Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318

NETGEAR

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

BETA
Version 1
August 2005

Trademarks

NETGEAR 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.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

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 generates, 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 measures:

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

EN 55 022 Declaration of Conformance

This is to certify that the FVG318 ProSafe 802.11g Wireless VPN Firewall is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das FVG318 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 FVG318 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.

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.

Product and Publication Details

Model Number:	FVG318
Publication Date:	August 2005
Product Family:	Router
Product Name:	FVG318 ProSafe 802.11g Wireless VPN Firewall
Home or Business Product:	Business
Language:	English

Contents

Chapter 1
About This Manual

This chapter describes the intended audience, scope, conventions, and formats of this manual.

Audience, Scope, Conventions, and Formats

This reference manual assumes that the reader has basic to intermediate computer and Internet skills. However, basic computer network, Internet, firewall, and VPN technologies tutorial information is provided in the Appendices and on the NETGEAR Web site.

This guide uses the following typographical conventions:

Table 1-1. Typographical Conventions

italics	Emphasis, books, CDs, URL names
bold	User input
`fixed`	Screen text, file and server names, extensions, commands, IP addresses

This guide uses the following formats to highlight special messages:

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

This manual is written for the FVG318 Wireless VPN Firewall according to these specifications.:

Table 1-2. Manual Scope

Product Version	FVG318 ProSafe 802.11g Wireless VPN Firewall
Manual Publication Date	August 2005

Note: Product updates are available on the NETGEAR, Inc. Web site 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 TOC button that displays the table of contents and an Index 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 Knowledge Base 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 several options, according to your needs.

- **Printing a Page in the HTML View**.

  Each page in the HTML version of the manual is dedicated to a major topic. Use the *Print* button on the browser toolbar to print the page contents.

- **Printing a 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 right of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.

    Note: 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*.

  – Click the print icon in the upper left of the 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.

- **Printing the Full 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 the 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.

Chapter 2
Introduction

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

Key Features of the Wireless VPN Firewall

The FVG318 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 FVG318 Wireless 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 FVG318 Wireless 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 FVG318 Wireless 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 FVG318 Wireless 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 FVG318 Wireless 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, "Network, Routing, and Firewall Basics."

- IP Address Sharing by NAT
  The FVG318 Wireless 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 FVG318 Wireless 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 FVG318 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 FVG318 Wireless 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 FVG318 Wireless VPN Firewall's front panel LEDs provide an easy way to monitor its status and activity.

Maintenance and Support

NETGEAR offers the following features to help you maximize your use of the FVG318 Wireless 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:

- FVG318 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 FVG318 Wireless VPN Firewall contains the status LEDs described below.

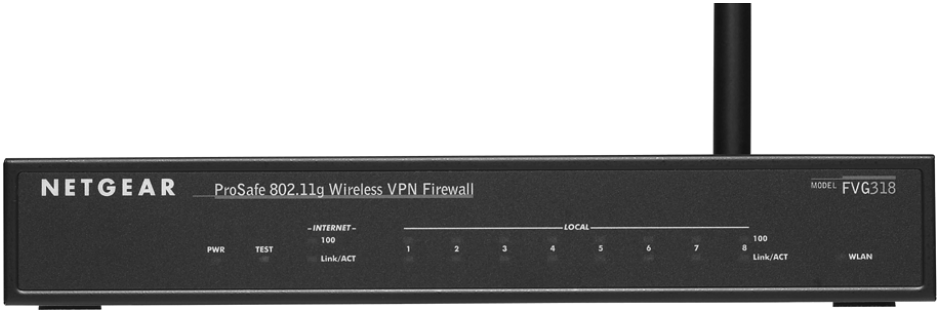


Figure 2-1: FVG318 front panel

You can use some of the LEDs to verify connections. Viewed from left to right, Table 2-1 describes the LEDs on the front panel of the firewall. These LEDs are green when lit.

Table 2-1. 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/Blink Off	The wireless interface is on/data transmission in progress. The wireless interface is off.

The FVG318 Rear Panel

The rear panel of the FVG318 Wireless VPN Firewall contains the port connections listed below.

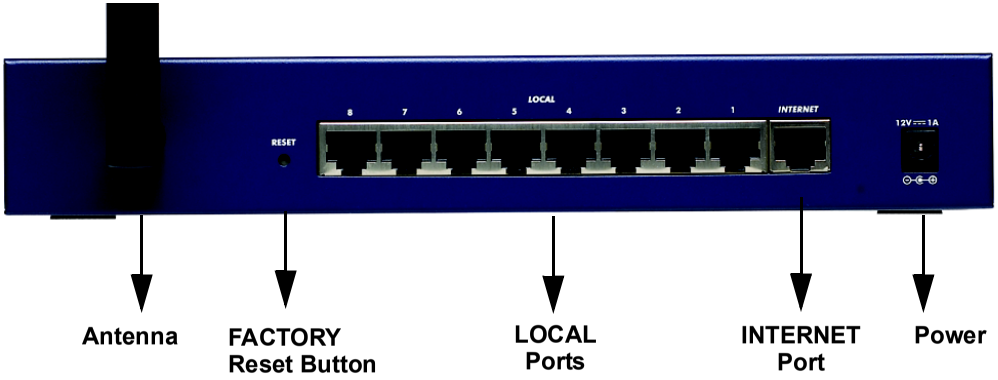


Figure 2-2: FVG318 rear panel

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

NETGEAR-Related Products

NETGEAR products related to the FVG318 are listed in the following table:

Table 2-2. NETGEAR-Related Products

Category	Wireless	Wired
Notebooks	WAG511 108 Mbps Dual Band PC Card WG511T 108 Mbps PC Card WG511 54 Mbps PC Card WG111 54 Mbps USB 2.0 Adapter MA521 802.11b PC Card MA111 802.11b USB Adapter	FA511 CardBus Adapter FA120 USB 2.0 Adapter
Desktops	WAG311 108 Mbps Dual Band PCI Adapter WG311T 108 Mbps PCI Adapter WG311 54 Mbps PCI Adapter WG111 54 Mbps USB 2.0 Adapter MA111 802.11b USB Adapter	FA311 PCI Adapter FA120 USB 2.0 Adapter
PDAs	MA701 802.11b Compact Flash Card	
Antennas and Accessories	ANT24O5 5 dBi Antenna ANT2409 Indoor/Outdoor 9 dBi Antenna ANT24D18 Indoor/Outdoor 18 dBi Antenna Antenna Cables–1.5, 3, 5, 10, and 30 m lengths VPN01L and VPN05L ProSafe VPN Client Software	

NETGEAR Product Registration, Support, and Documentation

Register your product at *http://www.NETGEAR.com/register*. Registration is required before you can use our telephone support service.

Product updates and Web support are always available by going to: *http://kbserver.netgear.com*.

Documentation is available on the *Resource CD* and at *http://kbserver.netgear.com*.

When the wireless VPN firewall is connected to the Internet, click the **Knowledge Base** or the **Documentation** link under the Web Support menu to view support information or the documentation for the wireless VPN firewall.

Chapter 3
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 FVG318 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.

Prepare to Install Your FVG318

- *For Cable Modem Service*: When you set up the wireless VPN firewall, 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 wireless VPN firewall setup.

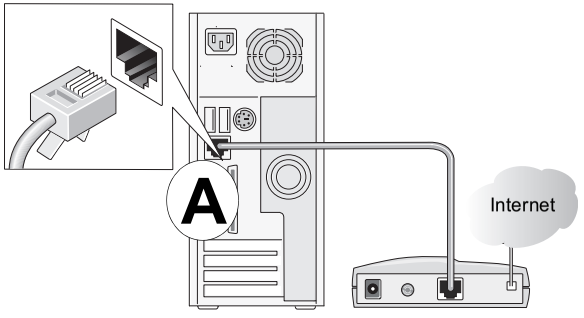
First, Connect the FVG318

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

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

b. Turn off your computer.

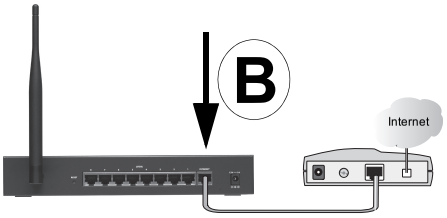
c. At the computer end only, disconnect the Ethernet cable (point **A** in the illustration) that connects your computer to the cable or DSL modem.

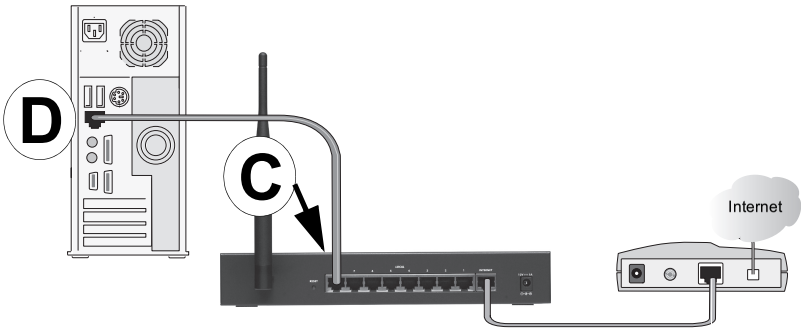


d. Securely insert the Ethernet cable from your modem into the FVG318 Internet port (point **B** in the illustration).

e. Securely insert one end of the blue 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)

.





2. Restart your network in the correct sequence

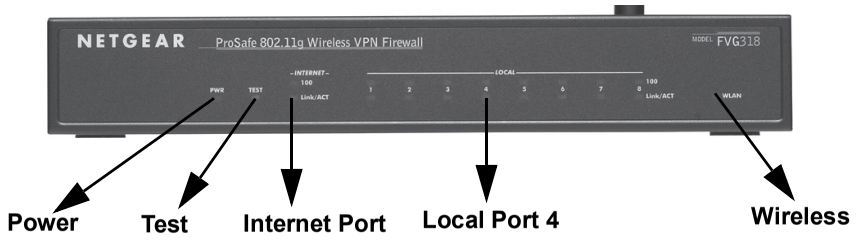
Warning: Failure to restart your network in the correct sequence could prevent you from connecting to the Internet.

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:



- *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 wireless VPN firewall 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.

Now, Configure the FVG318 for Internet Access and Wireless Connectivity

Use the Smart Wizard configuration assistant to configure the FVG318.

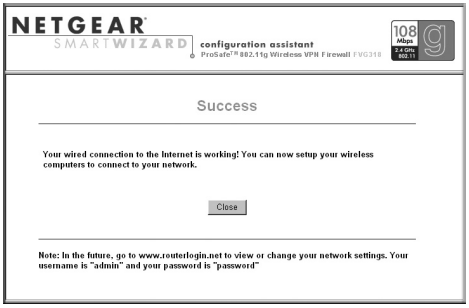
1. From the Ethernet connected computer you just set up, open a browser. With the FVG318 in its factory default state, your browser will display the NETGEAR Smart Wizard welcome page.

   Note: If you do not see this page, type **http://www.routerlogin.net** in the browser address bar and click Enter.

   If you still cannot connect to the FVG318, verify your computer networking setup. Your computer should be set to obtain *both* IP and DNS server addresses automatically, which is usually so. For help with this, please see the *Reference Manual* or animated tutorials on the *Resource CD*.

Click **OK** to proceed.

2. Follow the Smart Wizard prompts to connect to the Internet and set up wireless connectivity.
3. Click **Done** on the Success screen and, if prompted, click **OK** to finish and close the screen.
4. Verify wireless connectivity. Connect to the Internet or log in to the FVG318 from a computer with a wireless adapter. For wireless connectivity problems, see the Troubleshooting Tips below or in the *Reference Manual* on the CD.



Note: The configuration wizard only appears when the FVG318 is in its factory default state. After you configure the FVG318, it will not appear again. You can always connect to the router configuration menu to change its settings. To do so, open a browser and go to **http://www.routerlogin.net**. Then, when prompted, enter **admin** as the user name and **password** for the password both in lower case letters.

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

Overview of How to Access the FVG318 Wireless VPN Firewall

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

Table 3-1. Ways to access the firewall

Firewall State	Access Options	Description
Factory Default **Note**: The wireless VPN firewall is supplied in the factory default state. Also, the factory default state is restored when you use the factory reset button. See "Backing Up the Configuration" on page 8-7 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 wireless VPN firewall, the wireless VPN firewall will automatically connect to that browser and display the Configuration Assistant welcome page. There is no need to enter the wireless VPN firewall 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://www.routerlogin.net/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 wireless VPN firewall 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's Configuration Assistant welcome page rather than the browser's home page.

Table 3-1. Ways to access the firewall (continued)

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

How to Log On to the FVG318 After Configuration Settings Have Been Applied

1. Connect to the wireless VPN firewall by typing **http://www.routerlogin.net** in the address field of your browser, then press **Enter**.

Figure 3-1: Login URL

2. For security reasons, the firewall has its own user name and password. When prompted, enter **admin** for the firewall user name and **password** for the firewall password, both in lower case letters. To change the password, see "Changing the Administrator Password" on page 8-8

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

   A login window like the one shown below opens:

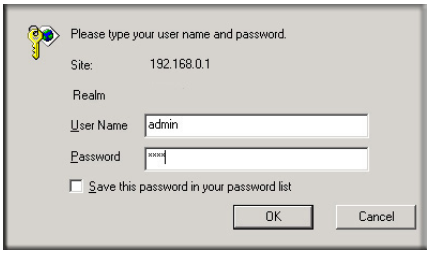


Figure 3-2: Login window

Once you have entered your user name and password, your Web browser should find the FVG318 Wireless VPN Firewall and display the home page as shown below.

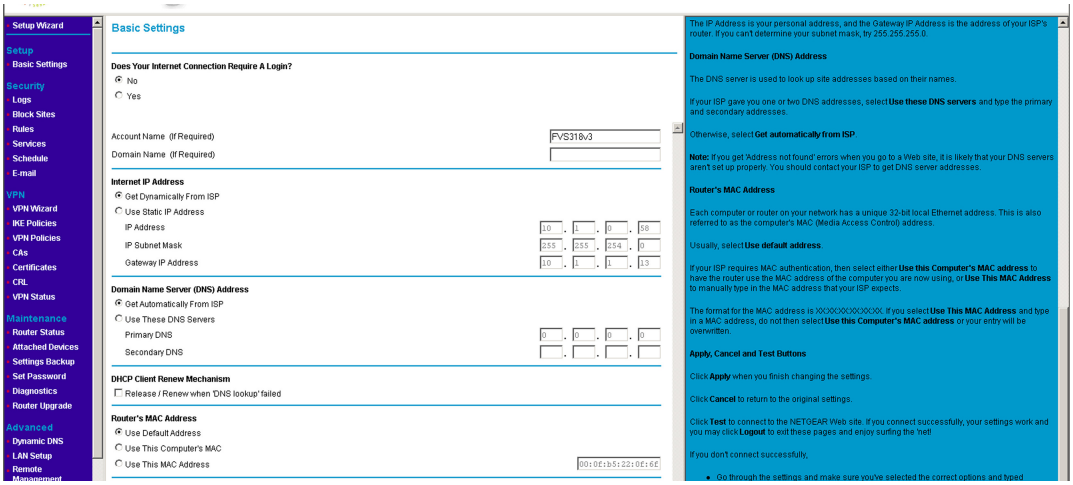


Figure 3-3: Login result: FVG318 home page NEED NEW SCREEN

When the wireless VPN firewall is connected to the Internet, click the **Knowledge Base** or the **Documentation** link under the Web Support menu to view support information or the documentation for the wireless VPN firewall.

If you do not click **Logout**, the wireless VPN firewall will wait five minutes after there is no activity before it automatically logs you out.

How to Bypass the Configuration Assistant

1. When the wireless VPN firewall is in the factory default state, type **http://www.routerlogin.net/basicsetting.htm** in your browser, then press **Enter**.

When the wireless VPN firewall is in the factory default state, a user name and password are not required.

2. The browser then displays the FVG318 settings home page shown in "Login result: FVG318 home page NEED NEW SCREEN" on page 3-8.

   If you do not click **Logout**, the wireless VPN firewall waits five minutes after there is no activity before it automatically logs you out.

Using the Smart Setup Wizard

You can use the Smart Setup Wizard to assist with manual configuration or to verify the Internet connection. The Smart Setup Wizard is not the same as the Smart Wizard Configuration Assistant (as illustrated in Figure 3-5) that only appears when the firewall is in its factory default state. After you configure the wireless VPN firewall, the Smart Wizard Configuration Assistant will not appear again.

To use the Smart Setup Wizard to assist with manual configuration or to verify the Internet connection settings, follow this procedure.

1. Connect to the wireless VPN firewall by typing **http://www.routerlogin.net** in the address field of your browser, then press **Enter**.
2. For security reasons, the firewall has its own user name and password. When prompted, enter **admin** for the firewall user name and **password** for the firewall password, both in lower case letters. To change the password, see "Changing the Administrator Password" on page 8-8

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

   Once you have entered your user name and password, your Web browser should find the FVG318 Wireless VPN Firewall and display the home page as shown in Figure 3-3.
3. Click **Setup Wizard** on the upper left of the main menu.
4. Click **Next** to proceed. Input your ISP settings, as needed.
5. At the end of the Setup Wizard, click the **Test** button to verify your Internet connection. If you have trouble connecting to the Internet, use the Troubleshooting Tips "Troubleshooting Tips" on page 3-4 to correct basic problems, or refer to Chapter 10, "Troubleshooting."

How to Manually Configure Your Internet Connection

You can manually configure your firewall using the menu below, or you can allow the Setup Wizard to determine your configuration as described in the previous section.

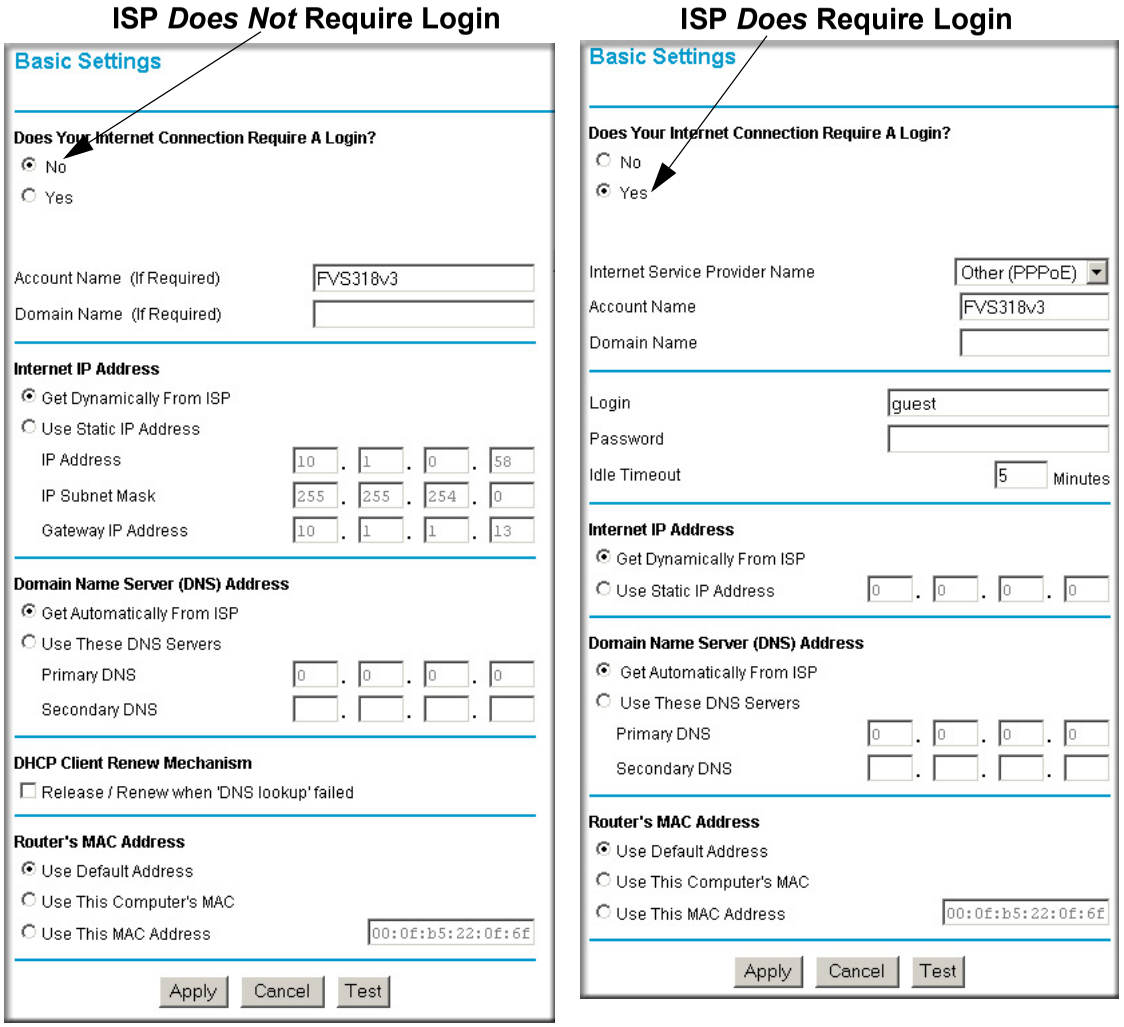


Figure 3-4: Browser-based configuration Basic Settings menu NEED NEW SCREENs

You can manually configure the firewall using the Basic Settings menu shown in Figure 3-4 using these steps:

1. Log in to the firewall at its default address of **http://www.routerlogin.net** using a browser like Internet Explorer or Netscape® Navigator.
2. Click the **Basic Settings** link under the **Setup** section of the main menu.
3. If your Internet connection does not require a login, click **No** at the top of the **Basic Settings** menu and fill in the settings according to the instructions below. If your Internet connection does require a login, click **Yes**, and skip to step 4.

   a. Account:
   Enter your Account Name (may also be called Host Name) and Domain Name. These parameters may be necessary to access your ISP's services such as mail or news servers.

   b. Internet IP Address:
   If your ISP has assigned you a permanent, fixed (static) IP address for your PC, select "Use static IP address". Enter the IP address that your ISP assigned. Also enter the netmask and the Gateway IP address. The Gateway is the ISP's firewall to which your firewall will connect.

   c. Domain Name Server (DNS) Address:
   If you know that your ISP does not automatically transmit DNS addresses to the firewall during login, select "Use these DNS servers" and enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

   Note: After completing the DNS configuration, restart the computers on your network so that these settings take effect.

   d. Firewall's MAC Address:
   This section determines the Ethernet MAC address that will be used by the firewall on the Internet port. Some ISPs will register the Ethernet MAC address of the network interface card in your PC when your account is first opened. They will then only accept traffic from the MAC address of that PC. This feature allows your firewall to masquerade as that PC by "cloning" its MAC address.

   To change the MAC address, select "Use this Computer's MAC address." The firewall will then capture and use the MAC address of the PC that you are now using. You must be using the one PC that is allowed by the ISP. Or, select "Use this MAC address" and enter it.

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

4. If your Internet connection does require a login, fill in the settings according to the instructions below. Select Yes if you normally must launch a login program such as Enternet or WinPOET in order to access the Internet.

   Note: After you finish setting up your firewall, you will no longer need to launch the ISP's login program on your PC in order to access the Internet. When you start an Internet application, your firewall will automatically log you in.

   a. For connections that require a login using protocols such as PPPoE, PPTP, Telstra Bigpond Cable broadband connections, select your Internet service provider from the drop-down list.

Figure 3-5: Basic Settings ISP list

   b. The screen will change according to the ISP settings requirements of the ISP you select.

   c. Fill in the parameters for your ISP according to the Wizard-detected procedures starting on page 3-9.

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

Chapter 4
Wireless Configuration

This chapter describes how to configure the wireless features of your FVG318 Wireless 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 Appendix E, "Wireless Networking Basics."

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

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the FVG318 Wireless VPN Firewall. The latency, data throughput performance, and notebook power consumption also vary depending on your configuration choices. For best results, place your wireless VPN firewall:

- 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

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.

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 FVG318 Wireless VPN Firewall provides highly effective security features which are covered in detail in this chapter.

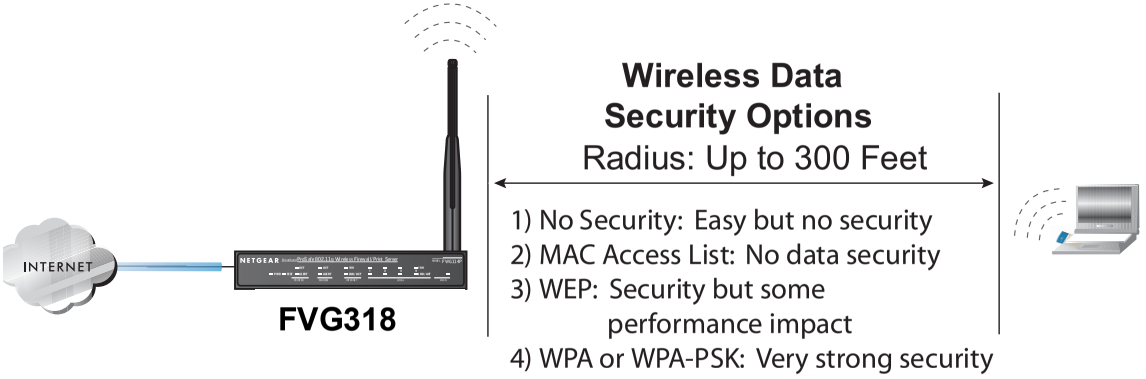


Figure 4-1: FVG318 wireless data security options

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.

- **WPA/WPA2 with Radius or WPA/WPA2-PSK.** Wi-Fi Protected Access (WPA and WPA2) data encryption provides data security. 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.

Understanding Wireless Settings

To configure the wireless settings of your FVG318, click the Wireless link in the Setup section of the main menu. The wireless settings menu will appear, as shown below.

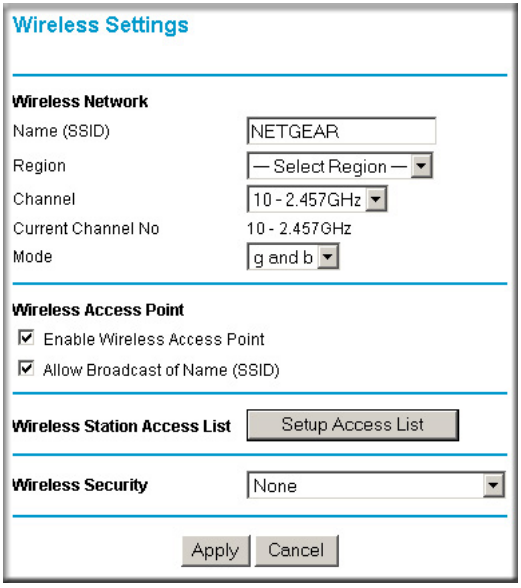


Figure 4-2: Wireless Settings menu

	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 wireless VPN firewall 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 Channels" on page E-7.
  - **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 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. If selected, you must configure the Radius Server Settings.
  - **WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)**: Use WPA-PSK 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, and enter the WPA passphrase (Network key).
  - **WPA-PSK and WPA2-PSK**: This selection allows clients to use either WPA (with AES encryption) or WPA2 (with TKIP encryption). If selected, encryption must be TKIP + AES.

Default Factory Settings

The FVG318 default factory settings shown below. You can restore these defaults with the Factory Default Restore button on the rear panel as seen in the illustration "FWG114P v2 Rear Panel" on page 2-9. After you install the FVG318 Wireless VPN Firewall, use the procedures below to customize any of the settings to better meet your networking needs.

FEATURE	DEFAULT FACTORY SETTINGS
SSID	**NETGEAR**
RF Channel	**11 until the region is selected**
Access Point	**Enabled**
SSID broadcast	**Enabled**
Wireless Card Access List for Access Point Connections	**All wireless stations allowed**
WEP Security	**Disabled**
Authentication Type	**Open System**

Before You Change the SSID and WEP Settings

Take the following steps:

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 wireless VPN firewall 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.

How to Set Up and Test 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.

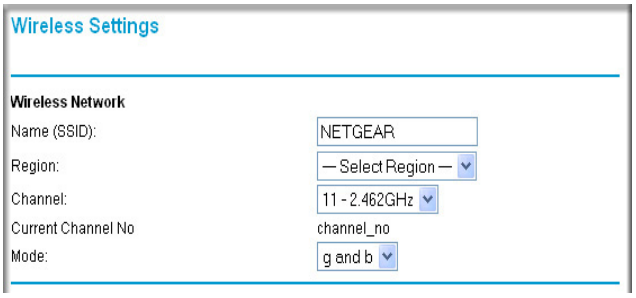


Figure 4-3: Wireless Settings menu

2. Set the Regulatory Domain correctly.
3. 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 FVG318 ProSafe 802.11g Wireless VPN Firewall. If they do not match, you will not get a wireless connection to the FVG318.

4. 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 wireless VPN firewall. For more information on the wireless channel frequencies please refer to "Wireless Channels" on page E-7.

5. Depending on the types of wireless adapters you have in your computers, choose from the Mode drop-down list.
6. For initial configuration and test, leave the Wireless Card Access List set to "All Wireless Stations" and the Encryption Strength set to "Disable."

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

	Note: If you are configuring the FVG318 from a wireless computer and you change the wireless VPN firewall'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.

8. 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 wireless VPN firewall.

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

How to Restrict 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. Click **Wireless** in the main menu of the FVG318. From the Wireless Settings menu, click **Setup Access List**.

