

Reference Manual for the Model FVM318 Cable/DSL ProSafe Wireless VPN Security Firewall

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA
Phone 1-888-NETGEAR

SM-FVM318NA-0
December 2002

© 2002 by NETGEAR, Inc. All rights reserved.

Trademarks

NETGEAR, the Netgear logo, The Gear Guy, Everybody's Connecting and Auto Uplink are trademarks or registered trademarks of Netgear, Inc. in the United States and/or other countries. Microsoft and Windows are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other brand and product names are trademarks or registered trademarks of their respective holders. Information is subject to change without notice. All rights reserved.

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) Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) from all persons and must not be co-located or operating in conjunction with any other antenna or radio transmitter. Installers and end-users must follow the installation instructions provided in this user guide.

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 FVM318 Cable/DSL ProSafe Wireless VPN Security Firewall is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das FVM318 Cable/DSL ProSafe Wireless VPN Security 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 FVM318 Cable/DSL ProSafe Wireless VPN Security 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

PLEASE REFER TO THE SUPPORT INFORMATION CARD THAT SHIPPED WITH YOUR PRODUCT.

By registering your product at www.NETGEAR.com/register, we can provide you with faster expert technical support and timely notices of product and software upgrades.

NETGEAR, INC.

Support Information

Phone: 1-888-NETGEAR (For US & Canada only)

For other countries see your Support information card

E-mail: Support@NETGEAR.com

Web site: www.NETGEAR.com

Contents

Preface

About This Manual

Chapter 1

Introduction

Key Features of the FVM318	1-1
Virtual Private Networking (VPN)	1-1
Enhanced Wireless Security Through IPSec	1-2
A Powerful, True Firewall with Content Filtering	1-2
Autosensing Ethernet Connections with Auto Uplink™	1-2
Extensive Protocol Support	1-3
Easy Installation and Management	1-4
What's in the Box?	1-5
The Firewall's Front Panel	1-5
The Firewall's Rear Panel	1-7

Chapter 2

Connecting the Firewall to the Internet

What You Will Need Before You Begin	2-1
Cabling and Computer Hardware Requirements	2-1
Network Configuration Requirements	2-1
Internet Configuration Requirements	2-2
Where Do I Get the Internet Configuration Parameters?	2-2
Connecting the FVM318 to Your LAN	2-4
PPPoE Wizard-Detected Option	2-9
Dynamic IP Wizard-Detected Option	2-10
Fixed IP Account Wizard-Detected Option	2-11
Manually Configuring Your Internet Connection	2-12

Chapter 3

Wireless Configuration

Considerations For A Wireless Network	3-1
---	-----

Observe Performance, Placement and Range Guidelines	3-1
Implement Appropriate Wireless Security	3-2
Understanding Wireless Settings	3-3
Wireless Network Settings	3-3
Restricting Access Based on the Wireless Card Access List	3-4
Choosing Authentication and Security Encryption Methods	3-4
Automatic Authentication Scheme Selection	3-4
Encryption Strength Choices	3-5
Disable 3-5	
IPSec 3-5	
64 or 128 bit WEP 3-6	
Configuring IPSec Wireless Connections	3-12
Using SoftRemoteLT Instead of SoftRemote Basic	3-17

Chapter 4

Protecting Your Network

Protecting Access to Your FVM318 firewall	4-1
Configuring Basic Firewall Services	4-3
Blocking Functions, Keywords, Sites, and Services	4-3
Blocking Services	4-5
Setting Times and Scheduling Firewall Services	4-7

Chapter 5

Virtual Private Networking

FVM318 VPN Overview	5-1
FVM318 VPN Configuration Planning	5-3
Network to Network VPN Tunnel Configuration Worksheet 5-4	
Network Configuration Settings 5-5	
PC to Network VPN Tunnel Configuration Worksheet 5-9	
Monitoring the PC VPN Connection Using SafeNet Tools	5-18
Manual Keying	5-19
Blank VPN Tunnel Configuration Worksheets	5-22

Chapter 6

Managing Your Network

Network Management Information	6-1
Viewing Router Status and Usage Statistics	6-1
Viewing Attached Devices	6-4

Viewing, Selecting, and Saving Logged Information	6-5
Selecting What Information to Include in the Log	6-6
Enabling SYSLOG	6-7
Examples of log messages	6-7
Activation and Administration	6-7
Dropped Packets	6-7
Enabling Security Event E-mail Notification	6-8
Backing Up, Restoring, or Erasing Your Settings	6-9
Running Diagnostic Utilities and Rebooting the Router	6-11
Enabling Remote Management	6-12
Upgrading the Router's Firmware	6-13
Chapter 7	
Advanced Configuration	
Configuring Advanced Security	7-1
Setting Up A Default DMZ Server	7-1
Respond to Ping on Internet WAN Port	7-2
Configuring LAN IP Settings	7-2
LAN TCP/IP Setup	7-2
MTU Size	7-4
Using the Router as a DHCP Server	7-4
Configuring Dynamic DNS	7-7
Using Static Routes	7-8
Chapter 8	
Troubleshooting	
Basic Functions	8-1
Power LED Not On	8-2
Test LED Never Turns On or Test LED Stays On	8-2
Local or Internet Port Link LEDs Not On	8-2
Troubleshooting the Web Configuration Interface	8-3
Troubleshooting the ISP Connection	8-4
Troubleshooting a TCP/IP Network Using a Ping Utility	8-5
Restoring the Default Configuration and Password	8-7
Problems with Date and Time	8-8

Appendix A
Technical Specifications

Appendix B
Network, Routing, Firewall, and Wireless Basics

Related Publications	B-1
Basic Router Concepts	B-1
Internet Security and Firewalls	B-10
Wireless Networking	B-12
Wireless Network Configuration	B-12
Ad Hoc Mode (Peer-to-Peer Workgroup)	B-12
Infrastructure Mode	B-12
Extended Service Set Identification (ESSID)	B-13
Authentication and WEP Encryption	B-13
802.11b Authentication	B-13
Open System Authentication	B-14
Shared Key Authentication	B-15
Overview of WEP Parameters	B-16
Key Size	B-17
WEP Configuration Options	B-17
Wireless Channel Selection	B-18
Ethernet Cabling	B-19
How Does VPN Work?	B-21
IKE: Managing and Exchanging Keys	B-21
Negotiating the SA - the Internet Key Exchange (IKE)	B-22
Authentication: Phase 1	B-22
Key Exchange: Phase 2	B-23
Two Common Applications of VPN	B-23
Accessing Network Resources from a VPN Client PC	B-23
Linking Two Networks Together	B-24
Additional Reading	B-24

Appendix C
Preparing Your Network

Preparing Your Computers for TCP/IP Networking	C-1
Configuring Windows 95, 98, and Me for TCP/IP Networking	C-2
Configuring Windows NT4, 2000 or XP for IP Networking	C-7

Configuring the Macintosh for TCP/IP Networking	C-17
Verifying the Readiness of Your Internet Account	C-19
Restarting the Network	C-22

Glossary

Index

List of Procedures

Procedure 2-1: Record Your Internet Connection Information	2-3
Procedure 2-2: Connecting the Firewall to Your LAN	2-4
Procedure 2-3: Configuring the Internet Connection Manually	2-13
Procedure 3-1: Set Up and Test Basic Wireless Connectivity	3-7
Procedure 3-2: Restrict Wireless Access by MAC Address	3-9
Procedure 3-3: Configure WEP	3-10
Procedure 3-4: Configure Basic IPSec Wireless Connections	3-13
Procedure 3-5: Configuring the SoftRemoteLT Full Client	3-18
Procedure 4-1: Changing the Administrator Password	4-1
Procedure 4-2: Changing the Administrator Login Timeout	4-3
Procedure 4-3: Blocking Functions, Keywords, and Sites	4-4
Procedure 4-4: Configuring Services Blocking	4-6
Procedure 4-5: Setting Your Time Zone	4-8
Procedure 4-6: Scheduling Firewall Services	4-9
Procedure 5-1: Configuring a Network to Network VPN Tunnel	5-4
Procedure 5-2: Configuring a Remote PC to Network VPN	5-8
Procedure 5-3: Deleting a Security Association	5-19
Procedure 5-4: Using Manual Keying as an Alternative to IKE	5-19
Procedure 6-1: Backup the Configuration to a File	6-9
Procedure 6-2: Restore a Configuration from a File	6-10
Procedure 6-3: Erase the Configuration	6-10
Procedure 6-4: Configure Remote Management	6-12
Procedure 6-5: Router Upgrade	6-14
Procedure 7-1: Using Reserved IP Addresses	7-5
Procedure 7-2: Configuring LAN TCP/IP Settings	7-6
Procedure 7-3: Configuring Dynamic DNS	7-7
Procedure 7-4: Configuring Static Routes	7-9
Procedure 8-5: Testing the LAN Path to Your Firewall	8-6
Procedure 8-6: Testing the Path from Your PC to a Remote Device	8-7
Procedure 8-7: Using the Default Reset button	8-8

Preface

About This Manual

Thank you for purchasing the NETGEAR® FVM318 Cable/DSL ProSafe Wireless VPN Security Firewall. This manual describes the features of the firewall and provides installation and configuration instructions.

Audience

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

Typographical Conventions

This guide uses the following typographical conventions:

italics Media titles, UNIX files, commands, URLs, and directory names.

bold times roman User input

Internet Protocol (IP) First time an abbreviated term is used.

`courier font` Screen text, user-typed command-line entries.

[Enter] Named keys in text are shown enclosed in square brackets. The notation [Enter] is used for the Enter key and the Return key.

[Ctrl]+C Two or more keys that must be pressed simultaneously are shown in text linked with a plus (+) sign.

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.



Warning: This format is used to highlight information about the possibility of injury or equipment damage.



Danger: This format is used to alert you that there is the potential for incurring an electrical shock if you mishandle the equipment.

Chapter 1

Introduction

This chapter describes the features of the NETGEAR® FVM318 Cable/DSL ProSafe Wireless VPN Security Firewall.

Key Features of the FVM318

The FVM318 firewall is a complete security solution that protects your network from attacks and intrusions while allowing secure connections with other trusted users over the Internet and across your local wireless network.

Unlike simple Internet sharing routers that rely on network address translation (NAT) for security, the FVM318 firewall uses Stateful Packet Inspection, widely considered as the most effective method of filtering IP traffic, to ensure secure firewall filtering. The FVM318 firewall allows Internet access for up to 253 users.

Applying the full strength of Internet Protocol Security (IPSec) encryption across the wireless network, the FVM318 firewall provides a level of wireless security unmatched by other wireless routers that use WEP encryption.

Virtual Private Networking (VPN)

The FVM318 firewall provides a secure encrypted connection between your local area network (LAN) and remote networks or clients. It includes the following VPN features:

- Supports 70 external VPN connections and 32 local wireless VPN connections.
- Supports industry standard VPN protocols
The FVM318 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.

Enhanced Wireless Security Through IPSec

The FVM318 firewall allows you to easily create an IPSec-encrypted VPN tunnel from your wireless PC to the firewall.

- Easy to deploy - The included SafeNet SoftRemote Basic VPN client requires only three parameters to configure a secure connection to the firewall.
- 256 bit AES encryption provides a much higher level of protection than WEP.

A Powerful, True Firewall with Content Filtering

Unlike simple Internet sharing NAT routers, the FVM318 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 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 FVM318 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.

- With its content filtering feature, the FVM318 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.

Autosensing Ethernet Connections with Auto Uplink™

With its internal 8-port 10/100 switch, the FVM318 can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. The LAN 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.

Extensive Protocol Support

The FVM318 supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). [Appendix B-1, “Network, Routing, Firewall, and Wireless Basics”](#) provides further information on TCP/IP.

- IP Address Sharing by NAT

The FVM318 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 FVM318 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. See [Appendix C-1, “Preparing Your Computers for TCP/IP Networking”](#) for instructions on configuring your computers for DHCP.

- DNS Proxy

When DHCP is enabled and no DNS addresses are specified, the firewall provides its own address as a DNS server to the attached PCs. The firewall obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.

- Point-to-Point Protocol over Ethernet (PPPoE)

PPPoE connects computers 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, and 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 a Dynamic DNS service to register your dynamic IP address.

Easy Installation and Management

You can install, configure, and operate the FVM318 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 Configuration Manager.

- 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 FVM318 when you 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

What's in the Box?

The product package should contain the following items:

- FVM318 Cable/DSL ProSafe Wireless VPN Security Firewall.
- AC power adapter.
- Category 5 (CAT5) Ethernet cable.
- *FVM318 Resource CD*, including:
 - This manual.
 - Application Notes, Tools, and other helpful information.
 - SafeNet SoftRemote Basic VPN client software.
- 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 FVM318 ([Figure 1-1](#)) contains various status LEDs.

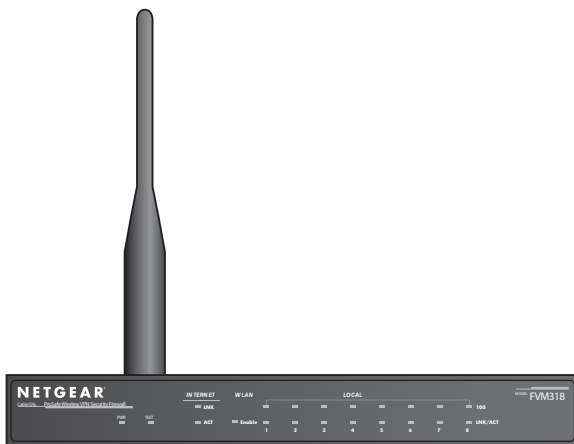


Figure 1-1: FVM318 Front Panel

You can use some of the LEDs to identify the status of the firewall and verify connections. [Table 1-1](#) 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 1-1: 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 LINK	On	The port detected a link with the Internet WAN connection.
ACT	On/Blinking	Blinking indicates data transmission.
WLAN	On	The wireless interface is enabled.
LOCAL 100	On Off	The Local port is operating at 100 Mbps. Indicates data transmission at 10 Mbps.
LINK/ACT	On/Blinking	The Local port has detected a link with a LAN connection. Blinking indicates data transmission.

The Firewall's Rear Panel

The rear panel of the FVM318 (Figure 1-2) contains the connections identified below.

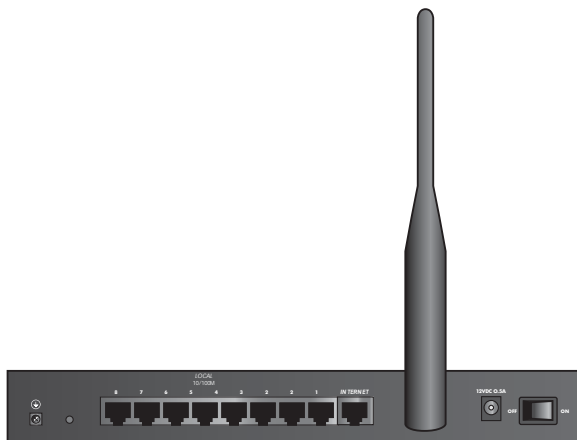


Figure 1-2: FVM318 Rear Panel

Viewed from left to right, 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.
- Wireless antenna.
- AC power adapter input.
- Power switch.

Chapter 2

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 FVM318 Cable/DSL ProSafe Wireless VPN Security 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 begin:

1. Have active Internet service such as that provided by a cable or DSL broadband account.
2. Locate the Internet Service Provider (ISP) configuration information for your account.
3. Connect the firewall to a cable or DSL modem and a computer as explained below.

Cabling and Computer Hardware Requirements

To use the FVM318 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.

Network Configuration Requirements

The FVM318 includes a built-in Web Configuration Manager. To access the configuration menus on the FVM318, you must use a Java[®]-enabled web browser program which supports HTTP uploads such as Microsoft Internet Explorer or Netscape[®] Navigator. NETGEAR recommends using Internet Explorer 5.0 or Netscape Navigator 4.7 or above. Free browser programs are readily available for Windows[®], Macintosh[®], or UNIX[®]/Linux[®].

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: For help with DHCP configuration, please refer to [Appendix C, "Preparing Your Network"](#).

The cable or DSL modem broadband access device must provide a standard 10 Mbps (10BASE-T) Ethernet interface.

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 IP Address which is also known as 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 provides 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. Record all the settings for each tab page.
 - For Windows 2000/XP, open the Local Area Network Connection, select the TCP/IP entry for the Ethernet adapter, and click Properties. Record all the settings for each tab page.
 - For Macintosh® computers, open the TCP/IP or Network control panel. Record all the settings for each section.
- You may also refer to the NETGEAR Router ISP Guide on the *FVM318 Resource CD* which provides Internet connection information for many ISPs.

Once you locate your Internet configuration parameters, record them on the page below.

Procedure 2-1: Record 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: _____

For Wireless Access: For configuration of the wireless network, record the following:

Wireless Network Name (SSID): _____

Encryption (circle one): WEP 64, WEP 128, or IPsec

WEP or IPsec key: _____

Connecting the FVM318 to Your LAN

This section provides instructions for connecting the FVM318 Cable/DSL ProSafe Wireless VPN Security Firewall to your LAN. The *Resource CD* included with your firewall contains an animated Installation Assistant to help you through this procedure.

Procedure 2-2: Connecting the Firewall to Your LAN

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.

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

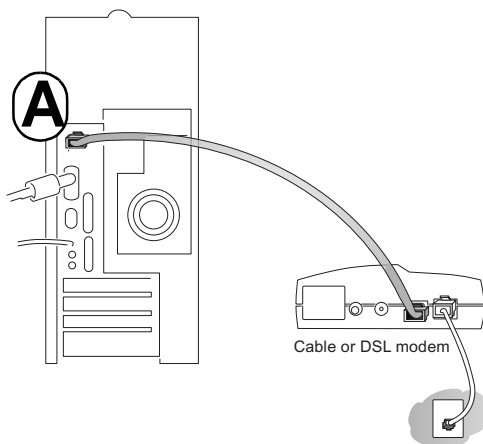


Figure 2-1: Disconnect the cable or DSL Modem

- c. Connect the Ethernet cable (A) from the modem to the FVM318's Internet port.

