Reference Manual for the Model FVS318 Broadband ProSafe VPN Firewall

NETGEAR

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

M-10146-01
June 2003

Trademarks

NETGEAR and Auto Uplink are trademarks or registered trademarks 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 FVS318 Broadband ProSafe 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 dasFVS318 Broadband ProSafe VPN Firewall gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

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

Certificate of the Manufacturer/Importer

It is hereby certified that the FVS318 Broadband ProSafe VPN Firewall has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

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.

Technical Support

Refer to the Support Information Card that shipped with your FVS318 Broadband ProSafe VPN Firewall .

World Wide Web

NETGEAR maintains a World Wide Web home page that you can access at the universal resource locator (URL) *http://www.netgear.com*. A direct connection to the Internet and a Web browser such as Internet Explorer or Netscape are required.

Contents

Chapter 4
Protecting Your Network

Chapter 5
Advanced WAN and LAN Configuration

Chapter 8
Troubleshooting

Appendix A
Technical Specifications

Appendix B
Networks, Routing, and Firewall Basics

Appendix C
Preparing Your Network

Appendix D
Virtual Private Networking

Appendix E
NETGEAR VPN Configuration
of FVS318 or FVM318 to FVL328

Appendix F
NETGEAR VPN Configuration
FVS318 or FVM318 to Cisco IOS

Appendix G
NETGEAR VPN Configuration
FVS318 or FVM318 with FQDN to FVL328

Glossary

Index

Chapter 1
About This Manual

Congratulations on your purchase of the NETGEAR® FVS318 Broadband ProSafe VPN Firewall . The FVS318 VPN Firewall provides connection for multiple personal computers (PCs) to the Internet through an external broadband access device (such as a cable modem or DSL modem).

Audience

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 website.

Scope

This manual is written for the FVS318 VPN Firewall according to these specifications.:

Table 1-1. Manual Specifications

Product Version	FVS318 Broadband ProSafe VPN Firewall
Product Final Assembly Number	FA-FVS318-02
Firmware Version Number	1.4
Manual Part Number	M-10146-01
Manual Publication Date	June 2003

Note: Product updates are available on the NETGEAR web site at *www.netgear.com/support/main.asp*. Documentation updates are available on the NETGEAR, Inc. web site at *www.netgear.com/docs*.

Typographical Conventions

This guide uses the following typographical conventions:

Table 1. Typographical conventions

italics	Emphasis.
bold times roman	User input.
[Enter]	Named keys in text are shown enclosed in square brackets. The notation [Enter] is used for the Enter key and the Return key.
SMALL CAPS	DOS file and directory names.

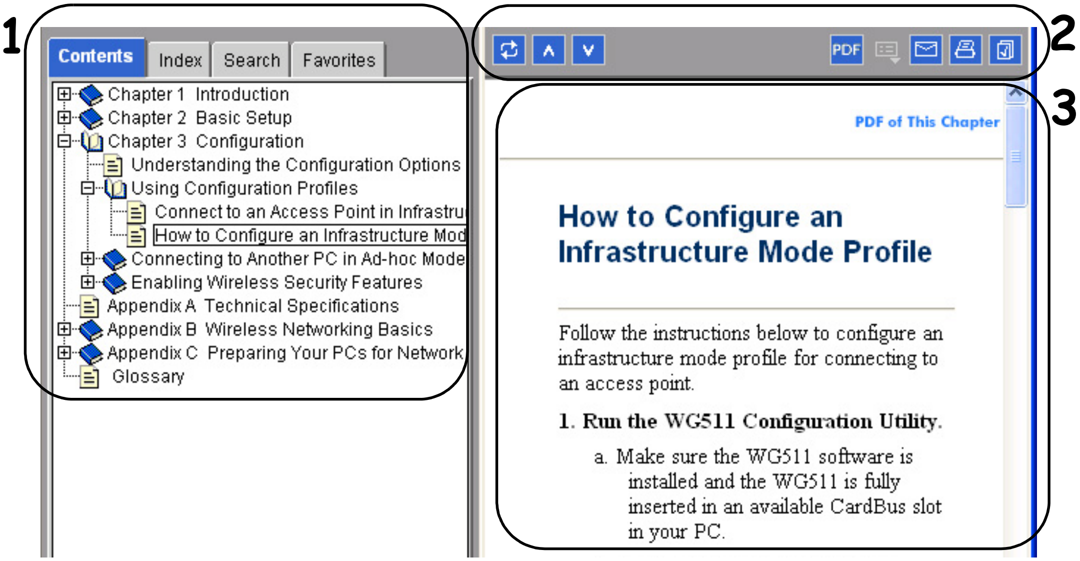
Special Message Formats

This guide uses the following formats to highlight special messages:

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

How to Use the HTML Version of this Manual

The HTML version of this manual includes these features.


1
2
3
Contents
Index
Search
Favorites
Chapter 1 Introduction
Chapter 2 Basic Setup
Chapter 3 Configuration
Understanding the Configuration Options
Using Configuration Profiles
Connect to an Access Point in Infrastru
How to Configure an Infrastructure Mod
Connecting to Another PC in Ad-hoc Mode
Enabling Wireless Security Features
Appendix A Technical Specifications
Appendix B Wireless Networking Basics
Appendix C Preparing Your PCs for Network
Glossary
PDF
PDF of This Chapter

How to Configure an Infrastructure Mode Profile

Follow the instructions below to configure an infrastructure mode profile for connecting to an access point.

1. Run the WG511 Configuration Utility.

a. Make sure the WG511 software is installed and the WG511 is fully inserted in an available CardBus slot in your PC.

Figure Preface -2: HTML version of this manual

1. **Left pane**. Use the left pane to view the Contents, Index, Search, and Favorites tabs.

   To view the HTML version of the manual, you must have a version 4 or later browser with Java or JavaScript enabled. To use the Favorites feature, your browser must be set to accept cookies. You can record a list of favorite pages in the manual for easy later retrieval.

2. **Toolbar buttons**. Use the toolbar buttons across the top to navigate, print pages, and more.

   – The *Show in Contents* button locates the currently displayed topic in the Contents tab.
   – *Previous/Next* buttons display the topic that precedes or follows the current topic.
   – The *PDF* button links to a PDF version of the full manual.
   – The *E-mail* button enables you to send feedback by e-mail to Netgear support.
   – The *Print* button prints the currently displayed topic. Using this button when a step-by-step procedure is displayed will send the entire procedure to your printer--you do not have to worry about specifying the correct range of pages.
   – The *Bookmark* button bookmarks the currently displayed page in your browser.

3. **Right pane**. Use the right pane to view the contents of the manual. Also, each page of the manual includes a “PDF of This Chapter” link at the top right which links to a PDF file containing just the currently selected chapter of the manual.

How to Print this Manual

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

- **A “How To ... ” Sequence of Steps in the HTML View**. Use the *Print* button on the upper right of the toolbar to print the currently displayed topic. Using this button when a step-by-step procedure is displayed will send the entire procedure to your printer--you do not have to worry about specifying the correct range of pages.
- **A Chapter**. Use the “PDF of This Chapter” link at the top right of any page.
  - Click “PDF of This Chapter” link at the top right of any page in the chapter you want to print. A new browser window opens showing the PDF version of the chapter you were viewing.
  - 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 an printer ink by selecting this feature.
- **The Full Manual**. Use the PDF button in the toolbar at the top right of the browser window.
  - Click PDF button. A new browser window opens showing the PDF version of the chapter you were viewing.
  - 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 an printer ink by selecting this feature.

Chapter 2
Introduction

This chapter describes the features of the NETGEAR FVS318 Broadband ProSafe VPN Firewall .

About the FVS318

The FVS318 is a complete security solution that protects your network from attacks and intrusions. Unlike simple Internet sharing routers that rely on Network Address Translation (NAT) for security, the FVS318 uses Stateful Packet Inspection for Denial of Service (DoS) attack protection and intrusion detection. The 8-port FVS318 provides highly reliable Internet access for up to 253 users.

Key Features

The FVS318 offers the following features.

- Trustworthy VPN Communications Over the Internet
- A Powerful, True Firewall
- Content Filtering
- Auto Uplink Ethernet Connection
- Extensive Protocol Support
- Easy Installation and Management
- Helpful Status Indicators

A description of these key features follows.

Virtual Private Networking (VPN)

The FVS318 VPN Firewall provides a secure encrypted connection between your local area network (LAN) and remote networks or clients. It includes the following VPN features:

- Supports 8 VPN connections.
- Supports industry standard VPN protocols
  The FVS318 VPN Firewall supports standard Manual or IKE keying methods, standard MD5 and SHA-1 authentication methods, and standard DES, 3DES, and AES encryption methods. It is compatible with many other VPN products.
- Supports up to 256 bit AES encryption for maximum security.

A Powerful, True Firewall

Unlike simple Internet sharing NAT routers, the FVS318 is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- Denial of Service (DoS) protection
  Automatically detects and thwarts Denial of Service (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 FVS318 will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the firewall to email the log to you at specified intervals. You can also configure the firewall to send immediate alert messages to your email address or email pager whenever a significant event occurs.

Content Filtering

With its content filtering feature, the FVS318 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.

Configurable Auto Uplink™ Ethernet Connection

With its internal 8-port 10/100 switch, the FVS318 can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. The 10/100 Mbps LAN and WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

The firewall incorporates Auto Uplink™ technology. Each LOCAL Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a 'normal' connection such as to a PC or an 'uplink' connection such as to a switch or hub. That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

Protocol Support

The FVS318 supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). Appendix B, "Networks, Routing, and Firewall Basics" provides further information on TCP/IP.

- IP Address Sharing by NAT
  The FVS318 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 Network Address Translation (NAT), allows the use of an inexpensive single-user ISP account.
- Automatic Configuration of Attached PCs by DHCP
  The FVS318 dynamically assigns network configuration information, including IP, gateway, and domain name server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of PCs on your local network.
- DNS Proxy
  When DHCP is enabled and no DNS addresses are specified, the firewall provides its own address as a DNS server to the attached PCs. The firewall obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.
- PPP over Ethernet (PPPoE)
  PPP over Ethernet is a protocol for connecting remote hosts to the Internet over a DSL connection by simulating a dial-up connection. This feature eliminates the need to run a login program such as EnterNet or WinPOET on your PC.
- PPTP login support for European ISPs, BigPond login for Telstra cable in Australia.
- Dynamic DNS
  Dynamic DNS services allow remote users to find your network using a domain name when your IP address is not permanently assigned. The firewall contains a client that can connect to many popular Dynamic DNS services to register your dynamic IP address.

Easy Installation and Management

You can install, configure, and operate the FVS318 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 firewall automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- Remote management
  The firewall allows you to login to the Web Management Interface from a remote location via 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.
- Diagnostic functions
  The firewall incorporates built-in diagnostic functions such as Ping, DNS lookup, and remote reboot. These functions allow you to test Internet connectivity and reboot the firewall. You can use these diagnostic functions directly from the FVS318 when your are connected on the LAN or when you are connected over the Internet via the remote management function.
- Visual monitoring
  The firewall’s front panel LEDs provide an easy way to monitor its status and activity.
- Flash EPROM for firmware upgrade
- Regional support, including ISPs like Telstra DSL and BigPond or Deutsche Telekom.

What’s in the Box?

The product package should contain the following items:

- FVS318 Broadband ProSafe VPN Firewall
- AC power adapter
- Category 5 (CAT5) Ethernet cable
- *Resource CD (SW-10021-01)*, including:
  - This manual
  - Application Notes, Tools, and other helpful information
- Warranty and registration card
- Support information 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 product for repair.

The Firewall’s Front Panel

The front panel of the FVS318 (Figure 2-1) contains status LEDs.

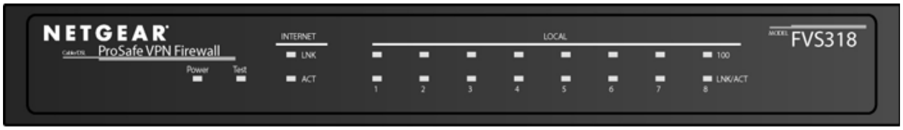


Figure 2-1: FVS318 Front Panel

You can use some of the LEDs to verify connections. Table 2-1 lists and describes each LED on the front panel of the firewall.

These LEDs are green when lit, except for the TEST LED, which is amber.

Table 2-1: LED Descriptions

Label	Activity	Description
POWER	On	Power is supplied to the firewall.
TEST	On Off	The system is initializing. The system is ready and running.
INTERNET and LOCAl		
100	On/Blinking	The port is operating at 100 Mbps.
LINK/ACT (Link/Activity)	On/Blinking	The port has detected a link with a connection and is operating at 10 Mbps. Blinking indicates data transmission.

The Firewall’s Rear Panel

The rear panel of the FVS318 (Figure 2-2) contains the connections identified below.

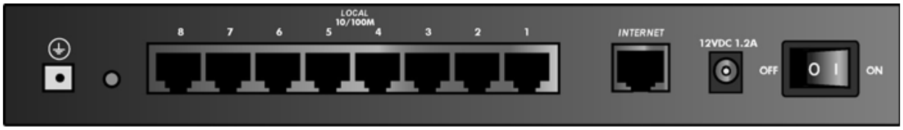


Figure 2-2: FVS318 Rear Panel

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

- Ground connector.
- Factory Default Reset push button.
- Eight Local Ethernet RJ-45 ports for connecting the firewall to the local computers.
- Internet WAN Ethernet RJ-45 port for connecting the firewall to a cable or DSL modem.
- AC power adapter input.
- Power switch.

Chapter 3
Connecting the Firewall to the Internet

This chapter describes how to set up the firewall on your Local Area Network (LAN), connect to the Internet, perform basic configuration of your FVS318 Broadband ProSafe VPN Firewall using the Setup Wizard, or how to manually configure your Internet connection.

What You Will Need Before You Begin

You need to prepare these three things before you can connect your firewall to the Internet:

1. A computer properly connected to the firewall as explained below.
2. Active Internet service such as that provided by a DSL or Cable modem account.
3. The Internet Service Provider (ISP) configuration information for your DSL or Cable modem account.

LAN Hardware Requirements

The FVS318 VPN Firewall connects to your LAN via twisted-pair Ethernet cables.

Computer Requirements

To use the FVS318 VPN Firewall on your network, each computer must have an installed Ethernet Network Interface Card (NIC) and an Ethernet cable. If the computer will connect to your network at 100 Mbps, you must use a Category 5 (CAT5) cable such as the one provided with your firewall.

Cable or DSL Modem Requirement

The cable modem or DSL modem must provide a standard 10 Mbps 10BASE-T or 100 Mbps 100BASE-T Ethernet interface.

LAN Configuration Requirements

For the initial connection to the Internet and configuration of your firewall, you will need to connect a computer to the firewall which is set to automatically get its TCP/IP configuration from the firewall via DHCP.

Note: Please refer to Appendix C, "Preparing Your Network" for assistance with DHCP configuration.

Internet Configuration Requirements

Depending on how your ISP set up your Internet account, you will need one or more of these configuration parameters to connect your firewall to the Internet:

- Host and Domain Names
- ISP Login Name and Password
- ISP Domain Name Server (DNS) Addresses
- Fixed or Static IP Address

Where Do I Get the Internet Configuration Parameters?

There are several ways you can gather the required Internet connection information.

- Your ISP should have provided you with all the information needed to connect to the Internet. If you cannot locate this information, you can ask your ISP to provide it or you can try one of the options below.
- If you have a computer already connected using the active Internet access account, you can gather the configuration information from that computer.
  - For Windows 95/98/ME, open the Network control panel, select the TCP/IP entry for the Ethernet adapter, and click Properties.
  - For Windows 2000/XP, open the Local Area Network Connection, select the TCP/IP entry for the Ethernet adapter, and click Properties.
  - For Macintosh computers, open the TCP/IP or Network control panel.
- You may also refer to the FVS318 *Resource CD (SW-10021-01)* for the NETGEAR Router ISP Guide which provides Internet connection information for many ISPs.

Once you locate your Internet configuration parameters, you may want to record them on the page below according to the instructions in “Worksheet for Recording Your Internet Connection Information” on page 3-3.

Worksheet for Recording Your Internet Connection Information

Print this page. Fill in the configuration parameters from your Internet Service Provider (ISP).

ISP Login Name: The login name and password are case sensitive and must be entered exactly as given by your ISP. Some ISPs use your full e-mail address as the login name. The Service Name is not required by all ISPs. If you connect using a login name and password, then fill in the following:

Login Name: ______________________________ Password: ____________________________

Service Name: _____________________________

Fixed or Static IP Address: If you have a static IP address, record the following information. For example, 169.254.141.148 could be a valid IP address.

Fixed or Static Internet IP Address: ______ . ______ . ______ . ______

Subnet Mask: ______ . ______ . ______ . ______

Gateway IP Address: ______ . ______ . ______ . ______

ISP DNS Server Addresses: If you were given DNS server addresses, fill in the following:

Primary DNS Server IP Address: ______ . ______ . ______ . ______

Secondary DNS Server IP Address: ______ . ______ . ______ . ______

Host and Domain Names: Some ISPs use a specific host or domain name like **CCA7324-A** or **home**. If you haven't been given host or domain names, you can use the following examples as a guide:

- If your main e-mail account with your ISP is **aaa@yyy.com**, then use **aaa** as your host name. Your ISP might call this your account, user, host, computer, or system name.
- If your ISP's mail server is **mail.xxx.yyy.com**, then use **xxx.yyy.com** as the domain name.

ISP Host Name: _________________________ ISP Domain Name: _______________________

How to Connect the FVS318 VPN Firewall

This section provides instructions for connecting the FVS318 Broadband ProSafe VPN Firewall to your Local Area Network (LAN).

Note: The Resource CD included with your firewall contains an animated Installation Assistant to help you through this procedure.

There are three steps to connecting your firewall:

1. Connect the firewall to your network
2. Log in to the firewall
3. Connect to the Internet

Follow the steps below to connect your firewall to your network. You can also refer to the Resource CD included with your firewall which contains an animated Installation Assistant to help you through this procedure.

1. **Connect the Firewall to Your LAN**
   a. Turn off your computer and Cable or DSL Modem.
   b. Disconnect the Ethernet cable (**A**) from your computer which connects to your Cable or DSL modem.

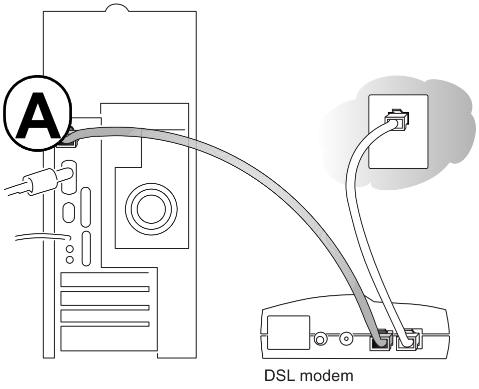


Figure 3-1: Disconnect the Cable or DSL Modem

c. Connect the Ethernet cable (**A)** from your Cable or DSL modem to the FVS318's Internet port.

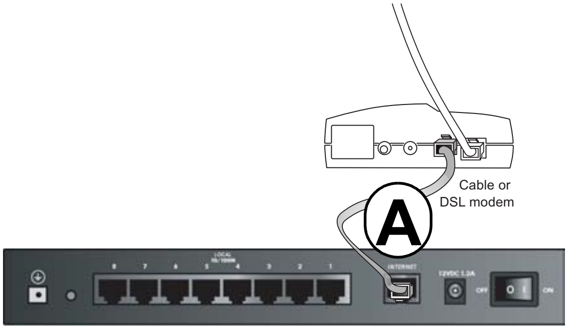


Figure 3-2: Connect the Cable or DSL Modem to the firewall

d. Connect the Ethernet cable (**B)** which came with the firewall from a Local port on the router to your computer.

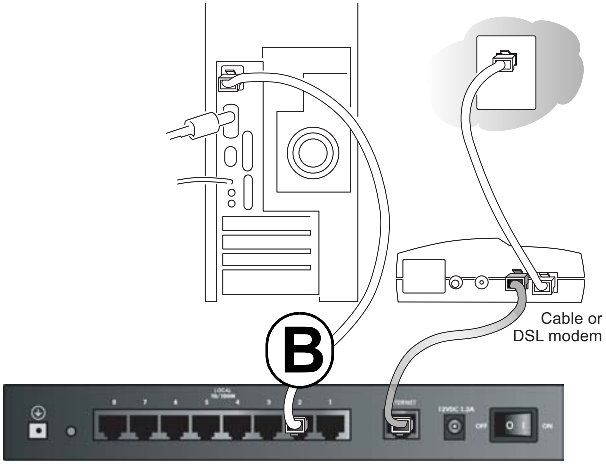


Figure 3-3: Connect the computers on your network to the firewall

Note: The FVS318 VPN Firewall incorporates Auto Uplink™ technology. Each LAN Ethernet port will automatically sense whether the cable plugged into the port should have a 'normal' connection (e.g. connecting to a PC) or an 'uplink' connection (e.g. connecting to a switch or hub). That port will then configure 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.

e. Turn on the Cable or DSL modem and wait about 30 seconds for the lights to stop blinking.

2. Log in to the Firewall

Note: To connect to the firewall, your computer needs to be configured to obtain an IP address automatically via DHCP. Please refer to Appendix C, "Preparing Your Network" for instructions on how to do this.

a. Turn on the firewall and wait for the Test light to stop blinking.

b. Now, turn on your computer.

Note: If you usually run software to log in to your Internet connection, do not run that software.

Now that the Cable or DSL Modem, firewall, and the computer are turned on, verify the following:

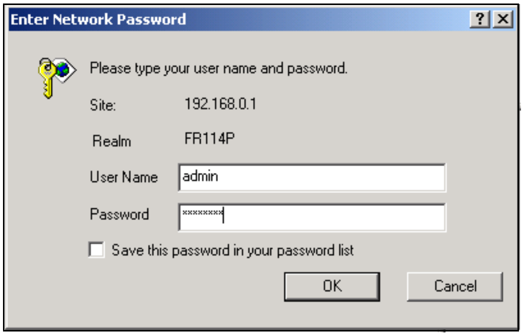
- When power on the firewall was first turned on, the PWR light went on, the TEST light turned on within a few seconds, and then went off after approximately 10 seconds.
- The firewall's LOCAL LINK/ACT lights are lit for any computers that are connected to it.
- The firewall's INTERNET LINK light is lit, indicating a link has been established to the cable or DSL modem.

c. Next, use a browser like Internet Explorer or Netscape to log in to the firewall at its default address of http://192.168.0.1.

http://192.168.0.1

Figure 3-4: Log in to the firewall

A login window opens as shown in Figure 3-5 below:



Enter Network Password

Please type your user name and password.

Site: 192.168.0.1

Realm FR114P

User Name admin

Password ********

□ Save this password in your password list

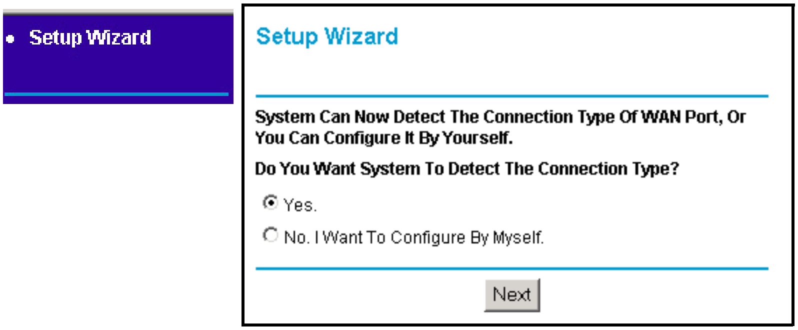
Figure 3-5: Login window

Note: If you were unable to connect to the firewall, please refer to "Basic Functions" on page 8-1.

d. 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.

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

3. Connect to the Internet



Setup Wizard

System Can Now Detect The Connection Type Of WAN Port, Or You Can Configure It By Yourself.

Do You Want System To Detect The Connection Type?

● Yes.

○ No. I Want To Configure By Myself.

Figure 3-6: Setup Wizard

a. You are now connected to the firewall. If you do not see the menu above, click the Setup Wizard link on the upper left of the main menu. Click the Yes button in the *Setup Wizard*.

b. Click Next and follow the steps in the Setup Wizard for inputting the configuration parameters from your ISP to connect to the Internet.

Note: If you choose not to use the Setup Wizard, you can manually configure your Internet connection settings by following the procedure "How to Manually Configure Your Internet Connection" on page 3-13.

Unless your ISP automatically assigns your configuration automatically via DHCP, you will need the configuration parameters from your ISP as you recorded them previously in "Worksheet for Recording Your Internet Connection Information" on page 3-3.

c. When the firewall successfully detects an active Ethernet connection with a broadband modem, the firewall's Internet LED goes on. The Setup Wizard reports which connection type it discovered, and displays the appropriate configuration menu. If the Setup Wizard finds no connection, you will be prompted to check the physical connection between your firewall and the cable or DSL line.

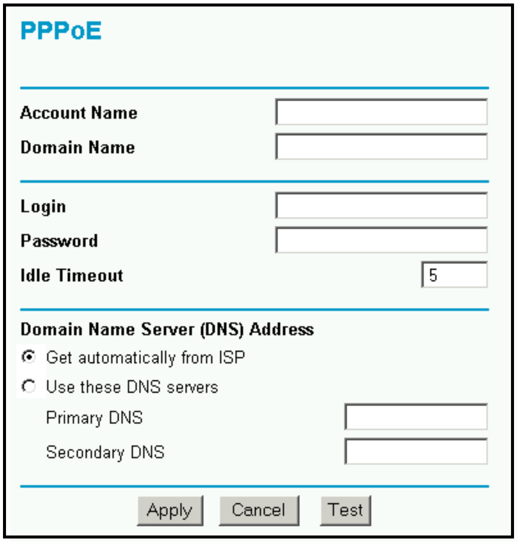
d. The Setup Wizard will report the type of connection it finds. The options are:

- Connections which require a login using PPPoE, DHCP, or Static (Fixed) IP connections. For PPTP or Telstra Bigpond Cable broadband, please refer to "How to Manually Configure Your Internet Connection" on page 3-13.
- Connections which use dynamic IP address assignment.
- Connections which use fixed IP address assignment.

The procedures for filling in the configuration menu for each type of connection follow below.

Wizard-Detected PPPoE Option

If the Setup Wizard determines that your Internet service account uses a login protocol such as PPP over Ethernet (PPPoE), you will be directed to a menu like the PPPoE menu in Figure 3-7:



PPPoE

Account Name	
Domain Name	
Login	
Password	
Idle Timeout	5

Domain Name Server (DNS) Address

● Get automatically from ISP

○ Use these DNS servers

Primary DNS	
Secondary DNS	

Figure 3-7: Setup Wizard menu for PPPoE login accounts

1. 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. If you leave the Domain Name field blank, the firewall will attempt to learn the domain automatically from the ISP. If this is not successful, you may need to enter it manually.
2. Enter the PPPoE login user name and password provided by your ISP. These fields are case sensitive. If you wish to change the login timeout, enter a new value in minutes. Entering zero will keep the router connected to the Internet indefinitely.

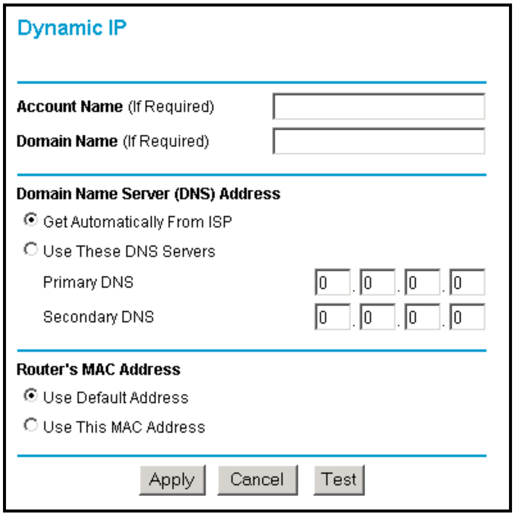
   Note: You will no longer need to launch the ISP's login program on your PC in order to access the Internet. When you start an Internet application, your firewall will automatically log you in.
3. Domain Name Server (DNS) Address: If you know that your ISP does not automatically transmit DNS addresses 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.

If you enter an address here, after you finish configuring the firewall, reboot your PCs so that the settings take effect.

4. Click on Apply to save your settings.
5. Click on the Test button to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to Chapter 8, Troubleshooting”.

Wizard-Detected Dynamic IP Option

If the Setup Wizard determines that your Internet service account uses Dynamic IP assignment, you will be directed to the menu shown in Figure 3-8 below:



Dynamic IP

Account Name (If Required)

Domain Name (If Required)

Domain Name Server (DNS) Address

● Get Automatically From ISP

○ Use These DNS Servers

Primary DNS 0 . 0 . 0 . 0

Secondary DNS 0 . 0 . 0 . 0

Router's MAC Address

● Use Default Address

○ Use This MAC Address

Figure 3-8: Setup Wizard menu for Dynamic IP address

1. 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. If you leave the Domain Name field blank, the firewall will attempt to learn the domain automatically from the ISP. If this is not successful, you may need to enter it manually.
2. 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.

A DNS server is a host on the Internet that translates Internet names (such as www.netgear.com) to numeric IP addresses. Typically your ISP transfers the IP address of one or two DNS servers to your firewall during login. If the ISP does not transfer an address, you must obtain it from the ISP and enter it manually here. If you enter an address here, you should reboot your PCs after configuring the firewall.

3. The Router's MAC Address is the Ethernet MAC address that will be used by the firewall on the Internet port.

   If your ISP allows access from only one specific computer's Ethernet MAC address, select "Use this MAC address." The firewall will then capture and use the MAC address of the computer that you are now using. You must be using the one computer that is allowed by the ISP. Otherwise, you can type in a MAC address.

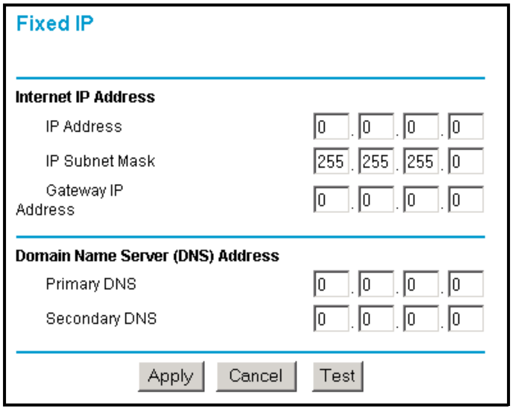
   Note: Some ISPs will register the Ethernet MAC address of the network interface card in your PC when your account is first opened. They will then only accept traffic from the MAC address of that PC. This feature allows your firewall to masquerade as that PC by using its MAC address.

4. Click on Apply to save your settings.

5. Click on the Test button to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to Chapter 8, Troubleshooting".

Wizard-Detected Fixed IP (Static) Option

If the Setup Wizard determines that your Internet service account uses Fixed IP assignment, you will be directed to the menu shown in Figure 3-9 below:



Fixed IP

Internet IP Address

IP Address 0 . 0 . 0 . 0

IP Subnet Mask 255 . 255 . 255 . 0

Gateway IP Address 0 . 0 . 0 . 0

Domain Name Server (DNS) Address

Primary DNS 0 . 0 . 0 . 0

Secondary DNS 0 . 0 . 0 . 0

Figure 3-9: Setup Wizard menu for Fixed IP address

1. Enter your assigned IP Address, Subnet Mask, and the IP Address of your ISP's gateway router. This information should have been provided to you by your ISP. You will need the configuration parameters from your ISP you recorded in "Worksheet for Recording Your Internet Connection Information" on page 3-3.
2. Enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

   A DNS servers are required to perform the function of translating an Internet name such as www.netgear.com to a numeric IP address. For a fixed IP address configuration, you must obtain DNS server addresses from your ISP and enter them manually here. You should reboot your PCs after configuring the firewall for these settings to take effect.
3. Click on Apply to save the settings.
4. Click on the Test button to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to Chapter 8, Troubleshooting.

Testing Your Internet Connection

After completing the Internet connection configuration, your can test your Internet connection. Log in to the firewall, then, from the Setup Basic Settings link, click on the Test button. If the NETGEAR website does not appear within one minute, refer to Chapter 8, Troubleshooting.

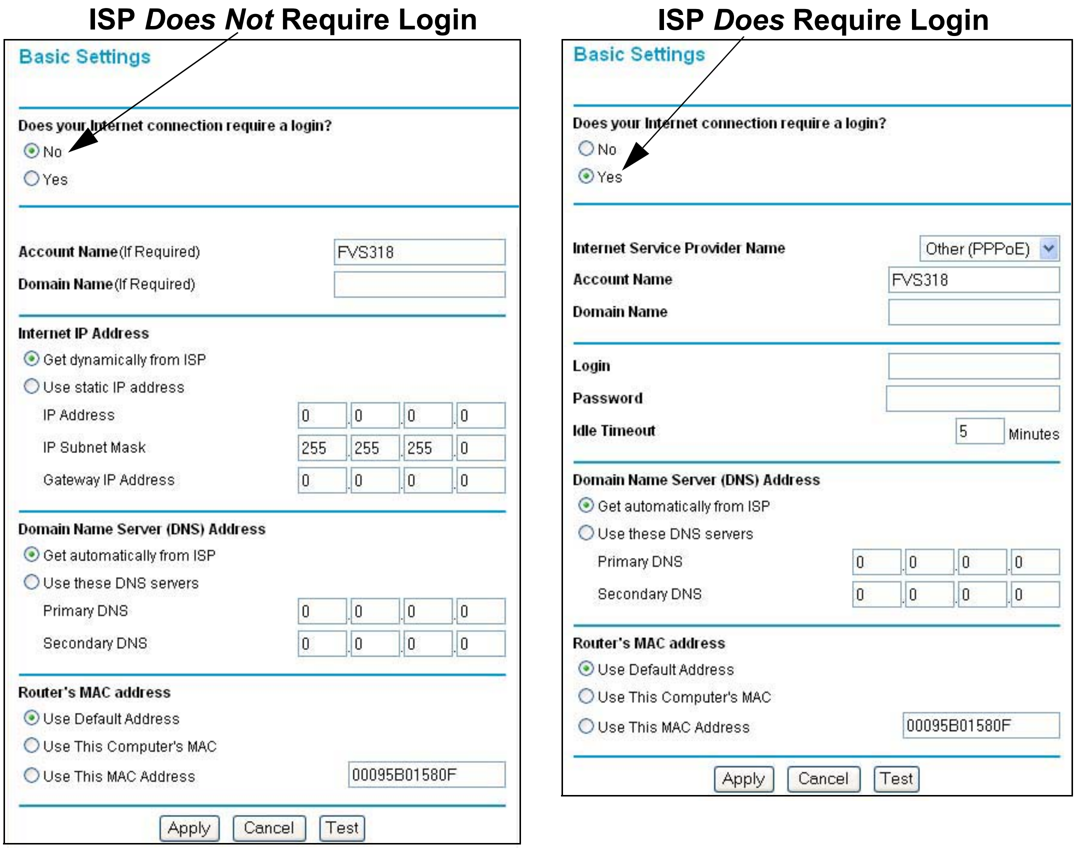
Your firewall is now configured to provide Internet access for your network. Your firewall automatically connects to the Internet when one of your computers requires access. It is not necessary to run a dialer or login application such as Dial-Up Networking or Enternet to connect, log in, or disconnect. These functions are performed by the firewall as needed.

To access the Internet from any computer connected to your firewall, launch a browser such as Microsoft Internet Explorer or Netscape Navigator. You should see the firewall's Internet LED blink, indicating communication to the ISP. The browser should begin to display a Web page.

The following chapters describe how to configure the Advanced features of your firewall, and how to troubleshoot problems that may occur.

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.



ISP *Does Not* Require Login

Basic Settings

Does your Internet connection require a login?
● No
○ Yes

Account Name (If Required)	FVS318
Domain Name (If Required)	

Internet IP Address
● Get dynamically from ISP
○ Use static IP address

IP Address	0	0	0	0
IP Subnet Mask	255	255	255	0
Gateway IP Address	0	0	0	0

Domain Name Server (DNS) Address
● Get automatically from ISP
○ Use these DNS servers

Primary DNS	0	0	0	0
Secondary DNS	0	0	0	0

Router's MAC address
● Use Default Address
○ Use This Computer's MAC
○ Use This MAC Address 00095B01580F

ISP *Does* Require Login

Basic Settings

Does your Internet connection require a login?
○ No
● Yes

Internet Service Provider Name	Other (PPPoE)
Account Name	FVS318
Domain Name	
Login	
Password	
Idle Timeout	5 Minutes

Domain Name Server (DNS) Address
● Get automatically from ISP
○ Use these DNS servers

Primary DNS	0	0	0	0
Secondary DNS	0	0	0	0

Router's MAC address
● Use Default Address
○ Use This Computer's MAC
○ Use This MAC Address 00095B01580F

Figure 3-10: Browser-based configuration Basic Settings menu

You can manually configure the firewall using the Basic Settings menu shown in Figure 3-10 using these steps:

1. Log in to the firewall at its default address of *http://192.168.0.1* using a browser like Internet Explorer or Netscape® Navigator.

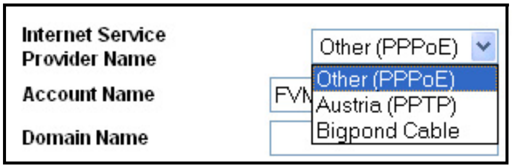
2. Click the Basic Settings link under the Setup section of the main menu.
3. If your Internet connection does not require a login, click No at the top of the Basic Settings menu and fill in the settings according to the instructions below. If your Internet connection does require a login, click Yes, and skip to step 4.
   a. 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 router 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. Gateway'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. Connections which require a login using protocols such as PPPoE, PPTP, Telstra Bigpond Cable broadband connections. Select your Internet service provider from the drop-down list.



Internet Service Provider Name: Other (PPPoE)

Account Name: FVM

Domain Name:

Figure 3-11: 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 3-7.

d. Click Apply to save your settings.

Chapter 4
Protecting Your Network

This chapter describes how to use the basic firewall features of the FVS318 Broadband ProSafe VPN Firewall to protect your network.

Protecting Access to Your FVS318 VPN Firewall

For security reasons, the firewall has its own user name and password. Also, after a period of inactivity for a set length of time, the administrator login will automatically disconnect. When prompted, enter **admin** for the firewall User Name and **password** for the firewall Password. You can use procedures below to change the firewall's password and the amount of time for the administrator's login timeout.

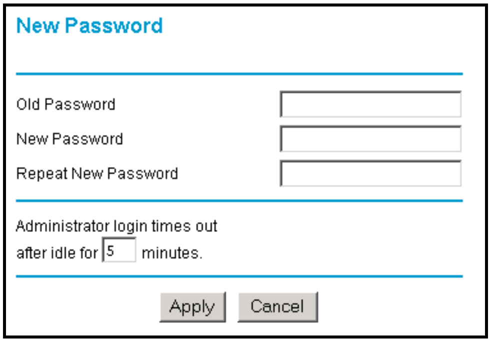
Note: The user name and password are not the same as any user name or password your may use to log in to your Internet connection.

NETGEAR recommends that you change this password to a more secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of both upper and lower case letters, numbers, and symbols. Your password can be up to 30 characters.

How to Change the Built-In Password

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 User Name, Password and LAN address you have chosen for the firewall.

2. From the Main Menu of the browser interface, under the Maintenance heading, select Set Password to bring up the menu shown in Figure 4-1.



New Password

Old Password

New Password

Repeat New Password

Administrator login times out after idle for 5 minutes.

Figure 4-1: Set Password menu

3. To change the password, first enter the old password, and then enter the new password twice.
4. Click Apply to save your changes.

Note: After changing the password, you will be required to log in again to continue the configuration. If you have backed up the firewall settings previously, you should do a new backup so that the saved settings file includes the new password.

How to Change the Administrator Login Timeout

For security, the administrator's login to the firewall configuration will timeout after a period of inactivity. To change the login timeout period:

1. In the Set Password menu, type a number in ‘Administrator login times out’ field.The suggested default value is 5 minutes.
2. Click Apply to save your changes or click Cancel to keep the current period.

Using Basic Firewall Services

Basic firewall services you can configure include access blocking and scheduling of firewall security. These topics are presented below.