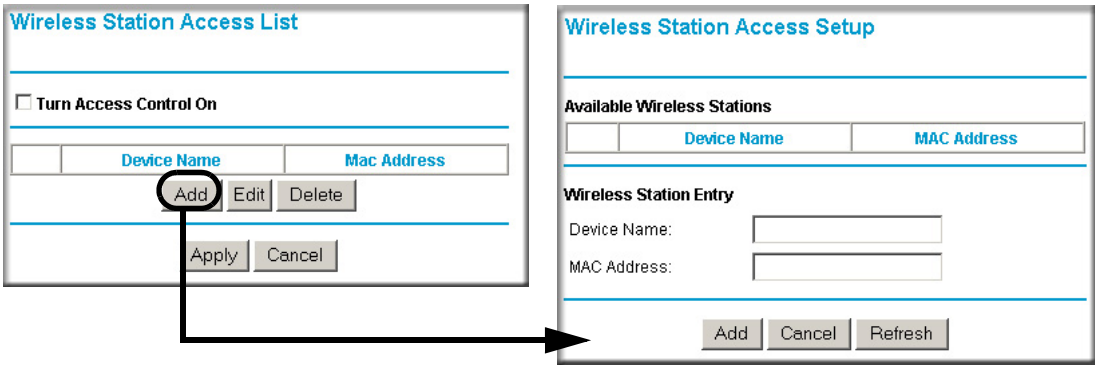


Figure 4-4: Wireless Station Access menu

3. Click the **Turn Access Control On** checkbox to enable MAC filtering.

4. Click **Add** to open the Wireless Card Access Setup menu. You can select a device from the list of available wireless cards the FVG318 has discovered in your area, or you can manually enter the MAC address and Device Name (usually the NetBIOS name).
5. Click **Add** to add this device to your MAC access control 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 wireless VPN firewall from a wired computer or from a wireless computer which is on the access control list to make any further changes.

6. Be sure to click **Apply** to save your trusted wireless PCs list settings. 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 the Delete button.

How to Configure WEP

	**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 wireless VPN firewall 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. Click **Wireless Settings** in the main menu of the FVG318.

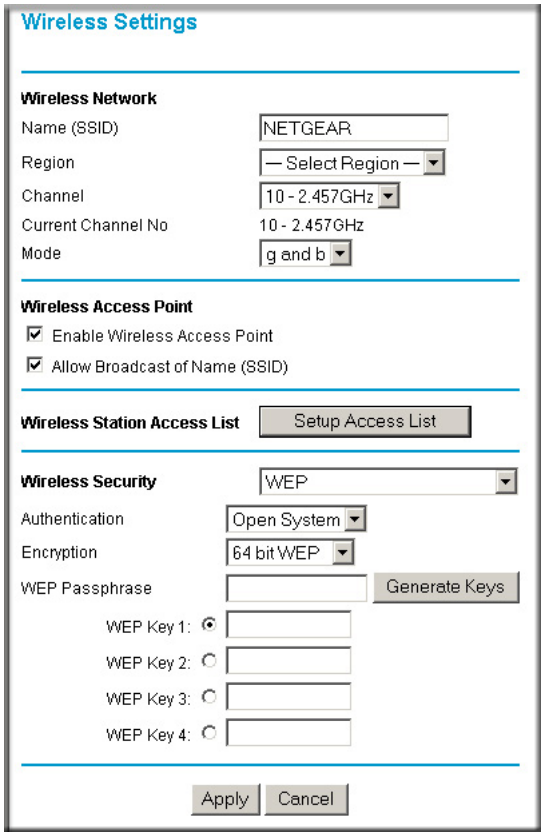


Figure 4-5: Wireless Settings menu (WEP)

3. Select **WEP** on the pulldown menu. The WEP options menu will open.
4. Choose the **Authentication Type** 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 "Overview of WEP Parameters" on page E-5 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.

How to Configure 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, 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 have set up.

2. Click **Wireless Settings** in the main menu of the FVG318.

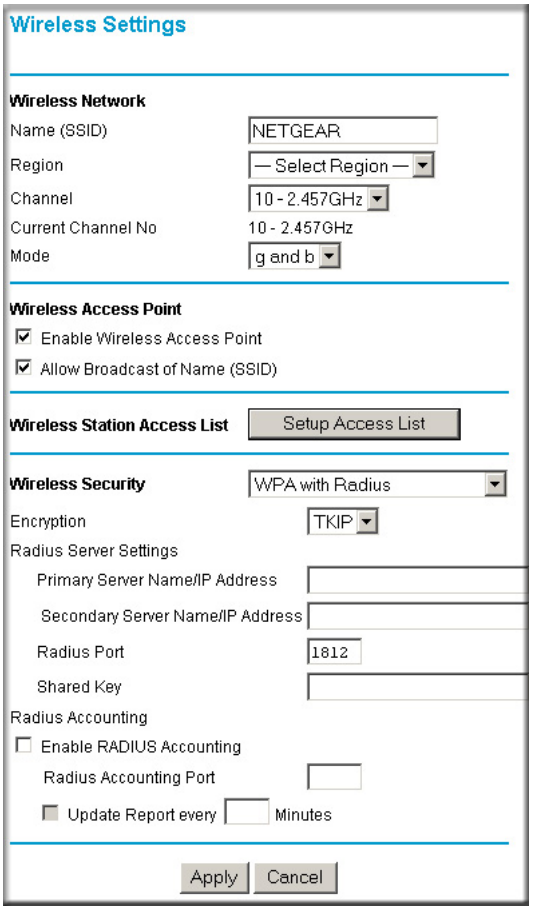


Figure 4-6: Wireless Settings menu (WPA with Radius)

3. Select **WPA with Radius** on the pulldown menu. The WPA with Radius menu will open.

   Encryption: There is no choice for encryption; this is displayed for your information. For WPA with Radius, TKIP is used.

4. Enter the Radius settings.

   - **Primary Server Name/IP Address**: This field is required. Enter the name or IP address of the primary Radius Server on your LAN.
   - **Secondary Radius Server Name/IP Address**: This field is optional. If you have a Secondary Radius Server on your LAN, enter its name or IP address here.

- **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.
- **Radius Accounting**: Enable Radius Accounting

  Enable this if you want to use the Radius Accounting system. If enabled, the following fields must be correct:

- **Radius Accounting Port**: Enter the port number used for Accounting data on the Radius Server.
- **Update Report**: Enable this if you wish to have this AP send Accounting update messages to the Radius accounting server periodically.

  If enabled, enter the desired Update Report interval in the field provided.

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

How to Configure 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, 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 have set up.

2. Click **Wireless Settings** in the main menu of the FVG318.

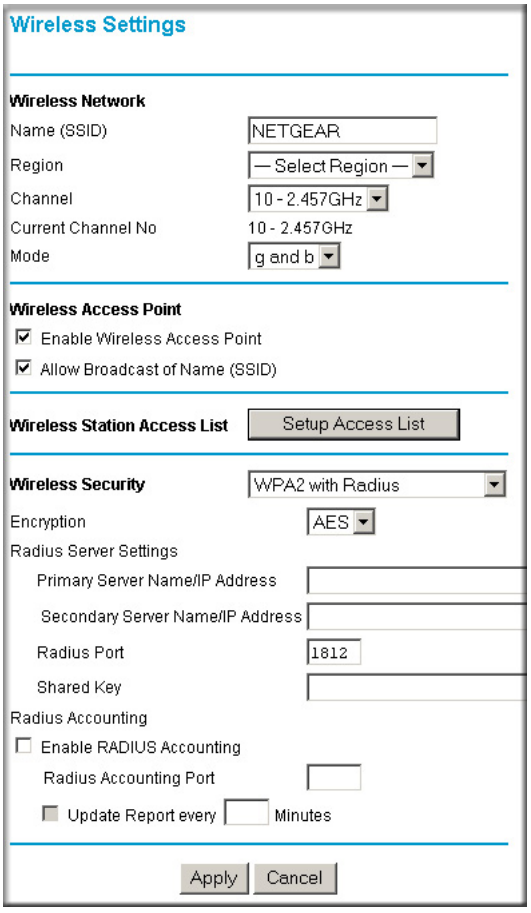


Figure 4-7: Wireless Settings menu (WPA2 with Radius)

3. Select **WPA2 with Radius** on the pulldown menu. The WPA2 with Radius menu will open.

   Encryption: There is no choice for encryption; this is displayed for your information. For WPA2 with Radius, AES is used.

4. Enter the Radius settings.

   - **Primary Server Name/IP Address**: This field is required. Enter the name or IP address of the primary Radius Server on your LAN.

- **Secondary Radius Server Name/IP Address**: This field is optional. If you have a Secondary Radius Server on your LAN, enter its name or IP address here.
- **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.
- **Radius Accounting**: Enable Radius Accounting

  Enable this if you want to use the Radius Accounting system. If enabled, the following fields must be correct:

- **Radius Accounting Port**: Enter the port number used for Accounting data on the Radius Server.
- **Update Report**: Enable this if you wish to have this AP send Accounting update messages to the Radius accounting server periodically.

  If enabled, enter the desired Update Report interval in the field provided.

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

How to Configure 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, 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 have set up.

2. Click **Wireless Settings** in the main menu of the FVG318.

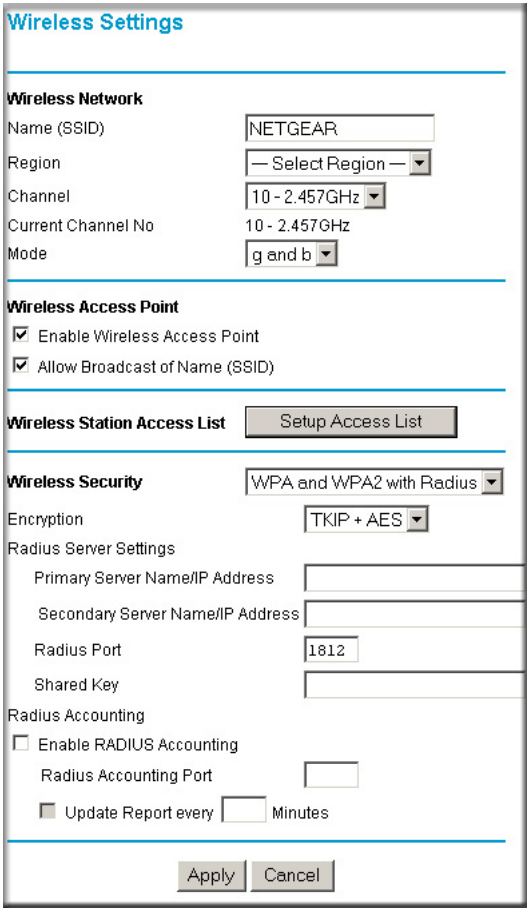


Figure 4-8: Wireless Settings menu (WPA and WPA2 with Radius)

3. Select **WPA and WPA2 with Radius** on the pulldown menu. The WPA and WPA2 with Radius menu will open.

   Encryption: There is no choice for encryption; this is displayed for your information. For WPA and WPA2 with Radius, WPA clients must use TKIP, and WPA2 clients must use AES.

4. Enter the Radius settings.

   - **Primary Server Name/IP Address**: This field is required. Enter the name or IP address of the primary Radius Server on your LAN.

- **Secondary Radius Server Name/IP Address**: This field is optional. If you have a Secondary Radius Server on your LAN, enter its name or IP address here.
- **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.
- **Radius Accounting**: Enable Radius Accounting

  Enable this if you want to use the Radius Accounting system. If enabled, the following fields must be correct:

- **Radius Accounting Port**: Enter the port number used for Accounting data on the Radius Server.
- **Update Report**: Enable this if you wish to have this AP send Accounting update messages to the Radius accounting server periodically.

  If enabled, enter the desired Update Report interval in the field provided.

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

How to Configure 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, 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 have set up.

2. Click **Wireless Settings** in the main menu of the FVG318.

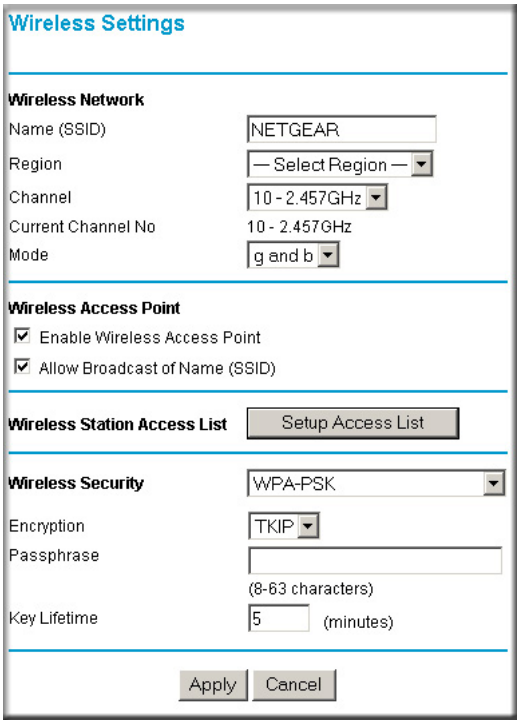


Figure 4-9: Wireless Settings menu (WPA-PSK)

3. Select **WPA-PSK** on the pulldown menu. The WPA-PSK menu will open.
4. Select the desired Encryption method. For WPA-PSK, you can choose TKIP or AES.
5. 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.
6. Enter the Key Lifetime. 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.
7. Click **Apply** to save your settings.

How to Configure 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, 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 have set up.
2. Click **Wireless Settings** in the main menu of the FVG318.

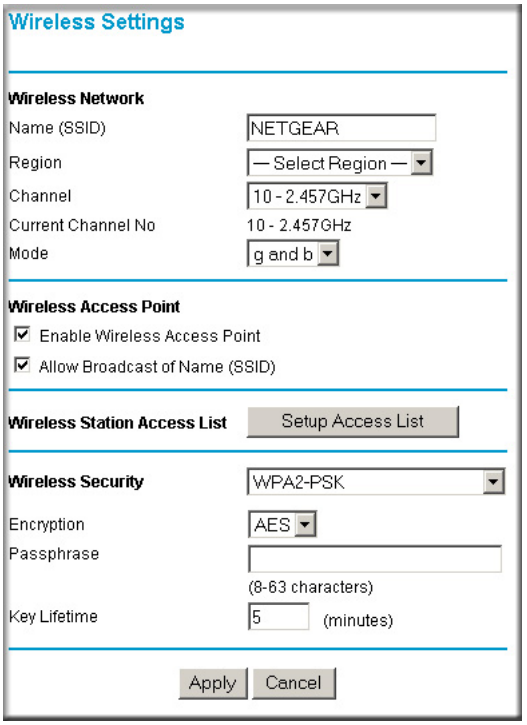


Figure 4-10: Wireless Settings menu (WPA2-PSK)

3. Select **WPA2-PSK** on the pulldown menu. The WPA2-PSK menu will open.

4. Select the desired Encryption method. For WPA2-PSK, the only option is AES.
5. 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.
6. Enter the Key Lifetime. 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.
7. Click **Apply** to save your settings.

How to Configure 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, 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 have set up.

2. Click **Wireless Settings** in the main menu of the FVG318.

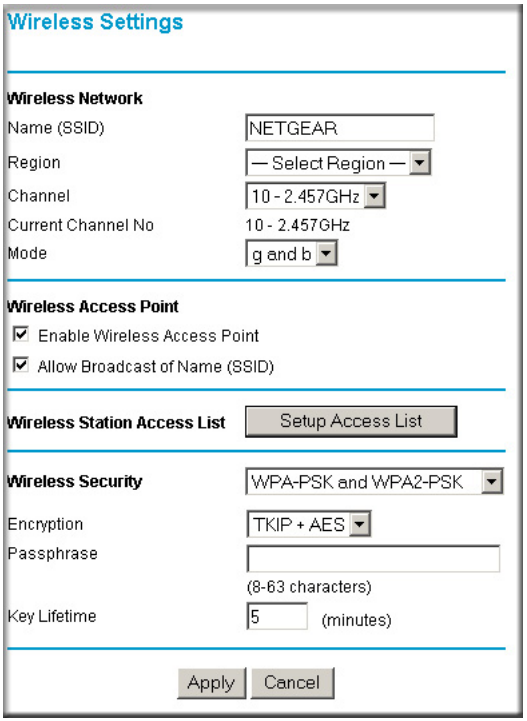


Figure 4-11: Wireless Settings menu (WPA-PSK and WPA2-PSK)

3. Select **WPA-PSK and WPA2-PSK** on the pulldown menu. The WPA-PSK and WPA2-PSK menu will open.
4. Select the desired Encryption method. For WPA-PSK and WPA2-PSK, the only option is TKIP + AES. WPA clients must use TKIP, and WPA2 clients must use AES.
5. 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.
6. Enter the Key Lifetime. 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.
7. Click **Apply** to save your settings.

Chapter 5
Firewall Protection and Content Filtering

This chapter describes how to use the content filtering features of the FVG318 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 FVG318 ProSafe 802.11g Wireless VPN Firewall 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 subheadings under the **Security** heading in the main menu of the browser interface. The subheadings are described below:

Block Sites

The FVG318 allows you to restrict access based on Web addresses and Web address keywords. Up to 255 entries are supported in the Keyword list. The Block Sites menu is shown in Figure 5-1:

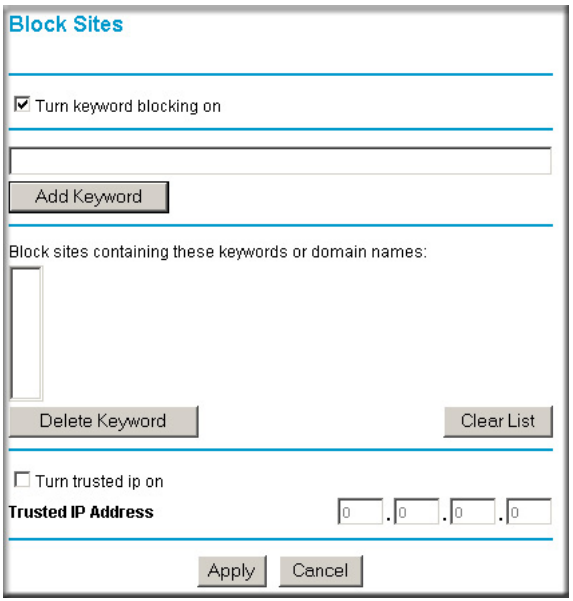


Figure 5-1: Block Sites menu

To enable keyword blocking, check **Turn keyword blocking on**, then click **Apply**.

To add a keyword or domain, type it in the Keyword box, click **Add Keyword**, then click **Apply**.

To delete a keyword or domain, select it from the list, click **Delete Keyword**, then click **Apply**.

Keyword application examples:

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

To specify a Trusted User, enter that PC's IP address in the **Trusted User** box and click **Apply**.

You may specify one Trusted User, which is a PC that will be exempt from blocking and logging. Since the Trusted User will be identified by an IP address, you should configure that PC with a fixed or reserved IP address.

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 5-2:

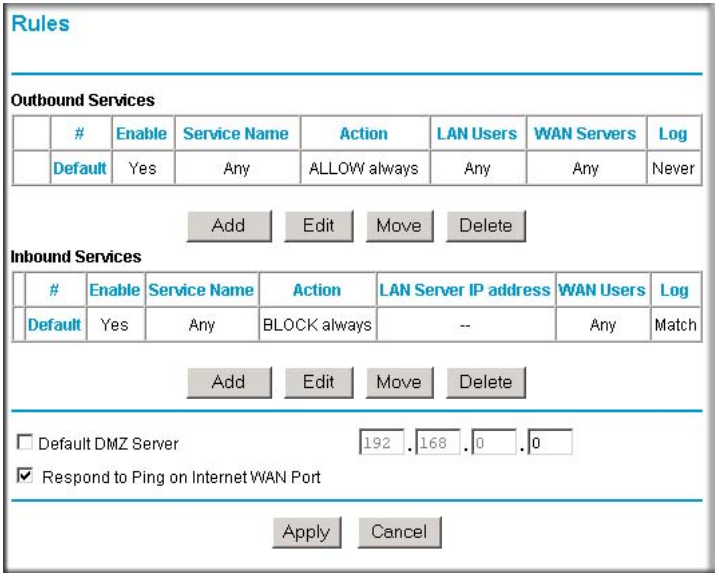


Figure 5-2: Rules menu

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 a new rule, click the **Add** button.

To edit an existing rule, select its button on the left side of the table and click **Edit**.

To delete an existing rule, select its button on the left side of the table and click **Delete**.

To move an existing rule to a different position in the table, select its button on the left side of the table and click **Move**. At the script prompt, enter the number of the desired new position and click **OK**.

An example of the menu for defining or editing a rule is shown in Figure 5-3. 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 FVG318 Wireless 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 5-3:

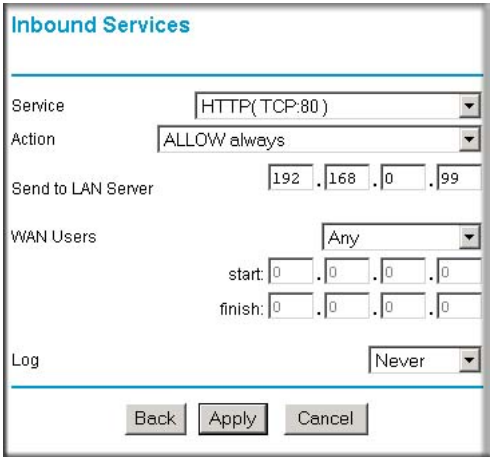


Figure 5-3: Rule example: a local public Web server

Inbound Rule Example: Allowing a Videoconference from Restricted Addresses

If you want to allow incoming videoconferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office, you can create an inbound rule. In the example shown in Figure 5-4, 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.

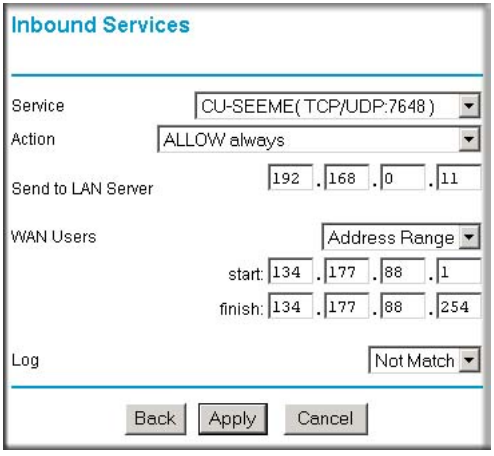


Figure 5-4: Rule example: a videoconference from restricted addresses

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 Dyamic 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 this 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. You can also have the firewall log any attempt to use Instant Messenger during that blocked period.

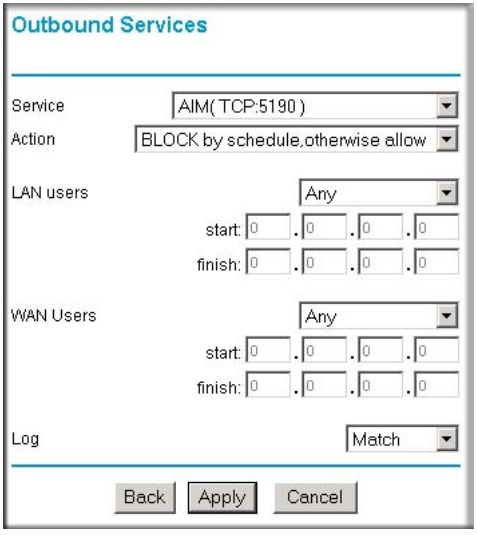


Figure 5-5: Rule example: blocking Instant Messenger

Order of Precedence for Rules

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

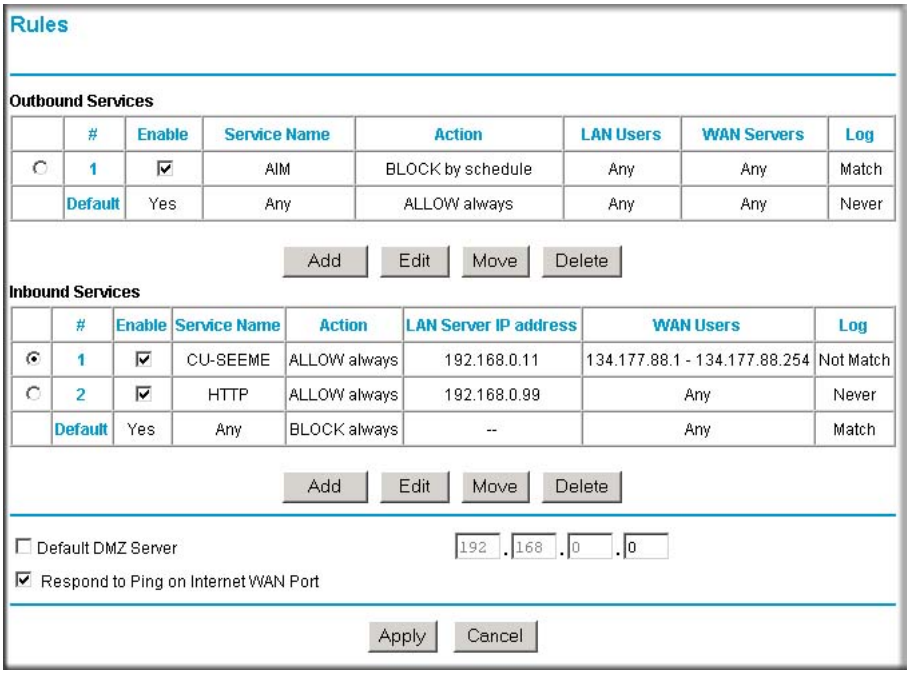


Figure 5-6: Rules table with examples

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 Move button allows 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 videoconferencing 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.

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.

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

1. Click **Default DMZ Server**.
2. Type the IP address for that server.
3. Click **Apply**.

Note: In this application, the use of the term "DMZ" has become common, although it is a misnomer. In traditional firewalls, a DMZ is actually a separate physical network port. A true DMZ port is for connecting servers that require greater access from the outside, and will therefore be provided with a different level of security by the firewall. A better term for our application is Exposed Host.

Respond to Ping on Internet WAN Port

If you want the firewall to respond to a ping from the Internet, click the **Respond to Ping on Internet WAN Port** check box. This should only be used as a diagnostic tool, since it allows your firewall to be discovered. Don't check this box unless you have a specific reason to do so.

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, as shown in Figure 5-7:

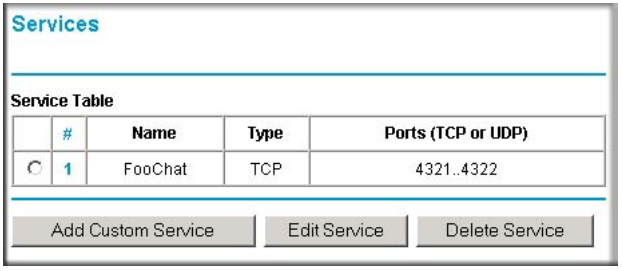


Figure 5-7: Services menu

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 newsgroups.

To add a service:

1. When you have the port number information, go the Services menu and click on the **Add Custom Service** button. The **Add Services** menu appears as shown in Figure 5-8:

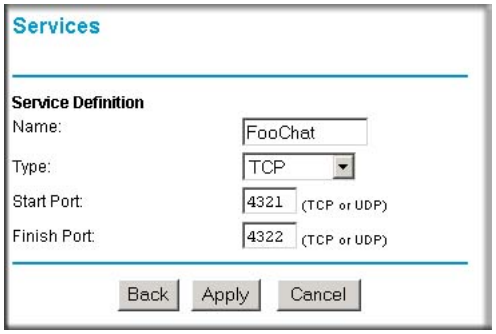


Figure 5-8: Add Custom Service menu

2. Enter a descriptive name for the service so that you will remember what it is.
3. Select whether the service uses TCP or UDP as its transport protocol.
   If you can't determine which is used, select both.
4. Enter the lowest port number used by the service.
5. Enter the highest port number used by the service.
   If the service only uses a single port number, enter the same number in both fields.
6. Click **Apply**.

The new service now appears in the Services menu, and in the Service name selection box in the Rules menu.

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 page shown below:

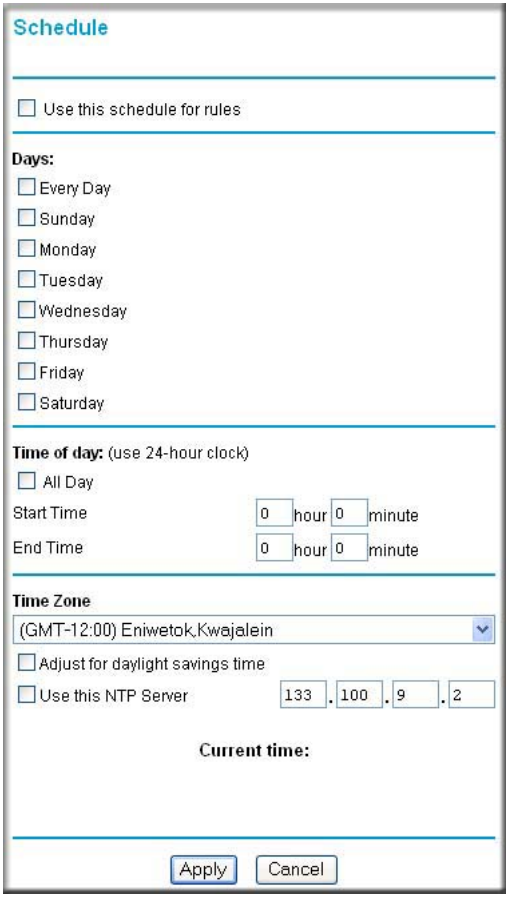


Figure 5-9: Schedule page

To block keywords or Internet domains based on a schedule, select Every Day or select one or more days. If you want to limit access completely for the selected days, select All Day. Otherwise, If you want to limit access during certain times for the selected days, type a Start Blocking time and an End Blocking time.

Note: Enter the values as 24-hour time. For example, to specify 10:30 am, enter 10 hours and 30 minutes; for 10:30 pm, enter 22 hours and 30 minutes.

Be sure to click **Apply** when you have finished configuring this page.

Time Zone

The FVG318 Wireless 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:

- Time Zone. Select your local time zone. This setting will be used for the blocking schedule and for time-stamping log entries.
- Daylight Savings Time. Check this box for 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 unselect it at the end. Enabling Daylight Savings Time will add one hour to the standard time.

Be sure to click **Apply** when you have finished configuring this menu.

