Regulatory Domain correctly.
4. Choose a suitable descriptive name for the wireless network name (SSID). In the SSID box, enter a value of up to 32 alphanumeric characters. The default SSID is NETGEAR.

Note: The characters are case sensitive. An access point always functions in infrastructure mode. The SSID for any wireless device communicating with the access point must match the SSID configured in the ProSafe 802.11g Wireless VPN Firewall. If they do not match, you will not get a wireless connection to the FVG318.

5. Set the Channel.

   It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless router or access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your VPN firewall router. For more information on the wireless channel frequencies please refer to “Wireless Channels” in “Wireless Communications” in Appendix B.
6. Depending on the types of wireless adapters you have in your computers, choose from the Mode drop-down list.

7. For initial configuration and test, leave the Wireless Card Access List set to “All Wireless Stations” and the Encryption Strength set to “Disable.”
8. Click **Apply** to save your changes.

➡	**Note:** If you are configuring the FVG318 from a wireless computer and you change the VPN firewall router’s SSID, channel, or security settings, you will lose your wireless connection when you click on Apply. You must then change the wireless settings of your computer to match the FVG318’s new settings.

9. Configure and test your PCs for wireless connectivity.

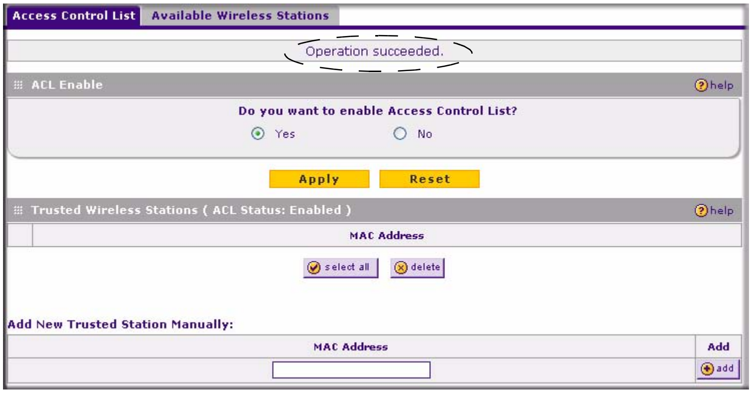
   Program the wireless adapter of your PCs to have the same SSID that you configured in the FVG318. Check that they have a wireless link and are able to obtain an IP address by DHCP from the VPN firewall router.

Once your PCs have basic wireless connectivity to the VPN firewall router, then you can configure the advanced options and wireless security functions.

Restricting Wireless Access by MAC Address

To restrict access based on MAC addresses, follow these steps:

1. Log in at the default LAN address of **http://192.168.0.1** with the default user name of **admin** and default password of **password**.
2. Select Network Configuration > Wireless Settings and click the **Setup Access List** link. The Access Control List screen will display.



Access Control List
Available Wireless Stations
ACL Enable
help
Apply
Reset
Trusted Wireless Stations (ACL Status: Enabled)
help
select all
delete
add

Operation succeeded.

Do you want to enable Access Control List?

● Yes ○ No

Add New Trusted Station Manually:

MAC Address	Add

Figure 3-4

3. Check the **Yes** radio box to enable MAC filtering and turn on the Access Control List. Then click **Apply.** An “Operation Succeed” message will display. Only Trusted Wireless Stations will be able to connect to the VPN firewall router.
4. You can add trusted devices by selecting a device from the list of available wireless cards the FVG318 has discovered in your area, or you can manually enter the MAC address.
   - Add a wireless station manually be entering the device MAC Address in the **Add New Trusted Station Manually** field and clicking **Add.** The station will be added to the **Trusted Wireless Stations** list (if **ACL Enable** has been enabled).
   - Click the **Available Wireless Stations** tab to view the list of available wireless stations within range of this VPN firewall router. To add a wireless station to the ACL, highlight its MAC address and click **Add to Trusted List.**

   > **Note:** When configuring the FVG318 from a wireless computer whose MAC address is not in the access control list, if you select Turn Access Control On, you will lose your wireless connection when you click Apply. You must then access the VPN firewall router from a wired computer or from a wireless computer which is on the access control list to make any further changes.

   Now, only devices on this list will be allowed to wirelessly connect to the FVG318.

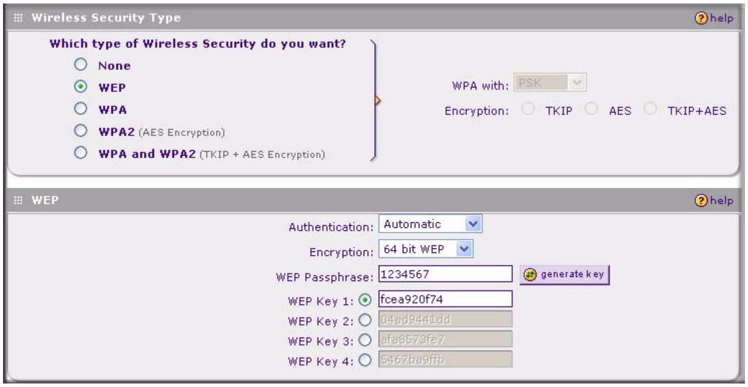
To remove a MAC address from the table, click to select it, then click **Delete**.

Configuring WEP Security Settings

> **Note:** When changing the wireless settings from a wireless computer, you will lose your wireless connection when you click Apply. You must then either configure your wireless adapter to match the new wireless settings or access the VPN firewall router from a wired computer to make any further changes.

To configure WEP data encryption, follow these steps:

1. Log in at the default LAN address of **http://192.168.0.1** with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you set up.
2. Select Network Configuration > Wireless Settings. The Wireless Settings screen will display.



Wireless Security Type

Which type of Wireless Security do you want?

○ None
● WEP
○ WPA
○ WPA2 (AES Encryption)
○ WPA and WPA2 (TKIP + AES Encryption)

WPA with: PSK

Encryption: ○ TKIP ○ AES ○ TKIP+AES

WEP

Authentication: Automatic

Encryption: 64 bit WEP

WEP Passphrase: 1234567

WEP Key 1: ● fcea920f74
WEP Key 2: ○ 04ad9441dd
WEP Key 3: ○ afa8573fe7
WEP Key 4: ○ 5467ba9ffb

Figure 3-5

3. In the Wireless Security Type section, select the WEP radio box. The WEP fields section will be highlighted.

4. Choose the **Authentication Type** (Automatic, Open System or Shared Key) and **Encryption Strength** options. You can manually or automatically program the four data encryption keys. These values must be identical on all PCs and Access Points in your network.

   – **Authentication Type**: Normally this can be left at the default value of “Automatic.” If set to “Open System” or “Shared Key”, wireless stations must use the same method.

   – **Encryption**: Select the desired WEP Encryption:

     - 64-bit (sometimes called 40-bit) encryption
     - 128-bit encryption

   – **WEP Keys**: If using WEP, you can manually or automatically program the four data encryption keys. These values must be identical on all PCs and Access Points in your network.

     - **Automatic Key Generation (Passphrase)**: Enter a word or group of printable characters (this phrase is case sensitive) in the Passphrase box and click the “Generate Keys” button to automatically configure the WEP Key(s).

     – If encryption is set to 64 bit, then each of the four key boxes will automatically be populated with key values.

     – If encryption is set to 128 bit, then only the selected WEP key box will automatically be populated with a key value.

- **Manual Entry Mode**: Enter ten hexadecimal digits (any combination of 0-9, a-f, or A-F). These hex values are not case sensitive. Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key box.
  - **For 64 bit WEP**: Enter ten hexadecimal digits (any combination of 0-9, A-F).
  - **For 128 bit WEP**: Enter twenty-six hexadecimal digits (any combination of 0-9, A-F).

Please refer to "Wireless Communications" in Appendix B, "Related Documents" for a full explanation of each of these options, as defined by the IEEE 802.11b wireless communication standard.

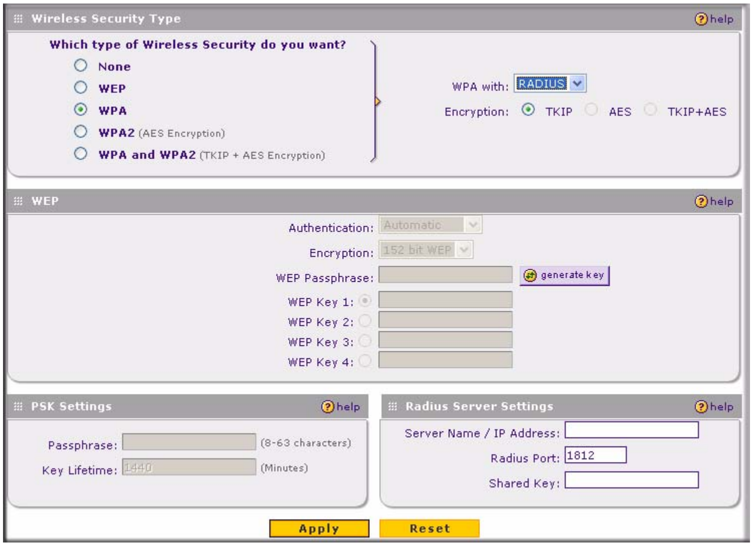
5. Click **Apply** to save your settings.

Configuring WPA with RADIUS

➡	**Note:** Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

To configure WPA with RADIUS:

1. Log in at the default LAN address of **http://192.168.0.1** with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Select Network Administration > Wireless Settings. The Wireless Settings Screen will display.



Wireless Security Type

Which type of Wireless Security do you want?

○ None
○ WEP
● WPA
○ WPA2 (AES Encryption)
○ WPA and WPA2 (TKIP + AES Encryption)

WPA with: RADIUS

Encryption: ● TKIP ○ AES ○ TKIP+AES

WEP

Authentication: Automatic
Encryption: 152 bit WEP
WEP Passphrase:
WEP Key 1: ●
WEP Key 2: ○
WEP Key 3: ○
WEP Key 4: ○

PSK Settings

Passphrase: (8-63 characters)
Key Lifetime: 1440 (Minutes)

Radius Server Settings

Server Name / IP Address:
Radius Port: 1812
Shared Key:

Figure 3-6

3. Select the **WPA** radio box and then select **RADIUS** from the **WPA with:** pull-down menu in the Wireless Security Type section. The RADIUS settings fields in the Radius Server Settings section will be highlighted.

> **Note:** The **Encryption** choice will be TKIP by default. For WPA with RADIUS, TKIP is used.

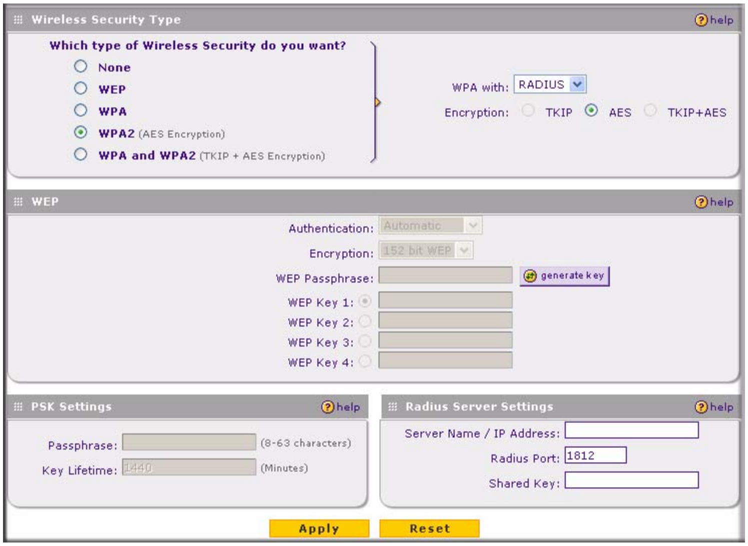
4. Enter the Radius Server Settings.
   - **Primary Server Name/IP Address**: This field is required. Enter the name or IP address of the primary Radius Server on your LAN.
   - **Radius Port**: Enter the port number used for connecting to the Radius Server.
   - **Shared Key**: Enter the desired value for the Shared Key. This must match the value used on the Radius server.
5. Click **Apply** to save your settings.

Configuring WPA2 with RADIUS

Note: Not all wireless adapters support WPA2. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA2. Nevertheless, the wireless adapter hardware and driver must also support WPA2. Consult the product document for your wireless adapter and WPA2 client software for instructions on configuring WPA2 settings.

To configure WPA2 with RADIUS:

1. Log in at the default LAN address of **http://192.168.0.1** with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Select Network Adminisration > Wireless Settings. The Wireless Settings Screen will display.



Wireless Security Type

Which type of Wireless Security do you want?

○ None
○ WEP
○ WPA
● WPA2 (AES Encryption)
○ WPA and WPA2 (TKIP + AES Encryption)

WPA with: RADIUS

Encryption: ○ TKIP ● AES ○ TKIP+AES

WEP

Authentication: Automatic

Encryption: 152 bit WEP

WEP Passphrase:

WEP Key 1: ●

WEP Key 2: ○

WEP Key 3: ○

WEP Key 4: ○

PSK Settings

Passphrase: (8-63 characters)

Key Lifetime: 1440 (Minutes)

Radius Server Settings

Server Name / IP Address:

Radius Port: 1812

Shared Key:

Figure 3-7

3. Select the **WPA2** radio box and then select **RADIUS** from the **WPA with:** pull-down menu in the Wireless Security Type section. The RADIUS settings fields in the Radius Server Settings section will be highlighted.

Note: The **Encryption** choice will be AES by default. For WPA2 with RADIUS, AES is used.

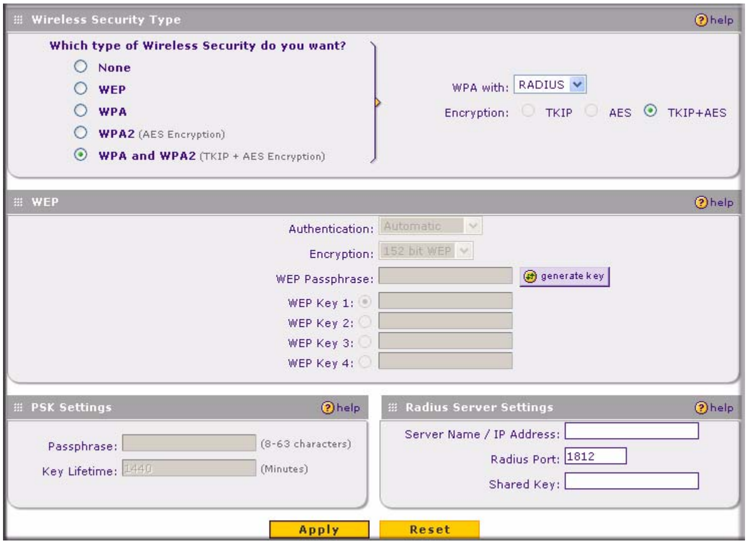
4. Enter the Radius Server Settings.
   - **Primary Server Name/IP Address**: This field is required. Enter the name or IP address of the primary Radius Server on your LAN.
   - **Radius Port**: Enter the port number used for connecting to the Radius Server.
   - **Shared Key**: Enter the desired value for the Shared Key. This must match the value used on the Radius server.
5. Click **Apply** to save your settings.

Configuring WPA and WPA2 with RADIUS

Note: Not all wireless adapters support WPA and WPA2. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA and WPA2. Nevertheless, the wireless adapter hardware and driver must also support WPA and WPA2. Consult the product document for your wireless adapter and WPA and WPA2 client software for instructions on configuring WPA and WPA2 settings.

To configure WPA and WPA2 with RADIUS:

1. Log in at the default LAN address of **http://192.168.0.1** with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Select Network Adminisration > Wireless Settings. The Wireless Settings Screen will display.



Wireless Security Type

Which type of Wireless Security do you want?

○ None
○ WEP
○ WPA
○ WPA2 (AES Encryption)
● WPA and WPA2 (TKIP + AES Encryption)

WPA with: RADIUS

Encryption: ○ TKIP ○ AES ● TKIP+AES

WEP

Authentication: Automatic

Encryption: 152 bit WEP

WEP Passphrase: [generate key]

WEP Key 1: ●
WEP Key 2: ○
WEP Key 3: ○
WEP Key 4: ○

PSK Settings

Passphrase: (8-63 characters)

Key Lifetime: 1440 (Minutes)

Radius Server Settings

Server Name / IP Address:

Radius Port: 1812

Shared Key:

[Apply] [Reset]

Figure 3-8

3. Select the **WPA and WPA2** radio box and then select **RADIUS** from the **WPA with:** pull-down menu in the Wireless Security Type section. The RADIUS settings fields in the Radius Server Settings section will be highlighted.

➡	**Note:** The **Encryption** choice will be TKIP+AES by default. For WPA/WPA2 with RADIUS, TKIP+AES is used.

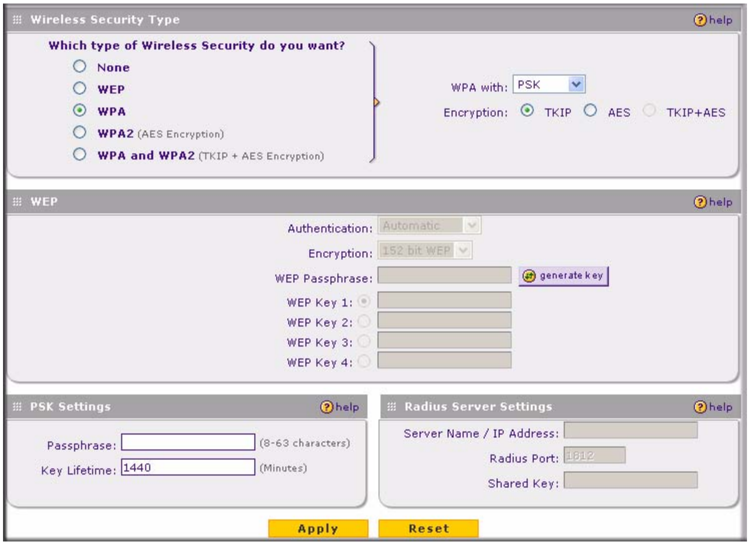
4. Enter the Radius Server Settings.
   - **Primary Server Name/IP Address**: This field is required. Enter the name or IP address of the primary Radius Server on your LAN.
   - **Radius Port**: Enter the port number used for connecting to the Radius Server.
   - **Shared Key**: Enter the desired value for the Shared Key. This must match the value used on the Radius server.
5. Click **Apply** to save your settings.

Configuring WPA-PSK

Note: Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

To configure WPA-PSK:

1. Log in at the default LAN address of **http://192.168.0.1**, with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Select Network Adminisration > Wireless Settings. The Wireless Settings Screen will display.



Wireless Security Type

Which type of Wireless Security do you want?

○ None
○ WEP
● WPA
○ WPA2 (AES Encryption)
○ WPA and WPA2 (TKIP + AES Encryption)

WPA with: PSK

Encryption: ● TKIP ○ AES ○ TKIP+AES

WEP

Authentication: Automatic

Encryption: 152 bit WEP

WEP Passphrase:

WEP Key 1: ●
WEP Key 2: ○
WEP Key 3: ○
WEP Key 4: ○

PSK Settings

Passphrase: (8-63 characters)

Key Lifetime: 1440 (Minutes)

Radius Server Settings

Server Name / IP Address:

Radius Port: 1812

Shared Key:

Figure 3-9

3. Select the **WPA** radio box and then select **PSK** from the **WPA with:** pull-down menu in the Wireless Security Type section. The PSK settings fields in the PSK Settings section will be highlighted.

➡	**Note:** The **Encryption** choice will be TKIP by default. For WPA+PSK, TKIP is used.

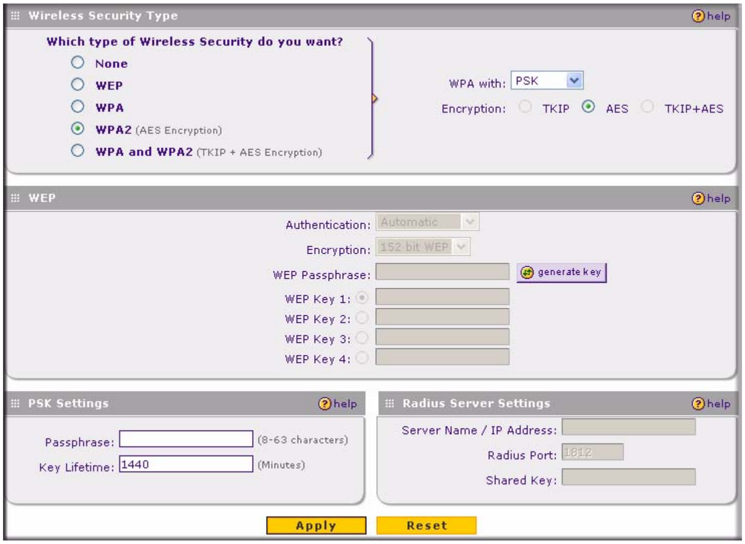
4. In the PSK Settings section:
   - Enter the pre-shared key in the **Passphrase** field. Enter a word or group of printable characters in the Passphrase box. The Passphrase must be 8 to 63 characters in length. The 256 Bit key used for encryption is generated from this passphrase.
   - Enter a value in the **Key Lifetime** field. This setting determines how often the encryption key is changed. Shorter periods provide greater security, but adversely affect performance. If desired, you can change the default value.
5. Click **Apply** to save your settings.

Configuring WPA2-PSK

➡	**Note:** Not all wireless adapters support WPA2. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA2. Nevertheless, the wireless adapter hardware and driver must also support WPA2. Consult the product document for your wireless adapter and WP2 client software for instructions on configuring WPA2 settings.

To configure WPA2-PSK:

1. Log in at the default LAN address of **http://192.168.0.1**, with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Select Network Adminisration > Wireless Settings. The Wireless Settings Screen will display.



Wireless Security Type

Which type of Wireless Security do you want?

○ None
○ WEP
○ WPA
● WPA2 (AES Encryption)
○ WPA and WPA2 (TKIP + AES Encryption)

WPA with: PSK

Encryption: ○ TKIP ● AES ○ TKIP+AES

WEP

Authentication: Automatic

Encryption: 152 bit WEP

WEP Passphrase:

WEP Key 1: ●

WEP Key 2: ○

WEP Key 3: ○

WEP Key 4: ○

PSK Settings

Passphrase: (8-63 characters)

Key Lifetime: 1440 (Minutes)

Radius Server Settings

Server Name / IP Address:

Radius Port: 1812

Shared Key:

Figure 3-10

3. Select the **WPA2** radio box and then select **PSK** from the **WPA with:** pull-down menu in the Wireless Security Type section. The PSK settings fields in the PSK Settings section will be highlighted.

➡	**Note:** The **Encryption** choice will be AES by default. For WPA2+PSK, AES is used.

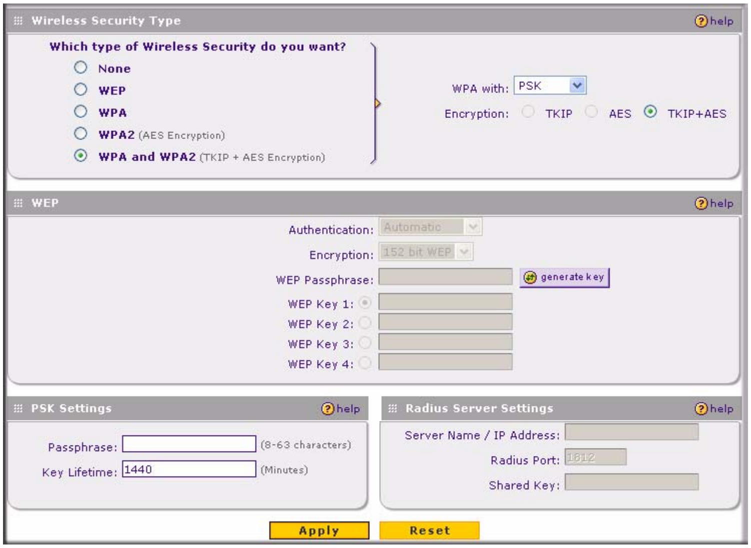
4. In the PSK Settings section:
   - Enter the pre-shared key in the **Passphrase** field. Enter a word or group of printable characters in the Passphrase box. The Passphrase must be 8 to 63 characters in length. The 256 Bit key used for encryption is generated from this passphrase.
   - Enter a value in the **Key Lifetime** field. This setting determines how often the encryption key is changed. Shorter periods provide greater security, but adversely affect performance. If desired, you can change the default value.
5. Click **Apply** to save your settings.

Configuring WPA-PSK and WPA2-PSK

Note: Not all wireless adapters support WPA and WPA2. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA and WPA2. Nevertheless, the wireless adapter hardware and driver must also support WPA and WPA2. Consult the product document for your wireless adapter and WPA and WPA2 client software for instructions on configuring WPA and WPA2 settings.

To configure WPA-PSK and WPA2-PSK:

1. Log in at the default LAN address of **http://192.168.0.1**, with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Select Network Administration > Wireless Settings. The Wireless Settings Screen will display.



Which type of Wireless Security do you want?

○ None
○ WEP
○ WPA
○ WPA2 (AES Encryption)
● WPA and WPA2 (TKIP + AES Encryption)

WPA with: PSK

Encryption: ○ TKIP ○ AES ● TKIP+AES

Authentication: Automatic

Encryption: 152 bit WEP

WEP Passphrase:

WEP Key 1: ●

WEP Key 2: ○

WEP Key 3: ○

WEP Key 4: ○

Passphrase: (8-63 characters)

Key Lifetime: 1440 (Minutes)

Server Name / IP Address:

Radius Port: 1812

Shared Key:

Figure 3-11

3. Select the **WPA and WPA2** radio box and then select **PSK** from the **WPA with:** pull-down menu in the Wireless Security Type section. The PSK settings fields in the PSK Settings section will be highlighted.

➡	**Note:** The **Encryption** choice will be TKIP+AES by default. For WPA and WPA2+PSK, TKIP+AES is used.

4. In the PSK Settings section:
   - Enter the pre-shared key in the **Passphrase** field. Enter a word or group of printable characters in the Passphrase box. The Passphrase must be 8 to 63 characters in length. The 256 Bit key used for encryption is generated from this passphrase.
   - Enter a value in the **Key Lifetime** field. This setting determines how often the encryption key is changed. Shorter periods provide greater security, but adversely affect performance. If desired, you can change the default value.
5. 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 802.11g Wireless VPN Firewall to protect your network. These features can be found by clicking on the **Security** heading in the main menu of the browser interface.

Firewall Protection and Content Filtering Overview

The ProSafe 802.11g Wireless VPN Firewall FVG318 provides you with Web content filtering options, plus browsing activity reporting and instant alerts via e-mail. Parents and 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. 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.

To configure these features of your firewall, click on the **Security > Block Sites** heading in the main menu of the browser interface. The Content Filtering features are described below:

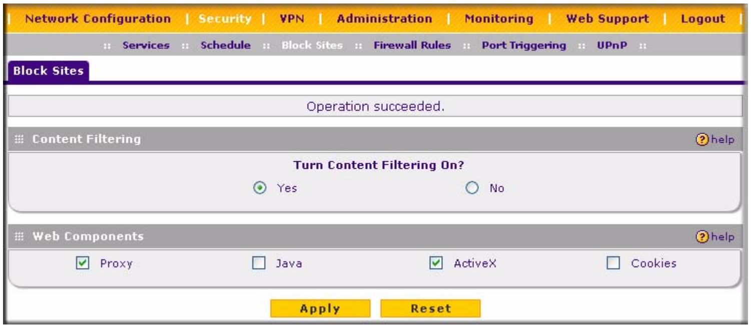
Block Sites

The FVG318 supports content filtering which allows you to block access to certain Internet sites. Up to 32 words in an Internet sites name (for example, a website URL) can be specified causing the site to be blocked.

Certain commonly used web components can also be blocked for increased security. Some of these components can be used by malicious websites to infect computers that access them. For example:

- **Proxy.** A proxy server 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.** Enabling this feature 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.
- **Active X.** Similar to Java applets, ActiveX controls are installed on Windows computers 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 cause many websites to not function properly.


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
:: Services :: Schedule :: Block Sites :: Firewall Rules :: Port Triggering :: UPnP ::
Block Sites
help
help
Apply
Reset

Operation succeeded.

Content Filtering

Turn Content Filtering On?

● Yes ○ No

Web Components

☑ Proxy ☐ Java ☑ ActiveX ☐ Cookies

Figure 4-1

To enable Content Filtering:

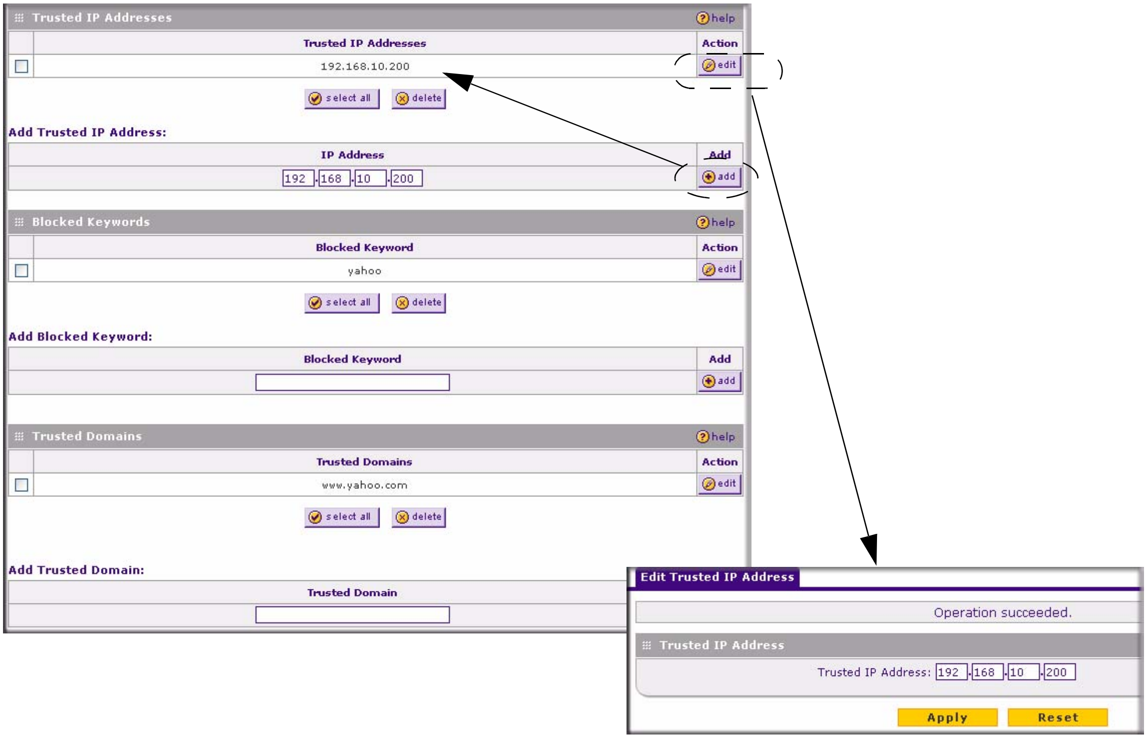
1. Select Security > Block Sites from the menu. The Block Sites screen will display.