The firewall provides a variety of options for blocking Internet based content and communications services. With its content filtering feature, the FVS318 VPN Firewall prevents objectionable content from reaching your PCs. The FVS318 allows you to control access to Internet content by screening for keywords within Web addresses. Key content filtering options include:

- Blocks access from your LAN to Internet locations that you specify as off-limits.
- ActiveX, Java, cookie, and web proxy filtering.
  - ActiveX and Java programs can be embedded in websites, and will be executed by your computer. These programs may sometimes include malicious content.
  - Cookies are small files that a website can store on your computer to track your activity. Some cookies can be helpful, but some may compromise your privacy.
  - Web proxies are computers on the Internet that act as relays for browsing. A web proxy can be used to bypass your web blocking methods.
- Keyword blocking of newsgroup names.
- Outbound Services Blocking limits access from your LAN to Internet locations or services that you specify as off-limits.
- Denial of Service (DoS) protection. Automatically detects and thwarts Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND Attack and IP Spoofing.
- Blocks unwanted traffic from the Internet to your LAN.

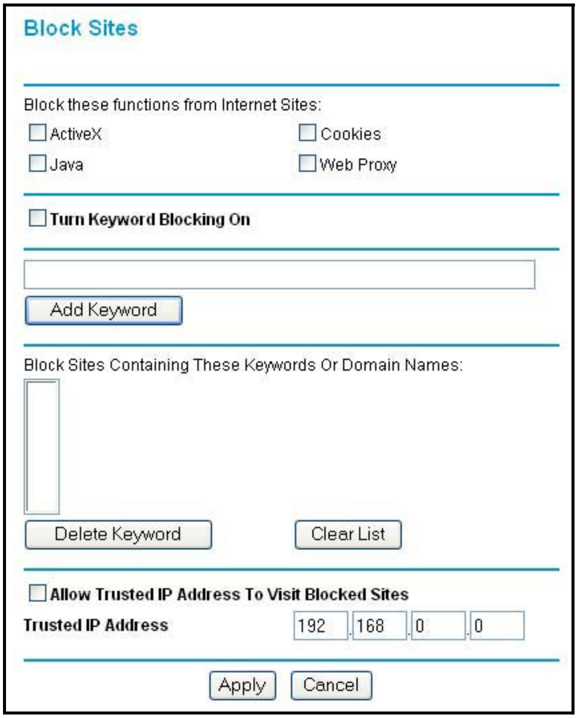
The section below explains how to configure your firewall to perform these functions.

How to Block Keywords and Sites

The FVS318 VPN Firewall allows you to restrict access to Internet content based on functions such as Java or Cookies, Web addresses and Web address keywords.

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 User Name, Password and LAN address you have chosen for the firewall.

2. Click on the Block Sites link of the Security menu.



Block Sites

Block these functions from Internet Sites:

□ ActiveX □ Cookies

□ Java □ Web Proxy

□ Turn Keyword Blocking On

Add Keyword

Block Sites Containing These Keywords Or Domain Names:

Delete Keyword Clear List

□ Allow Trusted IP Address To Visit Blocked Sites

Trusted IP Address 192 . 168 . 0 . 0

Apply Cancel

Figure 4-2: Block Sites menu

3. To block ActiveX, Java, Cookies, or Web Proxy functions for all Internet sites, click the check box next to the function and then click Apply. Be aware that blocking these functions can cause some web sites to not load or function properly.
4. To enable keyword blocking, check “Turn keyword blocking on”, enter a keyword or domain in the Keyword box, click Add Keyword, then click Apply. Each keyword can be up to 256 characters long.

   Some examples of Keyword application follow:

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

Up to 32 entries are supported in the Keyword list.

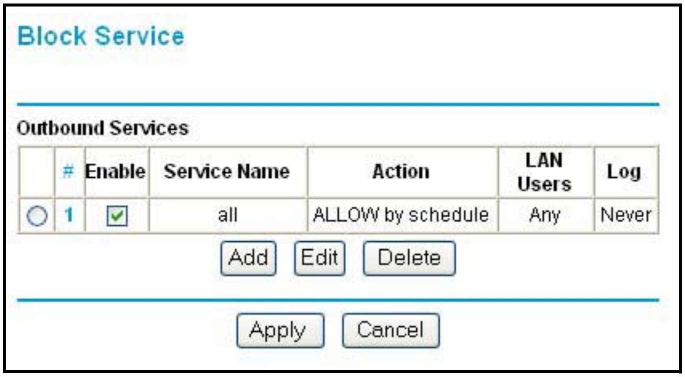
5. To delete a keyword or domain, select it from the list, click Delete Keyword, then click Apply.
6. To specify a Trusted User, enter that PC’s IP address in the Trusted User box and click Apply.

   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 IP address.
7. Click Apply to save your settings.

How to Block or Allow 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.

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 User Name, Password and LAN address you have chosen for the firewall.
2. Click on the Services link of the Security menu to display the Services menu shown in Figure 4-5:



Block Service

Outbound Services

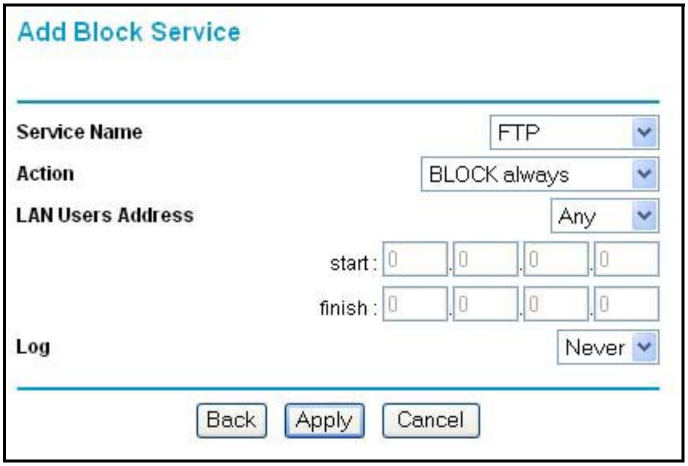
	#	Enable	Service Name	Action	LAN Users	Log
○	1	☑	all	ALLOW by schedule	Any	Never

Figure 4-3: Services menu

- To create a new entry, click the Add button.

- To edit an existing entry, select its button on the left side of the table and click Edit.
- To delete an existing entry, select its button on the left side of the table and click Delete.

3. Modify the menu shown below for defining or editing a service.



Add Block Service

Service Name: FTP

Action: BLOCK always

LAN Users Address: Any

start: 0 . 0 . 0 . 0

finish: 0 . 0 . 0 . 0

Log: Never

Figure 4-4: Add Services menu

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 Add 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. Allow always is the default and you can block always or choose to block or allow according to the schedule you have defined in the Schedule menu.

- LAN Users Address.

  Specify traffic originating on the LAN (outbound), 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.

- Log.

You can select whether the traffic will be logged. The choices are:

- Never - no log entries will be made for this service.
- Always - any traffic for this service type will be logged.
- Match - traffic of this type which matches the parameters and action will be logged.
- Not match - traffic of this type which does not match the parameters and action will be logged.

4. Click Apply to save your changes.

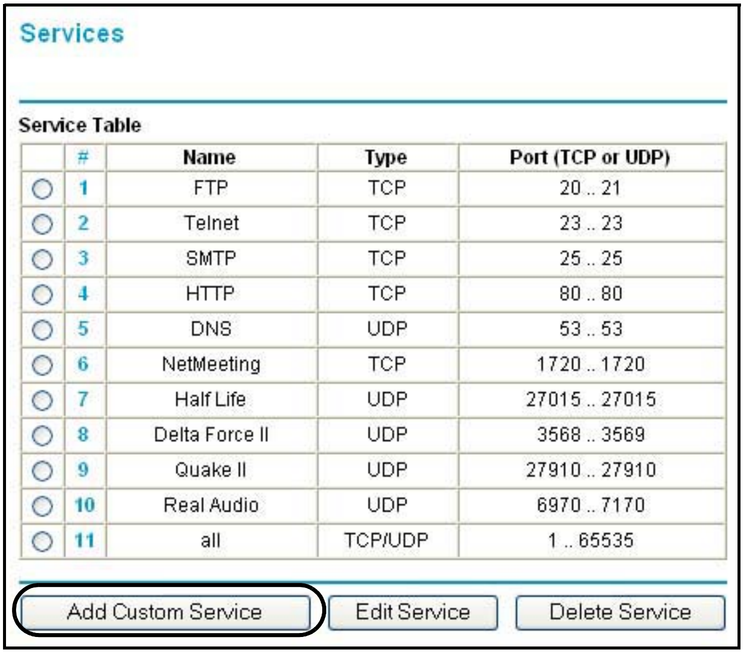
How to Add to the List of Services

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 FVS318 already holds a list of many service port numbers, you are not limited to these choices. Use the procedure below to create your own service definitions.

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 User Name, Password and LAN address you have chosen for the firewall.

2. Click on the Add Service link of the Security menu to display the Services list shown in Figure 4-5:



Services

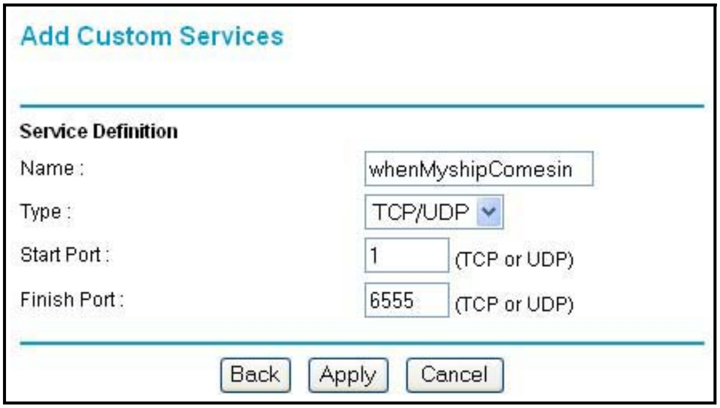
Service Table

	#	Name	Type	Port (TCP or UDP)
○	1	FTP	TCP	20 .. 21
○	2	Telnet	TCP	23 .. 23
○	3	SMTP	TCP	25 .. 25
○	4	HTTP	TCP	80 .. 80
○	5	DNS	UDP	53 .. 53
○	6	NetMeeting	TCP	1720 .. 1720
○	7	Half Life	UDP	27015 .. 27015
○	8	Delta Force II	UDP	3568 .. 3569
○	9	Quake II	UDP	27910 .. 27910
○	10	Real Audio	UDP	6970 .. 7170
○	11	all	TCP/UDP	1 .. 65535

Figure 4-5: Services table

- To create a new entry, click the Add Custom Service button.
- To edit an existing entry, select its button on the left side of the table and click Edit.
- To delete an existing entry, select its button on the left side of the table and click Delete.

3. Modify the menu shown below for defining or editing a service.



Add Custom Services

Service Definition

Name :	whenMyshipComesin
Type :	TCP/UDP
Start Port :	1 (TCP or UDP)
Finish Port :	6555 (TCP or UDP)

Figure 4-6: Add Services menu

The parameters are:

- Name.

  This name will appear in the drop-down list services to be allowed or blocked in the Add Block Service menu as seen in Figure 4-4 above.

- Type.

  Choose the type of traffic to be handled: TCP/UDP; TCP; or UDP.

- Start Port.

  Specify the starting port number here. If you select a single port, enter it in both the start and Finish boxes.

- Finish Port.

  Specify the ending port number here. If you select a single port, enter it in both the start and Finish boxes.

4. Click Apply to save your changes.

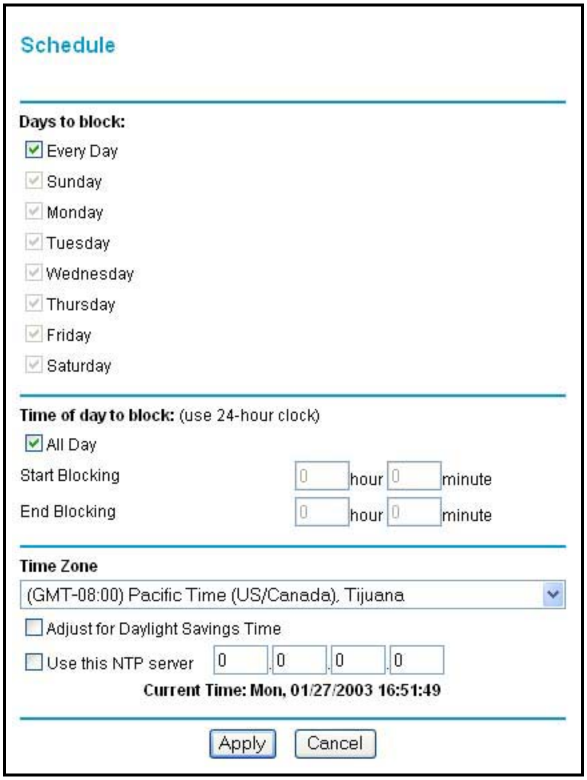
Setting Times and Scheduling Firewall Services

The FVS318 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 select your Time Zone from the list.

How to Set Your Time Zone

In order to localize the time for your log entries, you must specify your Time Zone:

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 User Name, Password and LAN address you have chosen for the firewall.
2. Click on the Schedule link of the Security menu to display menu shown below.



Schedule

Days to block:

☑ Every Day
☑ Sunday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday

Time of day to block: (use 24-hour clock)

☑ All Day

Start Blocking 0 hour 0 minute

End Blocking 0 hour 0 minute

Time Zone

(GMT-08:00) Pacific Time (US/Canada), Tijuana

□ Adjust for Daylight Savings Time

□ Use this NTP server 0 . 0 . 0 . 0

Current Time: Mon, 01/27/2003 16:51:49

Figure 4-7: Schedule Services menu

3. Select your Time Zone. This setting will be used for the blocking schedule according to your local time zone and for time-stamping log entries. Check the Daylight Savings Time box if your time zone is currently in daylight savings time.

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

4. The firewall has a list of publicly available NTP servers. If you would prefer to use a particular NTP server as the primary server, enter its IP address under Use this NTP Server.
5. Click Apply to save your settings.

How to Schedule Firewall Services

If you enabled services blocking in the Block Services menu or Port forwarding in the Ports menu, you can set up a schedule for when blocking occurs or when access isn't restricted.

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 User Name, Password and LAN address you have chosen for the firewall.
2. Click on the Schedule link of the Security menu to display menu shown above in the Schedule Services menu.
3. To block Internet services 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, to limit access during certain times for the selected days, enter Start Blocking and End Blocking times.

   Note: Enter the values as 24-hour time. For example, 10:30 am would be 10 hours and 30 minutes and 10:30 pm would be 22 hours and 30 minutes.

4. Click Apply to save your changes.

Chapter 5
Advanced WAN and LAN Configuration

This chapter describes how to configure the advanced features of your FVS318 Broadband ProSafe VPN Firewall .

Configuring Advanced WAN Settings

The FVS318 Broadband ProSafe VPN Firewall provides a variety of advanced features, such as:

- Setting up a Demilitarized Zone (DMZ) Server.
- Port forwarding for enabling networked gaming and various Internet services.
- Universal Plug and Play (UPnP) support to make accessing various games and services over easier.
- The flexibility of configuring your LAN TCP/IP settings.

These features are discussed below.

Setting Up A 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:** 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.

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 that you have configured in the Ports menu. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the Default DMZ Server.

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.

Enabling Access to Local Servers Through a FVS318

Although the Firewall causes your entire local network to appear as a single machine to the Internet, you can make local servers for different services (for example, FTP or HTTP) visible and available to the Internet. This is done using the Ports menu.

When a remote computer on the Internet wants to access a service at your IP address, the requested service is identified by a port number in the incoming IP packets. For example, a packet that is sent to the external IP address of your Firewall and destined for port number 80 is an HTTP (Web server) request. Many service port numbers are already defined in a Services list in the Ports menu, although you are not limited to these choices. See IETF RFC1700, "Assigned Numbers," for port numbers for common protocols. Use the Ports menu to configure the Firewall to forward incoming traffic to IP addresses on your local network based on the port number.

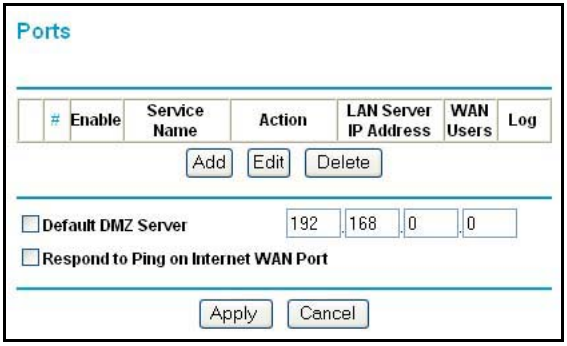
➡ **Note:** Some residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to the Acceptable Use Policy of your ISP.

Remember that port forwarding opens holes in your firewall. Only enable those ports that are necessary for your network.

How to Configure Port Forwarding to Local Servers

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 User Name, Password and LAN address you have chosen for the Firewall.

2. From the Main Menu of the browser interface, under Advanced, click on Ports to view the port forwarding menu, shown in Figure 5-1



Ports

	#	Enable	Service Name	Action	LAN Server IP Address	WAN Users	Log

□ Default DMZ Server 192.168.0.0

□ Respond to Ping on Internet WAN Port

Figure 5-1: Port Forwarding Menu

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.

How to Support Internet Services, Applications, or Games

Before starting, you'll need to determine which type of service, application or game you'll provide and the IP address of the computer that will provide each service. Be sure the computer’s IP address never changes. If the computers on your local network are assigned their IP addresses by the Firewall (by DHCP), use the Reserved IP address feature in the LAN IP menu to keep the computer’s IP address constant.

To set up a computer or server to be accessible to the Internet for an Internet service:

1. Click **Add** to bring up the Add Port menu.
2. From the Services list, select the Internet service, application or game you want to host. If the service, application or game does not appear in the Services list, define it using the Add Service menu as described on “How to Block or Allow Services“ on page 4-5.
3. Type the IP address of the computer in the Server IP Address box.
4. Click **Apply**.

Note: You may forward more than one type of service to a single computer or server.

How to Clear a Port Assignment

To edit or eliminate a port assignment entry:

1. Click the button next to that port in the table.
2. Click Delete or Edit.
3. Click Apply.

Local Web and FTP Server Example

If a local PC with a private IP address of 192.168.0.33 acts as a Web and FTP server, configure the Ports menu to forward HTTP (port 80) and FTP (port 21) to local address 192.168.0.33

In order for a remote user to access this server from the Internet, the remote user must know the IP address that has been assigned by your ISP. If this address is 172.16.1.23, for example, an Internet user can access your Web server by directing the browser to http://172.16.1.23. The assigned IP address can be found in the Maintenance Status Menu, where it is shown as the WAN IP Address.

Some considerations for this application are:

- If your account's IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires. In this case, you can also consider using a dynamic DNS service provider which enables your FVS318 to use a Fully Qualified Domain Name as its Internet address. Dynamic DNS services allow remote users to find your network using a domain name when your IP address is not permanently assigned.
- If the IP address of the local 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.
- Local PCs must access the local server using the PCs' local LAN address (192.168.0.33 in this example). Attempts by local PCs to access the server using the external IP address (172.16.1.23 in this example) will fail.

How to Set Up Computers for Half Life, KALI or Quake III

To set up an additional computer to play Half Life, KALI or Quake III:

1. Click **Add** to add a new Port entry to the table.
2. Select the game again from the Services list.

3. Change the beginning port number in the Start Port box.
   For these games, use the supplied number in the default listing and add +1 for each additional computer. For example, if you've already configured one computer to play Hexen II (using port 26900), the second computer's port number would be 26901, and the third computer would be 26902.
4. Type the same port number in the End Port box that you typed in the Start Port box.
5. Type the IP address of the additional computer in the Server IP Address box.
6. Click Apply.

Working with LAN IP Settings

The LAN IP Setup menu allows configuration of LAN IP services such as UPnP, DHCP and RIP. These features can be found under the Advanced heading in the Main Menu of the browser interface.

What Does UPnP Support Do for Me?

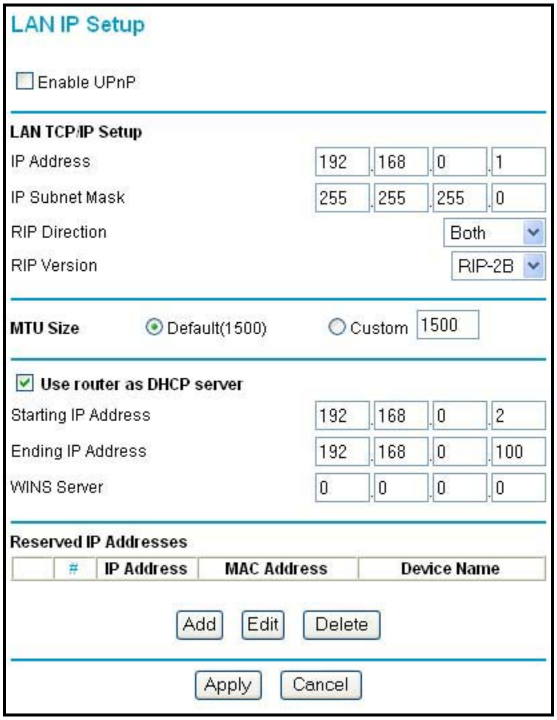
With the FVS318 Broadband ProSafe VPN Firewall , you can enable Microsoft UPnP for Network Address Translation (NAT) traversal. The scenarios that UPnP-enabled NAT traversal helps ensure include: multi-player gaming, peer-to-peer connections, real time communications, and remote assistance

NAT is a standard used to allow multiple computers or devices on a private network using private address ranges such as 10.0.x.x, 192.168.x.x, 172.x.x.x to share a single IP address. NAT is used in gateway devices such as FVS318 VPN Firewall that form the boundary between the public Internet and the private LAN. As IP packets from the private LAN traverse the gateway, NAT translates a private IP address and port number to a public IP address and port number, tracking those translations to keep individual sessions intact.

NAT can interfere with many of the new PC and home networking experiences, such as multi-player games, real time communications, and other peer-to-peer services, that people increasingly want to use in their homes or small businesses. These applications will not work if they a use private address on the public Internet or require simultaneous use of the same port number. Applications must use a public address, and, for each session, a unique port number. UPnP NAT Traversal can automatically solve many of the problems that NAT imposes on applications.

How to Enable UPnP

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 User Name, Password and LAN address you have chosen for the Firewall.
2. Click the LAN IP Setup link from the Advanced section of the main menu to display the menu shown in Figure 5-3



LAN IP Setup

☐ Enable UPnP

LAN TCP/IP Setup

IP Address	192 . 168 . 0 . 1
IP Subnet Mask	255 . 255 . 255 . 0
RIP Direction	Both
RIP Version	RIP-2B

MTU Size ● Default(1500) ○ Custom 1500

☑ **Use router as DHCP server**

Starting IP Address	192 . 168 . 0 . 2
Ending IP Address	192 . 168 . 0 . 100
WINS Server	0 . 0 . 0 . 0

Reserved IP Addresses

	#	IP Address	MAC Address	Device Name

Figure 5-2: Enabling UPnP via the LAN IP Setup Menu

3. Click the Enable UPnP check box.
4. Click Apply to save your changes.

Understanding 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 TCP/IP Setup 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 router.
- RIP Direction
  RIP (Router Information Protocol) allows a router to exchange routing information with other routers. 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 will broadcast its routing table periodically.
  — When set to Both or In Only, it will incorporate the RIP information that it receives.
  — When set to None, it will not send any RIP packets and will ignore any RIP packets received.
- RIP Version
  This controls the format and the broadcasting method of the RIP packets that the router 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. Both RIP-2B and RIP-2M send the routing data in RIP-2 format. RIP-2B uses subnet broadcasting. RIP-2M uses multicasting.

➡	**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.

Setting the MTU Size

The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs, particularly some using PPPoE, your router will need to automatically reduce the MTU. If the resulting setting is not suitable, you may need to reduce the MTU manually. This is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

Any packets sent through the Firewall that are larger than the configured MTU size will be repackaged into smaller packets to meet the MTU requirement. To change the MTU size:

1. Under MTU Size, select Custom.
2. Enter a new size between 64 and 1500.
3. Click Apply to save the new configuration.

Using the Router as a DHCP Server

By default, the Firewall will function 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 router'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.

Specify the pool of IP addresses to be assigned by setting the Starting IP Address and Ending IP Address. These addresses should be part of the same IP address subnet as the Firewall's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.0.2 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 is 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
- WINS Server, short for *Windows Internet Naming Service,* determines the IP address associated with a particular Windows computer. A WINS server records and reports a list of names and IP address of Windows PCs on its local network. If you connect to a remote network that contains a WINS server, enter the server's IP address here. This allows your PCs to browse the network using the Network Neighborhood feature of Windows.

How to Specify Reserved IP Addresses

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 access 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 router'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.

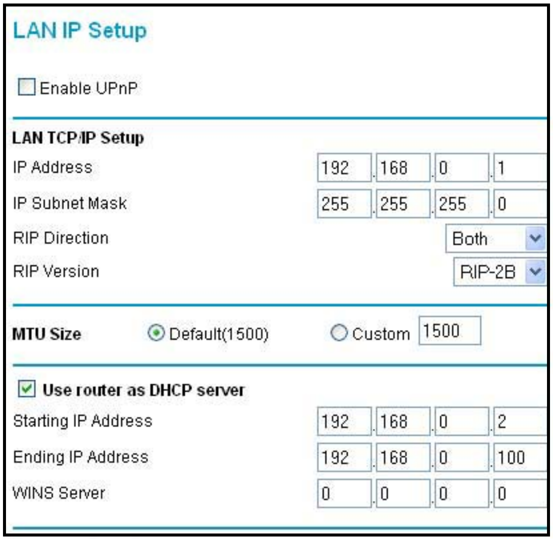
   Note: Reboot the PC to force a DHCP release and renew. Reserved addresses will not be assigned until the next time the PC contacts the router's DHCP server.

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.

How to Configure LAN TCP/IP Settings

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 User Name, Password and LAN address you have chosen for the Firewall.
2. From the Main Menu, under Advanced, click the LAN IP Setup link to view the menu, shown in Figure 5-3



LAN IP Setup

□ Enable UPnP

LAN TCP/IP Setup

IP Address	192 . 168 . 0 . 1
IP Subnet Mask	255 . 255 . 255 . 0
RIP Direction	Both
RIP Version	RIP-2B

MTU Size ● Default(1500) ○ Custom 1500

☑ **Use router as DHCP server**

Starting IP Address	192 . 168 . 0 . 2
Ending IP Address	192 . 168 . 0 . 100
WINS Server	0 . 0 . 0 . 0

Figure 5-3: LAN IP Setup Menu

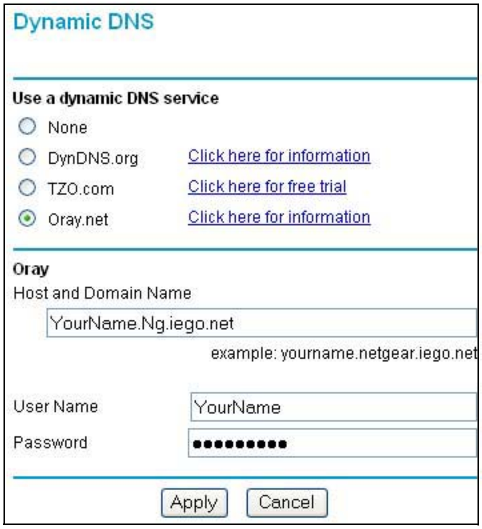
3. Enter the TCP/IP, MTU, or DHCP parameters.
4. Click Apply to save your changes.

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, who will allow you to register your domain to their IP address, and will forward traffic directed at 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 User Name, 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.



Dynamic DNS

Use a dynamic DNS service

○ None
○ DynDNS.org Click here for information
○ TZO.com Click here for free trial
● Oray.net Click here for information

Oray

Host and Domain Name: YourName.Ng.iego.net
example: yourname.netgear.iego.net

User Name: YourName
Password: ••••••••••

Figure 5-4: Dynamic DNS Setup Menu

3. Access the website of one of the dynamic DNS service providers whose names appear in the ‘Use a dynamic DNS service’ list, and register for an account.
   For example, for oray.net, click the link or go to www.oray.net.
4. Select the Use a dynamic DNS service radio button for the service you are using.
5. Type the FQDN that your dynamic DNS service provider gave you.
   If the URL the dynamic DNS service provider gave you is YourName.Ng.iego.net then this is your FQDN.
6. Type the User Name for your dynamic DNS account.
7. Type the Password (or key) for your dynamic DNS account.
8. Click Apply to save your configuration.

Note: The router supports only basic DDNS and the login and password may not be secure. 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 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 routers or multiple IP subnets located on your network.

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 router on your home network for connecting to the company where you are employed. This router’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.

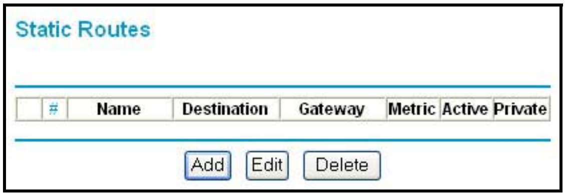
In this case you must define a static route, telling your Firewall that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100. The static route would look like Figure 5-6.

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 router at 192.168.0.100.
- A Metric value of 1 will work since the ISDN router is on the LAN.
- Private is selected only as a precautionary security measure in case RIP is activated.

How to Configure Static Routes

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 User Name, Password and LAN address you have chosen for the Firewall.
2. From the Main Menu of the browser interface, under Advanced, click on Static Routes to view the Static Routes menu, shown in Figure 5-5.



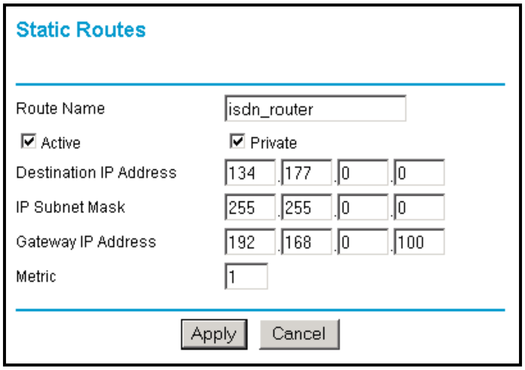
Static Routes

	#	Name	Destination	Gateway	Metric	Active	Private

Figure 5-5: Static Routes Table

3. To add or edit a Static Route:

a. Click the **Edit** button to open the Edit Menu, shown in Figure 5-6.



Static Routes

Route Name: isdn_router

☑ Active ☑ Private

Destination IP Address: 134 . 177 . 0 . 0

IP Subnet Mask: 255 . 255 . 0 . 0

Gateway IP Address: 192 . 168 . 0 . 100

Metric: 1

Figure 5-6: Static Route Entry and Edit Menu

b. Type a route name for this static route in the Route Name box under the table. This is for identification purpose only.

c. Select **Active** to make this route effective.

d. Select **Private** if you want to limit access to the LAN only. The static route will not be reported in RIP.

e. Type the Destination IP Address of the final destination.

f. Type the IP Subnet Mask for this destination. If the destination is a single host, type 255.255.255.255.

g. Type the Gateway IP Address, which must be a router on the same LAN segment as the Firewall.

h. Type a number between 1 and 15 as the Metric value. This represents the number of routers 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.

4. Click **Apply** to have the static route entered into the table.

Chapter 6
Virtual Private Networking

This chapter describes how to use the virtual private networking (VPN) features of the FVS318 VPN Firewall. VPN communications paths are called tunnels. VPN tunnels provide secure, encrypted communications between your local network and a remote network or computer.

Overview of VPN Configuration

Two common scenarios for configuring VPN tunnels are between two or more networks, and between a remote computer and a network.

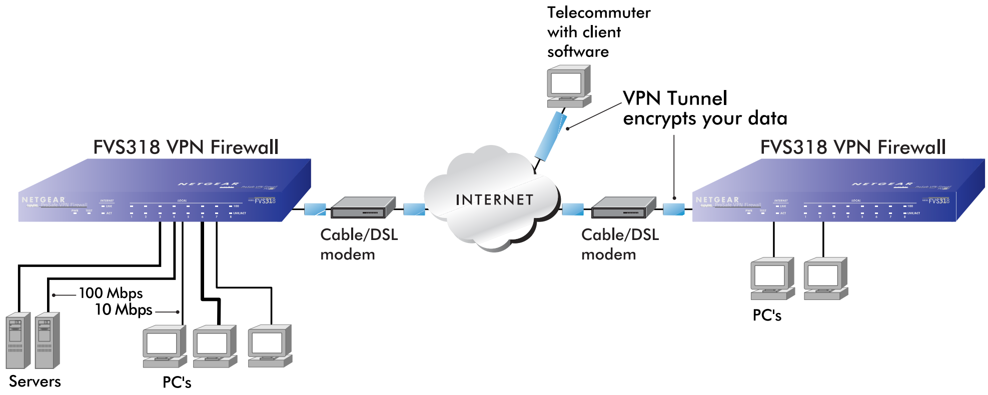


Figure 6-1: Secure access through FVS318 VPN routers

The FVS318 supports these configurations:

- Secure access between networks, such as a branch or home office and a main office.

  A VPN between two or more NETGEAR VPN-enabled routers is a good way to connect branch or home offices and business partners over the Internet. VPN tunnels also enable access to network resources when NAT is enabled and remote computers have been assigned private IP addresses.

- Secure access from a remote PC, such as a telecommuter connecting to an office network.

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 VPN client software. The FVS318 VPN Firewall router on your network is the other tunnel endpoint

- The FVS318 VPN Firewall supports up to eight concurrent tunnels.

These scenarios are described below.

> **Note:** The FVS318 VPN Firewall uses industry standard VPN protocols. However, due to variations in how manufacturers interpret these standards, many VPN products do not interoperate. NETGEAR provides support for connections between NETGEAR VPN Firewalls, and between an FVS318 VPN Firewall and the SafeNet SoftRemote VPN Client for Windows. This manual is written based on tests with the FVS318 and versions 8 and 9 of the SafeNet client. Although the FVS318 can interoperate with many other VPN products, it is not possible for NETGEAR to provide specific technical support for every other interconnection. Please see NETGEAR's web site for additional VPN information.

Understanding How FVS318 VPN Tunnels Are Configured

You create VPN tunnels definitions via the VPN Settings link under the Setup section of the main menu on the FVS318. The VPN tunnel configuration consists of these two kinds of information:

- **Connection.** Identifies the VPN endpoints by IPSec ID, IP address, or a fully qualified domain name (FQDN).

  Note: A FQDN is the complete URL of the router. Using a dynamic DNS service for a FVS318 with a dynamically-assigned IP address enables that FVS318 to both initiate and respond to requests to open a VPN tunnel. Otherwise, a FVS318 with a dynamically-assigned IP address can only initiate a request to open a VPN tunnel because no other initiators can know its IP address.

- **Security Association (SA).** There are three kinds of SA key exchange modes:
  - **IKE Main Mode**: Uses the Internet Key Exchange (IKE) protocol to define the authentication scheme and automatically generate the encryption keys. Main Mode authentication is slightly slower than Aggressive Mode but more secure.
  - **IKE Aggressive Mode**: Uses the IKE protocol to define the authentication scheme and automatically generate the encryption keys. Aggressive Mode authentication is slightly faster than Main Mode but less secure.

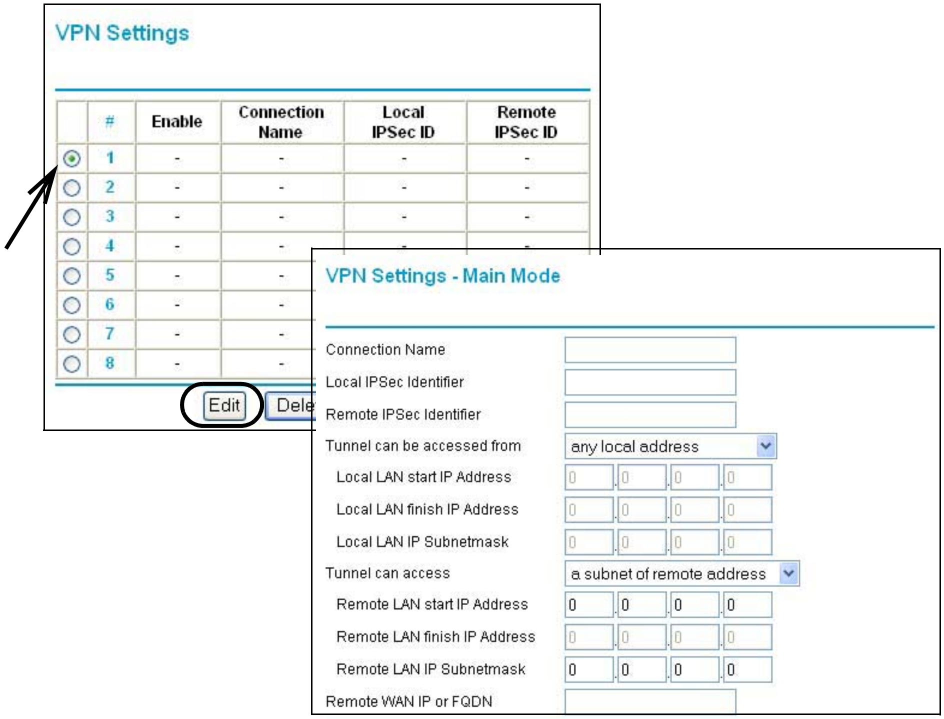
— **Manual Keys**: Does not use IKE. Rather, you manually enter all the authentication and key parameters. You have more control over the process however the process is much more complex and there are more opportunities for errors or configuration mismatches between you FVS318 and the corresponding VPN endpoint gateway or client workstation.

You need to configure matching VPN settings on both VPN endpoints. The outbound VPN settings on one end must match to the inbound VPN settings on other end, and vice versa.

Configuring VPN Network Connection Parameters

All VPN tunnels on the FVS318 VPN Firewall require configuring the same network parameters. This section describes those parameters and how to access them.

Click the VPN Settings link of the Setup section of the main menu, click the radio button of a VPN tunnel on the VPN Settings menu, and then click the Edit button to display the default Main Mode menu shown in Figure 6-2. The kinds of network connection information you provide are the same for the Main Mode, Aggressive Mode, and Manual Keys options.



VPN Settings

	#	Enable	Connection Name	Local IPSec ID	Remote IPSec ID
●	1	-	-	-	-
○	2	-	-	-	-
○	3	-	-	-	-
○	4	-	-	-	-
○	5	-	-		
○	6	-	-		
○	7	-	-		
○	8	-	-		

VPN Settings - Main Mode

Connection Name	
Local IPSec Identifier	
Remote IPSec Identifier	
Tunnel can be accessed from	any local address
Local LAN start IP Address	0 . 0 . 0 . 0
Local LAN finish IP Address	0 . 0 . 0 . 0
Local LAN IP Subnetmask	0 . 0 . 0 . 0
Tunnel can access	a subnet of remote address
Remote LAN start IP Address	0 . 0 . 0 . 0
Remote LAN finish IP Address	0 . 0 . 0 . 0
Remote LAN IP Subnetmask	0 . 0 . 0 . 0
Remote WAN IP or FQDN	

Figure 6-2: FVS318 VPN tunnel network connection configuration menu

The FVS318 VPN tunnel network connection fields are defined in the following table.