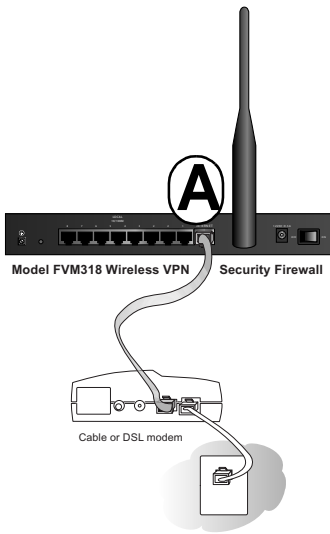


Figure 2-2: Connect the cable or DSL Modem to the firewall

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

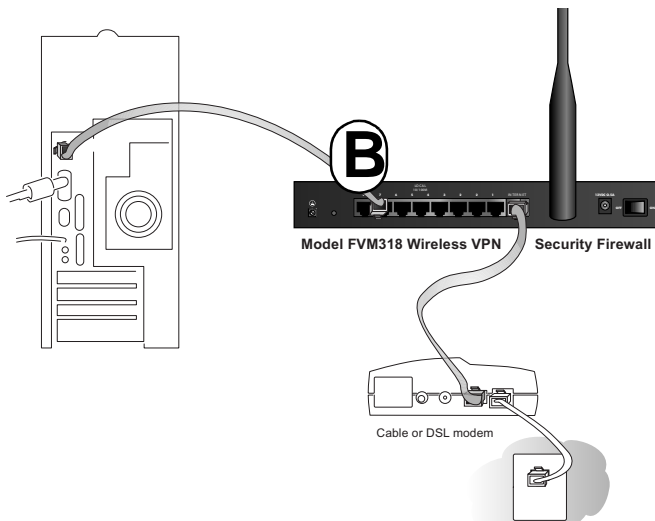


Figure 2-3: Connect the computers on your network to the firewall

Note: The FVM318 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 modem and wait about 30 seconds for the lights to stop blinking.
- f. Turn on the firewall and wait for the Test light to stop blinking.
- g. Now, turn on your computer. If you usually run software to log in to your Internet connection, do not run that software.
- h. Now that the modem, firewall, and computer are turned on, verify the following:
 - When 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 INTERNET LINK light is lit, indicating a link has been established to the cable or DSL modem.
 - The firewall's LOCAL LINK/ACT lights are lit for any computers connected to it.

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



Figure 2-4: Log in to the firewall.

A login window opens like the one shown below.

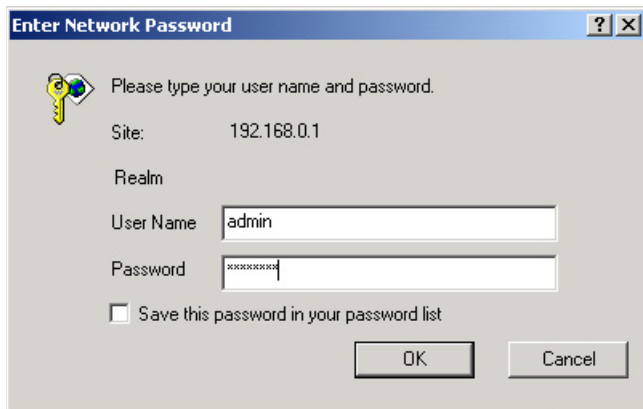


Figure 2-5: Login window

- b. 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**

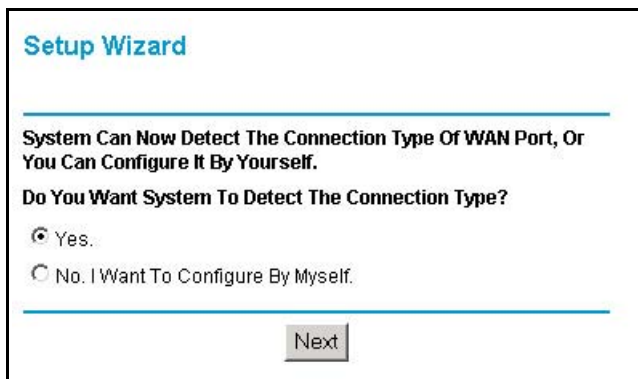


Figure 2-6: Setup Wizard

- 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.
- 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 [“Manually Configuring Your Internet Connection”](#) on page 2-12.

Unless your ISP assigns your configuration automatically via DHCP, you will need the configuration parameters from your ISP as you recorded them previously in [“Record Your Internet Connection Information”](#) on page 2-3.

- c. When the firewall successfully detects an active Internet service, 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 protocols such as PPPoE.

Note: Customers in Austria or Australia who use Internet accounts which require login will have to use the manual configuration procedure, [“Manually Configuring Your Internet Connection”](#) on page 2-12. The Smart Wizard will not detect these options.
 - 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.

PPPoE Wizard-Detected Option

If the Setup Wizard discovers that your ISP uses PPPoE, you will see this menu:

Figure 2-7: Setup Wizard menu for PPPoE accounts

- Enter the Account Name, Domain Name, Login, and password as provided by your ISP. These fields are case sensitive. The firewall will try to discover the domain automatically if you leave the Domain Name blank. Otherwise, you may need to enter it manually.
- To change the login timeout, enter a new value in minutes. This determines how long the firewall keeps the Internet connection active after there is no Internet activity from the LAN. Entering a timeout value of zero means never log out.

Note: You no longer need to run 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.

- 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: If you enter DNS addresses, restart your computers so that these settings take effect.

- Click Apply to save your settings.
- Click Test to verify that your Internet connection works. If the NETGEAR website does not appear within one minute, refer to [Chapter 8, Troubleshooting](#).

Dynamic IP Wizard-Detected Option

If the Setup Wizard discovers that your ISP uses Dynamic IP assignment, you will see this menu:

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

Secondary DNS

Router's MAC Address

Use Default Address

Use This MAC Address

Figure 2-8: Setup Wizard menu for Dynamic IP address accounts

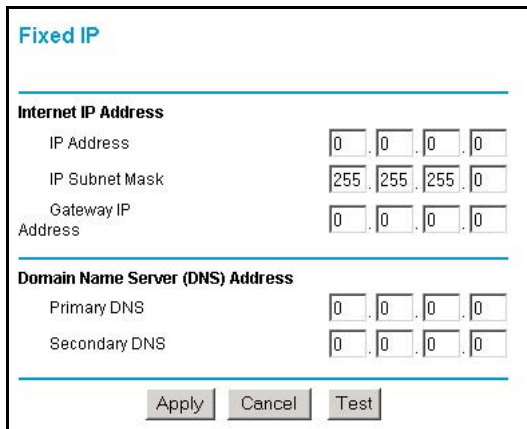
- Enter your Account Name (may also be called Host Name) and Domain Name. These parameters may be necessary to access your ISP's services such as mail or news servers. If you leave the Domain Name field blank, the firewall try to discover the domain. Otherwise, you may need to enter it manually.
- If 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: If you enter DNS addresses, restart your computers so that these settings take effect.

- Click Apply to save your settings.
- Click Test to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to [Chapter 8, Troubleshooting](#).

Fixed IP Account Wizard-Detected Option

If the Setup Wizard discovers that your ISP uses Fixed IP assignment, you will see this menu:



The screenshot shows a configuration window titled "Fixed IP". It is divided into two main sections: "Internet IP Address" and "Domain Name Server (DNS) Address".

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

At the bottom of the window are three buttons: "Apply", "Cancel", and "Test".

Figure 2-9: Setup Wizard menu for Fixed IP address accounts

- Fixed IP is also called Static IP. 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 ["Record Your Internet Connection Information"](#) on page 2-3.
- Enter the IP address of your ISP's Primary and Secondary DNS Server addresses.

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

- Click Apply to save the settings.
- Click Test to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to [Chapter 8, Troubleshooting](#).

Manually Configuring 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)
 Domain Name (If Required)

Internet IP Address

- Get dynamically from ISP
 Use static IP address

IP Address
 IP Subnet Mask
 Gateway IP Address

Domain Name Server (DNS) Address

- Get automatically from ISP
 Use these DNS servers

Primary DNS
 Secondary DNS

Router's MAC address

- Use Default Address
 Use This Computer's MAC
 Use This MAC Address

ISP Does Require Login

Basic Settings

Does your Internet connection require a login?

- No
 Yes

Internet Service Provider Name
 Account Name
 Domain Name

Login
 Password

Idle Timeout Minutes

Domain Name Server (DNS) Address

- Get automatically from ISP
 Use these DNS servers

Primary DNS
 Secondary DNS

Router's MAC address

- Use Default Address
 Use This Computer's MAC
 Use This MAC Address

Figure 2-10: Browser-based configuration Basic Settings menus

Procedure 2-3: Configuring the Internet Connection Manually

You can manually configure the firewall using the Basic Settings menu shown in [Figure 2-10](#) 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 3.
 - 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.

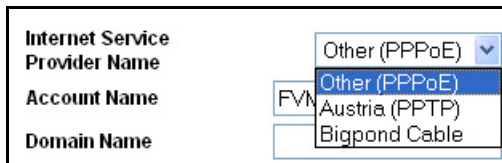
Note: After completing the DNS configuration, restart the computers on your network so that these settings take effect.
 - d. Gateway's MAC Address:
This section determines the Ethernet MAC address that will be used by the firewall on the Internet port. Some ISPs will register the Ethernet MAC address 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. Select your Internet service provider from the drop-down list.



The screenshot shows a configuration window with three text input fields on the left: "Internet Service Provider Name", "Account Name", and "Domain Name". To the right of these fields is a vertical stack of three dropdown menus. The top dropdown menu is open, showing a list of options: "Other (PPPoE)", "Other (PPPoE)", "Austria (PPTP)", and "Bigpond Cable". The first "Other (PPPoE)" option is highlighted in blue. The middle dropdown menu is partially visible and shows the text "FVM". The bottom dropdown menu is empty.

Figure 2-11: 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 2-9](#).
- d. Click Apply to save your settings.

Chapter 3

Wireless Configuration

This chapter describes how to configure the wireless features of your FVM318 Cable/DSL ProSafe Wireless VPN Security Firewall.

Considerations For A Wireless Network

In planning your wireless network, you should consider the level of security required. You should also select the physical placement of your firewall in order to maximize the network speed. For further information on wireless networking, refer to [“Wireless Networking”](#) in [Appendix B, “Network, Routing, Firewall, and Wireless Basics.”](#)

Observe Performance, Placement and Range Guidelines

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless firewall. The latency, data throughput performance, and notebook power consumption properties vary depending on your configuration choices.



Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router. For complete range/performance specifications, please see [Appendix A, “Technical Specifications.”](#)

For best results, place your firewall:

- Near the center of the area in which your PCs will operate.
- In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).
- Away from sources of interference, such as PCs, microwaves, and 2.4 GHz cordless phones.
- Away from large metal surfaces.

The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP and IPSec connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook PC but IPSec can use less.

Implement Appropriate Wireless Security

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment.



Note: Indoors, computers can connect over 802.11b wireless networks at a maximum range of up to 500 feet. Such distances can allow for others outside of your immediate area to access your network. It is important to take appropriate steps to secure your network from unauthorized access. The FVM318 firewall provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

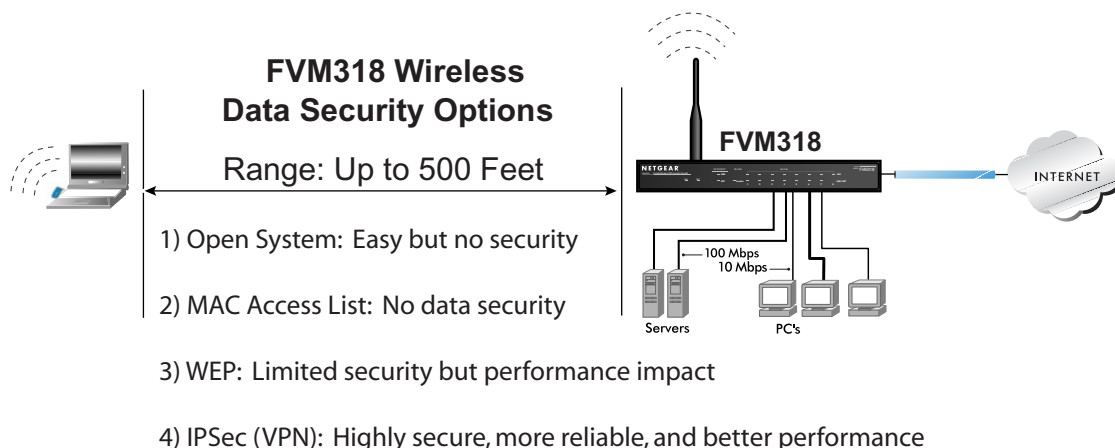


Figure 3-1: FVM318 wireless data security options

Restricting access by MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed. To block a determined eavesdropper, you should use one of the data encryption options of the firewall. Wired Equivalent Privacy (WEP) data encryption provides some security. However, a determined intruder can compromise WEP, there may be degradation of the data throughput on the wireless link, and WEP configurations can be less reliable. Unique to the FVM318, you can use the highly secure, reliable, high performance IPSec VPN communications protocols for your wireless connection.

Understanding Wireless Settings

To configure the Wireless settings of your firewall, click the Wireless link in the main menu of the browser interface. The Wireless Settings menu will appear, as shown below.



The screenshot shows a web interface titled "Wireless Settings". Below the title is a horizontal line. Underneath, the section "Wireless Network" is displayed. It contains three configuration fields: "Name(SSID) :" with a text input field containing "Wireless"; "Region :" with a dropdown menu showing "USA"; and "Channel :" with a dropdown menu showing "1".

Figure 3-2: Wireless Settings menu

Wireless Network Settings

The Wireless Settings menu sections are discussed below.

- **Name (SSID).** The Service Set Identification is also known as the wireless network name. Enter a value of up to 32 alphanumeric characters. Wireless access point devices like the FVM318 broadcast the SSID and any other wireless node in the same area can receive this SSID. This is not a security feature. It is simply the name of the wireless network. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device you want to participate in this wireless network will need to use this SSID. The FVM318 default SSID is: **Wireless**.
- **Region.** This field identifies the region where the FVM318 can be used. It may not be legal to operate the wireless features of the firewall in a region other than one of those identified on this drop-down list.
- **Channel.** This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby access point. For more information on the wireless channel frequencies please refer to [“Wireless Channel Selection” on page B-18](#).

Restricting Access Based on the Wireless Card Access List



Figure 3-3: Wireless Card Access List menu

This setting determines which hardware devices will be allowed to connect to the firewall.

- Everyone. The FVM318 will not restrict wireless access based on MAC address.
- Trusted PCs Only. Requires specifying the MAC address in the list if trusted PC MAC addresses before any device connecting wirelessly to the FVM318 will be allowed to connect to the firewall.

Choosing Authentication and Security Encryption Methods

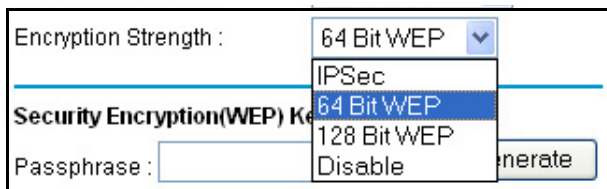


Figure 3-4: Encryption Strength



Note: Whichever Security Encryption settings you choose for the FVM318 will be enforced for all wireless connections. For example, if you choose IPsec, then the only wireless connections allowed will be those established according to the VPN tunnel settings you specify.

Automatic Authentication Scheme Selection

The FVM318 automatically selects the wireless appropriate authentication scheme based on the encryption strength you choose.

- For WEP encryption, the FVM318 will enforce the shared key wireless authentication scheme.
- For IPsec, the FVM318 will enforce the IPsec pre-shared key authentication scheme.
- For Disable, the FVM318 will use the Open System authentication scheme.

If your wireless adapter requires you to configure an authentication scheme, set it accordingly. Please refer to [“Authentication and WEP Encryption”](#) on page B-13 for a full explanation of each of these options, as defined by the IEEE 802.11b wireless communication standard.

Encryption Strength Choices

Choose the encryption strength from the drop-down list.

Disable

No encryption will be applied. This setting is useful for troubleshooting your wireless connection, but leaves your wireless data fully exposed.

IPSec

Selecting IPSec displays the IPSec connection list. Click Add to configure a new IPSec connection. To edit an existing connection, click the radio button next to the connection on the list, then click Edit. The IPSec settings screens are shown below.

IPSec Main and Aggressive Mode Settings

Wireless IPSEC Client Settings - Aggressive Mode	Wireless IPSEC Client Settings - Main Mode
Connection Name	Connection Name
User Name(Remote IPSEC Identifier)	Wireless Client IP Address
Pre-Shared Key	Pre-Shared Key
Mode: Aggressive Mode	Mode: Main Mode
Encryption Protocol: AES-256	Encryption Protocol: DES
Buttons: Back, Apply, Cancel	Buttons: Back, Apply, Cancel

Figure 3-5: IPSec main or aggressive mode settings

- Choose Aggressive or Main Mode. Aggressive Mode is the default. Aggressive Mode is required when you use the SafeNet SoftRemote Basic VPN Client for Windows which is included on the *FVM318 Resource CD*.
- Select the Encryption Protocol.

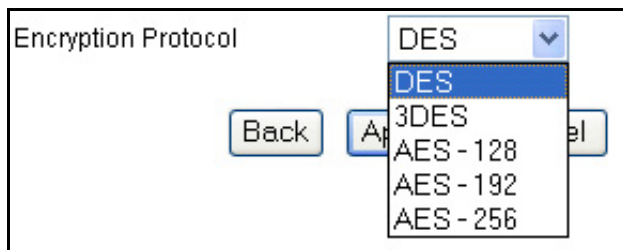


Figure 3-6: IPsec encryption protocol

DES is the least strong and AES - 256 is the strongest. AES - 256 is the default. The SafeNet SoftRemote Basic VPN Client for Windows requires either 3DES or AES - 256.

- 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. 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.

Once you have filled in the FVM318 settings, configure the wireless client accordingly.

64 or 128 bit WEP

When 64 Bit WEP or 128 Bit WEP is selected, WEP encryption will be applied.

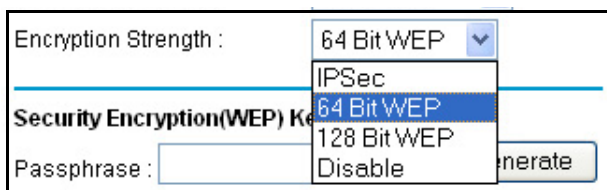


Figure 3-7: Encryption Strength

WEP provides some degree of privacy, but can be defeated without great difficulty. If WEP is enabled, you can manually or automatically program the four data encryption keys. These values must be identical on all PCs and access points in your network.

The screenshot shows a configuration window titled "Security Encryption". At the top, "Encryption Strength" is set to "64 Bit WEP" via a dropdown menu. Below this, the "Security Encryption(WEP) Key" section contains a "Passphrase" field with the text "\$9v!q~*g>" and a "Generate" button. There are four key fields: "Key1" (selected with a radio button) containing "e1c16b822e", "Key2" containing "c7d3183f58", "Key3" containing "11cd105216", and "Key4" containing "2034cf2b82". At the bottom of the window are "Apply" and "Cancel" buttons.