Getting E-Mail Notifications of Event Logs and Alerts

In order to receive logs and alerts by e-mail, you must provide your e-mail information in the Send alerts and logs by e-mail area:

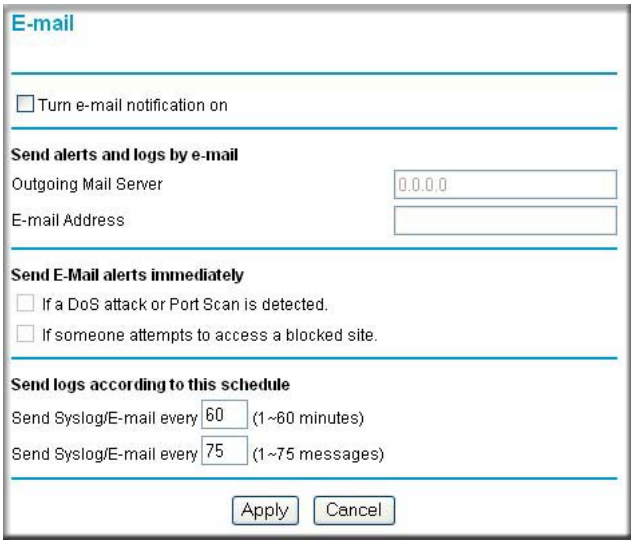


Figure 5-10: E-mail menu

- **Turn e-mail notification on.** Check this box if you wish to receive e-mail logs and alerts from the firewall.
- **Send alerts and logs by e-mail.** If your enable e-mail notification, these boxes cannot be blank. Enter the name or IP 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 e-mail address to which logs and alerts are sent. This e-mail address will also be used as the From address. If you leave this box blank, log and alert messages will not be sent via e-mail.
- **Send E-mail alerts immediately.** You can specify that logs are immediately sent to the specified e-mail address when any of the following events occur:
  - If a Denial of Service attack is detected.
  - If a Port Scan is detected.

  - If a user on your LAN attempts to access a Web site that you blocked using the Block Sites menu.

- **Send logs according to this schedule.** You can specify that logs are sent to you according to a schedule. Select whether you would like to receive the logs None, Hourly, Daily, Weekly, or When Full. Depending on your selection, you may also need to 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.

  If the Weekly, Daily or Hourly option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, the log is cleared from the firewall's memory. If the firewall cannot e-mail the log file, the log buffer may fill up. In this case, the firewall overwrites the log and discards its contents.

Be sure to click **Apply** when you have finished configuring this menu.

Viewing Logs of Web Access or Attempted Web Access

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'll receive these logs in an e-mail message. If you don't have e-mail notification enabled, you can view the logs here. An example is shown in Figure 5-11:

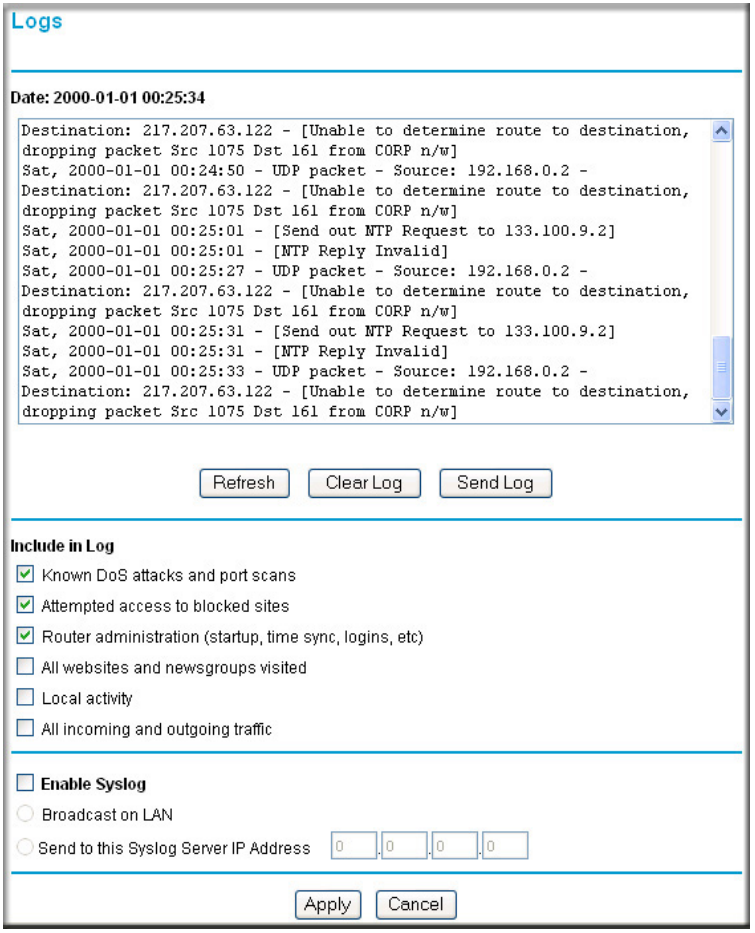


Figure 5-11: Logs menu

Log entries are described in Table 5-1

Table 5-1. 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 5-2

Table 5-2. Log action buttons

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

Syslog

You can configure the firewall to send system logs to an external PC that is running a syslog logging program. Enter the IP address of the logging PC and click the **Enable Syslog** check box.

Logging programs are available for Windows, Macintosh, and Linux computers.

Chapter 6
Basic Virtual Private Networking

This chapter describes how to use the virtual private networking (VPN) features of the FVG318 Wireless 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 6-2 provides an overview of the two most common VPN configurations: client-to-gateway and gateway-to-gateway.
- "Planning a VPN" on page 6-3 provides the VPN Committee (VPNC) recommended default parameters set by the VPN Wizard.
- "VPN Tunnel Configuration" on page 6-5 summarizes the two ways to configure a VPN tunnel: VPN Wizard (recommended for most situations) and Advanced (see Chapter 7, "Advanced Virtual Private Networking).
- "How to Set Up a Client-to-Gateway VPN Configuration" on page 6-5 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.
- "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 6-20 provides the steps needed to configure a VPN tunnel between two network gateways using the VPN Wizard.
- "VPN Tunnel Control" on page 6-26 provides the step-by-step procedures for activating, verifying, deactivating, and deleting a VPN tunnel once the VPN tunnel has been configured.
- Chapter 7, "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 C, "Virtual Private Networking" 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 B, "VPN Configuration of NETGEAR FVS318v3" 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 FVG318 Wireless 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 6-1).

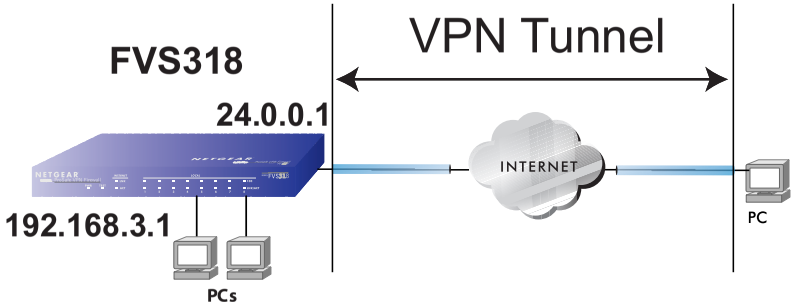


Figure 6-1: Client-to-gateway VPN tunnel

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 FVG318 Wireless VPN Firewall on your network is the other tunnel endpoint. See "How to Set Up a Client-to-Gateway VPN Configuration" on page 6-5 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 6-2).

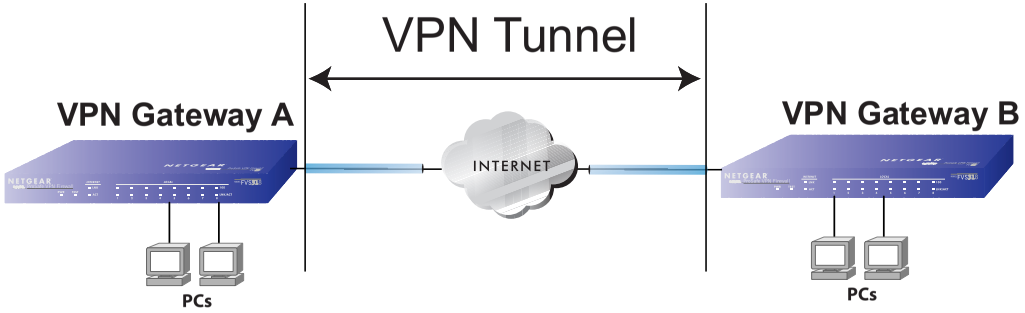


Figure 6-2: Gateway-to-gateway VPN tunnel

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 "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 6-20 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 6-1)
  - Advanced methods (see Chapter 7, "Advanced Virtual Private Networking")

Table 6-1. 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
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 "How to Set Up a Client-to-Gateway VPN Configuration" on page 6-5.
  - See "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 6-20.
- See Chapter 7, "Advanced Virtual Private Networking" when the VPN Wizard and its VPNC defaults (see Table 6-1 on page 6-4) are not appropriate for your special circumstances.

How to Set 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 6-3) involves the following two steps:

- "Step 1: Configuring the Client-to-Gateway VPN Tunnel on the FVG318" on page 6-6 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 6-9 configures the NETGEAR ProSafe VPN Client endpoint.

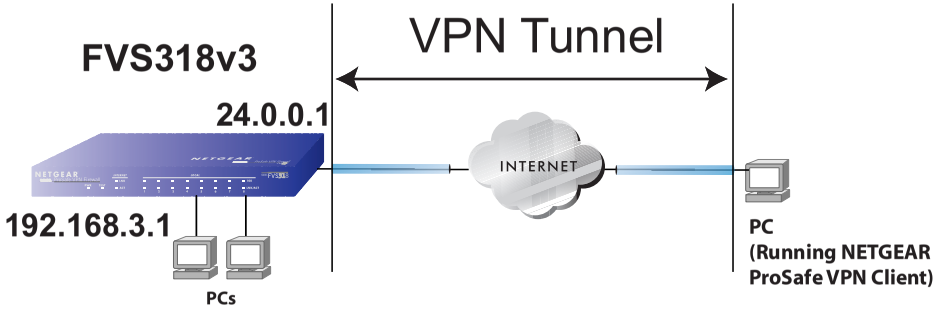


Figure 6-3: Client-to-gateway VPN tunnel

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 6-1 on page 6-4. If you have special requirements not covered by these VPNC-recommended parameters, refer to Chapter 7, "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**. Click the **VPN Wizard** link in the main menu to display this screen. Click **Next** to proceed.

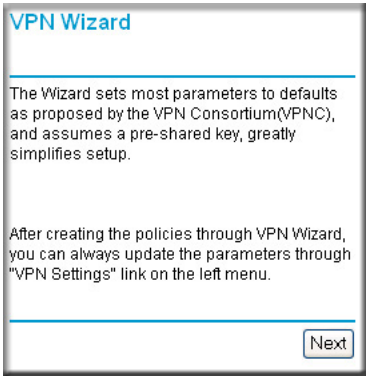


Figure 6-4: VPN Wizard start screen

2. Fill in the Connection Name and the pre-shared key, select the type of target end point, and click **Next** to proceed.

   Note: The Connection Name is arbitrary and not relevant to how the configuration functions.

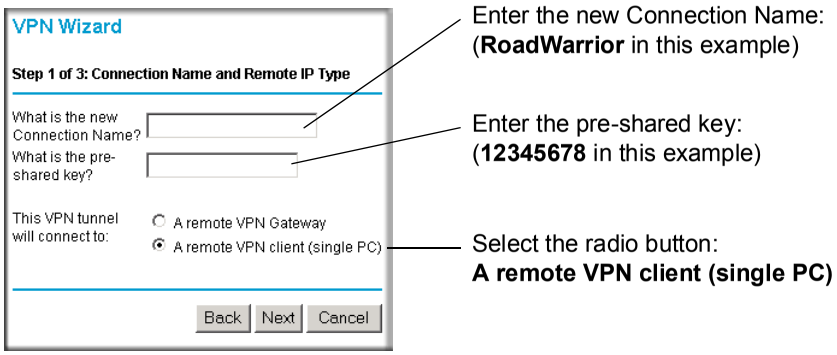


Figure 6-5: Connection Name and Remote IP Type

The Summary screen below displays.

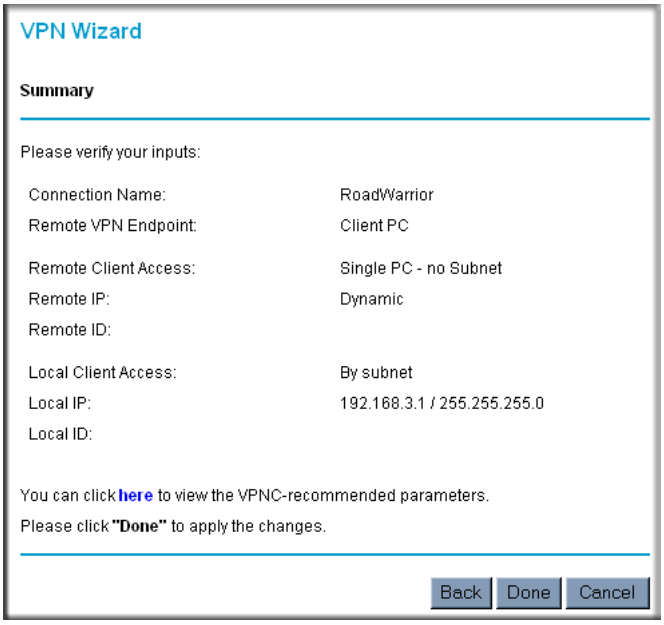


Figure 6-6: VPN Wizard Summary

To view the VPNC recommended authentication and encryption settings used by the VPN Wizard, click the **here** link (see Figure 6-6). Click **Back** to return to the **Summary** screen.

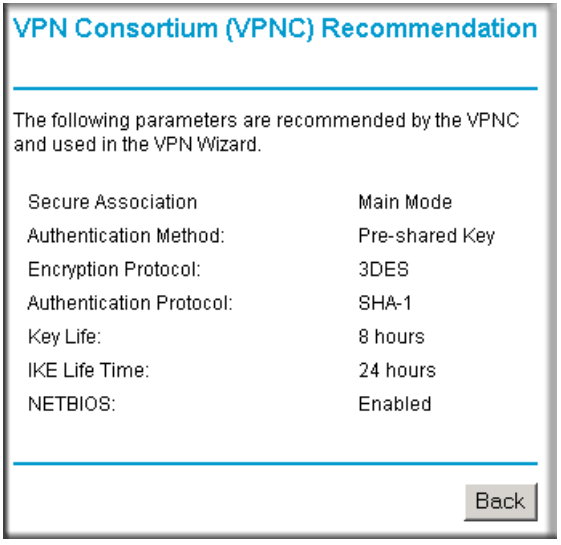


Figure 6-7: VPNC Recommended Settings

3. Click **Done** on the Summary screen (see Figure 6-6) to complete the configuration procedure. The VPN Policies menu below displays showing that the new tunnel is enabled.

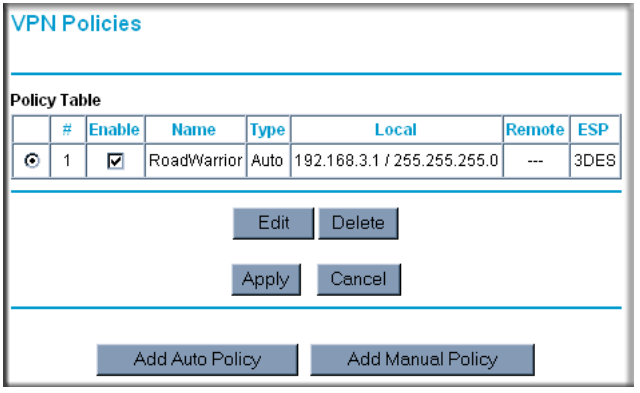


Figure 6-8: VPN Policies

To view or modify the tunnel settings, select the radio button next to the tunnel entry and click **Edit**.

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 () 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 6-18.

   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 6-5) 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.

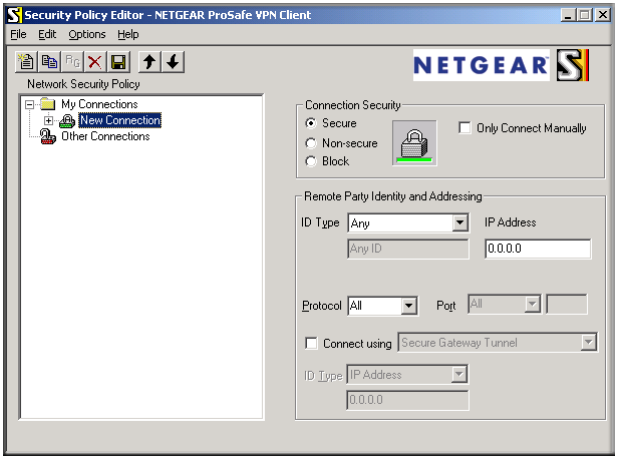


Figure 6-9: Security Policy Editor new connection

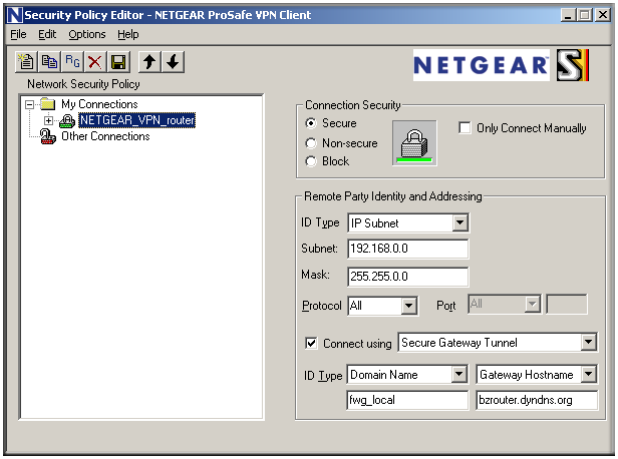


Figure 6-10: Security Policy Editor connection settings

c. Select Secure in the Connection Security check box.

d. Select IP Subnet in the ID Type menu.

   In this example, type **192.168.3.1** in the Subnet field as the network address of the FVG318.

e. Enter **255.255.255.0** in the Mask field as the LAN Subnet Mask of the FVG318.

f. Select All in the Protocol menu to allow all traffic through the VPN tunnel.

g. Select the Connect using Secure Gateway Tunnel check box.

h. Select IP Address in the ID Type menu below the check box.

i. Enter the public WAN IP Address of the FVG318 in the field directly below the ID Type menu. In this example, **22.23.24.25** would be used.

   The resulting Connection Settings are shown in Figure 6-10.

3. 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.

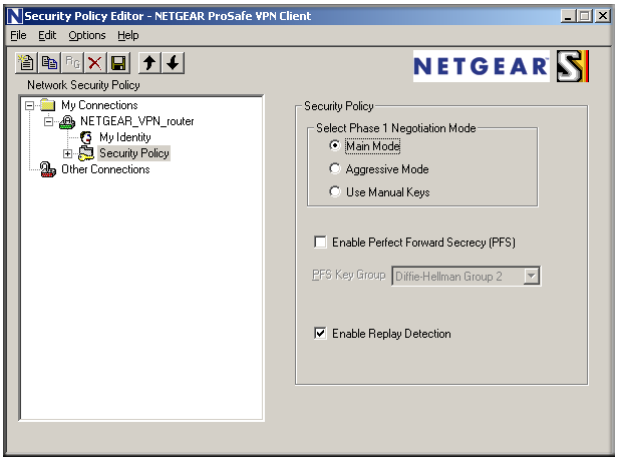


Figure 6-11: Security Policy Editor Security Policy

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

4. Configure the VPN Client Identity.

   In this step, you will 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**.

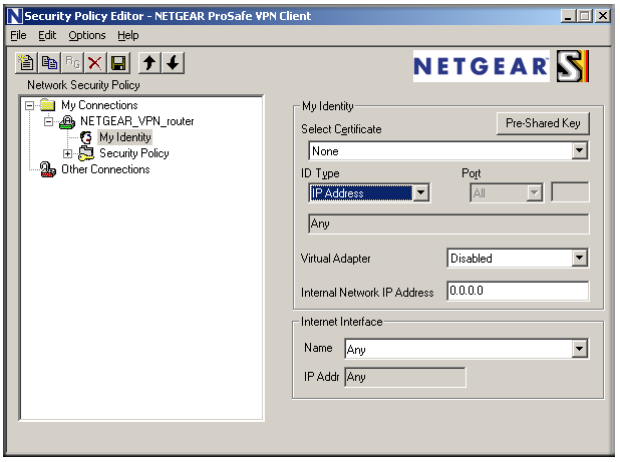


Figure 6-12: Security Policy Editor My Identity

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.

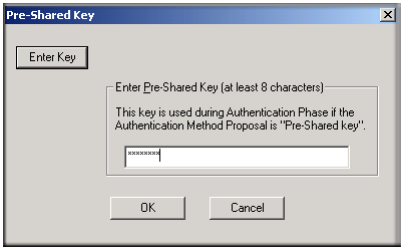


Figure 6-13: Security Policy Editor Pre-Shared Key

5. Configure the VPN Client Authentication Proposal.

   In this step, you will 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.

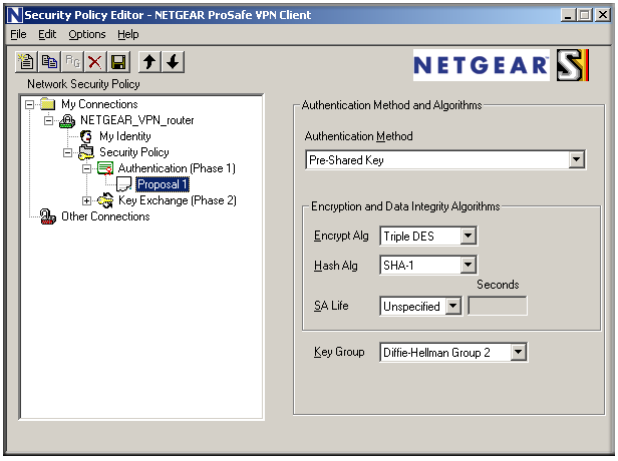


Figure 6-14: Security Policy Editor Authentication

   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.

6. Configure the VPN Client Key Exchange Proposal.

   In this step, you will 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.

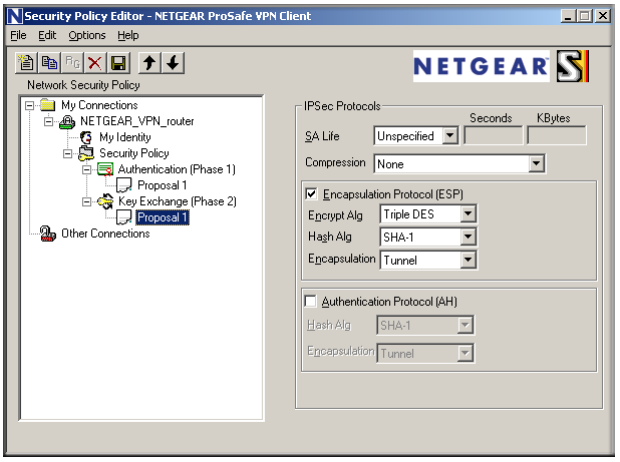


Figure 6-15: Security Policy Editor Key Exchange

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.

7. Save the VPN Client Settings.

   From the File menu at the top of the Security Policy Editor window, select 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.

8. Check the VPN Connection.

   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 taskbar, click the **Start** button, and then click **Run**.

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

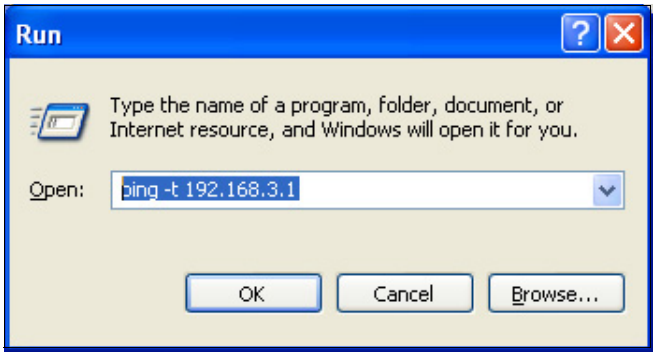


Figure 6-16: Running a Ping test to the LAN from the PC

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."

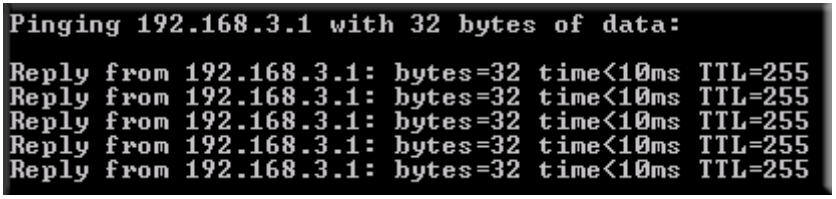


Figure 6-17: Ping test results

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 Wireless VPN Firewall (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.

1. To launch this function, click on the **Windows Start** button, then select **Programs**, then **NETGEAR ProSafe VPN Client**, then **Log Viewer**.

The Log Viewer screen for a similar successful connection is shown below:

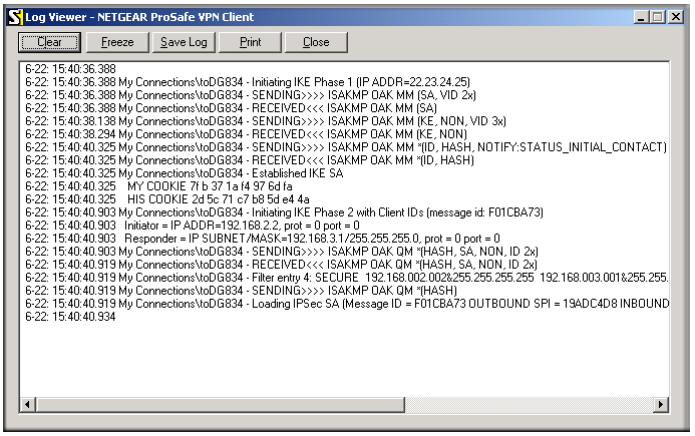


Figure 6-18: Log Viewer screen

	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:

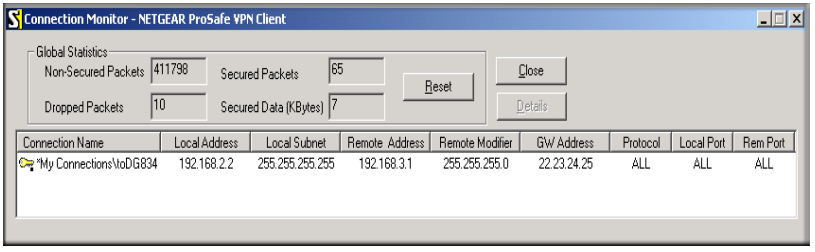


Figure 6-19: Connection Monitor screen

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.

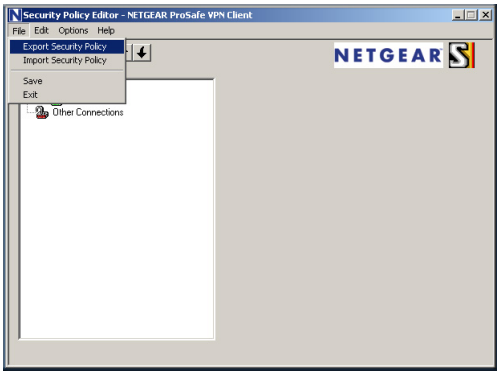
Note: While your PC is connected to a remote LAN through a VPN, you might not have normal Internet access. If this is the case, you will need to close the VPN connection in order to have normal Internet access.

Transferring a Security Policy to Another Client

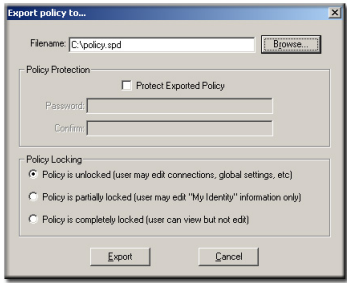
This section explains how to export and import a security policy as an **.spd** file so that an existing NETGEAR ProSafe VPN Client configuration can be copied to other PCs running the NETGEAR ProSafe VPN Client.

Exporting a Security Policy

The following procedure (Figure 6-20) enables you to export a security policy as an **.spd** file.



Step 1: Select **Export Security Policy** from the **File** pulldown.



Step 2: Click **Export** once you decide the name of the file and directory where you want to store the client policy.

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

Figure 6-20: Exporting a security policy

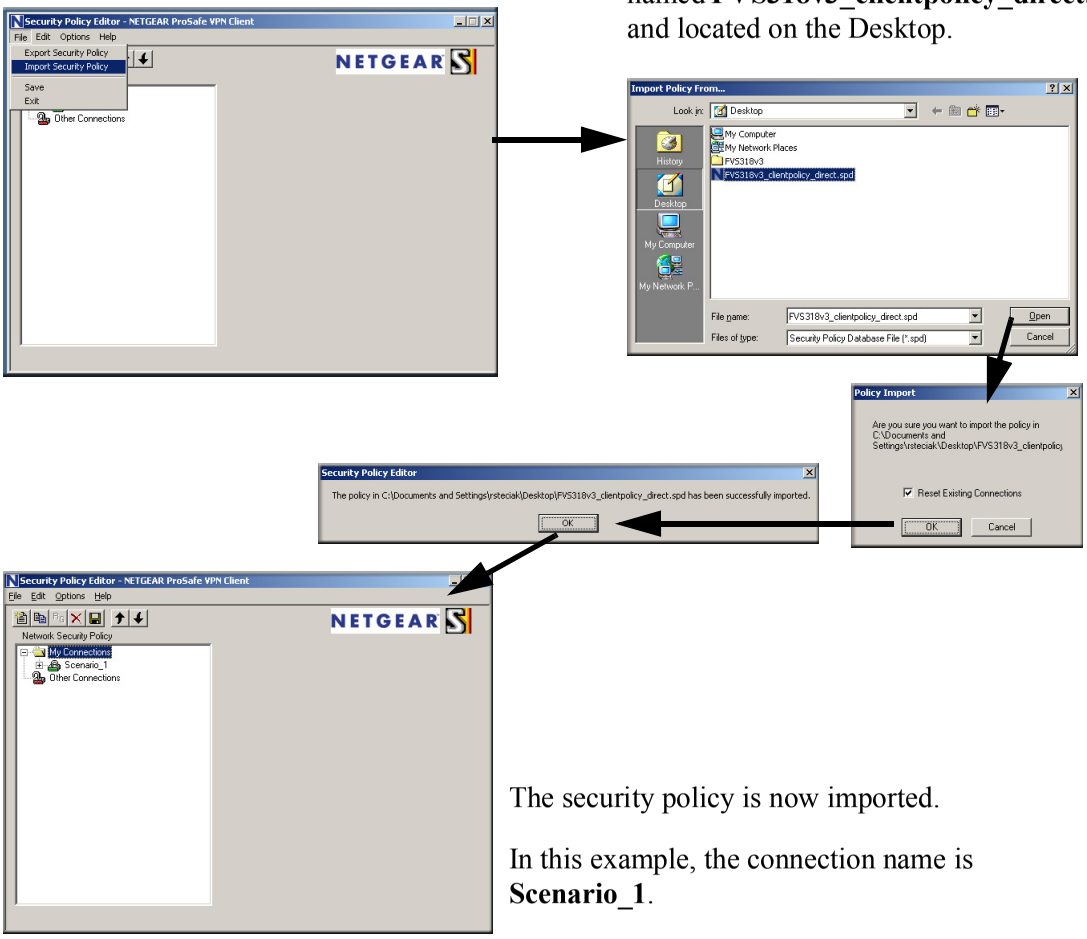
Importing a Security Policy

The following procedure (Figure 6-21) enables you to import an existing security policy.