2. Check the **Yes** radio box in the Content Filtering section and click **Apply.** This will enable content filtering and allow you to specify Web Components to be blocked.
3. Check the radio box for each Web Component you want to enable; then click **Apply.** The selected Web Component options will be blocked.

Once Content Filtering has been enabled you can add Trusted IP Addresses, Blocked Keywords and Trusted Domains.

Trusted Internet Addresses and Trusted Domains are Internet addresses and sites for which content filtering maybe bypassed. The Trusted IP Addresses table and the Trusted Domain table list the currently defined trusted IP addresses and domains.

The domain will appear in the Trusted Domain list. Any number of domain names can be added to the list. Those names entered in the Trusted Domain list will be bypassed by Keyword filtering. For example: If yahoo is added to the Blocked Keywords list and www.yahoo.com is added to the Trusted Domain list, then www.yahoo.com will be allowed but mail.yahoo.com will not allowed.



Trusted IP Addresses

	Trusted IP Addresses	Action
☐	192.168.10.200	edit

Add Trusted IP Address:

IP Address	Add
192 . 168 . 10 . 200	add

Blocked Keywords

	Blocked Keyword	Action
☐	yahoo	edit

Add Blocked Keyword:

Blocked Keyword	Add
	add

Trusted Domains

	Trusted Domains	Action
☐	www.yahoo.com	edit

Add Trusted Domain:

Trusted Domain

Edit Trusted IP Address

Operation succeeded.

Trusted IP Address

Trusted IP Address: 192 . 168 . 10 . 200

Figure 4-2

To add a Trusted IP Address or Trusted Domain:

1. In the appropriate field add the IP Address or Domain Name.
2. Click **Add.** The IP Address or Domain Name will appear in the appropriate table.
3. Click Edit adjacent to the entry to modify or change the selected IP Address or Domain Name. An Edit screen will display. When you have completed your changes, click **Apply.** The change will appear in the appropriate table.

To delete Trusted IP Addresses or Trusted Domain Names:

- Click **Select All** to select all the items in the list, and then click **Delete.**
- Select the checkbox adjacent to an item to delete only that entry, and then click **Delete.**

To add or modify a keyword:

1. Enter a new keyword in the **Blocked Keyword** field in the Add Blocked Keyword section and click **Add.** The Blocked Keyword will appear in the Blocked Keyword table.
2. Click **Add** adjacent to the keyword you want to modify. An Edit Keyword screen will display. When you have completed your changes, click **Apply.** The change will appear in the Blocked Keyword table.

To delete a keyword:

- Click **Select All** to select all the items in the list, and then click **Delete.**
- Select the checkboxes adjacent to the keywords you want to delete, and then click **Delete.**

The following are examples of Blocked Keyword application s:

- 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 websites with other domain suffixes (such as .edu or .gov) can be viewed.
- If you wish to block all Internet browsing access, enter the keyword “.”.

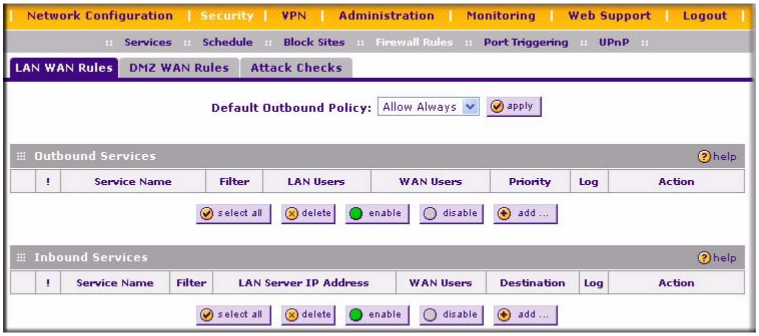
Using Rules to Block or Allow Specific Kinds of Traffic

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

A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the FVG318 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.

These default rules are shown in the Rules table of the Rules menu in Figure 4-3:


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Block Sites :: Firewall Rules :: Port Triggering :: UPnP
LAN WAN Rules
DMZ WAN Rules
Attack Checks
apply
help
select all
delete
enable
disable
add ...

Default Outbound Policy: Allow Always

Outbound Services

	!	Service Name	Filter	LAN Users	WAN Users	Priority	Log	Action

Inbound Services

	!	Service Name	Filter	LAN Server IP Address	WAN Users	Destination	Log	Action

Figure 4-3

You may define additional rules that specify exceptions to the default rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. You can also choose to log traffic that matches or does not match the rule you have defined.

To create, edit or change the order of a rule:

- Click **Add** under the Outbound Services table to add an Outbound rule or click **Add** under the Inbound Services table to add an Inbound rule.
- Click **Edit** adjacent to an existing rule. An Edit Rule screen will display. After you have completed your modifications, click **Apply.** The modified rule will appear in the appropriate table.
- In the **Action** column, change the order of a rule in the hierarchy of how rules are implemented by clicking the **Up** or **Down** icons.

To delete or disable/enable rules:

- Click **select all** to delete all the rules for a given service.
- Check the box adjacent to the rules you want to delete, and then click **Delete.**
- Check the box adjacent to the rule you want to enable or disable and then click the appropriate action: **Enable** or **Disable**.

An example of the menu for defining or editing a rule is shown in Figure 4-3. The parameters are:

- **Service**. From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the Services menu to add any additional services or applications that do not already appear.
- **Action**. Choose how you would like this type of traffic to be handled. You can block or allow always, or you can choose to block or allow according to the schedule you have defined in the Schedule menu.
- **Source Address**. Specify traffic originating on the LAN (outbound) or the WAN (inbound), and choose whether you would like the traffic to be restricted by source IP address. You can select Any, a Single address, or a Range. If you select a range of addresses, enter the range in the start and finish boxes. If you select a single address, enter it in the start box.
- **Destination Address**.The Destination Address will be assumed to be from the opposite (LAN or WAN) of the Source Address. As with the Source Address, you can select Any, a Single address, or a Range unless NAT is enabled and the destination is the LAN. In that case, you must enter a Single LAN address in the start box.
- **Log**. You can select whether the traffic will be logged. The choices are:
  - Never — no log entries will be made for this service.
  - Match — traffic of this type that matches the parameters and action will be logged.

Inbound Rules (Port Forwarding)

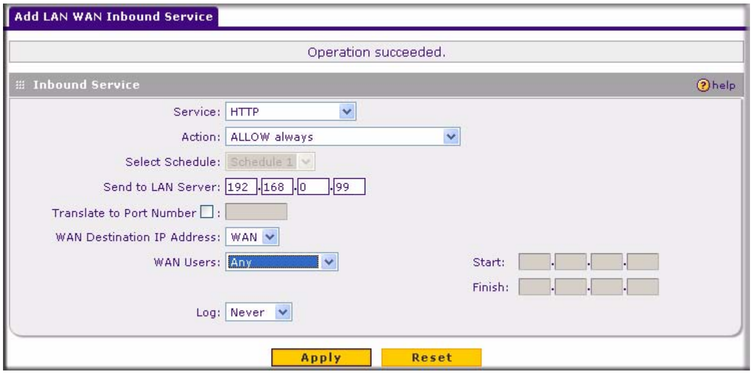
Because the FVG318 uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a Web server or game server) visible 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.

> **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. Only enable those ports that are necessary for your network. Following are two application examples of inbound rules:

Inbound Rule Example: 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. This rule is shown in Figure 4-4:



Add LAN WAN Inbound Service

Operation succeeded.

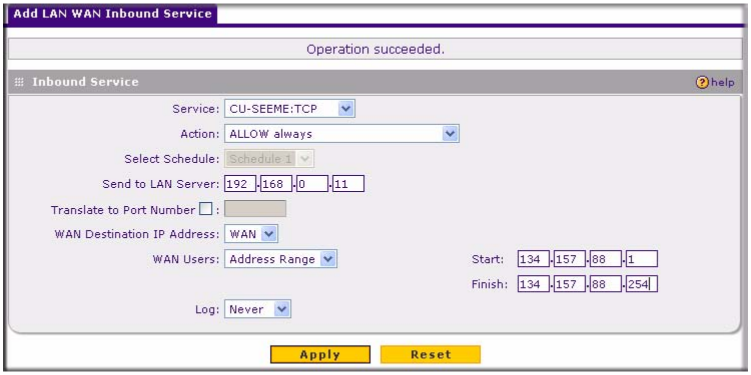
Inbound Service

Service: HTTP
Action: ALLOW always
Select Schedule: Schedule 1
Send to LAN Server: 192 . 168 . 0 . 99
Translate to Port Number □ :
WAN Destination IP Address: WAN
WAN Users: Any
Start: . . .
Finish: . . .
Log: Never

Figure 4-4

Inbound Rule Example: Allowing a Videoconference from Restricted Addresses

If you want to allow incoming video conferencing 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 only from a specified range of external IP addresses. In this case, we have also specified logging of any incoming CU-SeeMe requests that do not match the allowed parameters.



Add LAN WAN Inbound Service

Operation succeeded.

Inbound Service

Service: CU-SEEME:TCP
Action: ALLOW always
Select Schedule: Schedule 1
Send to LAN Server: 192 . 168 . 0 . 11
Translate to Port Number □ :
WAN Destination IP Address: WAN
WAN Users: Address Range
Start: 134 . 157 . 88 . 1
Finish: 134 . 157 . 88 . 254
Log: Never

Figure 4-5

Considerations for Inbound Rules

- If your external IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires. Consider using the Dynamic DNS feature in the Advanced menus so that external users can always find your network.
- 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 IP menu to keep the PC's IP address constant.
- Each local PC must access the local server using the PC's local LAN address (192.168.0.99 in Local Public Web Server example). Attempts by local PCs to access the server using the external WAN IP address will fail.

Outbound Rules (Service Blocking)

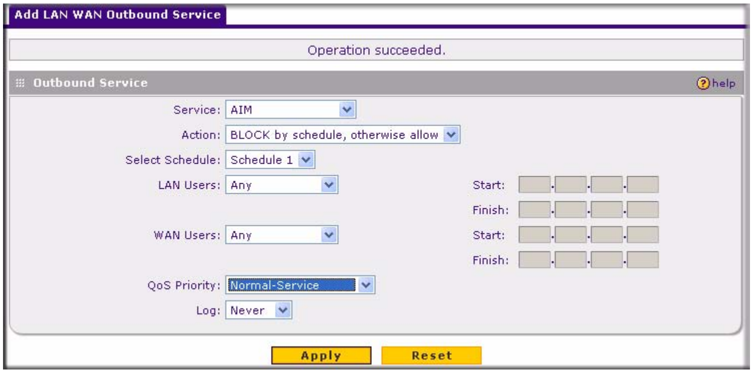
The FVG318 allows you to block the use of certain Internet services by PCs on your network. This is called service blocking or port filtering. You can define an outbound rule to block Internet access from a local PC based on:

- IP address of the local PC (source address)
- IP address of the Internet site being contacted (destination address)
- Time of day
- Type of service being requested (service port number)

Following is an application example of an outbound rule:

Outbound Rule Example: Blocking Instant Messenger

If you want 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.



Add LAN WAN Outbound Service

Operation succeeded.

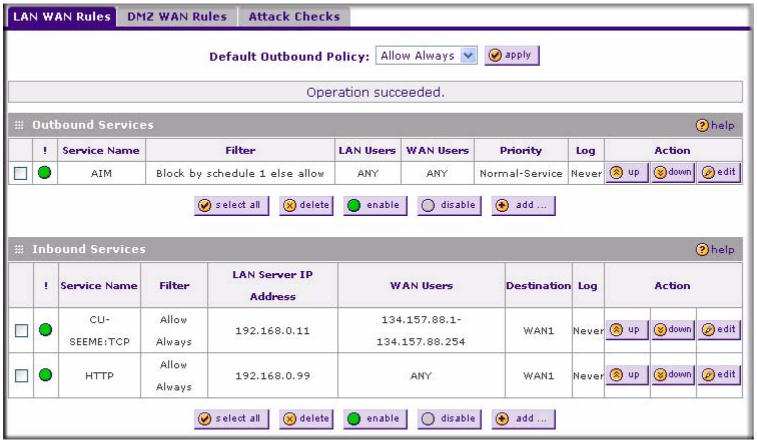
Outbound Service

Service:	AIM		
Action:	BLOCK by schedule, otherwise allow		
Select Schedule:	Schedule 1		
LAN Users:	Any	Start:	. . .
		Finish:	. . .
WAN Users:	Any	Start:	. . .
		Finish:	. . .
QoS Priority:	Normal-Service		
Log:	Never		

Figure 4-6

Order of Precedence for Rules

As you define new rules, they are added to the tables in the Rules table, as shown below:



Default Outbound Policy: Allow Always

Operation succeeded.

Outbound Services

	!	Service Name	Filter	LAN Users	WAN Users	Priority	Log	Action
□	●	AIM	Block by schedule 1 else allow	ANY	ANY	Normal-Service	Never	up down edit

Inbound Services

	!	Service Name	Filter	LAN Server IP Address	WAN Users	Destination	Log	Action
□	●	CU-SEEME:TCP	Allow Always	192.168.0.11	134.157.88.1-134.157.88.254	WAN1	Never	up down edit
□	●	HTTP	Allow Always	192.168.0.99	ANY	WAN1	Never	up down edit

Figure 4-7

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 default rules at the bottom. In some cases, the order of precedence of two or more rules may be important in determining the disposition of a packet. The Up or Down buttons allow you to relocate a defined rule to a new position in the table.

Default DMZ Server

Incoming traffic from the Internet is normally discarded by the firewall unless the traffic is a response to one of your local computers or a service for which you have configured an inbound rule. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the Default DMZ Server.

The Default DMZ Server feature is helpful when using some online games and video conferencing applications that are incompatible with NAT. The firewall is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, one local PC can run the application properly if that PC's IP address is entered as the Default DMZ Server for a particular service.

The DMZ Server screen is used for setting up a firewall rule for traffic coming from the WAN to the DMZ. Inbound traffic for a service can be configured to be blocked or allowed, by default, or set per a schedule (defined on the Schedule page under the Security menu).

To assign a computer or server to be a Default DMZ server:

1. Click the **DMZ WAN Rules** tab.
2. When the DMZ WAN Rules screen displays, click **Add.**
3. From the **Service** pull-down menu, select the service to allow or block.

   This is a unique name assigned to the service. The name usually indicates the type of traffic the rule covers such as ftp, ssh, telnet, ping, etc. Services not already in the list can be added from the Security < Services screen.
4. Enter the **Send to DMZ Service** address of the device on the DMZ which is hosting the server.

   Select the port number checkbox and enter a port number ONLY if the server is listening on a port other than the default. For example, if a machine on the DMZ side is running a telnet server on port 2000, then select the Translate to Port Number checkbox and type 2000 in the Port field. if it is listening on the default port 23, then the box can be left unchecked.
5. From the **WAN Users** pull-down menu, select the specific IP addresses on the WAN that will be affected by the rule. This rule will affect packets for the selected service to the defined IP address or range of IP addresses on the WAN side.
   - Any: All IP addresses on the WAN will be affected by the rule.
   - Single Address: A single WAN IP address will be affected by the rule.
   - Address Range: A range of IP addresses on the DMZ network will be affected by the rule.
6. Click **Apply** to save your settings.

Note: For security, NETGEAR strongly recommends that you avoid using the Default DMZ Server feature. When a computer is designated as the Default DMZ Server, 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.

Attack Checks

The Attack Check screen allows you to specify if the router should be protected against common attacks from the LAN and WAN networks. The various types of attack checks are defined below.

To access the Attack Check screen:

1. Select Security > Firewall Rules and click the **Attack Checks** tab. The Attack Checks screen will display.
2. Select the Attack Check types you want to enable. Descriptions of the various Attack Check types are described in the following table.
3. Click **Apply** to save your settings.

Attack Check Type		**Description**
WAN Security Checks		
	Respond to Ping On Internet Port	To configure the router to respond to an ICMP Echo (ping) packet coming in from the WAN side, check this box. This setting is usually used as a diagnostic tool for connectivity problems. It is recommended that the option be disabled at other times to prevent hackers from easily discovering the router via a ping.
	Enable Stealth Mode	If Stealth Mode is enabled, the router will not respond to port scans from the WAN, which makes it less susceptible to discovery and attacks.
	Block TCP Flood	If this option is enabled, the router will drop all invalid TCP packets and be protected protect from a SYN flood attack.
LAN Security Checks		
	Block UDP Flood	If this option is enabled, the router will not accept more than 20 simultaneous, active UDP connections from a single computer on the LAN.

Attack Check Type		Description
VPN Pass through		
	IPSec/PPTP/L2TP[a]	Typically, the router is used as a VPN Client or Gateway that connects to other VPN Gateways. When the router is in NAT mode, all packets going to the Remote VPN Gateway are first filtered through NAT and then encrypted, per the VPN policy.

[a] In situations where a VPN Client or Gateway on the LAN side of this router is connected to another VPN endpoint on the WAN (placing this router in between two VPN end points), all encrypted packets will be sent to this router. Since this router filters the encrypted packets through NAT, the packets become invalid.

IPSec, PPTP, and L2TP represent different types of VPN tunnels that can pass through this router. To allow the VPN traffic to pass through without filtering, the type of tunnel that will be used as a pass through must be enabled.

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 FVG318 already holds a list of many service port numbers, you are not limited to these choices. Use the Services menu 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.

To define a new service, first you must 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 of news groups.

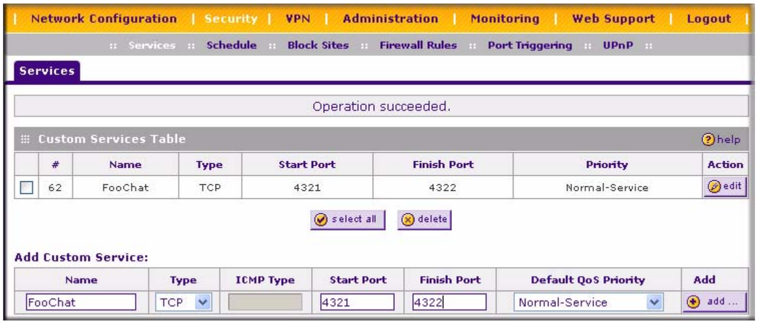
To add a service:

1. When you have the port number information, go the Security > Services. The Services screen will display.
2. In the Add Custom Services section:
    a. Enter a descriptive name for the service in the **Name** field (so that you will remember what it is).

b. From the **Type** pull-down menu, select whether the service uses TCP, UDP or ICMP as its transport protocol.

c. Enter the lowest port number used by the service in the **Start Port** field.

a. Enter the highest port number used by the service in the **Finish Port** field.
If the service only uses a single port number, enter the same number in both fields.


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Block Sites :: Firewall Rules :: Port Triggering :: UPnP ::
Services
help
select all
delete
add ...

Operation succeeded.

Custom Services Table

	#	Name	Type	Start Port	Finish Port	Priority	Action
□	62	FooChat	TCP	4321	4322	Normal-Service	edit

Add Custom Service:

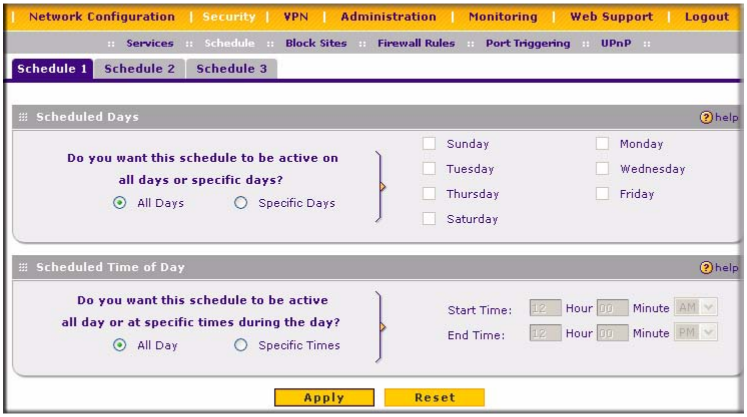
Name	Type	ICMP Type	Start Port	Finish Port	Default QoS Priority	Add
FooChat	TCP		4321	4322	Normal-Service	add ...

Figure 4-8

3. Click **Add**. The new service will appear in the Custom Services Table, and in the **Service** pull-down menu on the Firewall Rules Add/Edit screens.

Using a Schedule to Block or Allow Specific Traffic

If you enabled content filtering in the Block Sites menu, or if you defined an outbound rule to use a schedule, you can set up a schedule for when blocking occurs or when access is restricted. The firewall allows you to specify when blocking will be enforced by configuring the Schedule screen


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Block Sites :: Firewall Rules :: Port Triggering :: UPnP
Schedule 1
Schedule 2
Schedule 3
help
Apply
Reset

Scheduled Days

Do you want this schedule to be active on all days or specific days?

● All Days ○ Specific Days

□ Sunday □ Monday
□ Tuesday □ Wednesday
□ Thursday □ Friday
□ Saturday

Scheduled Time of Day

Do you want this schedule to be active all day or at specific times during the day?

● All Day ○ Specific Times

Start Time: 12 Hour 00 Minute AM

End Time: 12 Hour 00 Minute PM

Figure 4-9

To block keywords or Internet domains based on a schedule:

1. Select Security > Schedule from the menu. The Schedule 1 screen will display.
2. In the Scheduled Days section, select the All Days or Specific Days radio box. If you want to limit access completely for the selected days, select All Day. Otherwise, select the specific days that you want to limit access.
3. If you want to limit access during certain times for the selected days, select the All Day or Specific Times radio box in the **Schedule TIme of Day** section. If you selected Specific Times, then enter a Start Time and an End Time.
4. Click **Apply** to save your changes.
5. Configure Schedule 2 and Schedule 3, if required, following the previous steps.

Getting E-Mail Notifications of Firewall Logs

The VPN firewall can be configured to log and e-mail denial of service attacks, general attack information, login attempts, dropped packets, and so forth, to a specified e-mail address or a SysLog server.

In order to receive logs by e-mail, you must provide your e-mail information in the **Enable E-Mail Logs** section of the Firewall Logs & E-mail screen.

To receive firewall logs via email:

1. Select Monitoring > Firewall Logs & E-Mail. The FIrewall Logs & E-mail screen will display.

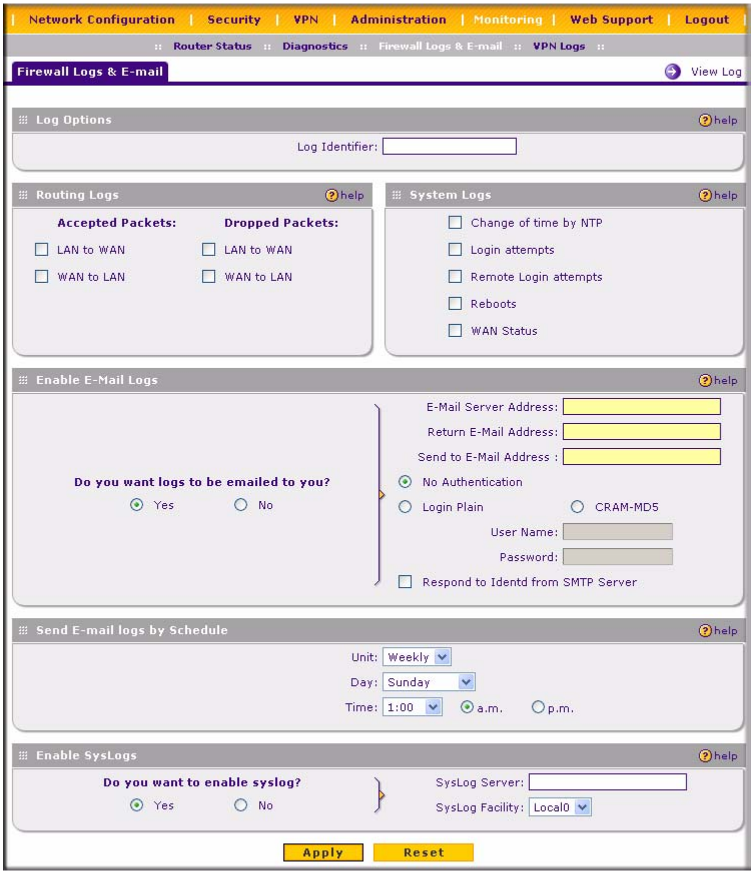
2. Enter the Log Identifier in the Log Options sections.

   Every logged message will contain a prefix for easier identification of the source of the message. The Log Identifier will be prefixed to both e-mail and Syslog messages.

3. Select which Routing Log packets you want to log.
   - Accepted Packets. Logs packets that were successfully transferred through the segment.
   - Dropped Packets. Logs packets that were blocked from being transferred through this segment.

> ➡ **Note:** If monitoring packets from a firewall rule, make sure that the firewall rule Log option is set to "Always."

4. Select the type of system events to be logged. The following system events can be recorded:
   - Change of Time by NTP. Logs a message when the system time changes after a request from a Network Time server.
   - Login Attempts. Logs a message when a login is attempted from the LAN network. Both, successful and failed login attempts will be logged.
   - Secure Login Attempt. Logs a message when a login is attempted using the Secure Remote Management URL (see "Enabling Remote Management Access" on page 8-8). Both, successful and failed login attempts will be logged.
   - Reboots. Record a message when the device has been rebooted through the Web interface.
   - All Unicast Traffic. All unicast packets directed to the router are logged.
   - All Broadcast/Multicast Traffic. All broadcast or multicast packets directed to the router are logged.
   - WAN Status: WAN link status related logs are enabled


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
:: Router Status :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Firewall Logs & E-mail
View Log
help
Apply
Reset

Log Options

Log Identifier:

Routing Logs

Accepted Packets:	Dropped Packets:
□ LAN to WAN	□ LAN to WAN
□ WAN to LAN	□ WAN to LAN

System Logs

□ Change of time by NTP
□ Login attempts
□ Remote Login attempts
□ Reboots
□ WAN Status

Enable E-Mail Logs

Do you want logs to be emailed to you?
● Yes ○ No

E-Mail Server Address:
Return E-Mail Address:
Send to E-Mail Address :
● No Authentication
○ Login Plain ○ CRAM-MD5
User Name:
Password:
□ Respond to Identd from SMTP Server

Send E-mail logs by Schedule

Unit: Weekly
Day: Sunday
Time: 1:00 ● a.m. ○ p.m.

Enable SysLogs

Do you want to enable syslog?
● Yes ○ No

SysLog Server:
SysLog Facility: Local0

Figure 4-10

5. **Enable E-Mail Logs.** Check the **Yes** radio box if you wish to receive e-mail logs from the firewall.

6. **Enter your E-Mail Address information.** If you enabled e-mail notification, these boxes cannot be blank.

    - Enter the **E-Mail Server Address** of your ISP’s outgoing (SMTP) mail server (such as mail.myISP.com). You may be able to find this information in the configuration menu of your e-mail program.

- Enter the **Return E-Mail Address** to which logs and alerts are sent. This e-mail address will also be used as the Send To E-mail address. If you leave this box blank, log and alert messages will not be sent via e-mail.

7. If the SMTP server requires authentication before accepting connections, select either **Login Plain** or **CRAM-MD5** and enter the **User Name** and **Password** to be used for authentication. To disable authentication, select the **No Authentication** radio box (default).
8. Check the **Respond to Identd from SMTP Server** radio box to configure the router to respond to an IDENT request from the SMTP server.
9. In the **Send logs according to this schedule** section, you can specify that logs are sent to you according to a schedule. From the **Unit** pull-down menu, select to receive logs **Never**, **Hourly**, **Daily**, or **Weekly.** Depending on your selection, specify:
   - **Day** for sending log
     Relevant when the log is sent weekly or daily.
   - **Time** for sending log
     Relevant when the log is sent daily or weekly.
10. If you want the router to send logs to a SysLog server, select the **Yes** radio box in the **Enable SysLogs** section and input the following fields:
    - **a.** SysLog Server. Enter the IP address or Internet Name of the SysLog server.
    - **b.** SysLog Facility. Select the appropriate syslog facility (Local0 to Local7).
11. Click **Apply** to save your settings.

> **Note:** You can configure the firewall to send system logs to an external PC that is running a syslog logging program. Logging programs are available for Windows, Macintosh, and Linux computers.

The firewall logs security-related events such as denied incoming and outgoing service requests, hacker probes, and administrator logins. If you enable content filtering in the Block Sites menu, the Log page will also show you when someone on your network tried to access a blocked site. If you enabled e-mail notification, you will receive these logs in an e-mail message. If you don't have e-mail notification enabled, you can view the logs, as well as e-mail the logs by clicking the **View Log** link on the Firewall Logs & E-mail screen.

Log entries are described in Table 4-1

Table 4-1. Log entry descriptions

Field	Description
Date and Time	The date and time the log entry was recorded.
Description or Action	The type of event and what action was taken if any.
Source IP	The IP address of the initiating device for this log entry.
Source port and interface	The service port number of the initiating device, and whether it originated from the LAN or WAN.
Destination	The name or IP address of the destination device or Web site.
Destination port and interface	The service port number of the destination device, and whether it’s on the LAN or WAN.

Log action buttons are described in Table 4-2

Table 4-2. Log action buttons

Button	Description
Refresh	Refresh the log screen.
Clear Log	Clear the log entries.
Send Log	Email the log immediately.

Chapter 5
Basic Virtual Private Networking

This chapter describes how to use the virtual private networking (VPN) features of the VPN firewall. VPN communications paths are called tunnels. VPN tunnels provide secure, encrypted communications between your local network and a remote network or computer.