Figure 3-8: 64 or 128 bit WEP encryption strength

Please refer to [“Overview of WEP Parameters” on page B-16](#) for a full explanation of each of these options, as defined by the IEEE 802.11b wireless communication standard.

There are two methods for creating WEP encryption keys:

- **Passphrase.** Enter a word or group of printable characters in the Passphrase box and click the Generate button.
- **Manual.** 64-bit WEP: Enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F).
128-bit WEP: Enter 26 hexadecimal digits (any combination of 0-9, a-f, or A-F).

Clicking the radio button selects which of the four keys will be active.

Procedure 3-1: Set Up and Test Basic Wireless Connectivity

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

1. Log in to the FVM318 firewall at its default LAN address of <http://192.168.0.1> with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click the Wireless Settings link in the main menu of the FVM318 firewall.



The screenshot shows the 'Wireless Settings' configuration page. It features a header 'Wireless Settings' and a section titled 'Wireless Network'. Under this section, there are three configuration fields: 'Name(SSID):' with a text input field containing the value 'Wireless'; 'Region:' with a dropdown menu currently set to 'USA'; and 'Channel:' with a dropdown menu currently set to '1'.

Figure 3-9: Wireless Settings menu

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

Wireless access point devices like the FVM318 broadcast the SSID and any other wireless node in the same area can receive this SSID. This is not a security feature. It is simply the name of the wireless network. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device you want to participate in this wireless network will need to use this SSID.

Note: The SSID of any wireless access adapters must match the SSID you configure in the FVM318 Cable/DSL ProSafe Wireless VPN Security Firewall. If they do not match, you will not get a wireless connection to the FVM318.

4. Set the Region. Select the region in which the wireless interface will operate.
5. Set the Channel. The default channel is 6.

This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless router or access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your firewall. For more information on the wireless channel frequencies please refer to [“Wireless Channel Selection” on page B-18](#).

6. For initial configuration and test, leave the Wireless Card Access List set to “Everyone” and the Encryption Strength set to “Disabled.”
7. Click Apply to save your changes.



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

8. Configure and test your PCs for wireless connectivity.

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

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

Procedure 3-2: Restrict Wireless Access by MAC Address

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

1. Log in to the FVM318 firewall at its default LAN address of <http://192.168.0.1> with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click the Wireless Settings link in the main menu of the FVM318 firewall.
3. From the Wireless Settings menu, click the Trusted PCs button to display the Wireless Access menu shown below.

#	Device Name	MAC Address
1	jsmith_laptop	00:30:AB:07:33:13

Figure 3-10. Wireless Access menu

4. Enter the MAC address of the authorized PC. Enter a descriptive name for the PC in the Device Name field. The MAC address is usually printed on the wireless card, or it may appear in the firewall's "Attached Devices" DHCP table.

Note: You can copy and paste the MAC addresses from the firewall's Attached Devices menu into the MAC Address box of this menu. To do this, configure each wireless PC to obtain a wireless link to the firewall. The PC should then appear in the Attached Devices menu.

5. Click Add to save your entry.
6. Click Back to return to the Wireless Settings menu
7. Be sure that the Trusted PCs only radio button is selected, then click Apply.

To edit a MAC address from the table, click on it to select it, then click the Edit or Delete button.



Note: When configuring the firewall from a wireless PC whose MAC address is not in the Trusted PC list, if you select Trusted PCs only, you will lose your wireless connection when you click on Apply. You must then access the firewall from a wired PC to make any further changes.

Procedure 3-3: Configure WEP

To configure WEP data encryption, follow these steps:

1. Log in to the FVM318 firewall at its default LAN address of <http://192.168.0.1> with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click the Wireless Settings link in the main menu of the FVM318 firewall.

- From the Security Encryption menu drop-down list, select the WEP encryption type you will use.

Security Encryption

Encryption Strength : 64 Bit WEP

Security Encryption(WEP) Key

Passphrase : \$9v!q~/*g>

Key1 : e1c16b822e

Key2 : c7d3183f58

Key3 : 11cd105216

Key4 : 2034cf2b82

Figure 3-11. Wireless Settings encryption menu

- You can manually or automatically program the four data encryption keys. These values must be identical on all PCs and Access Points in your network.
 - Automatic - Enter a word or group of printable characters in the Passphrase box and click the Generate button. The four key boxes will be automatically populated with key values.
 - Manual - Enter ten hexadecimal digits (any combination of 0-9, a-f, or A-F) Select which of the four keys will be active.

Please refer to [“Overview of WEP Parameters”](#) on page B-16 for a full explanation of each of these options, as defined by the IEEE 802.11b wireless communication standard.

- Click Apply to save your settings.



Note: When configuring the firewall from a wireless PC, if you configure WEP settings, you will lose your wireless connection when you click on Apply. You must then either configure your wireless adapter to match the firewall WEP settings or access the firewall from a wired PC to make any further changes.

Configuring IPsec Wireless Connections

Unique to the FVM318, you have the option of using the highly secure VPN communications protocols over your wireless connection.

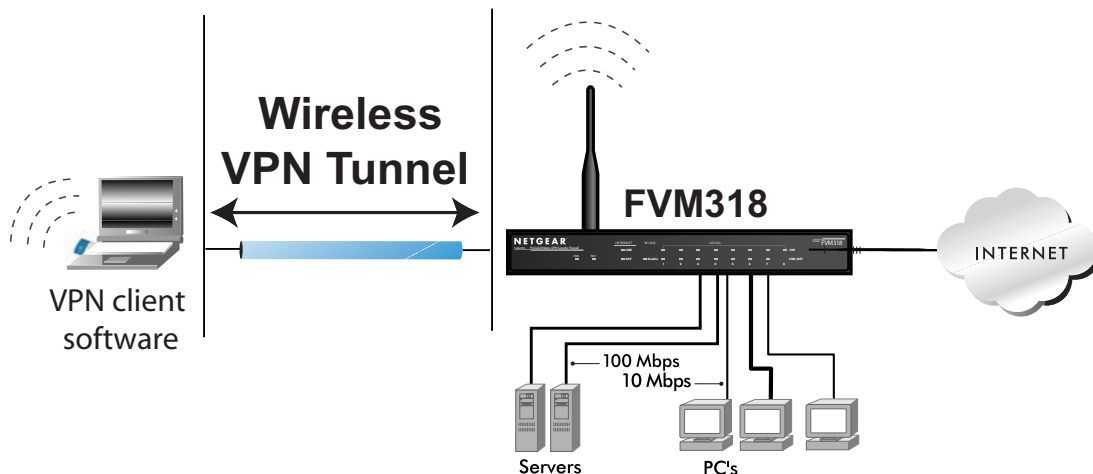


Figure 3-12. Configuring basic wireless IPsec VPN tunnel connections

To use the IPsec features of the FVM318, you must have VPN client software installed on your PC. The SafeNet SoftRemote Basic VPN client software included on the *FVM318 Resource CD* provides a simple and very easy way to set up wireless VPN connections to the FVM318. However, it only works with FVM318 wireless connections.

If you prefer the flexibility of using one VPN client software program for both your local wireless connections and remote VPN connections, then you should consider the SoftRemoteLT client which lets you pick from multiple configurations, depending on whether you are connecting over a local wireless link to the FVM318 or remotely over the Internet. Instructions for configuring the SoftRemote SoftRemoteLT for local wireless VPN connections to the FVM318 can be found at [“Using SoftRemoteLT Instead of SoftRemote Basic” on page 3-17](#). Instructions for configuring the SoftRemote SoftRemoteLT for remote VPN connections over the Internet to the FVM318 can be found at [“PC to LAN VPN access from a PC to an FVM318” on page 5-9](#).

Procedure 3-4: Configure Basic IPSec Wireless Connections

The SafeNet SoftRemote Basic VPN client installer program is on the *FVM318 Resource CD*. Observe the following guidelines when using the SafeNet SoftRemote Basic VPN client:

- The SoftRemote Basic client requires Windows 95 or later.
- The SoftRemote Basic client may not be compatible with other VPN clients. In this case you must uninstall the other client before installing SoftRemote Basic.
- If your PC will also be used for remote VPN connections, you should use the full version of SafeNet SoftRemote, not the Basic version.

1. Configure the FVM318 settings.

- Log in to the FVM318 at <http://192.168.0.1> with its default user name of **admin** and default password of **password**, or using whatever user name, password you have set up.
- Click the Wireless link in the main menu Setup section to display the menu shown below.

Wireless Settings

Wireless Network

Name (SSID):

Region:

Channel:

Wireless Card Access List

Everyone

Trusted PCs only

Security Encryption

Encryption Strength:

	Connection Name	Local IPSEC Identifier	Remote IPSEC Identifier
<input checked="" type="checkbox"/>	laptop	FVM318	jsmith

Figure 3-13. Wireless Settings menu, IPSec selected

- Click the Encryption Strength drop-down list box and select IPSec. The Wireless Settings menu will change to display the list of IPSec connections, as shown in [Figure 3-13](#):

- d. Click Add to display the IPsec client setting menu, as shown below.

Figure 3-14. IPsec Client Settings menu

- e. Enter a descriptive name for this PC in Connection Name. This name is for your convenience only, and is not used in the VPN negotiation.
- f. Enter the user name. An email address is an easy to remember user name.
- g. Enter a Pre-Shared Key value for this connection.
- h. Use the default Aggressive Mode and AES - 256 settings.

2. Install the SafeNet SoftRemote Basic VPN client software.

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

- a. Place the *FVM318 Resource CD* in your CD drive.
If the CD does not autostart, double click on the INDEX.HTM file on the CD.
- b. Install the SafeNet SoftRemote Basic VPN client.
After installation, a SafeNet icon shown below will appear in the taskbar tray of your PC.



Figure 3-15. SafeNet system tray icon with disabled indicator

At this point, the SafeNet icon has a diagonal red bar through it, indicating that the VPN client is currently disabled.

3. Configure the SoftRemote Basic VPN Client.

- a. In the taskbar tray, right-click on the SafeNet icon and select Edit Security Policy in the VPN client task menu, as shown below.



Figure 3-16. SafeNet system tray icon menu

The VPN client Security Policy menu will appear as shown below.

SafeNet Basic Client Configuration

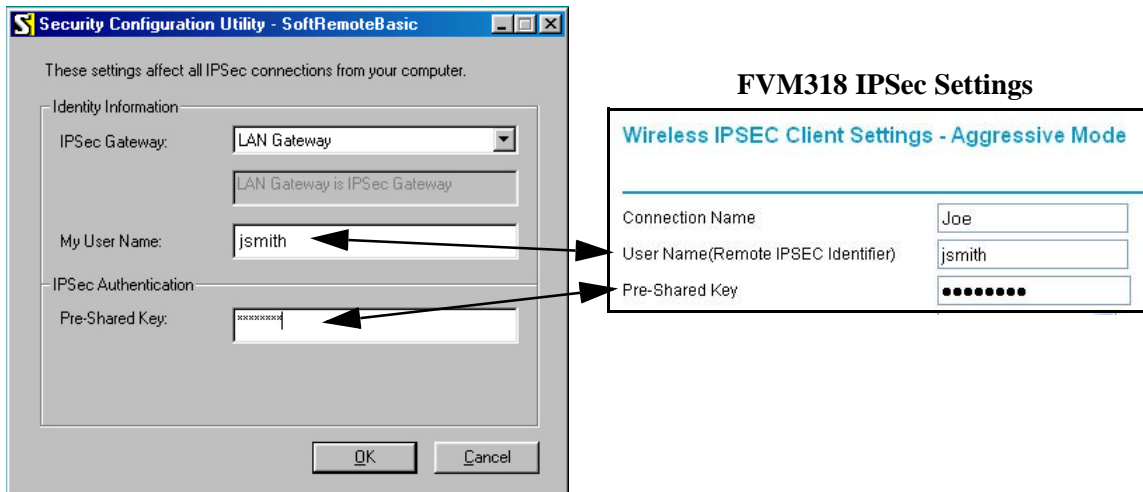


Figure 3-17. SafeNet basic configuration menu

- b. In most cases, you can leave the IPsec Gateway as “LAN Gateway”, which indicates the firewall. If you are not using the firewall as your network’s default gateway, change IPsec Gateway to indicate either the IP Address or the network name of the firewall.
- c. Enter the User Name and the Pre-Shared Key value that you programmed for this PC in the firewall’s IPsec Client Settings menu.
- d. Click OK.
- e. In the taskbar tray, right-click on the SafeNet icon and select Activate Security Policy in the task menu. The SafeNet icon will now appear without the red bar, as shown below.



Figure 3-18. SafeNet system tray icon showing enabled condition

4. Test the SoftRemote Basic VPN Connection.

To check the VPN Connection, you can initiate a request from the PC to the firewall. The simplest method is to ping from the PC to the firewall, as shown below:

- 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.

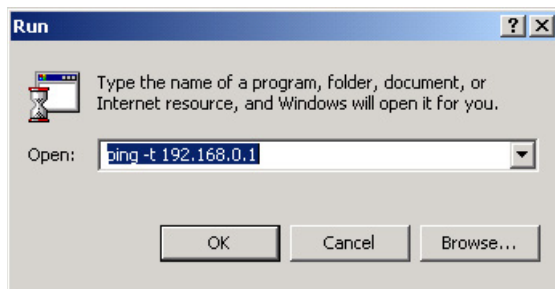


Figure 3-19. Run Ping from Windows Start Menu

This will cause a continuous ping to be sent to the firewall. Within thirty seconds, 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 3-20. Ping results

At this point, the SafeNet tray icon should change to read on as shown below:



Figure 3-21. SafeNet system tray icon showing ON condition

- c. Once the connection is established, you can open the browser of the PC and browse.

To view the firewall's connection log, go to the Router Status menu and click on Wireless VPN Log. The VPN client's log is written to the text file `isakmp.log`, which can be found in the directory in which the client is installed. Typically that directory is:

`C:\PROGRAM FILES\SAFENET\SOFTREMOTEBASIC`

Help is also available by right-clicking on the SafeNet taskbar icon and selecting Help.

Using SoftRemoteLT Instead of SoftRemote Basic

The SafeNet SoftRemote Basic VPN Client that is included with the firewall is only suitable for establishing a local wireless IPSec connection with the FVM318 firewall. If your PC is mobile, you may want to also use it to connect to your firewall over the Internet from a remote location. In that case you will need a full VPN Client. SafeNet's SoftRemoteLT VPN Client (or another version of SafeNet's full client) will serve both purposes.



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

Procedure 3-5: Configuring the SoftRemoteLT Full Client

To configure a policy for a secure local wireless connection to the FVM318 firewall using the SoftRemoteLT client, use the FVM318 configuration from “[Configure Basic IPsec Wireless Connections](#)” on page 3-13 and follow procedure below for configuring the full VPN client.

1. Install the SafeNet SoftRemoteLT Full VPN Client



Note: If you have installed the SoftRemote Basic client, you must uninstall it before installing SoftRemoteLT. During the uninstall process, you can choose to keep your existing security policy, simplifying the configuration of SoftRemoteLT. In SoftRemoteLT, you can configure multiple Security Policies, such as a policy for secure local wireless connection to the FVM318 firewall and a policy for connecting remotely from the Internet.

2. Open the Security Policy Editor.

To launch the SoftRemoteLT client, click on the Windows Start button, then select Programs, then SafeNet, then Security Policy Editor. The Security Policy Editor window will appear.

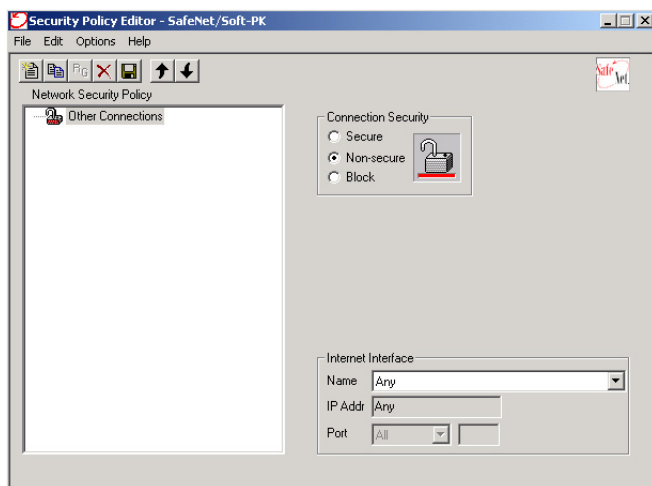


Figure 3-22. SafeNet Security Policy Editor

3. Create a VPN Connection.

You will need to provide: A descriptive name for the connection; and the LAN address of the FVM318 firewall.

- a. From the Edit menu at the top of the Security Policy Editor window, click Add, then Connection. A New Connection listing will appear in the list of policies.

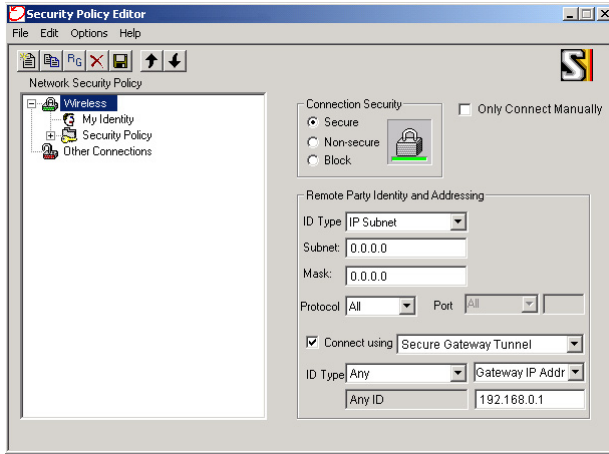


Figure 3-23. SafeNet Security Policy Editor new connection menu

- b. Click and rename the New Connection list item to indicate that this is the policy for your local wireless connection, such as **Wireless**.
- c. Select Secure on the right side of the Security Policy Editor window in the Connection Security box.
- d. Select IP Subnet in the ID Type menu.
- e. Type **0.0.0.0** in the Subnet and Mask fields.
- f. Select All in the Protocol menu to allow all traffic through the VPN tunnel.
- g. Check Connect using Secure Gateway Tunnel.
- h. Select Any in the ID Type menu below the checkbox.
- i. Select Gateway IP Address in the box to the right of ID Type.
- j. Enter the LAN IP Address of the FVM318 firewall in the lower right box (usually 192.168.0.1).

4. Configure the Security Policy.

Note: These settings do not depend on your network configuration information.

- a. In the Network Security Policy list on the left side of the Security Policy Editor window, expand the new connection by double clicking its name or clicking on the “+” symbol.