Step 1: Invoke the NETGEAR ProSafe VPN Client and select **Import Security Policy** from the **File** pulldown.

Step 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.



The security policy is now imported.

In this example, the connection name is **Scenario_1**.

Figure 6-21: Importing a security policy

How to Set 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 6-1 on page 6-4. If you have special requirements not covered by these VPNC-recommended parameters, refer to Chapter 7, "Advanced Virtual Private Networking" to set up the VPN tunnel.

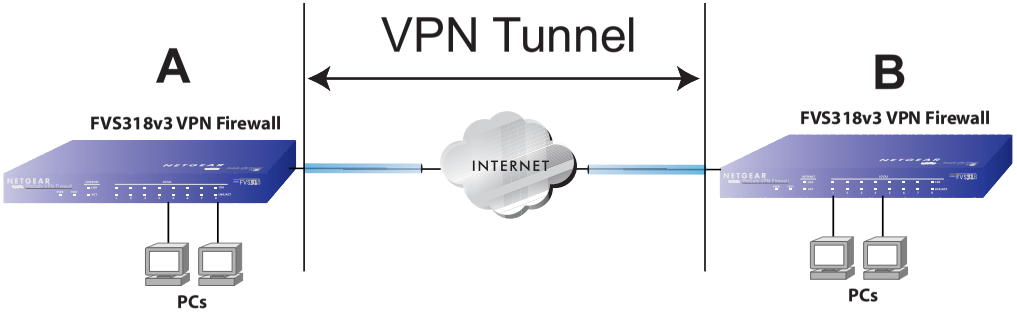


Figure 6-22: Gateway-to-Gateway VPN Tunnel

Follow the procedure below 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.

Procedure to Configure a Gateway-to-Gateway VPN Tunnel

Follow this procedure 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**. Click the **VPN Wizard** link in the main menu to display this screen. Click **Next** to proceed.

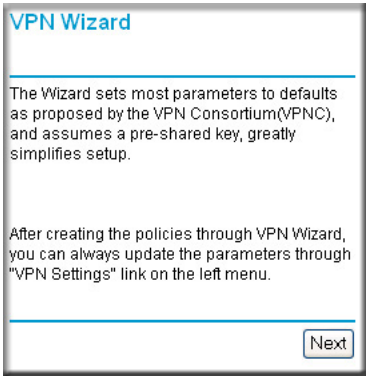


Figure 6-23: VPN Wizard start screen

2. Fill in the Connection Name and the pre-shared key, select the type of target end point, and click **Next** to proceed.

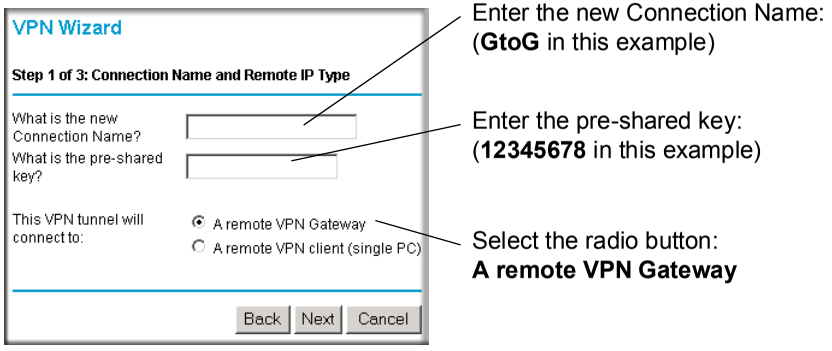


Figure 6-24: Connection Name and Remote IP Type

3. Fill in the IP Address or FQDN for the target VPN endpoint WAN connection and click **Next**.

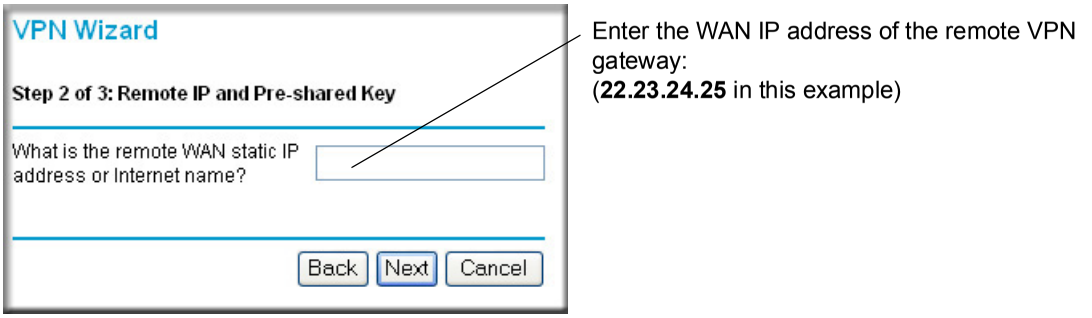


Figure 6-25: Remote IP

4. Identify the IP addresses at the target endpoint that can use this tunnel, and click **Next**.

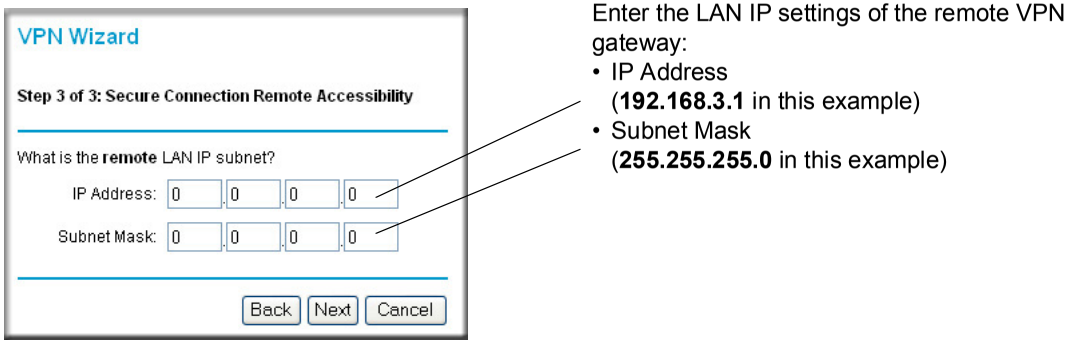


Figure 6-26: Secure Connection Remote Accessibility

The Summary screen below displays.

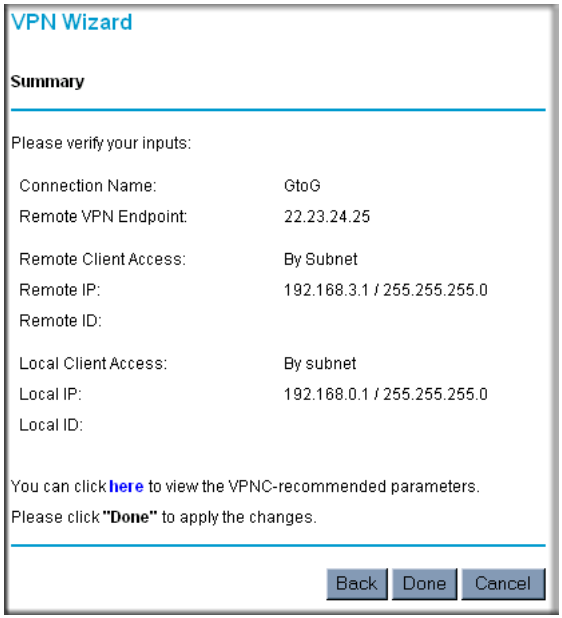


Figure 6-27: VPN Wizard Summary

To view the VPNC recommended authentication and encryption settings used by the VPN Wizard, click the **here** link (see Figure 6-27). Click **Back** to return to the Summary screen.

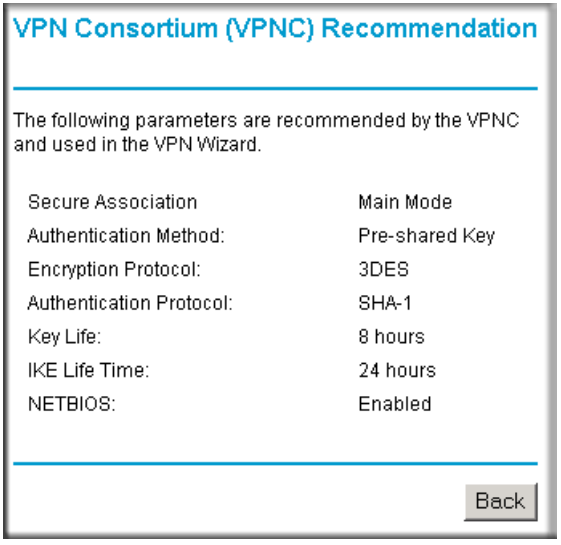


Figure 6-28: VPN Recommended Settings

5. Click **Done** on the Summary screen (see Figure 6-27) to complete the configuration procedure. The VPN Policies menu below displays showing that the new tunnel is enabled.

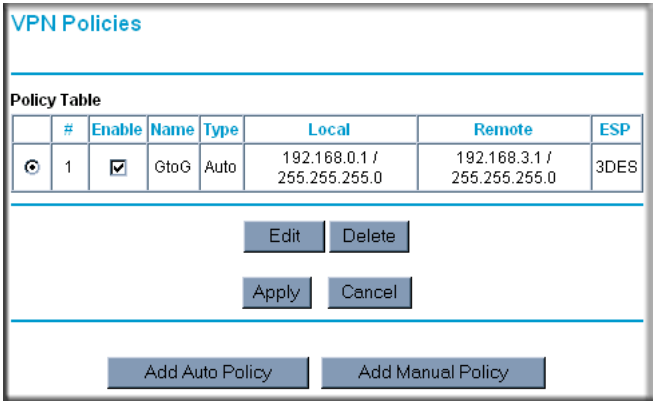


Figure 6-29: VPN Policies

6. Repeat for the FVG318 on LAN B. Pay special attention and use the following network settings as appropriate.
   - WAN IP of the remote VPN gateway (e.g., **14.15.16.17**)
   - LAN IP settings of the remote VPN gateway:
     — IP Address (e.g, **192.168.0.1**)
     — Subnet Mask (e.g., **255.255.255.0**)
     — Preshared Key (e.g., **12345678**)
7. 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 6-26 for information on the other ways.

   a. Open the FVG318 management interface and click on **VPN Status** under VPN to get the VPN Status/Log screen (Figure 6-30).

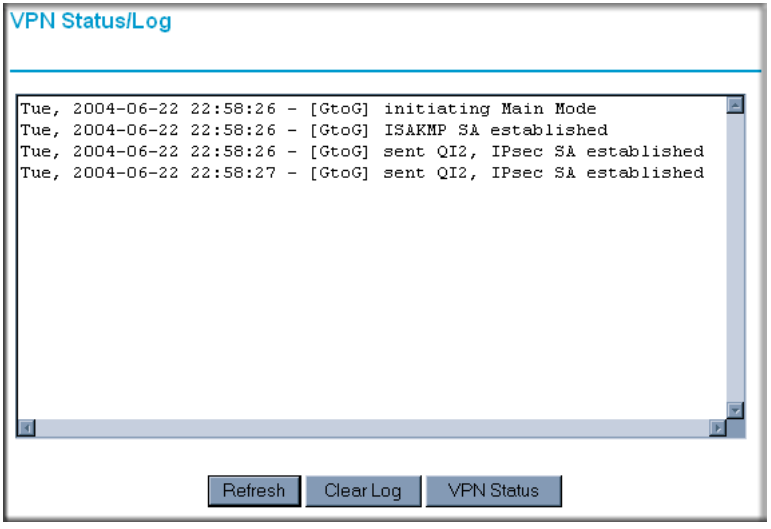


Figure 6-30: VPN Status/Log screen

   b. Click on **VPN Status** (Figure 6-32) to get the Current VPN Tunnels (SAs) screen (Figure 6-31). Click on **Connect** for the VPN tunnel you want to activate.

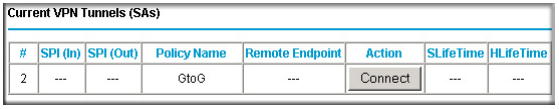


Figure 6-31: Current VPN Tunnels (SAs) Screen

c. Look at the VPN Status/Log screen (Figure 6-30) to verify that the tunnel is connected.

VPN Tunnel Control

Activating a VPN Tunnel

There are three ways to activate a VPN tunnel:

- Start using the VPN tunnel.
- Use the VPN Status page.
- Activate the VPN tunnel by pinging the remote endpoint.

Start Using a VPN Tunnel to Activate It

To use a VPN tunnel, use a Web browser to go to a URL whose IP address or range is covered by the policy for that VPN tunnel.

Using the VPN Status Page to Activate a VPN Tunnel

To use the VPN Status screen to activate a VPN tunnel, perform the following steps:

1. Log in to the Wireless VPN Firewall.
2. Open the FVG318 management interface and click on **VPN Status** under VPN to get the VPN Status/Log screen (Figure 6-32).

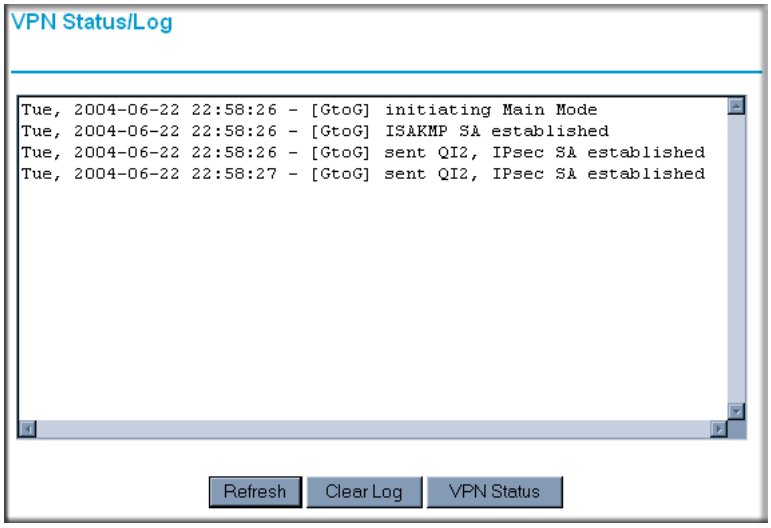


Figure 6-32: VPN Status/Log screen

3. Click **VPN Status** (Figure 6-32) to get the Current VPN Tunnels (SAs) screen (Figure 6-33). Click **Connect** for the VPN tunnel you want to activate.

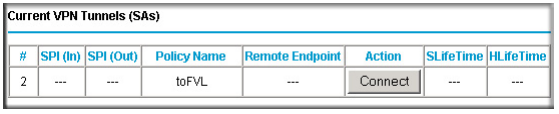


Figure 6-33: Current VPN Tunnels (SAs) screen

Activate the VPN Tunnel by Pinging the Remote Endpoint

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

To activate the VPN tunnel by pinging the remote endpoint (192.168.3.1), do the following steps depending on whether your configuration is client-to-gateway or gateway-to-gateway:

- **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 taskbar, click the **Start** button, and then click **Run**.

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

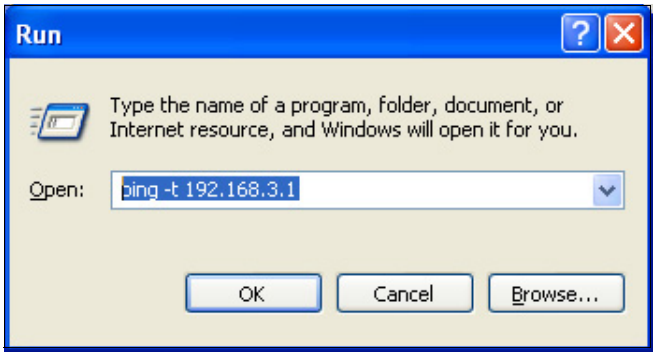


Figure 6-34: Running a Ping test to the LAN from the PC

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.

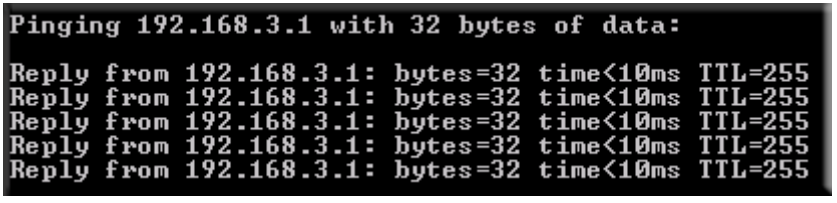


Figure 6-35: Ping test results

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 Wireless VPN Firewall (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**.

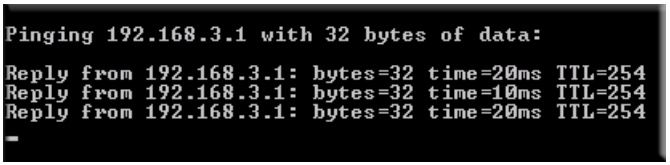


Figure 6-36: Pinging test results

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 Status page to determine the status of a VPN tunnel, perform the following steps:

1. Log in to the Wireless VPN Firewall.
2. Open the FVG318 management interface and click **VPN Status** under VPN to get the VPN Status/Log screen (Figure 6-37).

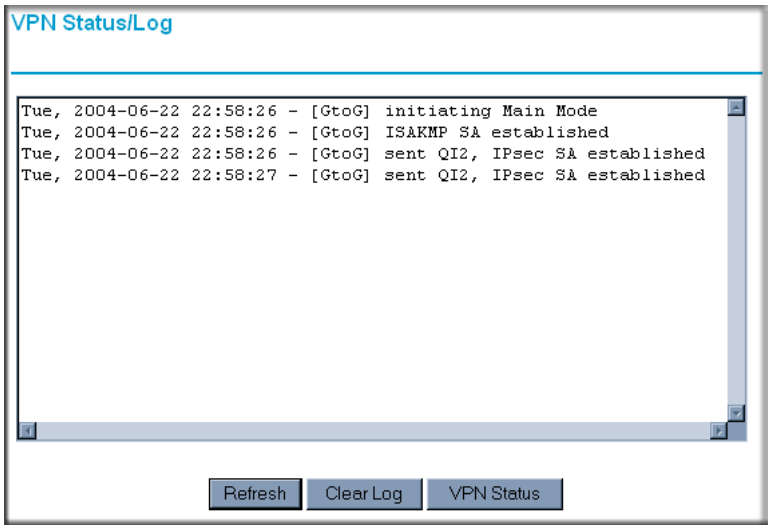


Figure 6-37: VPN Status/Log screen

Log—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.

3. Click **VPN Status** (Figure 6-37) to get the Current VPN Tunnels (SAs) screen (Figure 6-38).

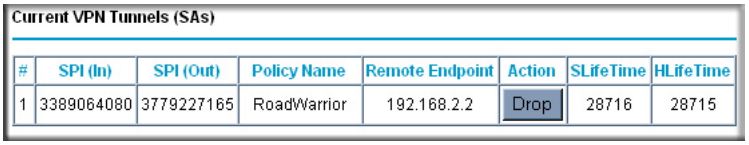


Figure 6-38: Current VPN Tunnels (SAs) screen

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.
- **Action**—the action will be either a **Drop** or a **Connect** button.
- **SLifeTime (Secs)**—the remaining Soft Lifetime for this SA in seconds. When the Soft Lifetime becomes zero, the SA (Security Association) will re-negotiated.
- **HLifeTime (Secs)**—the remaining Hard Lifetime for this SA in seconds. When the Hard Lifetime becomes zero, the SA (Security Association) will be terminated. (It will be re-established if required.)

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 page
- VPN Status page

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

To use the VPN Policies page to deactivate a VPN tunnel, perform the following steps:

1. Log in to the Wireless VPN Firewall.
2. Click on **VPN Policies** under VPN to get the VPN Policies screen below (Figure 6-39).

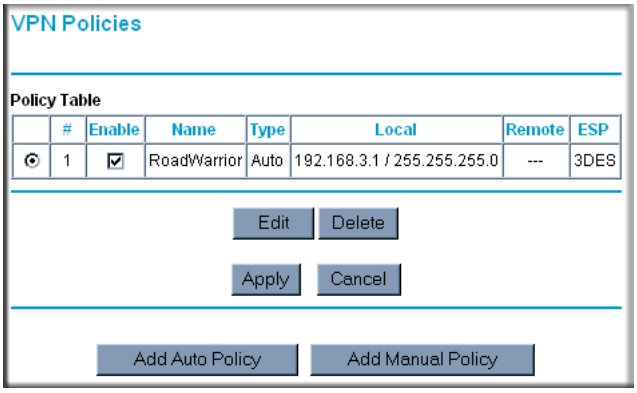


Figure 6-39: VPN Policies

3. Clear the Enable check box for the VPN tunnel you want to deactivate and click **Apply**. (To reactivate the tunnel, check the Enable box and click **Apply**.)

Using the VPN Status Page to Deactivate a VPN Tunnel

To use the VPN Status page to deactivate a VPN tunnel, perform the following steps:

1. Log in to the Wireless VPN Firewall.
2. Click **VPN Status** under VPN to get the VPN Status/Log screen (Figure 6-40).

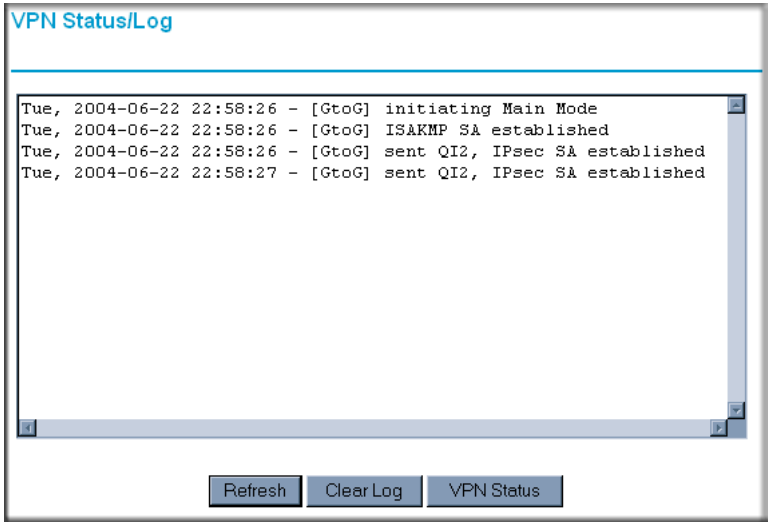


Figure 6-40: VPN Status/Log screen

3. Click **VPN Status** (Figure 6-40) to get the Current VPN Tunnels (SAs) screen (Figure 6-41). Click **Drop** for the VPN tunnel you want to deactivate.

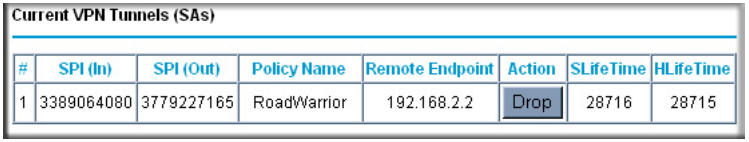


Figure 6-41: Current VPN Tunnels (SAs) screen

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 Page to Deactivate a VPN Tunnel" on page 6-30).

Deleting a VPN Tunnel

To delete a VPN tunnel:

1. Log in to the Wireless VPN Firewall.
2. Click **VPN Policies** under VPN to display the VPN Policies screen (Figure 6-42). Select the radio button for the VPN tunnel to be deleted and click the **Delete** button.

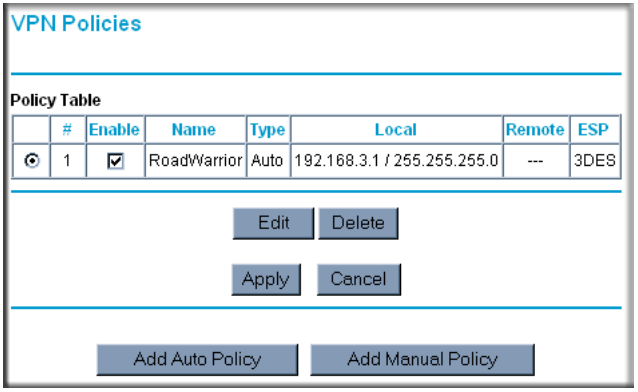


Figure 6-42: VPN Policies

Chapter 7
Advanced Virtual Private Networking

This chapter describes how to use the advanced virtual private networking (VPN) features of the FVG318 Wireless VPN Firewall. See Chapter 6, "Basic Virtual Private Networking" for a description on how to use the basic VPN features.

Overview of FVG318 Policy-Based VPN Configuration

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.

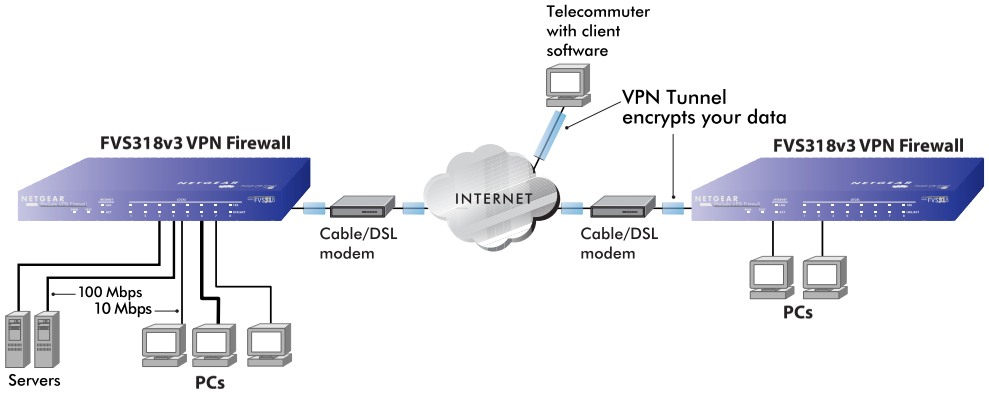


Figure 7-1: Secure access through FVG318 VPN firewalls

Using 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 FVG318 Wireless 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 Policies' Automatic Key and Authentication Management

Click the **IKE Policies** link from the VPN 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 7-2.

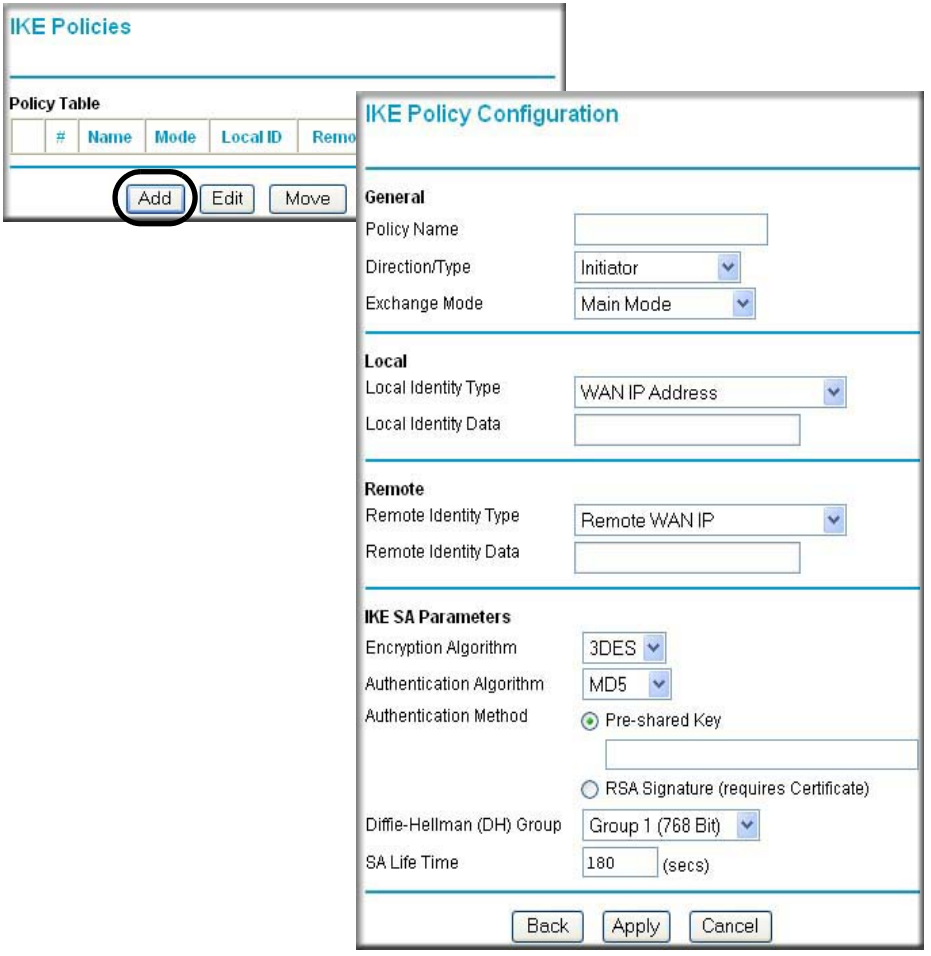


Figure 7-2: IKE - Policy Configuration Menu

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

Table 7-1. IKE Policy Configuration fields

Field	Description
General	These settings identify this policy and determine its major characteristics.
Policy Name	The descriptive name of the IKE 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 IKE policies.
Direction/Type	This setting is used when determining if the IKE policy matches the current traffic. The drop-down menu includes the following: • Initiator — Outgoing connections are allowed, but incoming are blocked. • Responder — Incoming connections are allowed, but outgoing are blocked. • Both Directions — Both outgoing and incoming connections are allowed. • Remote Access — This is to allow only incoming client connections, where the IP address of the remote client is unknown. If Remote Access is selected, the Exchange Mode must be Aggressive, and the Identities below (both Local and Remote) must be Name. On the matching VPN Policy, the IP address of the remote VPN endpoint should be set to 0.0.0.0.
Exchange Mode	Main Mode or Aggressive Mode. This setting must match the setting used on the remote VPN endpoint. • Main Mode is slower but more secure. Also, the Identity below must be established by IP address. • Aggressive Mode is faster but less secure. The Identity below can be by name (host name, domain name, and e-mail address) instead of by IP address.
Local	These parameters apply to the Local FVG318 Wireless VPN Firewall.
Local Identity Type	Use this field to identify the local FVG318. You can choose one of the following four options from the drop-down list: • By its Internet (WAN) port IP address. • By its Fully Qualified Domain Name (FQDN) — your domain name. • By a Fully Qualified User Name — your name, E-mail address, or other ID. • By DER ASN.1 DN — the binary DER encoding of your ASN.1 X.500 Distinguished Name.
Local Identity Data	This field lets you identify the local FVG318 by name.