The VPN information is organized as follows:

- "Overview of VPN Configuration" on page 5-2 provides an overview of the two most common VPN configurations: client-to-gateway and gateway-to-gateway.
- "Planning a VPN" on page 5-3 provides the VPN Committee (VPNC) recommended default parameters set by the VPN Wizard.
- "VPN Tunnel Configuration" on page 5-4 summarizes the two ways to configure a VPN tunnel: VPN Wizard (recommended for most situations) and Advanced (see Chapter 6, "Advanced Virtual Private Networking).
- "Setting Up a Client-to-Gateway VPN Configuration" on page 5-5 provides the steps needed to configure a VPN tunnel between a remote PC and a network gateway using the VPN Wizard and the NETGEAR ProSafe VPN Client.
- "Setting Up a Gateway-to-Gateway VPN Configuration" on page 5-19 provides the steps needed to configure a VPN tunnel between two network gateways using the VPN Wizard.
- "Activating a VPN Tunnel" on page 5-23 provides the step-by-step procedures for activating, verifying, deactivating, and deleting a VPN tunnel once the VPN tunnel has been configured.
- Chapter 6, "Advanced Virtual Private Networking" provides the steps needed to configure VPN tunnels when there are special circumstances and the VPNC recommended defaults of the VPN Wizard are inappropriate.
- Appendix B, "Related Documents" has a link to "Virtual Private Networking (VPN)" which discusses Virtual Private Networking (VPN) Internet Protocol security (IPSec). IPSec is one of the most complete, secure, and commercially available, standards-based protocols developed for transporting data.
- Appendix C, "VPN Configuration of NETGEAR FVG318" presents a case study on how to configure a secure IPSec VPN tunnel from a NETGEAR FVG318 to a FVL328. This case study follows the VPN Consortium interoperability profile guidelines (found at *http://www.vpnc.org/InteropProfiles/Interop-01.html*).

Overview of VPN Configuration

Two common scenarios for configuring VPN tunnels are between a remote personal computer and a network gateway and between two or more network gateways. The FVG318 supports both of these types of VPN configurations. The VPN firewall supports up to eight concurrent tunnels.

Client-to-Gateway VPN Tunnels

Client-to-gateway VPN tunnels provide secure access from a remote PC, such as a telecommuter connecting to an office network (see Figure 5-1).

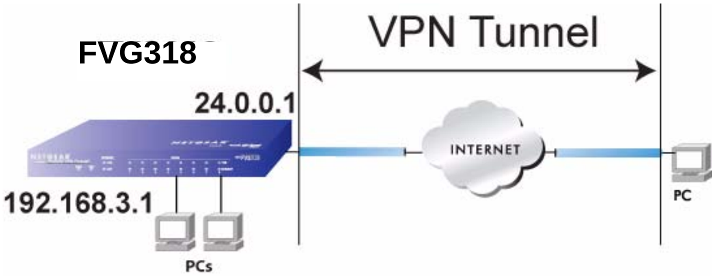


Figure 5-1

A VPN client access allows a remote PC to connect to your network from any location on the Internet. In this case, the remote PC is one tunnel endpoint, running the VPN client software. The VPN firewall on your network is the other tunnel endpoint. See "Setting Up a Client-to-Gateway VPN Configuration" on page 5-5 to set up this configuration.

Gateway-to-Gateway VPN Tunnels

Gateway-to-gateway VPN tunnels provide secure access between networks, such as a branch or home office and a main office (see Figure 5-2).

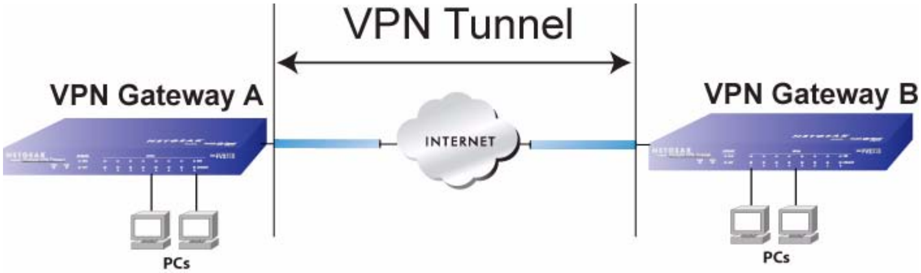


Figure 5-2

A VPN between two or more NETGEAR VPN-enabled firewalls is a good way to connect branch or home offices and business partners over the Internet. VPN tunnels also enable access to network resources across the Internet. In this case, use FVG318s on each end of the tunnel to form the VPN tunnel end points. See "Setting Up a Gateway-to-Gateway VPN Configuration" on page 5-19 to set up this configuration.

Planning a VPN

To set up a VPN connection, you must configure each endpoint with specific identification and connection information describing the other endpoint. You must configure the outbound VPN settings on one end to match the inbound VPN settings on other end, and vice versa.

This set of configuration information defines a security association (SA) between the two VPN endpoints. When planning your VPN, you must make a few choices first:

- Will the local end be any device on the LAN, a portion of the local network (as defined by a subnet or by a range of IP addresses), or a single PC?
- Will the remote end be any device on the remote LAN, a portion of the remote network (as defined by a subnet or by a range of IP addresses), or a single PC?
- Will either endpoint use Fully Qualified Domain Names (FQDNs)? Many DSL accounts are provisioned with DHCP addressing, where the IP address of the WAN port can change from time to time. Under these circumstances, configuring the WAN port with a dynamic DNS (DynDNS) service provider simplifies the configuration task. When DynDNS is configured on the WAN port, configure the VPN using FDQN.

  FQDNs supplied by Dynamic DNS providers can allow a VPN endpoint with a dynamic IP address to initiate or respond to a tunnel request. Otherwise, the side using a dynamic IP address must always be the initiator.
- What method will you use to configure your VPN tunnels?
  - The VPN Wizard using VPNC defaults (see Table 5-1)
  - Advanced methods (see Chapter 6, "Advanced Virtual Private Networking")

Table 5-1. Parameters recommended by the VPNC and used in the VPN Wizard

Parameter	Factory Default
Secure Association	Main Mode
Authentication Method	Pre-shared Key
Encryption Method	3DES

Table 5-1. Parameters recommended by the VPNC and used in the VPN Wizard

Parameter	Factory Default
Authentication Protocol	SHA-1
Diffie-Hellman (DH) Group	Group 2 (1024 bit)
Key Life	8 hours
IKE Life Time	24 hours
NETBIOS	Enabled

- What level of IPSec VPN encryption will you use?
  - DE – The Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56 bit key. Faster but less secure than 3DES.
  - 3DES – (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.
  - AES
- What level of authentication will you use?
  - MDS – 128 bits, faster but less secure.
  - SHA-1 – 160 bits, slower but more secure.

➡ **Note:** NETGEAR publishes additional interoperability scenarios with various gateway and client software products.

VPN Tunnel Configuration

There are two tunnel configurations and three ways to configure them:

- Use the VPN Wizard to configure a VPN tunnel (recommended for most situations):
  - See "Setting Up a Client-to-Gateway VPN Configuration" on page 5-5.
  - See "Setting Up a Gateway-to-Gateway VPN Configuration" on page 5-19.
- See Chapter 6, "Advanced Virtual Private Networking" when the VPN Wizard and its VPNC defaults (see Table 5-1 on page 5-4) are not appropriate for your special circumstances.

Setting Up a Client-to-Gateway VPN Configuration

Setting up a VPN between a remote PC running the NETGEAR ProSafe VPN Client and a network gateway (see Figure 5-3) involves the following two steps:

- "Step 1: Configuring the Client-to-Gateway VPN Tunnel on the FVG318" on page 5-5 uses the VPN Wizard to configure the VPN tunnel between the remote PC and network gateway.
- "Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC" on page 5-7 configures the NETGEAR ProSafe VPN Client endpoint.

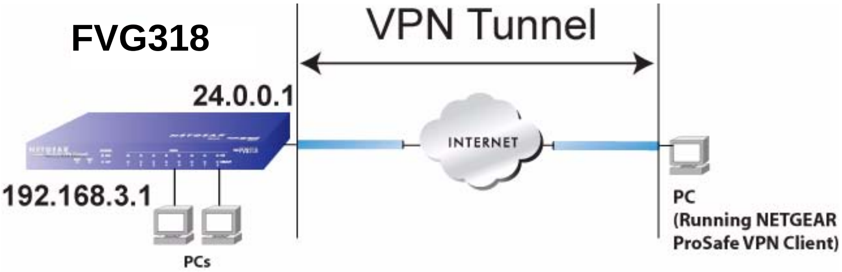


Figure 5-3

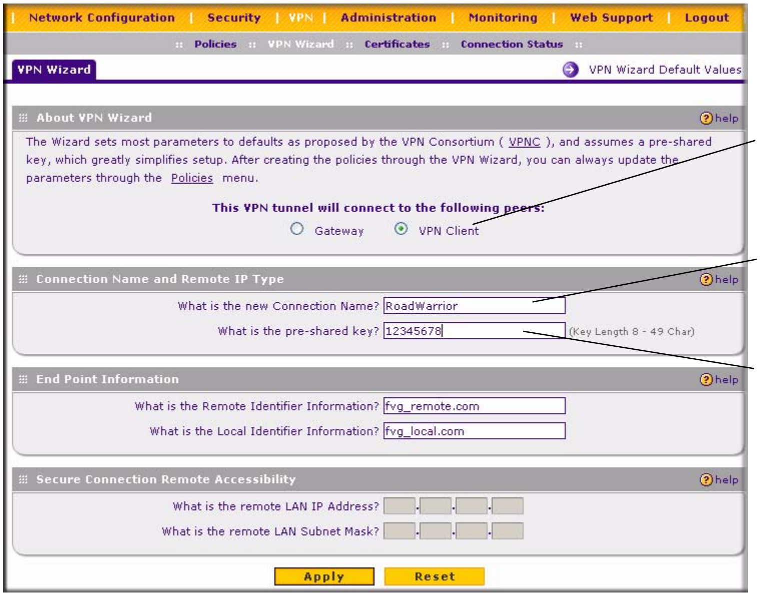
Step 1: Configuring the Client-to-Gateway VPN Tunnel on the FVG318

➡	**Note:** This section uses the VPN Wizard to set up the VPN tunnel using the VPNC default parameters listed in Table 5-1 on page 5-4. If you have special requirements not covered by these VPNC-recommended parameters, refer to Chapter 6, "Advanced Virtual Private Networking" to set up the VPN tunnel.

Follow this procedure to configure a client-to-gateway VPN tunnel using the VPN Wizard.

1. Log in to the FVG318 at its LAN address of **http://192.168.0.1** with its default user name of **admin** and password of **password**.

2. Select **VPN > VPN Wizard** from the menu. The WPN Wizard screen will display.


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
Policies :: VPN Wizard :: Certificates :: Connection Status ::
VPN Wizard
VPN Wizard Default Values
help
Apply
Reset

About VPN Wizard

The Wizard sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a pre-shared key, which greatly simplifies setup. After creating the policies through the VPN Wizard, you can always update the parameters through the Policies menu.

This VPN tunnel will connect to the following peers:

○ Gateway ● VPN Client

Connection Name and Remote IP Type

What is the new Connection Name? RoadWarrior

What is the pre-shared key? 12345678 (Key Length 8 - 49 Char)

End Point Information

What is the Remote Identifier Information? fvg_remote.com

What is the Local Identifier Information? fvg_local.com

Secure Connection Remote Accessibility

What is the remote LAN IP Address? . . .

What is the remote LAN Subnet Mask? . . .

Select the radio button: **A remote VPN client (single PC)**

Enter the new Connection Name: (**RoadWarrior** in this example)

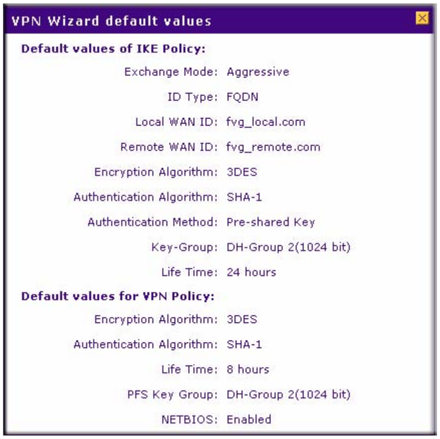
Enter the pre-shared key: (**12345678** in this example)

Figure 5-4

3. Check the VPN Client radio button and enter the Connection Name and the pre-shared key. The End Point Information will be populated automatically for access by remote PCs running VPN client software.

⇨	**Note:** The Connection Name is arbitrary and is used for management and identification purposes only.

4. Click the VPN Wizard Default Values link on the VPN Wizard screen to display the VPN default values shown below. The Wizard sets most parameters to defaults as proposed by the VPN Consortium.



VPN Wizard default values

Default values of IKE Policy:

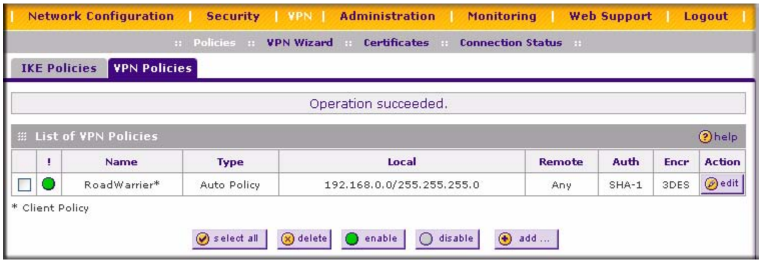
Exchange Mode:	Aggressive
ID Type:	FQDN
Local WAN ID:	fvg_local.com
Remote WAN ID:	fvg_remote.com
Encryption Algorithm:	3DES
Authentication Algorithm:	SHA-1
Authentication Method:	Pre-shared Key
Key-Group:	DH-Group 2(1024 bit)
Life Time:	24 hours

Default values for VPN Policy:

Encryption Algorithm:	3DES
Authentication Algorithm:	SHA-1
Life Time:	8 hours
PFS Key Group:	DH-Group 2(1024 bit)
NETBIOS:	Enabled

Figure 5-5

5. Click **Apply** on the VPN Wizard screen to complete the configuration procedure. The VPN Policies screen will display showing that the new tunnel is enabled.



Operation succeeded.

List of VPN Policies

	!	Name	Type	Local	Remote	Auth	Encr	Action
□	●	RoadWarrier*	Auto Policy	192.168.0.0/255.255.255.0	Any	SHA-1	3DES	edit

* Client Policy

Figure 5-6

To view or modify the tunnel settings, click **Edit**.

To enable/disable the tunnel, select the checkbox and click **Enable** or **Disable.**

Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC

This procedure describes how to configure the NETGEAR ProSafe VPN Client. This example assumes the PC running the client has a dynamically assigned IP address.

The PC must have the NETGEAR ProSafe VPN Client program installed that supports IPSec. Go to the NETGEAR Web site (*http://www.netgear.com*) and select VPN01L_VPN05L in the Product Quick Find drop-down menu for information on how to purchase the NETGEAR ProSafe VPN Client.

➡ **Note:** Before installing the NETGEAR ProSafe VPN Client software, be sure to turn off any virus protection or firewall software you may be running on your PC.

1. Install the NETGEAR ProSafe VPN Client on the remote PC and reboot.

a. You may need to insert your Windows CD to complete the installation.

b. If you do not have a modem or dial-up adapter installed in your PC, you may see the warning message stating "The NETGEAR ProSafe VPN Component requires at least one dial-up adapter be installed." You can disregard this message.

c. Install the IPSec Component. You may have the option to install either the VPN Adapter or the IPSec Component or both. The VPN Adapter is not necessary.

d. The system should show the ProSafe icon (S) in the system tray after rebooting.

e. Double-click the system tray icon to open the Security Policy Editor.

2. Add a new connection.

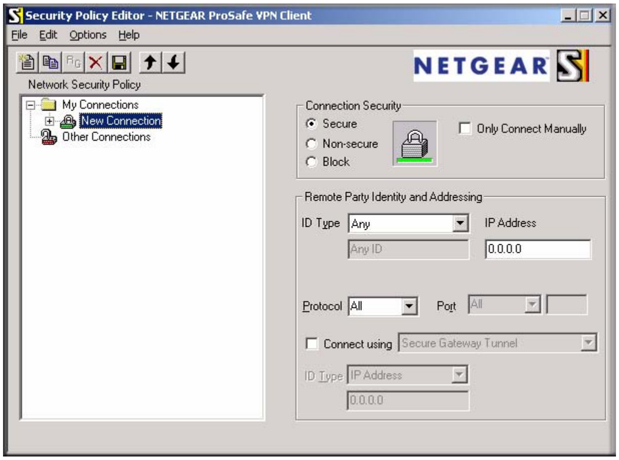
➡ **Note:** The procedure in this section explains how to create a new security policy from scratch. For the procedure on how to import an existing security policy that has already been created on another client running the NETGEAR ProSafe VPN Client, see "Transferring a Security Policy to Another Client" on page 5-17.

a. Run the NETGEAR ProSafe Security Policy Editor program and create a VPN Connection.

b. From the Edit menu of the Security Policy Editor, click **Add**, then **Connection**. A "New Connection" listing appears in the list of policies. Rename the "New Connection" so that it matches the Connection Name you entered in the VPN Settings of the FVG318 on LAN A.

Note: In this example, the Connection Name used on the client side of the VPN tunnel is **NETGEAR_VPN_router** and it does not have to match the **RoadWarrior** Connection Name used on the gateway side of the VPN tunnel (see Figure 5-8) because Connection Names are unrelated to how the VPN tunnel functions.

Tip: Choose Connection Names that make sense to the people using and administrating the VPN.



Network Security Policy
- My Connections
  - New Connection
- Other Connections

Connection Security
● Secure
○ Non-secure
○ Block
□ Only Connect Manually

Remote Party Identity and Addressing
ID Type: Any
Any ID
IP Address: 0.0.0.0
Protocol: All
Port: All
□ Connect using: Secure Gateway Tunnel
ID Type: IP Address
0.0.0.0

Figure 5-7

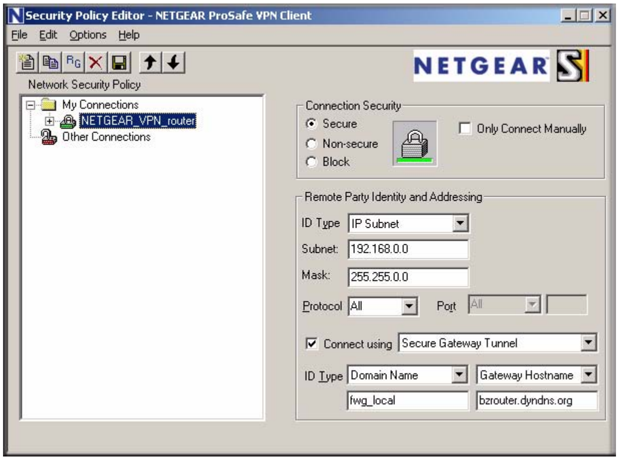
3. Enter the connection settings for the new connection:
   a. Select Secure in the Connection Security check box
   b. Select IP Subnet in the ID Type menu.

      In this example, type **192.168.0.0** in the Subnet field as the network address of the FVG318.
   c. Enter **255.255.255.0** in the Mask field as the LAN Subnet Mask of the FVG318.
   d. Select All in the Protocol menu to allow all traffic through the VPN tunnel.
   e. Select the Connect using Secure Gateway Tunnel check box.

f. Select Domain Name in the ID Type menu below the check box.

g. Enter the public WAN IP Domain Name of the FVG318 in the field directly below the ID Type menu. In this example, **fvg_local.com** would be used.

The resulting Connection Settings are shown in Figure 5-8.



Connection Security
● Secure
○ Non-secure
○ Block
□ Only Connect Manually

Remote Party Identity and Addressing
ID Type: IP Subnet
Subnet: 192.168.0.0
Mask: 255.255.0.0
Protocol: All
Port: All
☑ Connect using: Secure Gateway Tunnel
ID Type: Domain Name | Gateway Hostname
fwg_local | bzrouter.dyndns.org

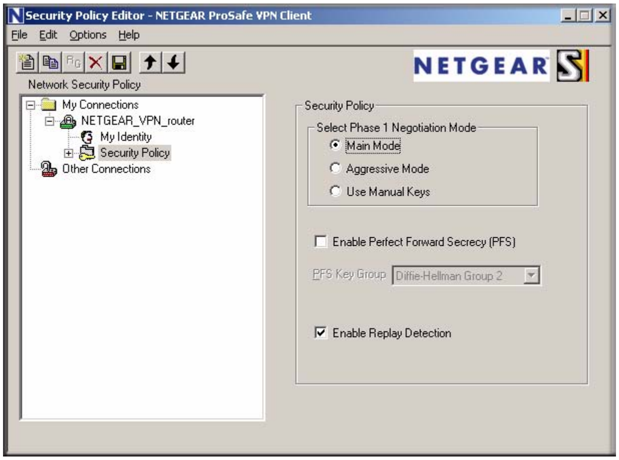
Figure 5-8

4. Configure the Security Policy in the NETGEAR ProSafe VPN Client software.

a. In the Network Security Policy list, expand the new connection by double clicking its name or clicking on the “+” symbol. My Identity and Security Policy subheadings appear below the connection name.

b. Click on the **Security Policy** subheading to show the Security Policy menu.

c. Select the Main Mode in the Select Phase 1 Negotiation Mode check box.



Security Policy

Select Phase 1 Negotiation Mode

● Main Mode

○ Aggressive Mode

○ Use Manual Keys

☐ Enable Perfect Forward Secrecy (PFS)

PFS Key Group: Diffie-Hellman Group 2

☑ Enable Replay Detection

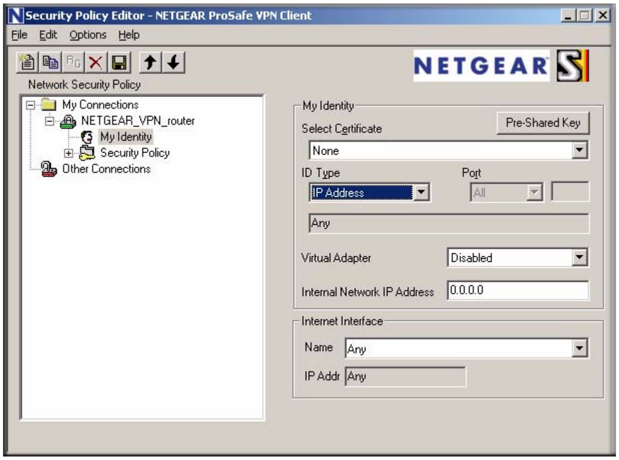
Figure 5-9

5. Configure the VPN Client Identity. Provide information about the remote VPN client PC. You will need to provide:

   – The Pre-Shared Key that you configured in the FVG318.

   – Either a fixed IP address or a “fixed virtual” IP address of the VPN client PC.

   a. In the Network Security Policy list on the left side of the Security Policy Editor window, click on **My Identity**.



My Identity

Select Certificate: None

ID Type: IP Address

Port: All

Any

Virtual Adapter: Disabled

Internal Network IP Address: 0.0.0.0

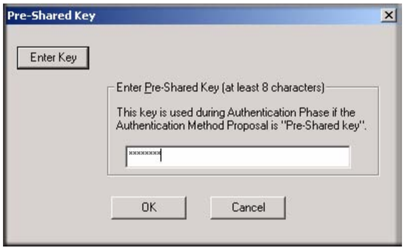
Internet Interface

Name: Any

IP Addr: Any

Figure 5-10

- **b.** Choose None in the Select Certificate box.
- **c.** Select IP Address in the ID Type box. If you are using a virtual fixed IP address, enter this address in the Internal Network IP Address box. Otherwise, leave this box empty.
- **d.** In the Internet Interface box, select the adapter you use to access the Internet. Select PPP Adapter in the Name menu if you have a dial-up Internet account. Select your Ethernet adapter if you have a dedicated Cable or DSL line. You may also choose Any if you will be switching between adapters or if you have only one adapter.
- **e.** Click the **Pre-Shared Key** button. In the Pre-Shared Key dialog box, click the **Enter Key** button. Enter the FVG318’s Pre-Shared Key and click **OK**. In this example, **12345678** is entered. This field is case sensitive.



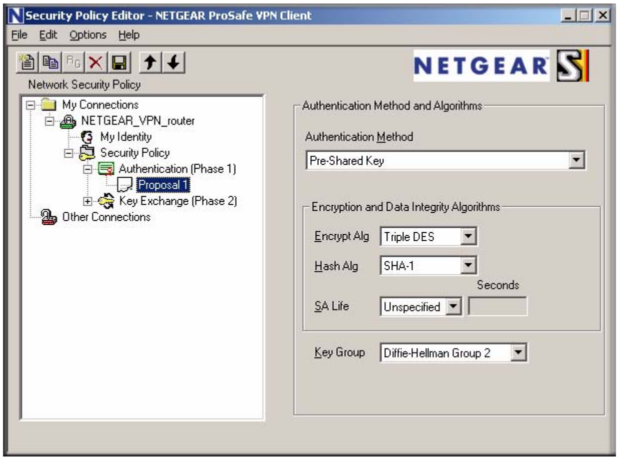
Enter Pre-Shared Key (at least 8 characters)

This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".

****

Figure 5-11

6. Configure the VPN Client Authentication Proposal. Provide the type of encryption (DES or 3DES) to be used for this connection. This selection must match your selection in the FVG318 configuration.
   - **a.** In the Network Security Policy list on the left side of the Security Policy Editor window, expand the Security Policy heading by double clicking its name or clicking on the “+” symbol.
   - **b.** Expand the Authentication subheading by double clicking its name or clicking on the “+” symbol. Then select Proposal 1 below Authentication.



Authentication Method: Pre-Shared Key

Encrypt Alg: Triple DES

Hash Alg: SHA-1

SA Life: Unspecified

Key Group: Diffie-Hellman Group 2

Figure 5-12

c. In the Authentication Method menu, select Pre-Shared key.

d. In the Encrypt Alg menu, select the type of encryption. In this example, use Triple DES.

e. In the Hash Alg menu, select SHA-1.

f. In the SA Life menu, select Unspecified.

g. In the Key Group menu, select Diffie-Hellman Group 2.

7. Configure the VPN Client Key Exchange Proposal. Provide the type of encryption (DES or 3DES) to be used for this connection. This selection must match your selection in the FVG318 configuration.

   a. Expand the Key Exchange subheading by double clicking its name or clicking on the “+” symbol. Then select Proposal 1 below Key Exchange.

   b. In the SA Life menu, select Unspecified.

   c. In the Compression menu, select None.

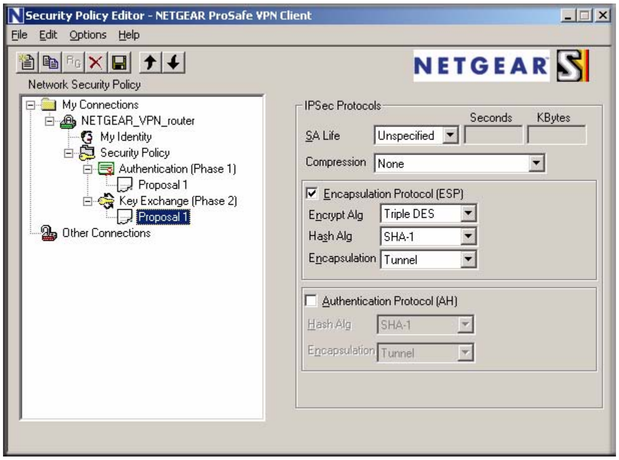
   d. Check the Encapsulation Protocol (ESP) check box.

   e. In the Encrypt Alg menu, select the type of encryption. In this example, use Triple DES.

   f. In the Hash Alg menu, select SHA-1.

   g. In the Encapsulation menu, select Tunnel.

   h. Leave the Authentication Protocol (AH) check box unchecked.



Network Security Policy

- My Connections
  - NETGEAR_VPN_router
    - My Identity
    - Security Policy
      - Authentication (Phase 1)
        - Proposal 1
      - Key Exchange (Phase 2)
        - Proposal 1
- Other Connections

IPSec Protocols

		Seconds	KBytes
SA Life	Unspecified		
Compression	None		

☑ Encapsulation Protocol (ESP)

Encrypt Alg	Triple DES
Hash Alg	SHA-1
Encapsulation	Tunnel

☐ Authentication Protocol (AH)

Hash Alg	SHA-1
Encapsulation	Tunnel

Figure 5-13

8. Save the VPN Client Settings. From the File menu at the top of the Security Policy Editor window, click **Save**.

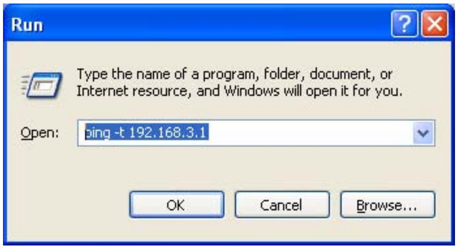
After you have configured and saved the VPN client information, your PC will automatically open the VPN connection when you attempt to access any IP addresses in the range of the remote VPN firewall's LAN.

To check the VPN connection.

Initiate a request from the remote PC to the FVG318's network by using the "Connect" option in the NETGEAR ProSafe menu bar. The NETGEAR ProSafe client will report the results of the attempt to connect. Since the remote PC has a dynamically assigned WAN IP address, it must initiate the request.

To perform a ping test using our example, start from the remote PC:

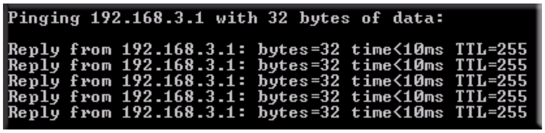
1. Establish an Internet connection from the PC.
2. On the Windows tasteable, click the **Start** button, and then click **Run**.
3. Type `ping -t 192.168.3.1` , and then click **OK**.



Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
ping -t 192.168.3.1
OK
Cancel
Browse...