My Identity and Security Policy subheadings should appear below the connection name.

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

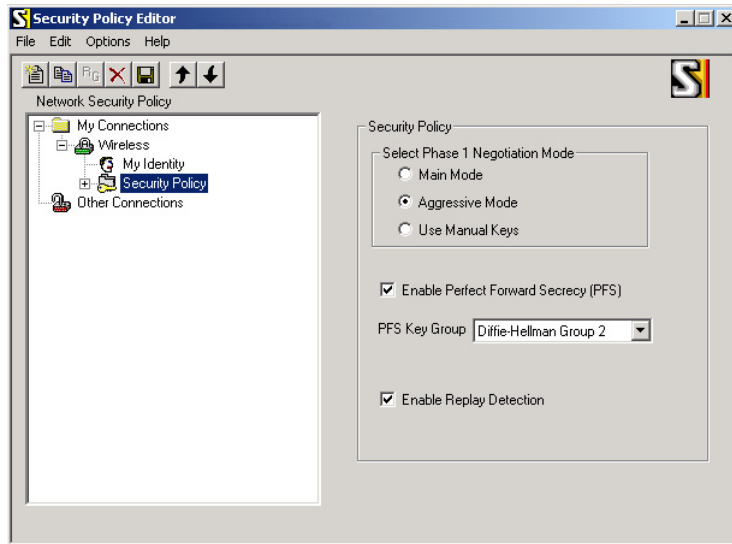


Figure 3-24. SafeNet Security Policy Editor edit security policy menu

- c. Select Aggressive Mode in the Select Phase 1 Negotiation Mode box.
- d. Check the Enable Perfect Forward Secrecy (PFS) checkbox.
- e. Select Diffie-Hellman Group 2 for PFS Key Group.
- f. Check the Enable Replay Detection checkbox.

5. Configure the VPN Client Identity

In this step, you will provide information about your client PC. You will need to provide:

- The User Name that you configured in the FVM318 firewall.
- The Pre-Shared Key that you configured in the FVM318 firewall.

- a. Click on My Identity in the Network Security Policy list on the left side of the Security Policy Editor window.

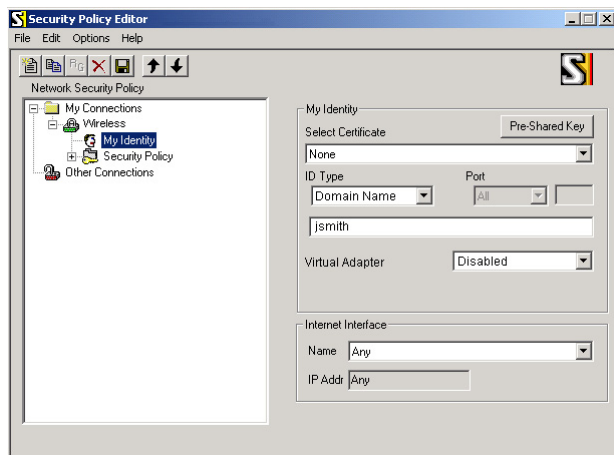


Figure 3-25. SafeNet Security Policy Editor edit identity menu

- b. Choose None in the Select Certificate menu.
- c. Select Domain Name in the ID Type menu.
- d. In the box below ID Type, enter the user name that you configured in the FVM318 firewall.
- e. Select Disabled in the Virtual Adapter box.
- f. In the Internet Interface box, select your wireless adapter or you may choose Any if you will be switching between adapters or if you have only one adapter.
- g. Click the Pre-Shared Key button.
- h. Click the Enter Key button in the Pre-Shared Key dialog box.
- i. Enter the Pre-Shared Key that you configured in the FVM318 firewall and click OK. Note that this field is case sensitive.

6. Configure VPN Client Authentication Proposal

Note: These settings do not depend on your network configuration information.

- a. In the Network Security Policy list on the left side of the Security Policy Editor window, expand the Security Policy heading by double clicking its name or clicking on the “+” symbol.

- b. Expand the Authentication subheading by double clicking its name or clicking on the “+” symbol. Then select Proposal 1 below Authentication.
- c. Select Pre-Shared key in the Authentication Method menu.
- d. Select AES-256 in the Encrypt Alg menu. If your VPN client does not offer this selection, select Triple DES.
- e. Select SHA-1 in the Hash Alg menu.
- f. Select Seconds and enter **21600** in the SA Life menu.
- g. Select Diffie-Hellman Group 2 in the Key Group menu.

7. **Configure VPN Client Key Exchange Proposal.**

Note: These settings do not depend on your network configuration information.

- a. Expand the Key Exchange subheading by double clicking its name or clicking on the “+” symbol.
- b. Select Proposal 1 below Key Exchange.
- c. In the SA Life menu, select Seconds and enter 21600.
- d. Select None in the Compression menu.
- e. Check the Encapsulation Protocol (ESP) checkbox.
- f. Select AES-256 in the Encrypt Alg menu. If your VPN client does not offer this selection, select Triple DES.
- g. Select SHA-1 in the Hash Alg menu.
- h. Select Tunnel in the Encapsulation menu.
- i. Leave the Authentication Protocol (AH) checkbox unchecked.

8. **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, you can test the VPN connection in the manner described in [“SafeNet system tray icon showing enabled condition” on page 3-16](#). You can also use the log and connection monitors described in [“Monitoring the PC VPN Connection Using SafeNet Tools” on page 5-18](#).

Chapter 4

Protecting Your Network

This chapter describes how to use the basic firewall features of the FVM318 Cable/DSL ProSafe Wireless VPN Security Firewall to protect your network.

Protecting Access to Your FVM318 firewall

For security reasons, the firewall has its own user name and password to protect access to its configuration menus. 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 you may use to log in to your Internet connection.

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.

Procedure 4-1: Changing the Administrator 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** and default password of **password**, or using whatever password and LAN address you have chosen for the firewall.

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

New Password

Old Password

New Password

Repeat New Password

Administrator login times out
after idle for minutes.

Figure 4-1: Set Password menu

- To change the password, first enter the old password, and then enter the new password twice.
- 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.

Procedure 4-2: Changing 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.

Configuring Basic Firewall Services

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

Blocking Functions, Keywords, Sites, and Services

The firewall provides a variety of options for blocking Internet based content and communications services. Those basic options include:

With its content filtering feature, the FVM318 firewall prevents objectionable content from reaching your PCs. The FVM318 allows you to control access to Internet with filtering options which include the following:

- Keyword blocking of newsgroup names.
- 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.
- Outbound Services Blocking limits access from your LAN to Internet locations or services that you specify as off-limits.
- Blocks unwanted traffic from the Internet to your LAN.
- Blocks access from your LAN to Internet locations that you specify as off-limits.

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

Procedure 4-3: Blocking Functions, Keywords, and Sites

The FVM318 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 password and LAN address you have chosen for the firewall.
2. Click the Block Sites link of the Security section of the main menu to view the screen below.

The screenshot shows the 'Block Sites' configuration page. At the top, there is a title 'Block Sites'. Below it, a section titled 'Block these functions from Internet Sites:' contains four checkboxes: 'ActiveX', 'Cookies', 'Java', and 'Web Proxy'. The 'Turn Keyword Blocking On' checkbox is checked. Below this is a text input field for a keyword, followed by an 'Add Keyword' button. A section titled 'Block Sites Containing These Keywords Or Domain Names:' contains a list box with no items. Below the list box are 'Delete Keyword' and 'Clear List' buttons. At the bottom, there is a checkbox for 'Allow Trusted IP Address To Visit Blocked Sites' and a 'Trusted IP Address' field with four input boxes containing '192', '168', '0', and '0'. At the very bottom are 'Apply' and 'Cancel' buttons.

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.
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.

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.

Blocking Services

Firewalls are used to regulate specific traffic passing through from one side of the firewall to the other. You can restrict outbound (LAN to WAN) traffic to what outside resources you want local users to be able to access. In addition to the kind of blocking of sites discussed above, you can block services like Telnet or Instant Messenger.

By default, the FVM318 regulates inbound and outbound traffic in these ways:

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

You may define exceptions to the default outbound settings by adding Block Services definitions to the Outbound Services table. In this way, you can block or allow access based on the service or application destination IP addresses, and time of day. You can also choose to log traffic that matches or does not match what you have defined.

Procedure 4-4: Configuring Services Blocking

1. Log in to the firewall at its default LAN address of <http://192.168.0.1> with its default user name of **admin**, default password of **password**, or using whatever password and LAN address you have chosen for the firewall.
2. Click the Block Services link of the Security section of the main menu to display this screen.

The screenshot shows the 'Block Service' configuration page. At the top, there is a title 'Block Service'. Below it is a section titled 'Outbound Services' containing a table with the following columns: #, Enable, Service Name, Action, LAN Users, and Log. Below the table are three buttons: 'Add', 'Edit', and 'Delete'. At the bottom of the page are two buttons: 'Apply' and 'Cancel'.

Figure 4-3: Block Services menu

- To create a new Block Services rule, click the Add button.
 - To edit an existing Block Services rule, select its button on the left side of the table and click Edit.
 - To delete an existing Block Services rule, select its button on the left side of the table and click Delete.
3. Modify the menu below to define or edit how a service is regulated.

The screenshot shows the 'Add Block Service' configuration page. It features several fields and dropdown menus: 'Service Name' (FTP), 'Action' (BLOCK always), 'LAN Users Address' (Any), 'start' (IP address fields), 'finish' (IP address fields), and 'Log' (Never). At the bottom are three buttons: 'Back', 'Apply', and 'Cancel'.

Figure 4-4: Add Block 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. You can block or allow always, or you can choose to block or allow according to the schedule you have defined in the Schedule menu.

- 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 definition.

Setting Times and Scheduling Firewall Services

The FVM318 firewall uses the [Network Time Protocol](#) (NTP) to obtain the current time and date from one of several time servers on the Internet. In order to localize the time for your log entries, you must select your time zone from the list.

Procedure 4-5: Setting 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 password and LAN address you have chosen for the firewall.
2. Click on the Schedule link of the Security menu to display the menu shown below.

Schedule

Use this schedule for rules

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 hour minute

End Blocking hour minute

Time Zone

(GMT-08:00)Pacific Time (US Canada) ▼

Adjust for daylight savings time

Use this NTP Server

Current time: Wed, 2002-05-01 15:32:06

Figure 4-5: 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.

Procedure 4-6: Scheduling 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 password and LAN address you have chosen for the firewall.
2. Click on the Schedule link of the Security 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.

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

Virtual Private Networking

This chapter describes how to use the VPN features of the FVM318 firewall. VPN tunnels provide secure, encrypted communications between your local wireless and Ethernet network, and remote networks or computers.

FVM318 VPN Overview

Two common scenarios for configuring VPN tunnels are between two or more networks, and between a remote computer and a network. The FVM318 adds the option of VPN tunnels over wireless links to the FVM318.

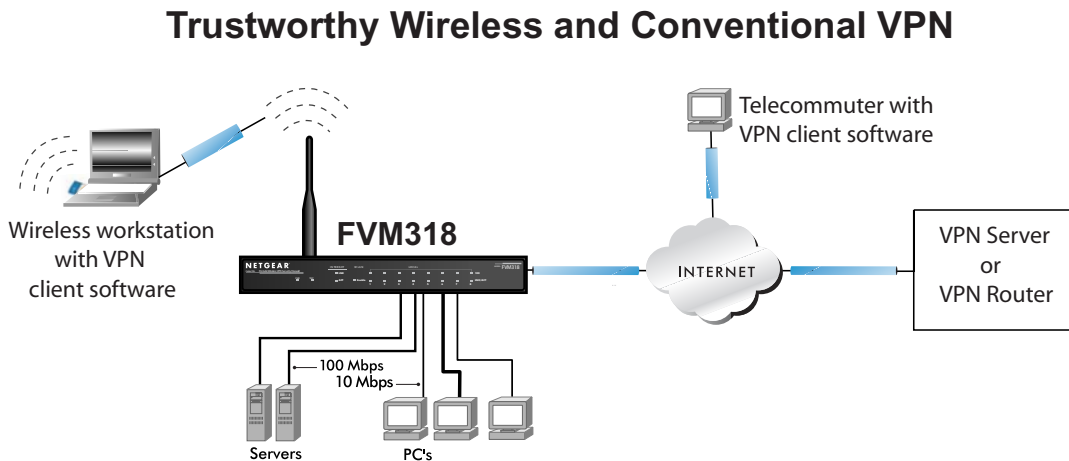


Figure 5-1: Secure access through VPN tunnels

The FVM318 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.

In this configuration, based on the remote LAN IP and subnet mask addresses specified in the VPN settings of the remote system, some or all of the network resources connected to the FVM318 are visible to the users connected via the tunnel from the remote network.

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

VPN client access allows a remote workstation to connect to your network from any location on the Internet. In this case, the remote workstation is one tunnel endpoint, running VPN client software. The FVM318 firewall router on your network is the other tunnel endpoint. In this configuration, all of the network resources connected to the FVM318 are visible to the user connected via the tunnel from the remote PC.

- Secure wireless access from local workstations over 802.11b wireless links using IPSec VPN tunnels.

Wireless VPN client access allows a local wireless workstation to securely connect to your network. In this case, the local wireless workstation is one tunnel endpoint, running VPN client software. The FVM318 firewall router on your network is the other tunnel endpoint. In this configuration, all of the network resources connected to the FVM318 are visible to the user connected via the tunnel from the local wireless workstation.

- 70 external VPN connections and 32 local wireless VPN connections. The FVM318 firewall supports up to 70 WAN plus 32 wireless LAN (WLAN) concurrent tunnels.

These scenarios are described below.



Note: The FVM318 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 FVS318, FVL328, and FVM318 firewalls, and between an these firewalls and the SafeNet SoftRemote VPN Client for Windows. Although the FVM318 can interoperate with many other VPN products, it is not possible for NETGEAR to provide specific technical support for every other interconnection. Please see <http://www.netgear.com/docs> for additional VPN configuration information.

FVM318 VPN Configuration Planning

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 5-22](#).

To set up a VPN connection, you must configure each endpoint with specific identification and connection information describing the other endpoint. 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 remote end be a network or a single PC?
- At least one side must have a fixed IP address. 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? IKE is an automated method for establishing an SA.
- For the WAN connection, what level of IPSec VPN encryption will you use, 56 bit DES, 168 bit 3DES, AES (128, 192, or 256)? Longer keys are more secure but the throughput will be slower if the other endpoint encrypts via software rather than the hardware-based encryption in the FVM318 firewall.
 - 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. 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.
- For the wireless LAN connection, what level of IPSec VPN encryption will you use, 56 bit DES, 168 bit 3DES, AES (128, 192, or 256)? Longer keys are more secure but the throughput will be slower if the other endpoint encrypts via software rather than the hardware-based encryption in the FVM318 firewall. For instructions on configuring wireless VPN connections, please see [“Configuring IPSec Wireless Connections”](#) on [page 3-12](#).

Procedure 5-1: Configuring a Network to Network VPN Tunnel

Follow this procedure to configure a VPN tunnel between two LANs via a FVM318 at each end.

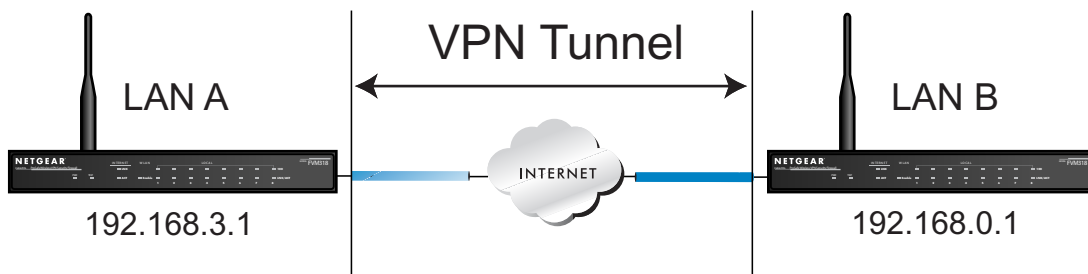


Figure 5-2: LAN to LAN VPN access from an FVM318 to an FVM318

The sample configuration worksheet below is filled in with the parameters used in this procedure. A blank worksheet is provided on [page 5-22](#).

Network to Network VPN Tunnel Configuration Worksheet

IKE Tunnel Security Association Settings			
Connection Name:			VPNAB
Local IPSec Identifier	LAN A:		LAN_A
	LAN B		LAN_B
PreShared Key:			r>T(h4&3@#kB
Secure Association -- Main Mode or Aggressive Mode:			Main
Perfect Forward Secrecy:			Enabled
WAN Encryption Protocol:			DES
DES, 3DES, or AES -128, -192, or -256			
Wireless Encryption Protocol:			N/A
-- IPSec (DES, 3DES, or AES -128, -192, or -256)			
-- WEP (64-bit or 128-bit)			
Key Life in seconds:			3600 (1 hour)
IKE Life Time in seconds:			28800 (8 hours)
FVM318 Network IP Settings			
Network	LAN IP Network Address	Subnet Mask	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

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

This procedure uses the settings in the configuration worksheet above. To configure your network, print and fill out the blank “[Network to Network IKE VPN Tunnel Configuration Worksheet](#)” on page 5-22 for your network configuration. Then follow the procedures below.

- a. Log in to the FVM318 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.

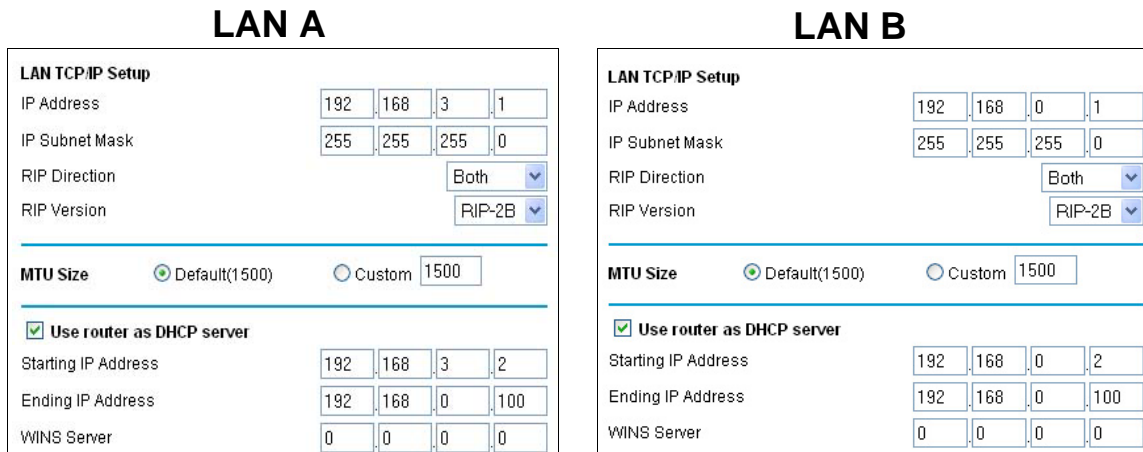


Figure 5-3: Configuring the Local LAN (A) via the LAN IP Setup Menu

- b. For this example, configure the FVM318 settings on LANs A and B as follows:

Network Configuration Settings

FVM318 Network IP Settings				
Network	LAN IP	Network Address	Subnet Mask	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 PCs on network A.