Table 7-1. IKE Policy Configuration fields

Field	Description
Remote	These parameters apply to the target remote FVG318, VPN gateway, or VPN client.
Remote Identity Type	Use this field to identify the remote FVG318. You can choose one of the following four options from the drop-down list: • By its Internet (WAN) port IP address. • By its Fully Qualified Domain Name (FQDN) — your domain name. • By a Fully Qualified User Name — your name, E-mail address, or other ID. • By DER ASN.1 DN — the binary DER encoding of your ASN.1 X.500 Distinguished Name.
Remote Identity Data	This field lets you identify the target remote FVG318 by name.
IKE SA Parameters	These parameters determine the properties of the IKE Security Association.
Encryption Algorithm	Choose the encryption algorithm for this IKE policy: • DES is the default • 3DES is more secure
Authentication Algorithm	If you enable Authentication Header (AH), this menu lets you to select from these authentication algorithms: • MD5 — the default • SHA-1 — more secure
Authentication Method	You may select Pre-Shared Key or RSA Signature.
Pre-Shared Key	Specify the key according to the requirements of the Authentication Algorithm you selected. • For MD5, the key length should be 16 bytes. • For SHA-1, the key length should be 20 bytes.
RSA Signature	RSA Signature requires a certificate.
Diffie-Hellman (D-H) Group	The DH Group setting determines the bit size used in the key exchange. This must match the value used on the remote VPN gateway or client.
SA Life Time	The amount of time in seconds before the Security Association expires; over an hour (3600) is common.

VPN Policy Configuration for Auto Key Negotiation

An already defined IKE policy is required for VPN - Auto Policy configuration. From the VPN Policies section of the main menu, you can navigate to the VPN - Auto Policy configuration menu.

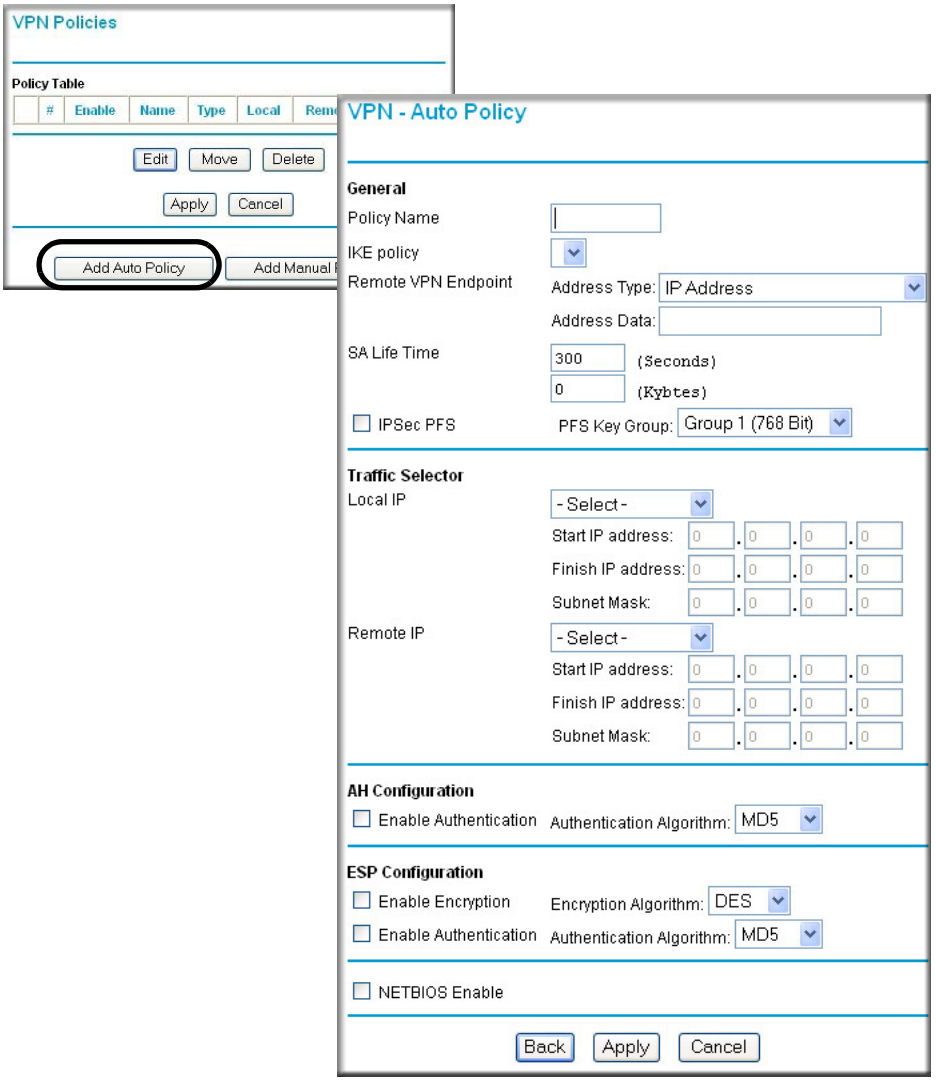


Figure 7-3: VPN - Auto Policy menu

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

Table 7-1. VPN – Auto Policy Configuration Fields

Field	Description
General	These settings identify this policy and determine its major characteristics.
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.
IKE Policy	The existing IKE policies are presented in a drop-down list. **Note:** Create the IKE policy BEFORE creating a VPN - Auto policy.
Remote VPN Endpoint	The address used to locate the remote VPN firewall or client to which you wish to connect. The remote VPN endpoint must have this FVG318's Local IP values entered as its Remote VPN Endpoint. • By its Fully Qualified Domain Name (FQDN) — your domain name. • By its IP Address.
Address Type	The address type used to locate the remote VPN firewall or client to which you wish to connect. • By its Fully Qualified Domain Name (FQDN) — your domain name. • By its IP Address.
Address Data	The address used to locate the remote VPN firewall or client to which you wish to connect. The remote VPN endpoint must have this FVG318's Local Identity Data entered as its Remote VPN Endpoint. • By its Fully Qualified Domain Name (FQDN) — your domain name. • By its IP Address.
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.
IPSec PFS	If enabled, security is enhanced by ensuring that the key is changed at regular intervals. Also, even if one key is broken, subsequent keys are no easier to break. Each key has no relationship to the previous key.
PFS Key Group	If PFS is enabled, this setting determines the DH group bit size used in the key exchange. This must match the value used on the remote gateway.

Table 7-1. VPN – Auto Policy Configuration Fields

Field	Description
Traffic Selector	These settings determine if and when a VPN tunnel will be established. If network traffic meets *all* criteria, then a VPN tunnel will be created.
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
Authenticating Header (AH) Configuration	AH specifies the authentication protocol for the VPN header. These settings must match the remote VPN endpoint.
Enable Authentication	Use this check box to enable or disable AH for this VPN policy.
Authentication Algorithm	If you enable AH, then select the authentication algorithm: • MD5 — the default • SHA1 — more secure
Encapsulated Security Payload (ESP) Configuration	ESP provides security for the payload (data) sent through the VPN tunnel. Generally, you will want to enable both Encryption and Authentication. Two ESP modes are available: • Plain ESP encryption • ESP encryption with authentication These settings must match the remote VPN endpoint.
Enable Encryption	Use this check box to enable or disable ESP Encryption.
Encryption Algorithm	If you enable ESP encryption, then select the encryption algorithm: • DES — the default • 3DES — more secure
Enable Authentication	Use this check box to enable or disable ESP transform for this VPN policy. You can select the ESP mode also with this menu. Two ESP modes are available: • Plain ESP • ESP with authentication

Table 7-1. VPN – Auto Policy Configuration Fields

Field	Description
Authentication Algorithm	If you enable AH, then use this menu to select which authentication algorithm will be employed. The choices are: • MD5 — the default • SHA1 — more secure
NETBIOS Enable	Check this if you wish NETBIOS traffic to be forwarded over the VPN tunnel. The NETBIOS protocol is used by Microsoft Networking for such features as Network Neighborhood.

VPN Policy Configuration for Manual Key Exchange

With Manual Key Management, you will not use an IKE policy. You must manually type in all the required key information. Click the **VPN Policies** link from the VPN section of the main menu to display the menu shown below.

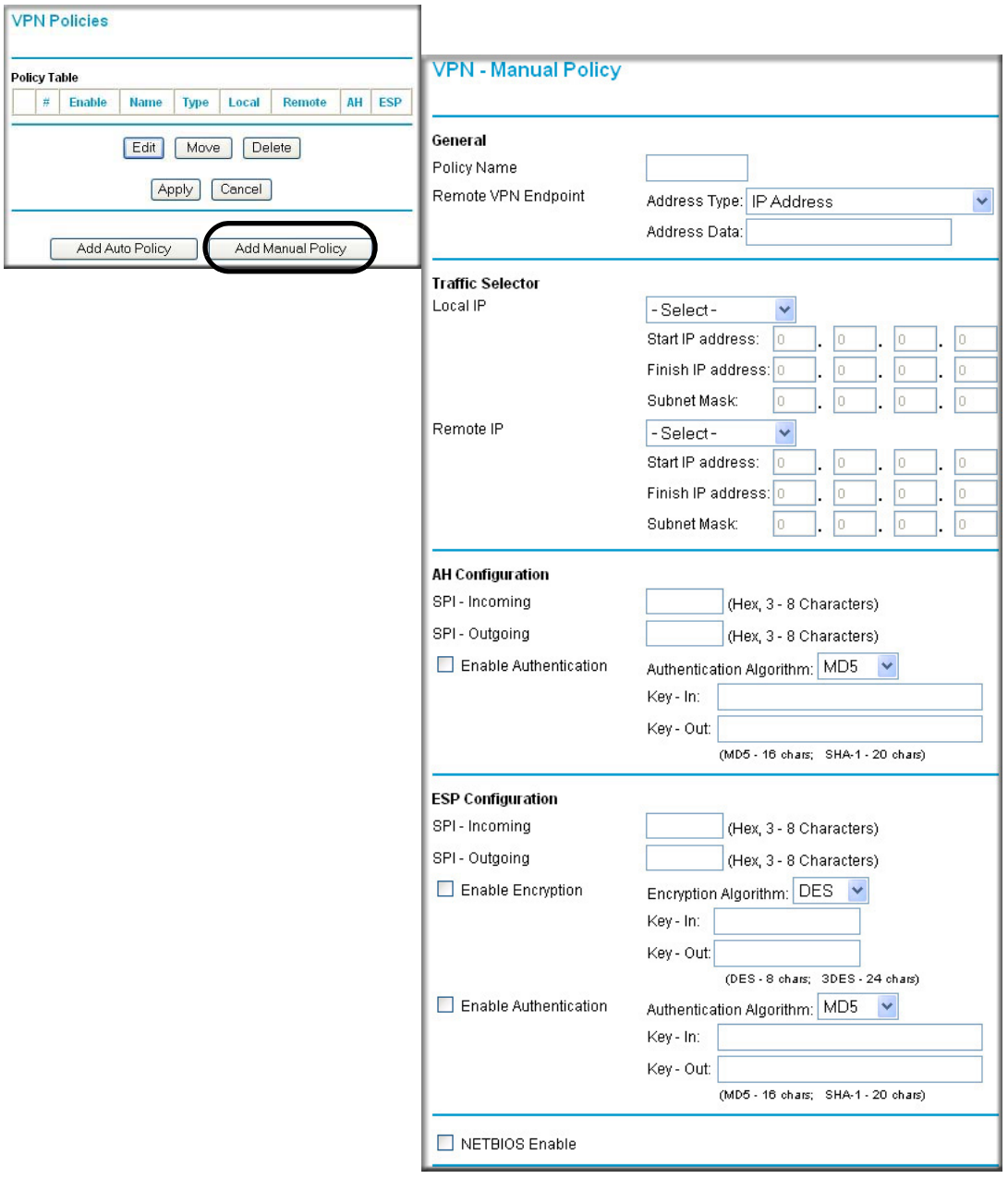


Figure 7-4: VPN - Manual Policy menu

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

Table 7-1. VPN Manual Policy Configuration Fields

Field	Description
General	These settings identify this policy and determine its major characteristics.
Policy Name	The 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 used to help you identify VPN policies.
Remote VPN Endpoint	The WAN Internet IP address of the remote VPN firewall or client to which you wish to connect. The remote VPN endpoint must have this FVG318's WAN Internet IP address entered as its Remote VPN Endpoint.
Traffic Selector	These settings determine if and when a VPN tunnel will be established. If network traffic meets *all* criteria, then a VPN tunnel will be created.
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
Authenticating Header (AH) Configuration	AH specifies the authentication protocol for the VPN header. These settings must match the remote VPN endpoint. **Note:** The Incoming settings here must match the Outgoing settings on the remote VPN endpoint, and the Outgoing settings here must match the Incoming settings on the remote VPN endpoint.
SPI - Incoming	Enter a hexadecimal value (3 - 8 chars). Any value is acceptable, provided the remote VPN endpoint has the same value in its Outgoing SPI field.
SPI - Outgoing	Enter a hexadecimal value (3 - 8 chars). Any value is acceptable, provided the remote VPN endpoint has the same value in its Incoming SPI field.
Enable Authentication	Use this check box to enable or disable AH. Authentication is often not used. In this case, leave the check box unchecked.

Table 7-1. VPN Manual Policy Configuration Fields

Field	Description
Authentication Algorithm	If you enable AH, then select the authentication algorithm: • MD5 — the default • SHA1 — more secure Enter the keys in the fields provided. For MD5, the keys should be 16 characters. For SHA-1, the keys should be 20 characters.
Key - In	Enter the keys. • For MD5, the keys should be 16 characters. • For SHA-1, the keys should be 20 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Authentication Algorithm Key - Out field.
Key - Out	Enter the keys in the fields provided. • For MD5, the keys should be 16 characters. • For SHA-1, the keys should be 20 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Authentication Algorithm Key - In field.
Encapsulated Security Payload (ESP) Configuration	ESP provides security for the payload (data) sent through the VPN tunnel. Generally, you will want to enable both encryption and authentication. when you use ESP. Two ESP modes are available: • Plain ESP encryption • ESP encryption with authentication These settings must match the remote VPN endpoint.
SPI - Incoming	Enter a hexadecimal value (3 - 8 chars). Any value is acceptable, provided the remote VPN endpoint has the same value in its Outgoing SPI field.
SPI - Outgoing	Enter a hexadecimal value (3 - 8 chars). Any value is acceptable, provided the remote VPN endpoint has the same value in its Incoming SPI field.
Enable Encryption	Use this check box to enable or disable ESP Encryption.
Encryption Algorithm	If you enable ESP Encryption, then select the Encryption Algorithm: • DES — the default • 3DES — more secure
Key - In	Enter the key in the fields provided. • For DES, the key should be eight characters. • For 3DES, the key should be 24 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Encryption Algorithm Key - Out field.
Key - Out	Enter the key in the fields provided. • For DES, the key should be eight characters. • For 3DES, the key should be 24 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Encryption Algorithm Key - In field.

Table 7-1. VPN Manual Policy Configuration Fields

Field	Description
Enable Authentication	Use this check box to enable or disable ESP authentication for this VPN policy.
Authentication Algorithm	If you enable authentication, then use this menu to select the algorithm: • MD5 — the default • SHA1 — more secure
Key - In	Enter the key. • For MD5, the key should be 16 characters. • For SHA-1, the key should be 20 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Authentication Algorithm Key - Out field.
Key - Out	Enter the key in the fields provided. • For MD5, the key should be 16 characters. • For SHA-1, the key should be 20 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Authentication Algorithm Key - In field.
NETBIOS Enable	Check this if you wish NETBIOS traffic to be forwarded over the VPN tunnel. The NETBIOS protocol is used by Microsoft Networking for such features as Network Neighborhood.

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.

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.

Walk-Through of 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.

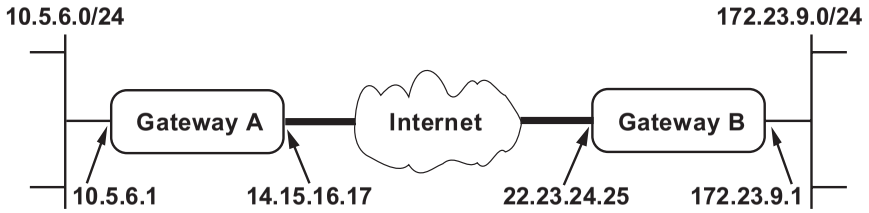


Figure 7-5: VPN Consortium Scenario 1

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 Scenario 1: FVG318 to 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 the Figure 5-2 on page 5-3.

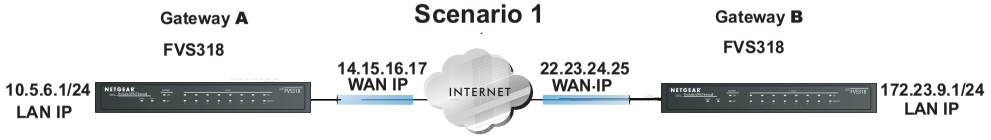


Figure 7-6: LAN to LAN VPN access from an FVG318 to an FVG318

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. From the main menu Setup section, click the **Basic Setup** link to go back to the Basic Settings menu.

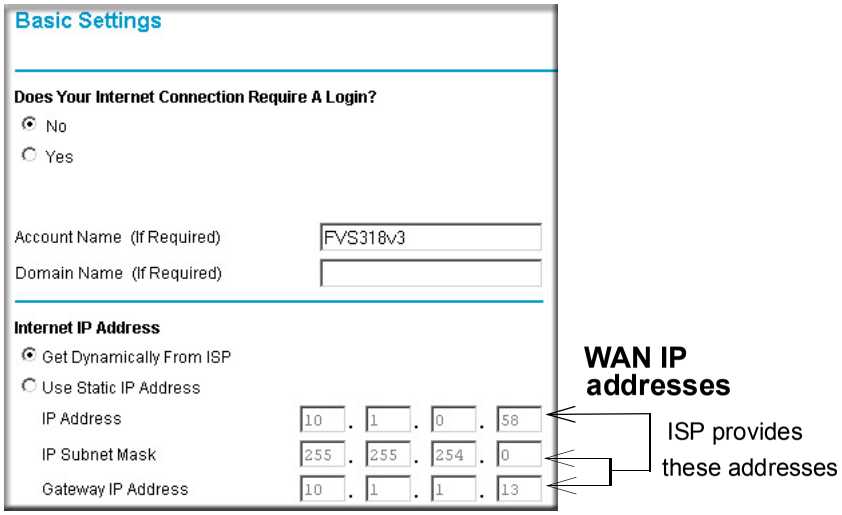


Figure 7-7: FVG318 Internet IP Address menu

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 in the Basic Settings topics, please see "How to Manually Configure Your Internet Connection" on page 3-10.

c. From the main menu Advanced section, click the **LAN IP Setup** link. The following menu appears

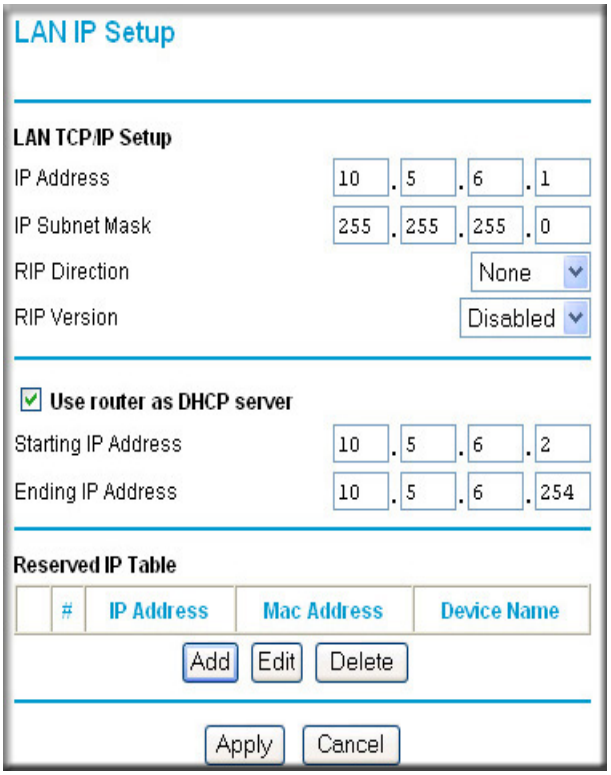


Figure 7-8: LAN IP Setup menu

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 9-3.

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. From the main menu VPN section, click on the **IKE Policies** link, and then click the **Add** button to display the screen below.

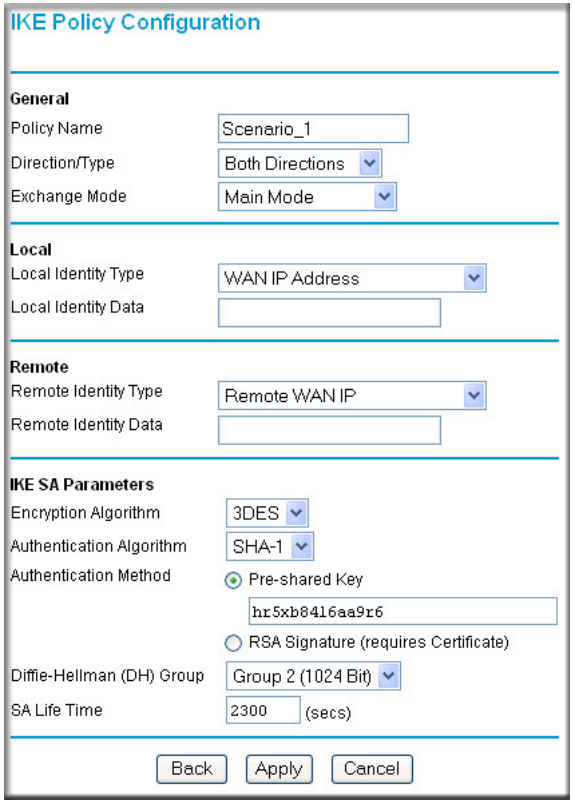


Figure 7-9: Scenario 1 IKE Policy

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 Policies' Automatic Key and Authentication Management" on page 7-3.

4. **Set up the FVG318 VPN -Auto Policy illustrated below.**

   a. From the main menu VPN section, click on the **VPN Policies** link, and then click on the **Add Auto Policy** button.

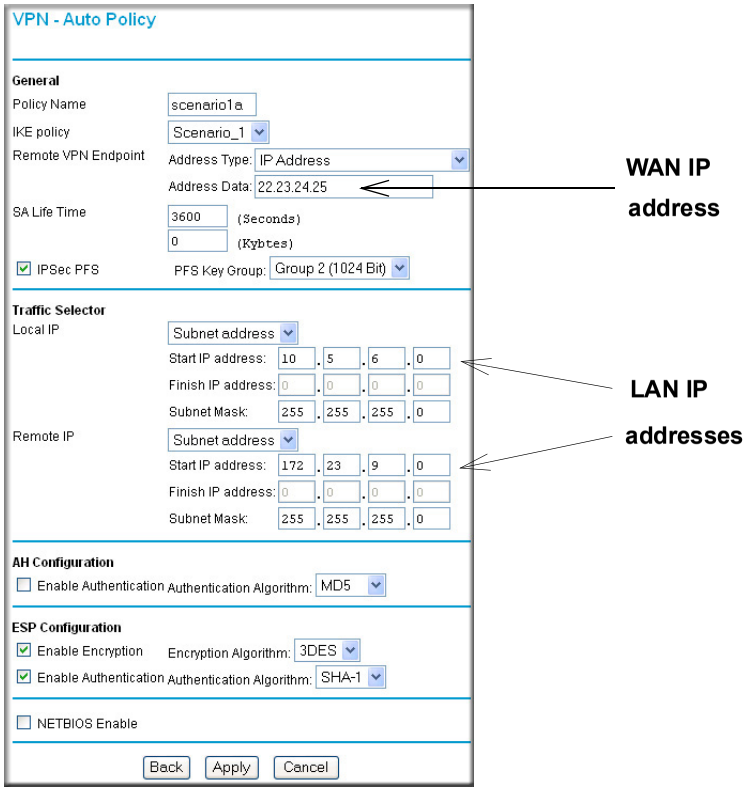


Figure 7-10: Scenario 1 VPN - Auto Policy

   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 Policies' Automatic Key and Authentication Management" on page 7-3.

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.**

How to Check VPN Connections

You can test connectivity and view VPN status information on the FVG318 (see also "VPN Tunnel Control" on page 6-26).

Testing the Gateway A FVG318 LAN and the Gateway B LAN

1. Using our example, from a PC attached to the FVG318 on LAN A, on a Windows PC click the **Start** button on the taskbar 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, 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**.
   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 seen in Figure 5-2 on page 5-3. 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. 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 will report the status and data transmission statistics of the VPN tunnels for each policy.

FVG318 Scenario 2: FVG318 to FVG318 with RSA 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.

Note: Before completing this configuration scenario, make sure the correct Time Zone is set on the FVG318. For instructions on this topic, see "Time Zone" on page 5-13.

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. From the main menu VPN section, click the **CAs** link.
   c. Click **Add** to add a CA.
   d. Click **Browse** to locate the *trust.txt* file.
   e. Click **Upload**.
3. **Create a certificate request for the FVG318.**
   a. From the main menu VPN section, click the **Certificates** link.

b. Click the **Generate Request** button to display the screen illustrated in Figure 7-11 below.

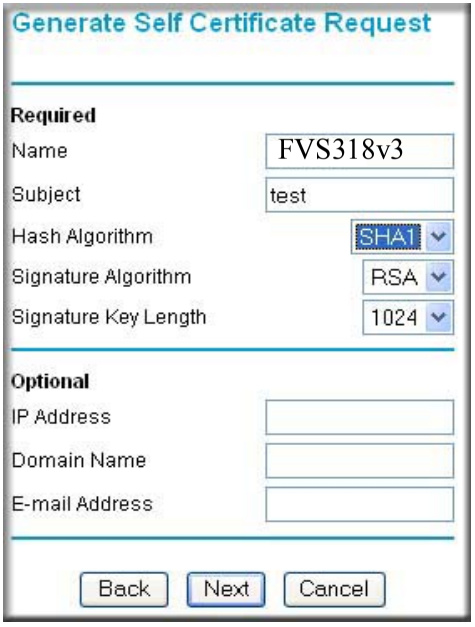


Figure 7-11: Generate Self Certificate Request menu

c. Fill in the fields on the Add Self Certificate screen.

- Required
  - 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.
- Optional
  - 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 you e-mail address here.

d. Click the **Next** button to continue. The FVG318 generates a Self Certificate Request as shown below.

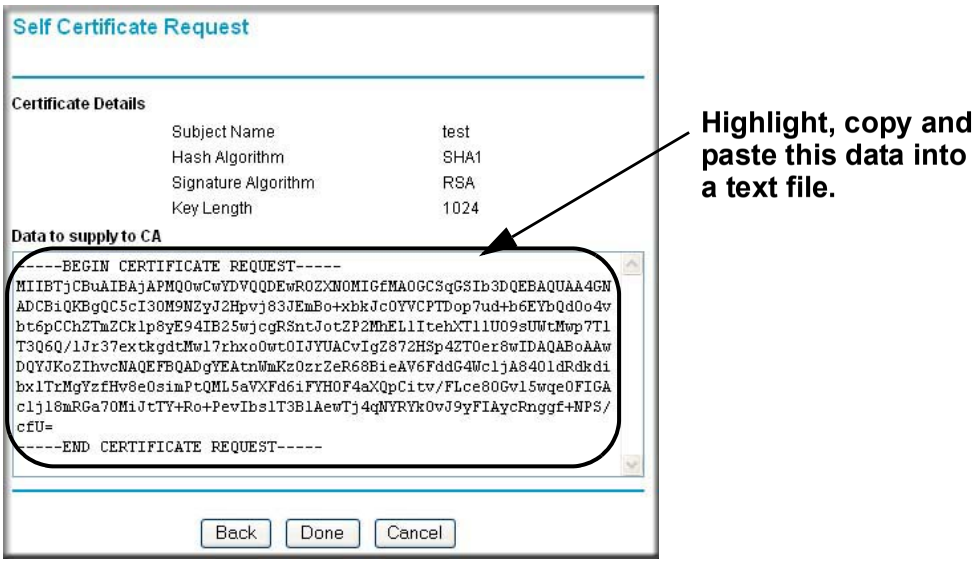


Figure 7-12: Self Certificate Request data

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.

c. When you have finished gathering the Self Certificate Request data, click the **Done** button. You will return to the Certificates screen where your pending "FVG318" Self Certificate Request will be listed, as illustrated in Figure 7-13 below.

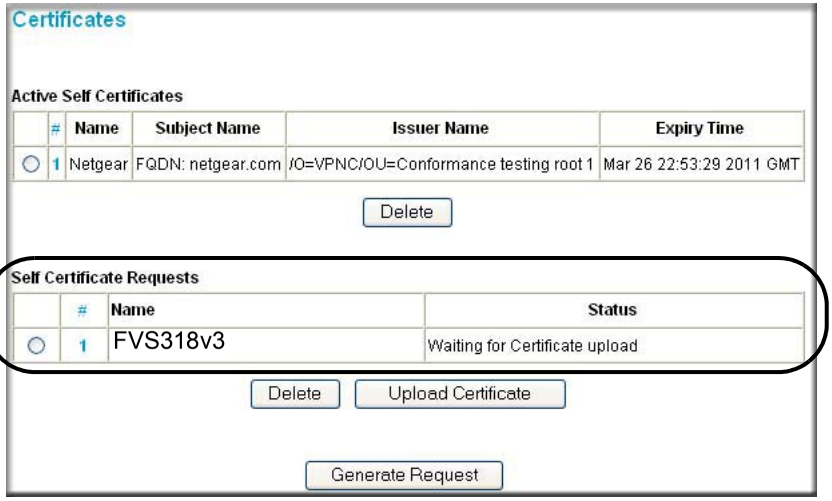


Figure 7-13: Self Certificate Requests table

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.**

   a. From the main menu VPN section, click the **Certificates** link.

   b. Click the radio button of the Self Certificate Request you want to upload.

   c. Click the **Upload Certificate** button.