Figure 5-14

This will cause a continuous ping to be sent to the first FVG318. After between several seconds and two minutes, the ping response should change from “timed out” to “reply”, as shown below.



```
Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time<10ms TTL=255
Reply from 192.168.3.1: bytes=32 time<10ms TTL=255
Reply from 192.168.3.1: bytes=32 time<10ms TTL=255
Reply from 192.168.3.1: bytes=32 time<10ms TTL=255
Reply from 192.168.3.1: bytes=32 time<10ms TTL=255
```

Figure 5-15

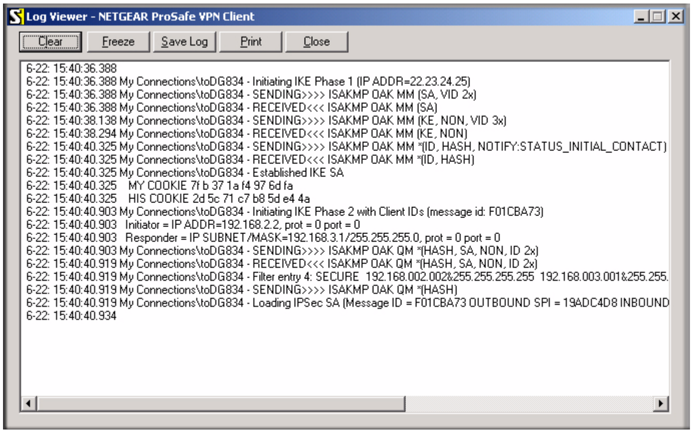
Once the connection is established, you can open the browser of the PC and enter the LAN IP address of the remote FVG318. After a short wait, you should see the login screen of the VPN Firewall Router (unless another PC already has the FVG318 management interface open).

Monitoring the Progress and Status of the VPN Client Connection

Information on the progress and status of the VPN client connection can be viewed by opening the NETGEAR ProSafe Log Viewer.

To launch this function:

1. Click the Window**s Start** button, and select **Programs > NETGEAR ProSafe VPN Client > Log Viewer**. The Log Viewer screen for a similar successful connection is shown below:

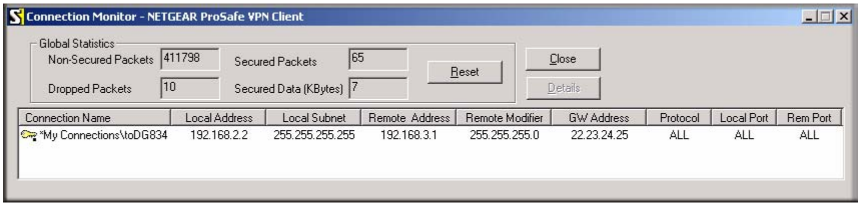


```
6-22: 15:40:36.388
6-22: 15:40:36.388 My Connections\toDG834 - Initiating IKE Phase 1 (IP ADDR=22.23.24.25)
6-22: 15:40:36.388 My Connections\toDG834 - SENDING>>>> ISAKMP OAK MM (SA, VID 2x)
6-22: 15:40:36.388 My Connections\toDG834 - RECEIVED<<< ISAKMP OAK MM (SA)
6-22: 15:40:38.138 My Connections\toDG834 - SENDING>>>> ISAKMP OAK MM (KE, NON, VID 3x)
6-22: 15:40:38.294 My Connections\toDG834 - RECEIVED<<< ISAKMP OAK MM (KE, NON)
6-22: 15:40:40.325 My Connections\toDG834 - SENDING>>>> ISAKMP OAK MM *(ID, HASH, NOTIFY:STATUS_INITIAL_CONTACT)
6-22: 15:40:40.325 My Connections\toDG834 - RECEIVED<<< ISAKMP OAK MM *(ID, HASH)
6-22: 15:40:40.325 My Connections\toDG834 - Established IKE SA
6-22: 15:40:40.325   MY COOKIE 7f b 37 1a f4 97 6d fa
6-22: 15:40:40.325   HIS COOKIE 2d 5c 71 c7 b8 5d e4 4a
6-22: 15:40:40.903 My Connections\toDG834 - Initiating IKE Phase 2 with Client IDs (message id: F01CBA73)
6-22: 15:40:40.903  Initiator = IP ADDR=192.168.2.2, prot = 0 port = 0
6-22: 15:40:40.903  Responder = IP SUBNET/MASK=192.168.3.1/255.255.255.0, prot = 0 port = 0
6-22: 15:40:40.903 My Connections\toDG834 - SENDING>>>> ISAKMP OAK QM *(HASH, SA, NON, ID 2x)
6-22: 15:40:40.919 My Connections\toDG834 - RECEIVED<<< ISAKMP OAK QM *(HASH, SA, NON, ID 2x)
6-22: 15:40:40.919 My Connections\toDG834 - Filter entry 4: SECURE  192.168.002.002&255.255.255.255  192.168.003.001&255.255.
6-22: 15:40:40.919 My Connections\toDG834 - SENDING>>>> ISAKMP OAK QM *(HASH)
6-22: 15:40:40.919 My Connections\toDG834 - Loading IPSec SA (Message ID = F01CBA73 OUTBOUND SPI = 19ADC4D8 INBOUND
6-22: 15:40:40.934
```

Figure 5-16

> **Note:** Use the active VPN tunnel information and pings to determine whether a failed connection is due to the VPN tunnel or some reason outside the VPN tunnel.

2. The Connection Monitor screen for a similar connection is shown below:



Global Statistics

Non-Secured Packets	411798	Secured Packets	65
Dropped Packets	10	Secured Data (KBytes)	7

Connection Name	Local Address	Local Subnet	Remote Address	Remote Modifier	GW Address	Protocol	Local Port	Rem Port
*My Connections\toDG834	192.168.2.2	255.255.255.255	192.168.3.1	255.255.255.0	22.23.24.25	ALL	ALL	ALL

Figure 5-17

In this example you can see the following:

- The FVG318 has a public IP WAN address of 22.23.24.25.
- The FVG318 has a LAN IP address of 192.168.3.1.
- The VPN client PC has a dynamically assigned address of 192.168.2.2.

While the connection is being established, the Connection Name field in this menu will say “SA” before the name of the connection. When the connection is successful, the “SA” will change to the yellow key symbol shown in the illustration above.

Note: While your PC is connected to a remote LAN through a VPN, you might not have normal Internet access. If this is the case, you will need to close the VPN connection in order to have normal Internet access.

Transferring a Security Policy to Another Client

This section explains how to export and import a security policy as an **.spd** file so that an existing NETGEAR ProSafe VPN Client configuration can be copied to other PCs running the NETGEAR ProSafe VPN Client.

The following procedure (Figure 5-18) enables you to export a security policy as an **.spd** file.

To export a security policy:

1. Select **Export Security Policy** from the **File** pull-down menu.

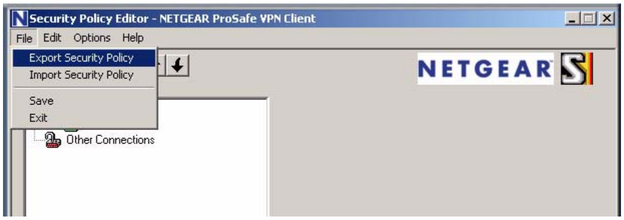
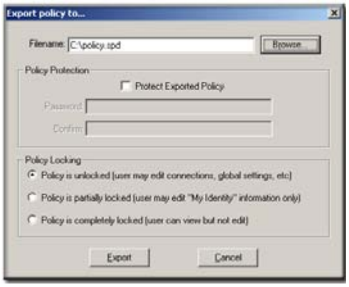


Figure 5-18

2. Once you decide the name of the file and directory where you want to store the client policy, click **Export.**

   In this example, the exported policy is named **policy.spd** and is being stored on the C drive.



Export policy to...

Filename: C:\policy.spd

Policy Protection

□ Protect Exported Policy

Password:

Confirm:

Policy Locking

● Policy is unlocked (user may edit connections, global settings, etc)

○ Policy is partially locked (user may edit "My Identity" information only)

○ Policy is completely locked (user can view but not edit)

Figure 5-19

To import an existing Security Policy:

1. Invoke the NETGEAR ProSafe VPN Client and select **Import Security Policy** from the **File** pull-down menu.

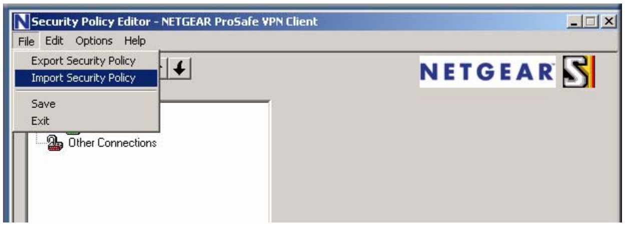
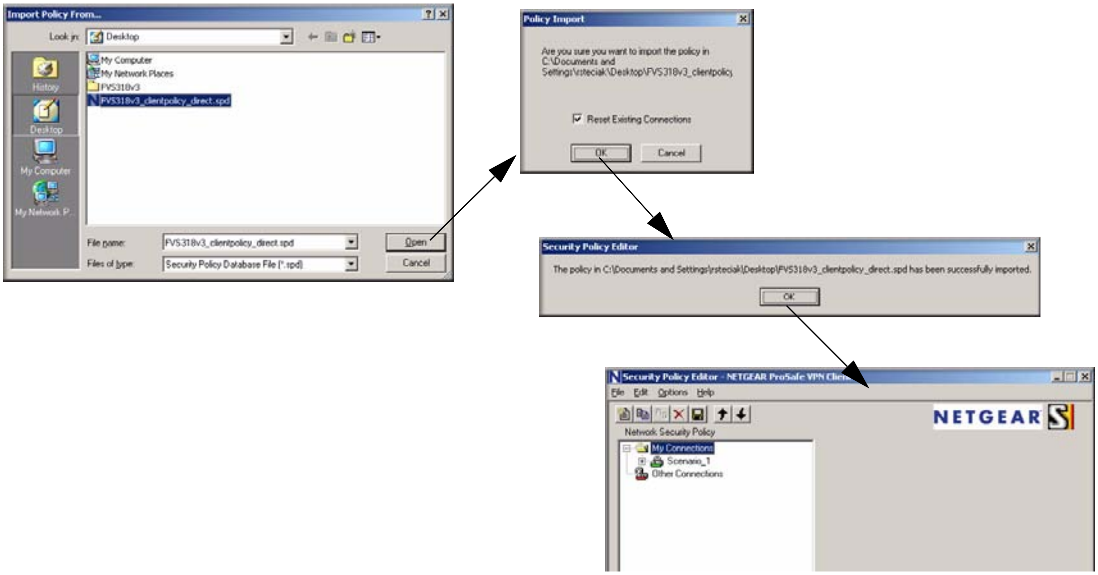


Figure 5-20

2. Select the security policy to import.

   In this example, the security policy file is named **FVS318v3_clientpolicy_direct.spd** and located on the Desktop.



Look in: Desktop

File name: FVS318v3_clientpolicy_direct.spd

Files of type: Security Policy Database File (*.spd)

Are you sure you want to import the policy in C:\Documents and Settings\rsteciak\Desktop\FVS318v3_clientpolicy

☑ Reset Existing Connections

The policy in C:\Documents and Settings\rsteciak\Desktop\FVS318v3_clientpolicy_direct.spd has been successfully imported.

Figure 5-21

The security policy is now imported. In this example, the connection name is **Scenario_1**

Setting Up a Gateway-to-Gateway VPN Configuration

➡	**Note:** This section uses the VPN Wizard to set up the VPN tunnel using the VPNC default parameters listed in Table 5-1 on page 5-4. If you have special requirements not covered by these VPNC-recommended parameters, refer to Chapter 6, "Advanced Virtual Private Networking" to set up the VPN tunnel.

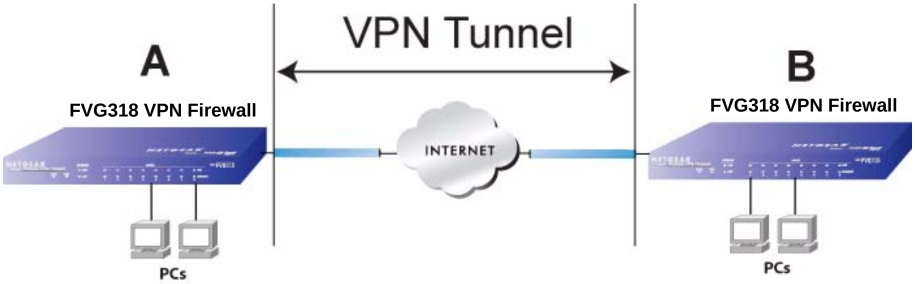


Figure 5-22

The following procedure will show how to set the LAN IPs on each FVG318 to different subnets and configure each properly for the Internet.

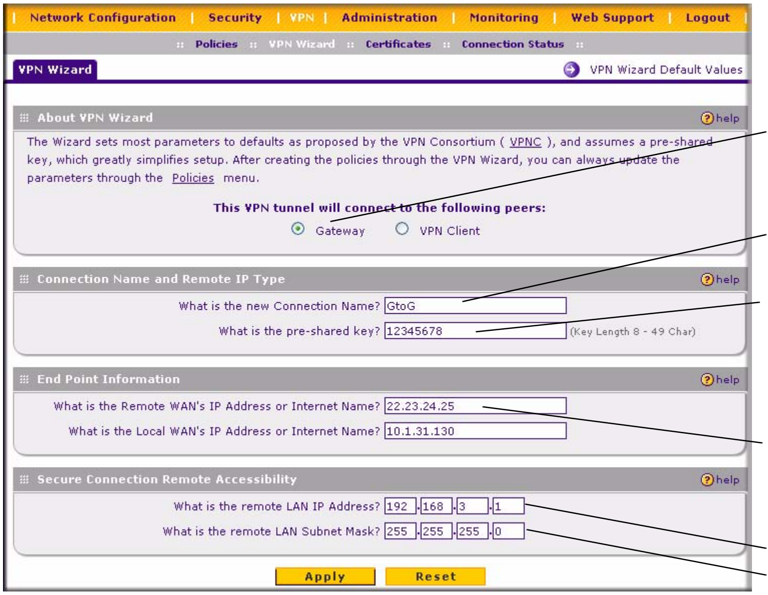
- The LAN IP address ranges of each VPN endpoint must be different. The connection will fail if both are using the NETGEAR default address range of 192.168.0.x.
- In this example, LAN A uses 192.168.0.1 and LAN B uses 192.168.3.1.

To configure a gateway-to-gateway VPN tunnel using the VPN Wizard.

1. Log in to the FVG318 on LAN A at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and password of **password**.
2. Select **VPN > VPN Wizard** from the main menu. The VPN Wizard screen will display.
3. Select the Gateway radio box in the About VPN Wizard section.
4. In the Connection Name and Remote IP Type section, enter the Connection Name and the pre-shared key.

5. In the End Point Information section, enter the Remote WANs IP Address or Internet Name and the Local WAN's IP Address or Internet Name. Both local and remote ends must be defined as either IP addresses or Internet Names (FQDNs).

> **Note:** The Local IP Address field can be left as the default address unless you are using a different IP Address or FQDN.


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Policies :: VPN Wizard :: Certificates :: Connection Status ::
VPN Wizard
VPN Wizard Default Values
help
Apply
Reset

About VPN Wizard

The Wizard sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a pre-shared key, which greatly simplifies setup. After creating the policies through the VPN Wizard, you can always update the parameters through the Policies menu.

This VPN tunnel will connect to the following peers:

● Gateway ○ VPN Client

Connection Name and Remote IP Type

What is the new Connection Name? GtoG

What is the pre-shared key? 12345678 (Key Length 8 - 49 Char)

End Point Information

What is the Remote WAN's IP Address or Internet Name? 22.23.24.25

What is the Local WAN's IP Address or Internet Name? 10.1.31.130

Secure Connection Remote Accessibility

What is the remote LAN IP Address? 192 . 168 . 3 . 1

What is the remote LAN Subnet Mask? 255 . 255 . 255 . 0

Select the radio button:
A remote VPN Gateway

Enter the new Connection Name: (**GtoG** in this example)

Enter the pre-shared key: (**12345678** in this example)

Enter the WAN IP address of the remote VPN gateway: (**22.23.24.25** in this example)

Enter the LAN IP settings of the remote VPN gateway. For example:

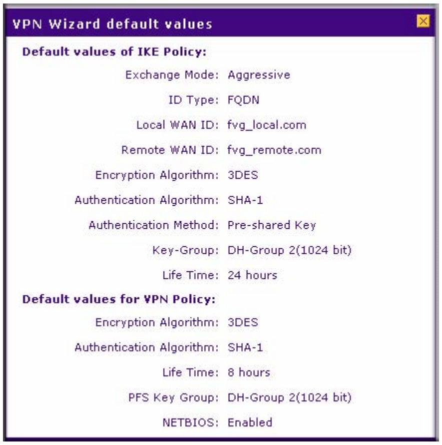
- IP Address (**192.168.3.1**)
- Subnet Mask (**255.255.255.0**)

Figure 5-23

6. In the Security Connection Remote Accessibility section, enter the remote LAN IP address and Subnet Mask at the target endpoint that can use this tunnel.

> **Note:** The IP Address range on the remote LAN must be different from the IP Address range on the local LAN.

You can view the VPNC recommended authentication and encryption settings used by the VPN Wizard by clicking the VPN Wizard Default Values link.



Default values of IKE Policy:

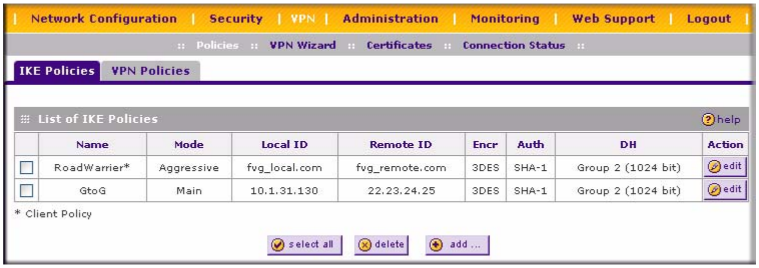
Exchange Mode:	Aggressive
ID Type:	FQDN
Local WAN ID:	fvg_local.com
Remote WAN ID:	fvg_remote.com
Encryption Algorithm:	3DES
Authentication Algorithm:	SHA-1
Authentication Method:	Pre-shared Key
Key-Group:	DH-Group 2(1024 bit)
Life Time:	24 hours

Default values for VPN Policy:

Encryption Algorithm:	3DES
Authentication Algorithm:	SHA-1
Life Time:	8 hours
PFS Key Group:	DH-Group 2(1024 bit)
NETBIOS:	Enabled

Figure 5-24

7. Click **Apply** to complete the configuration procedure. The IKE Policies menu will display the local and remote WAN connection points as shown below.



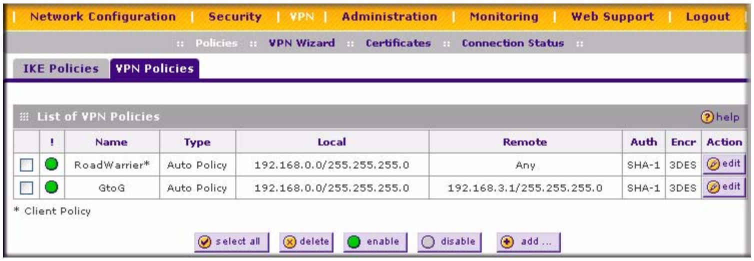
List of IKE Policies

	Name	Mode	Local ID	Remote ID	Encr	Auth	DH	Action
□	RoadWarrier*	Aggressive	fvg_local.com	fvg_remote.com	3DES	SHA-1	Group 2 (1024 bit)	edit
□	GtoG	Main	10.1.31.130	22.23.24.25	3DES	SHA-1	Group 2 (1024 bit)	edit

* Client Policy

Figure 5-25

8. Click the VPN Policy to display the VPN Policies showing that the new tunnel is enabled.



List of VPN Policies

	!	Name	Type	Local	Remote	Auth	Encr	Action
□	●	RoadWarrier*	Auto Policy	192.168.0.0/255.255.255.0	Any	SHA-1	3DES	edit
□	●	GtoG	Auto Policy	192.168.0.0/255.255.255.0	192.168.3.1/255.255.255.0	SHA-1	3DES	edit

* Client Policy

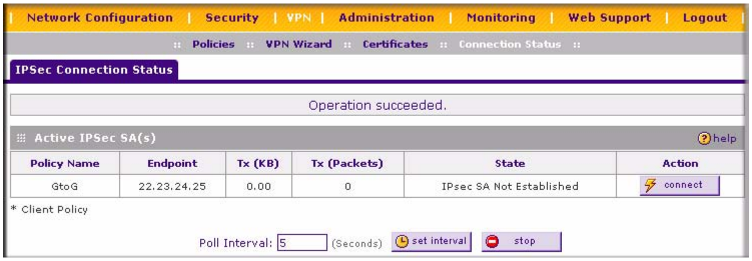
Figure 5-26

To configure a gateway-to-gateway VPN tunnel using the VPN Wizard on LAN B:.

1. Log in to the FVG318 on LAN B at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and password of **password**.
2. Repeat the VPN Wizard process for the FVG318 on LAN B. Pay special attention and use the following network settings as appropriate.
   - WAN IP of the remote VPN gateway (for example, **14.15.16.17**)
   - LAN IP settings of the remote VPN gateway:
     - – IP Address (for example, **192.168.0.1**)
     - – Subnet Mask (for example, **255.255.255.0**)
     - – Preshared Key (for example, **12345678**)
3. Use the VPN Status screen to activate the VPN tunnel by performing the following steps:

> Note: The VPN Status screen is only one of three ways to active a VPN tunnel. See "Activating a VPN Tunnel" on page 5-23 for information on the other ways.

a. Open the FVG318, open **VPN > Connection Status** to get the IPSec Connection Status screen (Figure 5-27).


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Policies :: VPN Wizard :: Certificates :: Connection Status ::
IPSec Connection Status
help
connect
set interval
stop

Operation succeeded.

Active IPSec SA(s)

Policy Name	Endpoint	Tx (KB)	Tx (Packets)	State	Action
GtoG	22.23.24.25	0.00	0	IPsec SA Not Established	connect

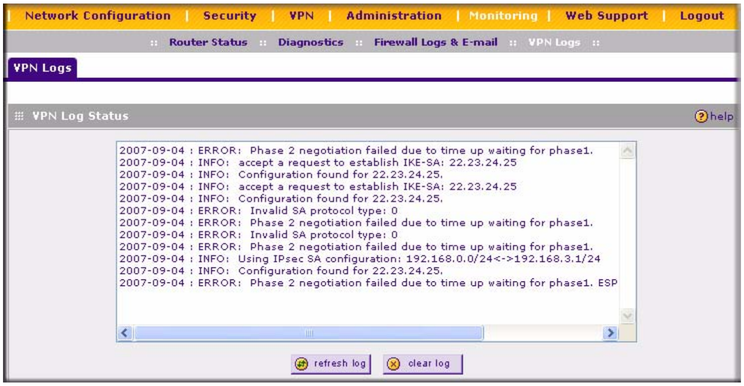
* Client Policy

Poll Interval: 5 (Seconds)

Figure 5-27

b. Click **Connect** for the VPN tunnel you want to activate.

c. Look at the VPN Logs by selecting **Monitoring < VPN Logs** to verify that the tunnel is connected.


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
:: Router Status :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
VPN Logs
VPN Log Status
help
refresh log
clear log

```
2007-09-04 : ERROR:  Phase 2 negotiation failed due to time up waiting for phase1.
2007-09-04 : INFO:  accept a request to establish IKE-SA: 22.23.24.25
2007-09-04 : INFO:  Configuration found for 22.23.24.25.
2007-09-04 : INFO:  accept a request to establish IKE-SA: 22.23.24.25
2007-09-04 : INFO:  Configuration found for 22.23.24.25.
2007-09-04 : ERROR:  Invalid SA protocol type: 0
2007-09-04 : ERROR:  Phase 2 negotiation failed due to time up waiting for phase1.
2007-09-04 : ERROR:  Invalid SA protocol type: 0
2007-09-04 : ERROR:  Phase 2 negotiation failed due to time up waiting for phase1.
2007-09-04 : INFO:  Using IPsec SA configuration: 192.168.0.0/24<->192.168.3.1/24
2007-09-04 : INFO:  Configuration found for 22.23.24.25.
2007-09-04 : ERROR:  Phase 2 negotiation failed due to time up waiting for phase1. ESP
```

Figure 5-28

Activating a VPN Tunnel

There are three ways to activate a VPN tunnel:

- Start using the VPN tunnel.
- Use the IPSec Connection Status screen.
- Activate the VPN tunnel by pinging the remote endpoint.

To use a VPN tunnel:

1. Open a Web browser.
2. Go to the URL whose IP address or IP address range is covered by the policy for that VPN tunnel.

To use the IPSec Connection Status screen to activate a VPN tunnel:

1. Log in to the VPN Firewall Router.
2. Open the FVG318 VPN > Connection Status screen to get the IPSec Connection Status screen (Figure 5-27).
3. Click **Connect** adjacent to the policy to get the VPN tunnel you want to activate.

To activate the VPN tunnel by pinging the remote endpoint, select your configuration (either client-to-gateway or gateway-to-gateway):

➡	**Note:** This section uses 192.168.3.1 for an example remote endpoint LAN IP address.

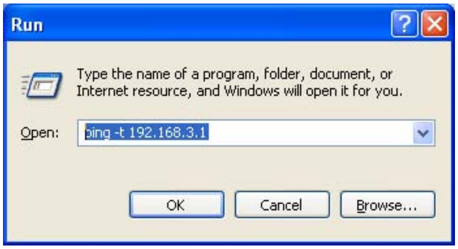
- **Client-to-Gateway Configuration** – to check the VPN Connection, you can initiate a request from the remote PC to the FVG318's network by using the "Connect" option in the NETGEAR ProSafe menu bar. The NETGEAR ProSafe client will report the results of the attempt to connect. Since the remote PC has a dynamically assigned WAN IP address, it must initiate the request.

  To perform a ping test using our example, start from the remote PC:

  a. Establish an Internet connection from the PC.

  b. On the Windows task bar, click the **Start** button, and then click **Run**.

  c. Type **ping -t 192.168.3.1** and then click **OK**.



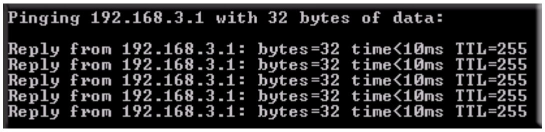
Run
?
X
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
OK
Cancel
Browse...

Open: ping -t 192.168.3.1

Figure 5-29

This will cause a continuous ping to be sent to the first FVG318. Within two minutes, the ping response should change from "timed out" to "reply."

➡	**Note:** Use **Ctrl-C** to stop the pinging.



```
Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time<10ms TTL=255
Reply from 192.168.3.1: bytes=32 time<10ms TTL=255
Reply from 192.168.3.1: bytes=32 time<10ms TTL=255
Reply from 192.168.3.1: bytes=32 time<10ms TTL=255
Reply from 192.168.3.1: bytes=32 time<10ms TTL=255
```

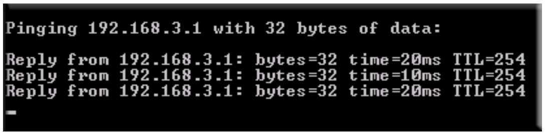
Figure 5-30

Once the connection is established, you can open the browser of the PC and enter the LAN IP address of the remote FVG318. After a short wait, you should see the login screen of the VPN Firewall Router (unless another PC already has the FVG318 management interface open).

- **Gateway-to-Gateway Configuration**. Test the VPN tunnel by pinging the remote network from a PC attached to the FVG318.

  a. Open a command prompt (**Start** -> **Run** -> **cmd**).

  b. Type **ping 192.168.3.1**.



```
Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time=20ms TTL=254
Reply from 192.168.3.1: bytes=32 time=10ms TTL=254
Reply from 192.168.3.1: bytes=32 time=20ms TTL=254
-
```

Figure 5-31

Note: The pings may fail the first time. If so, then try the pings a second time.

Verifying the Status of a VPN Tunnel

To use the VPN Logs screen to determine the status of a VPN tunnel, perform the following steps:

1. Log in to the VPN Firewall Router.

2. Open the FVG318 Monitoring > VPN Logs to get the VPN Logs screen (see Figure 5-28).

This log shows the details of recent VPN activity, including the building of the VPN tunnel. If there is a problem with the VPN tunnel, refer to the log for information about what might be the cause of the problem.

- Click **Refresh** to see the most recent entries.
- Click **Clear Log** to delete all log entries.

To Use the IPSec Connection Status screen to change the status of a VPN connection:

3. Click **VPN** > **Connection Status** (Figure 5-26) to get the IPSec Connection Status screen (Figure 5-27).

   This page lists the following data for each active VPN Tunnel.

   - **SPI –** each SA has a unique SPI (Security Parameter Index) for traffic in each direction. For Manual key exchange, the SPI is specified in the Policy definition. For Automatic key exchange, the SPI is generated by the IKE protocol.
   - **Policy Name** – The name of the VPN policy associated with this SA.
   - **Remote Endpoint** – The IP address on the remote VPN Endpoint.
   - **Tx (KB) –** The number of KBs of data transmitted over this SA.
   - **Tx (Packets) –** The number of IP packets transmitted over this SA.
   - **State –** Displays the current status of the SA for IKE policies. The status can be either Not Connected or IPSec SA Established.
   - **Action –** Click Connect to build the SA (connection) or Drop to terminate the SA (connection), as required.

   The screen refreshes automatically to display the most current status for an SA. The settings for page refresh are:

   - **Poll Interval –** Time in seconds, after which the page will automatically reload.
   - **Set Interval –** You can set a new value in the Poll Interval text field and click Set Interval to set a new interval value.
   - **Stop** – If you click Stop, the polling interval will cease.

Deactivating a VPN Tunnel

Sometimes a VPN tunnel must be deactivated for testing purposes. There are two ways to deactivate a VPN tunnel:

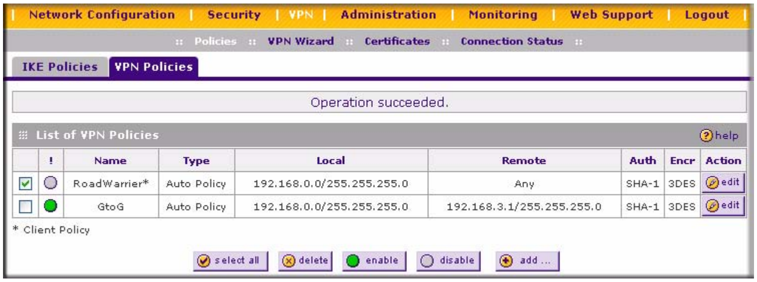
- Policy table on VPN Policies screen
- Connection Status screen

Using the Policy Table on the VPN Policies Screen to Deactivate a VPN Tunnel

To use the VPN Policies screen to deactivate a VPN tunnel:

1. Log in to the VPN Firewall Router.
2. Select **VPN** > **VPN Policies** and click the **VPN Policies** tab to get the VPN Policies screen below (Figure 5-32).