2. Configure the VPN settings on each FVM318.

- a. From Setup section of the main menu of the FVM318, click the VPN Settings link. Click Add. The VPN Settings - Main Mode window opens as shown below:

Figure 5-4: VPN Settings - Main Mode IKE Edit menu

- b. Fill in the Connection Name VPN settings as illustrated.
 - The Connection Names of LANs A and B can be the same: **VPNAB**
 - Local IPSec Identifier name in the FVM318 on LAN A: **LAN_A**
Note: This IPSec name must not be used in any other SA in this VPN network.
 - Local IPSec Identifier in the FVM318 on LAN B: **LAN_B**
 - Remote IPSec Identifier in the FVM318 on LAN A: **LAN_B**
 - Remote IPSec Identifier in the FVM318 on LAN B: **LAN_A**
 - Remote LAN IP Address in the FVM318 on LAN A: **192.168.0.1**
and Remote Subnet Mask in the FVM318 on LAN A: **255.255.255.0**
This is the LAN IP Address for the FVM318 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 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 FVM318 on LAN B: **192.168.3.1**
and Remote Subnet Mask in the FVM318 on LAN B: **255.255.255.0**
This is the LAN IP Address for the FVM318 on LAN A.
- Remote WAN IP Address in the FVM318 on LAN A: **10.0.0.1**
This is the WAN IP Address for the FVM318 on LAN B.

You can look up the WAN IP Address of the FVM318 on LAN B by viewing the its WAN Status screen. When the FVM318 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 FVM318 on LAN A as the WAN IP Address for the FVM318 on LAN B.

Note: Only one side may have a dynamic IP address, and that side must always initiate the connection.

- Remote WAN IP Address in the FVM318 on LAN B: **24.0.0.1**
This is the WAN IP Address for the FVM318 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 FVM318:
- Enable Perfect Forward Secrecy.
 - For Encryption Protocol, select: DES.
 - Enter the PreShared Key. In this example, enter **r>T(h4&3@#kB** as the PreShared Key. With IKE, a preshared key that you make up is used for mutual identification. The PreShared 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 FVM318 has a dynamically assigned WAN IP address, you must initiate the request from that FVM318's network. The simplest method is to ping the LAN IP address of the other FVM318.

- a. Using our example, from a PC attached to the FVM318 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.

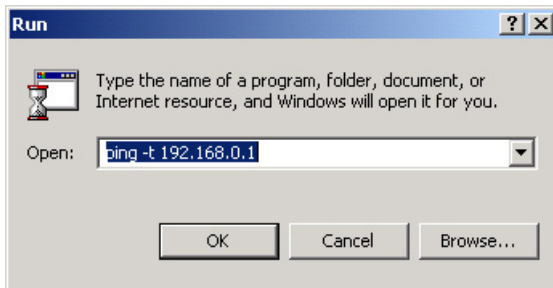


Figure 5-5: Running a Ping test from Windows

- c. This will cause a continuous ping to be sent to the first FVM318. 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 5-6: 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.

Procedure 5-2: Configuring 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 FVM318 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, Version 5 or later. The SafeNet VPN Client can be purchased from SafeNet at <http://www.safenet-inc.com>.

Note: If your situation is different, for example, if you wish to use different VPN client software, please see <http://www.netgear.com/docs> for additional VPN configuration information.

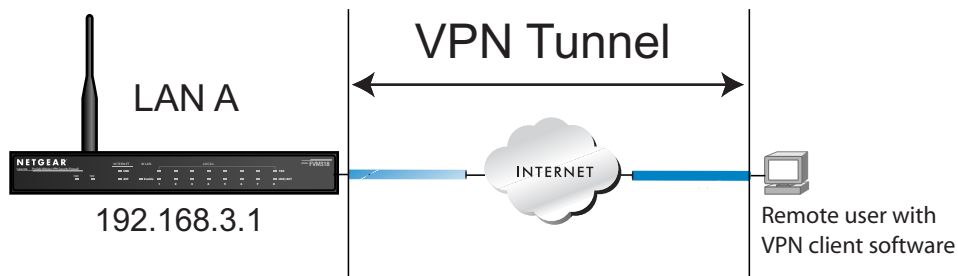


Figure 5-7: PC to LAN VPN access from a PC to an FVM318

The sample configuration worksheet below is filled in with the parameters used in the procedure below. A blank worksheet is on [page 5-23](#).

PC to Network VPN Tunnel Configuration Worksheet

IKE Tunnel Security Association Settings				
Connection Name:	VPNLANPC			
PreShared Key:	r>T(h4&3@#kB			
Secure Association -- Main Mode or Aggressive Mode:	Main			
Perfect Forward Secrecy:	Enabled			
WAN Encryption Protocol	DES			
-- Null				
-- IPSec (DES, 3DES, or AES 128, 192, or 256)				
Wireless Encryption Protocol	N/A			
-- Disable				
-- IPSec (DES, 3DES, or AES 128, 192, or 256)				
-- WEP (64-bit or 128-bit)				
Key Life in seconds:	3600 (1 hour)			
IKE Life Time in seconds:	28800 (8 hours)			
FVM318 and PC IP Settings				
	Local IPSec Identifier	LAN IP Address	Subnet Mask	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 FVM318 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:

Local IPSec Identifier:

Remote IPSec Identifier:

Remote LAN IP Address:

Remote LAN Subnet Mask:

Remote WAN IP Address:

Secure Association:

Perfect Forward Secrecy: Enabled Disabled

Encryption Protocol:

PreShared Key:

Key Life: Seconds

IKE Life Time: Seconds

NETBIOS Enable

Figure 5-8: 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 5-14.](#)
 - 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.

Note: Only one side can have a dynamic IP address, and 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 PreShared 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. Install and Configure the SafeNet VPN Client Software on the PC.



Note: Before installing the SafeNet SoftRemote Basic 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

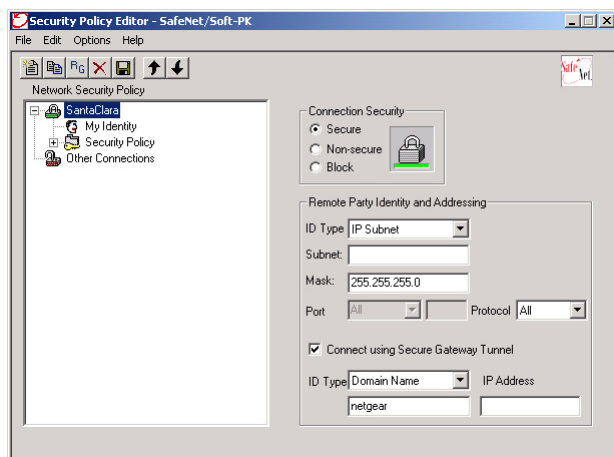


Figure 5-9: Security Policy Editor New Connection

b. Add a new connection

- Run the SafeNet Security Policy Editor program and, using the [“PC to Network VPN Tunnel Configuration Worksheet”](#) on page 5-9, 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 FVM318 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 FVM318. The network address is the LAN IP Address of the FVM318 with 0 as the last number.
- Enter **255.255.255.0** in the Mask field as the LAN Subnet Mask of the FVM318
- 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 FVM318 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.

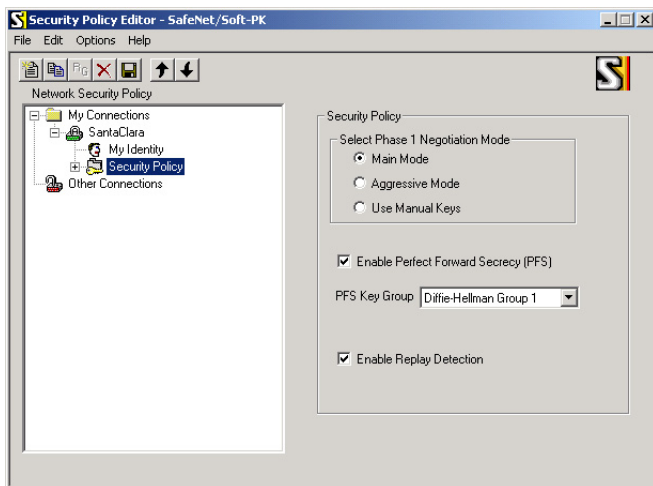


Figure 5-10: Security Policy Editor Security Policy

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

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

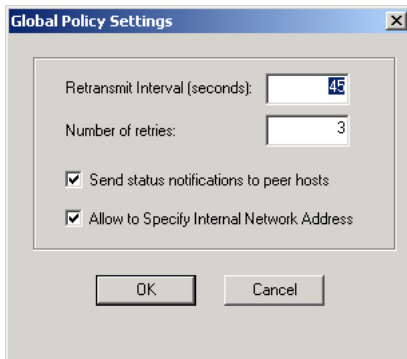


Figure 5-11: Security Policy Editor Global Policy Options

- 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 PreShared Key that you configured in the FVM318.
- 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.

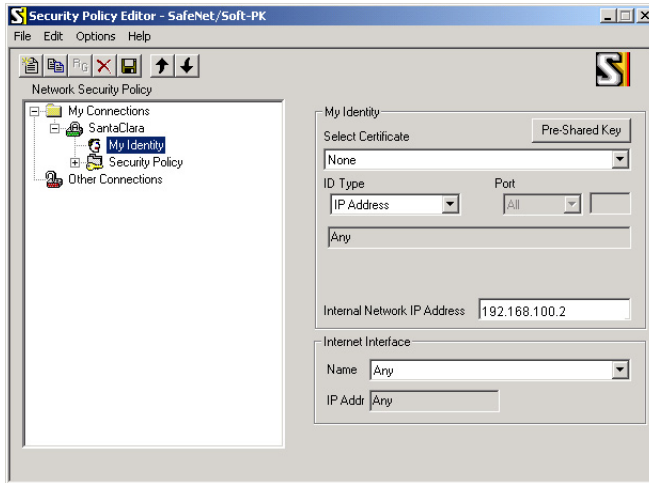


Figure 5-12: Security Policy Editor My Identity

- 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 FVM318's Pre-Shared Key and click OK. In this example, **r>T(h4&3@#kB** would be 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 FVM318 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 FVM318 in [“Configuring a Remote PC to Network VPN” on page 5-8](#). 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 FVM318 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 FVM318 in [“Configuring a Remote PC to Network VPN” on page 5-8](#). 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 FVM318's network. Since the remote PC has a dynamically assigned WAN IP address, it must initiate the request. The simplest method is to ping from the remote PC to the LAN IP address of the FVM318. Using our example, start from the remote PC:

- a. Establish an Internet connection from the PC.
- b. On the Windows taskbar, click the Start button, and then click Run.
- c. Type `ping -t 192.168.3.1` , and then click OK.

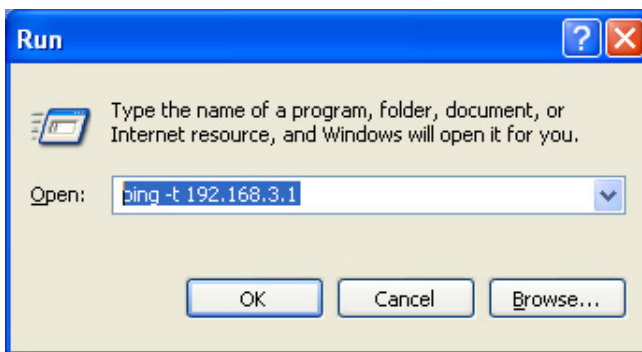


Figure 5-13: Running a Ping test to the LAN from the PC

This will cause a continuous ping to be sent to the first FVM318. 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 5-14: 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 FVM318. 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:

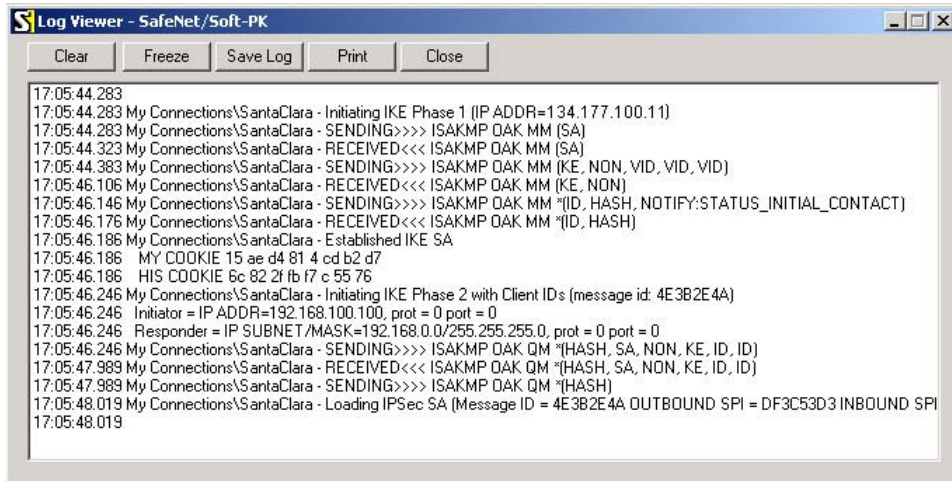


Figure 5-15: Log Viewer screen

The Connection Monitor screen for this connection is shown below:

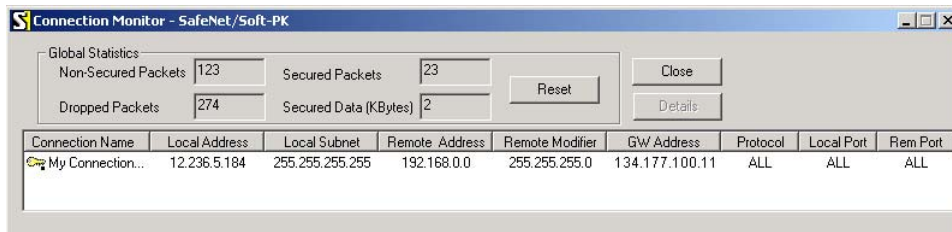


Figure 5-16: Connection Monitor screen

In this example you can see the following:

- The FVM318 has a public IP WAN address of 134.177.100.11
- The FVM318 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.

Procedure 5-3: Deleting a Security Association

To delete a security association:

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

Manual Keying

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.

Procedure 5-4: Using Manual Keying as an Alternative to IKE

1. When editing the VPN Settings, you may select manual keying. At that time, the edit menu changes to look like the screen below:

VPN Settings - Manual Keys

Connection Name

Local IPSec Identifier

Remote IPSec Identifier

Remote LAN IP Address

Remote LAN Subnet Mask

Remote WAN IP Address

Secure Association

Incoming SPI

Outgoing SPI

Encryption Protocol

Encryption Key

Authentication Protocol

Authentication Key

NETBIOS Enable

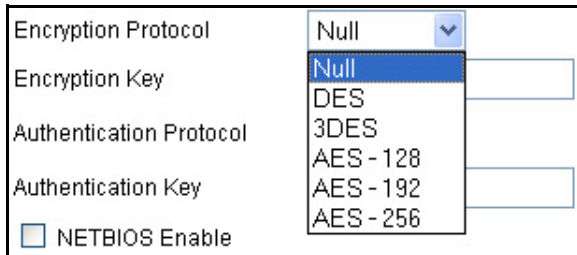
Figure 5-17: VPN Edit menu for Manual Keying

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:



The screenshot shows a configuration window with the following fields and options:

- Encryption Protocol: A dropdown menu with 'Null' selected and a list of options: Null, DES, 3DES, AES - 128, AES - 192, and AES - 256.
- Encryption Key: An empty text input field.
- Authentication Protocol: A dropdown menu (not visible in the screenshot).
- Authentication Key: An empty text input field.
- NETBIOS Enable: A checkbox that is currently unchecked.

Figure 5-18: VPN encryption options

- a. Null - Fastest, but no security.
- b. 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.
- c. 3DES - (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.
- d. 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. 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.
- e. Enter a hexadecimal Encryption Key
 - For DES, enter 16 hexadecimal [0-9,A-F] characters.
 - For 3DES, enter 48 hexadecimal [0-9,A-F] characters.

The encryption key must match exactly the key used by the remote router or host.

5. Select the Authentication Protocol
 - MD5 (default) - 128 bits, faster but less secure.
 - SHA-1 - 160 bits, slower but more secure.
6. Enter 32 hexadecimal characters for the Authentication Key. The authentication key must match exactly the key used by the remote router or host.
7. Click the NETBIOS Enable check box to allow NETBIOS over the VPN tunnel.
8. Click Apply to enter the SA into the table.

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 5-1: Network to Network IKE VPN Tunnel Configuration Worksheet

IKE Tunnel Security Association Settings				
Connection Name:				
PreShared Key:				
Secure Association -- Main Mode or Aggressive Mode:				
Perfect Forward Secrecy:				
WAN Encryption Protocol				
-- Null				
-- IPSec (DES, 3DES, or AES 128, 192, or 256)				
Wireless Encryption Protocol				
-- Disable				
-- IPSec (DES, 3DES, or AES 128, 192, or 256)				
-- WEP (64-bit or 128-bit)				
Key Life in seconds:				
IKE Life Time in seconds:				
FVM318 Network IP Settings				
Network	Local IPSec Identifier	LAN IP Network Address	Subnet Mask	Gateway IP (WAN IP Address)

Table 5-2: PC to Network IKE VPN Tunnel Settings Configuration Worksheet

IKE Tunnel Security Association Settings				
Connection Name:				
PreShared Key:				
Secure Association -- Main Mode or Aggressive Mode:				
Perfect Forward Secrecy:				
WAN Encryption Protocol				
-- Null				
-- IPSec (DES, 3DES, or AES 128, 192, or 256)				
Wireless Encryption Protocol				
-- Disable				
-- IPSec (DES, 3DES, or AES 128, 192, or 256)				
-- WEP (64-bit or 128-bit)				
Key Life in seconds:				
IKE Life Time in seconds:				
FVM318 and PC IP Settings				
	Local IPSec Identifier	LAN IP Network Address	Subnet Mask	Gateway IP (WAN IP Address)
Network:				
PC:				

Chapter 6

Managing Your Network

This chapter describes how to perform network management tasks with your FVM318 Cable/DSL ProSafe Wireless VPN Security Firewall.