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

   e. Click the **Upload** button.

f. You will now see the "FVG318" entry in the Active Self Certificates table and the pending "FVG318" Self Certificate Request is gone, as illustrated below.

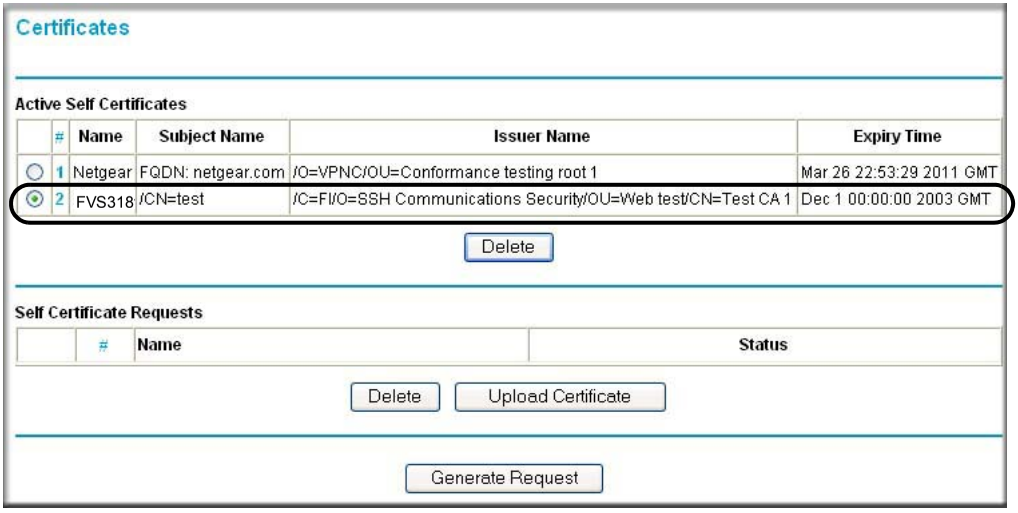


Figure 7-14: Self Certificates table

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** (see "Scenario 1 IKE Policy" on page 7-19) except now use the RSA Signature instead of the shared key.

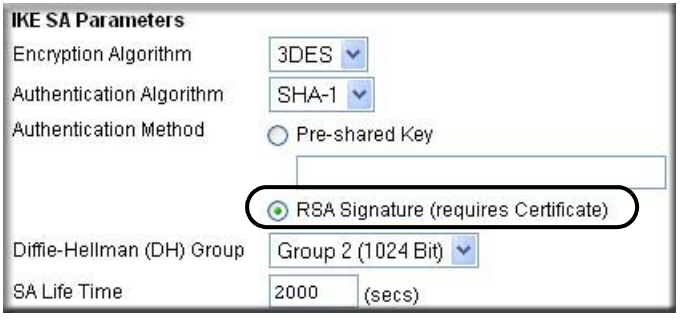


Figure 7-15: IKE policy using RSA Signature

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 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. From the main menu VPN section, click the **CRL** link.

c. Click **Add** to add a CRL.

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

e. Click **Upload**.

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 8
Maintenance

This chapter describes how to use the maintenance features of your FVG318 ProSafe 802.11g Wireless VPN Firewall. These features can be found by clicking on the Maintenance heading in the main menu of the browser interface.

Viewing Wireless VPN Firewall Status Information

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

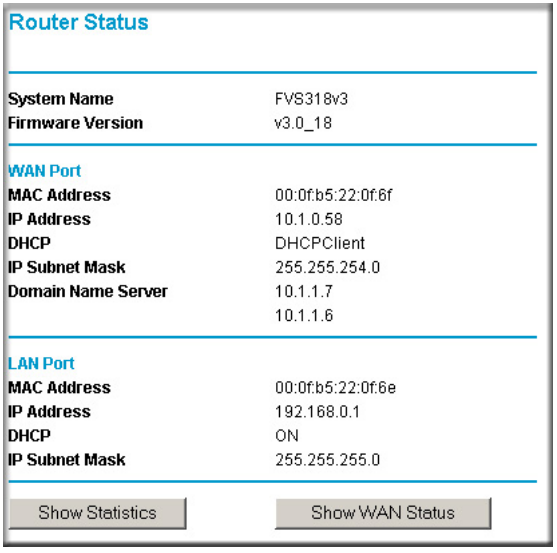


Figure 8-1: Router Status screen

This screen shows the following parameters:

Table 8-1. FVG318 Status fields

Field	Description
System Name	The System Name assigned to the firewall.
Firmware Version	The firewall firmware version.
WAN Port	These parameters apply to the Internet (WAN) port of the firewall.
MAC Address	The MAC address used by the Internet (WAN) port of the firewall.
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.
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.
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.
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 WAN Status** to display the WAN connection status.

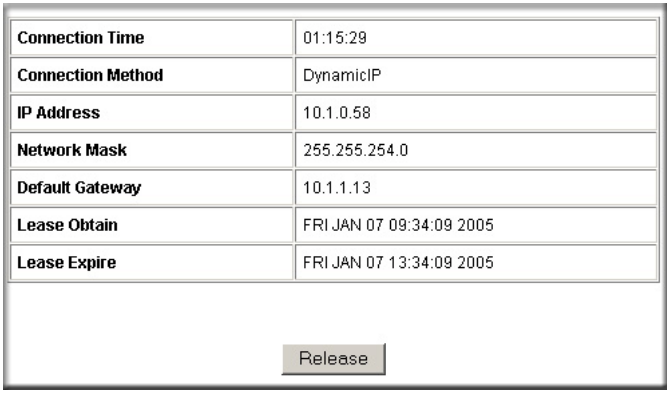


Figure 8-2: WAN Connection Status screen

This screen shows the following statistics:.

Table 8-1. Connection Status fields

Field	Description
Connection Time	The length of time the firewall has been connected to your Internet service provider's network.
Connection Method	The method used to obtain an IP address from your Internet service provider.
IP Address	The WAN (Internet) IP address assigned to the firewall.
Network Mask	The WAN (Internet) subnet mask assigned to the firewall.
Default Gateway	The WAN (Internet) default gateway the firewall communicates with.

Log action buttons are described in Table 8-2

Table 8-2. Connection Status action buttons

Button	Description
Renew	Click the **Renew** button to renew the DHCP lease.

Click **Show Statistics** to display firewall usage statistics.

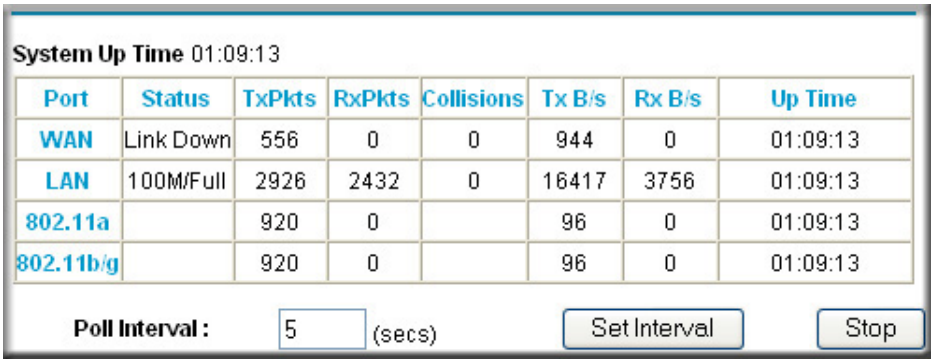


Figure 8-3: Router Statistics screen

This screen shows the following statistics:

Table 8-1. Router Statistics fields

Field	Description
Interface	The statistics for the WAN (Internet), LAN (local), 802.11a, and 802.11b/g interfaces. For each interface, the screen displays:
Status	The link status of the interface.
TxPkts	The number of packets transmitted on this interface since reset or manual clear.
RxPkts	The number of packets received on this interface since reset or manual clear.
Collisions	The number of collisions on this interface since reset or manual clear.
Tx B/s	The current transmission (outbound) bandwidth used on the interfaces.
Rx B/s	The current reception (inbound) bandwidth used on the interfaces.
Up Time	The amount of time since the firewall was last restarted.
Up Time	The time elapsed since this port acquired the link.
Poll Interval	Specifies the intervals at which the statistics are updated in this window. Click on **Stop** to freeze the display.

WAN Status action buttons are described in the table below:

Table 8-2. Connection Status action buttons

Field	Description
Set Interval	Enter a time and click the button to set the polling frequency.
Stop	Click the **Stop** button to freeze the polling information.

Viewing a List of Attached Devices

The Attached Devices menu contains a table of all IP devices that the firewall has discovered on the local network. From the main menu of the browser interface, under the Maintenance heading, select Attached Devices to view the table, shown below.

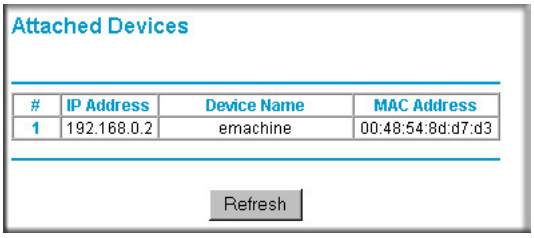


Figure 8-4: Attached Devices menu

For each device, the table shows the IP address, NetBIOS Host Name (if available), and Ethernet MAC address. Note that if the firewall is rebooted, the table data is lost until the firewall rediscovers the devices. To force the firewall to look for attached devices, click the **Refresh** button.

Upgrading the Firewall Software

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

The routing software of the FVG318 Wireless 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 FVG318 Wireless VPN Firewall must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer or Netscape Navigator 5.0 or above.

From the main menu of the browser interface, under the Maintenance heading, select the Router Upgrade heading to display the menu shown below.

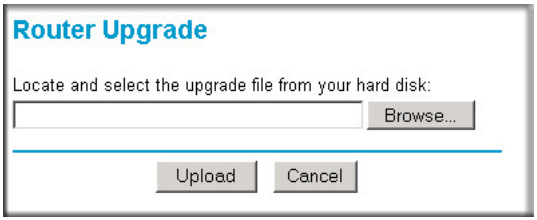


Figure 8-5: Router Upgrade menu

To upload new firmware:

1. Download and unzip the new software file from NETGEAR.
2. In the Router Upgrade menu, click the **Browse** button and browse to the location of the binary (.BIN) upgrade file
3. Click **Upload**.

   Note: When uploading software to the FVG318 Wireless 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 one minute.

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

Configuration File Management

The configuration settings of the FVG318 Wireless 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.

From the main menu of the browser interface, under the Maintenance heading, select the Settings Backup heading to bring up the menu shown below.

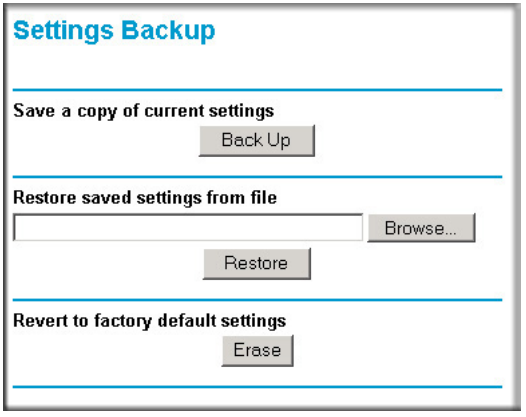


Figure 8-6: Settings Backup menu

You can use the Settings Backup menu to back up your configuration in a file, restore from that file, or erase the configuration settings.

Backing Up the Configuration

To save your settings, select the Backup tab. Click the **Backup** button. Your browser will extract the configuration file from the firewall and prompts 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.

Restoring the Configuration

To restore your settings from a saved configuration file, enter the full path to the file on your PC or click the **Browse** button to browse to the file. When you have located it, click the **Restore** button to send the file to the firewall. The firewall will then reboot automatically.

Erasing the Configuration

It is sometimes desirable to restore the firewall to a known blank condition. To do this, see the Erase function, which will restore all factory settings. After an erase, the firewall's password will be **password**, the LAN IP address will be 192.168.0.1, and the firewall's DHCP client will be enabled.

To erase the configuration, click the **Erase** button.

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 10-7.

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.

From the main menu of the browser interface, under the Maintenance heading, select Set Password to bring up this menu.

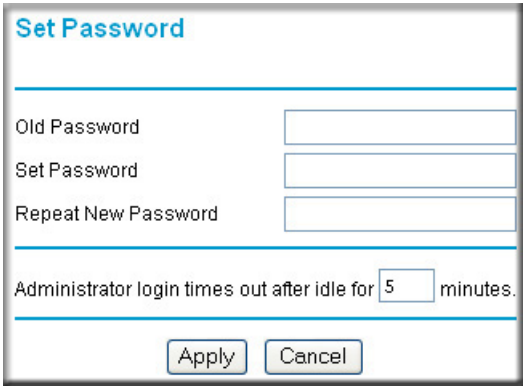


Figure 8-7: Set Password menu

To change the password, first enter the old password, and then enter the new password twice. Click **Apply**. To change the login idle timeout, change the number of minutes and click **Apply**.

Chapter 9
Advanced Configuration

This chapter describes how to configure the advanced features of your FVG318 ProSafe 802.11g Wireless VPN Firewall. These features can be found under the Advanced heading in the main menu of the browser interface.

How to Configure 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. From the main menu of the browser interface, under Advanced, click on **Dynamic DNS**.
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 and RIP. From the main menu of the browser interface, under Advanced, click on **LAN IP Setup** to view the menu shown below.

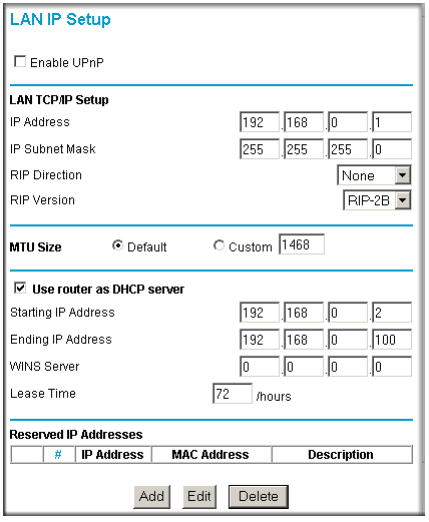


Figure 9-1: LAN IP Setup Menu

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.
- RIP Direction
  RIP (Router Information Protocol) allows a firewall to exchange routing information with other firewalls. 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.
- RIP Version
  This controls the format and the broadcasting method of the RIP packets that the firewall sends. (It recognizes both formats when receiving.) By default, this is set for RIP-1.
  - 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.

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 "IP Configuration by DHCP" on page B-10" 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 192.168.0.253, 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 Basic Settings menu; otherwise, the firewall's LAN IP address)
- Secondary DNS server (if you entered a secondary DNS address in the Basic 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 **Add** button.
2. In the IP Address box, 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.)
3. Type the MAC Address of the PC or server.
   (**Tip**: If the PC is already present on your network, you can copy its MAC address from the Attached Devices menu and paste it here.)
4. 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 the button next to the reserved address you want to edit or delete.
2. Click **Edit** or **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.

From the Main Menu of the browser interface, under Advanced, click on **Static Routes** to view the Static Route table shown below.

Figure 9-2: Static Routes table

To add or edit a Static Route:

1. Click the **Add** button to open the Add/Edit menu, shown below.

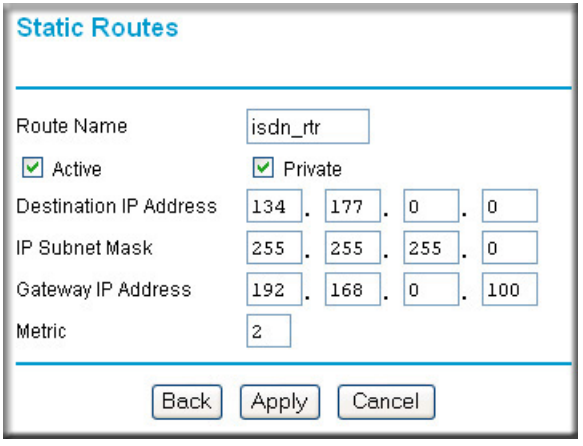


Figure 9-3: Static Route Entry and Edit menu

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.
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.

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 9-3.

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 Wireless 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 the Turn Remote Management On check box.
2. 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.

   a. To allow access from any IP address on the Internet, select Everyone.

   b. To allow access from a range of IP addresses on the Internet, select IP address range. Enter a beginning and ending IP address to define the allowed range.

   c. To allow access from a single IP address on the Internet, select Only this PC. Enter the IP address that will be allowed access.
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.
5. When accessing your firewall from the Internet, the Secure Sockets Layer (SSL) will be enabled. You will enter *https://* and type your firewall's WAN IP address into your browser, followed by a colon (:) and the custom port number. For example, if your WAN IP address is 134.177.0.123 and you use port number 8080, type the following in your browser:

   https://134.177.0.123:8080

   If you do not use the SSL *https://address*, but rather use *http://address*, the FVG318 will automatically attempt to redirect to *https://address.*

   Note: The first time you remotely connect the FVG318 with a browser via SSL, you may get a message regarding the SSL certificate. If you are using a Windows computer with Internet Explorer 5.5 or higher, simply click **Yes** to accept the certificate.

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.

Chapter 10
Troubleshooting

This chapter gives information about troubleshooting your FVG318 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 10-7.

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 10-7.
- 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 "How to Manually Configure Your Internet Connection" on page 3-10.

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 10-2".
  - — 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 "How to Manually Configure Your Internet Connection" on page 3-10.

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 Erase function of the firewall (see "Erasing the Configuration" on page 8-8).
- 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.

1. Press and hold the **Reset** button until the Test LED turns on and begins blinking (about 10 seconds).
2. 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 FVG318 Wireless VPN Firewall uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000. Cause: The 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
Technical Specifications

This appendix provides technical specifications for the FVG318 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 (32° to 104° F)
Operating humidity:	90% maximum relative humidity, noncondensing

Electromagnetic Emissions	
Meets requirements of:	FCC Part 15 Class B
	VCCI Class B
	EN 55 022 (CISPR 22), Class B
Interface Specifications	
LAN:	10BASE-T or 100BASE-Tx, RJ-45
WAN:	10BASE-T or 100BASE-Tx, RJ-45

Appendix B
VPN Configuration of NETGEAR FVS318v3

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 B-6)
- FVS318v3 to FVS318v2 (see page B-13)
- FVS318v3 to FVL328 (see page B-20)
- FVS318v3 to VPN Client (see page B-27)

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.

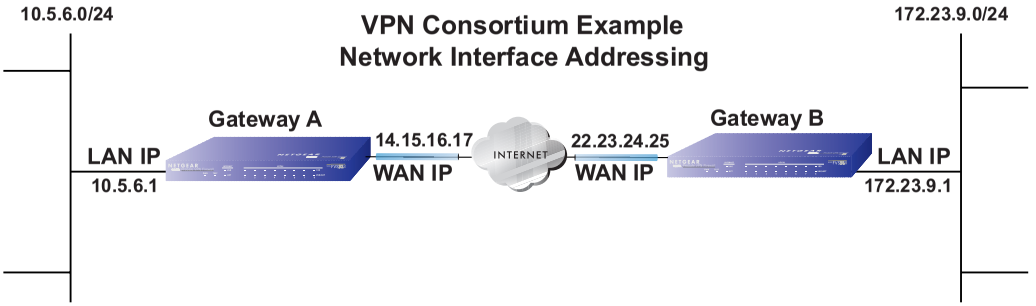


Figure B-1: Addressing and subnets used for this case study

Configuring the Gateways

Configure each gateway as summarized in Figure B-2 and Figure B-3:

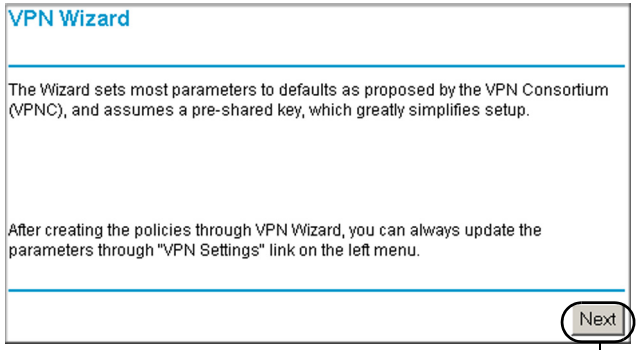
1. **Configure Gate A.**
   a. **Log in to the router at Gateway A.**
   b. **Use the VPN Wizard to configure this router.**

      Enter the requested information as prompted by the VPN Wizard:

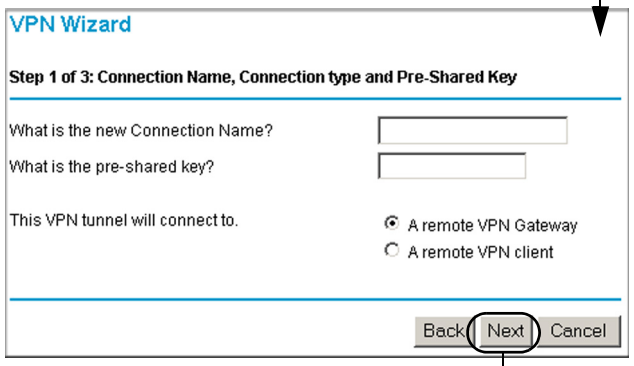
      - Connection Name and Pre-Shared Key
      - Remote WAN IP address
      - Remote LAN IP Subnet: IP Address and Subnet Mask:
2. **Repeat the above steps for Gateway B.**
   a. **Log in to the router at Gateway B.**
   b. **Use the VPN Wizard to configure this router.**

      Enter the requested information as prompted by the VPN Wizard.

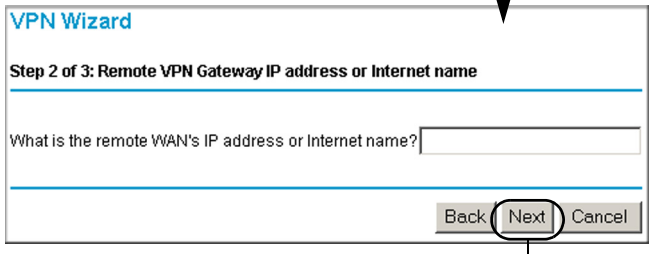
	Note: The WAN and LAN IP addresses must be unique at each end of the VPN tunnel.



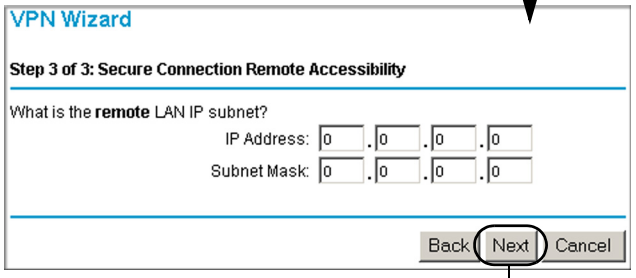
Step 1: Click VPN Wizard on the Side Menu Bar



Step 2: Enter the following:
- **Connection name**
- **Pre-Shared Key (must be the same for each end)**
- **Select "A remote VPN Gateway"**



Step 3: Enter the remote WAN's IP address



Step 4: Enter the following:
- **Remote LAN IP Address**
- **Remote LAN Subnet Mask**

to Figure B-3

Figure B-2: NETGEAR's VPN Wizard for the router at each gateway (part 1 of 2)

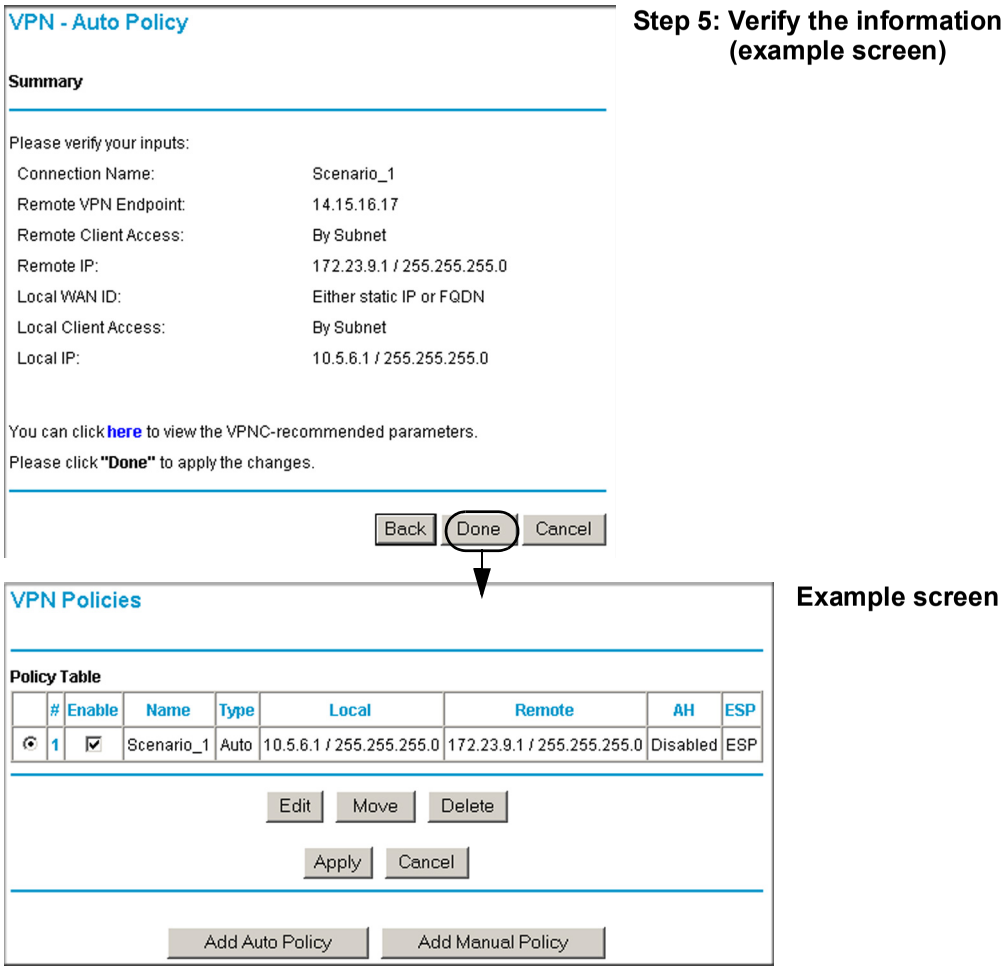


Figure B-3: NETGEAR's VPN Wizard for the router at a gateway A (part 2 of 2)

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:

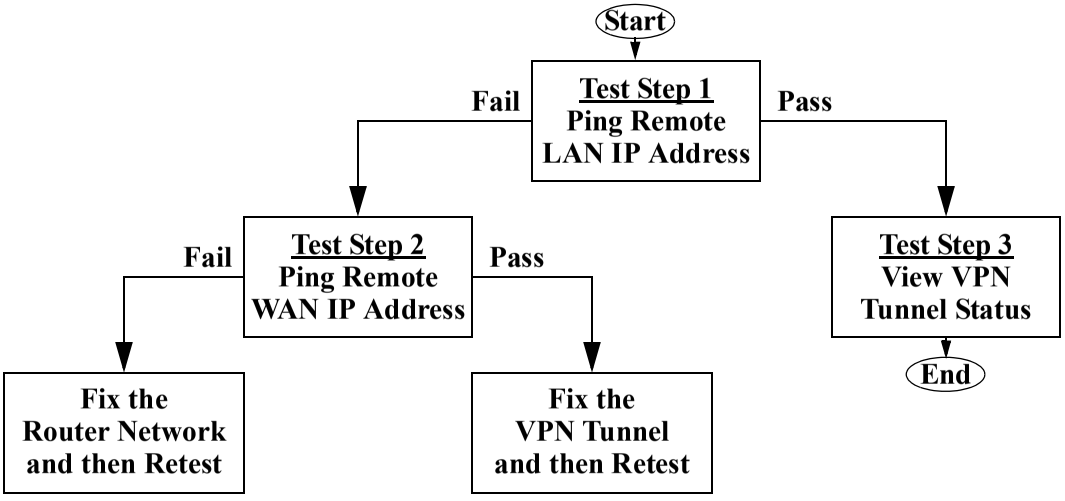


Figure B-4: Testing Flowchart

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 B-1. 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
Model/Firmware Tested:		
	NETGEAR-Gateway A	FVS318v3 with firmware version v3.0_14
	NETGEAR-Gateway B	FVS318v3 with firmware version v3.0_14
IP Addressing:		
	NETGEAR-Gateway A	Static IP address
	NETGEAR-Gateway B	Static IP address

Configuring the VPN Tunnel

Note: This scenario assumes all ports are open on the FVG318.

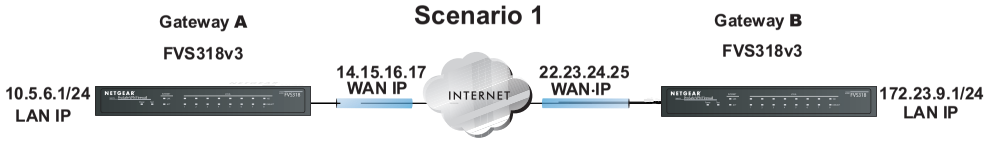


Figure B-5: LAN to LAN VPN access from an FVG318 to an FVG318

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 B-5).**

   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.**

   Follow the steps listed in Figure B-2 and Figure B-3 using the following parameters as illustrated in Figure B-6:

   - 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 as in the illustration (Figure B-5).**

   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.**

   Follow the steps listed in Figure B-2 and Figure B-3, but use the following parameters instead as illustrated in Figure B-6:

   - 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 11).