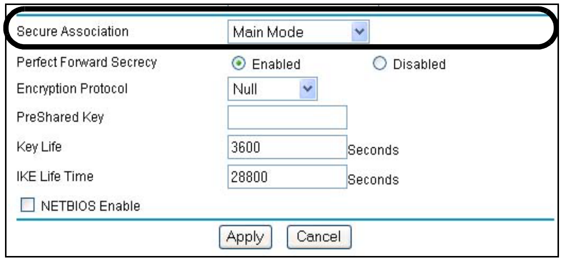
Table 6-1. VPN network connection configuration fields

Field	Description
Connection Name	The descriptive name of the VPN tunnel. Each tunnel should have a unique name. It is only used to help you identify VPN tunnels.
Local IPSec identifier	Enter a Local IPSec Identifier name for this endpoint. This name must be entered in the other VPN endpoint as the Remote IPSec Identifier.
Remote IPSec identifier	Enter a Remote IPSec Identifier name for the remote endpoint. This name must be entered in the other VPN endpoint as the Local IPSec Identifier.
Tunnel can be accessed from ...	Use this field to manage what IP addresses in your LAN can use this VPN tunnel. You can choose one of the following four options: 1. Any local address. This selection will enable any device on your LAN to communicate with the designated devices on the remote LAN communications through this tunnel. 2. A subnet of local addresses. Enter the Local LAN start IP address and subnet mask. For a discussion of calculating IP addresses based on a subnet mask, refer to "Netmask" on page B-4. 3. A range of local addresses, such as members of a department on your LAN. Enter the start and finish Local IP addresses. 4. A single local address, such as a single PC.
Tunnel can access ...	Use this field to manage what IP addresses in the remote connection can use this VPN tunnel. You can choose one of the following four options: 1. A subnet of remote addresses. Enter a subnet for the remote LAN. For a discussion of calculating IP addresses based on a subnet mask, refer to "Netmask" on page B-4. 2. A range of remote addresses, such as members of a department. Enter the start and finish Local IP addresses. 3. A single remote address, such as a single PC. • If the PC is connected directly to the Internet, enter the PC's public IP address. • If the PC is connected to the Internet through a NAT router, select "A subnet of remote addresses" and enter the remote PC's LAN IP address in the Remote LAN start IP Address field, along with a Remote LAN IP Subnet Mask of 255.255.255.255. Then enter the NAT router's public (WAN) IP address or FQDN in the Remote WAN IP or FQDN field below. 4. The Remote WAN IP or FQDN. Enables traffic to the target remote VPN endpoint PC or VPN gateway identified by a WAN IP address or a FQDN. Enter the remote WAN IP address or FQDN.
Remote WAN IP or FQDN	Enter the remote WAN IP address or FQDN.

Configuring a SA Using IKE Main Mode

The most common configuration scenarios will use IKE to manage the authentication and encryption keys. The IKE protocol performs negotiations between the two VPN endpoints to automatically generate required parameters. The IKE Main Mode settings are introduced below. The IKE Aggressive Mode settings are introduced in the section after this one.

Click the VPN Settings link of the Setup section of the main menu, click the radio button of a VPN tunnel, and then click the Edit button display the Main Mode menu shown in Figure 6-3.



Secure Association	Main Mode	
Perfect Forward Secrecy	● Enabled	○ Disabled
Encryption Protocol	Null	
PreShared Key		
Key Life	3600 Seconds	
IKE Life Time	28800 Seconds	
□ NETBIOS Enable		

Figure 6-3: IKE - VPN Settings Main Mode Configuration Menu

The Security Association IKE Main Mode configuration fields are defined in the following table.

Table 6-1. Security Association Main Mode Configuration Fields

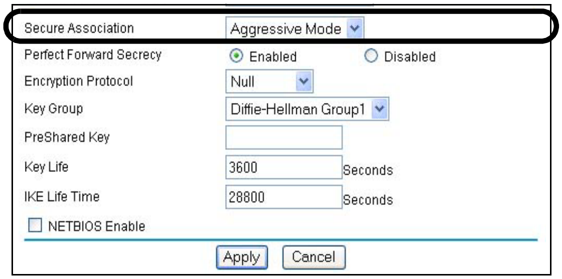
Field	Description
Secure Association	Choose Main Mode key exchange mode for this VPN tunnel: • **IKE Main Mode -- the default.** • IKE Aggressive Mode -- faster but less secure. • Manual Keys -- more control but more complex.
Perfect Forward Secrecy	Perfect Forward Secrecy provides additional security by means of a shared secret value. If one key is compromised, previous and subsequent keys are secure because they are not derived from previous keys.
Encryption Protocol	The level of encryption. Longer keys are more secure but throughput may slow. • Null - Fastest but no security. • DES - 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 or AES. • 3DES - (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys. • AES - 128, - 192, or - 256. Advanced Encryption Standard. Most secure.

Table 6-1. Security Association Main Mode Configuration Fields

Field	Description
Pre-Shared Key	Specify the key. Any value is acceptable, provided the remote VPN endpoint has the same value in its Pre-Shared Key field.
Key Life	The default is 3600 seconds (one hour).
IKE Life Time	At the end of this time, the connection will drop, the security association will be re-established, and the connection will be reactivated. The default is 28800 seconds (eight hours).
NETBIOS Enable	If you need to run Microsoft networking functions such as Network Neighborhood, click the NETBIOS Enable check box to allow NETBIOS traffic over the VPN tunnel.

Configuring a SA Using IKE Aggressive Mode

Click the VPN Settings link of the Setup section of the main menu, and then click the radio button of a VPN tunnel, and then click the Edit button and choose Aggressive Mode from the Security Association drop-down list to display the Aggressive Mode menu shown in Figure 6-4.



Secure Association: Aggressive Mode
Perfect Forward Secrecy: ● Enabled ○ Disabled
Encryption Protocol: Null
Key Group: Diffie-Hellman Group1
PreShared Key:
Key Life: 3600 Seconds
IKE Life Time: 28800 Seconds
□ NETBIOS Enable

Figure 6-4: IKE - VPN Settings Aggressive Mode Configuration Menu

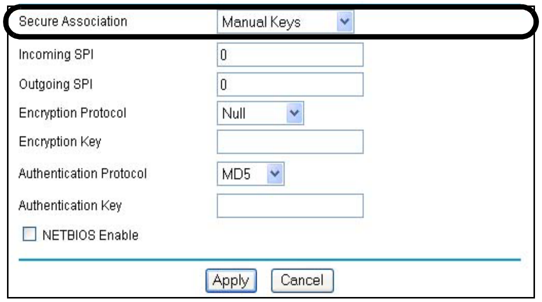
The Security Association IKE Aggressive Mode fields are defined in the following table.

Table 6-1. Security Association Aggressive Mode Configuration Fields

Field	Description
Secure Association	Choose Aggressive Mode key exchange mode for this VPN tunnel: • IKE Main Mode -- the default. • **IKE Aggressive Mode -- faster but less secure.** • Manual Keys -- more control but more complex.
Perfect Forward Secrecy	Perfect Forward Secrecy (PFS) provides additional security by means of a shared secret value. With PFS, if one key is compromised, previous and subsequent keys are secure because they are not derived from previous keys.
Encryption Protocol	Longer keys are more secure but the throughput could be slower. • Null - Fastest but no security. • DES - 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 or AES. • 3DES - (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys. • AES - 128, - 192, or - 256. Most secure. Advanced Encryption Standard is a symmetric 128-bit block data encryption technique.
Key Group	This setting determines the Diffie-Hellman group bit size used in the key exchange. This must match the value used on the remote gateway.
Pre-Shared Key	Specify the key. Any value is acceptable, provided the remote VPN endpoint has the same value in its Pre-Shared Key field.
Key Life	The default is 3600 seconds (one hour).
IKE Life Time	At the end of this time, the connection will drop, the security association will be re-established, and the connection will be reactivated. The default is 28800 seconds (eight hours).
NETBIOS Enable	If you need to run Microsoft networking functions such as Network Neighborhood, click the NETBIOS Enable check box.

Configuring a SA Using Manual Key Management

Click the VPN Settings link of the Setup section of the main menu, and then click the radio button of a VPN tunnel, and then click the Edit button and choose Aggressive Mode from the Security Association drop-down list to display the Manual Keys menu shown in Figure 6-5.



Secure Association: Manual Keys
Incoming SPI: 0
Outgoing SPI: 0
Encryption Protocol: Null
Encryption Key:
Authentication Protocol: MD5
Authentication Key:
□ NETBIOS Enable

Figure 6-5: IKE - VPN Settings Manual Key Configuration Menu

The Manual Keys configuration fields are defined in the following table.

Table 6-1.   VPN Manual Keys Configuration Fields

Field	Description
Secure Association	Choose Manual Keys key exchange mode for this VPN tunnel: • IKE Main Mode -- the default. • IKE Aggressive Mode -- faster but less secure. **• Manual Keys -- more control but more complex.**
Incoming SPI	Incoming Security Parameter Index. Enter a Hex value (3 - 8 chars). This string should not be used in any other SA. Any value is acceptable, provided the remote VPN endpoint has the same value in its “Outgoing SPI” field.
Outgoing SPI	Outgoing Security Parameter Index. Enter a Hex value (3 - 8 chars). This string should not be used in any other SA. Any value is acceptable, provided the remote VPN endpoint has the same value in its “Incoming SPI” field.
Encryption Protocol	The level of encryption will you use. Longer keys are more secure but the throughput could be slower. • Null - Fastest but no security. • DES - 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 or AES. • 3DES - (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys. • AES - 128, - 192, or - 256. Most secure. Advanced Encryption Standard, a symmetric 128-bit block data encryption technique. It is an iterated block cipher with a variable block length and a variable key length.
Key Group	This setting determines the Diffie-Hellman group bit size used in the key exchange. This must match the value used on the remote gateway.
Pre-Shared Key	Specify the key. Any value is acceptable, provided the remote VPN endpoint has the same value in its Pre-Shared Key field.

Table 6-1. VPN Manual Keys Configuration Fields

Field	Description
Authentication Protocol	Use this drop-down list to select the authentication protocol: • MD5 - the default • SHA1 - more secure
Authentication Key	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 Protocol Key field.
Key Life	The default is 3600 seconds (one hour).
IKE Life Time	At the end of this time, the connection will drop, the security association will be re-established, and the connection will be reactivated. The default is 28800 seconds (eight hours).
NETBIOS Enable	If you need to run Microsoft networking functions such as Network Neighborhood, click the NETBIOS Enable check box.

Planning a VPN

When you set up a VPN, it is helpful to plan the network configuration and record the configuration parameters on a worksheet. These topics are discussed below.

Note: NETGEAR will publish additional interoperability scenarios with various gateway and client software products. Look on the NETGEAR web site at www.netgear.com/docs/ for the HTML version of this manual.

When you set up a VPN, it is helpful to plan the network configuration and record the configuration parameters on a worksheet. These topics are discussed below and a blank worksheets are provided at the end of this chapter on page 6-31.

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 points. 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?
- At least one side must have a fixed IP address or you must be using a dynamic DNS service for FQDN configurations. Otherwise, if one side has a dynamic IP address, the side with a dynamic IP address must always be the initiator of the connection.
- Will you use the typical automated Internet Key Exchange (IKE) setup, or a Manual Keying setup in which you must specify each phase of the connection?
- For the WAN connection, what level of IPSec VPN encryption will you use?
  - DES - 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 or AES.
  - 3DES - (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.
  - AES - 128, - 192, or - 256. Most secure. Advanced Encryption Standard, a symmetric 128-bit block data encryption technique. The the key length can be specified to 128, 192 or 256 bits.The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES works at multiple network layers simultaneously.

How to Configure a Network to Network VPN Tunnel

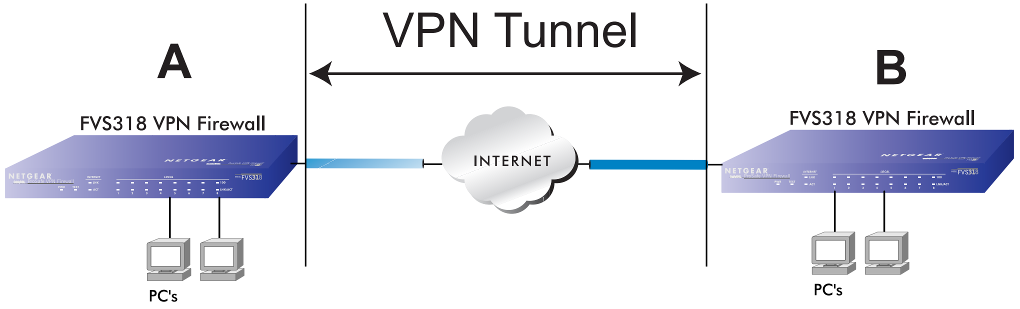


Figure 6-6: LAN to LAN VPN access through an FVS318 to an FVS318

Follow this procedure to configure a VPN tunnel between two FVS318 VPN Firewalls. The worksheet below shows the settings for this example. A blank worksheet is provided at page 6-31.

Table 6-1. Sample Network to Network IKE VPN Tunnel Configuration Worksheet

IKE Security Association Settings	
Connection Name:	**VPNAB**
Pre-Shared Key:	**r>T(h4&3@#kB**
Secure Association -- Main Mode or Aggressive Mode:	**Main**
Perfect Forward Secrecy:	**Enabled**
Encryption Protocol -- Null, DES, 3DES, or AES -128, -192, or -256:	**DES**
Key Life in seconds:	**3600 (1 hour)**
IKE Life Time in seconds:	**28800 (8 hours)**

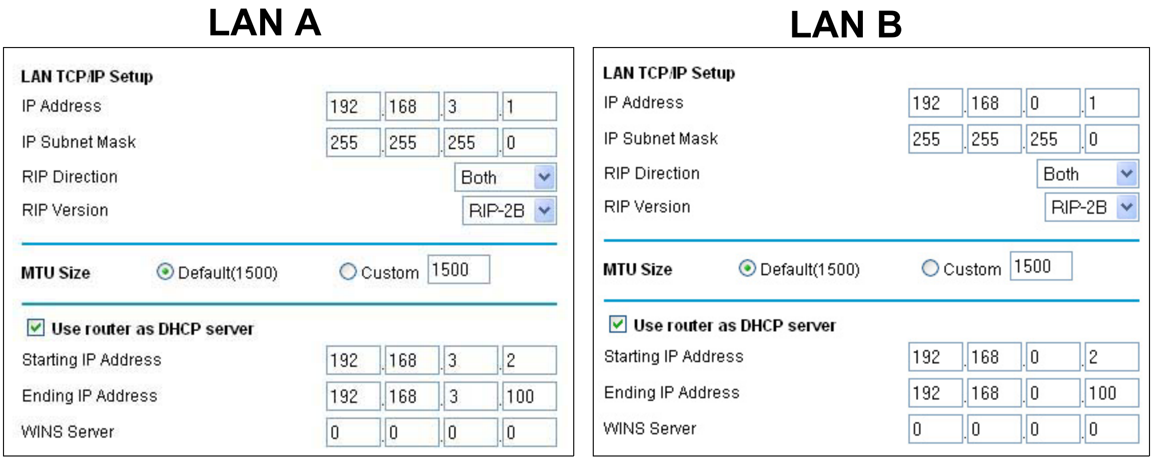
Network	Local IPSec ID	LAN IP Address	Subnet Mask	FQDN or Gateway IP (WAN IP Address)
LAN A	**LAN_A**	**192.168.3.1**	**255.255.255.0**	**24.0.0.1**
LAN B	**LAN_B**	**192.168.0.1**	**255.255.255.0**	**10.0.0.1**

1. **Set up the two LANs to have different IP address ranges.**

   Note: The LAN IP address ranges of each connected network must be different. The connection will fail if both are using the NETGEAR default address range of 192.168.0.x.

   This procedure uses the settings in the configuration worksheet above. A blank worksheet you can use to record your settings is provided on page 6-31.

   a. Log in to the FVS318 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 LAN IP Setup link in the main menu Advanced section to display the LAN TCP/IP Setup menu shown below.



LAN A

LAN TCP/IP Setup

IP Address	192 . 168 . 3 . 1
IP Subnet Mask	255 . 255 . 255 . 0
RIP Direction	Both
RIP Version	RIP-2B
MTU Size	● Default(1500) ○ Custom 1500

☑ **Use router as DHCP server**

Starting IP Address	192 . 168 . 3 . 2
Ending IP Address	192 . 168 . 3 . 100
WINS Server	0 . 0 . 0 . 0

LAN B

LAN TCP/IP Setup

IP Address	192 . 168 . 0 . 1
IP Subnet Mask	255 . 255 . 255 . 0
RIP Direction	Both
RIP Version	RIP-2B
MTU Size	● Default(1500) ○ Custom 1500

☑ **Use router as DHCP server**

Starting IP Address	192 . 168 . 0 . 2
Ending IP Address	192 . 168 . 0 . 100
WINS Server	0 . 0 . 0 . 0

Figure 6-7: Configuring the Local LAN (A) via the LAN IP Setup Menu

   b. For this example, configure the FVS318 settings on LANs A and B as follows:

Network Configuration Settings

Network	LAN IP Address	Subnet Mask	FQDN or Gateway IP (WAN IP Address)
LAN A	**192.168.3.1**	**255.255.255.0**	**24.0.0.1**
LAN B	**192.168.0.1**	**255.255.255.0**	**10.0.0.1**

   Note: If port forwarding, trusted user, or static routes are set up, you will need to change these configurations to match the 192.168.3.x network as well.

   c. Click Apply. Because you changed the Firewall's IP address, you are now disconnected.

d. Reboot all computers on network **A** and log back in to **FVS318 A** at the new address of *http://192.168.3.1*. The network configuration should now look like this:

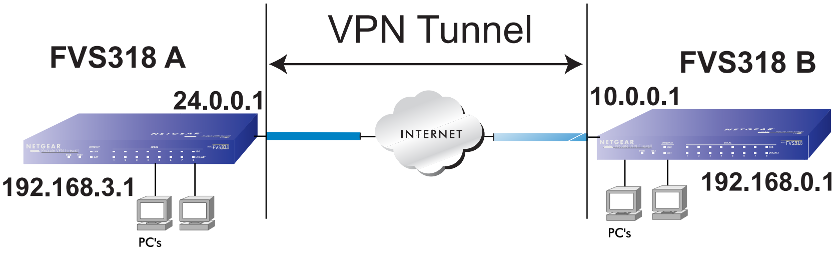
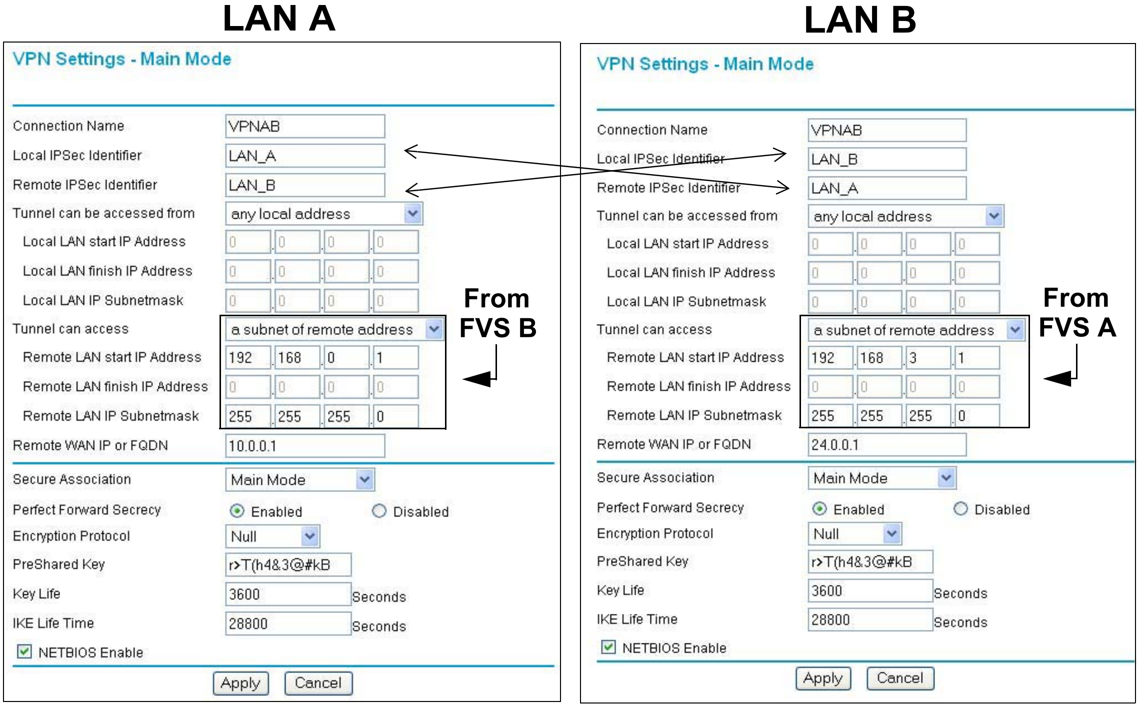


Figure 6-8: Network configuration

2. **Configure the VPN settings on each FVS318.**

   a. From the main menu, click the VPN Settings link, click the radio button of the tunnel you will update, and click Edit to view the VPN Settings - Main Mode window:



LAN A

VPN Settings - Main Mode

Connection Name	VPNAB
Local IPSec Identifier	LAN_A
Remote IPSec Identifier	LAN_B
Tunnel can be accessed from	any local address
Local LAN start IP Address	0 . 0 . 0 . 0
Local LAN finish IP Address	0 . 0 . 0 . 0
Local LAN IP Subnetmask	0 . 0 . 0 . 0
Tunnel can access	a subnet of remote address
Remote LAN start IP Address	192 . 168 . 0 . 1
Remote LAN finish IP Address	0 . 0 . 0 . 0
Remote LAN IP Subnetmask	255 . 255 . 255 . 0
Remote WAN IP or FQDN	10.0.0.1
Secure Association	Main Mode
Perfect Forward Secrecy	● Enabled ○ Disabled
Encryption Protocol	Null
PreShared Key	r>T(h4&3@#kB
Key Life	3600 Seconds
IKE Life Time	28800 Seconds
☑ NETBIOS Enable	

Apply Cancel

LAN B

VPN Settings - Main Mode

Connection Name	VPNAB
Local IPSec Identifier	LAN_B
Remote IPSec Identifier	LAN_A
Tunnel can be accessed from	any local address
Local LAN start IP Address	0 . 0 . 0 . 0
Local LAN finish IP Address	0 . 0 . 0 . 0
Local LAN IP Subnetmask	0 . 0 . 0 . 0
Tunnel can access	a subnet of remote address
Remote LAN start IP Address	192 . 168 . 3 . 1
Remote LAN finish IP Address	0 . 0 . 0 . 0
Remote LAN IP Subnetmask	255 . 255 . 255 . 0
Remote WAN IP or FQDN	24.0.0.1
Secure Association	Main Mode
Perfect Forward Secrecy	● Enabled ○ Disabled
Encryption Protocol	Null
PreShared Key	r>T(h4&3@#kB
Key Life	3600 Seconds
IKE Life Time	28800 Seconds
☑ NETBIOS Enable	

Apply Cancel

Figure 6-9: VPN Settings - Main Mode IKE Edit menu

b. For each FVS318, fill in the Connection Name VPN settings as illustrated above.

- The Connection Names can be the same: **VPNAB**
- Local IPSec Identifier name in the FVS318 on LAN A: **LAN_A**
  Note: The IPSec names must unique in this VPN network.
- Local IPSec Identifier in the FVS318 on LAN B: **LAN_B**
- Remote IPSec Identifier in the FVS318 on LAN A: **LAN_B**
- Remote IPSec Identifier in the FVS318 on LAN B: **LAN_A**
- Remote LAN IP Address in the FVS318 on LAN A: **192.168.0.1**
  and Remote Subnet Mask in the FVS318 on LAN A: **255.255.255.0**
  This is the LAN IP Address and Subnet Mask for the FVS318 on LAN B.

  Note: With these IP settings, using this VPN tunnel, you can connect to any device on LAN B. Alternatively, you can specify a single address, a subnet of local addresses, or a range of local addresses on LAN B which will limit the VPN tunnel to connecting to just those devices. For example, you can specify the IP address of a single address on LAN B and a Subnet Mask of 255.255.255.255 which will limit the VPN tunnel to connecting to just that device.
- Remote LAN IP Address in the FVS318 on LAN B: **192.168.3.1**
  and Remote Subnet Mask in the FVS318 on LAN B: **255.255.255.0**
  This is the LAN IP Address for the FVS318 on LAN A.
- Remote WAN IP Address in the FVS318 on LAN A: **10.0.0.1**
  This is the WAN IP Address for the FVS318 on LAN B.

  You can look up the WAN IP Address of the FVS318 on LAN B by viewing its WAN Status screen. When the FVS318 on LAN B is connected to the Internet, log in, go to its Maintenance menu Router Status link. If you find the WAN Port DHCP field says “DHCP Client” or “PPPOE,” then it is a dynamic address. For a dynamic address, you would enter 0.0.0.0 in the configuration screen of the FVS318 on LAN A as the WAN IP Address for the FVS318 on LAN B. Alternatively, you could use the FQDN of the FVS318.

  Note: If one FVS318 has a dynamic IP address and you do not use FQDN, that FVS318 must always initiate the connection.
- Remote WAN IP Address in the FVS318 on LAN B: **24.0.0.1**
  This is the WAN IP Address for the FVS318 on LAN A.

c. Under Secure Association, select Main Mode and fill in the settings below.

The IKE settings for each end point of the VPN tunnel must match exactly. To configure the IKE settings, enter the following settings in each FVS318:

- Enable Perfect Forward Secrecy.
- For Encryption Protocol, select: DES.
- Enter the Pre-Shared Key. In this example, enter **r>T(h4&3@#kB** as the Pre-Shared Key. With IKE, a pre-shared key that you make up is used for mutual identification. The Pre-Shared Key should be between 8 and 80 characters, and the letters are case sensitive. Entering a combination of letters, numbers and symbols, such as r>T(h4&3@#kB provides greater security.
- Key Life - Default is 3600 seconds (1 hour)
- IKE Life Time - Default is 28800 seconds (8 hours). A shorter time increases security, but users will be temporarily disconnected upon renegotiation.

d. If you need to run Microsoft networking functions such as Network Neighborhood, click the NETBIOS Enable check box to allow NETBIOS traffic over the VPN tunnel.

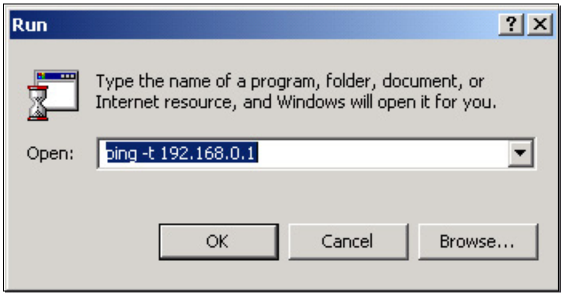
e. Click Apply to save the Security Association tunnel settings into the table.

3. Check the VPN Connection

To check the VPN Connection, you can initiate a request from one network to the other. If one FVS318 has a dynamically assigned WAN IP address, you must initiate the request from that FVS318's network. The simplest method is to ping the LAN IP address of the other FVS318.

a. Using our example, from a PC attached to the FVS318 on LAN A, on the Windows taskbar click the Start button, and then click Run.

b. Type `ping -t 192.168.0.1` , and then click OK.

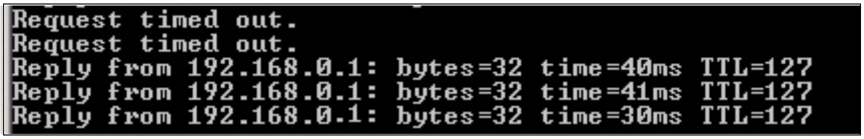


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: ping -t 192.168.0.1

Figure 6-10: Running a Ping test from Windows

c. This will cause a continuous ping to be sent to the first FVS318. After between several seconds and two minutes, the ping response should change from “timed out” to “reply.”



```
Request timed out.
Request timed out.
Reply from 192.168.0.1: bytes=32 time=40ms TTL=127
Reply from 192.168.0.1: bytes=32 time=41ms TTL=127
Reply from 192.168.0.1: bytes=32 time=30ms TTL=127
```

Figure 6-11: Ping test results

At this point the connection is established. Now that your VPN connection is working, whenever a PC on the second LAN needs to access an IP address on the first LAN, the Firewalls will automatically establish the connection.

How to Configure a Remote PC to Network VPN

This procedure describes linking a remote PC and a LAN. The LAN will connect to the Internet using an FVS318 with a fixed IP address. The PC can be connected to the Internet through dialup, cable or DSL modem, or other means, and we will assume it has a dynamically assigned IP address.

The PC must have a VPN client program that supports IPSec. NETGEAR recommends and supports the SafeNet SoftRemote (or Soft-PK) Secure VPN Client for Windows. The SafeNet VPN Client can be purchased from SafeNet at *http://www.safenet-inc.com*.

Note: If your situation is different, for example, if your remote PC is connected through a simple cable/DSL router, or if you wish to use different VPN client software, please refer to NETGEAR's web site for additional VPN applications information.

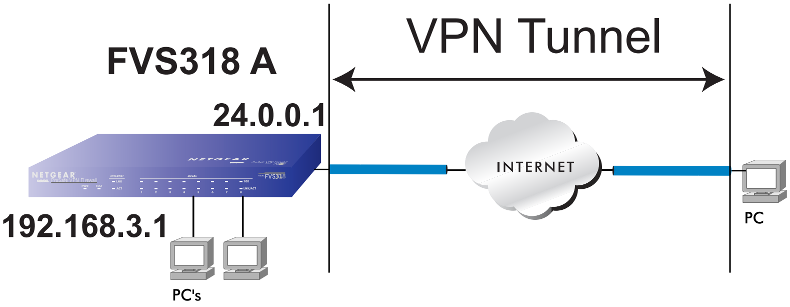


Figure 6-12: Remote PC to Local LAN (A) configuration

The worksheet below identifies the parameters used in the procedure below. A blank worksheet is at, "PC to Network IKE VPN Tunnel Settings Configuration Worksheet" on page 6-32.

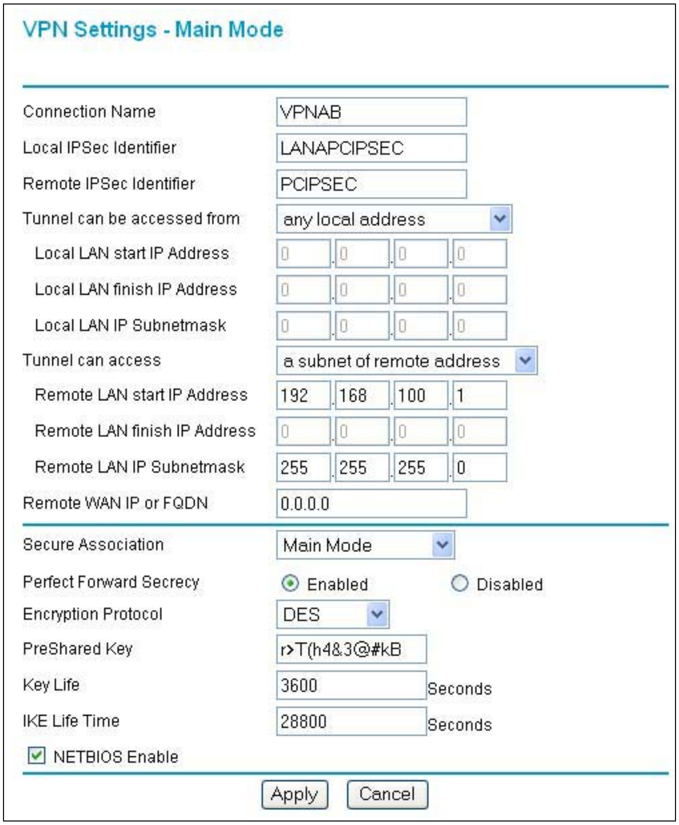
Table 6-2: PC to Network IKE VPN Tunnel Settings Configuration Worksheet

IKE Security Association Settings				
Connection Name:				**VPNLANPC**
Pre-Shared Key:				**r>T(h4&3@#kB**
Secure Association -- Main Mode, Aggressive Mode, or Manual Keys:				**Main**
Perfect Forward Secrecy:				**Enabled**
Encryption Protocol -- Null, DES, 3DES, or AES -128, -192, or -256:				**DES**
Key Life in seconds:				**3600 (1 hour)**
IKE Life Time in seconds:				**28800 (8 hours)**
Network	Local IPSec ID	LAN IP Address	Subnet Mask	FQDN or Gateway IP (WAN IP Address)
Network: LAN A	**LANAPCIPSEC**	**192.168.3.1**	**255.255.255.0**	**24.0.0.1**
Computer: PC	**PCIPSEC**	**192.168.100.2**	**255.255.255.255**	**0.0.0.0**

1. **Configure the VPN Tunnel on the FVS318 on LAN A.**

   To configure the Firewall, follow these steps:

   a. From the Setup Menu, click the VPN Settings link, then click Add to configure a new VPN tunnel. The VPN Settings - IKE window opens as shown below:



VPN Settings - Main Mode

Connection Name	VPNAB	
Local IPSec Identifier	LANAPCIPSEC	
Remote IPSec Identifier	PCIPSEC	
Tunnel can be accessed from	any local address	
Local LAN start IP Address	0.0.0.0	
Local LAN finish IP Address	0.0.0.0	
Local LAN IP Subnetmask	0.0.0.0	
Tunnel can access	a subnet of remote address	
Remote LAN start IP Address	192.168.100.1	
Remote LAN finish IP Address	0.0.0.0	
Remote LAN IP Subnetmask	255.255.255.0	
Remote WAN IP or FQDN	0.0.0.0	
Secure Association	Main Mode	
Perfect Forward Secrecy	● Enabled	○ Disabled
Encryption Protocol	DES	
PreShared Key	r>T(h4&3@#kB	
Key Life	3600	Seconds
IKE Life Time	28800	Seconds

☑ NETBIOS Enable

Figure 6-13: VPN Edit menu for connecting with a VPN client

b. Fill in the Connection Name VPN settings as illustrated.

- Connection Name: **VPNLANPC**
- Local IPSec Identifier: **LANAPCIPSEC**
  Note: This IPSec name must not be used in any other SA in this VPN network.
- Remote IPSec Identifier: **PCIPSEC**
- Remote LAN IP Address: **192.168.100.2**
  Since the remote network is a single PC, and its IP address is unknown, we will assume it is assigned dynamically. We will choose an arbitrary "fixed virtual" IP address to define this connection. This IP address will be used in the configuration of the VPN client. See "Configure the VPN Client Identity" on page 6-22.
- Remote Subnet Mask: **255.255.255.255** since this is a single PC.

- Remote WAN IP Address: **0.0.0.0** since the remote PC has a dynamically assigned IP address. Alternatively, you could use the FQDN of the PC.

Note: If one side has a dynamic IP address and you do not use FQDN, that side must always initiate the connection.

c. Under Secure Association, select Main Mode and fill in the settings below.

- Enable Perfect Forward Secrecy.
- For Encryption Protocol, select: **DES**
- Enter the case sensitive Pre-Shared Key: **r>T(h4&3@#kB**
  This combination of letters, numbers and symbols, provides greater security.
- Key Life - Default is **3600** seconds (1 hour)
- IKE Life Time - Default is **28800** seconds (8 hours). A shorter time increases security, but users will be temporarily disconnected upon renegotiation.

d. If you need to run Microsoft networking functions such as Network Neighborhood, click the NETBIOS Enable check box to allow NETBIOS traffic over the VPN tunnel.

e. Click Apply to save the Security Association tunnel settings into the table.

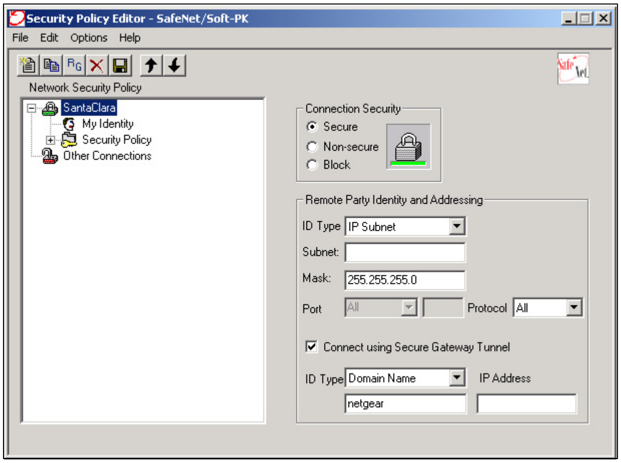
2. Set Up the SafeNet VPN Client Software on the PC.

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

a. **Install the SafeNet Secure VPN Client.**

- You may need to insert your Windows CD to complete the installation.
- If you do not have a modem or dial-up adapter installed in your PC, you may see the warning message stating “The SafeNet VPN Component requires at least one dial-up adapter be installed.” You can disregard this message.
- Install the IPSec Component. You may have the option to install either or both of the VPN Adapter or the IPSec Component. The VPN Adapter is not necessary.

Reboot your PC after installing the client software.s



Network Security Policy

- SantaClara
  - My Identity
  - Security Policy
- Other Connections

Connection Security

● Secure
○ Non-secure
○ Block

Remote Party Identity and Addressing

ID Type: IP Subnet
Subnet:
Mask: 255.255.255.0
Port: All Protocol: All

☑ Connect using Secure Gateway Tunnel

ID Type: Domain Name IP Address
netgear

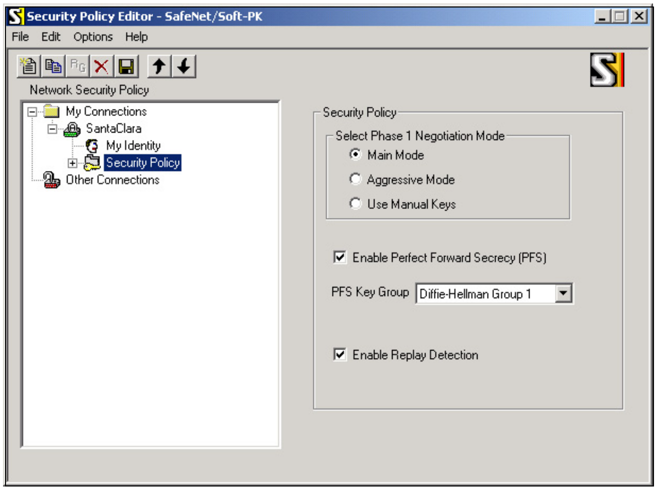
Figure 6-14: Security Policy Editor New Connection

b. **Add a new connection**

- Run the SafeNet Security Policy Editor program and, using the "PC to Network IKE VPN Tunnel Settings Configuration Worksheet" on page 6-17, create a VPN Connection.
- 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 FVS318 on LAN A. In this example, it would be **VPNLANPC.**
- Select Secure in the Connection Security box.
- Select IP Subnet in the ID Type menu.
- In this example, type **192.168.3.0** in the Subnet field as the network address of the FVS318. The network address is the LAN IP Address of the FVS318 with 0 as the last number.
- Enter **255.255.255.0 i**n the Mask field as the LAN Subnet Mask of the FVS318
- Select All in the Protocol menu to allow all traffic through the VPN tunnel.
- Check the Connect using Secure Gateway Tunnel checkbox.
- Select IP Address in the ID Type menu below the checkbox.
- Enter the public WAN IP Address of the FVS318 in the field directly below the ID Type menu. In this example, **24.0.0.1** would be used.

c. **Configure the Security Policy in the SafeNet VPN Client Software.**

- 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.
- Click on the Security Policy subheading to show the Security Policy menu.



Security Policy

Select Phase 1 Negotiation Mode

● Main Mode

○ Aggressive Mode

○ Use Manual Keys

☑ Enable Perfect Forward Secrecy (PFS)

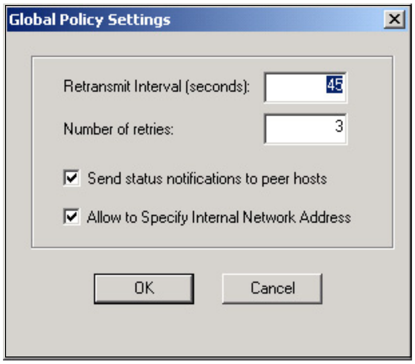
PFS Key Group: Diffie-Hellman Group 1

☑ Enable Replay Detection

Figure 6-15: Security Policy Editor Security Policy

- Select Main Mode in the Select Phase 1 Negotiation Mode box.
- Check the Enable Perfect Forward Secrecy (PFS) checkbox.
- Select Diffie-Hellman Group 1 for the PFS Key Group.
- Check the Enable Replay Detection checkbox.

d. **Configure the Global Policy Settings.**



Global Policy Settings

Retransmit Interval (seconds): 45

Number of retries: 3

☑ Send status notifications to peer hosts

☑ Allow to Specify Internal Network Address

Figure 6-16: Security Policy Editor Global Policy Options

- From the Options menu at the top of the Security Policy Editor window, select Global Policy Settings.
- Increase the Retransmit Interval period to 45 seconds.
- Check the Allow to Specify Internal Network Address checkbox and click OK.