Network Management Information

The FVM318 firewall provides a variety of status and usage information which is discussed below.

Viewing Router Status and Usage Statistics

From the main menu Maintenance section, select Router Status to view the screen below.

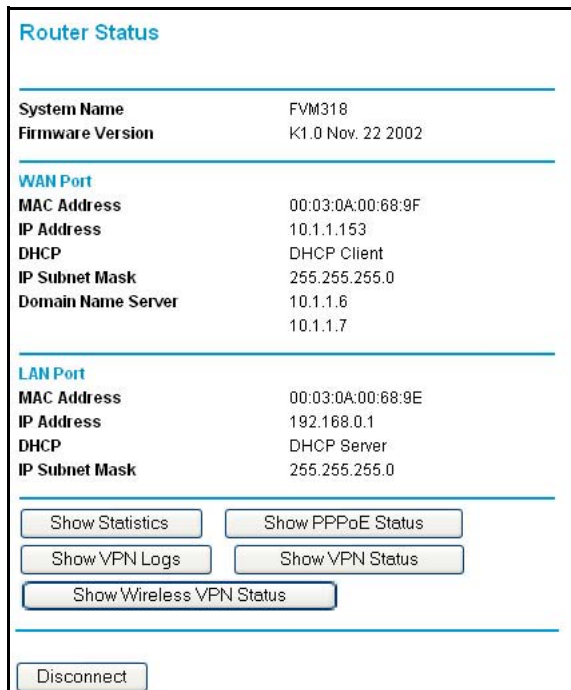


Figure 6-1: Router Status screen

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 6-1](#). This screen shows the following parameters:

Table 6-1. 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 Server	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 (LAN) 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 LAN port of the firewall. The default is 192.168.0.1
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.
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

Click on the “Show Statistics” button to display firewall usage statistics, as shown in [Figure 6-2](#) 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: (secs)

Figure 6-2. Router Statistics screen

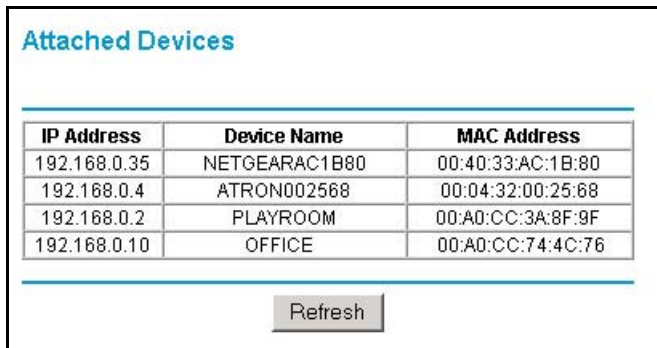
This screen shows the following statistics:.

Table 6-2. 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	The average line utilization —average CLU for this port.
Up Time	The time elapsed since this port acquired link.
System up Time	The time elapsed since the last power cycle or reset.
Set Interval	Specifies the intervals at which the statistics are updated in this window. Click on Stop to freeze the display.
Stop	Stops the polling update of the statistics.

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 6-3](#)



The screenshot shows a web interface titled "Attached Devices". It contains a table with three columns: "IP Address", "Device Name", and "MAC Address". The table lists four devices. Below the table is a "Refresh" button.

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 6-3: 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.



Note: This information is for your convenience only, and may not be complete. Some devices may not appear.

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

Figure 6-4: Security Logs menu

Log entries are described in [Table 6-5](#)

Table 6-5: 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 6-6](#)

Table 6-6: 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 Include in the 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

Enabling SYSLOG

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:

The screenshot shows a configuration window titled "E-mail". It contains several sections:

- A checked checkbox labeled "Turn e-mail notification on".
- A section titled "Send alert and logs by e-mail" with two text input fields: "Outgoing Mail Server" containing "mail.netgear.com" and "E-mail Address" containing "jsmith@netgear.com".
- A section titled "Send E-Mail alerts immediately" with three checked checkboxes:
 - "If a DoS attack is detected."
 - "If a Port Scan is detected."
 - "If someone attempts to access a blocked site."
- A section titled "Send logs according to this schedule" with three dropdown menus: "Daily", "Sunday", and "7:00". Below these are radio buttons for "a.m." (selected) and "p.m.".
- At the bottom are "Apply" and "Cancel" buttons.

Figure 6-7: 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 FVM318 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.



Note: Security information such as passwords and encryption keys are stored in this configuration file. Please store this file in a secure place.

Procedure 6-1: Backup 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 password and LAN address you have chosen for the firewall.

- From the Maintenance heading of the main menu, select Backup to view the menu seen below.

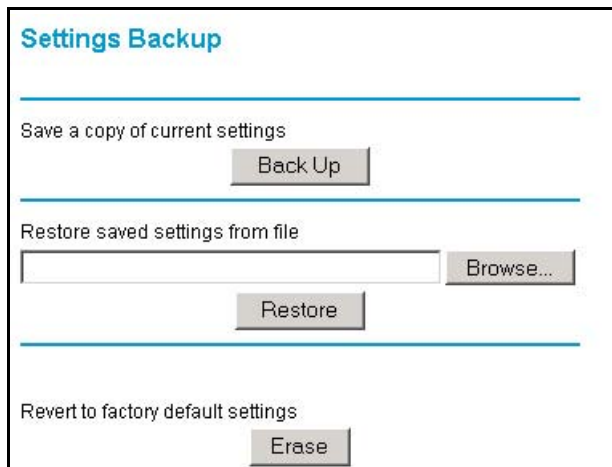


Figure 6-8: Settings Backup menu

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

Procedure 6-2: Restore a Configuration from a File

- Log in to the firewall at its default LAN address of <http://192.168.0.1> with its default user name of **admin**, default password of **password**, or using whatever password and LAN address you have chosen for the firewall.
- From the Maintenance heading of the main menu, select the Settings Backup menu as seen in [Figure 6-8](#).
- Enter the full path to the file on your network or click the Browse button to browse to the file.
- When you have located the `.cfg` file, click the Restore button to upload the file to the firewall.
- The firewall will then reboot automatically.

Procedure 6-3: 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 administrator user name will be **admin**, the password will be **password**, the LAN IP address will be 192.168.0.1, and the router's DHCP client will be enabled.

To restore the factory default configuration settings without knowing the login password or IP address, you must use the reset button on the rear panel of the firewall. See [“Using the Default Reset button” on page 8-8](#).

Running Diagnostic Utilities and Rebooting the Router

The FVM318 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 6-9](#).

Diagnostics

Ping an IP address

Perform a DNS Lookup

Internet Name

Display the Routing table

Trace the routing path

To this IP address

Reboot the router

Figure 6-9: Diagnostics menu

Enabling 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.

Procedure 6-4: Configure Remote Management

1. Log in to the firewall at its default LAN address of <http://192.168.0.1> with its default user name of **admin**, default password of **password**, or using whatever password and LAN address you have chosen for the firewall.
2. Select the Allow Remote Management check box.

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

For security, NETGEAR recommends that you restrict access to as few external IP addresses as practical.

- a. To allow access from any IP address on the Internet, select Everyone.
 - b. To allow access from a range of IP addresses on the Internet, select IP address range. Enter a beginning and ending IP address to define the allowed range.
 - c. To allow access from a single IP address on the Internet, select Only this PC. Enter the IP address that will be allowed access.
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, which is a common alternate for HTTP.