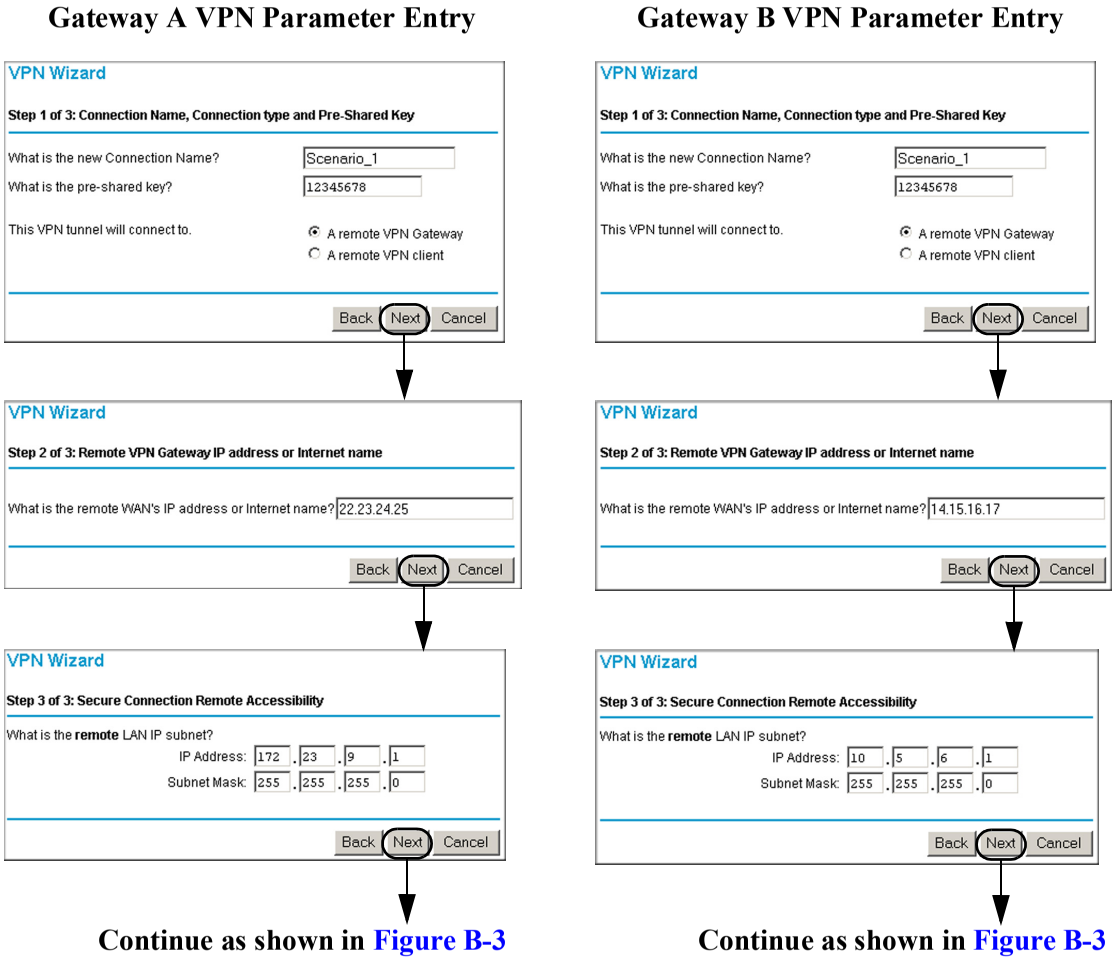


Figure B-6: VPN parameter entry at Gateway A (FVS318v3) and Gateway B (FVS318v3)

Viewing and Editing the VPN Parameters

The VPN Wizard sets up a VPN tunnel using the default parameters from the VPN Consortium (VPNC). The policy definitions to manage VPN traffic on the FVG318 are presented in Figure B-7 and Figure B-8.

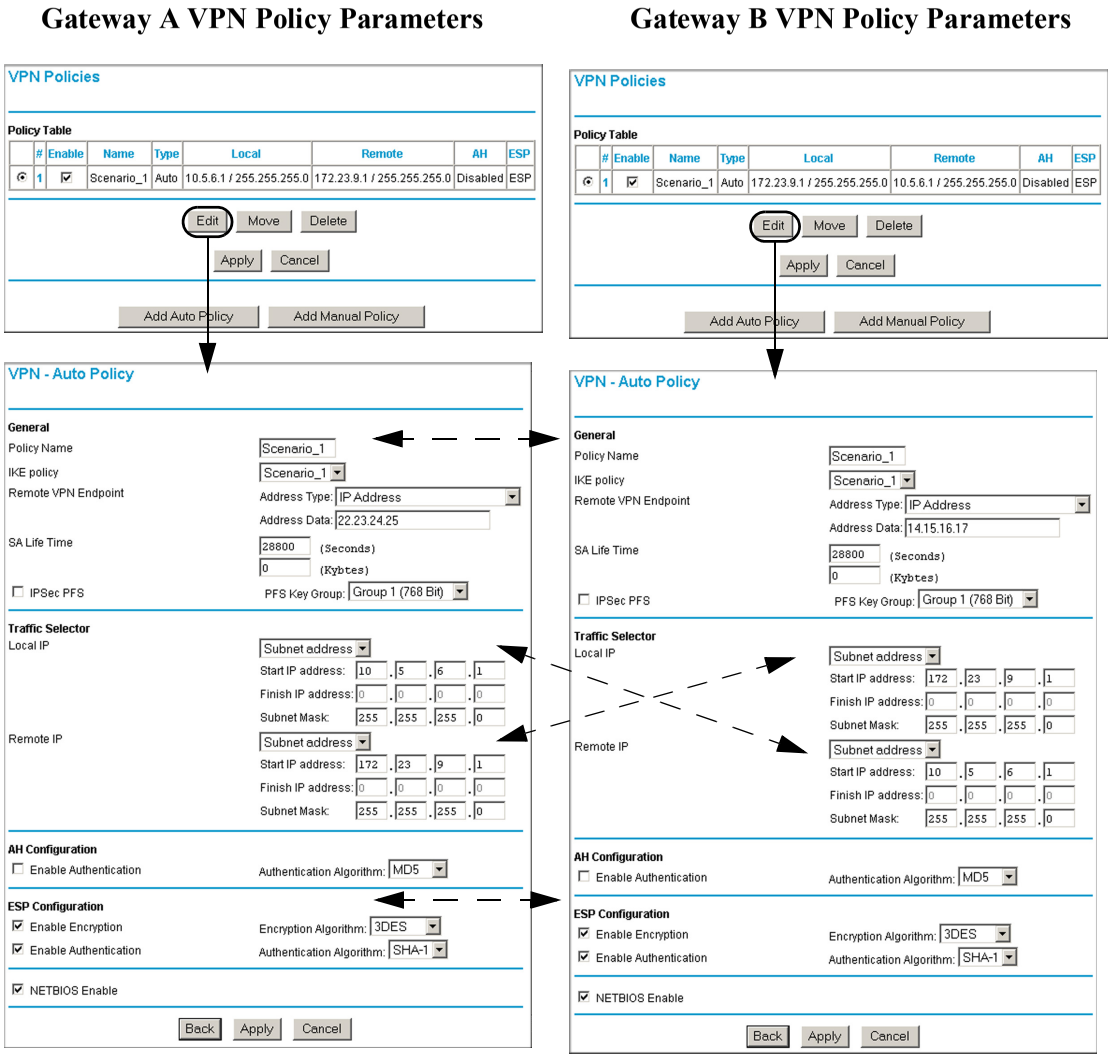


Figure B-7: VPN policies at Gateway A (FVS318v3) and Gateway B (FVS318v3)

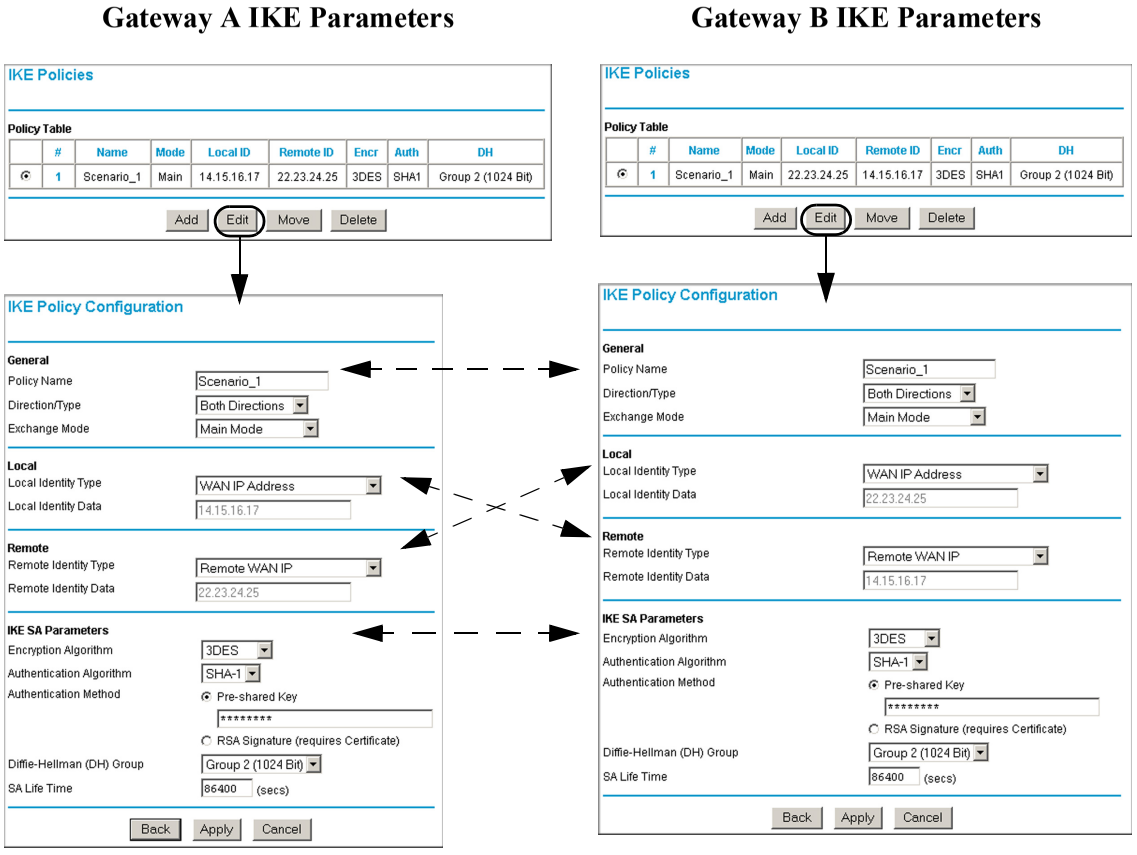


Figure B-8: IKE parameters at Gateway A (FVS318v3) and Gateway B (FVS318v3)

Note: 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 B-4. 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 taskbar 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.

VPN Status at Gateway A (FVS318v3)

IPSec SA

#	SPI	Policy Name	Endpoint	Protocol	Tx (KBytes)	HLifeTime	SLifeTime
1	4275228533	INScenario_1	14.15.16.17	ESP	10584	28630	0
2	3947861323	Scenario_1	22.23.24.25	ESP	10584	28630	28570

IKE SA

#	Policy Name	Endpoint	State	LifeTime in Secs
1	Scenario_1	22.23.24.25	SA_MATURE	86233

Status of VPN tunnel from Gateway B

Status of VPN tunnel to Gateway B

VPN Status at Gateway B (FVS318v3)

IPSec SA

#	SPI	Policy Name	Endpoint	Protocol	Tx (KBytes)	HLifeTime	SLifeTime
1	3947861323	INScenario_1	22.23.24.25	ESP	20604	28290	0
2	4275228533	Scenario_1	14.15.16.17	ESP	21108	28290	28200

IKE SA

#	Policy Name	Endpoint	State	LifeTime in Secs
1	Scenario_1	14.15.16.17	SA_MATURE	85891

Status of VPN tunnel from Gateway A

Status of VPN tunnel to Gateway A

Figure B-9: VPN Status for the FVS318v3 routers at Gateway A and Gateway B

The FVG318-to-FVS318v2 Case

Table B-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
Model/Firmware Tested:		
	NETGEAR-Gateway A	FVS318v3 with firmware version v3.0_14
	NETGEAR-Gateway B	FVS318v2 with firmware version V2.4
IP Addressing:		
	NETGEAR-Gateway A	Static IP address
	NETGEAR-Gateway B	Static IP address

Configuring the VPN Tunnel

Note: This scenario assumes all ports are open on the FVG318 and FVS318v2.

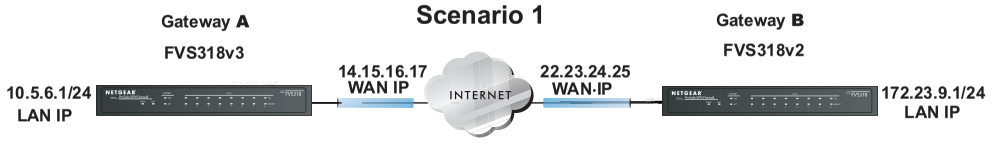


Figure B-10: LAN to LAN VPN access from an FVG318 to an FVS318v2

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 B-10).**

   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.**

   Follow the steps listed in Figure B-2 and Figure B-3 using the following parameters as illustrated in Figure B-11:

   - 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 as in the illustration (Figure B-10).**

   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.**

   Follow the steps listed in Figure B-2 and Figure B-3, but use the following parameters instead as illustrated in Figure B-11:

   - 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 18).

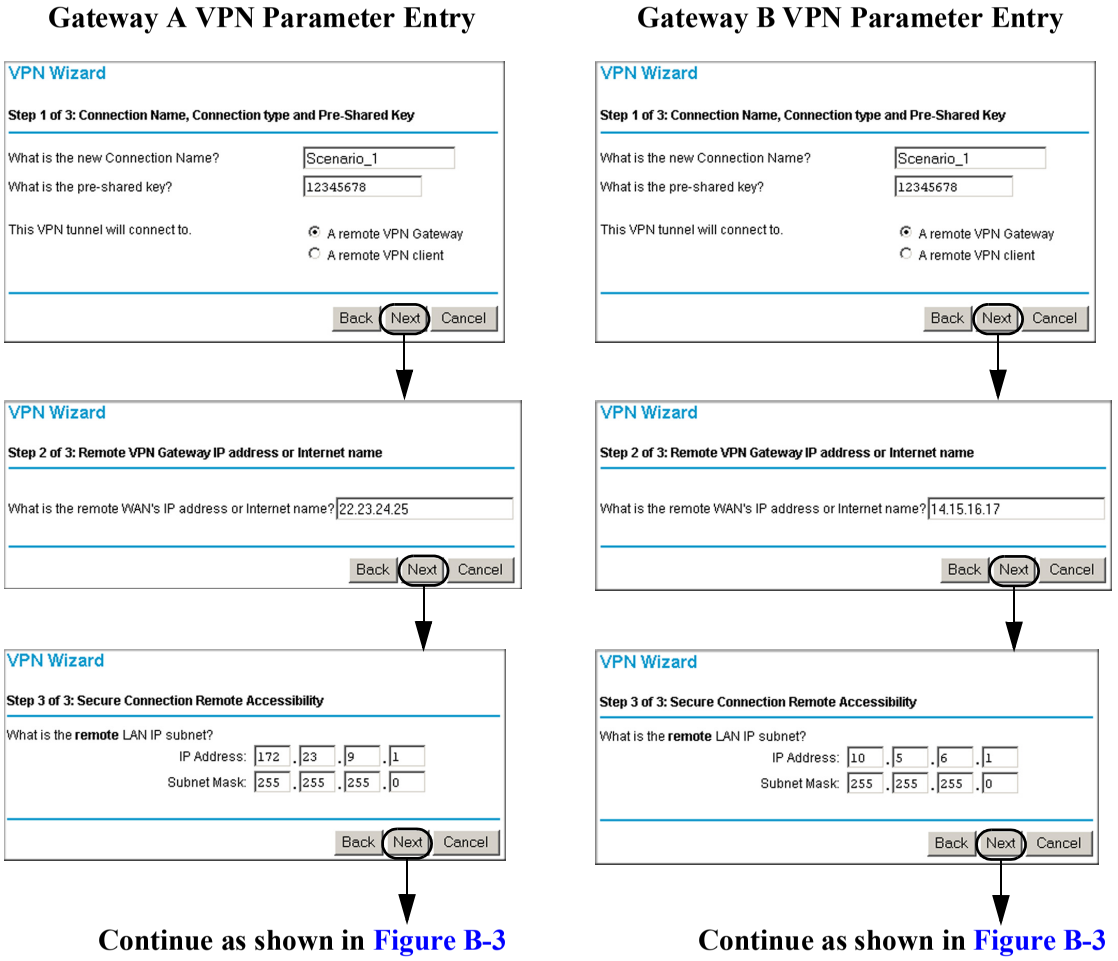


Figure B-11: VPN parameter entry at Gateway A (FVS318v3) and Gateway B (FVS318v2)

Viewing and Editing the VPN Parameters

The VPN Wizard sets up a VPN tunnel using the default parameters from the VPN Consortium (VPNC). The policy definitions to manage VPN traffic are presented in Figure B-12.

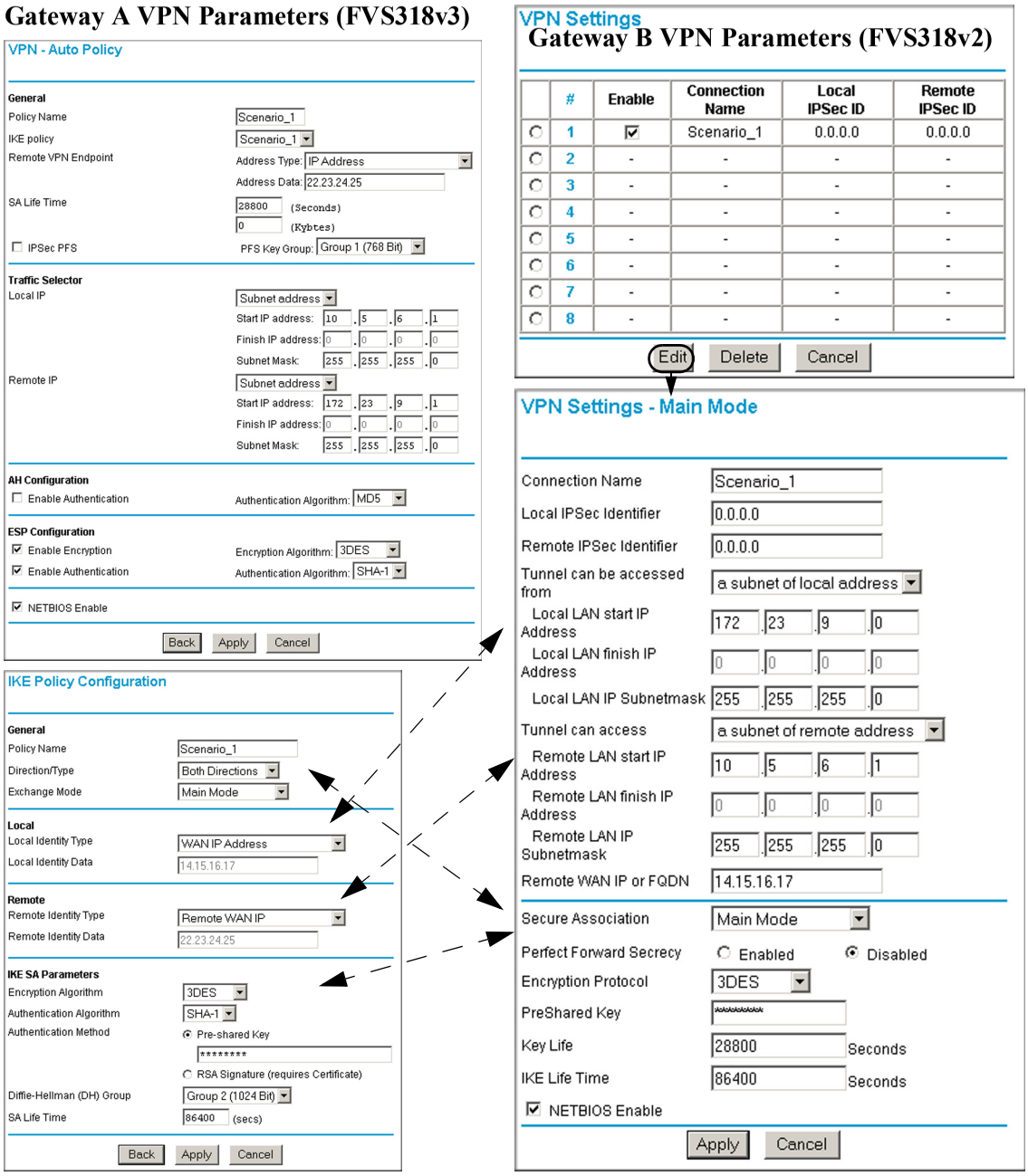


Figure B-12: VPN Parameters at Gateway A (FVS318v3) and Gateway B (FVS318v2)

	**Note:** 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

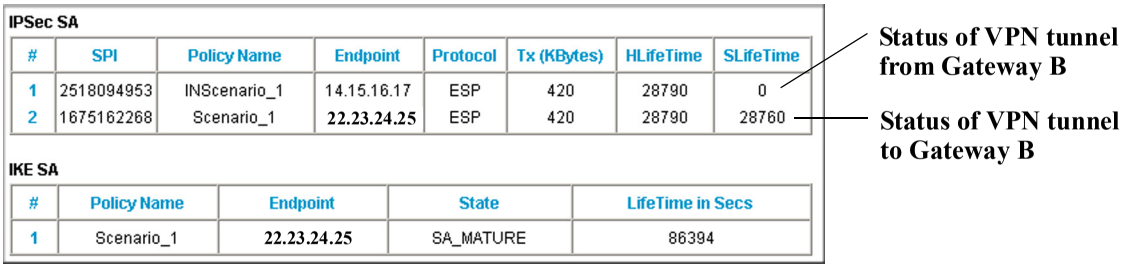
You can test connectivity and view VPN status information on the FVG318 according to the testing flowchart shown in Figure B-4. To test the VPN tunnel from the Gateway A LAN, do the following:

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 taskbar 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 and FVS318v2 event log and status of Security Associations, go to the FVG318 main menu VPN section and click the **VPN Status** link. For the FVS318v2, click **Show VPN Status** from the Router Status screen.

VPN Status at Gateway A (FVS318v3)



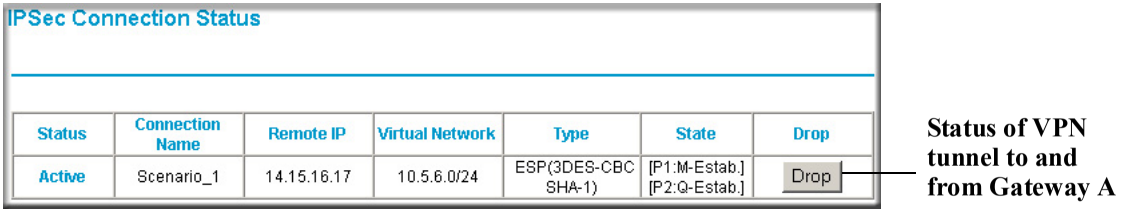
IPSec SA

#	SPI	Policy Name	Endpoint	Protocol	Tx (KBytes)	HLifeTime	SLifeTime
1	2518094953	INScenario_1	14.15.16.17	ESP	420	28790	0
2	1675162268	Scenario_1	22.23.24.25	ESP	420	28790	28760

IKE SA

#	Policy Name	Endpoint	State	LifeTime in Secs
1	Scenario_1	22.23.24.25	SA_MATURE	86394

IPSec Connection Status at Gateway B (FVS318v2)



IPSec Connection Status

Status	Connection Name	Remote IP	Virtual Network	Type	State	Drop
Active	Scenario_1	14.15.16.17	10.5.6.0/24	ESP(3DES-CBC SHA-1)	[P1:M-Estab.] [P2:Q-Estab.]	Drop

Figure B-13: VPN Status for the routers at Gateway A (FVS318v3) and Gateway B (FVS318v2)

The FVG318-to-FVL328 Case

Table B-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
Date Tested:		November 2004
Model/Firmware Tested:		
	NETGEAR-Gateway A	FVS318v3 with firmware version v3.0_14
	NETGEAR-Gateway B	FVL328 with firmware version V2.0_01
IP Addressing:		
	NETGEAR-Gateway A	Static IP address
	NETGEAR-Gateway B	Static IP address

Configuring the VPN Tunnel

Note: This scenario assumes all ports are open on the FVG318 and FVL328.

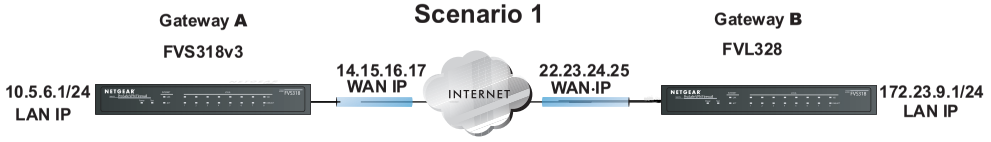


Figure B-14: LAN to LAN VPN access from an FVG318 to an FVL328

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 B-14).**

   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.**

   Follow the steps listed in Figure B-2 and Figure B-3 using the following parameters as illustrated in Figure B-15:

   - 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 as in the illustration (Figure B-14).**

   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.**

   Follow the steps listed in Figure B-2 and Figure B-3, but use the following parameters instead as illustrated in Figure B-15:

   - 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 25).

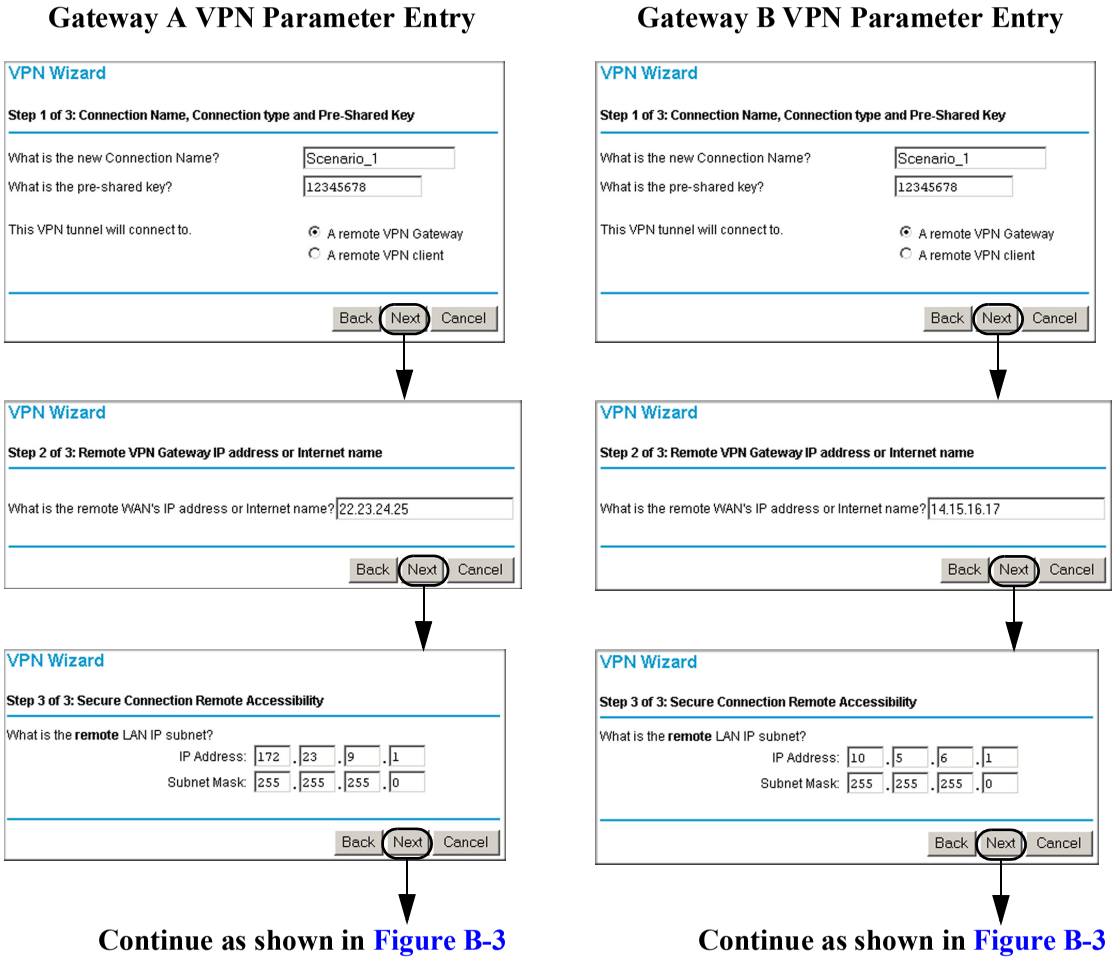


Figure B-15: VPN parameter entry at Gateway A (FVS318v3) and Gateway B (FVL328)

Viewing and Editing the VPN Parameters

The VPN Wizard sets up a VPN tunnel using the default parameters from the VPN Consortium (VPNC). The policy definitions to manage VPN traffic on the FVG318 and FVL328 are presented in Figure B-16 and Figure B-17.