3. Select the checkbox adjacent to the policy you want to disable and click **disable.** The VPN Policy will be disabled.


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
:: Policies :: VPN Wizard :: Certificates :: Connection Status ::
IKE Policies
VPN Policies

Operation succeeded.

List of VPN Policies

	!	Name	Type	Local	Remote	Auth	Encr	Action
☑	○	RoadWarrier*	Auto Policy	192.168.0.0/255.255.255.0	Any	SHA-1	3DES	edit
□	●	GtoG	Auto Policy	192.168.0.0/255.255.255.0	192.168.3.1/255.255.255.0	SHA-1	3DES	edit

* Client Policy

select all
delete
enable
disable
add ...

Figure 5-32

Using the VPN Status Page to Deactivate a VPN Tunnel

To use the VPN Connection Status screen to deactivate a VPN tunnel:

1. Log in to the VPN Firewall Router.
2. Select the **VPN** > **Connection Status** screen. The IPSec Connection Status screen will display.
3. In the **Action** column adjacent to the VPN tunnel you want to deactivate, click **Drop.**

> **Note:** When NETBIOS is enabled (which it is in the VPNC defaults implemented by the VPN Wizard), automatic traffic will reactivate the tunnel. To prevent reactivation from happening, either disable NETBIOS or disable the policy for the tunnel (see "Using the Policy Table on the VPN Policies Screen to Deactivate a VPN Tunnel" on page 5-26).

Deleting a VPN Tunnel

To delete a VPN tunnel:

1. Log in to the VPN Firewall Router.
2. Click **VPN** > **Policies** and click the **VPN Policies** tab to display the VPN Policies screen (Figure 5-32). Select the radio button for the VPN tunnel to be deleted and click **Delete**.

Chapter 6
Advanced Virtual Private Networking

This chapter describes how to use the advanced virtual private networking (VPN) features of the VPN firewall. See Chapter 5, "Basic Virtual Private Networking" for a description on how to use the basic VPN features.

The FVG318 uses state-of-the-art firewall and security technology to facilitate controlled and actively monitored VPN connectivity. Since the FVG318 strictly conforms to IETF standards, it is interoperable with devices from major network equipment vendors.

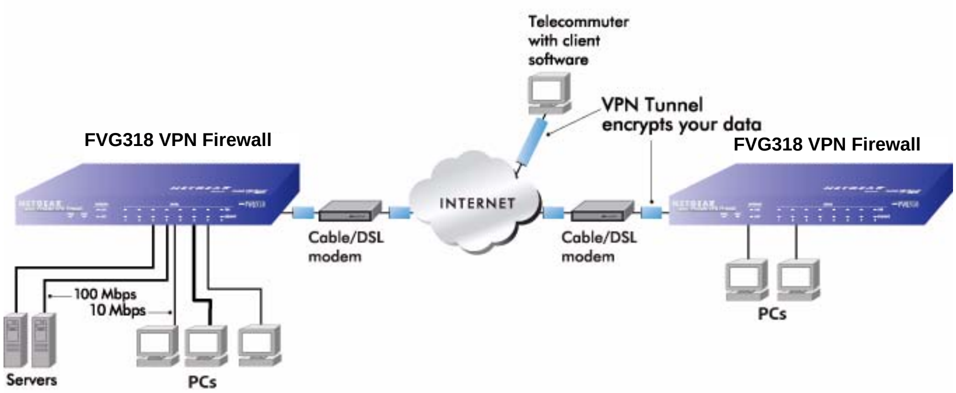


Figure 6-1

Using IKE and VPN Policies to Manage VPN Traffic

You create policy definitions to manage VPN traffic on the FVG318. There are two kinds of policies:

- **IKE Policies**. Define the authentication scheme and automatically generate the encryption keys. As an alternative option, to further automate the process, you can create an IKE policy that uses a trusted certificate authority to provide the authentication while the IKE policy still handles the encryption.

- **VPN Policies**. Apply the IKE policy to specific traffic that requires a VPN tunnel. Or, you can create a VPN policy that does not use an IKE policy but in which you manually enter all the authentication and key parameters.

Since VPN policies use IKE policies, you define the IKE policy first. The FVG318 also allows you to manually input the authentication scheme and encryption key values. In the case of manual key management there will not be any IKE policies.

In order to establish secure communication over the Internet with the remote site you need to configure matching VPN policies on both the local and remote VPN firewalls. The outbound VPN policy on one end must match to the inbound VPN policy on other end, and vice versa.

When the network traffic enters into the FVG318 from the LAN network interface, if there is no VPN policy found for a type of network traffic, then that traffic passes through without any change. However, if the traffic is selected by a VPN policy, then the IPSec authentication and encryption rules are applied to it as defined in the VPN policy.

By default, a new VPN policy is added with the least priority, that is, at the end of the VPN policy table.

Using Automatic Key Management

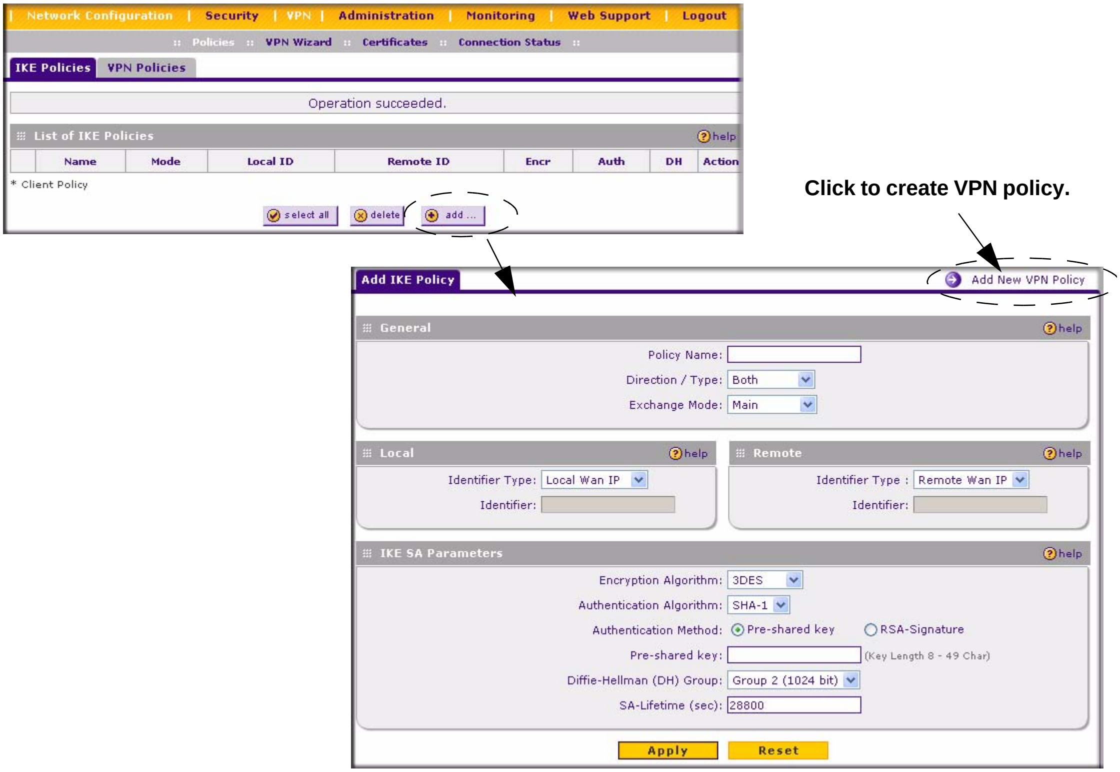
The most common configuration scenarios will use IKE policies to automatically manage the authentication and encryption keys. Based on the IKE policy, some parameters for the VPN tunnel are generated automatically. The IKE protocols perform negotiations between the two VPN endpoints to automatically generate required parameters.

Some organizations will use an IKE policy with a Certificate Authority (CA) to perform authentication. Typically, CA authentication is used in large organizations that maintain their own internal CA server. This requires that each VPN gateway have a certificate from the CA. Using CAs reduces the amount of data entry required on each VPN endpoint.

IKE Policy Automatic Key and Authentication Management

Click the **IKE Policies** tab from the VPN > Policies section of the main menu, and then click the **Add** button of the IKE Policies screen to display the IKE Policy Configuration menu shown in Figure 6-2.

The IKE Policy Configuration fields are defined in the following table.


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
:: Policies :: VPN Wizard :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
List of IKE Policies
help
select all
delete
add ...
Add IKE Policy
Add New VPN Policy
General
Local
Remote
IKE SA Parameters
Apply
Reset

Operation succeeded.

	Name	Mode	Local ID	Remote ID	Encr	Auth	DH	Action

* Client Policy

Policy Name:
Direction / Type: Both
Exchange Mode: Main

Identifier Type: Local Wan IP
Identifier:

Identifier Type : Remote Wan IP
Identifier:

Encryption Algorithm: 3DES
Authentication Algorithm: SHA-1
Authentication Method: ● Pre-shared key ○ RSA-Signature
Pre-shared key: (Key Length 8 - 49 Char)
Diffie-Hellman (DH) Group: Group 2 (1024 bit)
SA-Lifetime (sec): 28800

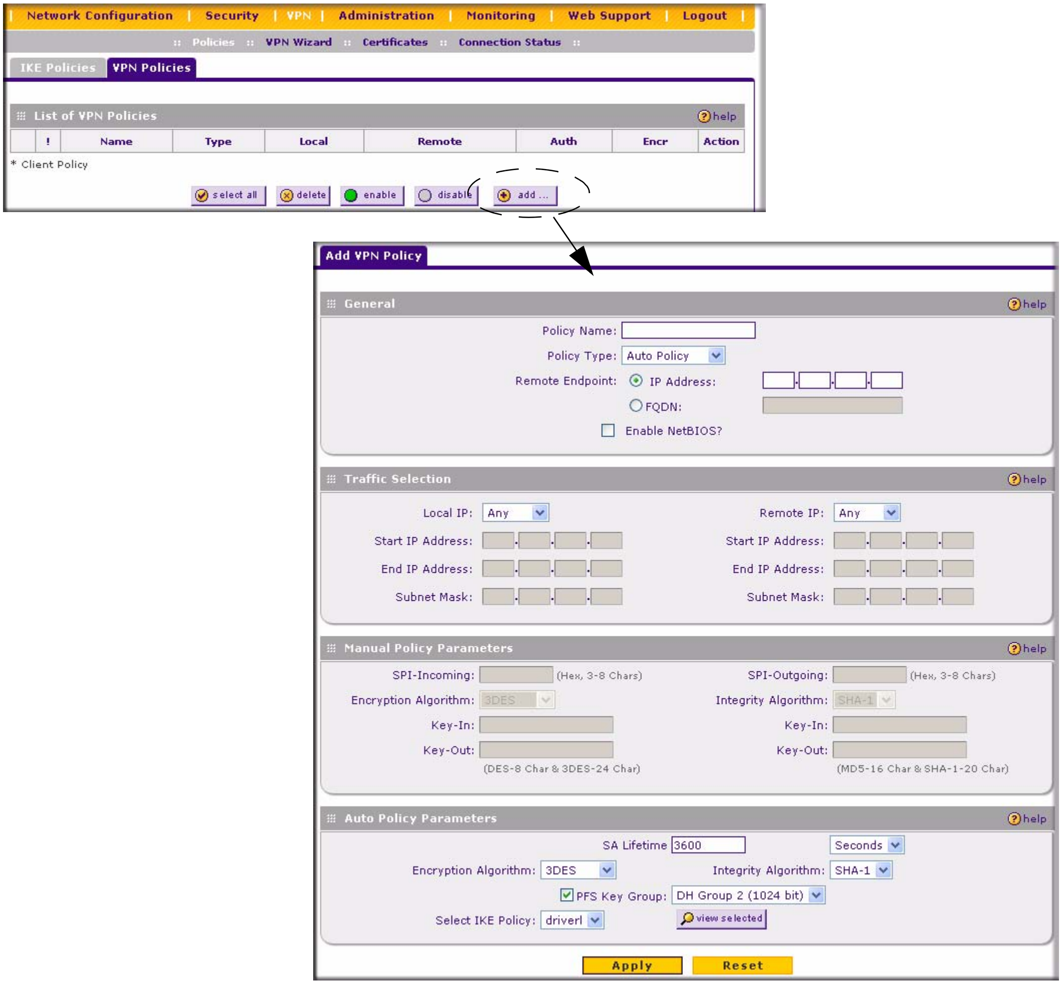
Click to create VPN policy.

Figure 6-2

VPN Policy Configuration for Auto Key and Manual Negotiation

Click the **Add New VPN Policy** link on the **Add IKE Policy** screen or select **VPN** > **Policies** and click the **VPN Policies** tab to navigate to the VPN Policies configuration screen.

- An already defined IKE policy is required for VPN Auto Policy configuration.
- With Manual Key Management, you will not use an IKE policy. You must manually type in all the required key information.



Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
:: Policies :: VPN Wizard :: Certificates :: Connection Status ::
IKE Policies
VPN Policies
help
select all
delete
enable
disable
add ...
help
help
help
help
view selected
Apply
Reset

List of VPN Policies

	!	Name	Type	Local	Remote	Auth	Encr	Action

* Client Policy

Add VPN Policy

General

Policy Name:

Policy Type: Auto Policy

Remote Endpoint: ● IP Address: ○ FQDN:

□ Enable NetBIOS?

Traffic Selection

Local IP: Any Remote IP: Any

Start IP Address: Start IP Address:

End IP Address: End IP Address:

Subnet Mask: Subnet Mask:

Manual Policy Parameters

SPI-Incoming: (Hex, 3-8 Chars) SPI-Outgoing: (Hex, 3-8 Chars)

Encryption Algorithm: 3DES Integrity Algorithm: SHA-1

Key-In: Key-In:

Key-Out: Key-Out:

(DES-8 Char & 3DES-24 Char) (MD5-16 Char & SHA-1-20 Char)

Auto Policy Parameters

SA Lifetime 3600 Seconds

Encryption Algorithm: 3DES Integrity Algorithm: SHA-1

☑ PFS Key Group: DH Group 2 (1024 bit)

Select IKE Policy: driverl

Figure 6-3

The VPN Manual and Auto Policy fields are defined in the following table.

Table 6-1. VPN Manual and Auto Policy Configuration Fields

Field	Description
General	These settings identify this policy and determine its major characteristics.

Table 6-1. VPN Manual and Auto Policy Configuration Fields (continued)

Field		Description
	Policy Name	The descriptive name of the VPN policy. Each policy should have a unique policy name. This name is not supplied to the remote VPN endpoint. It is only used to help you identify VPN policies.
	Policy Type:	A policy can be generated automatically or manually: To create an Auto VPN Policy, you must first create an IKE policy and then add the corresponding Auto Policy for that IKE Policy. • **Manual**: All settings (including the keys) for the VPN tunnel are manually input for each end point. No 3rd party server or organization is involved. • **Auto**: Some parameters for the VPN tunnel are generated automatically. This requires using the IKE (Internet Key Exchange) protocol to perform negotiations between the 2 VPN Endpoints.
	Remote End Point:	The IP address or Internet name (FQDN) of the remote gateway or client PC. Conversely, the remote VPN endpoint must have the FVG318 local IP values entered as it's Remote VPN Endpoint.
	NetBIOS	If enabled, it will allow NetBIOS broadcast to travel over the VPN tunnel
Traffic Selection		The IP addresses on both the remote and local sides that will be part of the tunnel. They can be either a single IP address, several IP addresses in a range, or an entire subnet.
	Local IP	The drop-down menu allows you to configure the source IP address of the outbound network traffic for which this VPN policy will provide security. Usually, this address is from your network address space. The choices are: • ANY for all valid IP addresses in the Internet address space • Single IP Address • Range of IP Addresses • Subnet Address
	Remote IP	The drop-down menu allows you to configure the destination IP address of the outbound network traffic for which this VPN policy will provide security. Usually, this address is from the remote site's corporate network address space. The choices are: • ANY for all valid IP addresses in the Internet address space • Single IP Address • Range of IP Addresses • Subnet Address

Table 6-1. VPN Manual and Auto Policy Configuration Fields (continued)

Field	Description
Manual Policy Parameters	The Manual Policy creates an SA (Security Association) based on static inputs
SPI-Incoming; SPI-Outgoing	Takes a hexadecimal value between 3 and 8 characters; for example: 0x1234
Encryption Algorithm:	The algorithm used to encrypt the data: • **Encryption Key-In**: Encryption key of the inbound policy. The length of the key depends on the algorithm chosen. The length is in characters as follows: DES – 8 characters 3DES – 24 characters AES-128 – 16 characters AES-192 – 24 characters AES-256 – 32 characters • **Encryption Key-Out:** Encryption key of the outbound policy. The length of the key depends on the algorithm chosen. Lengths for the outbound policy encryption key are the same as for the inbound policy.
Integrity Algorithm:	Algorithm used to verify the integrity of the data. • **Integrity Key-In**: The integrity key (for Encapsulated Security Payload (ESP) with encryption mode) for the inbound policy and depends on the algorithm chosen: MD5 – 16 characters SHA-1 – 20 characters • **Integrity Key-Out:** The integrity key (for ESP with encryption mode) for the outbound policy and depends on the algorithm chosen. Lengths are the same as for the inbound mode.
Auto Policy Parameters	
SA Life Time	The duration of the Security Association before it expires. • Seconds — the amount of time before the SA expires. Over an hour is common (3600). • Kbytes — the amount of traffic before the SA expires. One of these can be set without setting the other.
Encryption Algorithm	The encryption algorithm used to encrypt the data: • DES – the default • 3DES – more secure
Integrity Algorithm	Algorithm used to verify the integrity of the data. The choices are: • MD5 – the default • SHA1 – more secure

Table 6-1. VPN Manual and Auto Policy Configuration Fields (continued)

Field		Description
	PFS Key Group	Perfect Forward Secrecy (PFS) improves security. While this is slower, it will ensure that a Diffie-Hellman exchange is performed for every phase 2 negotiation. • DH Group 1 (768 bit) • DH Group 2 (1024 bit) • DH Group 5 (1536 bit)
	Select IKE Policy	The existing IKE policies are presented a drop-down list. You can also click **view selected** to review the settings of the selected IKE policy. This IKE policy will define the characteristics of phase 1 negotiation. **Note:** You must create the IKE policy before creating a VPN Auto Policy.

Using Digital Certificates for IKE Auto-Policy Authentication

Digital certificates are strings generated using encryption and authentication schemes that cannot be duplicated by anyone without access to the different values used in the production of the string. They are issued by Certification Authorities (CAs) to authenticate a person or a workstation uniquely. The CAs are authorized to issue these certificates by Policy Certification Authorities (PCAs), who are in turn certified by the Internet Policy Registration Authority (IPRA). The FVG318 is able to use certificates to authenticate users at the end points during the IKE key exchange process (see.

The certificates can be obtained from a certificate server that an organization might maintain internally or from the established public CAs. The certificates are produced by providing the particulars of the user being identified to the CA. The information provided may include the user's name, e-mail ID, and domain name.

Each CA has its own certificate. The certificates of a CA are added to the FVG318 and then can be used to form IKE policies for the user. Once a CA certificate is added to the FVG318 and a certificate is created for a user, the corresponding IKE policy is added to the FVG318. Whenever the user tries to send traffic through the FVG318, the certificates are used in place of pre-shared keys during initial key exchange as the authentication and key generation mechanism. Once the keys are established and the tunnel is set up the connection proceeds according to the VPN policy.

Certificate Revocation List (CRL)

Each Certification Authority (CA) maintains a list of the revoked certificates. The list of these revoked certificates is known as the Certificate Revocation List (CRL).

Whenever an IKE policy receives the certificate from a peer, it checks for this certificate in the CRL on the FVG318 obtained from the corresponding CA. If the certificate is not present in the CRL it means that the certificate is not revoked. IKE can then use this certificate for authentication. If the certificate is present in the CRL it means that the certificate is revoked, and the IKE will not authenticate the client.

You must manually update the FVG318 CRL regularly in order for the CA-based authentication process to remain valid.

VPN Configuration Scenarios on the FVG318

There are a variety of configurations you might implement with the FVG318. The scenarios listed below illustrate typical configurations you might use in your organization.

In order to help make it easier to set up an IPsec system, the following two scenarios are provided. These scenarios were developed by the VPN Consortium (*http://www.vpnc.org*). The goal is to make it easier to get the systems from different vendors to interoperate. NETGEAR is providing you with both of these scenarios in the following two formats:

- VPN Consortium Scenarios without any product implementation details
- VPN Consortium Scenarios based on the FVG318 User Interface

The purpose of providing these two versions of the same scenarios is to help you determine where the two vendors use different vocabulary. Seeing the examples presented in these different ways will reveal how systems from different vendors do the same thing.

The PC must have the NETGEAR ProSafe VPN Client program installed that supports IPSec. Go to the NETGEAR Web site (*http://www.netgear.com*) and select VPN01L_VPN05L in the Product Quick Find drop down menu for information on how to purchase the NETGEAR ProSafe VPN Client.

➡ **Note:** Before installing the NETGEAR ProSafe VPN Client software, be sure to turn off any virus protection or firewall software you may be running on your PC.

VPN Consortium Scenario 1: Gateway-to-Gateway with Preshared Secrets

The following is a typical gateway-to-gateway VPN that uses a preshared secret for authentication.

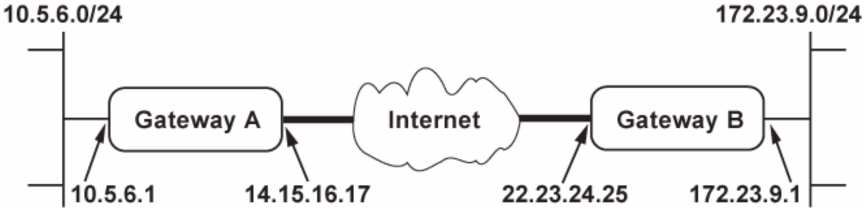


Figure 6-4

Gateway A connects the internal LAN 10.5.6.0/24 to the Internet. Gateway A's LAN interface has the address 10.5.6.1, and its WAN (Internet) interface has the address 14.15.16.17.

Gateway B connects the internal LAN 172.23.9.0/24 to the Internet. Gateway B's WAN (Internet) interface has the address 22.23.24.25. Gateway B's LAN interface address, 172.23.9.1, can be used for testing IPsec but is not needed for configuring Gateway A.

The IKE Phase 1 parameters used in Scenario 1 are:

- Main mode
- TripleDES
- SHA-1
- MODP group 2 (1024 bits)
- pre-shared secret of "hr5xb84l6aa9r6"
- SA lifetime of 28800 seconds (eight hours) with no kilobytes rekeying

The IKE Phase 2 parameters used in Scenario 1 are:

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kilobytes rekeying
- Selectors for all IP protocols, all ports, between 10.5.6.0/24 and 172.23.9.0/24, using IPv4 subnets

FVG318 Gateway A to FVG318 Gateway B (IKE and VPN Policies)

Note: This scenario assumes all ports are open on the FVG318. You can verify this by reviewing the security settings as seen in Figure 6-5

Note:

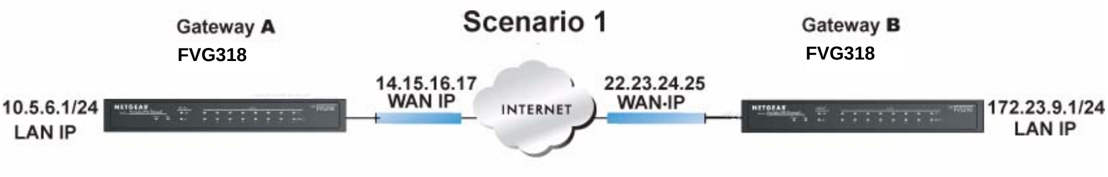


Figure 6-5

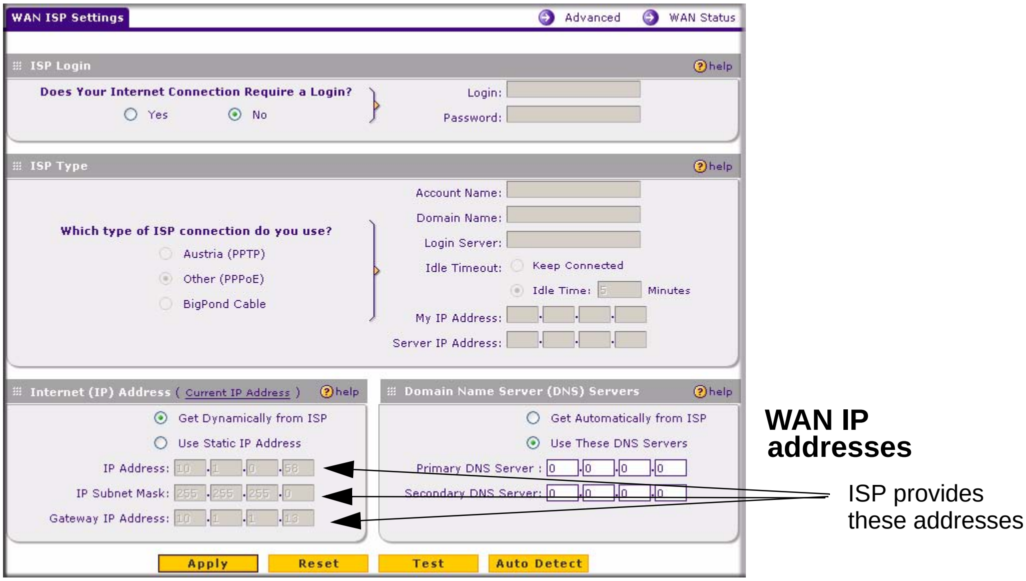
Use this scenario illustration and configuration screens as a model to build your configuration.

1. Log in to the FVG318 labeled Gateway A as in the illustration.

   Log in at the default address of **http://192.168.0.1** with the default user name of **admin** and default password of **password**, or using whatever password and LAN address you have chosen.

2. Configure the WAN (Internet) and LAN IP addresses of the FVG318.

   a. Select Network Configuration > WAN Settings to access the WAN ISP Settings menu.



ISP Login

Does Your Internet Connection Require a Login? ○ Yes ● No

Login:

Password:

ISP Type

Which type of ISP connection do you use?

○ Austria (PPTP)

● Other (PPPoE)

○ BigPond Cable

Account Name:

Domain Name:

Login Server:

Idle Timeout: ○ Keep Connected ● Idle Time: 5 Minutes

My IP Address:

Server IP Address:

Internet (IP) Address (Current IP Address)

● Get Dynamically from ISP

○ Use Static IP Address

IP Address: 10 . 1 . 0 . 58

IP Subnet Mask: 255 . 255 . 255 . 0

Gateway IP Address: 10 . 1 . 1 . 13

Domain Name Server (DNS) Servers

○ Get Automatically from ISP

● Use These DNS Servers

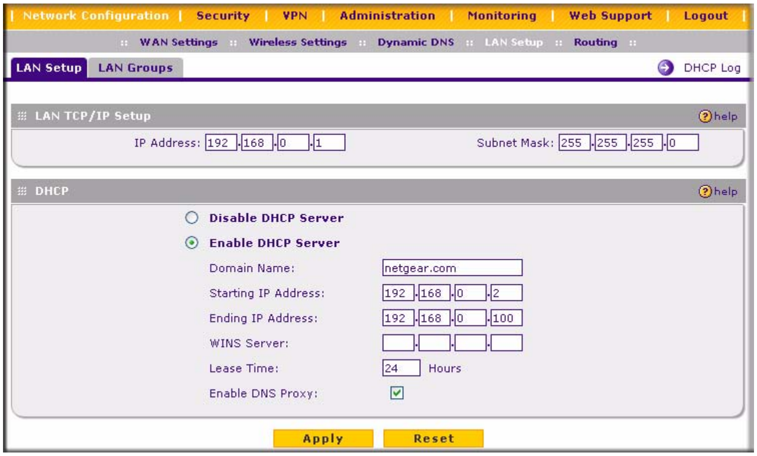
Primary DNS Server : 0 . 0 . 0 . 0

Secondary DNS Server: 0 . 0 . 0 . 0

Figure 6-6

b. Configure the WAN Internet Address according to the settings above and click **Apply** to save your settings. For more information on configuring the WAN IP settings, please see "Manually Configuring your Internet Connection" on page 2-7.

c. Select Network Configuration > LAN Setup. The LAN Setup screen will display.



LAN TCP/IP Setup

IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255 . 255 . 255 . 0

DHCP

○ Disable DHCP Server

● Enable DHCP Server

Domain Name: netgear.com

Starting IP Address: 192 . 168 . 0 . 2

Ending IP Address: 192 . 168 . 0 . 100

WINS Server:

Lease Time: 24 Hours

Enable DNS Proxy: ☑

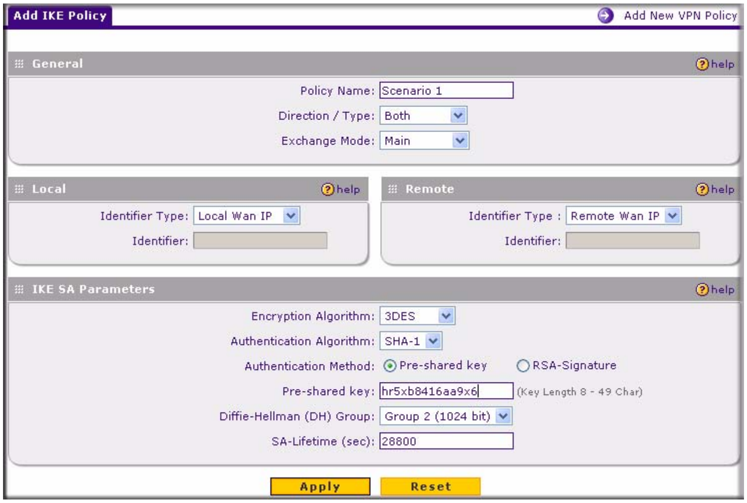
Figure 6-7

d. Configure the LAN IP address according to the settings above and click **Apply** to save your settings. For more information on LAN TCP/IP setup topics, please see "Configuring LAN TCP/IP Setup Parameters" on page 8-2.