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
```

Upgrading the Router's Firmware

The software of the FVM318 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.

Note: 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.

Procedure 6-5: Router Upgrade

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 password and LAN address you have chosen for the firewall.
3. From the main menu of the browser interface, under the Maintenance heading, click Router Upgrade to display the menu shown below.

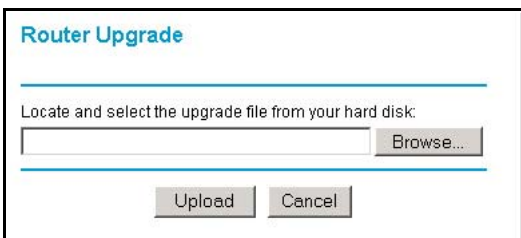



Figure 6-10: Router Upgrade menu

4. In the Router Upgrade menu, click the Browse button to locate the binary (.BIN or .IMG) upgrade file.
5. Click Upload to load the firmware into the firewall.

	<p>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.</p>
---	--

Chapter 7

Advanced Configuration

This chapter describes how to configure the advanced features of your FVM318 Cable/DSL ProSafe Wireless VPN Security Firewall.

Configuring Advanced Security

The FVM318 Cable/DSL ProSafe Wireless VPN Security Firewall provides a variety of advanced features, such as:

- Setting up a Demilitarized Zone (DMZ) Server
- 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 you need to assure secure network services, do not use the Default DMZ Server feature. When a computer is designated as the Default DMZ Server, it loses much of the protection of the firewall, and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

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.

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.

Configuring LAN IP Settings

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

LAN TCP/IP Setup

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.

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is disabled. If disabled, the router will not allow any device to automatically control the resources, such as port forwarding (mapping), of the router.

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.

MTU Size

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

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 Server*, 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.

Procedure 7-1: Using 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.

Note: If the PC is already present on your network, you can copy its MAC address from the Attached Devices menu and paste it here.

4. Click Apply to enter the reserved address into the table.

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

To edit or delete a reserved address entry:

1. Click the radio button next to the reserved address to select the entry you want to edit or delete.
2. Click Edit or Delete.

Procedure 7-2: Configuring 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 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 below.

The screenshot shows the 'LAN IP Setup' configuration page. At the top, there is a checkbox for 'Enable UPnP' which is unchecked. Below this is the 'LAN TCP/IP Setup' section, which includes fields for 'IP Address' (192, 168, 0, 1), 'IP Subnet Mask' (255, 255, 255, 0), 'RIP Direction' (Both), and 'RIP Version' (RIP-2B). The 'MTU Size' section has two radio buttons: 'Default(1500)' (selected) and 'Custom' (1500). The 'DHCP' section has a checked checkbox for 'Use router as DHCP server', followed by fields for 'Starting IP Address' (192, 168, 0, 2), 'Ending IP Address' (192, 168, 0, 100), and 'WINS Server' (0, 0, 0, 0). At the bottom, there is a table for 'Reserved IP Addresses' with columns for '#', 'IP Address', 'MAC Address', and 'Device Name'. Below the table are buttons for 'Add', 'Edit', and 'Delete'. At the very bottom of the form are 'Apply' and 'Cancel' buttons.

Figure 7-1: LAN IP Setup Menu

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

Configuring Dynamic DNS

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial dynamic DNS service, 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.

Procedure 7-3: Configuring Dynamic DNS

1. Log in to the firewall at its default LAN address of <http://192.168.0.1> with its default user name of **admin**, default password of **password**, or using whatever password and LAN address you have chosen for the firewall.
2. From the main menu of the browser interface, under Advanced, click on Dynamic DNS.
3. Access the website of one of the dynamic DNS service providers whose names appear in the ‘Select Service Provider’ box, and register for an account. For example, for dyndns.org, go to www.dyndns.org.
4. Select the “Use a dynamic DNS service” check box.
5. Select the name of your dynamic DNS Service Provider.
6. Type the Host Name that your dynamic DNS service provider gave you. The dynamic DNS service provider may call this the domain name. If your URL is myName.dyndns.org, then your Host Name is “myName.”
7. Type the user name for your dynamic DNS account.
8. Type the password (or key) for your dynamic DNS account.
9. If your dynamic DNS provider allows the use of wildcards in resolving your URL, you may select the Use wildcards check box to activate this feature. For example, the wildcard feature will cause *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org
10. Click Apply to save your configuration.



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

Using 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.

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 7-3](#).

In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Gateway IP Address fields specifies that all traffic for these addresses should be forwarded to the ISDN router at 192.168.0.100.

- A Metric value of 1 will work since the ISDN router is on the LAN. This represents the number of routers between your network and the destination. This is a direct connection so it is set to 1.
- Private is selected only as a precautionary security measure in case RIP is activated.

Procedure 7-4: Configuring 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 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 table, shown below.

#	Name	Destination	Gateway	Metric	Active	Private

Figure 7-2: Static Routes Table

3. To add or edit a Static Route, follow these steps:
 - a. Click the Edit button to open the Edit Menu, shown in [Figure 7-3](#).

Static Routes

Route Name:

Active Private

Destination IP Address: . . .

IP Subnet Mask: . . .

Gateway IP Address: . . .

Metric:

Figure 7-3: 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. Click the Active check box to make this route effective.
 - d. Click the Private check box 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 8

Troubleshooting

This chapter gives information about troubleshooting your FVM318 Cable/DSL ProSafe Wireless VPN Security 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 ["Using the Default Reset button" on page 8-8](#).

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-17](#) 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 [“Using the Default Reset button” on page 8-8](#).
- 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 [“Manually Configuring Your Internet Connection”](#) on page 2-12.

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-11. 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-11.

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.

Procedure 8-5: 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.

Procedure 8-6: 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 [“Manually Configuring Your Internet Connection” on page 2-12](#).

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 6-9](#)).

- 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.

Procedure 8-7: Using the Default Reset button

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. Press and hold the Default Reset button until the Test LED turns on (about 10 seconds).
2. Release the Default Reset button and wait for the firewall to reboot.



Note: If this method does not work, hold the reset button for up to 60 seconds, until the Test LED begins blinking rapidly, then release it and allow the router 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 FVM318 firewall uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

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

Appendix A

Technical Specifications

This appendix provides technical specifications for the FVM318 Cable/DSL ProSafe Wireless VPN Security Firewall.

Network Protocol and Standards Compatibility

Data and Routing Protocols: TCP/IP, RIP-1, RIP-2, DHCP, PPTP, Telstra BigPond, 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, RJ-45

Wireless

Radio Data Rate 1, 2, 5.5, 11Mbps Auto Rate Sensing
 Frequency 2.4-2.5Ghz
 Data Encoding: Direct Sequence Spread Spectrum (DSSS)

802.11b Operating Range		<u>Outdoor environment</u>	<u>Indoor environment</u>
	@ 11 Mbps	398 ft (120 m)	198 ft (60 m)
	@ 5.5 Mbps	561 ft (170 m)	264 ft (80 m)
	@ 2 Mbps	890 ft (270 m)	430 ft (130 m)
	@ 1 Mbps	1485 ft (450 m)	660 ft (200 m)

Maximum Computers Per
 Wireless Network: Limited by the amount of wireless network traffic generated
 by each node. Typically 30-70 nodes.

802.11b Operating Frequency 2.412 ~ 2.462 GHz (US) 2.457 ~ 2.462 GHz (Spain)
 Ranges 2.412 ~ 2.484 GHz (Japan) 2.457 ~ 2.472 GHz (France)
 2.412 ~ 2.472 GHz (Europe ETSI)

802.11b Encryption 40-bits (also called 64-bits), 128-bits WEP data encryption

Appendix B

Network, Routing, Firewall, and Wireless Basics

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

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 FVM318 Cable/DSL ProSafe Wireless VPN Security 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 FVM318 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.

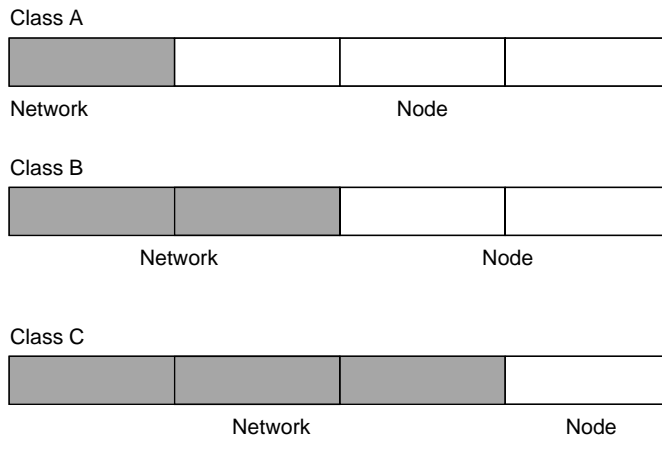


Figure 8-1: Three Main Address Classes

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 8-2: 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 192.68.135.126, 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 8-1. 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 masklength formats.

Table 8-2. Netmask Formats

Dotted-Decimal	Masklength
255.0.0.0	/8
255.255.0.0	/16

Table 8-2. Netmask Formats

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
255.255.255.254	/31
255.255.255.255	/32

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

Choose your private network number from this range. The DHCP server of the FVM318 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 \(IETF\)](http://www.ietf.org) 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 FVM318 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.

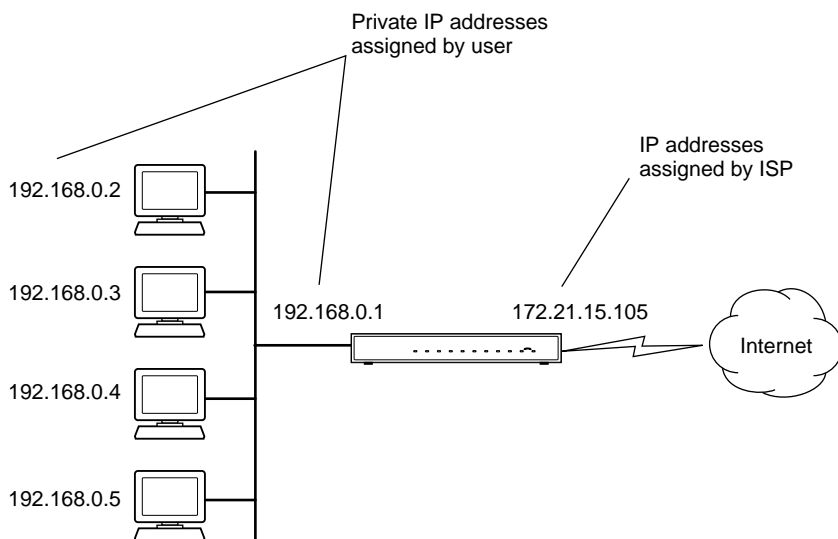


Figure 8-3: Single IP Address Operation Using NAT

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 FVM318 firewall has the capacity to act as a DHCP server.

The FVM318 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 process, the network behind the 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.

Wireless Networking

The FVM318 firewall conforms to the Institute of Electrical and Electronics Engineers (IEEE) 802.11b standard for wireless LANs (WLANs). On an 802.11b wireless link, data is encoded using direct-sequence spread-spectrum (DSSS) technology and is transmitted in the unlicensed radio spectrum at 2.5GHz. The maximum data rate for the wireless link is 11 Mbps, but it will automatically back down from 11 Mbps to 5.5, 2, and 1 Mbps when the radio signal is weak or when interference is detected.

The 802.11b standard is also called Wireless Ethernet or Wi-Fi by the Wireless Ethernet Compatibility Alliance (WECA, see <http://www.wi-fi.net>), an industry standard group promoting interoperability among 802.11b devices.

Wireless Network Configuration

The 802.11b standard offers two methods for configuring a wireless network - ad hoc and infrastructure.

Ad Hoc Mode (Peer-to-Peer Workgroup)

In an ad hoc network, computers are brought together as needed; thus, there is no structure or fixed points to the network - each node can generally communicate with any other node. There is no Access Point involved in this configuration. This mode enables you to quickly set up a small wireless workgroup and allows workgroup members to exchange data or share printers as supported by Microsoft networking in the various Windows operating systems. Some vendors also refer to ad hoc networking as peer-to-peer group networking.

In this configuration, network packets are directly sent and received by the intended transmitting and receiving stations. As long as the stations are within range of one another, this is the easiest and least expensive way to set up a wireless network.

Infrastructure Mode

With a wireless Access Point, you can operate the wireless LAN in the infrastructure mode. This mode provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage, interacting with wireless nodes via an antenna.

In the infrastructure mode, the wireless access point converts airwave data into wired Ethernet data, acting as a bridge between the wired LAN and wireless clients. Connecting multiple Access Points via a wired Ethernet backbone can further extend the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one Access Point domain to another and still maintain seamless network connection.

Extended Service Set Identification (ESSID)

The Extended Service Set Identification (ESSID) is one of two types of Service Set Identification (SSID). In an ad hoc wireless network with no access points, the Basic Service Set Identification (BSSID) is used. In an infrastructure wireless network that includes an access point, the ESSID is used, but may still be referred to as SSID.

An SSID is a thirty-two character (maximum) alphanumeric key identifying the name of the wireless local area network. Some vendors refer to the SSID as network name. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.

Authentication and WEP Encryption

The absence of a physical connection between nodes makes the wireless links vulnerable to eavesdropping and information theft. To provide a certain level of security, the IEEE 802.11 standard has defined two types of authentication methods, Open System and Shared Key. With Open System authentication, a wireless PC can join any network and receive any messages that are not encrypted. With Shared Key authentication, only those PCs that possess the correct authentication key can join the network. By default, IEEE 802.11 wireless devices operate in an Open System network.

Wired Equivalent Privacy (WEP) data encryption is used when the wireless devices are configured to operate in Shared Key authentication mode. There are two shared key methods implemented in most commercially available products, 64-bit and 128-bit WEP data encryption.

802.11b Authentication

The 802.11b standard defines several services that govern how two 802.11b devices communicate. The following events must occur before an 802.11b Station can communicate with an Ethernet network through an access point such as the one built in to the FVM318:

1. Turn on the wireless station.

2. The station listens for messages from any access points that are in range.
3. The station finds a message from an access point that has a matching SSID.
4. The station sends an authentication request to the access point.
5. The access point authenticates the station.
6. The station sends an association request to the access point.
7. The access point associates with the station.
8. The station can now communicate with the Ethernet network through the access point.

An access point must authenticate a station before the station can associate with the access point or communicate with the network. The IEEE 802.11b standard defines two types of authentication: Open System and Shared Key.

- Open System Authentication allows any device to join the network, assuming that the device SSID matches the access point SSID. Alternatively, the device can use the “ANY” SSID option to associate with any available Access Point within range, regardless of its SSID.
- Shared Key Authentication requires that the station and the access point have the same WEP Key to authenticate. These two authentication procedures are described below.

Open System Authentication

The following steps occur when two devices use Open System Authentication:

1. The station sends an authentication request to the access point.
2. The access point authenticates the station.
3. The station associates with the access point and joins the network.

This process is illustrated in below.

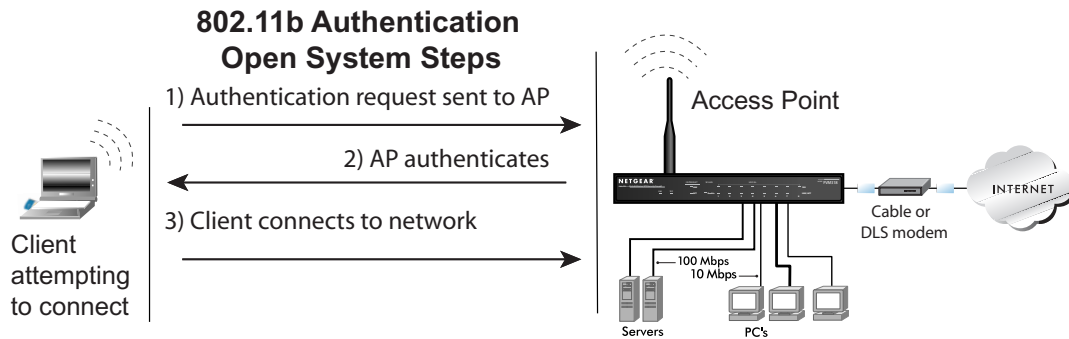


Figure 8-4: 802.11b open system authentication

Shared Key Authentication

The following steps occur when two devices use Shared Key Authentication:

1. The station sends an authentication request to the access point.
2. The access point sends challenge text to the station.
3. The station uses its configured 64-bit or 128-bit default key to encrypt the challenge text, and sends the encrypted text to the access point.
4. The access point decrypts the encrypted text using its configured WEP Key that corresponds to the station's default key. The access point compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, then the access point and the station share the same WEP Key and the access point authenticates the station.
5. The station connects to the network.

If the decrypted text does not match the original challenge text (i.e., the access point and station do not share the same WEP Key), then the access point will refuse to authenticate the station and the station will be unable to communicate with either the 802.11b network or Ethernet network.

This process is illustrated in below.

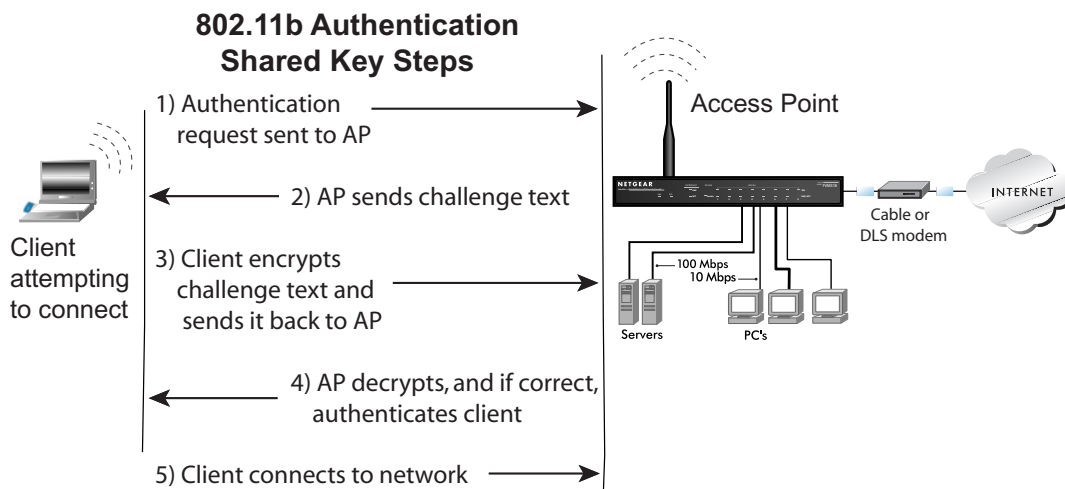


Figure 8-5: 802.11b shared key authentication

Overview of WEP Parameters

Before enabling WEP on an 802.11b network, you must first consider what type of encryption you require and the key size you want to use. Typically, there are three WEP Encryption options available for 802.11b products:

1. **Do Not Use WEP:** The 802.11b network does not encrypt data. For authentication purposes, the network uses Open System Authentication.