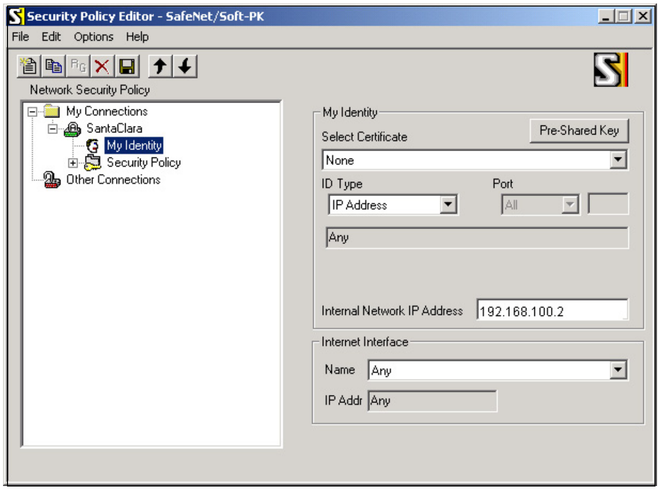
e. **Configure the VPN Client Identity**

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 FVS318.

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

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



Select Certificate: None

ID Type: IP Address

Port: All

Any

Internal Network IP Address: 192.168.100.2

Name: Any

IP Addr: Any

Figure 6-17: Security Policy Editor My Identity

- Choose None in the Select Certificate menu.
- Select IP Address in the ID Type menu. If you are using a virtual fixed IP address, enter this address in the Internal Network IP Address box. Otherwise, leave this box empty. Use **192.168.100.2** for this example.
- 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 dedicated Cable or DSL line. You may also choose Any if you will be switching between adapters or if you have only one adapter.
- Click the Pre-Shared Key button. In the Pre-Shared Key dialog box, click the Enter Key button. Enter the FVS318's Pre-Shared Key and click OK. In this example, **r>T(h4&3@#kB** would entered. Note that this field is case sensitive.

f. **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 FVS318 configuration.

- 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.

- Expand the Authentication subheading by double clicking its name or clicking on the "+" symbol. Then select Proposal 1 below Authentication.
- In the Authentication Method menu, select Pre-Shared key.
- In the Encrypt Alg menu, select the type of encryption to correspond with what you configured for the Encryption Protocol in the FVS318 in Figure 6-13. In this example, use DES.
- In the Hash Alg menu, select MD5.
- In the SA Life menu, select Unspecified.
- In the Key Group menu, select Diffie-Hellman Group 1.

g. **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 FVS318 configuration.

- Expand the Key Exchange subheading by double clicking its name or clicking on the "+" symbol. Then select Proposal 1 below Key Exchange.
- In the SA Life menu, select Unspecified.
- In the Compression menu, select None.
- Check the Encapsulation Protocol (ESP) checkbox.
- In the Encrypt Alg menu, select the type of encryption to correspond with what you configured for the Encryption Protocol in the FVS318 in Figure 6-13. In this example, use DES.
- In the Hash Alg menu, select MD5.
- In the Encapsulation menu, select Tunnel.
- Leave the Authentication Protocol (AH) checkbox unchecked.

h. **Save the VPN Client Settings.**

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

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 router's LAN.

3. Check the VPN Connection.

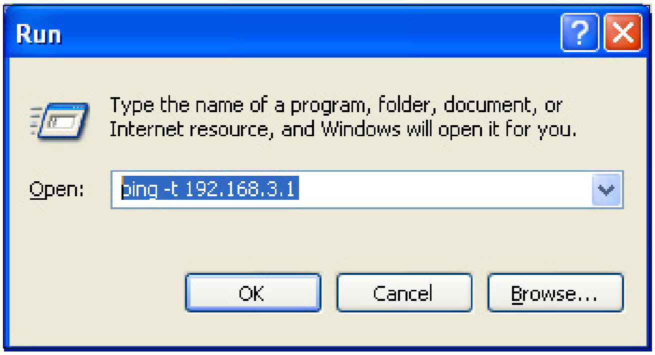
To check the VPN Connection, you can initiate a request from the remote PC to the FVS318's network by using the "Connect" option in the SafeNet menu bar. The SafeNet client will report the results of the attempt to connect. Since the remote PC has a dynamically assigned WAN IP address, it must initiate the request.

Another method is to ping from the remote PC to the LAN IP address of the FVS318. 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.

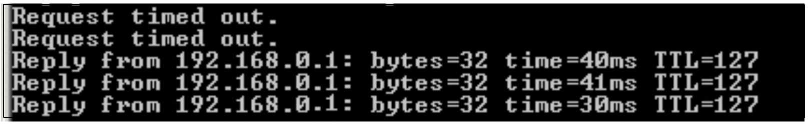
c. Type **`ping -t 192.168.3.1`** , and then click OK.


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

Open: ping -t 192.168.3.1

Figure 6-18: Running a Ping test to the LAN from the PC

This will cause a continuous ping to be sent to the first FVS318. After between several seconds and two minutes, the ping response should change from "timed out" to "reply."



```
Request timed out.
Request timed out.
Reply from 192.168.0.1: bytes=32 time=40ms TTL=127
Reply from 192.168.0.1: bytes=32 time=41ms TTL=127
Reply from 192.168.0.1: bytes=32 time=30ms TTL=127
```

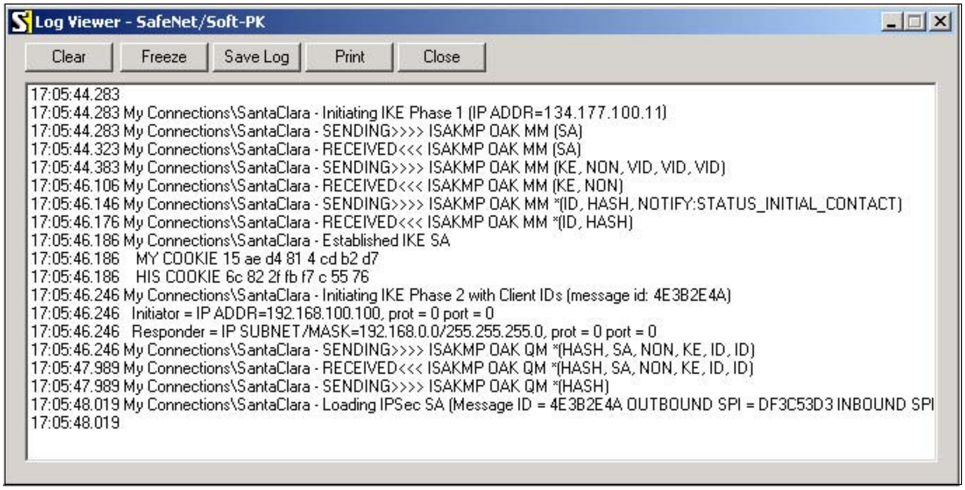
Figure 6-19: Ping test results

Once the connection is established, you can open the browser of the remote PC and enter the LAN IP Address of the remote FVS318. After a short wait, you should see the login screen of the Firewall.

Monitoring the PC VPN Connection Using SafeNet Tools

Information on the progress and status of the VPN client connection can be viewed by opening the SafeNet Connection Monitor or Log Viewer. To launch these functions, click on the Windows Start button, then select Programs, then SafeNet SoftRemote, then either the Connection Monitor or Log Viewer.

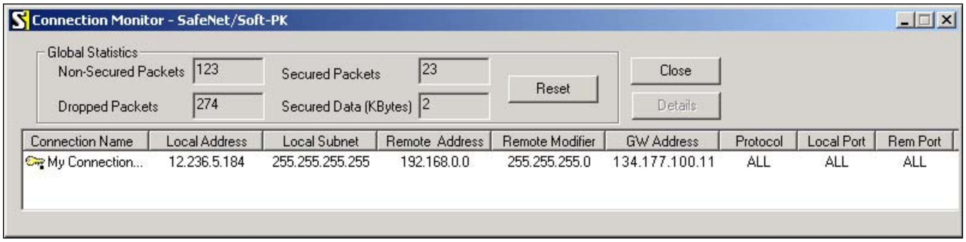
The Log Viewer screen for a successful connection is shown below:



```
17:05:44.283
17:05:44.283 My Connections\SantaClara - Initiating IKE Phase 1 (IP ADDR=134.177.100.11)
17:05:44.283 My Connections\SantaClara - SENDING>>>> ISAKMP OAK MM (SA)
17:05:44.323 My Connections\SantaClara - RECEIVED<<< ISAKMP OAK MM (SA)
17:05:44.383 My Connections\SantaClara - SENDING>>>> ISAKMP OAK MM (KE, NON, VID, VID, VID)
17:05:46.106 My Connections\SantaClara - RECEIVED<<< ISAKMP OAK MM (KE, NON)
17:05:46.146 My Connections\SantaClara - SENDING>>>> ISAKMP OAK MM *(ID, HASH, NOTIFY:STATUS_INITIAL_CONTACT)
17:05:46.176 My Connections\SantaClara - RECEIVED<<< ISAKMP OAK MM *(ID, HASH)
17:05:46.186 My Connections\SantaClara - Established IKE SA
17:05:46.186    MY COOKIE 15 ae d4 81 4 cd b2 d7
17:05:46.186    HIS COOKIE 6c 82 2f fb f7 c 55 76
17:05:46.246 My Connections\SantaClara - Initiating IKE Phase 2 with Client IDs (message id: 4E3B2E4A)
17:05:46.246   Initiator = IP ADDR=192.168.100.100, prot = 0 port = 0
17:05:46.246   Responder = IP SUBNET/MASK=192.168.0.0/255.255.255.0, prot = 0 port = 0
17:05:46.246 My Connections\SantaClara - SENDING>>>> ISAKMP OAK QM *(HASH, SA, NON, KE, ID, ID)
17:05:47.989 My Connections\SantaClara - RECEIVED<<< ISAKMP OAK QM *(HASH, SA, NON, KE, ID, ID)
17:05:47.989 My Connections\SantaClara - SENDING>>>> ISAKMP OAK QM *(HASH)
17:05:48.019 My Connections\SantaClara - Loading IPSec SA (Message ID = 4E3B2E4A OUTBOUND SPI = DF3C53D3 INBOUND SPI
17:05:48.019
```

Figure 6-20: Log Viewer screen

The Connection Monitor screen for this connection is shown below:



Global Statistics

Non-Secured Packets 123 Secured Packets 23

Dropped Packets 274 Secured Data (KBytes) 2

Connection Name	Local Address	Local Subnet	Remote Address	Remote Modifier	GW Address	Protocol	Local Port	Rem Port
My Connection...	12.236.5.184	255.255.255.255	192.168.0.0	255.255.255.0	134.177.100.11	ALL	ALL	ALL

Figure 6-21: Connection Monitor screen

In this example you can see the following:

- The FVS318 has a public IP WAN address of 134.177.100.11
- The FVS318 has a LAN IP address of 192.168.0.1
- The VPN client PC has a dynamically assigned address of 12.236.5.184
- The VPN client PC is using a “virtual fixed” IP address of 192.168.100.100

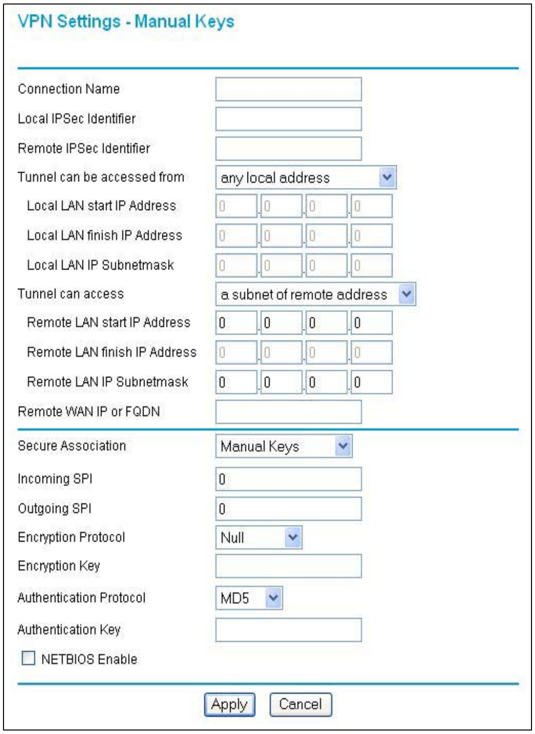
While the connection is being established, the Connection Name field in this menu will say “SA” before the name of the connection. When the connection is successful, the “SA” will change to the yellow key symbol shown in the illustration above.

➡	**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.

How to Configure Manual Keys as an Alternative to IKE

As an alternative to IKE, you may use Manual Keying, in which you must specify each phase of the connection. Follow the steps to configure Manual Keying.

1. When editing an entry in the VPN Settings menu table, you may select manual keying. At that time, the edit menu changes to look like the screen below: The network connection settings would be configured the same way the IKE options detailed in the previous example procedures.



VPN Settings - Manual Keys

Connection Name	
Local IPSec Identifier	
Remote IPSec Identifier	
Tunnel can be accessed from	any local address
Local LAN start IP Address	0 . 0 . 0 . 0
Local LAN finish IP Address	0 . 0 . 0 . 0
Local LAN IP Subnetmask	0 . 0 . 0 . 0
Tunnel can access	a subnet of remote address
Remote LAN start IP Address	0 . 0 . 0 . 0
Remote LAN finish IP Address	0 . 0 . 0 . 0
Remote LAN IP Subnetmask	0 . 0 . 0 . 0
Remote WAN IP or FQDN	
Secure Association	Manual Keys
Incoming SPI	0
Outgoing SPI	0
Encryption Protocol	Null
Encryption Key	
Authentication Protocol	MD5
Authentication Key	

□ NETBIOS Enable

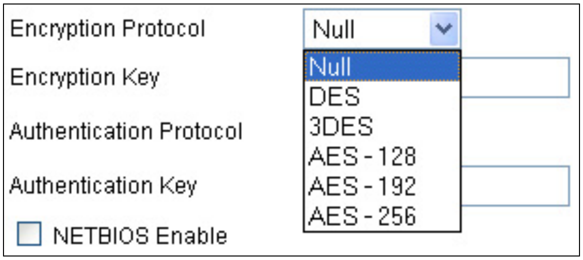
Figure 6-22: VPN Manual Keying menu

2. Incoming SPI - Enter a Security Parameter Index that the remote host will send to identify the Security Association (SA). This will be the remote host’s Outgoing SPI.
3. Outgoing SPI - Enter a Security Parameter Index that this Firewall will send to identify the Security Association (SA). This will be the remote host’s Incoming SPI.

The SPI should be a string of hexadecimal [0-9,A-F] characters, and should not be used in any other Security Association.

Note: For simplicity or troubleshooting, the Incoming and Outgoing SPI can be identical.

4. For Encryption Protocol, select one:



Encryption Protocol: Null

Encryption Key

Authentication Protocol

Authentication Key

□ NETBIOS Enable

Figure 6-23: VPN encryption options

- Null - Fastest, but no security.
- DES - Faster but less secure than 3DES or AES.
- 3DES - (Triple DES) higher level of security than DES.
- AES - 128, - 192, or - 256. Most secure.

5. Enter the key according to the requirements of the Encryption Protocol you selected. Enter an Encryption Key in hexadecimal characters [0-9,A-F].

   – For DES, the key should be 8 characters.
   – For 3DES, the key should be 24 characters.
   – For AES 128, the key should be 16 characters
   – For AES 192, the key should be 24 characters
   – For AES 256, the key should be 32 characters

   Any value is acceptable, provided the remote VPN endpoint has the same value in its Pre-Shared Key field.The encryption key must match exactly the key used by the remote router or host.

6. Select the Authentication Protocol

   - MD5 (default) - 128 bits, faster but less secure.
   - SHA-1 - 160 bits, slower but more secure.

7. Enter hexadecimal characters [0-9,A-F] for the Authentication Key. The authentication key must match exactly the key used by the remote router or host.

   – For MD5, the key should be 16 characters.
   – For SHA-1, the key should be 20 characters.

8. Click the NETBIOS Enable check box to allow NETBIOS over the VPN tunnel.
9. Click Apply to update the SA in the VPN Settings table.

How to Delete a Security Association

To delete a security association:

1. Log in to the Firewall.
2. Click the VPN Settings link.
3. In the VPN Settings Security Association table, select the radio button for the security association to be deleted.
4. Click the Delete button.
5. Click the Update button.

Blank VPN Tunnel Configuration Worksheets

The blank configuration worksheets below are provided to aid you in collecting and recording the parameters used in the VPN configuration procedure.

Table 6-3: Network to Network IKE VPN Tunnel Configuration Worksheet

IKE Tunnel Security Association Settings

Connection Name:

Pre-Shared Key:

Secure Association -- Main Mode, Aggressive Mode, or Manual Keys:

Perfect Forward Secrecy:

Encryption Protocol -- Null, DES, 3DES, or AES -128, -192, or -256:

Key Life in seconds:

IKE Life Time in seconds:

Network	Local IPSec ID	LAN IP Address	Subnet Mask	FQDN or Gateway IP (WAN IP Address)

Table 6-4: PC to Network IKE VPN Tunnel Settings Configuration Worksheet

IKE Tunnel Security Association Settings

Connection Name:

Pre-Shared Key:

Secure Association -- Main Mode, Aggressive Mode, or Manual Keys:

Perfect Forward Secrecy:

Encryption Protocol -- Null, DES, 3DES, or AES -128, -192, or -256:

Key Life in seconds:

IKE Life Time in seconds:

Network	Local IPSec ID	LAN IP Address	Subnet Mask	FQDN or Gateway IP (WAN IP Address)
Network:				
PC:				

Chapter 7
Managing Your Network

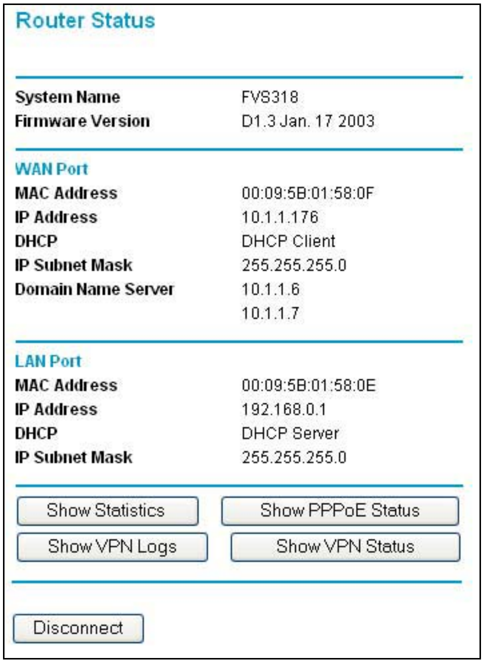
This chapter describes how to perform network management tasks with your FVS318 Broadband ProSafe VPN Firewall .

Network Management Information

The FVS318 provides a variety of status and usage information which is discussed below.

Viewing Router Status and Usage Statistics

From the Main Menu, under Maintenance, select Router Status to view the screen in Figure 7-1.



Router Status

System Name	FVS318
Firmware Version	D1.3 Jan. 17 2003
WAN Port	
MAC Address	00:09:5B:01:58:0F
IP Address	10.1.1.176
DHCP	DHCP Client
IP Subnet Mask	255.255.255.0
Domain Name Server	10.1.1.6 10.1.1.7
LAN Port	
MAC Address	00:09:5B:01:58:0E
IP Address	192.168.0.1
DHCP	DHCP Server
IP Subnet Mask	255.255.255.0

Figure 7-1: Router Status screen

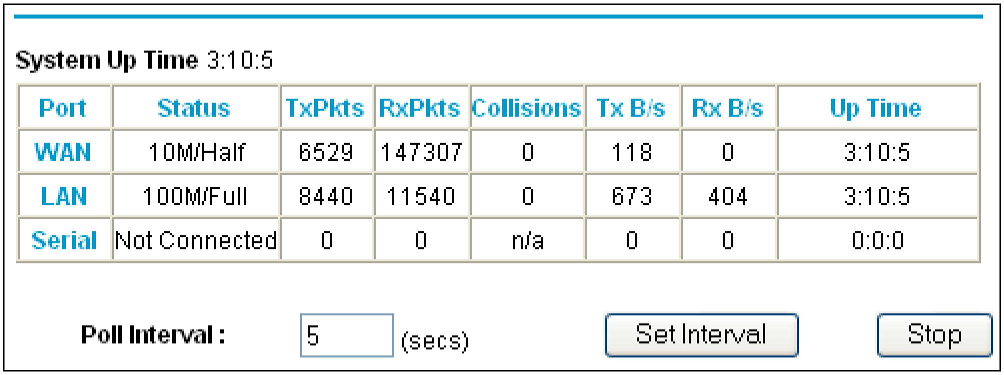
The Router Status menu provides a limited amount of status and usage information. From the Main Menu of the browser interface, under Maintenance, select Router Status to view the status screen, shown in Figure 7-1.

This screen shows the following parameters:

Table 7-1. Menu 3.2 - Router Status Fields

Field	Description
System Name	This field displays the Host Name assigned to the firewall in the Basic Settings menu.
Firmware Version	This field displays the firewall firmware version.
WAN Port	These parameters apply to the Internet (WAN) port of the firewall.
MAC Address	This field displays the Ethernet MAC address being used by the Internet (WAN) port of the firewall.
IP Address	This field displays the IP address being used by the Internet (WAN) port of the firewall. If no address is shown, the firewall cannot connect to the Internet.
DHCP	If set to None, the firewall is configured to use a fixed IP address on the WAN. If set to Client, the firewall is configured to obtain an IP address dynamically from the ISP
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Internet (WAN) port of the firewall.
Domain Name Servers (DNS)	This field displays the DNS Server IP addresses being used by the firewall. These addresses are usually obtained dynamically from the ISP.
LAN Port	These parameters apply to the Local (WAN) port of the firewall.
MAC Address	This field displays the Ethernet MAC address being used by the Local (LAN) port of the firewall.
IP Address	This field displays the IP address being used by the Local (LAN) port of the firewall. The default is 192.168.0.1
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Local (LAN) port of the firewall. The default is 255.255.255.0
DHCP	If set to OFF, the firewall will not assign IP addresses to local PCs on the LAN. If set to ON, the firewall is configured to assign IP addresses to local PCs on the LAN.

Click on the “Show Statistics” button to display firewall usage statistics, as shown in Figure 7-2 below:



System Up Time 3:10:5

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	10M/Half	6529	147307	0	118	0	3:10:5
LAN	100M/Full	8440	11540	0	673	404	3:10:5
Serial	Not Connected	0	0	n/a	0	0	0:0:0

Poll Interval : 5 (secs)

Figure 7-2. Router Statistics screen

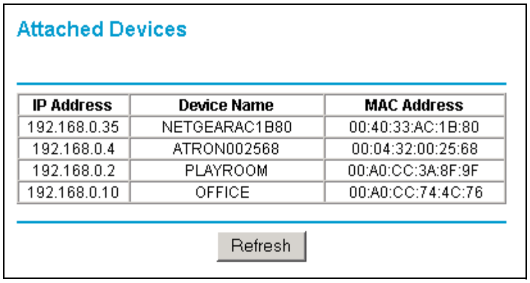
This screen shows the following statistics:.

Table 7-2. Router Statistics Fields

Field	Description
WAN, LAN, or Serial Port	The statistics for the WAN (Internet), LAN (local), and Serial ports. For each port, the screen displays:
Status	The link status of the port.
TxPkts	The number of packets transmitted on this port since reset or manual clear.
RxPkts	The number of packets received on this port since reset or manual clear.
Collisions	The number of collisions on this port since reset or manual clear.
Tx B/s	The current line utilization—percentage of current bandwidth used on this port.
Tx B/s Up Time	The average line utilization —average CLU for this port. The time elapsed since this port acquired link.
System up Time	The time elapsed since the last power cycle or reset.
Poll Interval	Specifies the intervals at which the statistics are updated in this window. Click on Stop to freeze the display.

Viewing 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 in Figure 7-3



Attached Devices

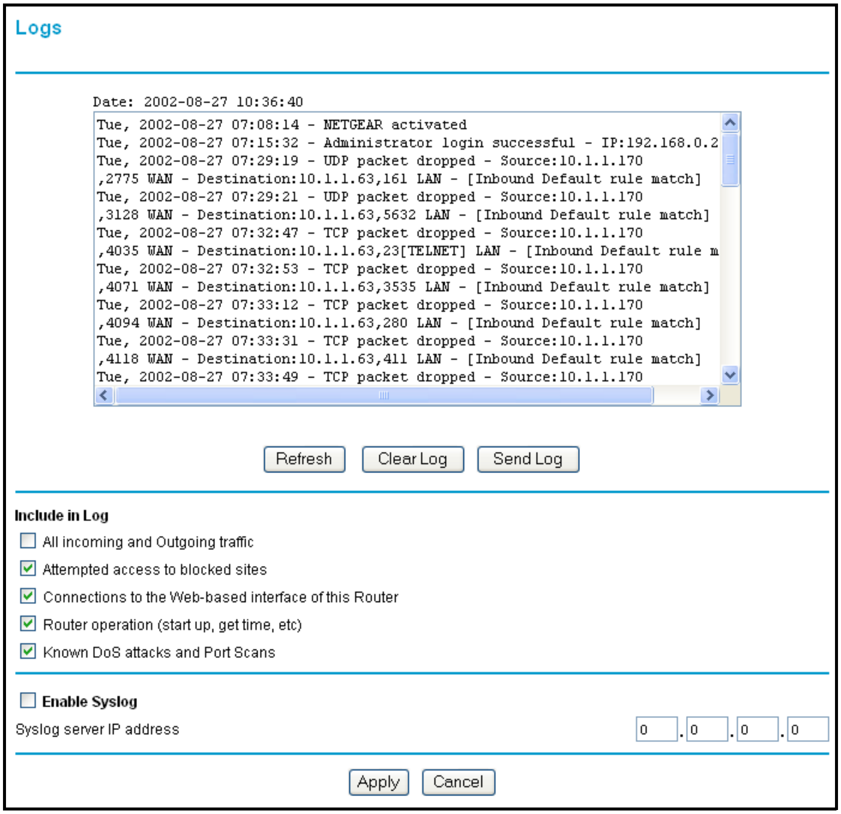
IP Address	Device Name	MAC Address
192.168.0.35	NETGEARAC1B80	00:40:33:AC:1B:80
192.168.0.4	ATRON002568	00:04:32:00:25:68
192.168.0.2	PLAYROOM	00:A0:CC:3A:8F:9F
192.168.0.10	OFFICE	00:A0:CC:74:4C:76

Figure 7-3: Attached Devices menu

For each device, the table shows the IP address, NetBIOS Host Name, if available, and the 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.

Viewing, Selecting, and Saving Logged Information

The firewall will log security-related events such as denied incoming service requests, hacker probes, and administrator logins. If you enabled content filtering in the Block Sites menu, the Logs page shows 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 below.



Logs

```
Date: 2002-08-27 10:36:40
Tue, 2002-08-27 07:08:14 - NETGEAR activated
Tue, 2002-08-27 07:15:32 - Administrator login successful - IP:192.168.0.2
Tue, 2002-08-27 07:29:19 - UDP packet dropped - Source:10.1.1.170
,2775 WAN - Destination:10.1.1.63,161 LAN - [Inbound Default rule match]
Tue, 2002-08-27 07:29:21 - UDP packet dropped - Source:10.1.1.170
,3128 WAN - Destination:10.1.1.63,5632 LAN - [Inbound Default rule match]
Tue, 2002-08-27 07:32:47 - TCP packet dropped - Source:10.1.1.170
,4035 WAN - Destination:10.1.1.63,23[TELNET] LAN - [Inbound Default rule m
Tue, 2002-08-27 07:32:53 - TCP packet dropped - Source:10.1.1.170
,4071 WAN - Destination:10.1.1.63,3535 LAN - [Inbound Default rule match]
Tue, 2002-08-27 07:33:12 - TCP packet dropped - Source:10.1.1.170
,4094 WAN - Destination:10.1.1.63,280 LAN - [Inbound Default rule match]
Tue, 2002-08-27 07:33:31 - TCP packet dropped - Source:10.1.1.170
,4118 WAN - Destination:10.1.1.63,411 LAN - [Inbound Default rule match]
Tue, 2002-08-27 07:33:49 - TCP packet dropped - Source:10.1.1.170
```

Include in Log

- □ All incoming and Outgoing traffic
- ☑ Attempted access to blocked sites
- ☑ Connections to the Web-based interface of this Router
- ☑ Router operation (start up, get time, etc)
- ☑ Known DoS attacks and Port Scans

□ **Enable Syslog**

Syslog server IP address 0 . 0 . 0 . 0

Figure 7-4: Security Logs menu

Log entries are described in Table 7-5

Table 7-5: Security 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 website.
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 7-6

Table 7-6: Security Log action buttons

Field	Description
Refresh	Click this button to refresh the log screen.
Clear Log	Click this button to clear the log entries.
Send Log	Click this button to email the log immediately.
Apply	Click this button to apply the current settings.
Cancel	Click this button to clear the current settings.

Selecting What Information to Log

Besides the standard information listed above, you can choose to log additional information. Those optional selections are as follows:

- All incoming and outgoing traffic
- Attempted access to blocked site
- Connections to the Web-based interface of this Router

- Router operation (start up, get time, etc.)
- Known DoS attacks and Port Scans

Saving Log Files on a Server

You can choose to write the logs to a PC running a syslog program. To activate this feature, check the box under Syslog and enter the IP address of the server where the log file will be written.

Examples of log messages

Following are examples of log messages. In all cases, the log entry shows the timestamp as: Day, Year-Month-Date Hour:Minute:Second

Activation and Administration

```
Tue, 2002-05-21 18:48:39 - NETGEAR activated
```

[This entry indicates a power-up or reboot with initial time entry.]

```
Tue, 2002-05-21 18:55:00 - Administrator login successful - IP:192.168.0.2
Thu, 2002-05-21 18:56:58 - Administrator logout - IP:192.168.0.2
```

[This entry shows an administrator logging in and out from IP address 192.168.0.2.]

```
Tue, 2002-05-21 19:00:06 - Login screen timed out - IP:192.168.0.2
```

[This entry shows a time-out of the administrator login.]

```
Wed, 2002-05-22 22:00:19 - Log emailed
```

[This entry shows when the log was emailed.]

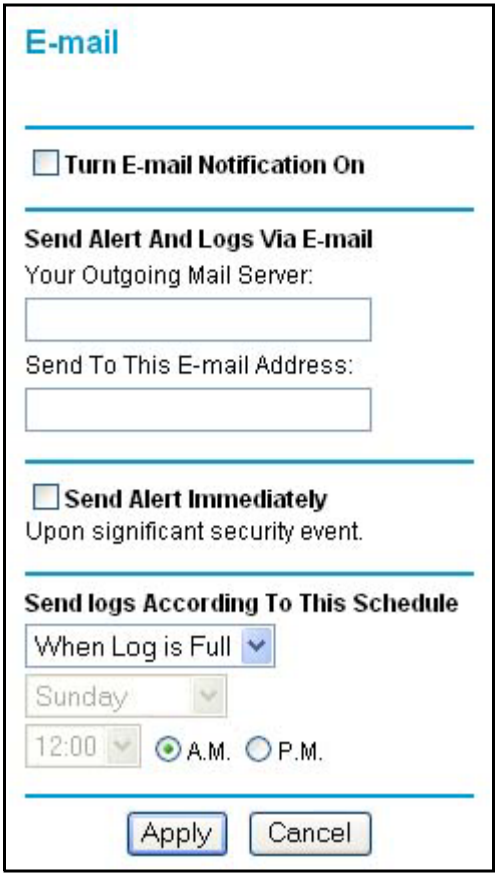
Dropped Packets

```
Wed, 2002-05-22 07:15:15 - TCP packet dropped - Source:64.12.47.28,4787,WAN -
Destination:134.177.0.11,21,LAN - [Inbound Default rule match]
Sun, 2002-05-22 12:50:33 - UDP packet dropped - Source:64.12.47.28,10714,WAN -
Destination:134.177.0.11,6970,LAN - [Inbound Default rule match]
Sun, 2002-05-22 21:02:53 - ICMP packet dropped - Source:64.12.47.28,0,WAN -
Destination:134.177.0.11,0,LAN - [Inbound Default rule match]
```

[These entries show an inbound FTP (port 21) packet, UDP packet (port 6970), and ICMP packet (port 0) being dropped as a result of the default inbound rule, which states that all inbound packets are denied.]

Enabling Security Event E-mail Notification

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



E-mail

☐ Turn E-mail Notification On

Send Alert And Logs Via E-mail

Your Outgoing Mail Server:

Send To This E-mail Address:

☐ Send Alert Immediately

Upon significant security event.

Send logs According To This Schedule

When Log is Full

Sunday

12:00 ● A.M. ○ P.M.

Apply Cancel

Figure 7-7: E-mail menu

- Turn e-mail notification on
  Check this box if you wish to receive e-mail logs and alerts from the firewall.

- Your outgoing mail server
  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. If you leave this box blank, log and alert messages will not be sent via e-mail.
- Send to this e-mail address
  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.

You can specify that logs are automatically sent to the specified e-mail address with these options:

- Send alert immediately
  Check this box if you would like immediate notification of a significant security event, such as a known attack, port scan, or attempted access to a blocked site.
- Send logs according to this schedule
  Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.
  – Day for sending log
    Specifies which day of the week to send the log. Relevant when the log is sent weekly or daily.
  – Time for sending log
    Specifies the time of day to send the 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.

Backing Up, Restoring, or Erasing Your Settings

The configuration settings of the FVS318 VPN Firewall are stored in a configuration file in the firewall. This file can be backed up to your computer, restored, or reverted to factory default settings. The procedures below explain how to do these tasks.

How to Back Up the Configuration to a File

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 User Name, Password and LAN address you have chosen for the firewall.

2. From the Maintenance heading of the Main Menu, click the Settings Backup link to display the menu seen in Figure 7-8.

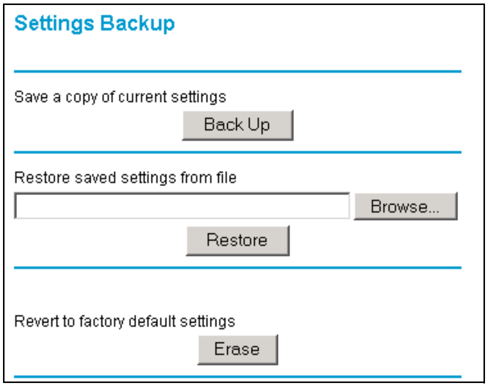

Settings Backup
Save a copy of current settings
Back Up
Restore saved settings from file
Browse...
Restore
Revert to factory default settings
Erase

Figure 7-8: Settings Backup menu

3. Click Backup to save a copy of the current settings.
4. Store the `.cfg` file on a computer on your network.

How to Restore a Configuration from a File

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 User Name, Password and LAN address you have chosen for the firewall.
2. From the Maintenance heading of the Main Menu, select the Settings Backup menu as seen in Figure 7-8.
3. Enter the full path to the file on your network or click the Browse button to browse to the file.
4. When you have located the `.cfg` file, click the Restore button to upload the file to the firewall.
5. The firewall will then reboot automatically.

How to Erase the Configuration

It is sometimes desirable to restore the firewall to the factory default settings. This can be done by using the Erase function.

1. To erase the configuration, from the Maintenance menu Settings Backup link, click the Erase button on the screen.
2. The firewall will then reboot automatically.

   After an erase, the firewall's password will be **password**, the LAN IP address will be 192.168.0.1, and the router's DHCP client will be enabled.

Note: To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the firewall. See "Restoring the Default Configuration and Password" on page 8-7.

Running Diagnostic Utilities and Rebooting the Router

The FVS318 VPN Firewall has a diagnostics feature. You can use the diagnostics menu to perform the following functions from the firewall:

- Ping an IP Address to test connectivity to see if you can reach a remote host.
- Perform a DNS Lookup to test if an Internet name resolves to an IP address to verify that the DNS server configuration is working.
- Display the Routing Table to identify what other routers the router is communicating with.
- Trace the Routing Path to identify any connectivity or congestion problems in the network.
- Reboot the Router to enable new network configurations to take effect or to clear problems with the router's network connection.

From the Main Menu of the browser interface, under the Maintenance heading, select the Router Diagnostics heading to display the menu shown in Figure 7-9.

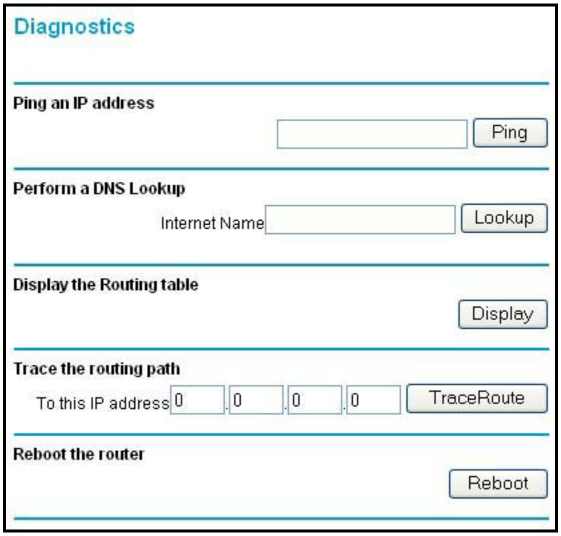


Figure 7-9: Diagnostics menu

How to Enable Remote Management

Using the Remote Management page, you can allow a user or users on the Internet to configure, upgrade and check the status of your NETGEAR Cable/DSL ProSafe VPN Firewall.

Note: Be sure to change the router's default 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.

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 User Name, Password and LAN address you have chosen for the firewall.
2. Select the Allow Remote Management check box.
3. Specify what external addresses will be allowed to access the firewall's remote management. **Note:** For security reasons, restrict access to as few external IP addresses as is 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.

4. 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.

5. Click Apply to have your changes take effect.

When accessing your router from the Internet, you will type your router's WAN IP address into your browser's Address (in IE) or Location (in Netscape) box, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, enter in your browser:

```
http://134.177.0.123:8080
```

How to Upgrade the Router’s Firmware

The software of the FVS318 VPN Firewall is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR.

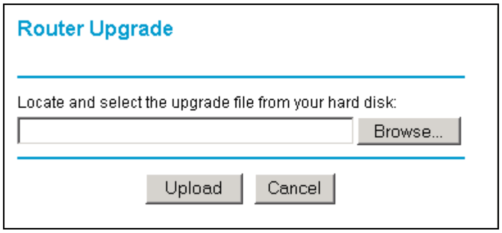
Upgrade files can be downloaded from NETGEAR's website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN or .IMG) file before uploading it to the firewall.

The Web browser used to upload new firmware into the firewall must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer 5.0 or Netscape Navigator 4.7 and above.

Note: Product updates are available on the NETGEAR web site at *www.netgear.com/support/main.asp*. Documentation updates are available on the NETGEAR, Inc. web site at *www.netgear.com/docs*.

1. Download and unzip the new software file from NETGEAR.

2. 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 User Name, Password and LAN address you have chosen for the firewall.
3. From the Main Menu of the browser interface, under the Maintenance heading, select the Router Upgrade heading to display the menu shown in Figure 7-10.


Router Upgrade

Locate and select the upgrade file from your hard disk:

Figure 7-10: Router Upgrade menu

4. In the Router Upgrade menu, click the **Browse** to locate the binary (.BIN or .IMG) upgrade file.
5. Click **Upload**.

Note: When uploading software to the 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 clear the configuration and reconfigure the firewall after upgrading.

Chapter 8
Troubleshooting

This chapter gives information about troubleshooting your FVS318 Broadband ProSafe VPN Firewall . For the common problems listed, go to the section indicated.

- Is the firewall on?
- Have I connected the firewall correctly?

  Go to "Basic Functions" on page 8-1.
- I can't access the firewall's configuration with my browser.

  Go to "Troubleshooting the Web Configuration Interface" on page 8-3.
- I've configured the firewall but I can't access the Internet.

  Go to "Troubleshooting the ISP Connection" on page 8-4.
- I can't remember the firewall's configuration password.
- I want to clear the configuration and start over again.

  Go to "Restoring the Default Configuration and Password" on page 8-7.

Basic Functions

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

1. When power is first applied, verify that the Power LED is on.
2. Verify that the Test LED lights within a few seconds, indicating that the self-test procedure is running.
3. After approximately 10 seconds, verify that:
   a. The Test LED is not lit.
   b. The Local port Link LEDs are lit for any local ports that are connected.
   c. The Internet Link port LED is lit.

If a port's Link LED is lit, a link has been established to the connected device. If a port is connected to a 100 Mbps device, verify that the port's 100 LED is lit.

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 12VDC power adapter supplied by NETGEAR for this product.