> **Note:** After you click Apply to change the LAN IP address settings, your workstation will be disconnected from the FVG318. You will have to log on with **http://10.5.6.1** which is now the address you use to connect to the built-in Web-based configuration manager of the FVG318.

3. Set up the IKE Policy illustrated below on the FVG318.

a. Select VPN > Policies. The IKE Policies screen will display. Click **Add** to display the Add IKE Policy screen shown below.



Add IKE Policy

Add New VPN Policy

General

Policy Name: Scenario 1
Direction / Type: Both
Exchange Mode: Main

Local

Identifier Type: Local Wan IP
Identifier:

Remote

Identifier Type : Remote Wan IP
Identifier:

IKE SA Parameters

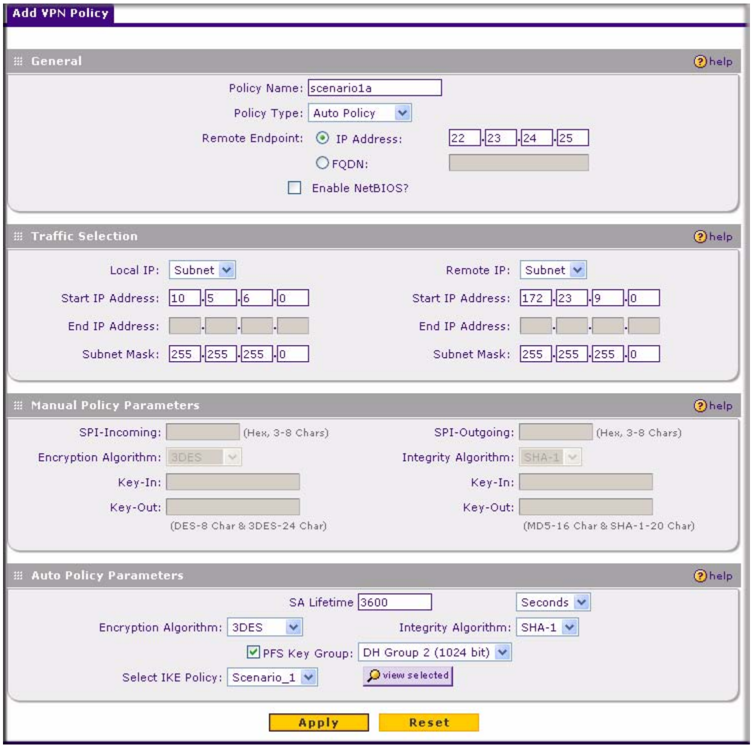
Encryption Algorithm: 3DES
Authentication Algorithm: SHA-1
Authentication Method: ● Pre-shared key ○ RSA-Signature
Pre-shared key: hr5xb8416aa9x6 (Key Length 8 - 49 Char)
Diffie-Hellman (DH) Group: Group 2 (1024 bit)
SA-Lifetime (sec): 28800

Figure 6-8

b. Configure the IKE Policy according to the settings in the illustration above and click **Apply** to save your settings. For more information on IKE Policy topics, please see "IKE Policy Automatic Key and Authentication Management" on page 6-2.

4. Set up the FVG318 VPN Auto Policy as illustrated below.

a. Select VPN > Policies and click the VPN Policies tab. The VPN Policies screen will display. Click **Add** to display the Add VPN Policy screen.



Add VPN Policy

General

Policy Name: scenario1a

Policy Type: Auto Policy

Remote Endpoint: ● IP Address: 22.23.24.25

○ FQDN:

□ Enable NetBIOS?

Traffic Selection

Local IP:	Subnet	Remote IP:	Subnet
Start IP Address:	10.5.6.0	Start IP Address:	172.23.9.0
End IP Address:	. . .	End IP Address:	. . .
Subnet Mask:	255.255.255.0	Subnet Mask:	255.255.255.0

Manual Policy Parameters

SPI-Incoming:	(Hex, 3-8 Chars)	SPI-Outgoing:	(Hex, 3-8 Chars)
Encryption Algorithm:	3DES	Integrity Algorithm:	SHA-1
Key-In:		Key-In:	
Key-Out:		Key-Out:	
	(DES-8 Char & 3DES-24 Char)		(MD5-16 Char & SHA-1-20 Char)

Auto Policy Parameters

SA Lifetime 3600 Seconds

Encryption Algorithm: 3DES Integrity Algorithm: SHA-1

☑ PFS Key Group: DH Group 2 (1024 bit)

Select IKE Policy: Scenario_1

Figure 6-9

b. Configure the VPN Policy according to the settings in the illustration above and click **Apply** to save your settings. For more information on VPN Policy topics, please see "VPN Policy Configuration for Auto Key and Manual Negotiation" on page 6-3.

5. After applying these changes, all traffic from the range of LAN IP addresses specified on FVG318 A and FVG318 B will flow over a secure VPN tunnel.

Checking Your VPN Connections

You can test connectivity and view VPN status information on the FVG318 (see also "Activating a VPN Tunnel" on page 5-23).

To test the Gateway A FVG318 LAN and the Gateway B LAN connection:

1. Using our example, from a PC attached to the FVG318 on LAN A, on a Windows PC click the Start button on the task bar and then click Run.
2. Type **`ping -t  172.23.9.1`**, and then click **OK**.
3. This will cause a continuous ping to be sent to the LAN interface of Gateway B. Within two minutes, the ping response should change from timed out to reply.
4. At this point the connection is established.
5. To test connectivity between the FVG318 Gateway A and Gateway B WAN ports, follow these steps:
   - **a.** Using our example, log in to the FVG318 on LAN A and then select Monitoring > Diagnostics from the menu.
   - **b.** To test connectivity to the WAN port of Gateway B, enter **22.23.24.25** in the IP Address field in the **Ping or Trace an IP Address** section, and then click **Ping**.
   - **c.** This causes a ping to be sent to the WAN interface of Gateway B. Within two minutes, the ping response should change from timed out to reply. You may have to run this test several times before you get the reply message back from the target FVG318.
   - **d.** At this point the connection is established.

➡	**Note:** If you want to ping the FVG318 as a test of network connectivity, be sure the FVG318 is configured to respond to a ping on the Internet WAN port by checking the check box. However, to preserve a high degree of security, you should turn off this feature when you are finished with testing.

6. To view the FVG318 event log and status of Security Associations, follow these steps:
   - **a.** Select the Monitoring > VPN Logs to view the VPN Log Status of the FVG318 and go to VPN > IPSec Connection Status to view the Active IPsec SA(s) policies.
   - **b.** The log screen displays a history of the VPN connections, and the IP Connection Status screen will show the IPSec SA table that will report the status and data transmission statistics of the VPN tunnels for each policy.

VPN Consortium Scenario 2: FVG318 Gateway to Gateway with Digital Certificates

The following is a typical gateway-to-gateway VPN that uses Public Key Infrastructure x.509 (PKIX) certificates for authentication. The network setup is identical to the one given in Scenario 1. The IKE Phase 1 and Phase 2 parameters are identical to the ones given in Scenario 1, with the exception that the identification is done with signatures authenticated by PKIX certificates.

WAN IP Address

LAN IP Addresses

> **Note:** Before completing this configuration scenario, make sure the correct Time Zone is set on the FVG318. For instructions on this topic, see "Configuring Your Time Zone" on page 2-11.

1. Obtain a root certificate.

   a. Obtain the root certificate (that includes the public key) from a Certificate Authority (CA)

   > **Note:** The procedure for obtaining certificates differs from a CA like Verisign and a CA such as a Windows 2000 certificate server, which an organization operates for providing certificates for its members. For example, an administrator of a Windows 2000 certificate server might provide it to you via e-mail.

   b. Save the certificate as a text file called *trust.txt*.

2. Install the trusted CA certificate for the Trusted Root CA.

   a. Log in to the FVG318.

   b. Select VPN > Certificates from the menu.

   c. In the **Self Certificate Requests** section, click **Browse** to locate the *trust.txt* file.

   d. Click **Upload**.

3. Create a certificate request for the FVG318.

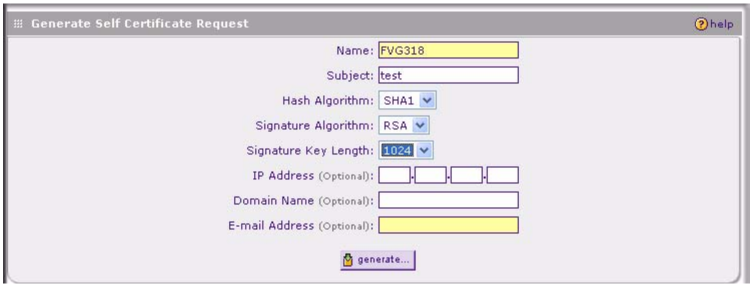
   e. Fill in the required fields on the Generate Self Certificate section.

      - Name. Enter a name to identify this certificate.
      - Subject. 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 certificates should have the same value in the Subject field.

- Hash Algorithm. Select the desired option: MD5 or SHA1.
- Signature Algorithm. Select the desired option: DSS or RSA.
- Signature Key Length. Select the desired option: 512, 1024, or 2048.

f. Fill in any optional fields on the Add Self Certificate screen that may apply.

- IP Address. If you use “IP type” in the IKE policy, you should input the IP Address here. Otherwise, you should leave this blank.
- Domain Name. If you have a domain name, you can enter it here. Otherwise, you should leave this blank.
- E-mail address. You can enter your e-mail address here.

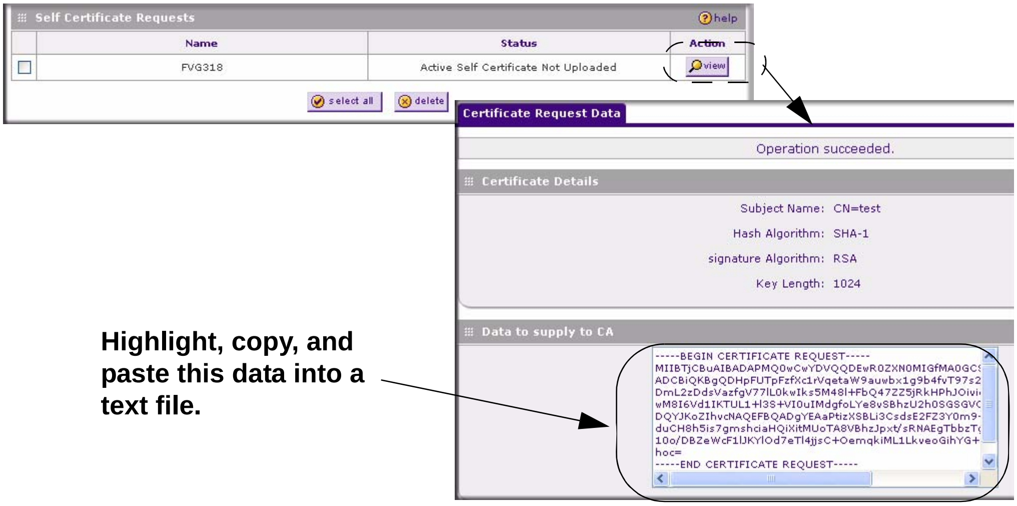


Generate Self Certificate Request

Name:	FVG318
Subject:	test
Hash Algorithm:	SHA1
Signature Algorithm:	RSA
Signature Key Length:	1024
IP Address (Optional):	. . .
Domain Name (Optional):	
E-mail Address (Optional):	

Figure 6-10

g. Click **Generate** The FVG318 generates a pending Self Certificate Request as shown below. Click **view** to display the data.



□	Name	Status	Action
□	FVG318	Active Self Certificate Not Uploaded	view

Operation succeeded.

Subject Name: CN=test
Hash Algorithm: SHA-1
signature Algorithm: RSA
Key Length: 1024