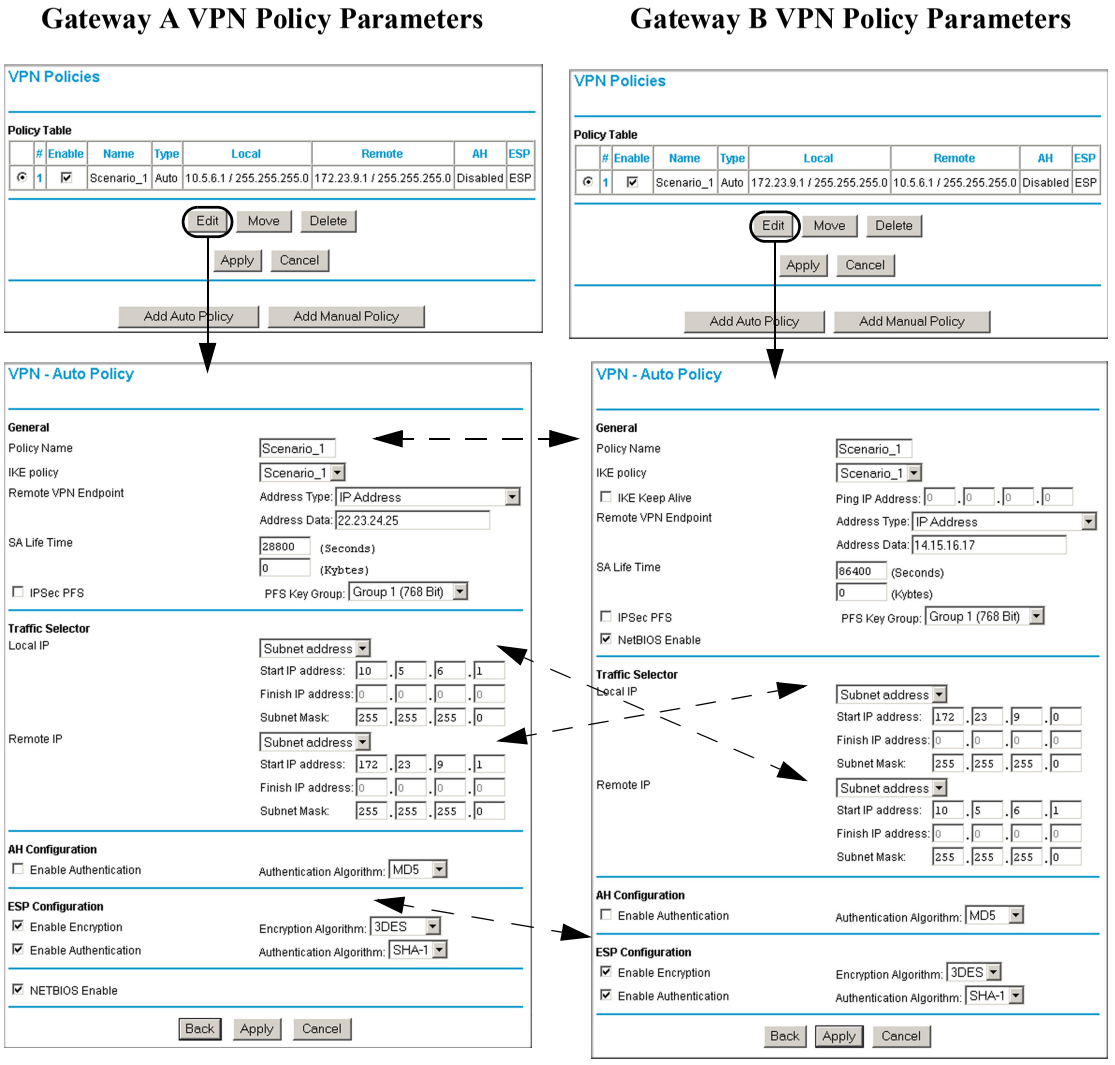


Figure B-16: VPN policies at Gateway A (FVS318v3) and Gateway B (FVL328)

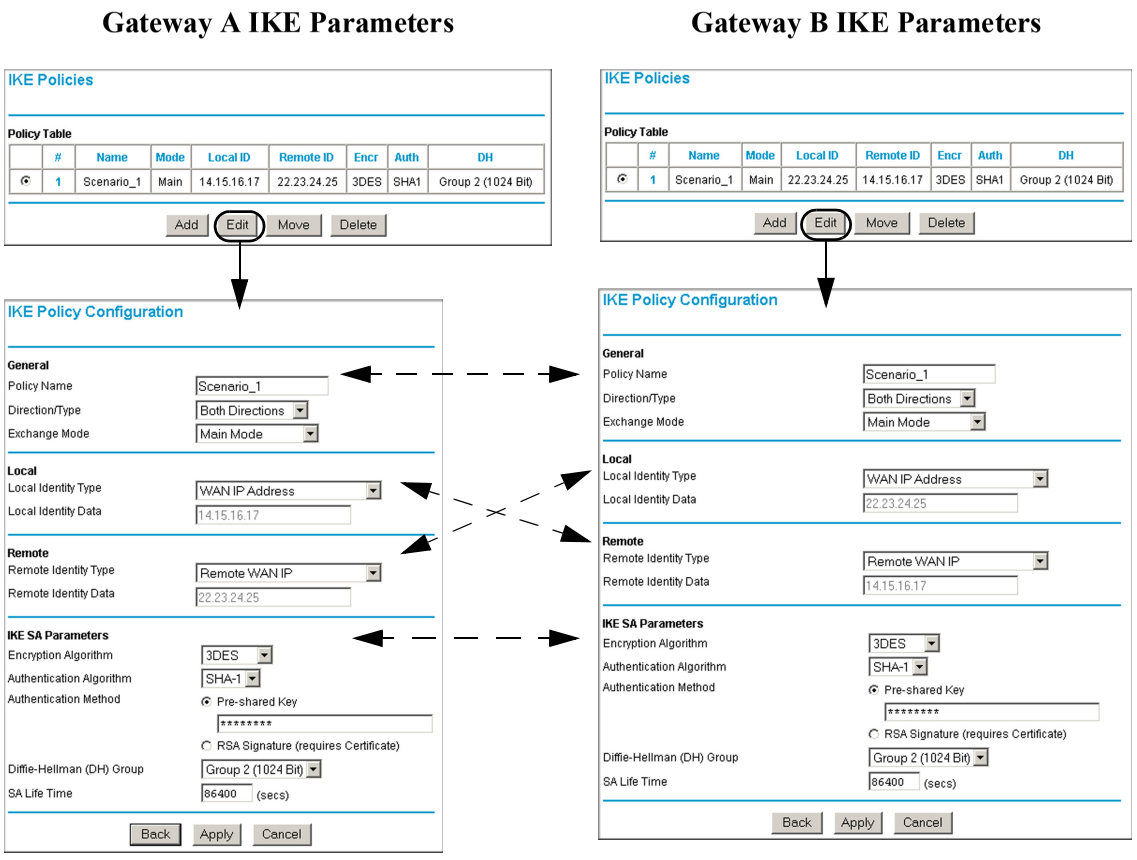


Figure B-17: IKE parameters at Gateway A (FVS318v3) and Gateway B (FVL328)

Note: 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 B-4. 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 taskbar 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 VPN section and click the **VPN Status** link. For the FVL328, click **VPN Status** on the VPN Status/Log screen.

VPN Status at Gateway A (FVS318v3)

IPSec SA

#	SPI	Policy Name	Endpoint	Protocol	Tx (KBytes)	HLifeTime	SLifeTime
1	3968809181	INScenario_1	14.15.16.17	ESP	360	28790	0
2	2149271209	Scenario_1	22.23.24.25	ESP	360	28790	28730

IKE SA

#	Policy Name	Endpoint	State	LifeTime in Secs
1	Scenario_1	22.23.24.25	SA_MATURE	86395

Status of VPN tunnel from Gateway B

Status of VPN tunnel to Gateway B

IPSec Connection Status at Gateway B (FVL328)

IPSec Connection Status

#	Policy Name	Endpoint	Tx (KBytes)	State	Action
1	Scenario_1	14.15.16.17	13010	Phase 1: M-ESTABLISHED / Phase 2: ESTABLISHED	Drop

Status of VPN tunnel to and from Gateway A

Figure B-18: VPN Status for the routers at Gateway A (FVS318v3) and Gateway B (FVL328)

The FVG318-to-VPN Client Case

Table B-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
Model/Firmware Tested:		
	NETGEAR-Gateway A	FVS318v3 with firmware version v3.0_14
	NETGEAR-Client B	NETGEAR ProSafe VPN Client v10.3.5
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 B-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

Note: This scenario assumes all ports are open on the FVG318.

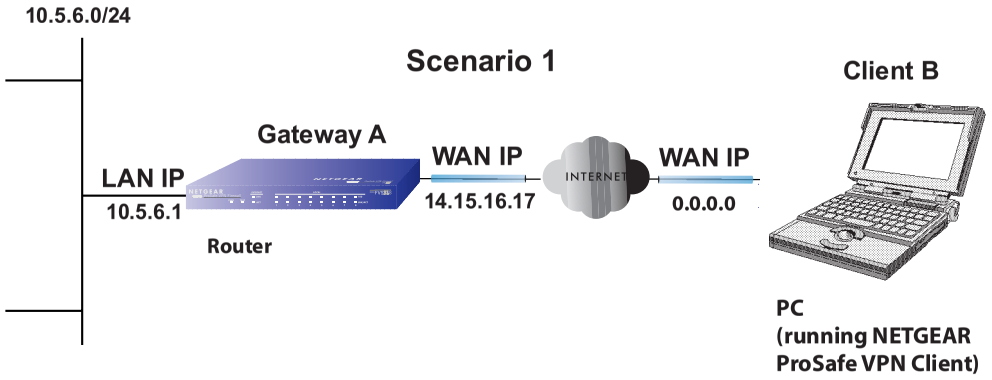


Figure B-19: LAN to PC VPN access from an FVG318 to a VPN Client

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 B-19).**

   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.**

   Follow the steps illustrated in Figure B-19 (the resulting parameter screens are shown in Figure B-20):

   - 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**

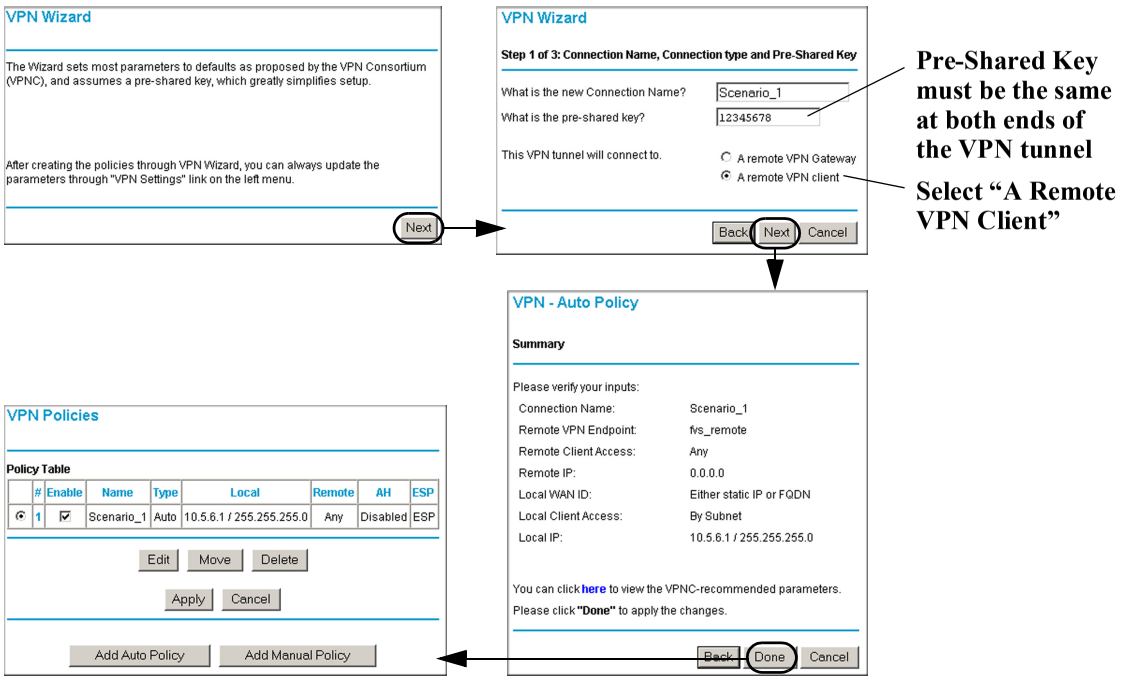


Figure B-20: VPN Wizard at Gateway A (FVS318v3)

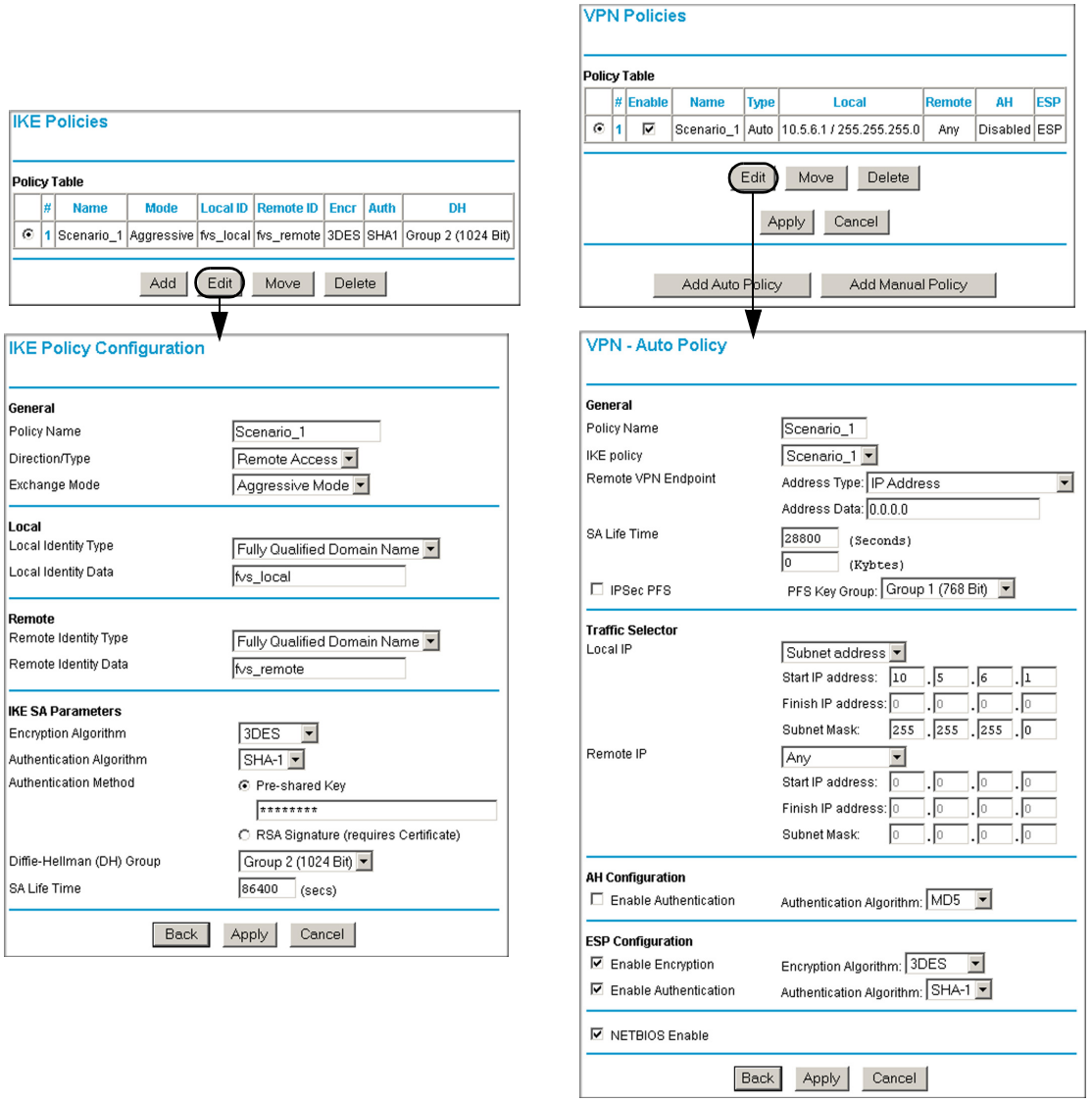


Figure B-21: VPN parameters at Gateway A (FVS318v3)

3. **Set up the VPN Client at Gateway B as in the illustration (Figure B-19).**

   a. Right-mouse-click the ProSafe icon ( ) 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.)

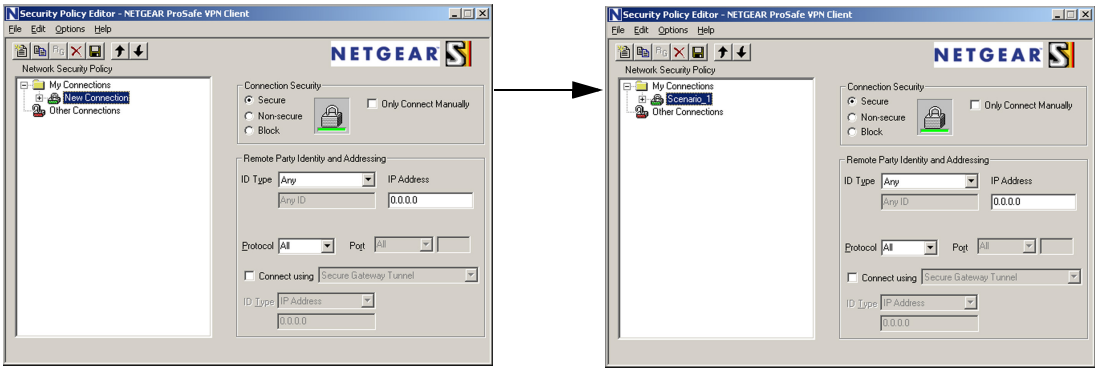


Figure B-22: Adding and renaming a new connection

c. Program the **Scenario_1** connection screen as follows (see Figure B-23):

- 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 Autopolicy** screen shown in Figure B-21 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 B-21 for the gateway router. Also, **Gateway IP Address** must match the WAN IP address of the gateway router shown in Figure B-19.)
- 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.

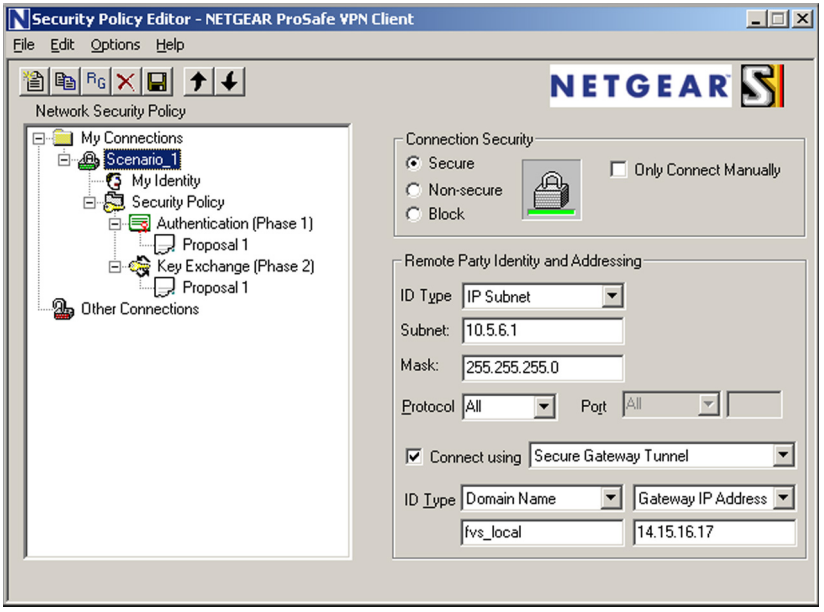


Figure B-23: Scenario_1 connection screen parameters

d. Select **Security Policy** on the left hierarchy menu and then select **Aggressive Mode** under **Select Phase 1 Negotiation Mode** (see Figure B-24). (The **Select Phase 1 Negotiation Mode** choice must match the **Exchange Mode** setting for the **General IKE Policy Configuration** parameters shown in Figure B-21 for the gateway router.)

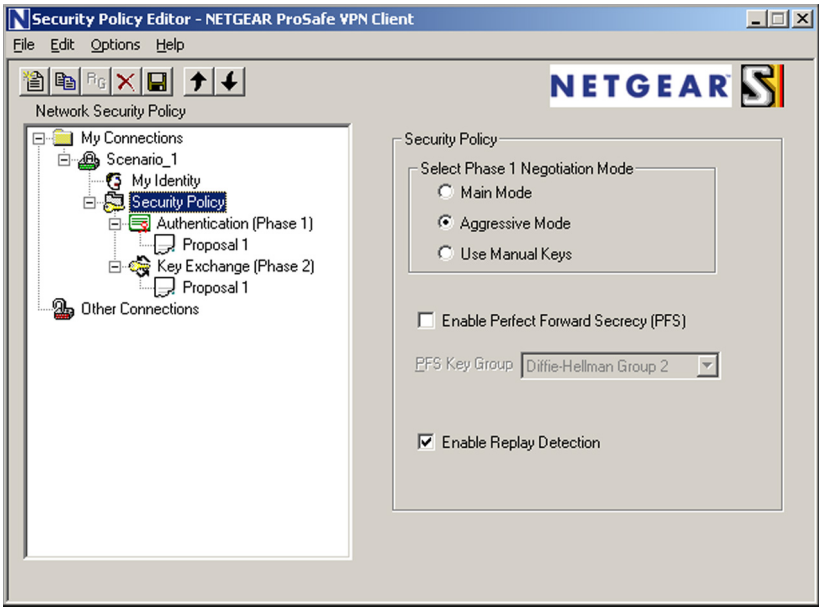


Figure B-24: Scenario_1 Security Policy screen parameters

e. Select My Identity on the left hierarchy menu and program the screen as follows (see Figure B-25):

- 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 B-20.)
- 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 B-21 for the gateway router.)

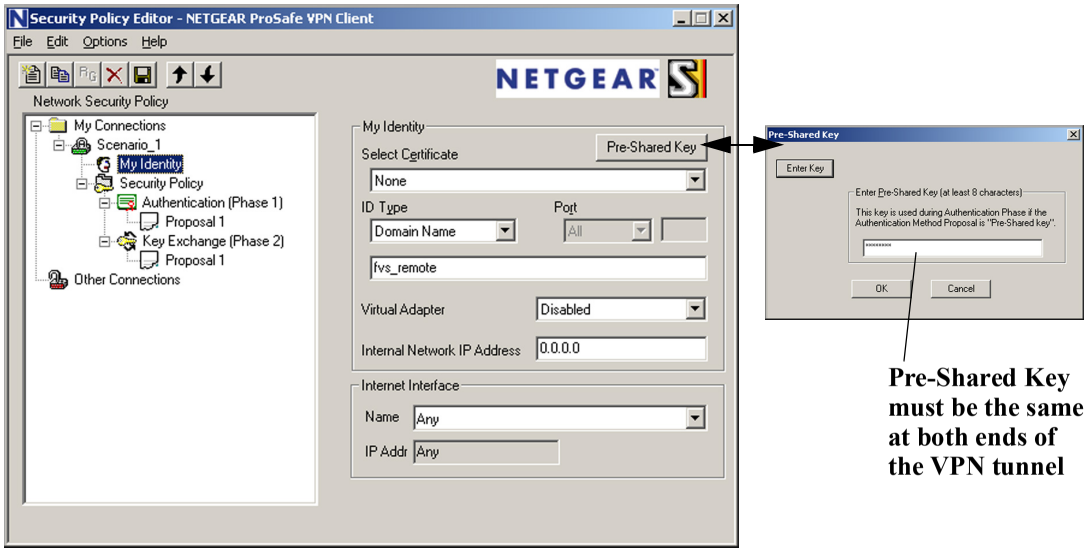


Figure B-25: Scenario_1 My Identity screen parameters

f. Verify the **Authentication (Phase 1)** and **Key Exchange (Phase 1) Proposal 1** screen parameters (see Figure B-26) match the **IKE SA Parameters** of the **IKE Policy Configuration** screen shown in Figure B-21 for the gateway router.

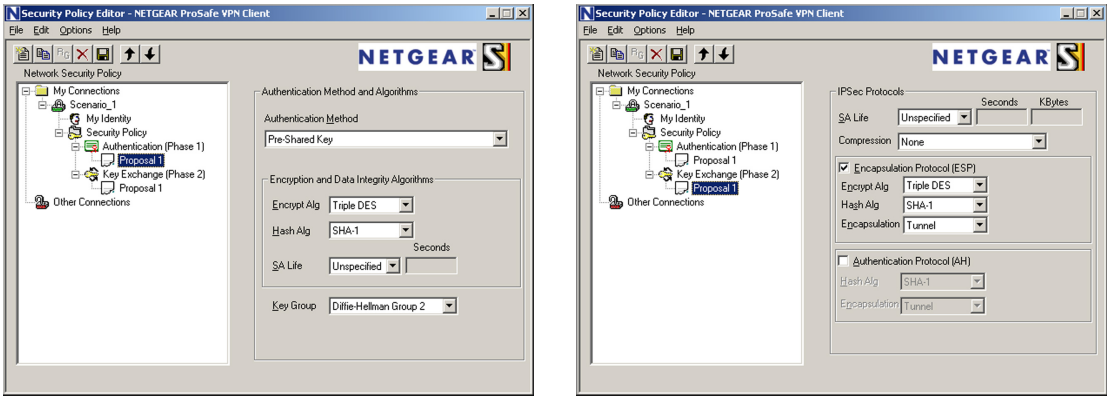


Figure B-26: Scenario_1 Proposal 1 parameters for Authentication and Key Exchange

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 36). 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 B-4. 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 B-27). 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 taskbar 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.

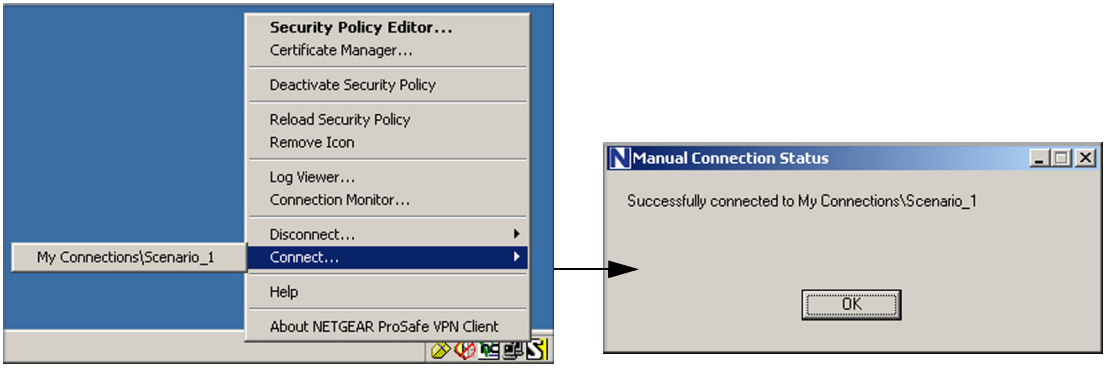


Figure B-27: Scenario_1 connection launch from VPN Client PC

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 taskbar 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**.

   See Figure B-28 for the resulting status screens.

VPN Status at Gateway A (FVS318v3)

IPSec SA

#	SPI	Policy Name	Endpoint	Protocol	Tx (KBytes)	HLifeTime	SLifeTime
1	4261259565	INScenario_1	14.15.16.17	ESP	0	28630	0
2	3619489328	Scenario_1	22.23.24.25	ESP	0	28630	28600

Status of VPN tunnel from Gateway B

Status of VPN tunnel to Gateway B

IKE SA

#	Policy Name	Endpoint	State	LifeTime in Secs
1	Scenario_1	22.23.24.25	SA_MATURE	0

Connection Monitor at Gateway B (remote VPN Client)

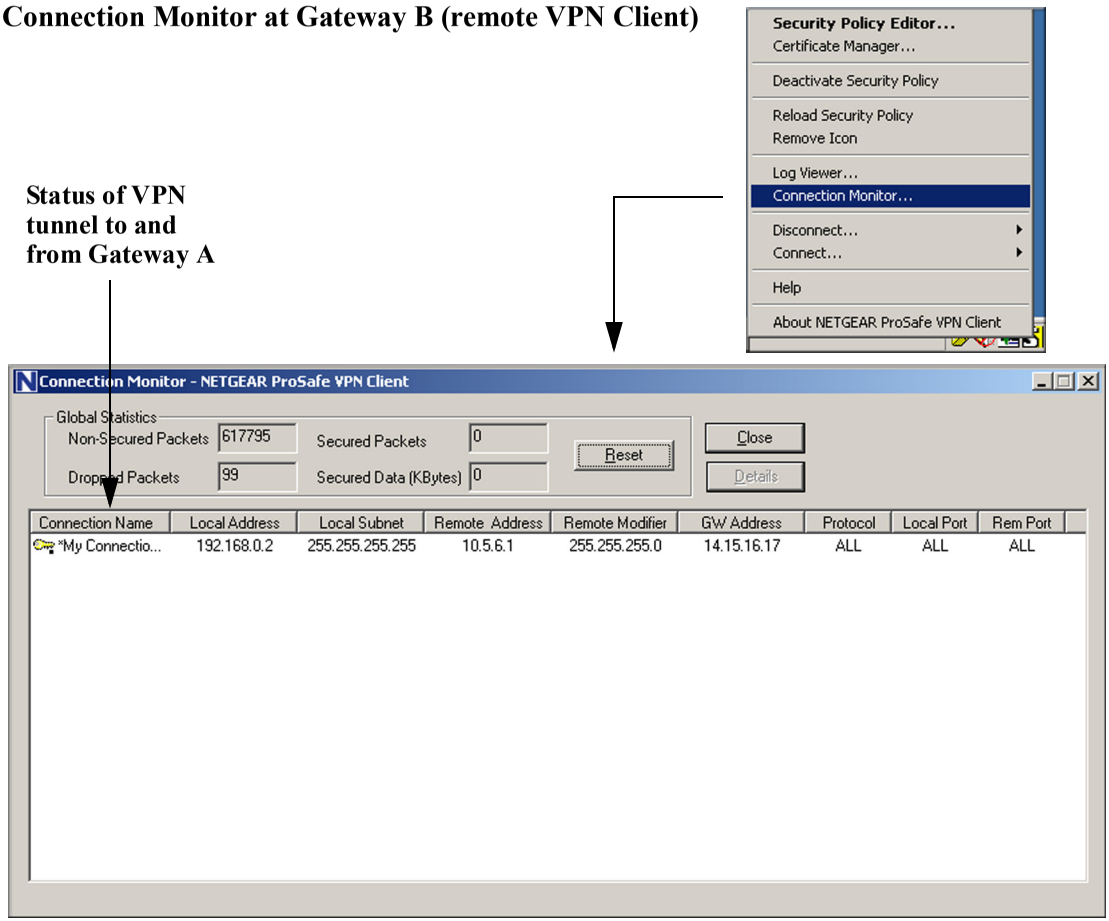


Figure B-28: VPN Status for Gateway A (FVS318v3) and Gateway B (VPN Client)