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

Test LED Never Turns On or Test LED Stays On

When the firewall is turned on, the Test LED turns on for about 10 seconds and then turns off. If the Test LED does not turn on, or if it stays on, there is a fault within the firewall.

If you experience problems with the Test LED:

- Cycle the power to see if the firewall recovers and the LED blinks for the correct amount of time.

If all LEDs including the Test LED 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 8-7.

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

Local or Internet Port Link LEDs Not On

If either the Local or Internet Port Link LEDs 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 PC.

- Make sure that power is turned on to the connected hub or PC.
- 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. Refer to "Verifying TCP/IP Properties" on page C-6 or "Configuring the Macintosh for TCP/IP Networking" on page C-15 to find your PC's IP address. Follow the instructions in Appendix C to configure your PC.

  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 8-7.
- 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 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 3-13.

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.netgear.com) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. If you entered a DNS address during the firewall’s configuration, reboot your PC and verify the DNS address as described in “DHCP Configuration of TCP/IP in Windows 2000 ” on page C-10. 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 as described in “DHCP Configuration of TCP/IP in Windows 2000 ” on page C-10.

Troubleshooting a TCP/IP Network Using a Ping Utility

Most TCP/IP terminal devices and routers 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 easier 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 on 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 "Local or Internet Port Link LEDs Not On" on page 8-2.

     — Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and 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 as described in "Verifying TCP/IP Properties" on page C-6.
- — 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 3-13.

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 Web Configuration Manager (see "Backing Up, Restoring, or Erasing Your Settings" on page 7-9).
- Use the Default Reset button on the rear panel of the firewall. Use this method for cases when the administration password or IP address is not known.

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

To restore the factory default configuration settings, follow these steps:

1. Turn the firewall off.
2. While pressing the Default Reset button, turn the firewall on.
3. Keep holding the button until the TEST LED turns off (about 10 seconds later), then blinks (about 20 seconds total).

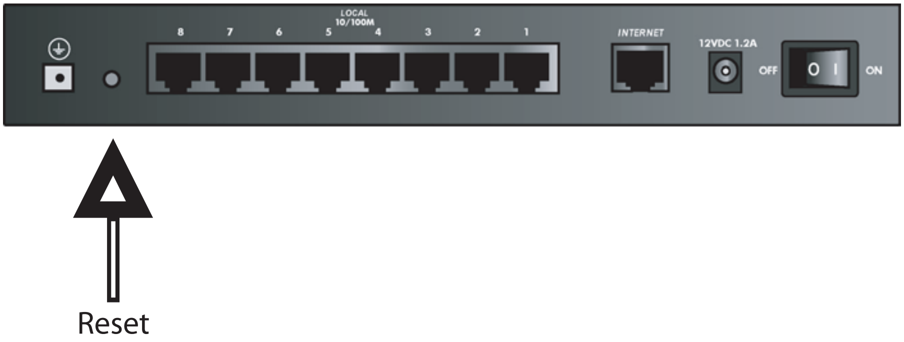


Figure 8-1. Using Reset Button

4. Release the Default 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 FVS318 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

Technical Specifications

The technical specifications for the FVS318 Broadband ProSafe VPN Firewall are presented in the following table.

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 @ 1.2A output, 20W maximum
Physical Specifications	
Dimensions:	H: 1.56 in (3.96 cm) W: 10.0 in (25.4 cm) D: 9.0 in (17.8 cm)
Weight:	2.72 lb. (1.23 Kg)
Environmental Specifications	
Operating temperature:	32°-140° F (0° to 40° C)
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	
Local:	10BASE-T or 100BASE-Tx, RJ-45
Internet:	10BASE-T or 100BASE-Tx, RJ-45

Appendix B
Networks, Routing, and Firewall Basics

This chapter provides an overview of IP networks, routing, and firewalls.

Related Publications

As you read this document, you may be directed to various RFC documents for further information. An RFC is a Request For Comment (RFC) published by the Internet Engineering Task Force (IETF), an open organization that defines the architecture and operation of the Internet. The RFC documents outline and define the standard protocols and procedures for the Internet. The documents are listed on the World Wide Web at *www.ietf.org* and are mirrored and indexed at many other sites worldwide.

Basic Router Concepts

Large amounts of bandwidth can be provided easily and relatively inexpensively in a local area network (LAN). However, providing high bandwidth between a local network and the Internet can be very expensive. Because of this expense, Internet access is usually provided by a slower-speed wide-area network (WAN) link such as a cable or DSL modem. In order to make the best use of the slower WAN link, a mechanism must be in place for selecting and transmitting only the data traffic meant for the Internet. The function of selecting and forwarding this data is performed by a router.

What is a Router?

A router is a device that forwards traffic between networks based on network layer information in the data and on routing tables maintained by the router. In these routing tables, a router builds up a logical picture of the overall network by gathering and exchanging information with other routers in the network. Using this information, the router chooses the best path for forwarding network traffic.

Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connection they support. The FVS318 Broadband ProSafe VPN Firewall is a small office router that routes the IP protocol over a single-user broadband connection.

Routing Information Protocol

One of the protocols used by a router to build and maintain a picture of the network is the Routing Information Protocol (RIP). Using RIP, routers periodically update one another and check for changes to add to the routing table.

The FVS318 VPN Firewall supports both the older RIP-1 and the newer RIP-2 protocols. Among other improvements, RIP-2 supports subnet and multicast protocols. RIP is not required for most home applications.

IP Addresses and the Internet

Because TCP/IP networks are interconnected across the world, every machine on the Internet must have a unique address to make sure that transmitted data reaches the correct destination. Blocks of addresses are assigned to organizations by the Internet Assigned Numbers Authority (IANA). Individual users and small organizations may obtain their addresses either from the IANA or from an Internet service provider (ISP). You can contact IANA at www.iana.org.

The Internet Protocol (IP) uses a 32-bit address structure. The address is usually written in dot notation (also called dotted-decimal notation), in which each group of eight bits is written in decimal form, separated by decimal points.

For example, the following binary address:

```
11000011  00100010  00001100  00000111
```

is normally written as:

```
195.34.12.7
```

The latter version is easier to remember and easier to enter into your computer.

In addition, the 32 bits of the address are subdivided into two parts. The first part of the address identifies the network, and the second part identifies the host node or station on the network. The dividing point may vary depending on the address range and the application.

There are five standard classes of IP addresses. These address classes have different ways of determining the network and host sections of the address, allowing for different numbers of hosts on a network. Each address type begins with a unique bit pattern, which is used by the TCP/IP software to identify the address class. After the address class has been determined, the software can correctly identify the host section of the address. The follow figure shows the three main address classes, including network and host sections of the address for each address type.

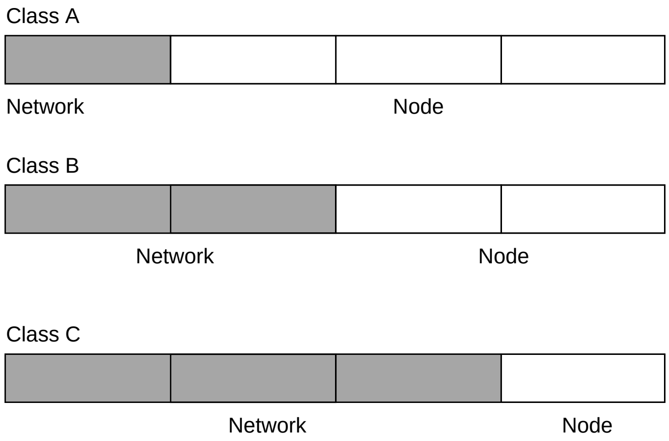


Figure B-1: Three Main Address Classes

The five address classes are:

- Class A
  Class A addresses can have up to 16,777,214 hosts on a single network. They use an eight-bit network number and a 24-bit node number. Class A addresses are in this range:

  `1.x.x.x to 126.x.x.x.`

- Class B
  Class B addresses can have up to 65,354 hosts on a network. A Class B address uses a 16-bit network number and a 16-bit node number. Class B addresses are in this range:

  `128.1.x.x to 191.254.x.x.`

- Class C
  Class C addresses can have 254 hosts on a network. Class C addresses use 24 bits for the network address and eight bits for the node. They are in this range:

  `192.0.1.x to 223.255.254.x.`

- Class D
  Class D addresses are used for multicasts (messages sent to many hosts). Class D addresses are in this range:

  `224.0.0.0 to 239.255.255.255.`

- Class E
  Class E addresses are for experimental use.

This addressing structure allows IP addresses to uniquely identify each physical network and each node on each physical network.

For each unique value of the network portion of the address, the base address of the range (host address of all zeros) is known as the network address and is not usually assigned to a host. Also, the top address of the range (host address of all ones) is not assigned, but is used as the broadcast address for simultaneously sending a packet to all hosts with the same network address.

Netmask

In each of the address classes previously described, the size of the two parts (network address and host address) is implied by the class. This partitioning scheme can also be expressed by a netmask associated with the IP address. A netmask is a 32-bit quantity that, when logically combined (using an AND operator) with an IP address, yields the network address. For instance, the netmasks for Class A, B, and C addresses are 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively.

For example, the address 192.168.170.237 is a Class C IP address whose network portion is the upper 24 bits. When combined (using an AND operator) with the Class C netmask, as shown here, only the network portion of the address remains:

```
11000000  10101000  10101010  11101101 (192.168.170.237)
```

combined with:

```
11111111  11111111  11111111  00000000 (255.255.255.0)
```

Equals:

```
11000000  10101000  10101010  00000000 (192.168.170.0)
```

As a shorter alternative to dotted-decimal notation, the netmask may also be expressed in terms of the number of ones from the left. This number is appended to the IP address, following a backward slash (/), as “/n.” In the example, the address could be written as 192.168.170.237/24, indicating that the netmask is 24 ones followed by 8 zeros.

Subnet Addressing

By looking at the addressing structures, you can see that even with a Class C address, there are a large number of hosts per network. Such a structure is an inefficient use of addresses if each end of a routed link requires a different network number. It is unlikely that the smaller office LANs would have that many devices. You can resolve this problem by using a technique known as subnet addressing.

Subnet addressing allows us to split one IP network address into smaller multiple physical networks known as subnetworks. Some of the node numbers are used as a subnet number instead. A Class B address gives us 16 bits of node numbers translating to 64,000 nodes. Most organizations do not use 64,000 nodes, so there are free bits that can be reassigned. Subnet addressing makes use of those bits that are free, as shown below.

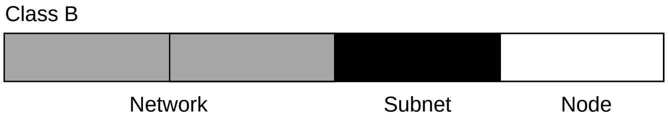


Figure B-2: Example of Subnetting a Class B Address

A Class B address can be effectively translated into multiple Class C addresses. For example, the IP address of 172.16.0.0 is assigned, but node addresses are limited to 255 maximum, allowing eight extra bits to use as a subnet address. The IP address of 172.16.97.235 would be interpreted as IP network address 172.16, subnet number 97, and node number 235. In addition to extending the number of addresses available, subnet addressing provides other benefits. Subnet addressing allows a network manager to construct an address scheme for the network by using different subnets for other geographical locations in the network or for other departments in the organization.

Although the preceding example uses the entire third octet for a subnet address, note that you are not restricted to octet boundaries in subnetting. To create more network numbers, you need only shift some bits from the host address to the network address. For instance, to partition a Class C network number (192.68.135.0) into two, you shift one bit from the host address to the network address. The new netmask (or subnet mask) is 255.255.255.128. The first subnet has network number 192.68.135.0 with hosts 192.68.135.1 to 129.68.135.126, and the second subnet has network number 192.68.135.128 with hosts 192.68.135.129 to 192.68.135.254.

➡	**Note:** The number 192.68.135.127 is not assigned because it is the broadcast address of the first subnet. The number 192.68.135.128 is not assigned because it is the network address of the second subnet.

The following table lists the additional subnet mask bits in dotted-decimal notation. To use the table, write down the original class netmask and replace the 0 value octets with the dotted-decimal value of the additional subnet bits. For example, to partition your Class C network with subnet mask 255.255.255.0 into 16 subnets (4 bits), the new subnet mask becomes 255.255.255.240.

Table B-1. Netmask Notation Translation Table for One Octet

Number of Bits	Dotted-Decimal Value
1	128
2	192
3	224
4	240
5	248
6	252
7	254
8	255

The following table displays several common netmask values in both the dotted-decimal and the mask length formats.

Table B-2. Netmask Formats

Dotted-Decimal	Masklength
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30

Table B-2. Netmask Formats

255.255.255.254	/31
255.255.255.255	/32

NETGEAR strongly recommends that you configure all hosts on a LAN segment to use the same netmask for the following reasons:

- So that hosts recognize local IP broadcast packets

  When a device broadcasts to its segment neighbors, it uses a destination address of the local network address with all ones for the host address. In order for this scheme to work, all devices on the segment must agree on which bits comprise the host address.

- So that a local router or bridge recognizes which addresses are local and which are remote

Private IP Addresses

If your local network is isolated from the Internet (for example, when using NAT), you can assign any IP addresses to the hosts without problems. However, the IANA has reserved the following three blocks of IP addresses specifically for private networks:

```
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255
```

NETGEAR recommends that you choose your private network number from this range. The DHCP server of the FVS318 VPN Firewall is preconfigured to automatically assign private addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines explained here. For more information about address assignment, refer to RFC 1597, *Address Allocation for Private Internets,* and RFC 1466, *Guidelines for Management of IP Address Space*. The Internet Engineering Task Force (IETF) publishes RFCs on its Web site at www.ietf.org.

Single IP Address Operation Using NAT

In the past, if multiple PCs on a LAN needed to access the Internet simultaneously, you had to obtain a range of IP addresses from the ISP. This type of Internet account is more costly than a single-address account typically used by a single user with a modem, rather than a router. The FVS318 VPN Firewall employs an address-sharing method called Network Address Translation (NAT). This method allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your ISP.

The router accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. The internal LAN IP addresses can be either private addresses or registered addresses. For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

The following figure illustrates a single IP address operation.

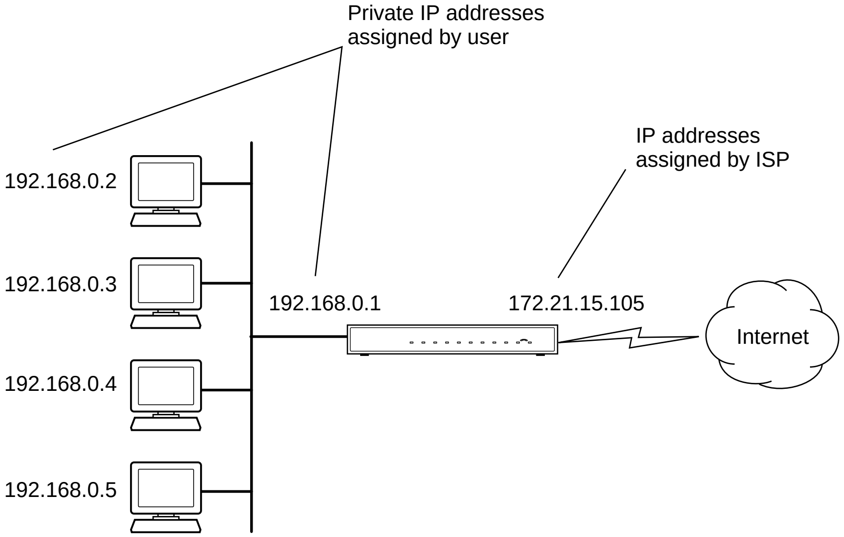


Figure B-3: Single IP Address Operation Using NAT

This scheme offers the additional benefit of firewall-like protection because the internal LAN addresses are not available to the Internet through the translated connection. All incoming inquiries are filtered out by the router. This filtering can prevent intruders from probing your system. However, using port forwarding, you can allow one PC (for example, a Web server) on your local network to be accessible to outside users.

MAC Addresses and Address Resolution Protocol

An IP address alone cannot be used to deliver data from one LAN device to another. To send data between LAN devices, you must convert the IP address of the destination device to its media access control (MAC) address. Each device on an Ethernet network has a unique MAC address, which is a 48-bit number assigned to each device by the manufacturer. The technique that associates the IP address with a MAC address is known as address resolution. Internet Protocol uses the Address Resolution Protocol (ARP) to resolve MAC addresses.

If a device sends data to another station on the network and the destination MAC address is not yet recorded, ARP is used. An ARP request is broadcast onto the network. All stations on the network receive and read the request. The destination IP address for the chosen station is included as part of the message so that only the station with this IP address responds to the ARP request. All other stations discard the request.

Related Documents

The station with the correct IP address responds with its own MAC address directly to the sending device. The receiving station provides the transmitting station with the required destination MAC address. The IP address data and MAC address data for each station are held in an ARP table. The next time data is sent, the address can be obtained from the address information in the table.

For more information about address assignment, refer to the IETF documents RFC 1597, *Address Allocation for Private Internets,* and RFC 1466, *Guidelines for Management of IP Address Space*.

For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

Domain Name Server

Many of the resources on the Internet can be addressed by simple descriptive names such as *www.NETGEAR.com*. This addressing is very helpful at the application level, but the descriptive name must be translated to an IP address in order for a user to actually contact the resource. Just as a telephone directory maps names to phone numbers, or as an ARP table maps IP addresses to MAC addresses, a domain name system (DNS) server maps descriptive names of network resources to IP addresses.

When a PC accesses a resource by its descriptive name, it first contacts a DNS server to obtain the IP address of the resource. The PC sends the desired message using the IP address. Many large organizations, such as ISPs, maintain their own DNS servers and allow their customers to use the servers to look up addresses.

IP Configuration by DHCP

When an IP-based local area network is installed, each PC must be configured with an IP address. If the PCs need to access the Internet, they should also be configured with a gateway address and one or more DNS server addresses. As an alternative to manual configuration, there is a method by which each PC on the network can automatically obtain this configuration information. A device on the network may act as a Dynamic Host Configuration Protocol (DHCP) server. The DHCP server stores a list or pool of IP addresses, along with other information (such as gateway and DNS addresses) that it may assign to the other devices on the network. The FVS318 VPN Firewall has the capacity to act as a DHCP server.

The FVS318 VPN Firewall also functions as a DHCP client when connecting to the ISP. The firewall can automatically obtain an IP address, subnet mask, DNS server addresses, and a gateway address if the ISP provides this information by DHCP.

Internet Security and Firewalls

When your LAN connects to the Internet through a router, an opportunity is created for outsiders to access or disrupt your network. A NAT router provides some protection because by the very nature of the Network Address Translation (NAT) process, the network behind the NAT router is shielded from access by outsiders on the Internet. However, there are methods by which a determined hacker can possibly obtain information about your network or at the least can disrupt your Internet access. A greater degree of protection is provided by a firewall router.

What is a Firewall?

A firewall is a device that protects one network from another, while allowing communication between the two. A firewall incorporates the functions of the NAT router, while adding features for dealing with a hacker intrusion or attack. Several known types of intrusion or attack can be recognized when they occur. When an incident is detected, the firewall can log details of the attempt, and can optionally send email to an administrator notifying them of the incident. Using information from the log, the administrator can take action with the ISP of the hacker. In some types of intrusions, the firewall can fend off the hacker by discarding all further packets from the hacker's IP address for a period of time.

Stateful Packet Inspection

Unlike simple Internet sharing routers, a firewall uses a process called stateful packet inspection to ensure secure firewall filtering to protect your network from attacks and intrusions. Since user-level applications such as FTP and Web browsers can create complex patterns of network traffic, it is necessary for the firewall to analyze groups of network connection states. Using Stateful Packet Inspection, an incoming packet is intercepted at the network layer and then analyzed for state-related information associated with all network connections. A central cache within the firewall keeps track of the state information associated with all network connections. All traffic passing through the firewall is analyzed against the state of these connections in order to determine whether or not it will be allowed to pass through or rejected.

Denial of Service Attack

A hacker may be able to prevent your network from operating or communicating by launching a Denial of Service (DoS) attack. The method used for such an attack can be as simple as merely flooding your site with more requests than it can handle. A more sophisticated attack may attempt to exploit some weakness in the operating system used by your router or gateway. Some operating systems can be disrupted by simply sending a packet with incorrect length information.

Ethernet Cabling

Although Ethernet networks originally used thick or thin coaxial cable, most installations currently use unshielded twisted pair (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. A normal straight-through UTP Ethernet cable follows the EIA568B standard wiring as described below in Table B-1

.

Table B-1. UTP Ethernet cable wiring, straight-through

Pin	Wire color	Signal
1	Orange/White	Transmit (Tx) +
2	Orange	Transmit (Tx) -
3	Green/White	Receive (Rx) +
4	Blue	
5	Blue/White	
6	Green	Receive (Rx) -
7	Brown/White	
8	Brown	

Category 5 Cable Quality

Category 5 distributed cable that meets ANSI/EIA/TIA-568-A building wiring standards can be a maximum of 328 feet (ft.) or 100 meters (m) in length, divided as follows:

20 ft. (6 m) between the hub and the patch panel (if used)

295 ft. (90 m) from the wiring closet to the wall outlet

10 ft. (3 m) from the wall outlet to the desktop device

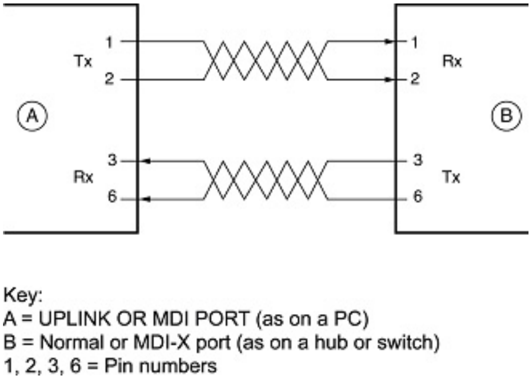
The patch panel and other connecting hardware must meet the requirements for 100 Mbps operation (Category 5). Only 0.5 inch (1.5 cm) of untwist in the wire pair is allowed at any termination point.

A twisted pair Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or Cat 5, by the Electronic Industry Association (EIA). This rating will be printed on the cable jacket. A Category 5 cable will meet specified requirements regarding loss and crosstalk. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

Inside Twisted Pair Cables

For two devices to communicate, the transmitter of each device must be connected to the receiver of the other device. The crossover function is usually implemented internally as part of the circuitry in the device. Computers and workstation adapter cards are usually media-dependent interface ports, called MDI or uplink ports. Most repeaters and switch ports are configured as media-dependent interfaces with built-in crossover ports, called MDI-X or normal ports. Auto Uplink technology automatically senses which connection, MDI or MDI-X, is needed and makes the right connection.

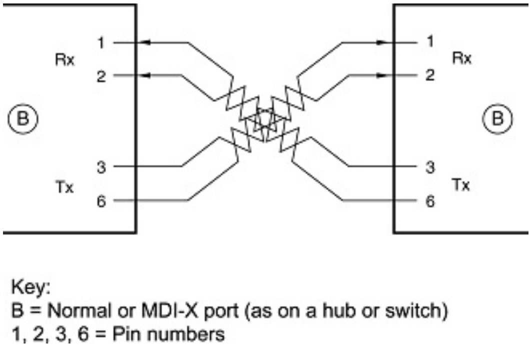
Figure B-4 illustrates straight-through twisted pair cable.



Key:
A = UPLINK OR MDI PORT (as on a PC)
B = Normal or MDI-X port (as on a hub or switch)
1, 2, 3, 6 = Pin numbers

Figure B-4: Straight-Through Twisted-Pair Cable

Figure B-5 illustrates crossover twisted pair cable.



Key:
B = Normal or MDI-X port (as on a hub or switch)
1, 2, 3, 6 = Pin numbers

Figure B-5: Crossover Twisted-Pair Cable

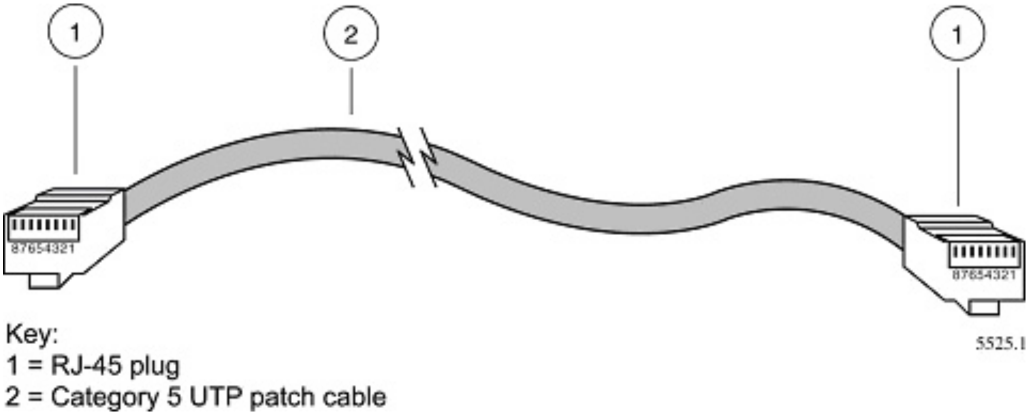


Figure B-6: Category 5 UTP Cable with Male RJ-45 Plug at Each End

Note: Flat “silver satin” telephone cable may have the same RJ-45 plug. However, using telephone cable results in excessive collisions, causing the attached port to be partitioned or disconnected from the network.

Uplink Switches, Crossover Cables, and MDI/MDIX Switching

In the wiring table above, the concept of transmit and receive are from the perspective of the PC, which is wired as Media Dependant Interface (MDI). In this wiring, the PC transmits on pins 1 and 2. At the hub, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X).

When connecting a PC to a PC, or a hub port to another hub port, the transmit pair must be exchanged with the receive pair. This exchange is done by one of two mechanisms. Most hubs provide an Uplink switch which will exchange the pairs on one port, allowing that port to be connected to another hub using a normal Ethernet cable. The second method is to use a crossover cable, which is a special cable in which the transmit and receive pairs are exchanged at one of the two cable connectors. Crossover cables are often unmarked as such, and must be identified by comparing the two connectors. Since the cable connectors are clear plastic, it is easy to place them side by side and view the order of the wire colors on each. On a straight-through cable, the color order will be the same on both connectors. On a crossover cable, the orange and blue pairs will be exchanged from one connector to the other.

The FVS318 VPN Firewall incorporates Auto Uplink™ technology (also called MDI/MDIX). Each LOCAL Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a normal connection (e.g. connecting to a PC) or an uplink connection (e.g. connecting to a router, switch, or hub). That port will then configure 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.

Appendix C
Preparing Your Network

This appendix describes how to prepare your network to connect to the Internet through the FVS318 Broadband ProSafe VPN Firewall and how to verify the readiness of broadband Internet service from an Internet service provider (ISP).

➡	**Note:** If an ISP technician configured your computer during the installation of a broadband modem, or if you configured it using instructions provided by your ISP, you may need to copy the current configuration information for use in the configuration of your firewall. Write down this information before reconfiguring your computers. Refer to "Obtaining ISP Configuration Information for Windows Computers" on page C-19 or "Obtaining ISP Configuration Information for Macintosh Computers" on page C-20 for further information.

Preparing Your Computers for TCP/IP Networking

Computers access the Internet using a protocol called TCP/IP (Transmission Control Protocol/ Internet Protocol). Each computer on your network must have TCP/IP installed and selected as its networking protocol. If a Network Interface Card (NIC) is already installed in your PC, then TCP/ IP is probably already installed as well.

Most operating systems include the software components you need for networking with TCP/IP:

- Windows® 95 or later includes the software components for establishing a TCP/IP network.
- Windows 3.1 does not include a TCP/IP component. You need to purchase a third-party TCP/ IP application package such as NetManage Chameleon.
- Macintosh Operating System 7 or later includes the software components for establishing a TCP/IP network.

- All versions of UNIX or Linux include TCP/IP components. Follow the instructions provided with your operating system or networking software to install TCP/IP on your computer.

In your IP network, each PC and the firewall must be assigned a unique IP addresses. Each PC must also have certain other IP configuration information such as a subnet mask (netmask), a domain name server (DNS) address, and a default gateway address. In most cases, you should install TCP/IP so that the PC obtains its specific network configuration information automatically from a DHCP server during bootup. For a detailed explanation of the meaning and purpose of these configuration items, refer to "Appendix B, "Networks, Routing, and Firewall Basics."

The FVS318 VPN Firewall is shipped preconfigured as a DHCP server. The firewall assigns the following TCP/IP configuration information automatically when the PCs are rebooted:

- PC or workstation IP addresses—192.168.0.2 through 192.168.0.254
- Subnet mask—255.255.255.0
- Gateway address (the firewall)—192.168.0.1

These addresses are part of the IETF-designated private address range for use in private networks.

Configuring Windows 95, 98, and Me for TCP/IP Networking

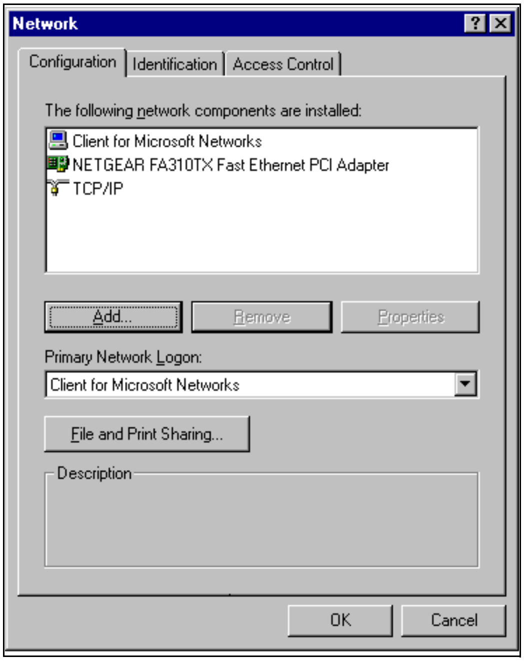
As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Install or Verify Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.

   The Network window opens, which displays a list of installed components:



Network

The following network components are installed:

Client for Microsoft Networks
NETGEAR FA310TX Fast Ethernet PCI Adapter
TCP/IP

Primary Network Logon:
Client for Microsoft Networks

Description

You must have an Ethernet adapter, the TCP/IP protocol, and Client for Microsoft Networks.

➡	**Note:** It is not necessary to remove any other network components shown in the Network window in order to install the adapter, TCP/IP, or Client for Microsoft Networks.

If you need to install a new adapter, follow these steps:

a. Click the Add button.

b. Select Adapter, and then click Add.

c. Select the manufacturer and model of your Ethernet adapter, and then click OK.

If you need TCP/IP:

a. Click the Add button.

b. Select Protocol, and then click Add.

c. Select Microsoft.

d. Select TCP/IP, and then click OK.

If you need Client for Microsoft Networks:

a. Click the Add button.

b. Select Client, and then click Add.

c. Select Microsoft.

d. Select Client for Microsoft Networks, and then click OK.

3. Restart your PC for the changes to take effect.

Enabling DHCP to Automatically Configure TCP/IP Settings

After the TCP/IP protocol components are installed, each PC must be assigned specific information about itself and resources that are available on its network. The simplest way to configure this information is to allow the PC to obtain the information from a DHCP server in the network.

You will find there are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP.

The following steps will walk you through the configuration process for each of these versions of Windows.

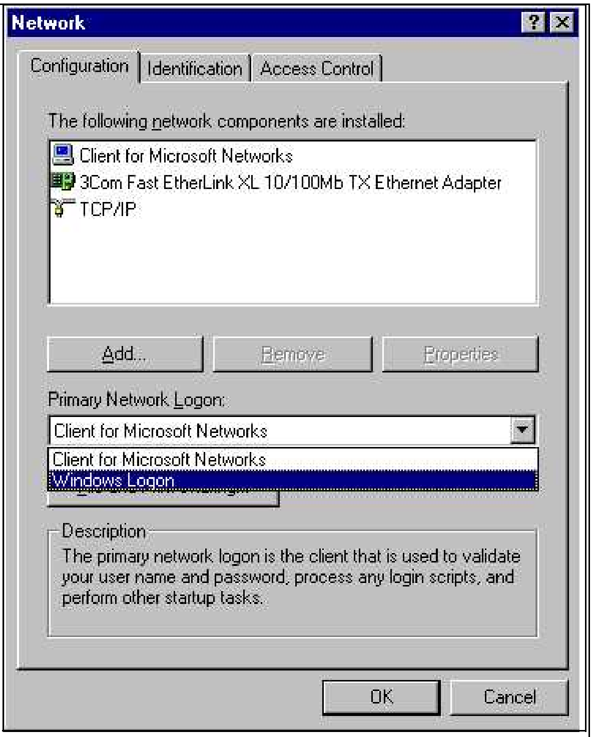
1

Locate your **Network Neighborhood** icon.

- If the Network Neighborhood icon is on the Windows desktop, position your mouse pointer over it and right-click your mouse button.
- If the icon is not on the desktop,
  - Click **Start** on the task bar located at the bottom left of the window.
  - Choose **Settings**, and then **Control Panel**.
  - Locate the **Network Neighborhood** icon and click on it. This will open the Network panel as shown below.

2

- Verify the following settings as shown:
  - Client for Microsoft Network exists
  - Ethernet adapter is present
  - TCP/IP is present
  - **Primary Network Logon** is set to Windows logon
- Click on the **Properties** button. The following TCP/IP Properties window will display.



Network

Configuration | Identification | Access Control

The following network components are installed:

Client for Microsoft Networks
3Com Fast EtherLink XL 10/100Mb TX Ethernet Adapter
TCP/IP

Primary Network Logon:

Client for Microsoft Networks

Client for Microsoft Networks
Windows Logon

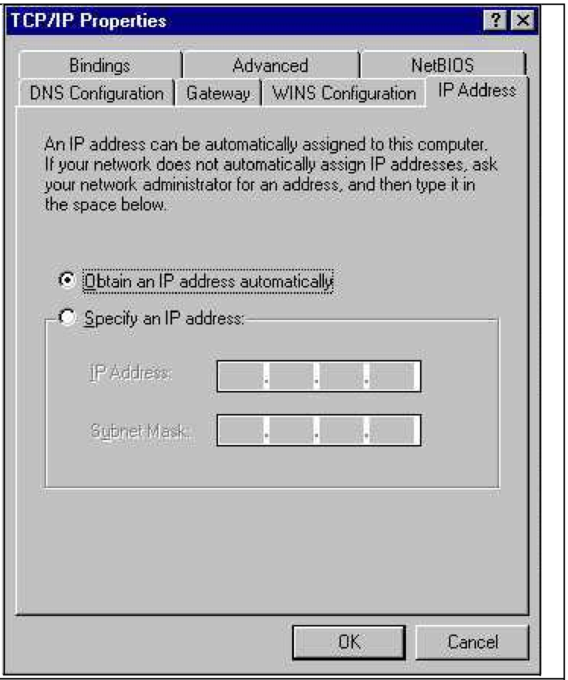
Description
The primary network logon is the client that is used to validate your user name and password, process any login scripts, and perform other startup tasks.

3

- By default, the **IP Address** tab is open on this window.
- Verify the following:

  Obtain an IP address automatically is selected. If not selected, click in the radio button to the left of it to select it. This setting is required to enable the DHCP server to automatically assign an IP address.
- Click **OK** to continue.
- Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.



TCP/IP Properties

An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

Subnet Mask: . . .

Selecting Windows' Internet Access Method

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Internet Options icon.
3. Select "I want to set up my Internet connection manually" or "I want to connect through a Local Area Network" and click Next.
4. Select "I want to connect through a Local Area Network" and click Next.
5. Uncheck all boxes in the LAN Internet Configuration screen and click Next.
6. Proceed to the end of the Wizard.

Verifying TCP/IP Properties

After your PC is configured and has rebooted, you can check the TCP/IP configuration using the utility *winipcfg.exe*:

1. On the Windows taskbar, click the Start button, and then click Run.

2. Type `winipcfg`, and then click OK.

   The IP Configuration window opens, which lists (among other things), your IP address, subnet mask, and default gateway.

3. From the drop-down box, select your Ethernet adapter.

   The window is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends for connecting through a router or gateway:

   - The IP address is between 192.168.0.2 and 192.168.0.254
   - The subnet mask is 255.255.255.0
   - The default gateway is 192.168.0.1

Configuring Windows NT4, 2000 or XP for IP Networking

As part of the PC preparation process, you may need to install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Install or Verify Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network and Dialup Connections icon.
3. If an Ethernet adapter is present in your PC, you should see an entry for Local Area Connection. Double-click that entry.
4. Select Properties.
5. Verify that ‘Client for Microsoft Networks’ and ‘Internet Protocol (TCP/IP)’ are present. If not, select Install and add them.
6. Select ‘Internet Protocol (TCP/IP)’, click Properties, and verify that “Obtain an IP address automatically is selected.
7. Click OK and close all Network and Dialup Connections windows.
8. Then, restart your PC.

DHCP Configuration of TCP/IP in Windows XP, 2000, or NT4

You will find there are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP.

The following steps will walk you through the configuration process for each of these versions of Windows.

DHCP Configuration of TCP/IP in Windows XP

1

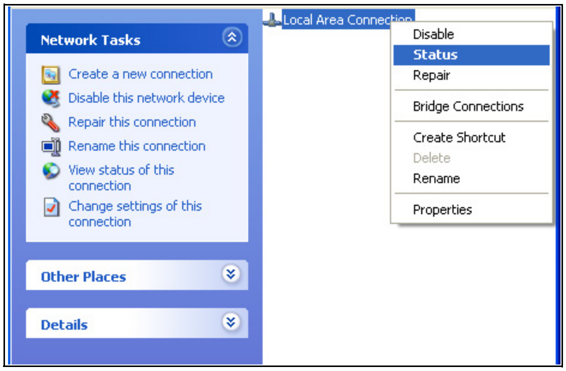
Open your **Network Connections** window.

- Select **Network** from the Windows XP new Start Menu.
- Click the **Network Connections** link on the Network Tasks list.

2

- Now the Network Connection window displays.

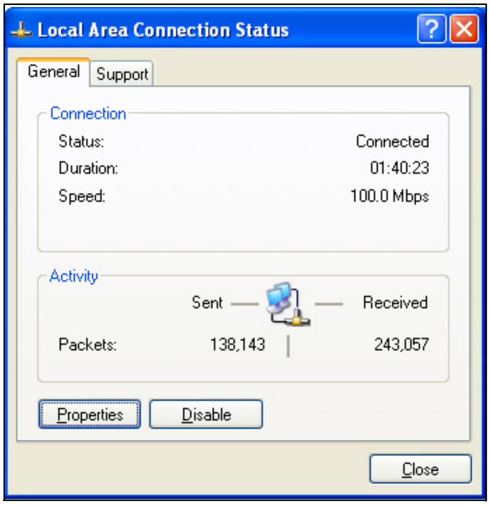
  The Connections List that shows all the network connections set up on the PC, located to the right of the window.
- Right-click on the **Connection** you will use and choose **Status**.



3

- Now you should be at the Local Area Network Connection Status window. This box displays the connection status, duration, speed, and activity statistics.

  Administrator logon access rights are needed to use this window.
- Click the **Properties** button to view details about the connection.



Local Area Connection Status

Connection

Status: Connected

Duration: 01:40:23

Speed: 100.0 Mbps

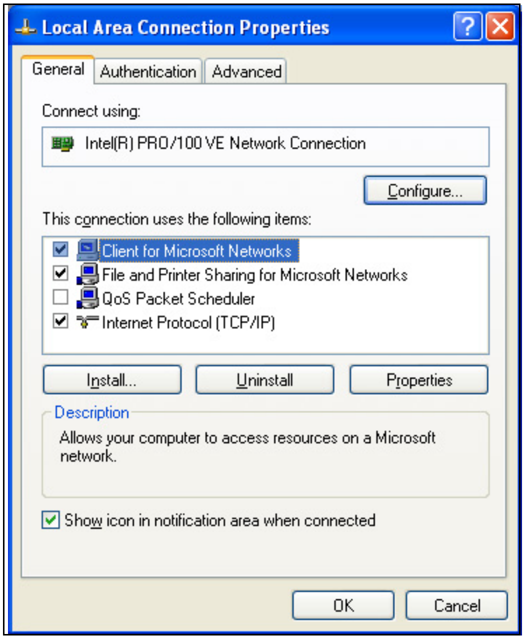
Activity

Sent — — Received

Packets: 138,143 | 243,057

4

- The TCP/IP details are presented on the Support tab page.
- Select **Internet Protocol,** and click the **Properties** button to view the configuration information**.**



Local Area Connection Properties

Connect using:

Intel(R) PRO/100 VE Network Connection

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☐ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

Allows your computer to access resources on a Microsoft network.