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBTjCBuAIBADAPMQ0wCwYDVQQDEwR0ZXN0MIGfMA0GCS
ADCBiQKBgQDHpFUTpFzfXc1rVqetaW9auwbx1g9b4fvT97s2
DmL2zDdsVazfgV77lL0kwIks5M48l+FbQ47ZZ5jRkHPhJOivi
wM8I6Vd1IKTUL1+l3S+VI0uIMdgfoLYe8vSBhzU2h0SGSGVC
DQYJKoZIhvcNAQEFBQADgYEAaPtizXSBLi3CsdsE2FZ3Y0m9-
duCH8h5is7gmshciaHQiXitMUoTA8VBhzJpxt/sRNAEgTbbzT
10o/DBZeWcF1lJKYlOd7eTl4jjsC+OemqkiML1LkveoGihYG+
hoc=
-----END CERTIFICATE REQUEST-----
```

Highlight, copy, and paste this data into a text file.

Figure 6-11

4. Transmit the Self Certificate Request data to the Trusted Root CA.

   a. Highlight the text in the Data to supply to CA area, copy it, and paste it into a text file.

   b. Give the certificate request data to the CA. In the case of a Windows 2000 internal CA, you might simply e-mail it to the CA administrator. The procedures of a CA like Verisign and a CA such as a Windows 2000 certificate server administrator will differ. Follow the procedures of your CA.

5. Receive the certificate back from the Trusted Root CA and save it as a text file.

➡	**Note:** In the case of a Windows 2000 internal CA, the CA administrator might simply email it to back to you. Follow the procedures of your CA. Save the certificate you get back from the CA as a text file called *final.txt*.

6. Upload the new certificate.

   c. Select the checkbox of the Self Certificate Request you want to upload.

   d. Browse to the location of the file you saved in Step 5 above that contains the certificate from the CA.

   e. Click **Upload** button.

   f. The “FVG318” certificate will display in the Active Self Certificates table and the pending “FVG318” Self Certificate Request will be deleted.

7. Associate the new certificate and the Trusted Root CA certificate on the FVG318.

   a. Create a new IKE policy called **Scenario_2** with all the same properties of **Scenario_1,** except now select the **RSA Signature** radio box instead of the Pre-shared key.

   b. Create a new VPN Auto Policy called **scenario2a** with all the same properties as **scenario1a** except that it uses the IKE policy called Scenario_2.

   Now, the traffic from devices within the range of the LAN subnet addresses on FVG318 A and Gateway B will be authenticated using the certificates rather than via a pre-shared key.

8. Set up Certificate Revocation List (CRL) checking.

   a. Get a copy of the CRL from the CA and save it as a text file.

> **Note:** The procedure for obtaining a CRL differs from a CA like Verisign and a CA such as a Windows 2000 certificate server, which an organization operates for providing certificates for its members. Follow the procedures of your CA.

   b. Select VPN > Certificates from the main menu and scroll down to the **Certificate Revocation Lists (CRL)** section.

   c. Click **Browse** to locate the CRL file.

   d. Click **Upload**. The CRL will be uploaded to the Certificate Revocation Lists (CRL) table.

   Now expired or revoked certificates will not be allowed to use the VPN tunnels managed by IKE policies which use this CA.

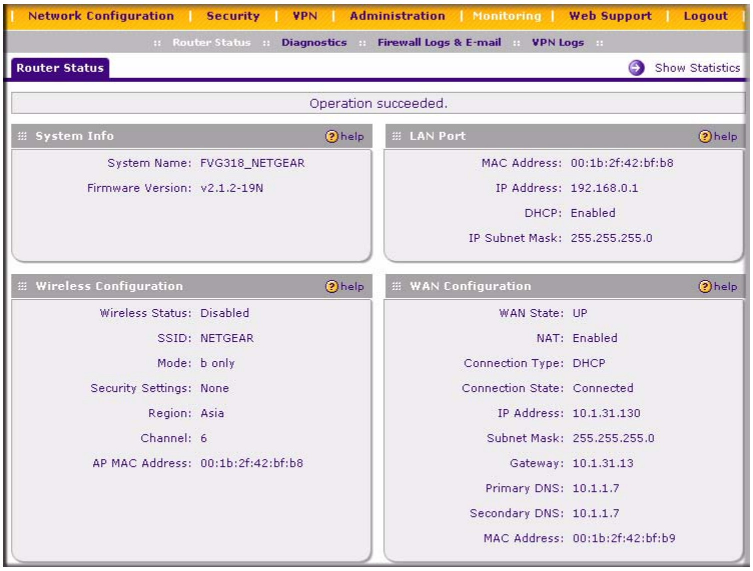
> **Note:** You must update the CRLs regularly in order to maintain the validity of the certificate-based VPN policies.

Chapter 7
Maintenance

This chapter describes how to use the maintenance features of your ProSafe 802.11g Wireless VPN Firewall. These features can be found by selecting Monitoring > Router Status from the main menu of the browser interface.

Viewing VPN Firewall Router Status Information

The Router Status menu provides status and usage information. From the main menu of the browser interface, click **Monitoring > Router Status** to view this screen.



Operation succeeded.

System Info

System Name: FVG318_NETGEAR
Firmware Version: v2.1.2-19N

LAN Port

MAC Address: 00:1b:2f:42:bf:b8
IP Address: 192.168.0.1
DHCP: Enabled
IP Subnet Mask: 255.255.255.0

Wireless Configuration

Wireless Status: Disabled
SSID: NETGEAR
Mode: b only
Security Settings: None
Region: Asia
Channel: 6
AP MAC Address: 00:1b:2f:42:bf:b8

WAN Configuration

WAN State: UP
NAT: Enabled
Connection Type: DHCP
Connection State: Connected
IP Address: 10.1.31.130
Subnet Mask: 255.255.255.0
Gateway: 10.1.31.13
Primary DNS: 10.1.1.7
Secondary DNS: 10.1.1.7
MAC Address: 00:1b:2f:42:bf:b9

Figure 7-1

This screen shows the following parameters:

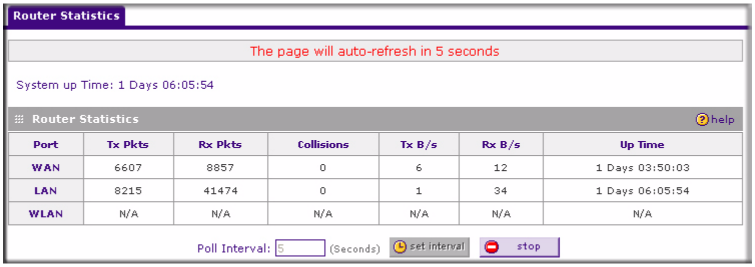
Table 7-1. FVG318 Status fields

Field		Description
	System Name	The System Name assigned to the firewall.
	Firmware Version	The firewall firmware version.
Wireless Configuration		The wireless settings of the router
	SSID:	The name of your wireless network. The default is NETGEAR.
	Mode	
	Security Settings	Shows what security has been associated with the wireless configuration. The default is none
	Region	Shows the region is which the wireless gateway is operating
	Channel	Indicates the operating channel of the wireless radio.
	AP MAC Address	The MAC address of the wireless access point.
WAN Port		These parameters apply to the Internet (WAN) port of the firewall.
	WAN State	Indicates if the WAN port is up or down.
	NAT	Indicates if the router is in NAT mode (enabled) or in routing mode (disabled).
	DHCP	The protocol on the WAN port used to obtain the WAN IP address. This field can show DHCP Client, Fixed IP, PPPoE, BPA or PPTP. For example, if set to Client, the firewall is configured to obtain an IP address dynamically from the ISP.
	Connection State	Indicates if the WAN port is connected or not.
	IP Address	The IP address used by the Internet (WAN) port of the firewall. If no address is shown, the firewall cannot connect to the Internet.
	IP Subnet Mask	The IP Subnet Mask being used by the Internet (WAN) port of the firewall.
	Gateway	Gateway address of the WAN port.
	Primary DNS	DNS server IP address of the WAN port.
	Secondary DNS	Secondary DNS server IP address of the WAN port (if not assigned, it will be the same as the primary DNS server).
	DHCP	The protocol on the WAN port used to obtain the WAN IP address. This field can show DHCP Client, Fixed IP, PPPoE, BPA or PPTP. For example, if set to Client, the firewall is configured to obtain an IP address dynamically from the ISP.
	MAC Address	The MAC address used by the Internet (WAN) port of the firewall.
LAN Port		These parameters apply to the Local (WAN) port of the firewall.
	MAC Address	The MAC address used by the LAN port of the firewall.

Table 7-1. FVG318 Status fields

Field		Description
	IP Address	The IP address used by the Local (LAN) port of the firewall. The default is 192.168.0.1
	IP Subnet Mask	The IP Subnet Mask used by the Local (LAN) port of the firewall. The default is 255.255.255.0
	DHCP	Identifies if the firewall’s built-in DHCP server is active for the LAN attached devices.

Click **Show Statistics** to display the WAN connection status,



Router Statistics

The page will auto-refresh in 5 seconds

System up Time: 1 Days 06:05:54

Router Statistics

Port	Tx Pkts	Rx Pkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	6607	8857	0	6	12	1 Days 03:50:03
LAN	8215	41474	0	1	34	1 Days 06:05:54
WLAN	N/A	N/A	N/A	N/A	N/A	N/A

Poll Interval: 5 (Seconds)

Figure 7-2

This screen shows the data transfer statistics for the WAN and LAN ports, including the duration they were enabled. The following data is displayed:.

Table 7-2. Connection Status fields

Field	Description
Tx packets	The number of IP packets going out through the port.
Rx Packets	The number of IP packets received by the port.
Collisions	The number of signal collisions that have occurred on the part. (A collision occurs when the port tries to send data at the same time as a port on another router or computer that is connected to this port.
Tx/Bs	The number of bytes going out of the port per second
Rx/Bs	The number of bytes received by the port per second.
Uptime	The duration the port as been active; the uptime is reset to zero when the router or port is restarted.

Upgrading the Firewall Software

The routing software of the FVG318 VPN firewall is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR. Upgrade files can be downloaded from NETGEAR's Web site. If the upgrade file is compressed (*.zip* file), you must first extract the binary (*.bin*) file before sending it to the firewall. The upgrade file can be sent to the firewall using your browser.

> **Note:** The Web browser used to upload new firmware into the VPN firewall must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer or Netscape Navigator 5.0 or above.

Select Administration > Settings Backup & Upgrade from the main menu of the browser interface. The Settings Backup and Firmware Upgrade screen will display.

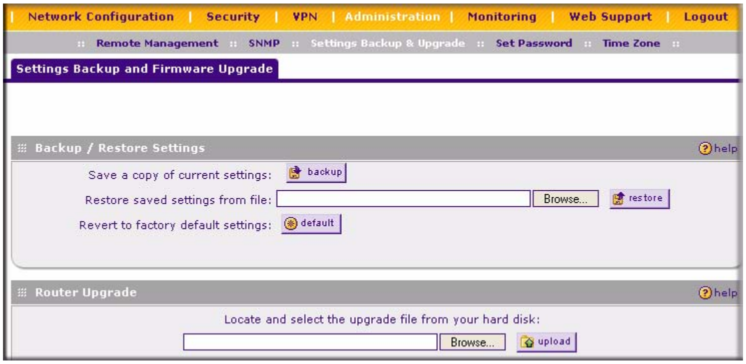

| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Set Password :: Time Zone ::
Settings Backup and Firmware Upgrade
Backup / Restore Settings
help
Save a copy of current settings:
backup
Restore saved settings from file:
Browse...
restore
Revert to factory default settings:
default
Router Upgrade
help
Locate and select the upgrade file from your hard disk:
Browse...
upload

Figure 7-3

To upload new firmware:

1. Download and unzip the new software file from NETGEAR and save it to a location on your local drive.
2. In the Router Upgrade section, click **Browse** and then browse to the location of the binary (*.bin*) upgrade file on you local drive.

3. Highlight the file and click **Upload**.

> **Note:** When uploading software to the VPN firewall, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it may corrupt the software. When the upload is complete, your firewall will automatically restart. The upgrade process will typically take about 1 minute.

In some cases, you may need to reconfigure the firewall after upgrading.

Backing Up and Restoring Settings

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.

You can use the Backup/Restore Settings section of the Settings Backup and Firmware Upgrade screen shown in Figure 7-3 to back up your configuration in a file, restore from that file, or revert to the factory default configuration settings.

To backup and restore your configuration:

1. Click **Backup**. Your browser will extract the configuration file from the firewall and prompt you for a location on your PC to store the file. You can give the file a meaningful name at this time, such as **sanjose.cfg**.
2. Click **Browse** to locate your backup file. When you have located it, click **Restore** to send the file to the firewall. The firewall will then reboot automatically.

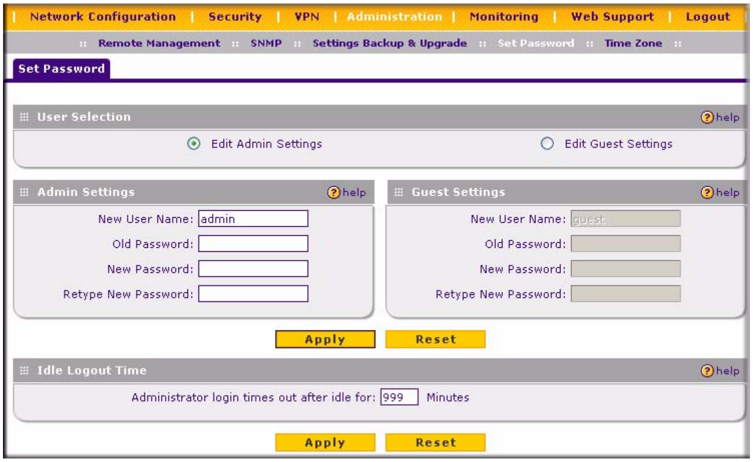
It is sometimes desirable to restore the firewall to a known blank condition. To erase the configuration and revert to the factory default settings, click **default.** After reverting to the factory default setting, the firewall password will be **password**, the LAN IP address will be 192.168.0.1, and the firewall DHCP client will be enabled.

To restore the factory default configuration settings without knowing the login password or IP address, you must use the reset button on the rear panel of the firewall. See “Restoring the Default Configuration and Password” on page 9-6.

Changing the Administrator Password

The default password for the firewall’s Web Configuration Manager is **password**. NETGEAR recommends that you change this password to a more secure password.

Select Administration > Set Password to display the Set Password screen..


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
Remote Management :: SNMP :: Settings Backup & Upgrade :: Set Password :: Time Zone
Set Password
User Selection
help
Admin Settings
Guest Settings
Idle Logout Time
Apply
Reset

● Edit Admin Settings ○ Edit Guest Settings

Admin Settings

New User Name: admin
Old Password:
New Password:
Retype New Password:

Guest Settings

New User Name: guest
Old Password:
New Password:
Retype New Password:

Administrator login times out after idle for: 999 Minutes

Figure 7-4

You can change the password for both the Administrator and Guest settings.

To change the password:

1. Select the radio button for the password you want to change: either Edit Admin Settings or Edit Guest Settings.
2. Enter a new User Name to change the login User Name. If no User Name change is required, leave this as is.
3. Enter the old password first, and then enter the new password twice and click **Apply**. \

To change the login idle timeout, change the number of minutes and click **Apply**.

Chapter 8
Advanced Configuration

This chapter describes how to configure the advanced features of your ProSafe 802.11g Wireless VPN Firewall FVG318.

Configuring Dynamic DNS

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. In this case, you can use a commercial dynamic DNS service, which will allow you to register your domain to their IP address, and will forward traffic directed to your domain to your frequently-changing IP address.

The firewall contains a client that can connect to a dynamic DNS service provider. To use this feature, you must select a service provider and obtain an account with them. After you have configured your account information in the firewall, whenever your ISP-assigned IP address changes, your firewall will automatically contact your dynamic DNS service provider, log in to your account, and register your new IP address.

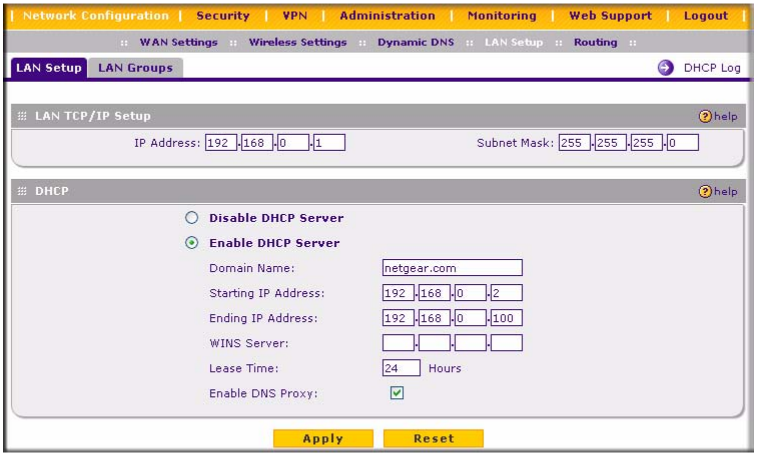
1. Log in to the firewall at its default LAN address of **http://192.168.0.1** with its default user name of **admin**, default password of **password**, or using whatever password and LAN address you have chosen for the firewall.
2. Select Network Configuration > Dynamic DNS on the main menu of the browser interface. The Dynamic DNS screen will display.
3. Access the Web site of one of the dynamic DNS service providers whose names appear in the menu, and register for an account.
   For example, for dyndns.org, go to *www.dyndns.org*.
4. Select the name of your dynamic DNS Service Provider.
5. Type the host and domain name that your dynamic DNS provider gave you. This will look like a URL, such as **myName.dyndns.org**.
6. Type the user name for your dynamic DNS account.
7. Type the password (or key) for your dynamic DNS account.

8. If your dynamic DNS provider allows the use of wildcards 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
9. Click **Apply** to save your configuration.

> **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.

Using the LAN IP Setup Options

The LAN IP Setup menu allows configuration of LAN IP services such as DHCP. Select Network Configuration > LAN Setup to view the screen shown below


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
WAN Settings :: Wireless Settings :: Dynamic DNS :: LAN Setup :: Routing
LAN Setup
LAN Groups
DHCP Log
help
help
Apply
Reset

LAN TCP/IP Setup

IP Address: 192 . 168 . 0 . 1   Subnet Mask: 255 . 255 . 255 . 0

DHCP

○ Disable DHCP Server

● Enable DHCP Server

Domain Name: netgear.com

Starting IP Address: 192 . 168 . 0 . 2

Ending IP Address: 192 . 168 . 0 . 100

WINS Server: . . .

Lease Time: 24 Hours

Enable DNS Proxy: ☑

Figure 8-1

Configuring LAN TCP/IP Setup Parameters

The firewall is shipped preconfigured to use private IP addresses on the LAN side, and to act as a DHCP server. The firewall's default LAN IP configuration is:

- LAN IP addresses: 192.168.0.1
- Subnet mask: 255.255.255.0

These addresses are part of the IETF-designated private address range for use in private networks, and should be suitable in most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in this menu.

The LAN IP parameters are:

- **IP Address**. This is the LAN IP address of the firewall.
- **IP Subnet Mask**. This is the LAN Subnet Mask of the firewall. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or firewall.

➡	**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.

Using the Firewall as a DHCP server

By default, the firewall functions as a DHCP (Dynamic Host Configuration Protocol) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the firewall's 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.

For most applications, the default DHCP and TCP/IP settings of the firewall are satisfactory. See "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 **Use router as DHCP server** check box. Otherwise, leave it checked.

To specify the pool of IP addresses to be assigned, set 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 192.168.0.2 and 192.168.0.100, 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 (if you entered a primary DNS address in the WAN Settings menu; otherwise, the firewall's LAN IP address)
- Secondary DNS server (if you entered a secondary DNS address in the WAN Settings menu

Using Address Reservation

When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time it accesses the firewall's DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.

To reserve an IP address:

1. Click the **LAN Groups** tab.
2. In the Add Known PCs and Devices section, enter a name for the PC in the Name field so that it is easily recognizable.
3. From the IP Address Type pull-down menu, select Reserved (DHCP Client).
4. Type the IP address to assign to the PC or server.
   (Choose an IP address from the firewall's LAN subnet, such as 192.168.0.X.)
5. Type the MAC Address of the PC or server.
6. Click **Apply** to enter the reserved address into the table.

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

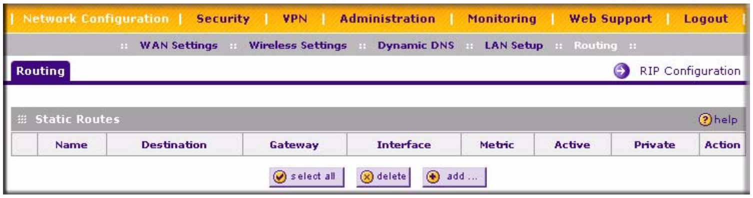
To edit or delete a reserved address entry:

1. Click **Edit** next to the reserved address you want to edit or delete and edit the fields on the Edit Known PC and Device screen. Click **Apply**.
2. Select the checkbox adjacent to the IP address you want to delete and click **Delete**.

Configuring Static Routes

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

Select Network Configuration > Routing to view the Static Route table shown on the Routing screen below.



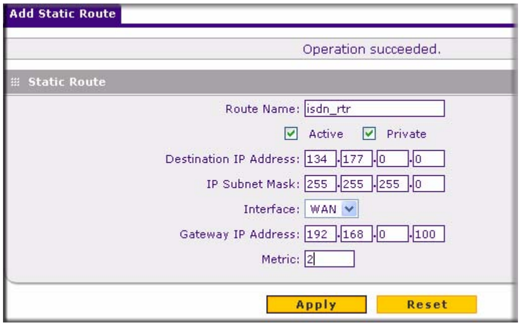
| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Wireless Settings :: Dynamic DNS :: LAN Setup :: Routing ::
Routing
RIP Configuration
Static Routes
help
select all
delete
add ...

	Name	Destination	Gateway	Interface	Metric	Active	Private	Action

Figure 8-2

To add a Static Route:

1. Click **Add** to open the Add screen shown below.



Route Name: isdn_rtr

☑ Active ☑ Private

Destination IP Address: 134 . 177 . 0 . 0

IP Subnet Mask: 255 . 255 . 255 . 0

Interface: WAN

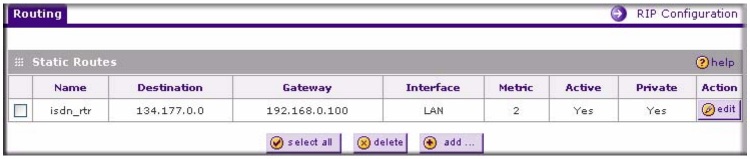
Gateway IP Address: 192 . 168 . 0 . 100

Metric: 2

Figure 8-3

2. Type a route name for this static route in the Route Name box. (This is for identification purpose only.)
3. Select Private if you want to limit access to the LAN only. The static route will not be reported in RIP. You must also select LAN from the Interface pull-down menu.
4. Select Active to make this route effective.

5. Type the Destination IP Address of the final destination.
6. Type the IP Subnet Mask for this destination.
   If the destination is a single host, type **255.255.255.255**.
7. Type the Gateway IP Address, which must be a firewall on the same LAN segment as the firewall.
8. Type a number between 1 and 15 as the Metric value.
   This represents the number of firewalls between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.
9. Click **Apply** to have the static route entered into the table as shown below.



Routing

RIP Configuration

Static Routes

help

	Name	Destination	Gateway	Interface	Metric	Active	Private	Action
□	isdn_rtr	134.177.0.0	192.168.0.100	LAN	2	Yes	Yes	edit

Figure 8-4

To edit the static route entry, click **Edit.**

Configuring RIP

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

Note: RIP is disabled by default.

To enable RIP:

1. Click the **RIP Configuration** link on the Routing screen (shown in **Figure 8-4** above).The RIP Configuration screen will display
2. Select the RIP Direction.The RIP Direction selection controls how the firewall sends and receives RIP packets. Both is the default.
   – When set to Both or Out Only, the firewall broadcasts its routing table periodically.

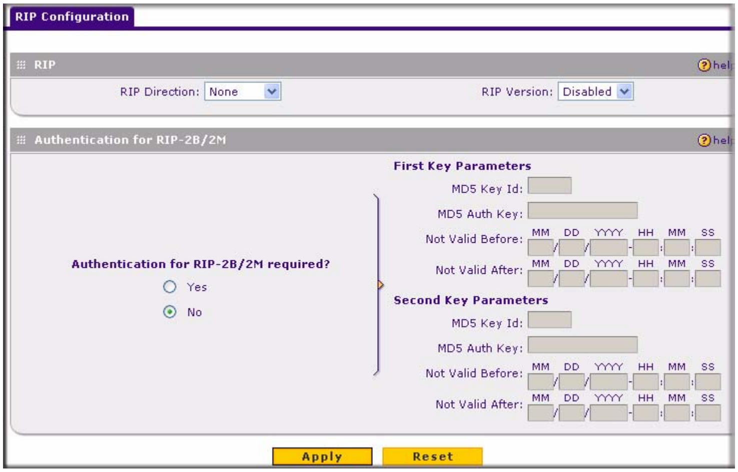
- When set to Both or In Only, it incorporates the RIP information that it receives.
- When set to None, it will not send any RIP packets and ignores any RIP packets received.

3. Enable the RIP Version. This controls the format and the broadcasting method of the RIP packets that the firewall sends. (It recognizes both formats when receiving.)

- RIP-1 is universally supported. RIP-1 is probably adequate for most networks, unless you have an unusual network setup.
- RIP-2 carries more information.
- RIP-2B uses subnet broadcasting.RIP-2B broadcasts data in the entire subnet.
- RIP-2M sends data to multicast addresses.

4. If authentication is required for RIP 2B/2M:

- Select the **Yes** radio box.
- Input the MD-5 keys and Effective Start and End dates for the First and Second Keys for MD5 based authentication between routers.



RIP Direction: None

RIP Version: Disabled

Authentication for RIP-2B/2M required?

○ Yes

● No

First Key Parameters

MD5 Key Id:

MD5 Auth Key:

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

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

Second Key Parameters

MD5 Key Id:

MD5 Auth Key:

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

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

Figure 8-5

5. Click **Apply.**

Static Route Example

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.

- You have an ISDN firewall on your home network for connecting to the company where you are employed. This firewall's address on your LAN is 192.168.0.100.
- Your company's network is 134.177.0.0.

When you first configured your firewall, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your firewall will forward your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company's firewall.

In this case you must define a static route, telling your firewall that 134.177.0.0 should be accessed through the ISDN firewall at 192.168.0.100. The static route would look like Figure 8-4.

In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Gateway IP Address fields specifies that all traffic for these addresses should be forwarded to the ISDN firewall at 192.168.0.100.
- A Metric value of 1 will work since the ISDN firewall is on the LAN.
- Private is selected only as a precautionary security measure in case RIP is activated.

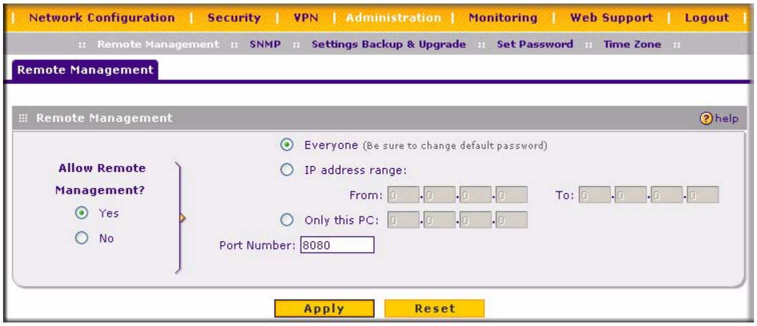
Enabling Remote Management Access

Using the Remote Management page, you can allow a user or users on the Internet to configure, upgrade and check the status of your FVG318 VPN firewall.

Note: Be sure to change the firewall's default configuration password 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.

To configure your firewall for Remote Management:

1. Select Administration > Remote Management from the main menu. The Remote Management screen will display.


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Set Password :: Time Zone ::
Remote Management
:: Remote Management
help
Apply
Reset

Allow Remote Management?

● Yes
○ No

● Everyone (Be sure to change default password)

○ IP address range:

From: 0 . 0 . 0 . 0 To: 0 . 0 . 0 . 0

○ Only this PC: 0 . 0 . 0 . 0

Port Number: 8080

Figure 8-6

2. Select the **Yes** radio box for Allow Remote Management.

- Specify what external addresses will be allowed to access the firewall's remote management.

Note: For enhanced security, restrict access to as few external IP addresses as practical.

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

3. Specify the Port Number that will be used for accessing the management interface.

Web browser access normally uses the standard HTTP service port 80. For greater security, you can change the remote management web interface to a custom port by entering that number in the box provided. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

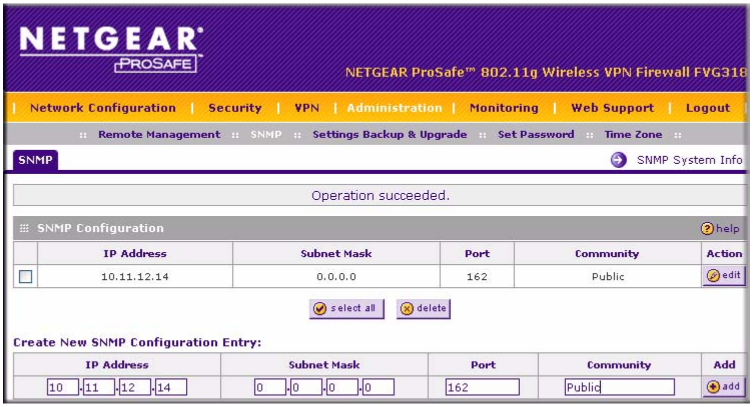
4. Click **Apply** to have your changes take effect.

Tip: If you are using a dynamic DNS service such as TZO, you can always identify the IP address of your FVG318 by running TRACERT from the Windows Start menu Run option. For example, type **tracert yourFVG318.mynetgear.net** and you will see the IP address your ISP assigned to the FVG318.

SNMP Administration

Simple Network Management Protocol (SNMP) lets you monitor and manage your router from an SNMP Manager. SNMP provides a remote means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. The router supports the SNMPv2c protocol version and can send traps to a specified community.

Select Administration > SNMP to access the SNMP screen shown below:


NETGEAR
PROSAFE
NETGEAR ProSafe™ 802.11g Wireless VPN Firewall FVG318
Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
Remote Management :: SNMP :: Settings Backup & Upgrade :: Set Password :: Time Zone
SNMP
SNMP System Info
help

Operation succeeded.

SNMP Configuration

	IP Address	Subnet Mask	Port	Community	Action
□	10.11.12.14	0.0.0.0	162	Public	edit

select all delete

Create New SNMP Configuration Entry:

IP Address	Subnet Mask	Port	Community	Add
10 . 11 . 12 . 14	0 . 0 . 0 . 0	162	Public	add

Figure 8-7

The SNMP Configuration table lists the IP addresses of SNMP agents to which the router will send trap messages. The following are present in the table:

- **IP Address**: The IP address of the SNMP manager or trap agent.
- **Subnet Mask**: The network mask used to determine the list of allowed SNMP managers.
- **Port**: The SNMP trap port of the IP address to which, the trap messages will be sent.
- **Community**: The community string to which the agent belongs. Most agents are configured to listen for traps in the Public community.

To create a new SNMP configuration entry:

1. Enter the IP address of an SNMP trap agent.
2. Enter the Subnet Mask. The network mask used to determine the list of allowed SNMP managers.
   - To allow any IP on the network to manager the device, enter 255.255.255.0.
   - For a specific host, enter 255.255.255.255.
   - To allow global access, enter 0.0.0.0.
3. Enter the SNMP trap port to which the trap messages will be sent.
4. Enter the community string to which the agent belongs. Most agents are configured to listen for traps in the **Public** community.
5. Click **Add** to create the new configuration. The configuration will be displayed in the SNMP Configuration table.

To Edit or modify the selected configuration.

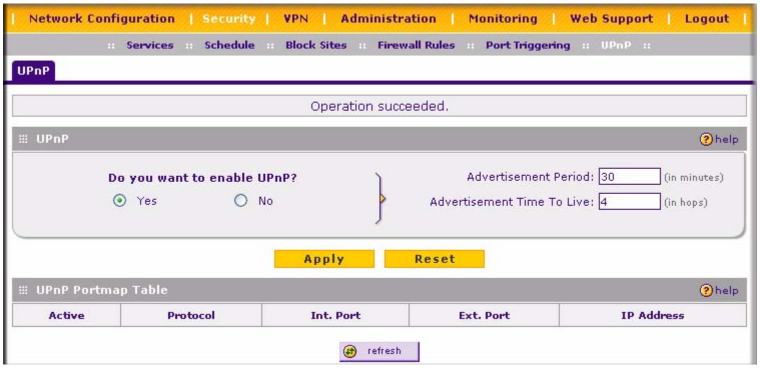
1. Click **Edit** adjacent to the entry you want to modify. The Edit SNMP Configuration screen will display.
2. After making any modifications, click **Apply.** Your changes will display in the SNMP Configuration table.

To view current SNMP System Information for the router:

1. Click the SNMP System Info link at the top right of the SNMP screen. The SNMP System Information screen displays the current SNMP configuration of the router.
2. The following MIB (Management Information Base) fields are displayed and be modified:
   - **SysContact**: The name of the contact person for this router. Examples: admin, John Doe.
   - **SysLocation**: The physical location of the router: Example: Rack #2, 4th Floor.
   - **SysName**: A name given for easy identification of the router.
3. Click **Apply** to save any changes made to SNMP System Information for this router.

Enabling Universal Plug and Play (UPnP)

UPnP (Universal Plug and Play) allows for automatic discovery of devices that can communicate with this router. This feature should be used with caution as it breaches firewall security. Select Security > UPnP to display the UPnP screen.



Operation succeeded.

UPnP

Do you want to enable UPnP?

● Yes ○ No

Advertisement Period: 30 (in minutes)

Advertisement Time To Live: 4 (in hops)

UPnP Portmap Table

Active	Protocol	Int. Port	Ext. Port	IP Address

Figure 8-8

To enable UPnP:

1. Select the **Yes** radio box for **Do you want to enable UPnP?** to enable UPnP. If disabled, the router will not allow for automatic device configuration.
2. Enter an Advertisement Period, in minutes, for how often this wireless gateway should broadcast its UPnP information to all devices within range.
3. Enter an Advertisement Time to Live, expressed in hops, for each UPnP packet. (This is the number of steps a packet is allowed to propagate before being discarded. Small values will limit the UPnP broadcast range (recommended).)
4. Click **Apply** to save your changes.

Chapter 9
Troubleshooting

This chapter gives information about troubleshooting your ProSafe 802.11g Wireless VPN Firewall. After each problem description, instructions are provided to help you diagnose and solve the problem.

Basic Functioning

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

1. When power is first applied, verify that the PWR LED is on.
2. After approximately 30 seconds, verify that:
    a. The TEST LED is not lit.
    b. The LAN port LEDs are lit for any local ports that are connected.
    c. The Internet port LED is lit.

    If a port's LED is lit, a link has been established to the connected device. If a LAN port is connected to a 100 Mbps device, verify that the port's LED is green. If the port is 10 Mbps, the LED will be green.

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 firewall is turned on:

- Make sure that the power cord is properly connected to your 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 firewall is turned on, the LEDs turn on briefly 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 firewall recovers.
- Clear the firewall's configuration to factory defaults. This will set the firewall's IP address to 192.168.0.1. This procedure is explained in "Restoring the Default Configuration and Password" on page 9-6.

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

LAN or Internet Port LEDs Not On

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

- Make sure that the Ethernet cable connections are secure at the 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 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 firewall's Web Configuration interface from a PC on your local network, check the following:

- Check the Ethernet connection between the PC and the firewall as described in the previous section.
- Make sure your PC's IP address is on the same subnet as the firewall. If you are using the recommended addressing scheme, your PC's address should be in the range of 192.168.0.2 to 192.168.0.254.

Note: If your PC's IP address is shown as 169.254.x.x: Recent versions of 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 firewall and reboot your PC.

- If your firewall's IP address has been changed and you don't know the current IP address, clear the firewall's configuration to factory defaults. This will set the firewall's IP address to 192.168.0.1. This procedure is explained in "Restoring the Default Configuration and Password" on page 9-6.
- 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 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 firewall is unable to access the Internet, you should first determine whether the firewall is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your 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 select an external site such as http://www.netgear.com
2. Access the main menu of the firewall's configuration at *http://192.168.0.1*
3. Under the Maintenance heading, select **Router Status**
4. Check that an IP address is shown for the WAN Port
   If 0.0.0.0 is shown, your firewall has not obtained an IP address from your ISP.

If your 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 firewall by performing the following procedure:

1. Turn off power to the cable or DSL modem.
2. Turn off power to your 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 firewall.

If your 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 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 firewall’s MAC address.

  OR

  Configure your firewall to spoof your PC’s MAC address. This can be done in the Basic Settings menu. Refer to “Manually Configuring your Internet Connection” on page 2-7.

If your 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. Alternatively, you may configure your PC manually with DNS addresses, as explained in your operating system documentation.
- Your PC may not have the firewall configured as its TCP/IP gateway.

  If your PC obtains its information from the firewall by DHCP, reboot the PC and verify the gateway address.

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 Firewall