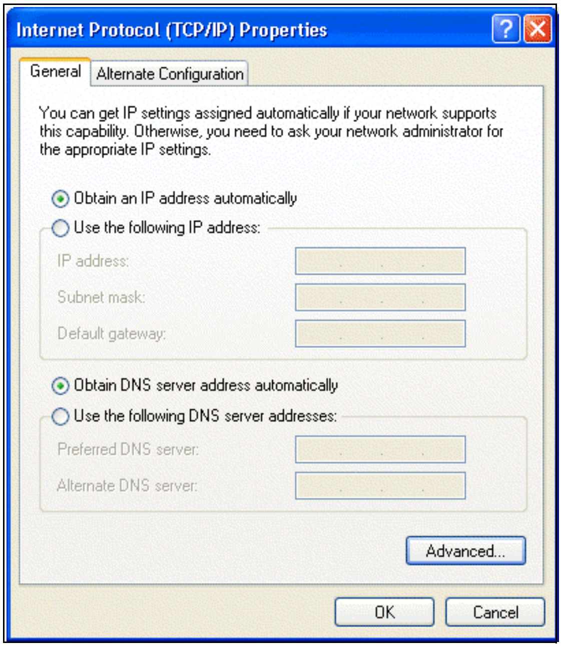
☑ Show icon in notification area when connected

5

- Verify that the **Obtain an IP address automatically** radio button is selected.
- Verify that **Obtain DNS server address automatically** radio button is selected.
- Click the **OK** button.

This completes the DHCP configuration of TCP/IP in Windows XP.

Repeat these steps for each PC with this version of Windows on your network.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

DHCP Configuration of TCP/IP in Windows 2000

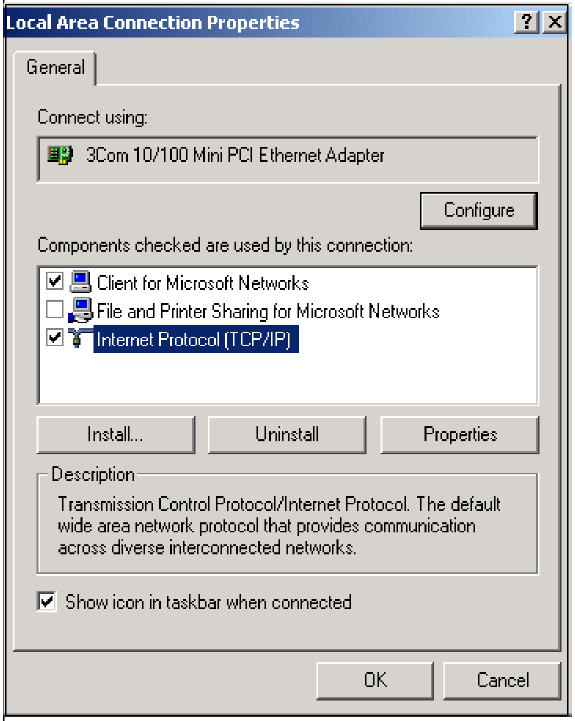
Once again, after you have installed the network card, TCP/IP for Windows 2000 is configured. TCP/IP should be added by default and set to DHCP without your having to configure it. However, if there are problems, follow these steps to configure TCP/IP with DHCP for Windows 2000.

1

- Click on the **My Network Places** icon on the Windows desktop. This will bring up a window called Network and Dial-up Connections.
- Right click on **Local Area Connection** and select **Properties**.

2

- The **Local Area Connection Properties** dialog box appears.
- Verify that you have the correct Ethernet card selected in the **Connect using:** box.
- Verify that at least the following two items are displayed and selected in the box of "Components checked are used by this connection:"
  - – Client for Microsoft Networks and
  - – Internet Protocol (TCP/IP).



Local Area Connection Properties

General

Connect using:

3Com 10/100 Mini PCI Ethernet Adapter

Components checked are used by this connection:

☑ Client for Microsoft Networks
☐ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

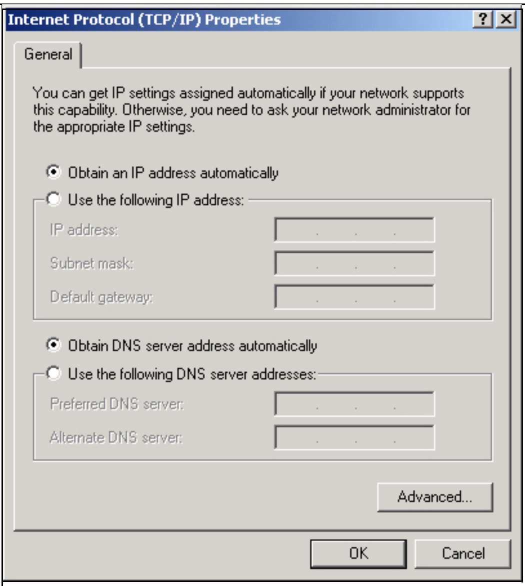
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in taskbar when connected

3

- With Internet Protocol (TCP/IP) selected, click on **Properties** button to open the Internet Protocol (TCP/IP) Properties dialogue box.
- Verify that
  - **Obtain an IP address automatically** is selected.
  - **Obtain DNS server address automatically** is selected.
- Click **OK** to return to Local Area Connection Properties.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

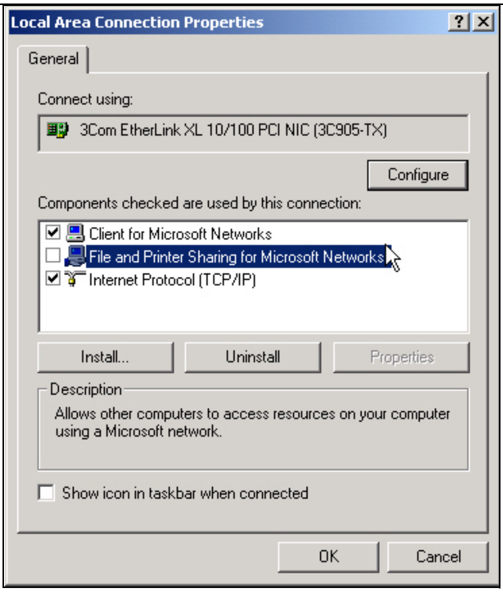
Preferred DNS server:

Alternate DNS server:

4

- Click **OK** again to complete the configuration process for Windows 2000.
- Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.



Local Area Connection Properties

General

Connect using:

3Com EtherLink XL 10/100 PCI NIC (3C905-TX)

Components checked are used by this connection:

☑ Client for Microsoft Networks

☐ File and Printer Sharing for Microsoft Networks

☑ Internet Protocol (TCP/IP)

Description

Allows other computers to access resources on your computer using a Microsoft network.

☐ Show icon in taskbar when connected

DHCP Configuration of TCP/IP in Windows NT4

Once you have installed the network card, you need to configure the TCP/IP environment for Windows NT 4.0. Follow this procedure to configure TCP/IP with DHCP in Windows NT 4.0.

1

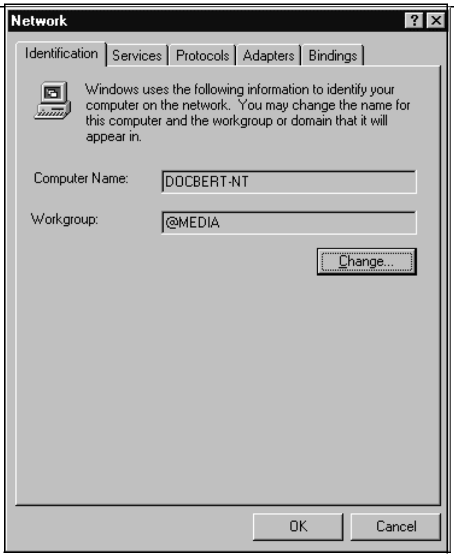
- Choose **Settings** from the Start Menu, and then select **Control Panel**. This will display Control Panel window.

2

- Double-click the **Network** icon in the Control Panel window.

  The Network panel will display.

- Select the **Protocols** tab to continue.



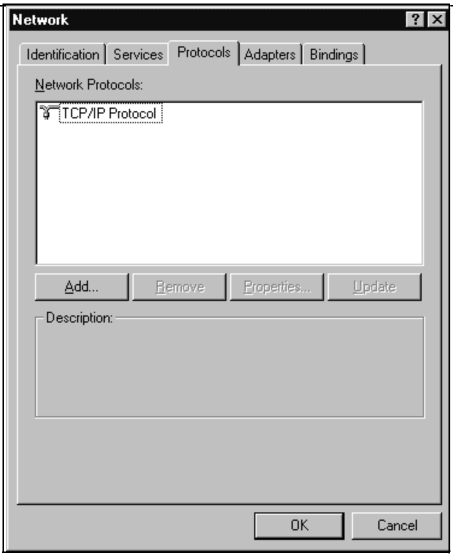
Windows uses the following information to identify your computer on the network. You may change the name for this computer and the workgroup or domain that it will appear in.

Computer Name: DOCBERT-NT

Workgroup: @MEDIA

3

- Highlight the **TCP/IP Protocol** in the **Network Protocols** box, and click on the **Properties** button.

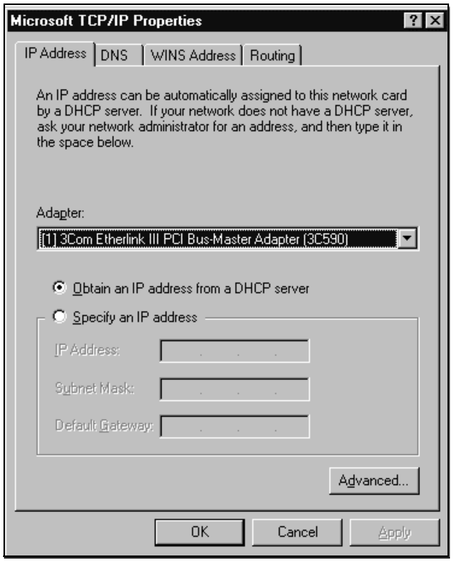


Network Protocols:
TCP/IP Protocol

4

- The **TCP/IP Properties** dialog box now displays.
- Click the **IP Address** tab.
- Select the radio button marked **Obtain an IP address from a DHCP server.**
- Click **OK**. This completes the configuration of TCP/IP in Windows NT.
- Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.



An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.

Adapter:
[1] 3Com Etherlink III PCI Bus-Master Adapter (3C590)

● Obtain an IP address from a DHCP server

○ Specify an IP address

IP Address: . . .

Subnet Mask: . . .

Default Gateway: . . .

Verifying TCP/IP Properties for Windows XP, 2000, and NT4

To check your PC’s TCP/IP configuration:

1. On the Windows taskbar, click the Start button, and then click Run.

   The Run window opens.

2. Type **`cmd`** and then click OK.

   A command window opens

3. Type **`ipconfig /all`**

   Your IP Configuration information will be listed, and should match the values below if you are using the default TCP/IP settings that NETGEAR recommends for connecting through a router or gateway:

   - The IP address is between 192.168.0.2 and 192.168.0.254
   - The subnet mask is 255.255.255.0
   - The default gateway is 192.168.0.1

4. Type **`exit`**

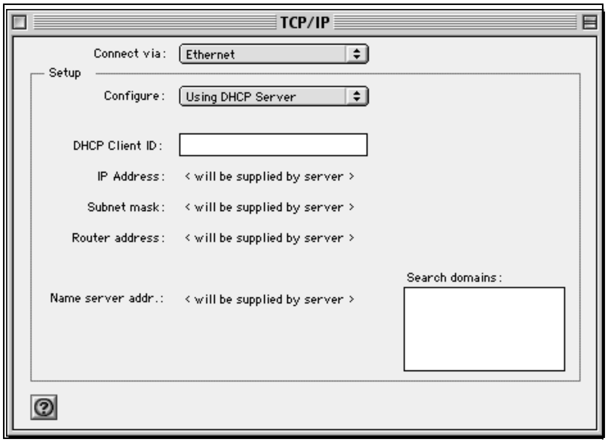
Configuring the Macintosh for TCP/IP Networking

Beginning with Macintosh Operating System 7, TCP/IP is already installed on the Macintosh. On each networked Macintosh, you will need to configure TCP/IP to use DHCP.

MacOS 8.6 or 9.x

1. From the Apple menu, select Control Panels, then TCP/IP.

The TCP/IP Control Panel opens:



Connect via: Ethernet

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Name server addr.: < will be supplied by server >

2. From the “Connect via” box, select your Macintosh’s Ethernet interface.
3. From the “Configure” box, select Using DHCP Server.

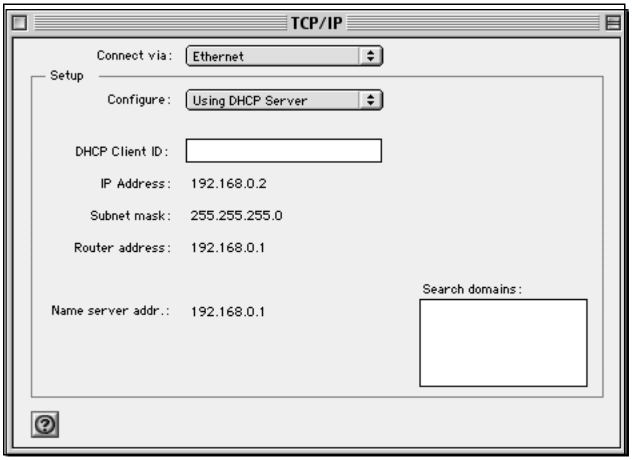
   You can leave the DHCP Client ID box empty.
4. Close the TCP/IP Control Panel.
5. Repeat this for each Macintosh on your network.

MacOS X

1. From the Apple menu, choose System Preferences, then Network.
2. If not already selected, select Built-in Ethernet in the Configure list.
3. If not already selected, Select Using DHCP in the TCP/IP tab.
4. Click Save.

Verifying TCP/IP Properties for Macintosh Computers

After your Macintosh is configured and has rebooted, you can check the TCP/IP configuration by returning to the TCP/IP Control Panel. From the Apple menu, select Control Panels, then TCP/IP.



TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: 192.168.0.2

Subnet mask: 255.255.255.0

Router address: 192.168.0.1

Search domains:

Name server addr.: 192.168.0.1

The panel is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

- The IP Address is between 192.168.0.2 and 192.168.0.254
- The Subnet mask is 255.255.255.0
- The Router address is 192.168.0.1

If you do not see these values, you may need to restart your Macintosh or you may need to switch the “Configure” setting to a different option, then back again to “Using DHCP Server”.

Verifying the Readiness of Your Internet Account

For broadband access to the Internet, you need to contract with an Internet service provider (ISP) for a single-user Internet access account using a cable modem or DSL modem. This modem must be a separate physical box (not a card) and must provide an Ethernet port intended for connection to a Network Interface Card (NIC) in a computer. Your firewall does not support a USB-connected broadband modem.

For a single-user Internet account, your ISP supplies TCP/IP configuration information for one computer. With a typical account, much of the configuration information is dynamically assigned when your PC is first booted up while connected to the ISP, and you will not need to know that dynamic information.

In order to share the Internet connection among several computers, your firewall takes the place of the single PC, and you need to configure it with the TCP/IP information that the single PC would normally use. When the firewall's Internet port is connected to the broadband modem, the firewall appears to be a single PC to the ISP. The firewall then allows the PCs on the local network to masquerade as the single PC to access the Internet through the broadband modem. The method used by the firewall to accomplish this is called Network Address Translation (NAT) or IP masquerading.

Are Login Protocols Used?

Some ISPs require a special login protocol, in which you must enter a login name and password in order to access the Internet. If you normally log in to your Internet account by running a program such as WinPOET or EnterNet, then your account uses PPP over Ethernet (PPPoE).

When you configure your router, you will need to enter your login name and password in the router's configuration menus. After your network and firewall are configured, the firewall will perform the login task when needed, and you will no longer need to run the login program from your PC. It is not necessary to uninstall the login program.

What Is Your Configuration Information?

More and more, ISPs are dynamically assigning configuration information. However, if your ISP does not dynamically assign configuration information but instead used fixed configurations, your ISP should have given you the following basic information for your account:

- An IP address and subnet mask
- A gateway IP address, which is the address of the ISP's router
- One or more domain name server (DNS) IP addresses
- Host name and domain suffix

  For example, your account's full server names may look like this:

  `mail.xxx.yyy.com`

  In this example, the domain suffix is `xxx.yyy.com`.

If any of these items are dynamically supplied by the ISP, your firewall automatically acquires them.

If an ISP technician configured your PC during the installation of the broadband modem, or if you configured it using instructions provided by your ISP, you need to copy the configuration information from your PC's Network TCP/IP Properties window or Macintosh TCP/IP Control Panel before reconfiguring your PC for use with the firewall. These procedures are described next.

Obtaining ISP Configuration Information for Windows Computers

As mentioned above, you may need to collect configuration information from your PC so that you can use this information when you configure the FVS318 VPN Firewall. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the firewall for Internet access:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.

   The Network window opens, which displays a list of installed components.
3. Select TCP/IP, and then click Properties.

   The TCP/IP Properties dialog box opens.
4. Select the IP Address tab.

   If an IP address and subnet mask are shown, write down the information. If an address is present, your account uses a fixed (static) IP address. If no address is present, your account uses a dynamically-assigned IP address. Click “Obtain an IP address automatically”.
5. Select the Gateway tab.

If an IP address appears under Installed Gateways, write down the address. This is the ISP's gateway address. Select the address and then click Remove to remove the gateway address.

6. Select the DNS Configuration tab.

   If any DNS server addresses are shown, write down the addresses. If any information appears in the Host or Domain information box, write it down. Click Disable DNS.

7. Click OK to save your changes and close the TCP/IP Properties dialog box.

   You are returned to the Network window.

8. Click OK.

9. Reboot your PC at the prompt. You may also be prompted to insert your Windows CD.

Obtaining ISP Configuration Information for Macintosh Computers

As mentioned above, you may need to collect configuration information from your Macintosh so that you can use this information when you configure the FVS318 VPN Firewall. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the firewall for Internet access:

1. From the Apple menu, select Control Panels, then TCP/IP.

   The TCP/IP Control Panel opens, which displays a list of configuration settings. If the "Configure" setting is "Using DHCP Server", your account uses a dynamically-assigned IP address. In this case, close the Control Panel and skip the rest of this section.

2. If an IP address and subnet mask are shown, write down the information.

3. If an IP address appears under Router address, write down the address. This is the ISP's gateway address.

4. If any Name Server addresses are shown, write down the addresses. These are your ISP's DNS addresses.

5. If any information appears in the Search domains information box, write it down.

6. Change the "Configure" setting to "Using DHCP Server".

7. Close the TCP/IP Control Panel.

Restarting the Network

Once you’ve set up your computers to work with the firewall, you must reset the network for the devices to be able to communicate correctly. Restart any computer that is connected to the firewall.

1. Turn off the modem, router, and PCs.
2. Turn on the modem.
3. Wait until the indicator lights on the modem show that it is synchronized with the broadband network.
4. Turn on the router and wait until the TEST LED turns off.
5. Restart the PCs.

After configuring all of your computers for TCP/IP networking and restarting them, and connecting them to the local network of your FVS318 VPN Firewall, you are ready to access and configure the firewall.

Appendix D
Virtual Private Networking

There have been many improvements in the Internet including Quality of Service, network performance, and inexpensive technologies, such as DSL. But one of the most important advances has been in 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.

What is a VPN?

A VPN is a shared network where private data is segmented from other traffic so that only the intended recipient has access. The term VPN was originally used to describe a secure connection over the Internet. Today, however, VPN is also used to describe private networks, such as Frame Relay, Asynchronous Transfer Mode (ATM), and Multiprotocol Label Switching (MPLS).

A key aspect of data security is that the data flowing across the network is protected by encryption technologies. Private networks lack data security, which allows data attackers to tap directly into the network and read the data. IPSec-based VPNs use encryption to provide data security, which increases the network's resistance to data tampering or theft.

IPSec-based VPNs can be created over any type of IP network, including the Internet, Frame Relay, ATM, and MPLS, but only the Internet is ubiquitous and inexpensive.

VPNs are traditionally used for:

- **Intranets:** Intranets connect an organization's locations. These locations range from the headquarters offices, to branch offices, to a remote employee's home. Often this connectivity is used for e-mail and for sharing applications and files. While Frame Relay, ATM, and MPLS accomplish these tasks, the shortcomings of each limits connectivity. The cost of connecting home users is also very expensive compared to Internet-access technologies, such as DSL or cable. Because of this, organizations are moving their networks to the Internet, which is inexpensive, and using IPSec to create these networks.

- **Remote Access:** Remote access enables telecommuters and mobile workers to access e-mail and business applications. A dial-up connection to an organization's modem pool is one method of access for remote workers, but is expensive because the organization must pay the associated long distance telephone and service costs. Remote access VPNs greatly reduce expenses by enabling mobile workers to dial a local Internet connection and then set up a secure IPSec-based VPN communications to their organization.
- **Extranets**: Extranets are secure connections between two or more organizations. Common uses for extranets include supply-chain management, development partnerships, and subscription services. These undertakings can be difficult using legacy network technologies due to connection costs, time delays, and access availability. IPSec-based VPNs are ideal for extranet connections. IPSec-capable devices can be quickly and inexpensively installed on existing Internet connections.

What Is IPSec and How Does It Work?

IPSec is an Internet Engineering Task Force (IETF) standard suite of protocols that provides data authentication, integrity, and confidentiality as data is transferred between communication points across IP networks. IPSec provides data security at the IP packet level. A packet is a data bundle that is organized for transmission across a network, and includes a header and payload (the data in the packet). IPSec emerged as a viable network security standard because enterprises wanted to ensure that data could be securely transmitted over the Internet. IPSec protects against possible security exposures by protecting data while in while in transit.

IPSec Security Features

IPSec is the most secure method commercially available for connecting network sites. IPSec was designed to provide the following security features when transferring packets across networks:

- **Authentication:** Verifies that the packet received is actually from the claimed sender.
- **Integrity:** Ensures that the contents of the packet did not change in transit.
- **Confidentiality:** Conceals the message content through encryption.

IPSec Components

IPSec contains the following elements:

- **Encapsulating Security Payload (ESP)**: Provides confidentiality, authentication, and integrity.
- **Authentication Header (AH)**: Provides authentication and integrity.
- **Internet Key Exchange (IKE)**: Provides key management and Security Association (SA) management.

Encapsulating Security Payload (ESP)

ESP provides authentication, integrity, and confidentiality, which protect against data tampering and, most importantly, provide message content protection.

IPSec provides an open framework for implementing industry standard algorithms, such as SHA and MD5. The algorithms IPSec uses produce a unique and unforgeable identifier for each packet, which is a data equivalent of a fingerprint. This fingerprint allows the device to determine if a packet has been tampered with. Furthermore, packets that are not authenticated are discarded and not delivered to the intended receiver.

ESP also provides all encryption services in IPSec. Encryption translates a readable message into an unreadable format to hide the message content. The opposite process, called decryption, translates the message content from an unreadable format to a readable message. Encryption/ decryption allows only the sender and the authorized receiver to read the data. In addition, ESP has an option to perform authentication, called ESP authentication. Using ESP authentication, ESP provides authentication and integrity for the payload and not for the IP header.

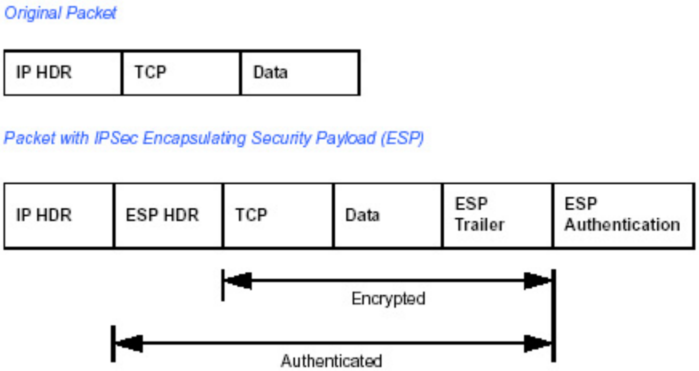


Figure D-1: Original packet and packet with IPSec Encapsulated Security Payload

The ESP header is inserted into the packet between the IP header and any subsequent packet contents. However, because ESP encrypts the data, the payload is changed. ESP does not encrypt the ESP header, nor does it encrypt the ESP authentication.

Authentication Header (AH)

AH provides authentication and integrity, which protect against data tampering, using the same algorithms as ESP. AH also provides optional anti-replay protection, which protects against unauthorized retransmission of packets. The authentication header is inserted into the packet between the IP header and any subsequent packet contents. The payload is not touched.

Although AH protects the packet's origin, destination, and contents from being tampered with, the identity of the sender and receiver is known. In addition, AH does not protect the data's confidentiality. If data is intercepted and only AH is used, the message contents can be read. ESP protects data confidentiality. For added protection in certain cases, AH and ESP can be used together. In the following table, IP HDR represents the IP header and includes both source and destination IP addresses.

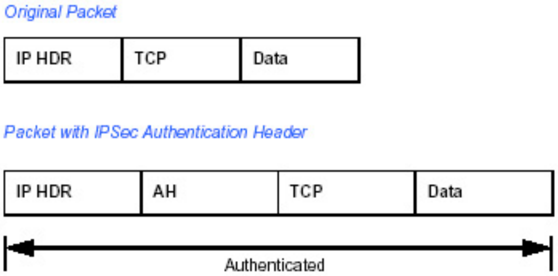


Figure D-2: Original packet and packet with IPSec Authentication Header

IKE Security Association

IPSec introduces the concept of the Security Association (SA). An SA is a logical connection between two devices transferring data. An SA provides data protection for unidirectional traffic by using the defined IPSec protocols. An IPSec tunnel typically consists of two unidirectional SAs, which together provide a protected, full-duplex data channel.

The SAs allow an enterprise to control exactly what resources may communicate securely, according to security policy. To do this an enterprise can set up multiple SAs to enable multiple secure VPNs, as well as define SAs within the VPN to support different departments and business partners.

Mode

SAs operate using modes. A mode is the method in which the IPSec protocol is applied to the packet. IPSec can be used in tunnel mode or transport mode. Typically, the tunnel mode is used for gateway-to-gateway IPSec tunnel protection, while transport mode is used for host-to-host IPSec tunnel protection. A gateway is a device that monitors and manages incoming and outgoing network traffic and routes the traffic accordingly. A host is a device that sends and receives network traffic.

- **Transport Mode:** The transport mode IPSec implementation encapsulates only the packet's payload. The IP header is not changed. After the packet is processed with IPSec, the new IP packet contains the old IP header (with the source and destination IP addresses unchanged) and the processed packet payload. Transport mode does not shield the information in the IP header; therefore, an attacker can learn where the packet is coming from and where it is going to. The previous packet diagrams show a packet in transport mode.
- **Tunnel Mode:** The tunnel mode IPSec implementation encapsulates the entire IP packet. The entire packet becomes the payload of the packet that is processed with IPSec. A new IP header is created that contains the two IPSec gateway addresses. The gateways perform the encapsulation/decapsulation on behalf of the hosts. Tunnel mode ESP prevents an attacker from analyzing the data and deciphering it, as well as knowing who the packet is from and where it is going.

Note: AH and ESP can be used in both transport mode or tunnel mode.

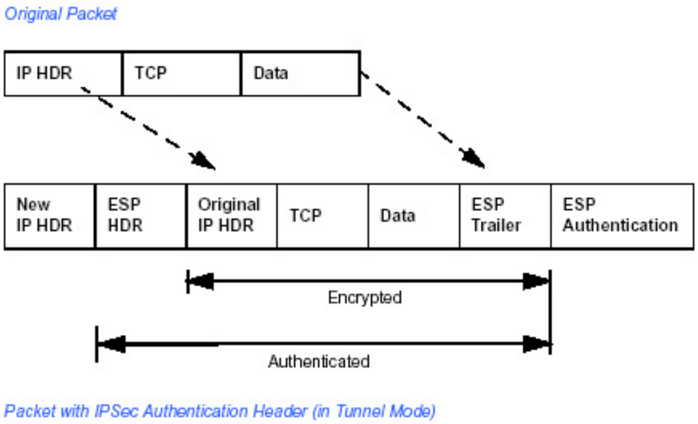


Figure D-3: Original packet and packet with IPSec ESP in Tunnel mode

Key Management

IPSec uses the Internet Key Exchange (IKE) protocol to facilitate and automate the SA setup and the exchange of keys between parties transferring data. Using keys ensures that only the sender and receiver of a message can access it.

IPSec requires that keys be re-created, or refreshed, frequently so that the parties can communicate securely with each other. IKE manages the process of refreshing keys; however, a user can control the key strength and the refresh frequency. Refreshing keys on a regular basis ensures data confidentiality between sender and receiver.

Understand the Process Before You Begin

This document provides case studies on how to configure secure IPSec VPN tunnels. This document assumes the reader has a working knowledge of NETGEAR management systems.

NETGEAR is a member of the VPN Consortium, a group formed to facilitate IPSec VPN vendor interoperability. The VPN Consortium has developed specific scenarios to aid system administrators in the often confusing process of connecting two different vendor implementations of the IPSec standard. The case studies in this TechNote follow the addressing and configuration mechanics defined by the VPN Consortium. Additional information regarding inter-vendor interoperability may be found at *http://www.vpnc.org/interop.html*.

It is a good idea to gather all the necessary information required to establish a VPN before you begin the configuration process. You should understand 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. Try to understand any incompatibilities before you begin, so that you minimize any potential complications which may arise from normal firewall or WAN processes.

If you are not a full-time system administrator, it is a good idea to familiarize yourself with the mechanics of a VPN. The brief description in this TechNote will help. Other good sources include:

- The NETGEAR VPN Tutorial – http://www.netgear.com/planetvpn/pvpn_2.html
- The VPN Consortium – http://www.vpnc.org/
- The VPN bibliography in “Additional Reading“ on page D-11.

VPN Process Overview

Even though IPSec is standards-based, each vendor has its own set of terms and procedures for implementing the standard. Because of these differences, it may be a good idea to review some of the terms and the generic processes for connecting two gateways before diving into to the specifics.

Network Interfaces and Addresses

The VPN gateway is aptly named because it functions as a "gatekeeper" for each of the computers connected on the Local Area Network behind it.

In most cases, each Gateway will have a "public" facing address (WAN side) and a "private" facing address (LAN side). These addresses are referred to as the "network interface" in documentation regarding the construction of VPN communication. Please note that the addresses used in the example.

Interface Addressing

This TechNote uses example addresses provided the VPN Consortium. It is important to understand that you will be using addresses specific to the devices that you are attempting to connect via IPSec VPN.

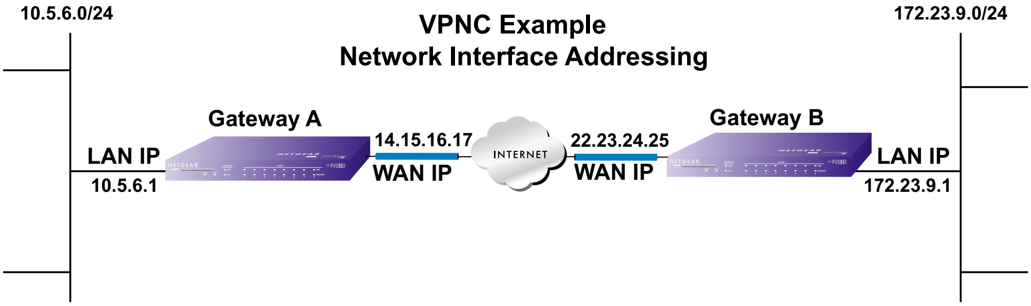


Figure D-4: VPNC Example Network Interface Addressing

It is also important to make sure the addresses do not overlap or conflict. That is, each set of addresses should be separate and distinct.

Table D-1. WAN (Internet/Public) and LAN (Internal/Private) Addressing

Gateway	LAN or WAN	VPNC Example Address
Gateway A	LAN (Private)	10.5.6.1
Gateway A	WAN (Public)	14.15.16.17
Gateway B	LAN (Private)	22.23.24.25
Gateway B	WAN (Public)	172.23.9.1

It will also be important to know the subnet mask of both gateway LAN Connections. Use the worksheet in Appendix A to gather the necessary address and subnet mask information to aid in the configuration and troubleshooting process.

Table D-2. Subnet Addressing

Gateway	LAN or WAN	Interface Name	Example Subnet Mask
Gateway A	LAN (Private)	Subnet Mask A	255.255.255.0
Gateway B	LAN (Private)	Subnet Mask B	255.255.255.0

Firewalls

It is important to understand that many gateways are also firewalls. VPN tunnels cannot function properly if firewall settings disallow all incoming traffic. Please refer to the firewall instructions for both gateways to understand how to open specific protocols, ports, and addresses that you intend to allow.

Setting Up a VPN Tunnel Between Gateways

A SA, frequently called a tunnel, is the set of information that allows two entities (networks, PCs, routers, firewalls, gateways) to “trust each other” and communicate securely as they pass information over the Internet.

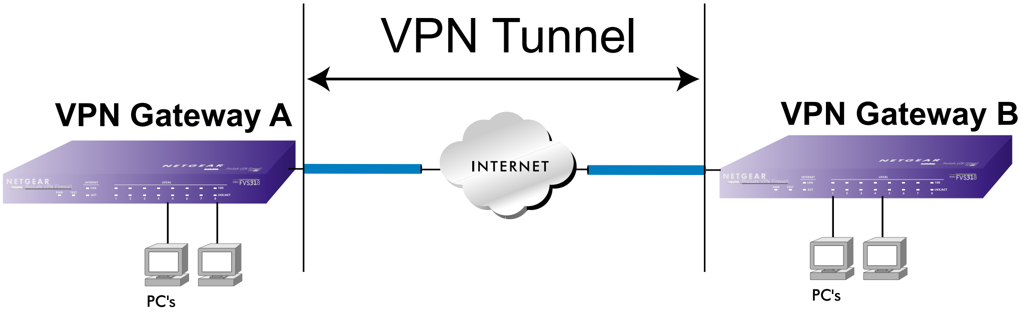


Figure D-5: VPN Tunnel SA

The SA contains all the information necessary for gateway A to negotiate a secure and encrypted communication stream with gateway B. This communication is often referred to as a "tunnel." The gateways contain this information so that it does not have to be loaded onto every computer connected to the gateways.

Each gateway must negotiate its Security Association with another gateway using the parameters and processes established by IPSec. As illustrated below, the most common method of accomplishing this process is via the Internet Key Exchange (IKE) protocol which automates some of the negotiation procedures. Alternatively, you can configure your gateways using manual key exchange, which involves manually configuring each paramter on both gateways.

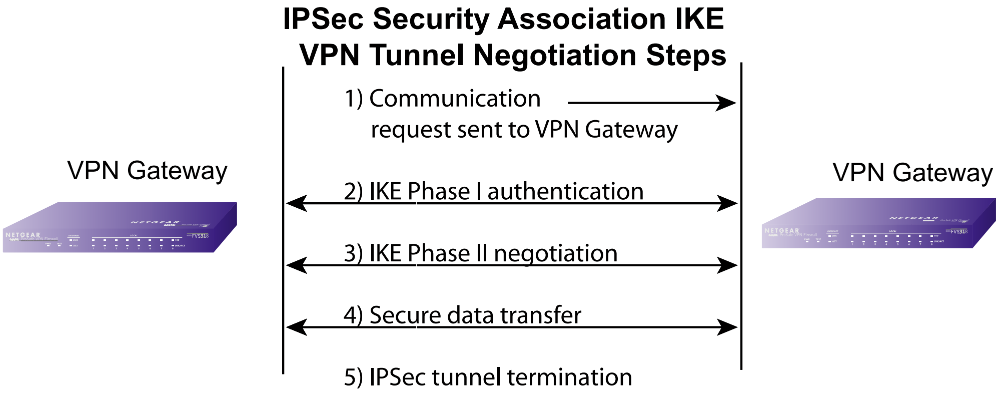

IPSec Security Association IKE
VPN Tunnel Negotiation Steps
VPN Gateway
VPN Gateway
1) Communication request sent to VPN Gateway
2) IKE Phase I authentication
3) IKE Phase II negotiation
4) Secure data transfer
5) IPSec tunnel termination

Figure D-6: IPSec SA negotiation

1. **The IPSec software on Host A initiates the IPSec process in an attempt to communicate with Host B.** The two computers then begin the Internet Key Exchange (IKE) process.

2. **IKE Phase I.**
   a. The two parties negotiate the encryption and authentication algorithms to use in the IKE SAs.
   b. The two parties authenticate each other using a predetermined mechanism, such as preshared keys or digital certificates.
   c. A shared master key is generated by the Diffie-Hellman Public key algorithm within the IKE framework for the two parties. The master key is also used in the second phase to derive IPSec keys for the SAs.
3. **IKE Phase II.**
   a. The two parties negotiate the encryption and authentication algorithms to use in the IPSec SAs.
   b. The master key is used to derive the IPSec keys for the SAs. Once the SA keys are created and exchanged, the IPSec SAs are ready to protect user data between the two VPN gateways.
4. **Data transfer.** Data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.
5. **IPSec tunnel termination.** IPSec SAs terminate through deletion or by timing out.

VPNC IKE Security Parameters

It is important to remember that both gateways must have the identical parameters set for the process to work correctly. The settings in these TechNote examples follow the examples given for Scenario 1 of the VPN Consortium.

VPNC IKE Phase I Parameters

The IKE Phase 1 parameters used:

- Main mode
- TripleDES
- SHA-1
- MODP group 1
- pre-shared secret of "hr5xb84l6aa9r6"
- SA lifetime of 28800 seconds (eight hours)

VPNC IKE Phase II Parameters

The IKE Phase 2 parameters used in Scenario 1 are:

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 1
- Perfect forward secrecy for rekeying
- SA lifetime of 28800 seconds (one hour)

Testing and Troubleshooting

Once you have completed the VPN configuration steps you can use PCs, located behind each of the gateways, to ping various addresses on the LAN-side of the other gateway.

You can troubleshoot connections using the VPN status and log details on the Netgear gateway to determine if IKE negotiation is working. Common problems encountered in setting up VPNs include:

- Parameters may be configured differently on Gateway A vs. Gateway B.
- Two LANs set up with similar or overlapping addressing schemes.
- So many required configuration parameters mean errors such as mistyped information or mismatched parameter selections on either side are more likely to happen.

Additional Reading

- *Building and Managing Virtual Private Networks*, Dave Kosiur, Wiley & Sons; ISBN: 0471295264
- *Firewalls and Internet Security: Repelling the Wily Hacker*, William R. Cheswick and Steven M. Bellovin, Addison-Wesley; ISBN: 0201633574
- *VPNs A Beginners Guide*, John Mains, McGraw Hill; ISBN: 0072191813
- [FF98] Floyd, S., and Fall, K., Promoting the Use of End-to-End Congestion Control in the Internet. IEEE/ACM Transactions on Networking, August 1999.

Relevant RFCs listed numerically:

- [RFC 791] *Internet Protocol DARPA Internet Program Protocol Specification*, Information Sciences Institute, USC, September 1981.
- [RFC 1058] *Routing Information Protocol*, C Hedrick, Rutgers University, June 1988.
- [RFC 1483] *Multiprotocol Encapsulation over ATM Adaptation Layer 5*, Juha Heinanen, Telecom Finland, July 1993.
- [RFC 2401] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol, RFC 2401, November 1998.
- [RFC 2407] D. Piper, The Internet IP Security Domain of Interpretation for ISAKMP, November 1998.
- [RFC 2474] K. Nichols, S. Blake, F. Baker, D. Black, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998.
- [RFC 2475] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, An Architecture for Differentiated Services, December 1998.
- [RFC 2481] K. Ramakrishnan, S. Floyd, A Proposal to Add Explicit Congestion Notification (ECN) to IP, January 1999.
- [RFC 2408] D. Maughan, M. Schertler, M. Schneider, J. Turner, Internet Security Association and Key Management Protocol (ISAKMP).
- [RFC 2409] D. Harkins, D.Carrel, Internet Key Exchange (IKE) protocol.
- [RFC 2401] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol.

Appendix E
NETGEAR VPN Configuration of FVS318 or FVM318 to FVL328

This appendix is a case study on how to configure a secure IPSec VPN tunnel from a NETGEAR FVS318 or FVM318 to a FVL328. This case study follows the VPN Consortium interoperability profile guidelines (found at *http://www.vpnc.org/InteropProfiles/Interop-01.html*). The configuration options and screens for the FVS318 and FVM318 are the same.

Configuration Profile

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.

Table E-1. Profile Summary

VPN Consortium Scenario:		Scenario 1
Type of VPN		LAN-to-LAN or Gateway-to-Gateway (not PC/Client-to-Gateway)
Security Scheme:		IKE with Preshared Secret/Key (not Certificate-based)
Date Tested:		April 2003
Model/Firmware Tested:		
	NETGEAR-Gateway A	FVS318 firmware version A1.4 or FVM318 firmware version 1.1
	NETGEAR-Gateway B	FVL328 with firmware version 1.4 Release 1A
IP Addressing:		
	NETGEAR-Gateway A	Static IP address
	NETGEAR-Gateway B	Static IP address

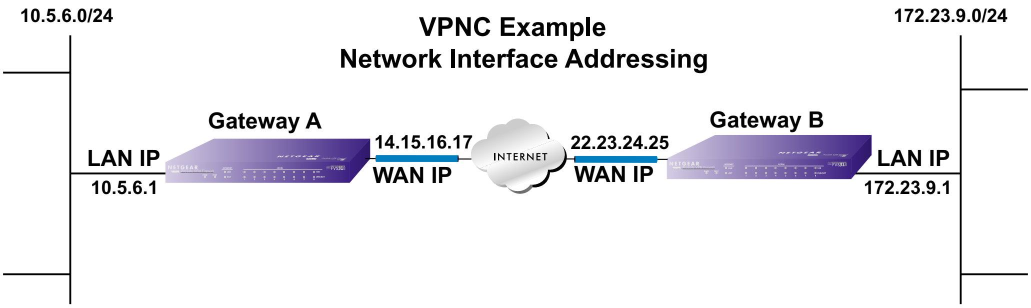


Figure E-1: Addressing and Subnets Used for Examples

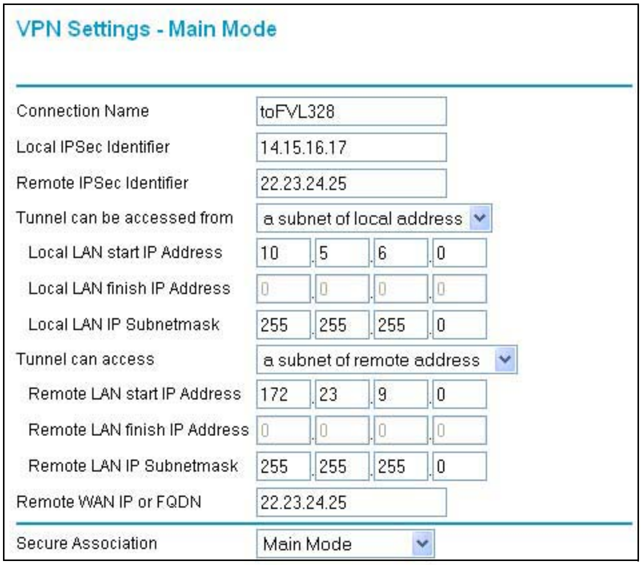
➡	**Note:** Product updates are available on the NETGEAR web site at *www.netgear.com/support/main.asp*. Documentation updates are available on the NETGEAR, Inc. web site at *www.netgear.com/docs*.

Step-By-Step Configuration of FVS318 or FVM318 Gateway A

1. Log in to the FVS318 or FVM318 labeled Gateway A as in the illustration.

   Out of the box, the FVS318 or FVM318 is set for its default LAN address of *http://192.168.0.1* with its default user name of **admin** and default password of **password**. For this example we will assume you have set the local LAN address as 10.5.6.1 for Gateway A and have set your own password.

2. Click on the VPN Settings link on the left side of the main menu.
   - *For the FVS318*: Click the radio button of the first available VPN tunnel. Click the Edit button below. This will take you to the VPN Settings – Main Mode Menu.
   - *For the FVM318*: Click Add. This will take you to the VPN Settings – Main Mode Menu.



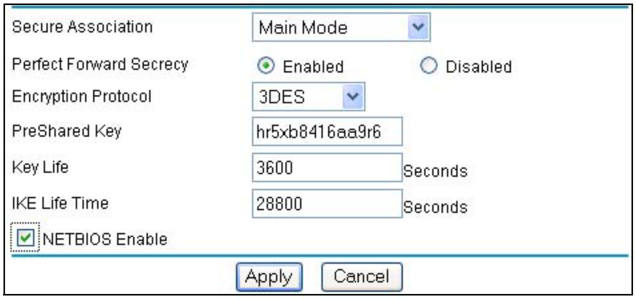
VPN Settings - Main Mode

Connection Name	toFVL328
Local IPSec Identifier	14.15.16.17
Remote IPSec Identifier	22.23.24.25
Tunnel can be accessed from	a subnet of local address
Local LAN start IP Address	10 . 5 . 6 . 0
Local LAN finish IP Address	0 . 0 . 0 . 0
Local LAN IP Subnetmask	255 . 255 . 255 . 0
Tunnel can access	a subnet of remote address
Remote LAN start IP Address	172 . 23 . 9 . 0
Remote LAN finish IP Address	0 . 0 . 0 . 0
Remote LAN IP Subnetmask	255 . 255 . 255 . 0
Remote WAN IP or FQDN	22.23.24.25
Secure Association	Main Mode

Figure E-2: NETGEAR FVS318 vA1.4 VPN Settings (part 1) – Main Mode

- In the Connection Name box, enter in a unique name for the VPN tunnel to be configured between the NETGEAR devices. For this example we have used **toFVL328**.
- Enter a Local IPSec Identifier name for the NETGEAR FVS318 Gateway A. This name must be entered in the other endpoint as Remote IPSec Identifier. In this example we used **14.15.16.17** as the local identifier.
- Enter a Remote IPSec Identifier name for the remote NETGEAR FVL328 Gateway B. This name must be entered in the other endpoint as Local IPSec Identifier. In this example we used **22.23.24.25** as the remote identifier.
- Choose “a subnet of local addresses” from the “Tunnel can be accessed from” pull-down menu.
- Type the starting LAN IP Address of Gateway A (**10.5.6.1** in our example) in the Local IP Local LAN start IP Address field.
- Type the LAN Subnet Mask of Gateway A (**255.255.255.0** in our example) in the Local LAN IP Subnetmask field.
- Choose “a subnet from local addresses” from the “Tunnel can access” pull-down menu.
- Type the starting LAN IP Address of Gateway B (**172.23.9.1** in our example) in the Local IP Remote LAN Start IP Address field.

- Type the LAN Subnet Mask of Gateway B (**255.255.255.0** in our example) in the Remote LAN IP Subnetmask field.
- Type the WAN IP address (**22.23.24.25** in our example) of Gateway B in the Remote WAN IP or FQDN field.



Secure Association	Main Mode
Perfect Forward Secrecy	● Enabled ○ Disabled
Encryption Protocol	3DES
PreShared Key	hr5xb8416aa9r6
Key Life	3600 Seconds
IKE Life Time	28800 Seconds

☑ NETBIOS Enable

Figure E-3: NETGEAR FVS318 vA1.4 VPN Settings (part 2) – Main Mode

- From the Secure Association drop-down box, select Main Mode.
- Next to Perfect Forward Secrecy, select the Enabled radio button.
- From the Encryption Protocol drop-down box, select 3DES.
- In the PreShared Key box, type a unique text string to be used as the shared key between Gateway A and Gateway B. In this example we used **hr5xb84l6aa9r6**. You must make sure the key is the same for both gateways.
- In the Key Life box, enter 3600 seconds.
- In the IKE Life Time, enter 28800 seconds.
- Check the NETBIOS Enable box if you wish to pass NetBIOS traffic over the VPN tunnel, allowing functions such as Microsoft Network Neighborhood browsing.

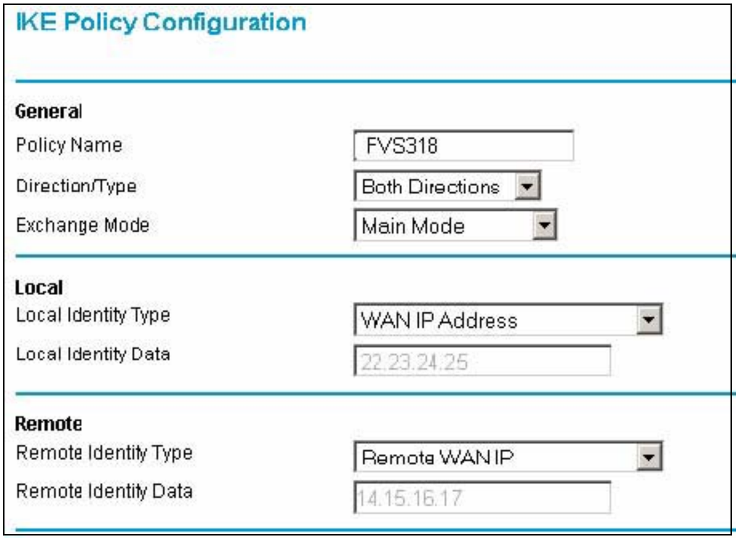
3. Click Apply to save all changes. This will return you to the VPN Settings screen.
4. When the screen returns to the VPN Settings, make sure the Enable checkbox is selected.

Step-By-Step Configuration of FVL328 Gateway B

1. Log in to the NETGEAR FVL328 labeled Gateway B as in the illustration.

   Out of the box, the FVL328 is set for its default LAN address of *http://192.168.0.1* with its default user name of **admin** and default password of **password**. For this example we will assume you have set the local LAN address as 172.23.9.1 for Gateway B and have set your own user name and password.

2. Click on the IKE Policies link under the VPN category link on the left side of the Settings management GUI. This will open the IKE Policies Menu. Click Add. This will open a new screen titled IKE Policy Configuration.



IKE Policy Configuration

General

Policy Name: FVS318

Direction/Type: Both Directions

Exchange Mode: Main Mode

Local

Local Identity Type: WAN IP Address

Local Identity Data: 22.23.24.25

Remote

Remote Identity Type: Remote WAN IP

Remote Identity Data: 14.15.16.17

Figure E-4: NETGEAR FVL328 v1.4 IKE Policy Configuration – Part 1

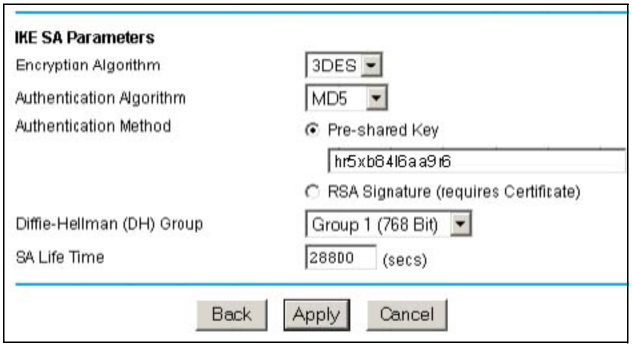
– Enter an appropriate name for the policy in the Policy Name field. This name is not supplied to the remote VPN Endpoint. It is used to help you manage the IKE policies. In our example we have used FVS318 as the Policy Name. In the Policy Name field type **FVS318**.

– From the Direction/Type drop-down box, select Both Directions

– From the Exchange Mode drop-down box, select Main Mode.

– From the Local Identity drop-down box, select WAN IP Address (WAN IP address will automatically be populated into the Local Identity Data field after policy is applied).

– From the Remote Identity drop-down box, select Remote WAN IP (WAN IP address will automatically be populated into the Local Identity Data field after policy is applied).



IKE SA Parameters

Encryption Algorithm	3DES
Authentication Algorithm	MD5
Authentication Method	● Pre-shared Key hr5xb84l6aa9r6 ○ RSA Signature (requires Certificate)
Diffie-Hellman (DH) Group	Group 1 (768 Bit)
SA Life Time	28800 (secs)

Figure E-5: NETGEAR FVL328 v1.4 IKE Policy Configuration – Part 2

– From the Encryption Algorithm drop-down box, select 3DES.

– From the Authentication Algorithm drop-down box, select MD5.

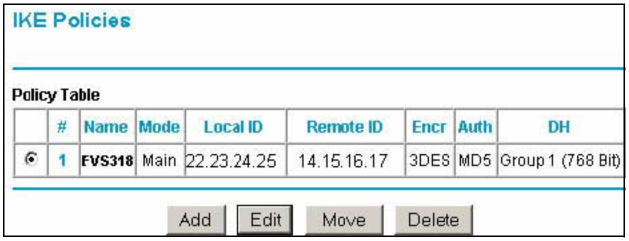
– From the Authentication Method radio button, select Pre-shared Key.

– In the Pre-Shared Key field, type **hr5xb84l6aa9r6**. You must make sure the key is the same for both gateways.

– From the Diffie-Hellman (DH) Group drop-down box, select Group 1 (768 Bit).

– In the SA Life Time field, type 28800.

3. Click the Apply Button. This will bring you back to the IKE Policies Menu.



IKE Policies

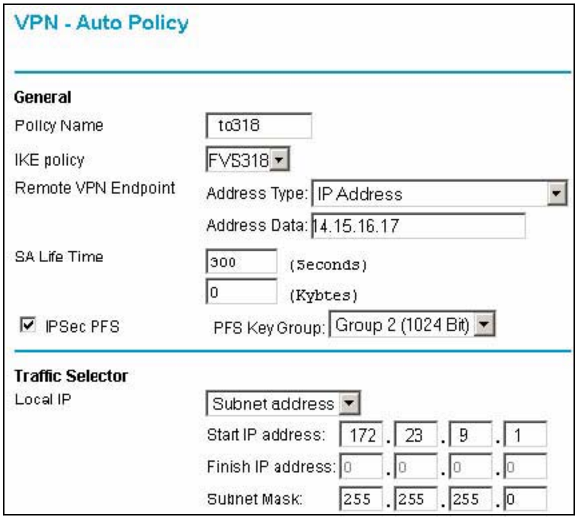
Policy Table

	#	Name	Mode	Local ID	Remote ID	Encr	Auth	DH
●	1	FVS318	Main	22.23.24.25	14.15.16.17	3DES	MD5	Group 1 (768 Bit)

Figure E-6: NETGEAR FVL328 v1.4 IKE Policies (Post Configuration)

The FVS318 IKE Policy is now displayed in the IKE Policies page.

4. Click on the VPN Policies link under the VPN category link on the left side of the main menu. This will take you to the VPN Policies Menu page. Click Add Auto Policy. This will open a new screen titled VPN – Auto Policy.



VPN - Auto Policy

General

Policy Name: to318

IKE policy: FVS318

Remote VPN Endpoint: Address Type: IP Address

Address Data: 14.15.16.17

SA Life Time: 300 (Seconds)

0 (Kybtes)

☑ IPSec PFS — PFS Key Group: Group 2 (1024 Bit)

Traffic Selector

Local IP: Subnet address

Start IP address: 172 . 23 . 9 . 1

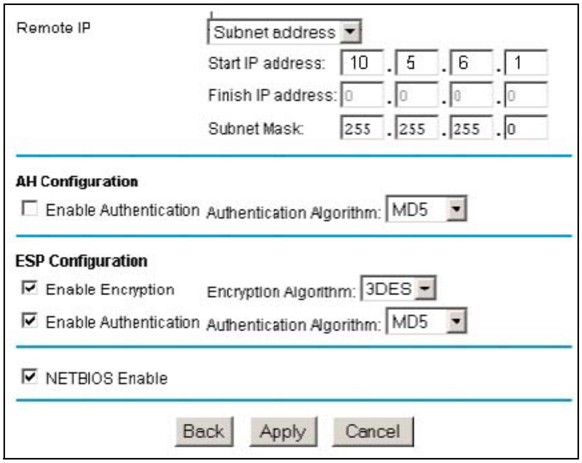
Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Figure E-7: NETGEAR FVL328 VPN v1.4 – Auto Policy (part 1)

- Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. In our example we have used "to318" as the Policy Name. In the Policy Name field type **to318**.
- From the IKE policy drop-down box, select the IKE Policy that was set up in the earlier step – this being the FVS318 IKE Policy.
- From the Remote VPN Endpoint Address Type drop-down box, select IP Address.
- Type the WAN IP Address of Gateway A (**14.15.16.17** in our example) in the **Remote** VPN Endpoint Address Data field.
- Type **300** in the SA Life Time (Seconds) field.
- Type **0** in the SA Life Time (Kbytes) field.
- Check the IPSec PFS checkbox.
- From the PFS Key Group drop-down box, select Group 2 (1024 Bit).
- From the Traffic Selector Local IP drop-down box, select "Subnet addresses".
- Type the starting LAN IP Address of Gateway B (**172.23.9.1** in our example) in the Local IP Start IP Address field.

– Type the LAN Subnet Mask of Gateway B (**255.255.255.0** in our example) in the Local IP Subnet Mask field.



Remote IP: Subnet address
Start IP address: 10 . 5 . 6 . 1
Finish IP address: 0 . 0 . 0 . 0
Subnet Mask: 255 . 255 . 255 . 0

AH Configuration
□ Enable Authentication Authentication Algorithm: MD5

ESP Configuration
☑ Enable Encryption Encryption Algorithm: 3DES
☑ Enable Authentication Authentication Algorithm: MD5

☑ NETBIOS Enable

Figure E-8: NETGEAR FVL328 VPN v1.4 – Auto Policy (part 2)

– From the Traffic Selector Remote IP drop-down box, select “Subnet addresses”.

– Type the starting LAN IP Address of Gateway A (**10.5.6.1** in our example) in the Remote IP Start IP Address field.

– Type the LAN Subnet Mask of Gateway A (**255.255.255.0** in our example) in the Remote IP Subnet Mask field.

– From the ESP Configuration Encryption Algorithm drop-down box, select 3DES.

– Select Enable Authentication in the ESP Configuration Enable Authentication checkbox.

– From the ESP Configuration Authentication Algorithm drop-down box, select MD5.

– Select NETBIOS Enable in the NETBIOS Enable checkbox to enable networking features such as Windows Network Neighborhood.

5. Click Apply. You will be taken back to the VPN Policies Menu page.
6. When the screen returns to the VPN Policies, make sure the Enable checkbox is selected. Click Apply.

Test the VPN Connection

1. From a PC behind the NETGEAR FVS318 or FVM318 gateway A attempt to ping the remote FVS318 gateway B LAN Interface address (example address 172.23.9.1).

   Note: You can run ping tests from Diagnostics link on the NETGEAR main menu or from a DOS prompt on a PC.

2. From a PC behind the FVL328 gateway B attempt to ping the remote NETGEAR FVS318 or FVM318 gateway A LAN Interface address (example address 10.5.6.1).
3. On either router, click on the Router Status link on the left side of the main menu. Click the Show VPN Status button below. This will take you to the IPSec Connection Status Screen. If the connection is functioning properly, the State fields will show “Estab.”
4. On either router, click on the Router Status link on the left side of the main menu. Click the Show VPN Logs button below. The FVS818 or FVM318 log files should be similar to the example below.

```
 13:19:02 - FVS318 IPSec:sizeof(connection)=1724 sizeof(state)=10048 sizeof(SA)=732
 13:19:42 - FVS318 IPsec:call  ipsecdoi_initiate
 13:19:42 - FVS318 IPsec:New State index:0, sno:1
 13:19:42 - FVS318 IPsec:Initiating Main Mode
 13:19:42 - FVS318 IPsec:main_outI1() policy=65
 13:19:42 - FVS318 IKE:[toFVL328] Initializing IKE Main Mode
 13:19:42 - FVS318 IKE:[toFVL328] TX >> MM_I1: 22.23.24.25
 13:19:42 - FVS318 IPsec:inserting event EVENT_RETRANSMIT, timeout in 10 seconds for #1
 13:19:42 - FVS318 IPsec:Receive Packet address:0x1806f14 from 22.23.24.25
 13:19:42 - FVS318 IPsec:main_inR1_outI2()
 13:19:42 - FVS318 IKE:[toFVL328] RX << MM_R1: 22.23.24.25
 13:19:42 - FVS318 IPsec:Oakley Transform 1 accepted
 13:19:42 - FVS318 IKE:OAKLEY_PRESHARED_KEY/OAKLEY_3DES_CBC/MODP1536
 13:19:42 - FVS318 IKE:[toFVL328] TX >> MM_I2: 22.23.24.25
 13:19:42 - FVS318 IPsec:inserting event EVENT_RETRANSMIT, timeout in 10 seconds for #1
 13:19:44 - FVS318 IPsec:Receive Packet address:0x1806f14 from 22.23.24.25
 13:19:44 - FVS318 IPsec:main_inR2_outI3()
 13:19:44 - FVS318 IKE:[toFVL328] RX << MM_R2: 22.23.24.25
 13:19:44 - FVS318 IKE:[toFVL328] TX >> MM_I3: 22.23.24.25
 13:19:44 - FVS318 IPsec:inserting event EVENT_RETRANSMIT, timeout in 10 seconds for #1
 13:19:46 - FVS318 IPsec:Receive Packet address:0x1806f14 from 22.23.24.25
 13:19:46 - FVS318 IPsec:main_inR3()
 13:19:46 - FVS318 IKE:[toFVL328] RX << MM_R3: 22.23.24.25
 13:19:46 - FVS318 IPsec:Decoded Peer's ID is ID_IPV4_ADDR:22.23.24.25and 22.23.24.25in st
 13:19:46 - FVS318 IPsec:inserting event EVENT_SA_REPLACE, timeout in 28740 seconds for #1
 13:19:46 - FVS318 IPsec:STATE_MAIN_I4: ISAKMP SA established
 13:19:46 - FVS318 IPsec:New State index:1, sno:2
 13:19:46 - FVS318 IPsec:quick_outI1()
 13:19:46 - FVS318 IPsec:New Message ID generated:570001
 13:19:46 - FVS318 IPsec:initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS
 13:19:46 - FVS318 IKE:[toFVL328] TX >> QM_I1: 211.26.0.186
 13:19:46 - FVS318 IPsec:in get_ipsec_spi() spi=cf01ea7d
 13:19:46 - FVS318 IPsec:My generated SPI=cf01ea7d
 13:19:46 - FVS318 IPsec:inserting event EVENT_RETRANSMIT, timeout in 10 seconds for #2
 13:19:48 - FVS318 IPsec:Receive Packet address:0x1806f14 from 22.23.24.25
 13:19:48 - FVS318 IPsec:loglog[3] ignoring informational payload, type IPSEC_RESPONDER_LIFETIME
 13:19:48 - FVS318 IPsec:quick_inR1_outI2()
 13:19:48 - FVS318 IKE:[toFVL328] RX << QM_R1: 22.23.24.25
 13:19:48 - FVS318 IKE:[ESP_3DES/AUTH_ALGORITHM_HMAC_SHA1/In SPI:cf01ea7d,Out
SPI:e51e148d]
 13:19:48 - FVS318 IPsec:****Install OUTBOUNDSA:
 13:19:48 - FVS318 IPsec: ESP(3DES-CBC SHA-1)
 13:19:48 - FVS318 IPsec:****Install INBOUND SA:
 13:19:48 - FVS318 IPsec: ESP(3DES-CBC SHA-1)
 13:19:48 - FVS318 IKE:[toFVL328] TX >> QM_I2: 22.23.24.25
 13:19:48 - FVS318 IKE:[toFVL328] established with 22.23.24.25 successfully
 13:19:48 - FVS318 IPsec:inserting event EVENT_SA_REPLACE, timeout in 3540 seconds for #2
 13:19:48 - FVS318 IPsec:STATE_QUICK_I2: sent QI2, IPsec SA established

End of Log ----------
```

Appendix F
NETGEAR VPN Configuration FVS318 or FVM318 to Cisco IOS

This appendix is a case study on how to configure a secure IPSec VPN tunnel from a NETGEAR FVS318 or FVM318 to a Cisco IOS VPN product. This case study follows the VPN Consortium interoperability profile guidelines (found at *http://www.vpnc.org/InteropProfiles/Interop-01.html*). The configuration screens for the FVS318 and FVM318 are the same.

Configuration Profile

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.

Table F-1. Summary

VPN Consortium Scenario:		Scenario 1
Type of VPN		LAN-to-LAN or Gateway-to-Gateway (not PC/Client-to-Gateway)
Security Scheme:		IKE with Preshared Secret/Key (not Certificate-based)
Date Tested:		April 2003
Model/Firmware Tested:		
	Gateway A	NETGEAR FVS318 firmware v A1.4 or FVM318 firmware v 1.1
	Gateway B	Cisco IOS v 12.2
IP Addressing:		
	Gateway A	Static IP address
	Gateway B	Static IP address

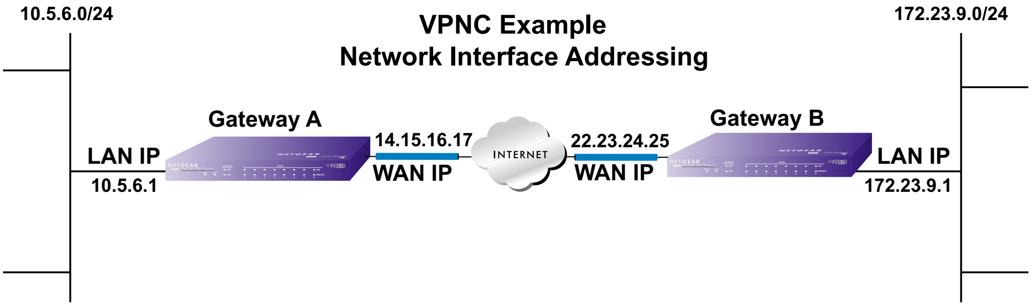


Figure F-1: Addressing and Subnet Used for Examples

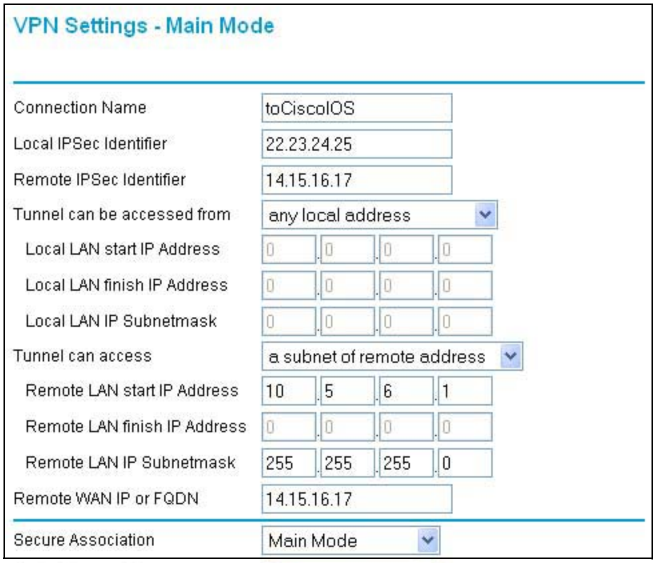
⇨	**Note:** Product updates are available on the NETGEAR web site at *www.netgear.com/support/main.asp*. Documentation updates are available on the NETGEAR, Inc. web site at *www.netgear.com/docs*.

Step-By-Step Configuration of FVS318 or FVM318 Gateway A

1. Log in to the FVS318 or FVM318 labeled Gateway A as in the illustration.

   Out of the box, the FVS318 or FVM318 is set for its default LAN address of *http://192.168.0.1* with its default user name of **admin** and default password of **password**. For this example we will assume you have set the local LAN address as 10.5.6.1 for Gateway A and have set your own password.

2. Click on the VPN Settings link on the left side of the main menu.
   – *For the FVS318*: Click the radio button of first available VPN tunnel. Click the Edit button below. This will take you to the VPN Settings – Main Mode Menu.
   – *For the FVM318*: Click Add. This will take you to the VPN Settings – Main Mode Menu.



VPN Settings - Main Mode

Connection Name	toCiscoIOS
Local IPSec Identifier	22.23.24.25
Remote IPSec Identifier	14.15.16.17
Tunnel can be accessed from	any local address
Local LAN start IP Address	0 . 0 . 0 . 0
Local LAN finish IP Address	0 . 0 . 0 . 0
Local LAN IP Subnetmask	0 . 0 . 0 . 0
Tunnel can access	a subnet of remote address
Remote LAN start IP Address	10 . 5 . 6 . 1
Remote LAN finish IP Address	0 . 0 . 0 . 0
Remote LAN IP Subnetmask	255 . 255 . 255 . 0
Remote WAN IP or FQDN	14.15.16.17
Secure Association	Main Mode

Figure F-2: NETGEAR FVS318 vA1.4 VPN Settings (part 1) – Main Mode

– In the Connection Name box, enter in a unique name for the VPN tunnel to be configured between the NETGEAR devices. For this example we have used "**toCiscoIOS**".

– Enter a Local IPSec Identifier name for the NETGEAR FVS318 Gateway A. This name must be entered in the other endpoint as Remote IPSec Identifier. In this example we used **22.23.24.25** as the local identifier.

– Enter a Remote IPSec Identifier name for the remote Cisco IOS Gateway B. This name must be entered in the other endpoint as Local IPSec Identifier. In this example we used **14.15.16.17** as the remote identifier.

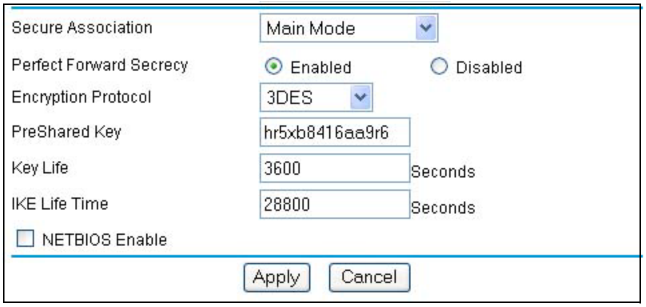
– Choose "a subnet of local addresses" from the "Tunnel can be accessed from" pull-down menu.

– Type the starting LAN IP Address of Gateway A (**172.23.9.1** in our example) in the Local IP Local LAN start IP Address field.

– Type the LAN Subnet Mask of Gateway A (**255.255.255.0** in our example) in the Local LAN IP Subnetmask field.

– Choose "a subnet of remote addresses" from the "Tunnel can access" pull-down menu.

- Type the starting LAN IP Address of Gateway B (**10.5.6.1** in our example) in the Local IP Remote LAN Start IP Address field.
- Type the finishing Subnet Mask of Gateway B (**255.255.255.0** in our example) in the Remote LAN IP Subnetmask field.
- Type the WAN IP address (**14.15.16.17** in our example) of Gateway A in the Remote WAN IP or FQDN field.



Secure Association: Main Mode

Perfect Forward Secrecy: ● Enabled ○ Disabled

Encryption Protocol: 3DES

PreShared Key: hr5xb8416aa9r6

Key Life: 3600 Seconds

IKE Life Time: 28800 Seconds

□ NETBIOS Enable

Figure F-3: NETGEAR FVS318 vA1.4 VPN Settings (part 2) – Main Mode

- From the Secure Association drop-down box, select Main Mode.
- Next to Perfect Forward Secrecy, select the Enabled radio button.
- From the Encryption Protocol drop-down box, select 3DES.
- In the PreShared Key box, type a unique text string to be used as the shared key between Gateway A and Gateway B. In this example we used **hr5xb84l6aa9r6**. You must make sure the key is the same for both gateways.
- In the Key Life box, enter **3600** seconds.
- In the IKE Life Time, enter **28800** seconds.
- Check the NETBIOS Enable box if you wish to pass NetBIOS traffic over the VPN tunnel, allowing functions such as Microsoft Network Neighborhood browsing.

3. Click Apply to save all changes. This will return you to the VPN Settings screen.
4. When the screen returns to the VPN Settings, make sure the Enable checkbox is selected.

Step-By-Step Configuration of Cisco IOS Gateway B

The following are the Cisco commands most relevant to building an inter-vendor VPN. Please refer to your Cisco documentation or www.cisco.com for additional information.

1. Log in to the Cisco router.
2. Type **enable**, to enter enable mode. Enter your **password**.
3. Type **config t** to enter the configuration mode at the command prompt.
4. Create an extended access list. Type **access-list 110 permit ip 172.23.9.0 0.0.0.255 10.5.6.0 0.0.0.255** at the command prompt. This specifies the protected ip traffic passing through the router. The first address is Gateway B in the above example and the second is Gateway A.
5. Define your IKE parameters. Type **crypto isakmp policy 1** at the command prompt.
6. In the **ISAKMP submenu** type the following commands:
   a. **encryption 3des**
   b. **authentication pre-share**
   c. **group 5**
   d. **lifetime 28800**
7. Define the pre-shared key by typing **crypto isakmp key hr5xb8416aa9r6 address 14.15.16.17**. The address used is the WAN address of Gateway A in the example at the beginning of this tech note.
8. Create a transform set by typing **crypto ipsec transform-set netgear esp-3des esp-sha-hmac**.
9. Create an IPSec policy by typing **crypto map netgearmap 10 ipsec-isakmp** at the command prompt. Type the following commands in to the IPSec policy submenu:
   a. **description vpn tunnel to netgear firewall router**
   b. **set peer 14.15.16.17**
   c. **set transform-set netgear**
   d. **set pfs group5**
   e. **match address 110**
10. To apply the crypto map to the public interface type crypto map netgearmap.
11. Exit interface command mode by typing **exit**.
12. Exit configuration mode by typing **exit**.
13. Reboot Cisco router.

The following is an example Cisco ISO Configuration file.

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname centralrouter
!
logging buffered 4096 debugging
enable secret 5 $1$8rrD$L9v.3jriubHGCQn3Vuw.Y1
!
username all
memory-size iomem 20
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip source-route
!
!
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 5
 lifetime 28800
crypto isakmp key hr5xb84l6aa9r6 address 14.15.16.17
!
!
crypto ipsec transform-set netgearmap esp-3des esp-sha-hmac
!
crypto map netgearmap 10 ipsec-isakmp
 description vpn tunnel to netgear firewall router
 set peer 14.15.16.17
 set transform-set netgear
 set pfs group5
 match address 115
!
!
!
!
```

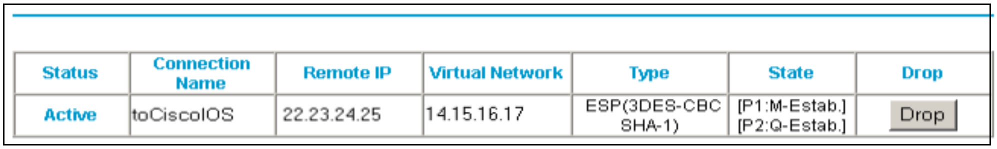
```
interface Ethernet0
 ip address 22.23.24.25 255.255.255.0
 ip nat outside
 half-duplex
 crypto map netgearmap
!
interface FastEthernet0
 ip address 172.23.9.1 255.255.255.0
 ip nat inside
 speed auto
!
interface Serial0
 no ip address
 shutdown
!
ip nat inside source route-map NONAT interface Ethernet0 overload ip
classless ip route 0.0.0.0 0.0.0.0 22.23.24.25 no ip http server ip pim
bidir-enable!
! access-list 110 remark except the private network from that nat rule
access-list 110 deny   ip 172.23.9.1 0.0.0.15 10.5.6.0 0.0.0.255
access-list 110 permit ip 172.23.9.1 0.0.0.15 any access-list 115 remark
INCLUDE PRIVATE NETWORK TO PRIVATE NETWORK IN VPN TUNNEL access-list 115
permit ip 172.23.9.1 0.0.0.15 10.5.60 0.0.0.255! route-map NONAT permit
10  match ip address 110! ! line con 0 line aux 0 line vty 0 4  password
pctg5tcd3  login! no scheduler allocate end
```

Test the VPN Connection

1. From a PC behind the NETGEAR Gateway A attempt to ping the remote Cisco IOS Gateway B LAN Interface address (example address 172.23.9.1).

   Note: You can run ping tests from the Diagnostics link of the NETGEAR main menu or from a DOS prompt on a PC.

2. From a PC behind the Cisco IOS Gateway B attempt to ping the remote NETGEAR gateway A LAN Interface address (example address 10.5.6.1).



Status	Connection Name	Remote IP	Virtual Network	Type	State	Drop
Active	toCiscoIOS	22.23.24.25	14.15.16.17	ESP(3DES-CBC SHA-1)	[P1:M-Estab.] [P2:Q-Estab.]	Drop

Figure F-4: NETGEAR FVS318 vA1.4 IPSec Connection Status Screen

3. From the NETGEAR Router Status link on the left side of the main menu, click the Show VPN Status button below. This will take you to the IPSec Connection Status Screen. If the connection is functioning properly, the State fields will be similar to the screen example above, with “Estab.” listed to the right of P1 and P2.

4. From the NETGEAR Router Status link on the left side of the main menu, click the Show VPN Logs button below. The NETGEAR FVS318 or FVM318 log files should be similar to the example below.