You can ping the 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 the **Start** button and select **Run**.
2. In the field provided, type ping followed by the IP address of the firewall, as in this example:

   ping 192.168.0.1

3. Click on **OK**.

   You should see a message like this one:

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

   If the path is working, you see this message:

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

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

   ```
   Request timed out
   ```

   If the path is not functioning correctly, you 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 Internet Port LEDs Not On" on page 9-2".
     - 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 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 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 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. Verify that the IP address of the firewall is listed as the default gateway.
- 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 firewall to "clone" or "spoof" the MAC address from the authorized PC. Refer to "Manually Configuring your 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 firewall's administration password to **password** and the IP address to 192.168.0.1. You can erase the current configuration and restore factory defaults in two ways:

- Use the Revert to Factory default settings function of the firewall (see "Backing Up and Restoring Settings" on page 7-5).

- Use the **Reset** button on the rear panel of the firewall. Use this method for cases when the administration password or IP address are not known.

  a. Press and hold the **Reset** button until the Test LED turns on and begins blinking (about 10 seconds).

  b. Release the **Reset** button and wait for the firewall to reboot.

Problems with Date and Time

The E-Mail menu in the Content Filtering section 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 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 firewall, wait at least five minutes and check the date and time again.
- Time is off by one hour. Cause: The firewall does not automatically sense Daylight Savings Time. In the E-Mail menu, check or uncheck the box marked **Adjust for Daylight Savings Time**.

Appendix A
Default Settings and Technical Specifications

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 below. (The Factory Default Restore button on the rear panel is shown in the illustration "The FVG318 Rear Panel" on page 1-6.)
- Pressing the reset button for a shorter period of time will simply cause your device to reboot.

After you install the VPN firewall, use the procedures below to customize any of the settings to better meet your networking needs.

Feature		**Default Behavior**
Router Login		
	User Login URL	http://192.168.0.1
	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	192.168.0.1
	Subnet Mask	255.255.255.0
	RIP Direction	None
	RIP Version	Disabled
	RIP Authentication	None
	DHCP Server	Enabled

Feature		Default Behavior
	DHCP Starting IP Address	192.168.0.2
	DHCP Ending IP Address	192.168.0.100
	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
Wireless		
	SSID Name	NETGEAR
	Security	Disabled
	SSID Broadcast	Enabled
	Transmission Speed	Auto[a]
	Country/Region	United States (in North America; otherwise, varies by region)
	RF Channel	11 until the region is selected
	Operating Mode	g and b until the region is selected
	Data Rate	Best
	Output Power	Full
	Access Point	Enabled
	Authentication Type	Open System
	Wireless Card Access List for Access Point Connections	All wireless stations allowed

[a] Maximum Wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

Technical Specifications

This appendix provides technical specifications for the ProSafe 802.11g Wireless VPN Firewall.

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 @ 1.2 A output, 18W maximum
Physical Specifications		
	Dimensions:	39.6 x 254 x 178 mm (1.6 x 10 x 7 in)
	Weight:	1.23 kg (2.72 lb)
Environmental Specifications		
	Operating temperature:	0° to 40° C (32º to 104º 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:	10BASE-T or 100BASE-Tx, RJ-45
	WAN:	10BASE-T or 100BASE-Tx, RJ-45

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
Windows XP and Vista Wireless Configuration Utilities	*http://documentation.netgear.com/reference/enu/winzerocfg/index.htm*
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
VPN Configuration of NETGEAR FVG318

This is a case study on how to configure a secure IPSec VPN tunnel on a NETGEAR FVS318v3. This case study follows the VPN Consortium interoperability profile guidelines (found at *http://www.vpnc.org/InteropProfiles/Interop-01.html*).

This study covers the following situations:

- FVS318v3 to FVS318v3 (see page C-3)
- FVS318v3 to FVS318v2 (see page C-7)
- FVS318v3 to FVL328 (see page C-10)
- FVS318v3 to VPN Client (see page C-13)

➡	**Note:** Product updates are available on the NETGEAR, Inc. Web site at *http://www.netgear.com/support/main.asp*.

Case Study Overview

The procedure for configuring a VPN tunnel between two gateway endpoints is as follows:

1. Gather the network information
2. Configure gateway A
3. Configure gateway B
4. Activate the VPN tunnel

Gathering the Network Information

The configuration in this document follows the addressing and configuration mechanics defined by the VPN Consortium. Gather all the necessary information before you begin the configuration process. Verify whether the firmware is up to date, all of the addresses that will be necessary, and all of the parameters that need to be set on both sides. Check that there are no firewall restrictions.

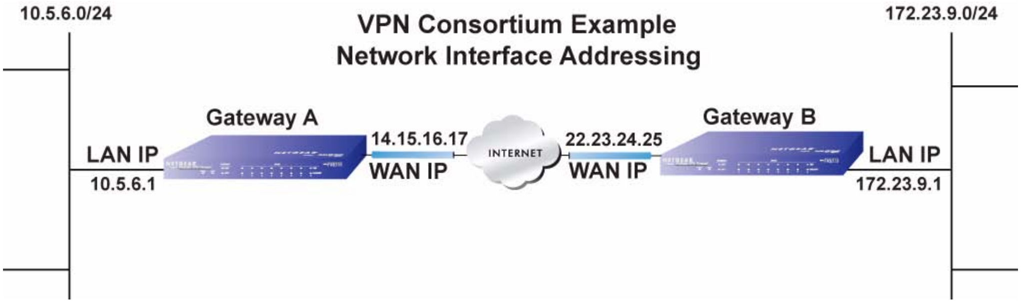


Figure C-1

Configuring the Gateways

Configure each gateway:

1. Configure Gate A.
   a. **Log in to the router at Gateway A.**
   b. **Use the VPN Wizard to configure this router.**

      Enter the requested information as prompted by the VPN Wizard:
      - Connection Name and Pre-Shared Key
      - Remote WAN IP address
      - Remote LAN IP Subnet: IP Address and Subnet Mask:
2. Repeat the above steps for Gateway B.
   a. **Log in to the router at Gateway B.**
   b. **Use the VPN Wizard to configure this router.**

      Enter the requested information as prompted by the VPN Wizard.

Note: The WAN and LAN IP addresses must be unique at each end of the VPN tunnel.

Note: The default log in address for the FVG318 router is **http://192.168.0.1** with the default user name of **admin** and default password of **password**. The login address will change to the local LAN IP subnet address after you configure the router. The user name and password will also change to the ones you have chosen to use in your installation.

Activating the VPN Tunnel

You can activate the VPN tunnel by testing connectivity and viewing the VPN tunnel status information as described in the following flowchart:

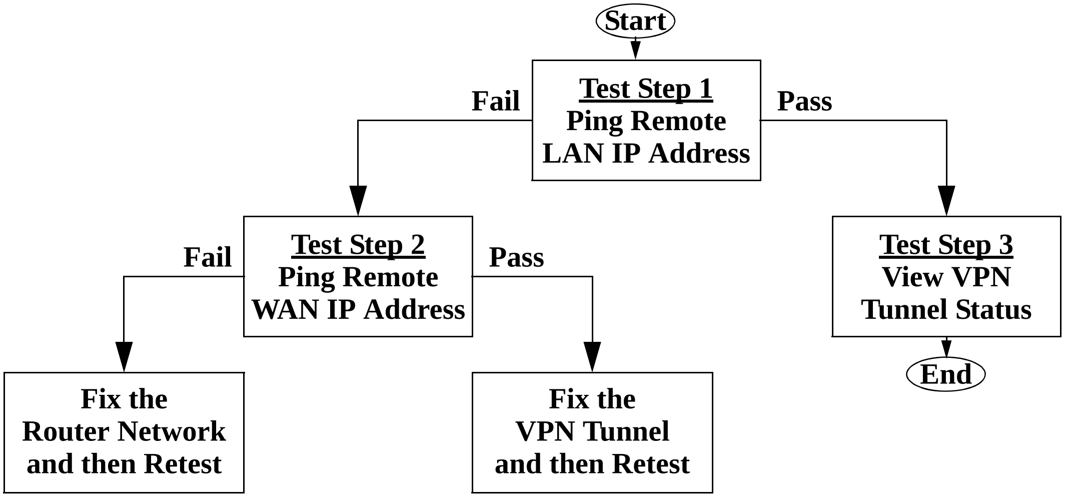


Figure C-2

All traffic from the range of LAN IP addresses specified on the router at Gateway A and the router at Gateway B will now flow over a secure VPN tunnel.

The FVG318-to-FVG318 Case

Table C-1. Policy Summary

VPN Consortium Scenario:	Scenario 1
Type of VPN	LAN-to-LAN or Gateway-to-Gateway

Table C-1. Policy Summary

Security Scheme:		IKE with Preshared Secret/Key
IP Addressing:		
	NETGEAR-Gateway A	Static IP address
	NETGEAR-Gateway B	Static IP address

Configuring the VPN Tunnel

This scenario assumes all ports are open on the FVG318.

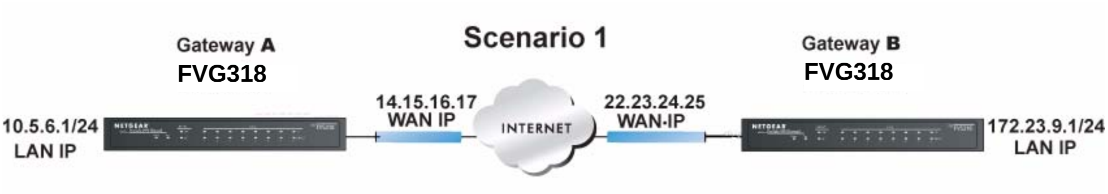


Figure C-3

Use this scenario illustration and configuration screens as a model to build your configuration.

1. Log in to the FVG318 labeled Gateway A.

   Log in at the default address of **http://192.168.0.1** with the default user name of **admin** and default password of **password** (or using whatever password and LAN address you have chosen).

   > **Note:** Based on the network addresses used in this example, you would log in to the LAN IP address of **http://10.5.6.1** at Gateway A.

2. Use the VPN Wizard to configure the FVG318 at Gateway A.
   - Connection Name: **Scenario_1** (in this example)
   - Pre-Shared Key: **12345678** (in this example), must be the same at both VPN tunnel endpoints
   - Remote WAN IP address: **22.23.24.25** (in this example), must be unique at each VPN tunnel endpoint
   - Remote LAN IP Subnet
     - IP Address: **172.23.9.1** (in this example), must be unique at each VPN tunnel endpoint

  - Subnet Mask: **255.255.255.0** (in this example)

3. Log in to the FVG318 labeled Gateway B.

Log in at the default address of **http://192.168.0.1** with the default user name of **admin** and default password of **password** (or using whatever password and LAN address you have chosen).

> **Note:** Based on the network addresses used in this example, you would log in to the LAN IP address of **http://172.23.9.1** at Gateway B

4. Repeat the process using the VPN Wizard to configure the FVG318 at Gateway B.

- Connection Name: **Scenario_1** (in this example)
- Pre-Shared Key: **12345678** (in this example), must be the same at both VPN tunnel endpoints
- Remote WAN IP address: **14.15.16.17** (in this example), must be unique at each VPN tunnel endpoint
- Remote LAN IP Subnet
  - IP Address: **10.5.6.1** (in this example), must be unique at each VPN tunnel endpoint
  - Subnet Mask: **255.255.255.0** (in this example)

All traffic from the range of LAN IP addresses specified on FVG318 A and FVG318 B will now flow over a secure VPN tunnel once the VPN tunnel is initiated (see "Initiating and Checking the VPN Connections" on page C-6).

Viewing and Editing the VPN Parameters

The VPN Wizard sets up a VPN tunnel using the default parameters from the VPN Consortium (VPNC).

- The Pre-Shared Key must be the same at both VPN tunnel endpoints.
- The remote WAN and LAN IP addresses for one VPN tunnel endpoint will be the local WAN and LAN IP addresses for the other VPN tunnel endpoint.
- The VPN Wizard ensures the other VPN parameters are the same at both VPN tunnel endpoints.

Initiating and Checking the VPN Connections

You can test connectivity and view VPN status information on the FVG318 according to the testing flowchart shown in Figure C-2. To test the VPN tunnel from the Gateway A LAN, do the following:

1. Test 1: Ping Remote LAN IP Address: To establish the connection between the FVG318 Gateway A and Gateway B tunnel endpoints, perform these steps at Gateway A:
   - **a.** From a Windows PC attached to the FVG318 on LAN A, click the **Start** button on the task bar and then click **Run**.
   - **b.** Type **ping -t 172.23.9.1**, and then click **OK** (you would type **ping -t 10.5.6.1** if testing from Gateway B).
   - **c.** This will cause a continuous ping to be sent to the LAN interface of Gateway B. Within two minutes, the ping response should change from timed out to reply.

   At this point the VPN-tunnel-endpoint-to-VPN-tunnel-endpoint connection is established.
2. Test 2: Ping Remote WAN IP Address (if Test 1 fails): To test connectivity between the Gateway A and Gateway B WAN ports, follow these steps:
   - **a.** Log in to the router on LAN A, go to the main menu Maintenance section, and click the **Diagnostics** link.
   - **b.** To test connectivity to the WAN port of Gateway B, enter **22.23.24.25**, and then click **Ping** (you would enter **14.15.16.17** if testing from Gateway B).
   - **c.** This causes a ping to be sent to the WAN interface of Gateway B. Within two minutes, the ping response should change from timed out to reply. You may have to run this test several times before you get the reply message back from the target FVG318.
   - **d.** At this point the gateway-to-gateway connection is verified.
3. Test 3: View VPN Tunnel Status: To view the FVG318 event log and status of Security Associations, follow these steps:
   - **a.** Go to the FVG318 main menu VPN section and click the **VPN Status** link.
   - **b.** The log screen displays a history of the VPN connections, and the IPSec SA and IKE SA tables report the status and data transmission statistics of the VPN tunnels for each policy.

The FVG318-to-FVS318v2 Case

Table C-2. Policy Summary

VPN Consortium Scenario:		Scenario 1
Type of VPN		LAN-to-LAN or Gateway-to-Gateway
Security Scheme:		IKE with Preshared Secret/Key
Date Tested:		November 2004
IP Addressing:		
	NETGEAR-Gateway A	Static IP address
	NETGEAR-Gateway B	Static IP address

Configuring the VPN Tunnel

This scenario assumes all ports are open on the FVG318 and FVS318v2.

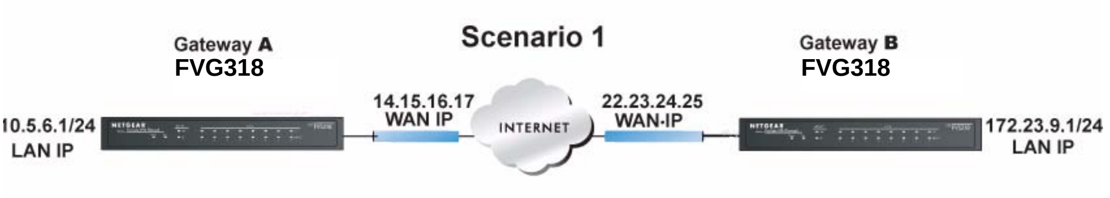


Figure C-4

Use this scenario illustration and configuration screens as a model to build your configuration.

1. Log in to the FVG318 labeled Gateway A as in the illustration (Figure C-4).

   Log in at the default address of **http://192.168.0.1** with the default user name of **admin** and default password of **password** (or using whatever password and LAN address you have chosen).

   > **Note:** Based on the network addresses used in this example, you would log in to the LAN IP address of **http://10.5.6.1** at Gateway A.
   >
   > **Note:**

2. Use the VPN Wizard to configure the FVG318 at Gateway A.

- Connection Name: **Scenario_1** (in this example)
- Pre-Shared Key: **12345678** (in this example), must be the same at both VPN tunnel endpoints
- Remote WAN IP address: **22.23.24.25** (in this example), must be unique at each VPN tunnel endpoint
- Remote LAN IP Subnet
  - IP Address: **172.23.9.1** (in this example), must be unique at each VPN tunnel endpoint
  - Subnet Mask: **255.255.255.0** (in this example)

3. Log in to the FVS318v2 labeled Gateway B.

Log in at the default address of **http://192.168.0.1** with the default user name of **admin** and default password of **password** (or using whatever password and LAN address you have chosen).

> **Note:** Based on the network addresses used in this example, you would log in to the LAN IP address of **http://172.23.9.1** at Gateway B.

4. Repeat the process using the VPN Wizard to configure the FVS318v2 at Gateway B.

- Connection Name: **Scenario_1** (in this example)
- Pre-Shared Key: **12345678** (in this example), must be the same at both VPN tunnel endpoints
- Remote WAN IP address: **14.15.16.17** (in this example), must be unique at each VPN tunnel endpoint
- Remote LAN IP Subnet
  - IP Address: **10.5.6.1** (in this example), must be unique at each VPN tunnel endpoint
  - Subnet Mask: **255.255.255.0** (in this example)

All traffic from the range of LAN IP addresses specified on FVG318 A and FVG318 B will now flow over a secure VPN tunnel once the VPN tunnel is initiated (see “Initiating and Checking the VPN Connections” on page C-9).

Viewing and Editing the VPN Parameters

The VPN Wizard sets up a VPN tunnel using the default parameters from the VPN Consortium (VPNC).

- The Pre-Shared Key must be the same at both VPN tunnel endpoints.

- The remote WAN and LAN IP addresses for one VPN tunnel endpoint will be the local WAN and LAN IP addresses for the other VPN tunnel endpoint.
- The VPN Wizard ensures the other VPN parameters are the same at both VPN tunnel endpoints.

Initiating and Checking the VPN Connections

You can test connectivity and view VPN status information on the FVG318 according to the testing flowchart shown in Figure C-2. To test the VPN tunnel from the Gateway A LAN, do the following:

1. Test 1: Ping Remote LAN IP Address: To establish the connection between the FVG318 Gateway A and FVS318v2 Gateway B tunnel endpoints, perform these steps at Gateway A:

   a. From a Windows PC attached to the FVG318 on LAN A, click the **Start** button on the task bar and then click **Run**.

   b. Type **ping -t 172.23.9.1**, and then click **OK** (you would type **ping -t 10.5.6.1** if testing from Gateway B).

   c. This will cause a continuous ping to be sent to the LAN interface of Gateway B. Within two minutes, the ping response should change from timed out to reply.

   At this point the VPN-tunnel-endpoint-to-VPN-tunnel-endpoint connection is established.

2. Test 2: Ping Remote WAN IP Address (if Test 1 fails): To test connectivity between the Gateway A and Gateway B WAN ports, follow these steps:

   a. Log in to the router on LAN A, go to the main menu Maintenance section, and click the **Diagnostics** link.

   b. To test connectivity to the WAN port of Gateway B, enter **22.23.24.25**, and then click **Ping** (you would enter **14.15.16.17** if testing from Gateway B).

   c. This causes a ping to be sent to the WAN interface of Gateway B. Within two minutes, the ping response should change from timed out to reply. You may have to run this test several times before you get the reply message back from the target FVS318v2.

   d. At this point the gateway-to-gateway connection is verified.

3. Test 3: View VPN Tunnel Status: To view the FVG318 VPN event logs, go to Monitoring > VPN Logs; to view the status of Security Associations, go to the FVG318 VPN > Connection Status. For the FVS318v2, click Show VPN Status from the Router Status screen.

The FVG318-to-FVL328 Case

Table C-3. Policy Summary

VPN Consortium Scenario:		Scenario 1
Type of VPN		LAN-to-LAN or Gateway-to-Gateway
Security Scheme:		IKE with Preshared Secret/Key
IP Addressing:		
	NETGEAR-Gateway A	Static IP address
	NETGEAR-Gateway B	Static IP address

Configuring the VPN Tunnel

This scenario assumes all ports are open on the FVG318 and FVL328.

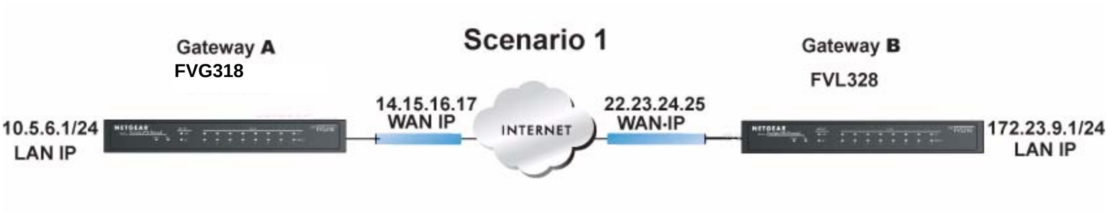


Figure C-5

Use this scenario illustration and configuration screens as a model to build your configuration.

1. Log in to the FVG318 labeled Gateway A.

   Log in at the default address of **http://192.168.0.1** with the default user name of **admin** and default password of **password** (or using whatever password and LAN address you have chosen).

   > **Note:** Based on the network addresses used in this example, you would log in to the LAN IP address of **http://10.5.6.1** at Gateway A.

2. Use the VPN Wizard to configure the FVG318 at Gateway A.
   - Connection Name: **Scenario_1** (in this example)

- Pre-Shared Key: **12345678** (in this example), must be the same at both VPN tunnel endpoints
- Remote WAN IP address: **22.23.24.25** (in this example), must be unique at each VPN tunnel endpoint
- Remote LAN IP Subnet
  - IP Address: **172.23.9.1** (in this example), must be unique at each VPN tunnel endpoint
  - Subnet Mask: **255.255.255.0** (in this example)

3. Log in to the FVL328 labeled Gateway B.

Log in at the default address of **http://192.168.0.1** with the default user name of **admin** and default password of **password** (or using whatever password and LAN address you have chosen).

> ➡ **Note:** Based on the network addresses used in this example, you would log in to the LAN IP address of **http://172.23.9.1** at Gateway B.

4. Repeat the process using the VPN Wizard to configure the FVL328 at Gateway B.

- Connection Name: **Scenario_1** (in this example)
- Pre-Shared Key: **12345678** (in this example), must be the same at both VPN tunnel endpoints
- Remote WAN IP address: **14.15.16.17** (in this example), must be unique at each VPN tunnel endpoint
- Remote LAN IP Subnet
  - IP Address: **10.5.6.1** (in this example), must be unique at each VPN tunnel endpoint
  - Subnet Mask: **255.255.255.0** (in this example)

All traffic from the range of LAN IP addresses specified on FVG318 A and FVL328 B will now flow over a secure VPN tunnel once the VPN tunnel is initiated (see "Initiating and Checking the VPN Connections" on page C-12).

Viewing and Editing the VPN Parameters

The VPN Wizard sets up a VPN tunnel using the default parameters from the VPN Consortium (VPNC).

- The Pre-Shared Key must be the same at both VPN tunnel endpoints.

- The remote WAN and LAN IP addresses for one VPN tunnel endpoint will be the local WAN and LAN IP addresses for the other VPN tunnel endpoint.
- The VPN Wizard ensures the other VPN parameters are the same at both VPN tunnel endpoints.

Initiating and Checking the VPN Connections

You can test connectivity and view VPN status information on the FVG318 and FVL328 according to the testing flowchart shown in Figure C-2. To test the VPN tunnel from the Gateway A LAN, do the following:

1. Test 1: Ping Remote LAN IP Address: To establish the connection between the FVG318 Gateway A and FVL328 Gateway B tunnel endpoints, perform these steps at Gateway A:
   a. From a Windows PC attached to the FVG318 on LAN A, click the **Start** button on the task bar and then click **Run**.
   b. Type **ping -t 172.23.9.1**, and then click **OK** (you would type **ping -t 10.5.6.1** if testing from Gateway B).
   c. This will cause a continuous ping to be sent to the LAN interface of Gateway B. Within two minutes, the ping response should change from timed out to reply.

   At this point the VPN-tunnel-endpoint-to-VPN-tunnel-endpoint connection is established.
2. Test 2: Ping Remote WAN IP Address (if Test 1 fails): To test connectivity between the Gateway A and Gateway B WAN ports, follow these steps:
   a. Log in to the router on LAN A, go to the main menu Maintenance section, and click the **Diagnostics** link.
   b. To test connectivity to the WAN port of Gateway B, enter **22.23.24.25**, and then click **Ping** (you would enter **14.15.16.17** if testing from Gateway B).
   c. This causes a ping to be sent to the WAN interface of Gateway B. Within two minutes, the ping response should change from timed out to reply. You may have to run this test several times before you get the reply message back from the target FVL328.
   d. At this point the gateway-to-gateway connection is verified.
3. Test 3: View VPN Tunnel Status: To view the FVG318 and FVL328 event log and status of Security Associations; go to the FVG318 main menu and select VPN > Connection Status. For the FVL328, click VPN Status on the VPN Status/Log screen.

The FVG318-to-VPN Client Case

Table C-4. Policy Summary

VPN Consortium Scenario:		Scenario 1
Type of VPN		PC/Client-to-Gateway
Security Scheme:		IKE with Preshared Secret/Key
Date Tested:		November 2004
IP Addressing:		
	NETGEAR-Gateway A	Static IP address
	NETGEAR-Client B	Dynamic IP address

Client-to-Gateway VPN Tunnel Overview

The operational differences between gateway-to-gateway and client-to-gateway VPN tunnels are summarized as follows:

Table C-5. Differences between VPN tunnel types

Operation	**Gateway-to-Gateway VPN Tunnels**	**Client-to-Gateway VPN Tunnels**
Exchange Mode	**Main Mode**—The IP addresses of both gateways are known (especially when FQDN is used), so each gateway can use the Internet source of the traffic for validation purposes.	**Aggressive Mode**—The IP address of the client is not known in advance, so the gateway is programmed to accept valid traffic sourced from any Internet location (i.e., less secure).
Direction/Type	**Both Directions**—Either end of the VPN tunnel may initiate traffic (usually).	**Remote Access**—The client end of the VPN tunnel must initiate traffic because its IP address is not know in advance, which prevents the gateway end of the VPN tunnel from initiating traffic.

Configuring the VPN Tunnel

This scenario assumes all ports are open on the FVG318.

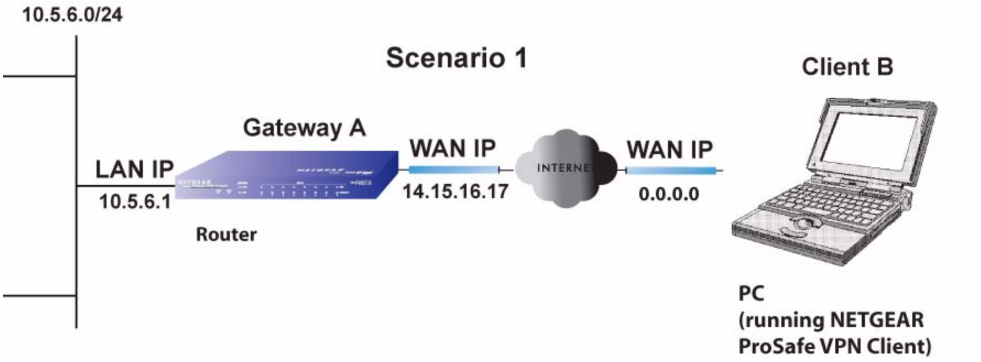


Figure C-6

Use this scenario illustration and configuration screens as a model to build your configuration.

1. Log in to the FVG318 labeled Gateway A

Log in at the default address of **http://192.168.0.1** with the default user name of **admin** and default password of **password** (or using whatever password and LAN address you have chosen).

> **Note:** Based on the network addresses used in this example, you would log in to the LAN IP address of **http://10.5.6.1** at Gateway A

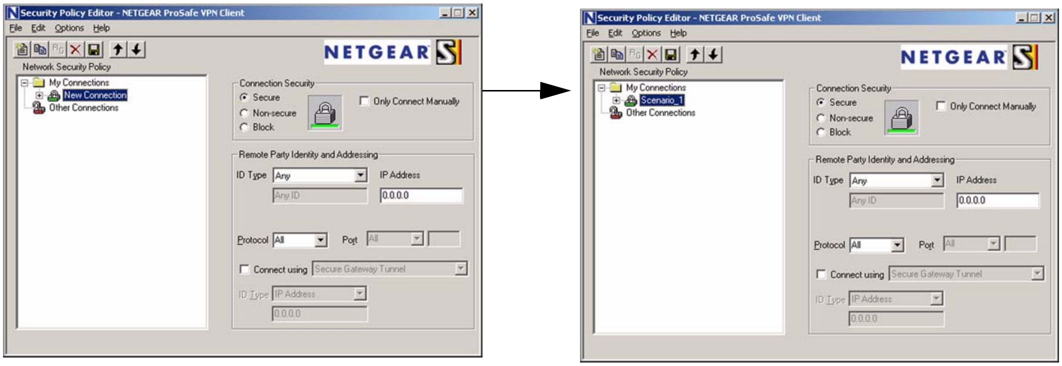
2. Use the VPN Wizard to configure the FVG318 at Gateway A.:

- Connection Name: **Scenario_1** (in this example)
- Pre-Shared Key: **12345678** (in this example), must be the same at both VPN tunnel endpoints
- Connection Type: **A Remote VPN Client**

3. Set up the VPN Client at Gateway B.

a. Right-mouse-click the ProSafe icon (S) in the system tray and select the Security Policy Editor. If you need to install the NETGEAR ProSafe VPN Client on your PC, consult the documentation that came with your software.

b. Add a new connection using the Edit/Add/Connection menu and rename it **Scenario_1**. (**Scenario_1** is used in this example to reflect the fact that the connection uses the Pre-Shared Key security scheme and encryption parameters proposed by the VPN Consortium, but you may want to choose a name for your connection that is meaningful to your specific installation. The name you choose does not have to match the name used at the gateway end of the VPN tunnel.)



Security Policy Editor - NETGEAR ProSafe VPN Client

Network Security Policy
- My Connections
  - New Connection
- Other Connections

Connection Security: ● Secure ○ Non-secure ○ Block — □ Only Connect Manually

Remote Party Identity and Addressing
ID Type: Any — Any ID — IP Address: 0.0.0.0
Protocol: All — Port: All
□ Connect using: Secure Gateway Tunnel
ID Type: IP Address — 0.0.0.0

Security Policy Editor - NETGEAR ProSafe VPN Client

Network Security Policy
- My Connections
  - Scenario_1
- Other Connections

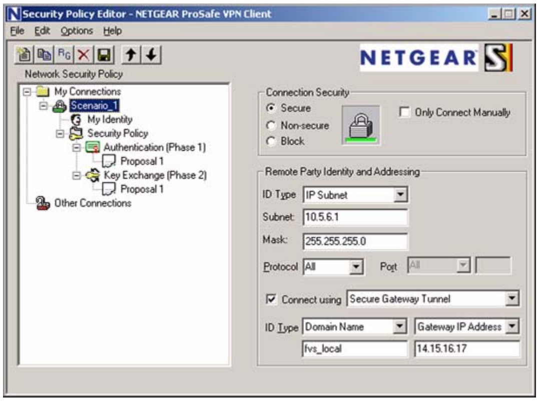
Connection Security: ● Secure ○ Non-secure ○ Block — □ Only Connect Manually

Remote Party Identity and Addressing
ID Type: Any — Any ID — IP Address: 0.0.0.0
Protocol: All — Port: All
□ Connect using: Secure Gateway Tunnel
ID Type: IP Address — 0.0.0.0

Figure C-7

c. Program the **Scenario_1** connection screen as follows (see Figure C-8):

- Connection Security: **Secure**
- Remote Party Identity and Addressing: Select **IP Subnet** from the ID Type menu and then enter **10.5.6.1** for **Subnet**, **255.255.255.0** for **Mask**, and leave **All** for **Protocol**. (The **Subnet** and **Mask** parameters entered here must match the **Start IP address** and **Subnet Mask** parameters of the **Local IP Traffic Selector** on the **VPN Auto policy** screen shown in Figure C-9 for the gateway router.)
- Enable **Connect Using Secure Gateway Tunnel**; select **Domain Name** for **ID_Type**; enter **fvs_local** for **Domain Name**; and enter **14.15.16.17** for **Gateway IP Address**. (**Domain Name** must match the **Local Identity Data** parameter of the **IKE Policy Configuration** screen shown in Figure C-8 for the gateway router. Also, **Gateway IP Address** must match the WAN IP address of the gateway router shown in Figure C-8.)
- Expand the Scenario_1 screen hierarchy by clicking the + sign in front of Scenario_1. Then expand the rest of the screen hierarchies by clicking the rest of the + signs.



Connection Security

● Secure ○ Non-secure ○ Block

□ Only Connect Manually

Remote Party Identity and Addressing

ID Type: IP Subnet

Subnet: 10.5.6.1

Mask: 255.255.255.0

Protocol: All Port: All

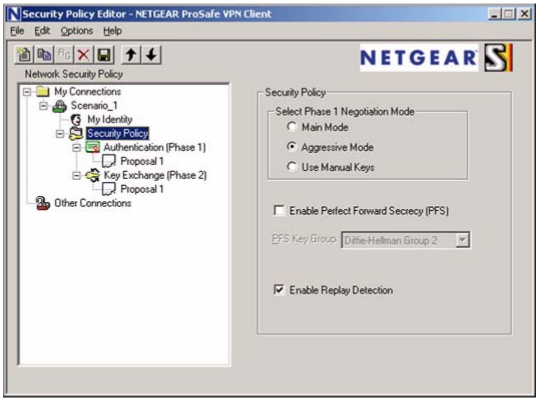
☑ Connect using Secure Gateway Tunnel

ID Type: Domain Name — Gateway IP Address

fvs_local — 14.15.16.17

Figure C-8

d. Select **Security Policy** on the left hierarchy menu and then select **Aggressive Mode** under **Select Phase 1 Negotiation Mode** (see Figure C-9). (The **Select Phase 1 Negotiation Mode** choice must match the **Exchange Mode** setting for the **General IKE Policy Configuration** parameters shown in Figure C-9 for the gateway router.)



Security Policy

Select Phase 1 Negotiation Mode

○ Main Mode

● Aggressive Mode

○ Use Manual Keys

□ Enable Perfect Forward Secrecy (PFS)

PFS Key Group: Diffie-Hellman Group 2

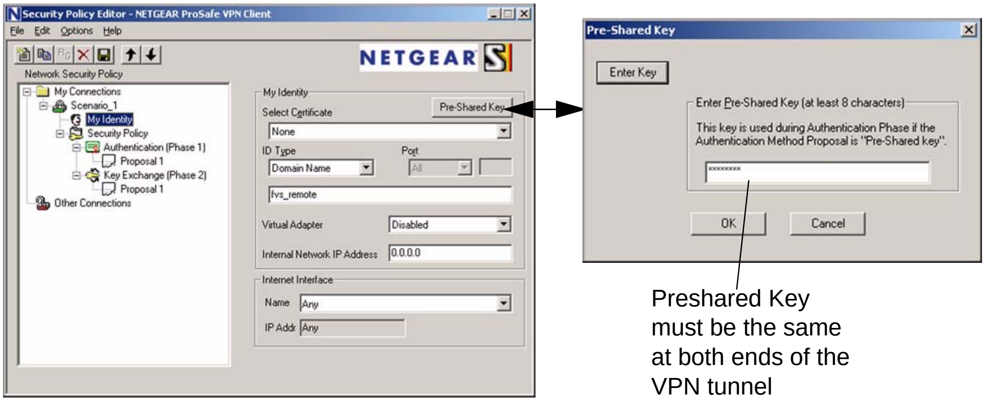
☑ Enable Replay Detection

Figure C-9

e. Select My Identity on the left hierarchy menu and program the screen as follows (see Figure C-10):

- Under **My Identity**, select **None** for **Select Certificate** (since we are using a Pre-Shared Key in this scenario). Then enter **12345678** for the **Pre-Shared Key** value. (The **Preshared-Key** value must match the value you entered in the VPN Wizard for the gateway **Pre-Shared Key** value shown in Figure C-10.)

- Under **My Identity**, select **Domain Name** for the **ID Type** and then enter **fvs_remote**. (**Domain Name** must match the **Remote Identity Data** parameter of the **IKE Policy Configuration** screen shown in Figure C-10 for the gateway router.)



My Identity

Select Certificate: None

ID Type: Domain Name

Port: All

fvs_remote

Virtual Adapter: Disabled

Internal Network IP Address: 0.0.0.0

Internet Interface

Name: Any

IP Addr: Any

Enter Pre-Shared Key (at least 8 characters)

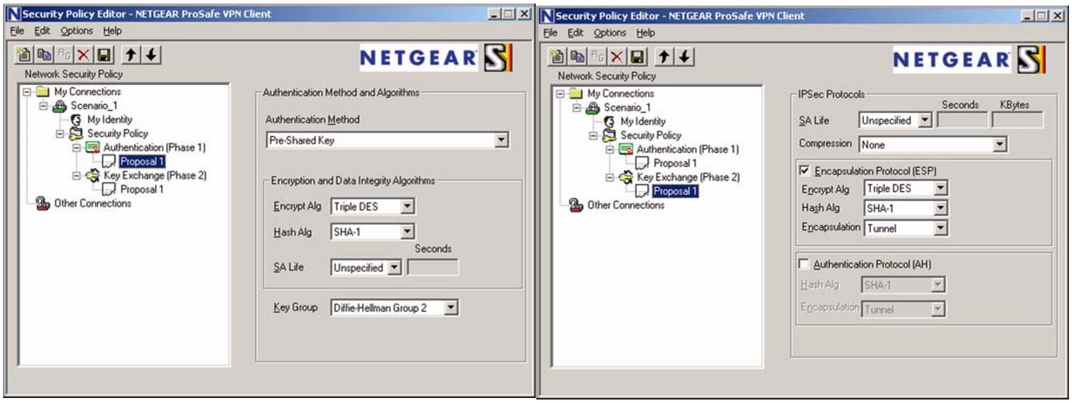
This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".

****

Preshared Key
must be the same
at both ends of the
VPN tunnel

Figure C-10

f. Verify the **Authentication (Phase 1)** and **Key Exchange (Phase 1) Proposal 1** screen parameters (see Figure C-11) match the **IKE SA Parameters** of the **IKE Policy Configuration** screen shown in Figure C-11 for the gateway router.



Authentication Method and Algorithms

Authentication Method: Pre-Shared Key

Encryption and Data Integrity Algorithms

Encrypt Alg: Triple DES

Hash Alg: SHA-1

SA Life: Unspecified Seconds

Key Group: Diffie-Hellman Group 2

IPSec Protocols

SA Life: Unspecified Seconds KBytes

Compression: None

☑ Encapsulation Protocol (ESP)

Encrypt Alg: Triple DES

Hash Alg: SHA-1

Encapsulation: Tunnel

□ Authentication Protocol (AH)

Hash Alg: SHA-1

Encapsulation: Tunnel

Figure C-11

g. Save the **Scenario_1** connection using Save under the File menu. You can also export the connection parameters using Export Security Policy under the File menu.

You are new ready to activate the tunnel, but you must do it from the client endpoint (see "Initiating and Checking the VPN Connections" on page C-18). In the client-to-gateway scenario, the gateway router will not know the client's IP address until the client initiates the traffic.

Initiating and Checking the VPN Connections

You can test connectivity and view VPN status information on the FVG318 and VPN Client according to the testing flowchart shown in Figure C-2. To test the VPN tunnel from the Gateway A LAN, do the following:

1. Test 1: Launch Scenario_1 Connection from Client PC: To check the VPN Connection, you can initiate a request from the remote PC to the VPN router's network by using the Connect option in the VPN Client's menu bar (see Figure C-12). Since the remote PC has a dynamically assigned WAN IP address, it must initiate the request.

   a. Open the popup menu by right-clicking on the system tray icon.

   b. Select **Connect** to open the **My Connections** list.

   c. Choose **Scenario_1**.

   The VPN Client reports the results of the attempt to connect. Once the connection is established, you can access resources of the network connected to the VPN router.

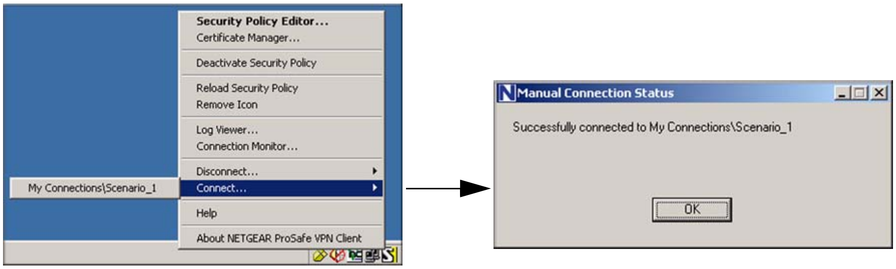
   Alternative Ping Test: To perform a ping test as an alternative, start from the remote PC:

   a. From a Windows Client PC, click the **Start** button on the task bar and then click **Run**.

   b. Type **ping -t 10.5.6.1**, and then click **OK**.

   c. This will cause a continuous ping to be sent to the LAN interface of Gateway A. Within two minutes, the ping response should change from timed out to reply.

   At this point the VPN-tunnel-endpoint-to-VPN-tunnel-endpoint connection is established.



Successfully connected to My Connections\Scenario_1

Figure C-12

2. Test 2: Ping Remote WAN IP Address (if Test 1 fails): To test connectivity between the Gateway A and Gateway B WAN ports, follow these steps:

   a. From a Windows Client PC, click the **Start** button on the task bar and then click **Run**.

   b. Type **ping -t 14.151.6.17**, and then click **OK**.

   c. This causes a ping to be sent to the WAN interface of Gateway A. Within two minutes, the ping response should change from timed out to reply. You may have to run this test several times before you get the reply message back from the target FVS318v3.

   d. At this point the gateway-to-gateway connection is verified.

3. Test 3: View VPN Tunnel Status: To view the FVG318 event log and status of Security Associations, go to the FVG318 main menu VPN section and click the VPN Status link. For the For the VPN Client, click VPN Status on the VPN Status/Log screen.

   a. Open the popup menu by right-clicking on the system tray icon.

   b. Select **Connection Monitor**.