```
Thur, 04/24/2003 13:19:02 - FVS318 IPSec:sizeof(connection)=1724 sizeof(state)=10048
sizeof(SA)=732
Thur, 04/24/2003 13:19:42 - FVS318 IPsec:call  ipsecdoi_initiate
Thur, 04/24/2003 13:19:42 - FVS318 IPsec:New State index:0, sno:1
Thur, 04/24/2003 13:19:42 - FVS318 IPsec:Initiating Main Mode
Thur, 04/24/2003 13:19:42 - FVS318 IPsec:main_outI1() policy=65
Thur, 04/24/2003 13:19:42 - FVS318 IKE:[toCiscoIOS] Initializing IKE Main Mode
Thur, 04/24/2003 13:19:42 - FVS318 IKE:[toCiscoIOS] TX >> MM_I1: 22.23.24.25
Thur, 04/24/2003 13:19:42 - FVS318 IPsec:inserting event EVENT_RETRANSMIT, timeout in 10
seconds for #1
Thur, 04/24/2003 13:19:42 - FVS318 IPsec:Receive Packet address:0x1806f14 from 22.23.24.25
Thur, 04/24/2003 13:19:42 - FVS318 IPsec:main_inR1_outI2()
Thur, 04/24/2003 13:19:42 - FVS318 IKE:[toCiscoIOS] RX << MM_R1: 22.23.24.25
Thur, 04/24/2003 13:19:42 - FVS318 IPsec:Oakley Transform 1 accepted
Thur, 04/24/2003 13:19:42 - FVS318 IKE:OAKLEY_PRESHARED_KEY/OAKLEY_3DES_CBC/
MODP1536
Thur, 04/24/2003 13:19:42 - FVS318 IKE:[toCiscoIOS] TX >> MM_I2: 22.23.24.25
Thur, 04/24/2003 13:19:42 - FVS318 IPsec:inserting event EVENT_RETRANSMIT, timeout in 10
seconds for #1
Thur, 04/24/2003 13:19:44 - FVS318 IPsec:Receive Packet address:0x1806f14 from 22.23.24.25
Thur, 04/24/2003 13:19:44 - FVS318 IPsec:main_inR2_outI3()
Thur, 04/24/2003 13:19:44 - FVS318 IKE:[toCiscoIOS] RX << MM_R2: 22.23.24.25
Thur, 04/24/2003 13:19:44 - FVS318 IKE:[toCiscoIOS] TX >> MM_I3: 22.23.24.25
Thur, 04/24/2003 13:19:44 - FVS318 IPsec:inserting event EVENT_RETRANSMIT, timeout in 10
seconds for #1
Thur, 04/24/2003 13:19:46 - FVS318 IPsec:Receive Packet address:0x1806f14 from 22.23.24.25
Thur, 04/24/2003 13:19:46 - FVS318 IPsec:main_inR3()
Thur, 04/24/2003 13:19:46 - FVS318 IKE:[toCiscoIOS] RX << MM_R3: 22.23.24.25
Thur, 04/24/2003 13:19:46 - FVS318 IPsec:Decoded Peer's ID is ID_IPV4_ADDR:22.23.24.25and
22.23.24.25in st
Thur, 04/24/2003 13:19:46 - FVS318 IPsec:inserting event EVENT_SA_REPLACE, timeout in 28740
seconds for #1
Thur, 04/24/2003 13:19:46 - FVS318 IPsec:STATE_MAIN_I4: ISAKMP SA established
Thur, 04/24/2003 13:19:46 - FVS318 IPsec:New State index:1, sno:2
Thur, 04/24/2003 13:19:46 - FVS318 IPsec:quick_outI1()
Thur, 04/24/2003 13:19:46 - FVS318 IPsec:New Message ID generated:570001
Thur, 04/24/2003 13:19:46 - FVS318 IPsec:initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS
Thur, 04/24/2003 13:19:46 - FVS318 IKE:[toCiscoIOS] TX >> QM_I1: 211.26.0.186
Thur, 04/24/2003 13:19:46 - FVS318 IPsec:in get_ipsec_spi() spi=cf01ea7d
Thur, 04/24/2003 13:19:46 - FVS318 IPsec:My generated SPI=cf01ea7d
Thur, 04/24/2003 13:19:46 - FVS318 IPsec:inserting event EVENT_RETRANSMIT, timeout in 10
seconds for #2
Thur, 04/24/2003 13:19:48 - FVS318 IPsec:Receive Packet address:0x1806f14 from 22.23.24.25
Thur, 04/24/2003 13:19:48 - FVS318 IPsec:loglog[3] ignoring informational payload, type
IPSEC_RESPONDER_LIFETIME
Thur, 04/24/2003 13:19:48 - FVS318 IPsec:quick_inR1_outI2()
Thur, 04/24/2003 13:19:48 - FVS318 IKE:[toCiscoIOS] RX << QM_R1: 22.23.24.25
Thur, 04/24/2003 13:19:48 - FVS318 IKE:[ESP_3DES/AUTH_ALGORITHM_HMAC_SHA1/In
SPI:cf01ea7d,Out SPI:e51e148d]
Thur, 04/24/2003 13:19:48 - FVS318 IPsec:****Install OUTBOUNDSA:
Thur, 04/24/2003 13:19:48 - FVS318 IPsec: ESP(3DES-CBC SHA-1)
Thur, 04/24/2003 13:19:48 - FVS318 IPsec:****Install INBOUND SA:
Thur, 04/24/2003 13:19:48 - FVS318 IPsec: ESP(3DES-CBC SHA-1)
```

```
Thur, 04/24/2003 13:19:48 - FVS318 IKE:[toCiscoIOS] TX >> QM_I2: 22.23.24.25
Thur, 04/24/2003 13:19:48 - FVS318 IKE:[toCiscoIOS] established with 22.23.24.25 successfully
Thur, 04/24/2003 13:19:48 - FVS318 IPsec:inserting event EVENT_SA_REPLACE, timeout in 3540
seconds for #2
Thur, 04/24/2003 13:19:48 - FVS318 IPsec:STATE_QUICK_I2: sent QI2, IPsec SA established
```

End of Log ----------

Appendix G
NETGEAR VPN Configuration
FVS318 or FVM318 with FQDN to FVL328

This appendix is a case study on how to configure a VPN tunnel from a NETGEAR FVS318 or FVM318 to a FVL328 using a Fully Qualified Domain Name (FQDN) to resolve the public address of one or both routers. This case study follows the VPN Consortium interoperability profile guidelines (found at *http://www.vpnc.org/InteropProfiles/Interop-01.html*). The configuration options and screens for the FVS318 and FVM318 are the same.

Configuration Profile

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.

Table G-1. Profile Summary

VPN Consortium Scenario:		Scenario 1
Type of VPN		LAN-to-LAN or Gateway-to-Gateway (not PC/Client-to-Gateway)
Security Scheme:		IKE with Preshared Secret/Key (not Certificate-based)
Date Tested:		April 2003
Model/Firmware Tested:		
	NETGEAR-Gateway A	FVS318 firmware version A1.4 or FVM318 firmware version 1.1
	NETGEAR-Gateway B	FVL328 with firmware version 1.4 Release 1A
IP Addressing:		
	NETGEAR-Gateway A	Fully Qualified Domain Name (FQDN)
	NETGEAR-Gateway B	Static IP address

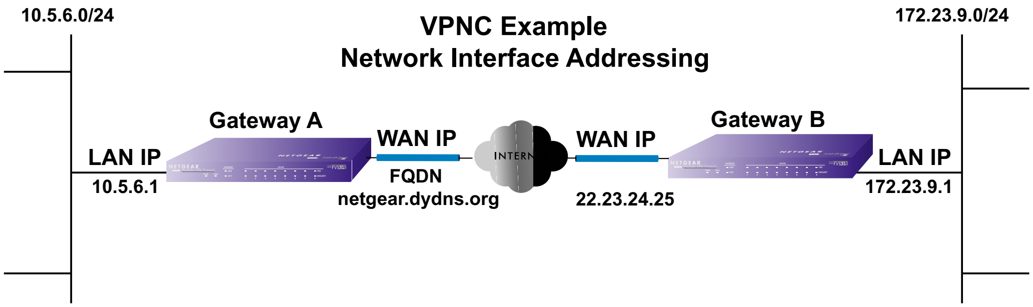


Figure G-1: Addressing and Subnet Used for Examples

Note: Product updates are available on the NETGEAR web site at *www.netgear.com/support/main.asp*. Documentation updates are available on the NETGEAR, Inc. web site at *www.netgear.com/docs*.

The Use of a Fully Qualified Domain Name (FQDN)

Many ISPs (Internet Service Providers) provide connectivity to their customers using dynamic instead of static IP addressing. This means that a user's IP address does not remain constant over time which presents a challenge for gateways attempting to establish VPN connectivity.

A Dynamic DNS (DDNS) service allows a user whose public IP address is dynamically assigned to be located by a host or domain name. It provides a central public database where information (such as email addresses, host names and IP addresses) can be stored and retrieved. Now, a gateway can be configured to use a 3rd party service in lieu of a permanent and unchanging IP address to establish bi-directional VPN connectivity.

To use DDNS, you must register with a DDNS service provider. Example DDNS Service Providers include:

Table G-1. Example DDNS Service Providers

DynDNS	www.dyndns.org
TZO.com	netgear.tzo.com
ngDDNS	ngddns.iego.net

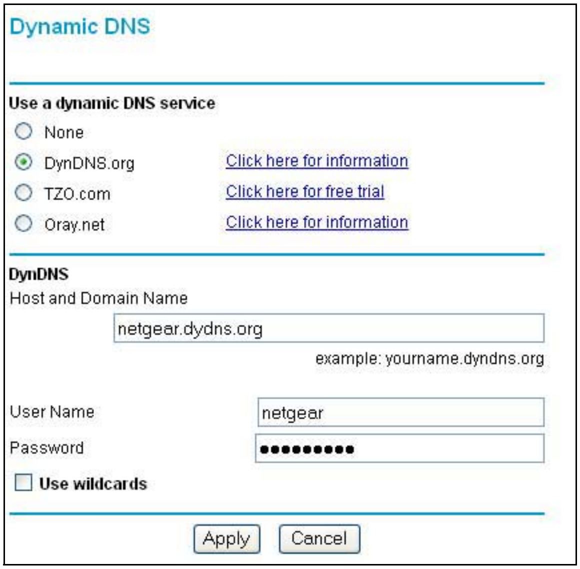
In this example, Gateway A is configured using an example FQDN provided by a DDNS Service provider. In this case we established the hostname **netgear.dyndns.org** for gateway A using the DynDNS service. Gateway B will use the DDNS Service Provider when establishing a VPN tunnel.

In order to establish VPN connectivity Gateway A must be configured to use Dynamic DNS, and Gateway B must be configured to use a DNS hostname to find Gateway A provided by a DDNS Service Provider. Again, the following step-by-step procedures assume that you have already registered with a DDNS Service Provider and have the configuration information necessary to set up the gateways.

Step-By-Step Configuration of FVS318 or FVM318 Gateway A

1. Log in to the FVS318 or FVM318 labeled Gateway A as in the illustration.

   Out of the box, the FVS318 or FVM318 is set for its default LAN address of *http://192.168.0.1* with its default user name of **admin** and default password of **password**. For this example we will assume you have set the local LAN address as 10.5.6.1 for Gateway A and have set your own password.
2. Click on the Dynamic DNS link on the left side of the main menu. This will take you to the Dynamic DNS Menu.
3. Access the website of one of the dynamic DNS service providers whose names appear in the ‘Use a dynamic DNS service’ list, and register for an account.
   For example, for dyndns.org, click the link or go to www.dyndns.org.



Dynamic DNS

Use a dynamic DNS service

○ None

● DynDNS.org Click here for information

○ TZO.com Click here for free trial

○ Oray.net Click here for information

DynDNS

Host and Domain Name: netgear.dydns.org

example: yourname.dyndns.org

User Name: netgear

Password: ●●●●●●●●●●

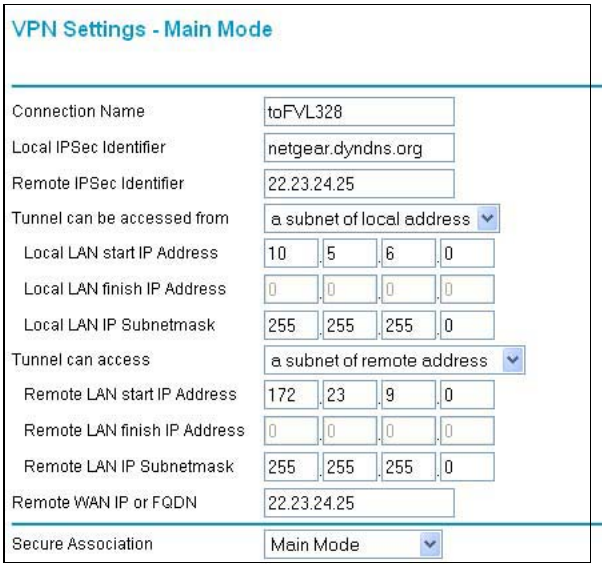
□ Use wildcards

Figure G-2: Dynamic DNS Setup Menu

4. Select the Use a dynamic DNS service radio button for the service you are using. In this example we are using www.DynDNS.org as the service provider.
   - Type the Host Name that your dynamic DNS service provider gave you.
     The dynamic DNS service provider may call this the domain name. In this example we are using dyndns.org as the domain suffix.
   - Type the User Name for your dynamic DNS account. In this example we used netgear as the Host Name. This means that the complete FQDN we are using is netgear.dyndns.org and your Host Name is "netgear."
   - Type the Password (or key) for your dynamic DNS account.
5. Click Apply to save your configuration.

➡	**Note:** The router supports only basic DDNS and the login and password may not be secure. 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.

6. Click on the VPN Settings link on the left side of the main menu.
   - *For the FVS318*: Click the radio button of the first available VPN tunnel. Click the Edit button below. This will take you to the VPN Settings – Main Mode Menu.
   - *For the FVM318*: Click Add. This will take you to the VPN Settings – Main Mode Menu.



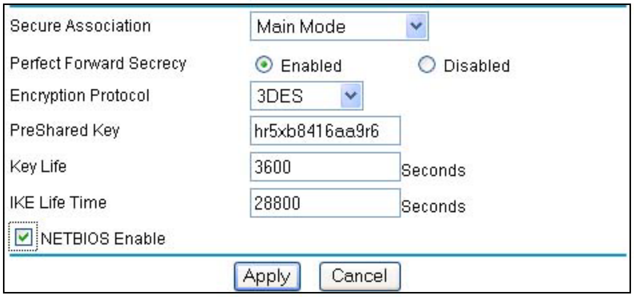
VPN Settings - Main Mode

Connection Name	toFVL328
Local IPSec Identifier	netgear.dyndns.org
Remote IPSec Identifier	22.23.24.25
Tunnel can be accessed from	a subnet of local address
Local LAN start IP Address	10 . 5 . 6 . 0
Local LAN finish IP Address	0 . 0 . 0 . 0
Local LAN IP Subnetmask	255 . 255 . 255 . 0
Tunnel can access	a subnet of remote address
Remote LAN start IP Address	172 . 23 . 9 . 0
Remote LAN finish IP Address	0 . 0 . 0 . 0
Remote LAN IP Subnetmask	255 . 255 . 255 . 0
Remote WAN IP or FQDN	22.23.24.25
Secure Association	Main Mode

Figure G-3: NETGEAR FVS318 vA1.4 VPN Settings (part 1) – Main Mode

- In the Connection Name box, enter in a unique name for the VPN tunnel to be configured between the NETGEAR devices. For this example we have used **toFVL328**.
- Enter a Local IPSec Identifier name for the NETGEAR FVS318 Gateway A. This name must be entered in the other endpoint as Remote IPSec Identifier. In this example we used **netgear.dyndns.org** (the FQDN) as the local identifier.
- Enter a Remote IPSec Identifier name for the remote NETGEAR FVL328 Gateway B. This name must be entered in the other endpoint as Local IPSec Identifier. In this example we used **22.23.24.25** as the remote identifier.
- Choose “a subnet of local addresses” from the” Tunnel can be accessed from” pull-down menu.
- Type the starting LAN IP Address of Gateway A (**10.5.6.1** in our example) in the Local IP Local LAN start IP Address field.

- Type the LAN Subnet Mask of Gateway A (**255.255.255.0** in our example) in the **Local** LAN IP Subnetmask field.
- Choose “a subnet of remote addresses” from the “Tunnel can access**”** pull-down menu.
- Type the starting LAN IP Address of Gateway B (**172.23.9.1** in our example) in the Local IP Remote LAN Start IP Address field.
- Type the LAN Subnet Mask of Gateway B (**255.255.255.0** in our example) in the Remote LAN IP Subnetmask field.
- Type the WAN IP address (**22.23.24.25** in our example) of Gateway B in the Remote WAN IP or FQDN field.



Secure Association	Main Mode	
Perfect Forward Secrecy	● Enabled	○ Disabled
Encryption Protocol	3DES	
PreShared Key	hr5xb8416aa9r6	
Key Life	3600	Seconds
IKE Life Time	28800	Seconds
☑ NETBIOS Enable		

Figure G-4: NETGEAR FVS318 vA1.4 VPN Settings (part 2) – Main Mode

- From the Secure Association drop-down box, select Main Mode.
- Next to Perfect Forward Secrecy, select the Enabled radio button.
- From the Encryption Protocol drop-down box, select 3DES.
- In the PreShared Key box, type a unique text string to be used as the shared key between Gateway A and Gateway B. In this example we used **hr5xb84l6aa9r6**. You must make sure the key is the same for both gateways.
- In the Key Life box, enter **3600** seconds.
- In the IKE Life Time, enter **28800** seconds.
- Check the NETBIOS Enable box if you wish to pass NetBIOS traffic over the VPN tunnel, allowing functions such as Microsoft Network Neighborhood browsing.

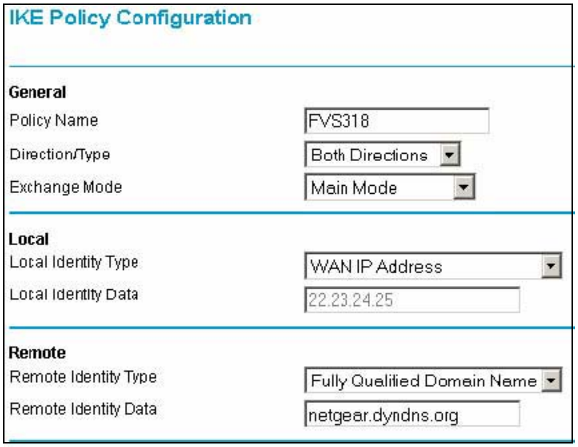
7. Click Apply to save all changes. This will return you to the VPN Settings screen.
8. When the screen returns to the VPN Settings, make sure the Enable checkbox is selected.

Step-By-Step Configuration of FVL328 Gateway B

1. Log in to the NETGEAR FVL328 labeled Gateway B as in the illustration.

   Out of the box, the FVL328 is set for its default LAN address of *http://192.168.0.1* with its default user name of **admin** and default password of **password**. For this example we will assume you have set the local LAN address as 172.23.9.1 for Gateway B.

2. Click IKE Policies link under the VPN category and click Add on the IKE Policies Menu.



IKE Policy Configuration

General	
Policy Name	FVS318
Direction/Type	Both Directions
Exchange Mode	Main Mode
Local	
Local Identity Type	WAN IP Address
Local Identity Data	22.23.24.25
Remote	
Remote Identity Type	Fully Qualified Domain Name
Remote Identity Data	netgear.dyndns.org

Figure G-5: NETGEAR FVL328 v1.4 IKE Policy Configuration – Part 1

– Enter an appropriate name for the policy in the Policy Name field. This name is not supplied to the remote VPN Endpoint. It is used to help you manage the IKE policies. In our example we have used FVS318 as the Policy Name. In the Policy Name field type **FVS318**.

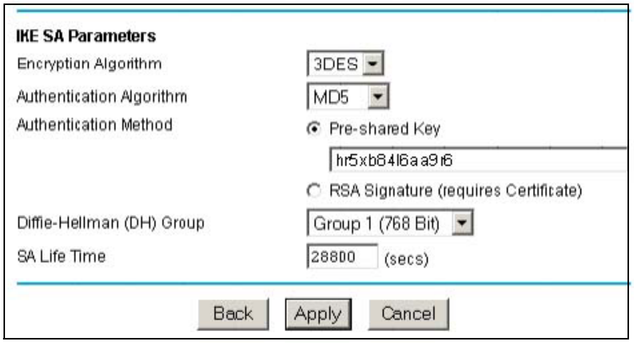
– From the Direction/Type drop-down box, select Both Directions

– From the Exchange Mode drop-down box, select Main Mode.

– From the Local Identity drop-down box, select WAN IP Address (WAN IP address will automatically be populated into the Local Identity Data field after policy is applied).

– From the Remote Identity drop-down box, select Fully Qualified Domain Name.

– Type the FQDN (**netgear.dnydns.org** in our example) in the Remote Identity Data field.



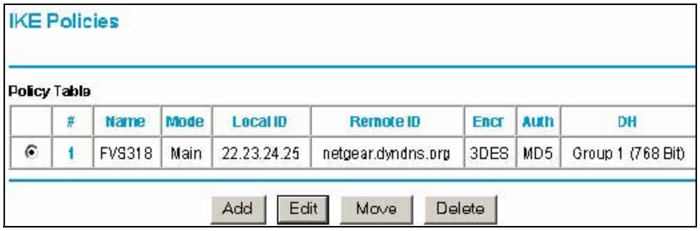
IKE SA Parameters

Encryption Algorithm	3DES
Authentication Algorithm	MD5
Authentication Method	● Pre-shared Key hr5xb84l6aa9r6 ○ RSA Signature (requires Certificate)
Diffie-Hellman (DH) Group	Group 1 (768 Bit)
SA Life Time	28800 (secs)

Figure G-6: NETGEAR FVL328 v1.4 IKE Policy Configuration – Part 2

- From the Encryption Algorithm drop-down box, select 3DES.
- From the Authentication Algorithm drop-down box, select MD5.
- From the Authentication Method radio button, select Pre-shared Key.
- In the Pre-Shared Key field, type **hr5xb84l6aa9r6**. You must make sure the key is the same for both gateways.
- From the Diffie-Hellman (DH) Group drop-down box, select Group 1 (768 Bit).
- In the SA Life Time field, type 28800.

3. Click Apply. This will bring you back to the IKE Policies Menu.



IKE Policies

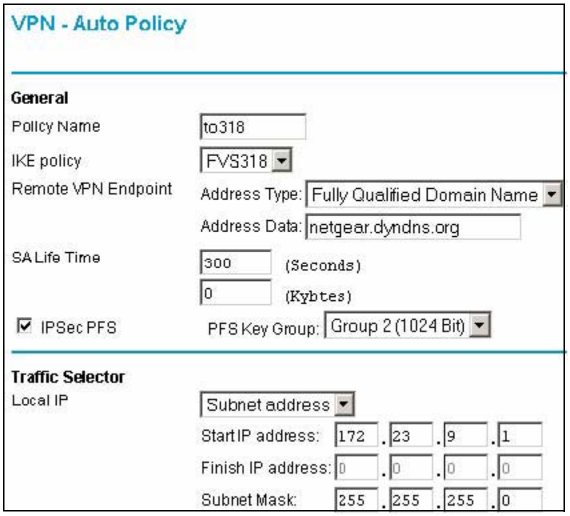
Policy Table

	#	Name	Mode	Local ID	Remote ID	Encr	Auth	DH
●	1	FVS318	Main	22.23.24.25	netgear.dyndns.org	3DES	MD5	Group 1 (768 Bit)

Figure G-7: NETGEAR FVL328 v1.4 IKE Policies (Post Configuration)

The FVS318 IKE Policy is now displayed in the IKE Policies page.

4. Click the VPN Policies link under the VPN category on the left side of the main menu. This will take you to the VPN Policies Menu page. Click Add Auto Policy. This will open a new screen titled VPN – Auto Policy.



VPN - Auto Policy

General

Policy Name: to318

IKE policy: FVS318

Remote VPN Endpoint: Address Type: Fully Qualified Domain Name

Address Data: netgear.dyndns.org

SA Life Time: 300 (Seconds)

0 (Kybtes)

☑ IPSec PFS — PFS Key Group: Group 2 (1024 Bit)

Traffic Selector

Local IP: Subnet address

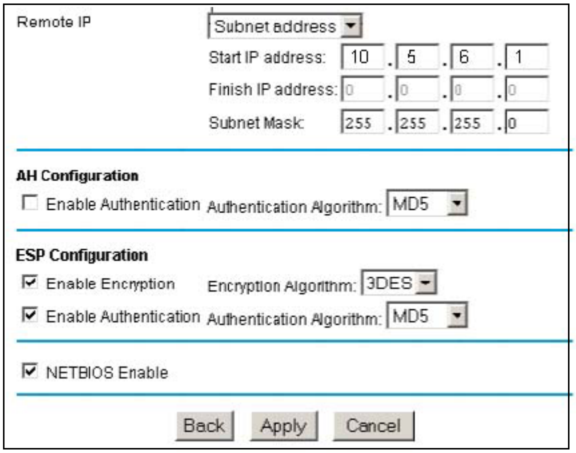
Start IP address: 172 . 23 . 9 . 1

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Figure G-8: NETGEAR FVL328 VPN v1.4 – Auto Policy (part 1)

- Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. In our example we have used to318 as the Policy Name. In the Policy Name field type **to318**.
- From the IKE policy drop-down box, select the IKE Policy that was set up in the earlier step – this being the FVS318 IKE Policy.
- From the Remote VPN Endpoint Address Type drop-down box, select IP Address.
- Type the WAN IP Address of Gateway A (**14.15.16.17** in our example) in the Remote VPN Endpoint Address Data field.
- Type **300** in the SA Life Time (Seconds) field.
- Type **0** in the SA Life Time (Kbytes) field.
- Check the IPSec PFS checkbox to enable Perfect Forward Secrecy.
- From the PFS Key Group drop-down box, select Group 2 (1024 Bit).
- From the Traffic Selector Local IP drop-down box, select Subnet addresses”.
- Type the starting LAN IP Address of Gateway B (**172.23.9.1** in our example) in the Local IP Start IP Address field.
- Type the LAN Subnet Mask of Gateway B (**255.255.255.0** in our example) in the Local IP Subnet Mask field.



Remote IP: Subnet address

Start IP address: 10 . 5 . 6 . 1

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

AH Configuration

□ Enable Authentication Authentication Algorithm: MD5

ESP Configuration

☑ Enable Encryption Encryption Algorithm: 3DES

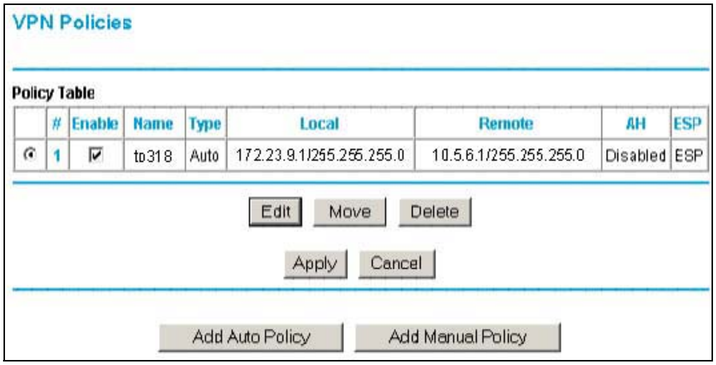
☑ Enable Authentication Authentication Algorithm: MD5

☑ NETBIOS Enable

Figure G-9: NETGEAR FVL328 VPN v1.4 – Auto Policy (part 2)

- From the Traffic Selector Remote IP drop-down box, select “Subnet addresses”.
- Type the starting LAN IP Address of Gateway A (**10.5.6.1** in our example) in the Remote IP Start IP Address field.
- Type the LAN Subnet Mask of Gateway A (**255.255.255.0** in our example) in the Remote IP Subnet Mask field.
- Select Enable Encryption in the ESP Configuration Enable Encryption checkbox.
- From the ESP Configuration Encryption Algorithm drop-down box, select 3DES.
- Select Enable Authentication in the ESP Configuration Enable Authentication checkbox.
- From the ESP Configuration Authentication Algorithm drop-down box, select MD5.
- Select NETBIOS Enable in the NETBIOS Enable checkbox to enable networking features like Windows Network Neighborhood.

5. Click the Apply Button. You will be taken back to the VPN Policies Menu page.



VPN Policies

Policy Table

	#	Enable	Name	Type	Local	Remote	AH	ESP
●	1	☑	to318	Auto	172.23.9.1/255.255.255.0	10.5.6.1/255.255.255.0	Disabled	ESP

Figure G-10: NETGEAR FVL328 v1.4 VPN Policies Menu (Post Configuration)

6. When the screen returns to the VPN Policies, make sure the Enable checkbox is selected. Click the Apply button.

Test the VPN Connection

1. From a PC behind the NETGEAR FVS318 or FVM318 gateway A attempt to ping the remote FVL328 gateway B LAN Interface address (example address 172.23.9.1).

   Note: You can run ping tests from NETGEAR main menu or from a DOS prompt on a PC.
2. From a PC behind the FVL328 gateway B attempt to ping the remote NETGEAR FVS318 or FVM318 gateway A LAN Interface address (example address 10.5.6.1).
3. On either router, click the Router Status link on the left side of the main menu. Click the Show VPN Status button below. This will take you to the IPSec Connection Status Screen. If the connection is functioning properly, the State fields will show “Estab.”
4. On either router, click the Router Status link on the left side of the main menu. Click the Show VPN Logs button to view the connection log.

Glossary

Use the list below to find definitions for technical terms used in this manual.

Numeric

3DES

3DES (Triple DES) achieves a high level of security by encrypting the data three times using DES with three different, unrelated keys.

10BASE-T

The IEEE specification for 10 Mbps Ethernet over Category 3, 4, or 5 twisted-pair cable.

100BASE-TX

The IEEE specification for 100 Mbps Fast Ethernet over Category 5 twisted-pair cable.

A

Access Control List

An ACL is a database that an Operating System uses to track each user's access rights to system objects (such as file directories and/or files).

ACL

See "Access Control List" on page 1.

ADSL

Short for asymmetric digital subscriber line, a technology that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).
ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

Address Resolution Protocol

An Internet Protocol that dynamically maps Internet addresses to physical (hardware) addresses on a LAN.

Advanced Network Device Layer/Software

Term for the Device Driver level.

AES

Advanced Encryption Standard, a symmetric 128-bit block data encryption technique.
It is an iterated block cipher with a variable block length and a variable key length. The block length and the key length can be independently specified to 128, 192 or 256 bits.The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES works at multiple network layers simultaneously.

AH

Authentication Header.

Aging

When an entry for a node is added to the lookup table of a switch, it is given a timestamp. Each time a packet is received from a node, the timestamp is updated. The switch has a user-configurable timer that erases the entry after a certain length of time with no activity from that node.

API

See “Application Programming Interface” on page 2.

Application Programming Interface

An API is an interface used by an programmer to interface with functions provided by an application.

ARP

See “ADSL” on page 1.

Auto-negotiation

A feature that allows twisted-pair ports to advertise their capabilities for speed, duplex and flow control. When connected to a port that also supports auto-negotiation, the link can automatically configure itself to the optimum setup.

Auto Uplink

Auto Uplink™ technology (also called MDI/MDIX) eliminates the need to worry about crossover vs. straight-through Ethernet cables. Auto Uplink™ will accommodate either type of cable to make the right connection.

B

Backbone

The part of a network used as a primary path for transporting traffic between network segments.

Bandwidth

The information capacity, measured in bits per second, that a channel could transmit. Bandwidth examples include 10 Mbps for Ethernet, 100 Mbps for Fast Ethernet, and 1000 Mbps (I Gbps) for Gigabit Ethernet.

Baud

The signaling rate of a line, that is, the number of transitions (voltage or frequency changes) made per second. Also known as line speed.

Broadcast

A packet sent to all devices on a network.

C

CA

A Certificate Authority is a trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs.

Cat 5

Category 5 unshielded twisted pair (UTP) cabling. An Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or Cat 5 or Cat V, by the Electronic Industry Association (EIA).
This rating will be printed on the cable jacket. Cat 5 cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

Certificate Authority

A Certificate Authority is a trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs.
The role of the CA in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be. Usually, this means that the CA has an arrangement with a financial institution, such as a credit card company, which provides it with information to confirm an individual's claimed identity. CAs are a critical component in data security and electronic_commerce because they guarantee that the two parties exchanging information are really who they claim to be.
the two parties exchanging information are really who they claim to be.

Class of Service

A term to describe treating different types of traffic with different levels of service priority. Higher priority traffic gets faster treatment during times of switch congestion

CRL

Certificate Revocation List. Each Certificate Authority (CA) maintains a revoked certificates list.

D

Denial of Service attack

DoS. A hacker attack designed to prevent your computer or network from operating or communicating.

DHCP

See “Dynamic Host Configuration Protocol.” on page 5.

DMZ

A Demilitarized Zone is used by a company that wants to host its own Internet services without sacrificing unauthorized access to its private network.

The DMZ sits between the Internet and an internal network's line of defense, usually some combination of firewalls and bastion hosts. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

DNS

Short for Domain Name System (or Service), an Internet service that translates domain names into IP addresses.

Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Domain Name

A descriptive name for an address or group of addresses on the Internet. Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as .com, .edu, .uk, etc. For example, in the address mail.NETGEAR.com, mail is a server name and NETGEAR.com is the domain.

DoS

A hacker attack designed to prevent your computer or network from operating or communicating.

DSL

Short for digital subscriber line, but is commonly used in reference to the asymmetric version of this technology (ADSL) that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).

ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

DSLAM

DSL Access Multiplexor. The piece of equipment at the telephone company central office that provides the ADSL signal.

Dynamic Host Configuration Protocol.

DHCP is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software tracks IP addresses rather than requiring an administrator to manage the task. A new computer can be added to a network without the hassle of manually assigning it a unique IP address.

E

ESP

Encapsulating Security Payload.

ESSID

The Extended Service Set Identification (ESSID) is a thirty-two character (maximum) alphanumeric key identifying the wireless local area network.

Ethernet

A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks transmit packets at a rate of 10 Mbps.

F

Fast Ethernet

An Ethernet system that is designed to operate at 100 Mbps.

Filtering

The process of screening a packet for certain characteristics, such as source address, destination address, or protocol. Filtering is used to determine whether traffic is to be forwarded, and can also prevent unauthorized access to a network or network devices.

Forwarding

When a frame is received on an input port on a switch, the address is checked against the lookup table. If the lookup table has recorded the destination address, the frame is automatically forwarded on an output port.

Full-duplex

A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.

G

Gateway

A local device, usually a router, that connects hosts on a local network to other networks.

H

Half-duplex

A system that allows packets to transmitted and received, but not at the same time. Contrast with full-duplex.

hop count

The number of routers that a data packet passes through on its way to its destination.

I

ICMP

See “Internet Control Message Protocol” on page 7.

IEEE

Institute of Electrical and Electronics Engineers. This American organization was founded in 1963 and sets standards for computers and communications.

IETF

Internet Engineering Task Force. An organization responsible for providing engineering solutions for TCP/IP networks. In the network management area, this group is responsible for the development of the SNMP protocol.

IKE

Internet Key Exchange. An automated method for exchanging and managing encryption keys between two VPN devices.

Internet Control Message Protocol

ICMP is an extension to the Internet Protocol (IP) that supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

Internet Protocol

The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it among all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the Internet. Packets can arrive in a different order than they were sent. The Internet Protocol just delivers them. It's up to another protocol, the Transmission Control Protocol (TCP) to put them back in the right order. IP is a connectionless protocol, which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (The reason the packets do get put in the right order is because of TCP, the connection-oriented protocol that keeps track of the packet sequence in a message.) In the Open Systems Interconnection (OSI) communication model, IP is in Layer 3, the Networking Layer. The most widely used version of IP today is IP version 4 (IPv4). However, IP version 6 (IPv6) is also beginning to be supported. IPv6 provides for much longer addresses and therefore for the possibility of many more Internet users. IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.

IP

See "Internet Protocol" on page 7.

IP Address

A four-byte number uniquely defining each host on the Internet, usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57). Ranges of addresses are assigned by Internic, an organization formed for this purpose.

IPSec

Internet Protocol Security. IPSec is a series of guidelines for securing private information transmitted over public networks. IPSec is a VPN method providing a higher level of security than PPTP.

IPX

Short for Internetwork Packet Exchange, a networking protocol used by the Novell NetWare operating systems.

Like UDP/IP, IPX is a datagram protocol used for connectionless communications. Higher-level protocols, such as SPX and NCP, are used for additional error recovery services.

ISP

Internet service provider.

L

LAN

See “Local Area Network” on page 8.

LDAP

See “Lightweight Directory Access Protocol” on page 8.

Lightweight Directory Access Protocol

A set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. Unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access. Although not yet widely implemented, LDAP should eventually make it possible for almost any application running on virtually any computer platform to obtain directory information, such as e-mail addresses and public keys. Because LDAP is an open protocol, applications need not worry about the type of server hosting the directory.

Local Area Network

A communications network serving users within a limited area, such as one floor of a building. A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers and is limited to a distance of 1,500 feet. LANs can be connected together, but if modems and telephones connect two or more LANs, the larger network constitutes what is called a WAN or Wide Area Network.

M

MAC

(1) Media Access Control. In LANs, the sublayer of the data link control layer that supports medium-dependent functions and uses the services of the physical layer to provide services to the logical link control (LLC) sublayer. The MAC sublayer includes the method of determining when a device has access to the transmission medium. (2) Message Authentication Code. In computer security, a value that is a part of a message or accompanies a message and is used to determine that the contents, origin, author, or other attributes of all or part of the message are as they appear to be. (*IBM Glossary of Computing Terms*)

MAC address

The Media Access Control address is a unique 48-bit hardware address assigned to every network interface card. Usually written in the form 01:23:45:67:89:ab.

Maximum Receive Unit

The size in bytes of the largest packet that can be sent or received.

Maximum Transmit Unit

The size in bytes of the largest packet that can be sent or received.

Mbps

Megabits per second.

MD5

MD5 creates digital signatures using a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

When using a one-way hash function, one can compare a calculated message digest against the message digest that is decrypted with a public key to verify that the message hasn't been tampered with. This comparison is called a "hashcheck."

MDI/MDIX

In cable wiring, the concept of transmit and receive are from the perspective of the PC, which is wired as a Media Dependant Interface (MDI). In MDI wiring, a PC transmits on pins 1 and 2. At the hub, switch, router, or access point, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X). See “Auto-negotiation” on page 2.

Most Significant Bit or Most Significant Byte

MSB. The portion of a number, address, or field that is farthest left when written as a single number in conventional hexadecimal ordinary notation. The part of the number having the most value.

MSB

MSB. The portion of a number, address, or field that is farthest left when written as a single number in conventional hexadecimal ordinary notation. The part of the number having the most value.

MTU

The size in bytes of the largest packet that can be sent or received.

N

NAT

See “Network Address Translation” on page 10.

NetBIOS

Network Basic Input Output System. An application programming interface (API) for sharing services and information on local-area networks (LANs). Provides for communication between stations of a network where each station is given a name. These names are alphanumeric names, 16 characters in length.

netmask

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 router.
A number that explains which part of an IP address comprises the network address and which part is the host address on that network. It can be expressed in dotted-decimal notation or as a number appended to the IP address. For example, a 28-bit mask starting from the MSB can be shown as 255.255.255.192 or as /28 appended to the IP address.

Network Address Translation

Sometimes referred to as Transparent Proxying, IP Address Overloading, or IP Masquerading. Involves use of a device called a Network Address Translator, which assigns a contrived, or logical, IP address and port number to each node on an organization's internal network and passes packets using these assigned addresses.

NIC

Network Interface Card. An adapter in a computer which provides connectivity to a network.

NID

Network Interface Device. The point of demarcation, where the telephone line comes into the house.

O

OS

Operating System.

P

packet

A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.

Perfect Forward Secrecy

Perfect Forward Secrecy (PFS) provides additional security by means of a Diffie-Hellman shared secret value. With PFS, if one key is compromised, previous and subsequent keys are secure because they are not derived from previous keys.

PKIX

PKIX. The most widely used standard for defining digital certificates.

Point-to-Point Protocol

PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.

PPP

A protocol allowing a computer using TCP/IP to connect directly to the Internet.

PPPoA

PPPoA. PPP over ATM is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPPoE

PPPoE. PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPP over ATM

PPPoA. PPP over ATM is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPP over Ethernet

PPPoE. PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPTP

Point-to-Point Tunneling Protocol. A method for establishing a virtual private network (VPN) by embedding Microsoft’s network protocol into Internet packets.

Protocol

A set of rules for communication between devices on a network.

PSTN

Public Switched Telephone Network.

Public Key Infrastructure

PKIX. The most widely used standard for defining digital certificates.
X.509 is actually an ITU Recommendation, which means that it has not yet been officially defined or approved. As a result, companies have implemented the standard in different ways. For example, both Netscape and Microsoft use X.509 certificates to implement SSL in their Web servers and browsers. But an X.509 Certificate generated by Netscape may not be readable by Microsoft products, and vice versa.

Q

QoS

See “Quality of Service” on page 12.

Quality of Service

QoS is a networking term that specifies a guaranteed level of throughput. Throughput is the amount of data transferred from one device to another or processed in a specified amount of time - typically, throughputs are measured in bytes per second (Bps).

R

RFC

Request For Comment. Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFCs can be found at *www.ietf.org*.

RIP

See “Routing Information Protocol” on page 12.

router

A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

Routing Information Protocol

RIP is the routing protocol used by the routed process on Berkeley-derived UNIX systems. Many networks use RIP; it works well for small, isolated, and topologically simple networks.

S

Simple Network Management Protocol

SNMP is the protocol governing network management and the monitoring of network devices and their functions. It is not necessarily limited to TCP/IP networks.

SNMP

See “Simple Network Management Protocol” on page 12.

SSID

A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name. *See also* Wireless Network Name and ESSID.

Segment

A section of a LAN that is connected to the rest of the network using a switch, bridge, or repeater.

Subnet Mask

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 router.

Switch

A device that interconnects several LANs to form a single logical LAN that comprises of several LAN segments. Switches are similar to bridges, in that they connect LANs of a different type; however they connect more LANs than a bridge and are generally more sophisticated.

T

TCP/IP

The main internetworking protocols used in the Internet. The Internet Protocol (IP) used in conjunction with the Transfer Control Protocol (TCP) form TCP/IP.

U

Universal Plug and Play

UPnP. A networking architecture that provides compatibility among networking technology. UPnP compliant routers provide broadband users at home and small businesses with a seamless way to participate in online games, videoconferencing and other peer-to-peer services.

UTP

Unshielded twisted pair is the cable used by 10BASE-T and 100BASE-Tx Ethernet networks.

V

VPN

Virtual Private Network. A method for securely transporting data between two private networks by using a public network such as the Internet as a connection.

W

WAN

See “Wide Area Network” on page 14.

Web

Also known as World-Wide Web (WWW) or W3. An Internet client-server system to distribute information, based upon the hypertext transfer protocol (HTTP).

WEB Proxy Server

A Web proxy server is a specialized HTTP server that allows clients access to the Internet from behind a firewall. The proxy server listens for requests from clients within the firewall and forwards these requests to remote Internet servers outside the firewall. The proxy server reads responses from the external servers and then sends them to internal client clients.

Wide Area Network

A WAN is a computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

Windows Internet Naming Service

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using the Windows Network Neighborhood feature.

WINS

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

Wireless Network Name (SSID)

Wireless Network Name (SSID) is the name assigned to a wireless network. This is the same as the SSID or ESSID configuration parameter.

Index