2. **Use WEP for Encryption:** A transmitting 802.11b device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving 802.11b device decrypts the data using the same WEP Key. For authentication purposes, the 802.11b network uses Open System Authentication.
3. **Use WEP for Authentication and Encryption:** A transmitting 802.11b device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving 802.11b device decrypts the data using the same WEP Key. For authentication purposes, the 802.11b network uses Shared Key Authentication.

Note: Some 802.11b access points also support **Use WEP for Authentication Only** (Shared Key Authentication without data encryption). The FVM318 does not support this option.

Key Size

The IEEE 802.11b standard supports two types of WEP encryption: 40-bit and 128-bit.

The 64-bit WEP data encryption method, allows for a five-character (40-bit) input. Additionally, 24 factory-set bits are added to the forty-bit input to generate a 64-bit encryption key. (The 24 factory-set bits are not user-configurable). This encryption key will be used to encrypt/decrypt all data transmitted via the wireless interface. Some vendors refer to the 64-bit WEP data encryption as 40-bit WEP data encryption since the user-configurable portion of the encryption key is 40 bits wide.

The 128-bit WEP data encryption method consists of 104 user-configurable bits. Similar to the forty-bit WEP data encryption method, the remaining 24 bits are factory set and not user configurable. Some vendors allow passphrases to be entered instead of the cryptic hexadecimal characters to ease encryption key entry.

128-bit encryption is stronger than 40-bit encryption, but 128-bit encryption may not be available outside of the United States due to U.S. export regulations.

When configured for 40-bit encryption, 802.11b products typically support up to four WEP Keys. Each 40-bit WEP Key is expressed as 5 sets of two hexadecimal digits (0-9 and A-F). For example, “12 34 56 78 90” is a 40-bit WEP Key.

When configured for 128-bit encryption, 802.11b products typically support four WEP Keys but some manufacturers support only one 128-bit key. The 128-bit WEP Key is expressed as 13 sets of two hexadecimal digits (0-9 and A-F). For example, “12 34 56 78 90 AB CD EF 12 34 56 78 90” is a 128-bit WEP Key.

Note: Typically, 802.11b access points can store up to four 128-bit WEP Keys but some 802.11b client adapters can only store one. Therefore, make sure that your 802.11b access and client adapters configurations match.

WEP Configuration Options

The WEP settings must match on all 802.11b devices that are within the same wireless network as identified by the SSID. In general, if your mobile clients will roam between access points, then all of the 802.11b access points and all of the 802.11b client adapters on the network must have the same WEP settings.

Note: Whatever keys you enter for an AP, you must also enter the same keys for the client adapter in the same order. In other words, WEP key 1 on the AP must match WEP key 1 on the client adapter, WEP key 2 on the AP must match WEP key 2 on the client adapter, etc.

Note: The AP and the client adapters can have different default WEP Keys as long as the keys are in the same order. In other words, the AP can use WEP key 2 as its default key to transmit while a client adapter can use WEP key 3 as its default key to transmit. The two devices will communicate as long as the AP's WEP key 2 is the same as the client's WEP key 2 and the AP's WEP key 3 is the same as the client's WEP key 3.

Wireless Channel Selection

IEEE 802.11 wireless nodes communicate with each other using radio frequency signals in the ISM (Industrial, Scientific, and Medical) band between 2.4 GHz and 2.5 GHz. Neighboring channels are 5 MHz apart. However, due to spread spectrum effect of the signals, a node sending signals using a particular channel will utilize frequency spectrum 12.5 MHz above and below the center channel frequency. As a result, two separate wireless networks using neighboring channels (for example, channel 1 and channel 2) in the same general vicinity will interfere with each other. Applying two channels that allow the maximum channel separation will decrease the amount of channel cross-talk, and provide a noticeable performance increase over networks with minimal channel separation.

The radio frequency channels used are listed in Table 8-1:

Table 8-1. 802.11 Radio Frequency Channels

Channel	Center Frequency	Frequency Spread
1	2412 MHz	2399.5 MHz - 2424.5 MHz
2	2417 MHz	2404.5 MHz - 2429.5 MHz
3	2422 MHz	2409.5 MHz - 2434.5 MHz
4	2427 MHz	2414.5 MHz - 2439.5 MHz
5	2432 MHz	2419.5 MHz - 2444.5 MHz
6	2437 MHz	2424.5 MHz - 2449.5 MHz
7	2442 MHz	2429.5 MHz - 2454.5 MHz
8	2447 MHz	2434.5 MHz - 2459.5 MHz
9	2452 MHz	2439.5 MHz - 2464.5 MHz
10	2457 MHz	2444.5 MHz - 2469.5 MHz
11	2462 MHz	2449.5 MHz - 2474.5 MHz
12	2467 MHz	2454.5 MHz - 2479.5 MHz
13	2472 MHz	2459.5 MHz - 2484.5 MHz

Note: The available channels supported by the wireless products in various countries are different.

The preferred channel separation between the channels in neighboring wireless networks is 25 MHz (5 channels). This means that you can apply up to three different channels within your wireless network. There are only 11 usable wireless channels in the United States. It is recommended that you start using channel 1 and grow to use channel 6, and 11 when necessary, as these three channels do not overlap.

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 and pinout as described in [Table 8-2](#).

Table 8-2. 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	

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 FVM318 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.

Cable Quality

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 or Cat V, 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.

How Does VPN Work?

A VPN can be thought of as a secure tunnel passing through the Internet, connecting two devices such as a PC or router, which form the two tunnel endpoints. At one endpoint, data is encapsulated and encrypted, then transmitted through the Internet. At the far endpoint, the data is received, unencapsulated and decrypted. Although the data may pass through several Internet routers between the endpoints, the encapsulation and encryption forms a virtual “tunnel” for the data.

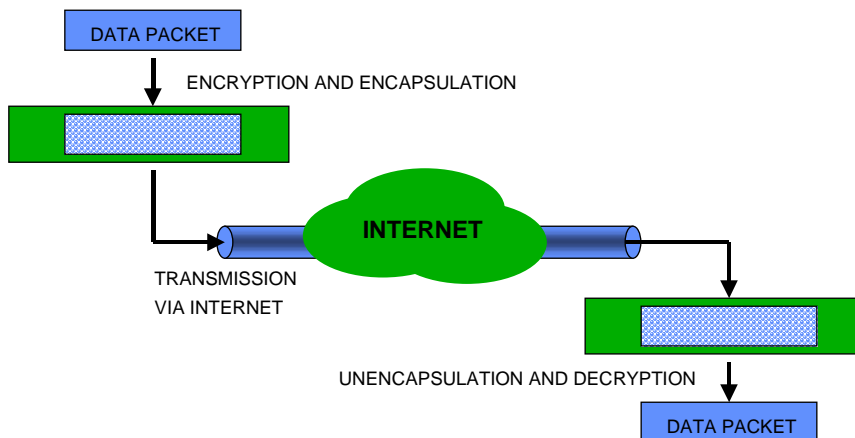


Figure 8-6: VPN overview

The tunnel endpoint device, which encodes or decodes the data, can either be a PC running VPN client software or a VPN-enabled router or server. Several software standards exist for VPN data encapsulation and encryption, such as PPTP and IPSec. Your FVM318 firewall uses both PPTP and IPSec.

To set up a VPN connection, you must configure each endpoint with specific identification and connection information describing the other endpoint. This set of configuration information defines a security association (SA) between the two points.

IKE: Managing and Exchanging Keys

IKE (Internet Key Exchange protocol) is the protocol used to perform key exchange between IPSec devices. In order to initiate communication, the following tasks need to be done:

- Negotiate security protocols, encryption algorithms and keys with all communicating peers

- Exchange keys
- Keep track of the agreements

Negotiating the SA - the Internet Key Exchange (IKE)

IKE provides a way to:

- Ensure that the key exchange and the IPSec communication occurs only between authenticated parties;
- Negotiate the protocols, algorithms and keys to be used between the two IPSec hosts
- Securely update and renegotiate SAs when they have expired.

IKE functions in two phases:

1. Phase 1. The peers establish a secure channel. After Phase 1, all IKE packets are encrypted.
2. Phase 2. The peers negotiate a general purpose SA.

IKE provides three modes of key exchange and setting up of SAs. Two of the modes are used in the first phase and one in the second.

Authentication: Phase 1

Main mode or Aggressive mode can be chosen in the first phase.

- **Main mode.** This mode accomplishes the first phase by establishing a secure channel before sending a user identity.

Main mode secures an IKE SA in three two-way exchanges between the initiator and the responder.

- a. Both agree on basic algorithms and hashes.
 - b. Both exchange Diffie-Hellman public keys and pass nonces. Nonce is a cryptographic term for a fresh random number that is used only once.
 - c. Both parties verify each other's identity. This exchange is already encrypted.
- **Aggressive mode.** Unlike Main mode, it does not protect identities because it establishes the secure channel after the information has been exchanged.

Aggressive mode establishes a connection with two exchanges. Only one of these is a round-trip exchange.

- a. The initiator generates a Diffie-Hellman public value, sending it with the nonce.

- b. The responder sends its own Diffie-Hellman value.
- c. The initiator confirms the exchange.

Key Exchange: Phase 2

Quick mode is used in the second phase. Quick mode negotiates the IPsec SA.

- Once the SA has been established, the parties use Quick mode to negotiate security services and generate fresh key material.
- A single SA negotiation results in two SAs, one inbound and one outbound. Both SAs are one-way.

Two Common Applications of VPN

Two common applications of VPN are:

- Secure access from a remote PC, such as a telecommuter connecting to an office network
- Secure access between two networks, such as a branch office and a main office

These applications are described below.

Accessing Network Resources from a VPN Client PC

VPN client remote 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 NETGEAR VPN-enabled router on your network is the other tunnel endpoint, as shown below.



Figure 8-7: Client to LAN access through VPN router

In some cases, the client PC may connect to the Internet through a local non-VPN-enabled router, as shown below:



Figure 8-8: Client to LAN access through simple router to VPN router

If the non-VPN router is performing NAT, it must support “VPN-passthrough” of IPSec-encoded data.

Linking Two Networks Together

A VPN between two NETGEAR VPN-enabled routers is a good way to connect branch offices and business partners over the Internet, offering an affordable, high-performance alternative to leased site-to-site lines. The VPN also provides access to remote network resources when NAT is enabled and remote computers have been assigned private IP addresses.



Figure 8-9: LAN to LAN access through VPN router to VPN router

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 C

Preparing Your Network

This appendix describes how to prepare your network to connect to the Internet through the FVM318 Cable/DSL ProSafe Wireless VPN Security 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-20 or [“Obtaining ISP Configuration Information for Macintosh Computers”](#) on page C-21 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, “Network, Routing, Firewall, and Wireless Basics.”](#)

The FVM318 firewall is shipped configured as a DHCP server by default. 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

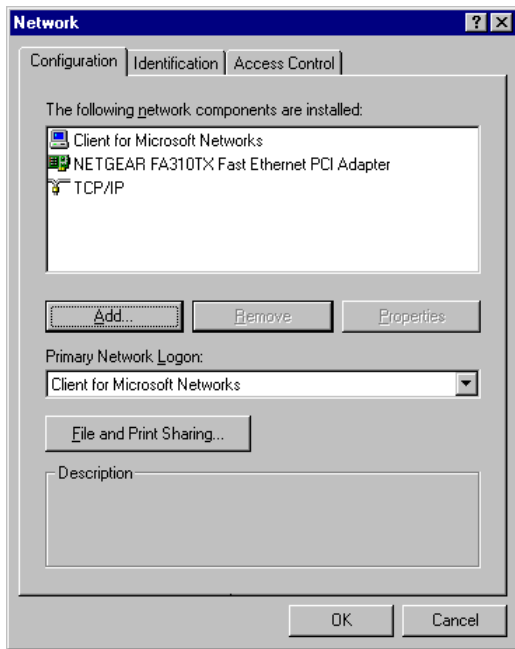
As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

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:



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 in Windows 95B, 98, and Me

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.

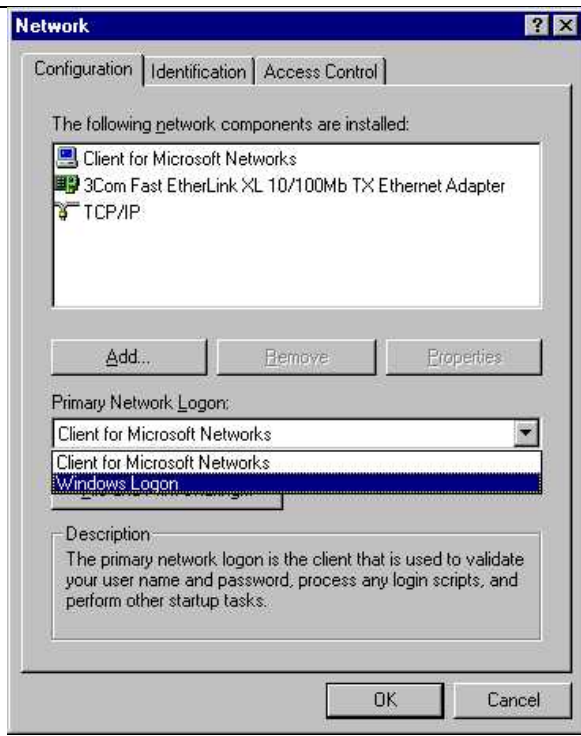
- If the Network Neighborhood icon is on the Windows desktop, position your mouse pointer over it and right-click your mouse button.
- If the icon is not on the desktop,
 - Click **Start** on the task bar located at the bottom left of the window.
 - Choose **Settings**, and then **Control Panel**.
 -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

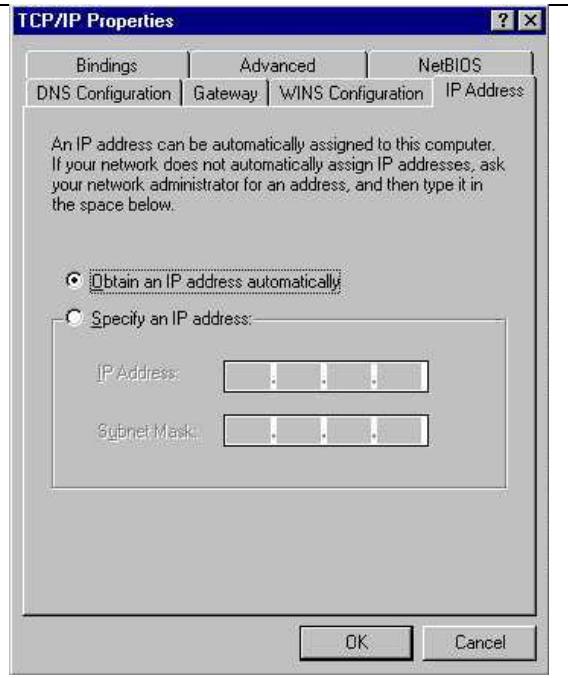


3

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.



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 *wiipcfg.exe*:

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

2. Type `winiipcfg`, 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

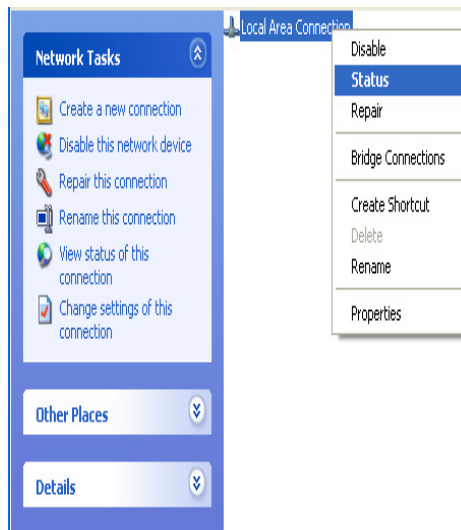
Locate your **Network Neighborhood** icon.

- Select **Control Panel** from the Windows XP new Start Menu.
- Select the **Network Connections** icon on the Control Panel. This will take you to the next step.

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.

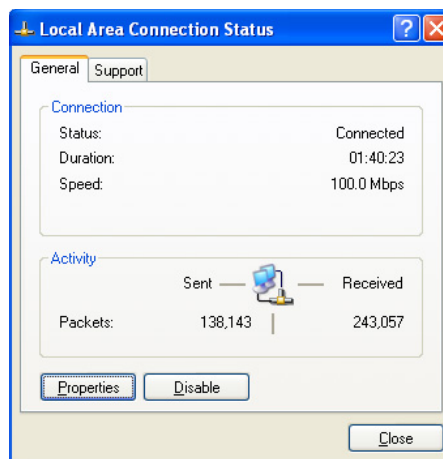
- Right-click on the **Connection with the wireless icon** and choose **Status**.



3

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

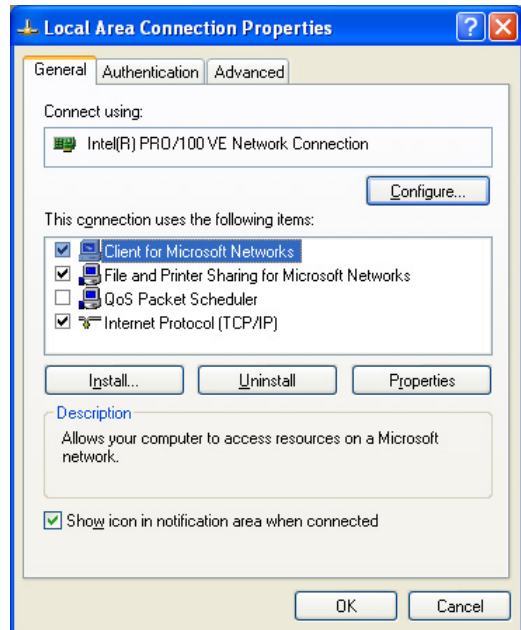
- Administrator logon access rights are needed to use this window.
- Click the **Properties** button to view details about the connection.



4

The TCP/IP details are presented on the Support tab page.

- Select **Internet Protocol**, and click **Properties** to view the configuration information.



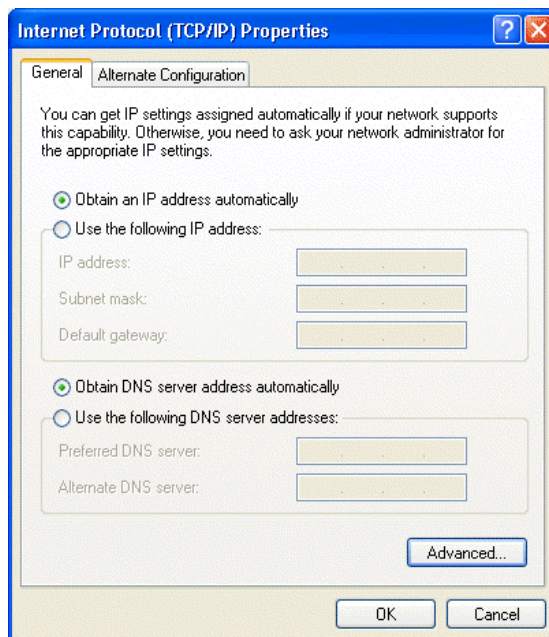
5

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.



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, you may need to know how to do it manually. Remember, Cox only sets up TCP/IP dynamically, (i.e., it uses DHCP to obtain TCP/IP settings). Following are the steps to configure TCP/IP with DHCP for Windows 2000.

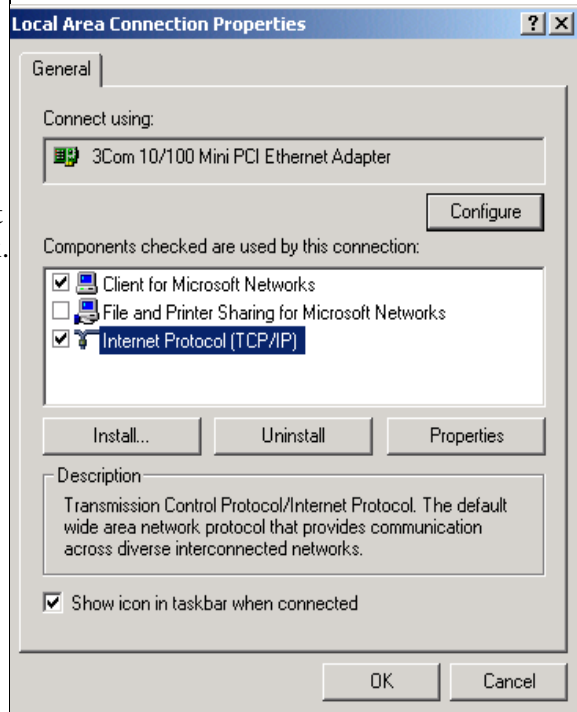
1

- 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

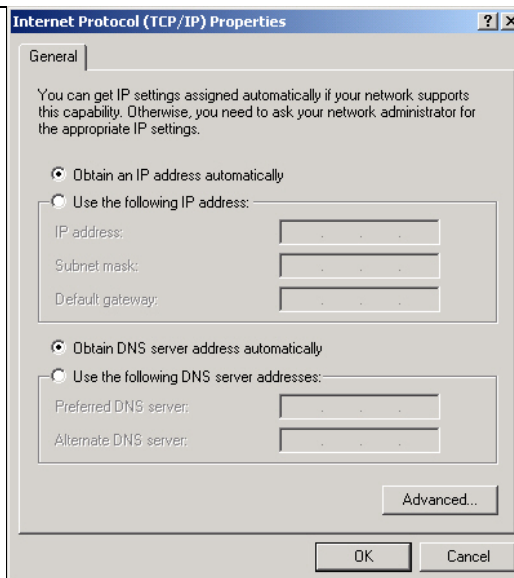
The **Local Area Connection Properties** dialog box appears.

- 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)
- Click **OK**.



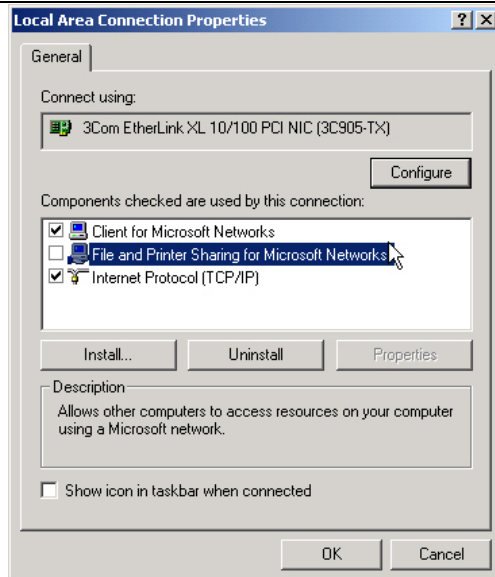
3

- With Internet Protocol (TCP/IP) selected, click on **Properties** 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.



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.



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. Again, remember Cox only sets up TCP/IP dynamically (i.e., it uses DHCP to obtain TCP/IP settings).

Following are the procedures you use to configure TCP/IP with DHCP in Windows NT 4.0.

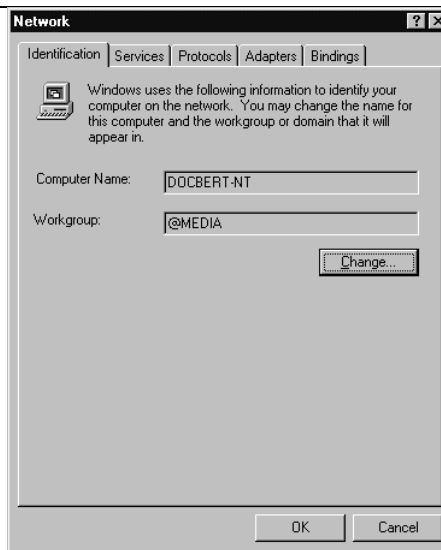
1

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

2

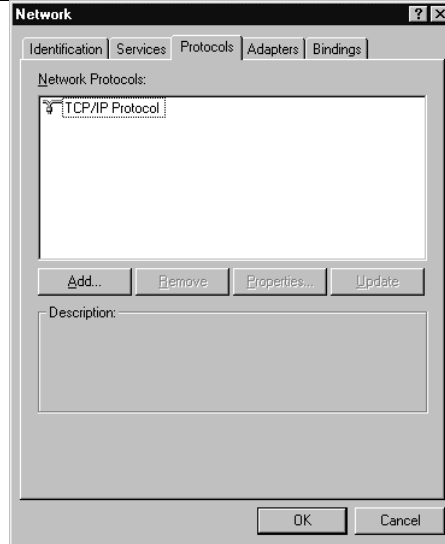
- Double-click the **Network** icon in the Control Panel window.

The Network panel will display.
- Select the **Protocols** tab to continue.



3

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



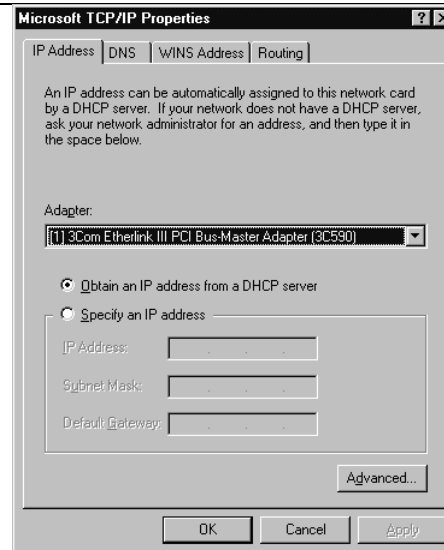
4

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.



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`

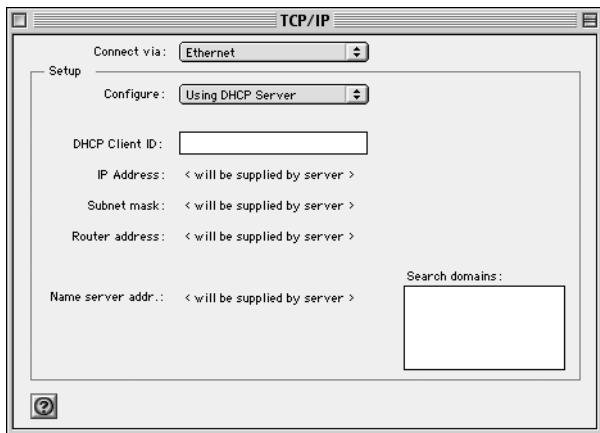
Configuring the Macintosh for TCP/IP Networking

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:



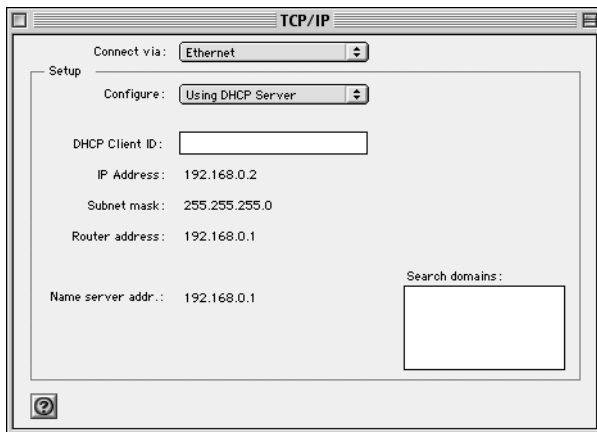
2. From the “Connect via” box, select your Macintosh’s Ethernet interface.
3. From the “Configure” box, select Using DHCP Server.
You can leave the DHCP Client ID box empty.
4. Close the TCP/IP Control Panel.
5. Repeat this for each Macintosh on your network.

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.



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 FVM318 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 FVM318 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.

After configuring all of your computers for TCP/IP networking and restarting them, and connecting them to the local network of your FVM318 firewall, you are ready to access and configure the firewall.

Glossary

10BASE-T	IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.
100BASE-Tx	IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.
3DES	3DES (Triple DES) achieves a high level of security by encrypting the data three times using DES with three different, unrelated keys.
802.11b	IEEE specification for wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz.
ADSL	<i>See</i> Asymmetric Digital Subscriber Line.
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.
Denial of Service attack	DoS. A hacker attack designed to prevent your computer or network from operating or communicating.
DES	The Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56 bit key. <i>See</i> also 3DES.
Diffie-Hellman	Diffie Hellman shared secret algorithm is a method for securely exchanging a shared secret between two parties, in real-time, over an untrusted network. A shared secret allows two parties, who may not have ever communicated previously, to encrypt their communications. As such, it is used by several protocols, including Secure Sockets Layer (SSL) and Internet Protocol Security (IPSec).
DHCP	<i>See</i> Dynamic Host Configuration Protocol.

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	<i>See</i> Domain Name Server.
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.
Domain Name Server	DNS. A Domain Name Server resolves descriptive names of network resources (such as www.NETGEAR.com) to numeric IP addresses.
DSL	<i>See</i> Asymmetric Digital Subscriber Line
Asymmetric Digital Subscriber Line	A technology for sending data over regular telephone lines. ADSL allows data rates up to 8 Mbps downstream and 640 Kbps upstream.
Dynamic Host Configuration Protocol	DHCP. An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.
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.
gateway	A local device, usually a router, that connects hosts on a local network to other networks.
IETF	Internet Engineering Task Force. An open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. Working groups of the IETF propose standard protocols and procedures for the Internet, which are published as RFCs (Request for Comment) at www.ietf.org .
IKE	Internet Key Exchange. An automated method for exchanging and managing encryption keys between two VPN devices.

IP	Internet Protocol. The main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.
IP Address	A four-position number uniquely defining each host on the Internet. Ranges of addresses are assigned by Internic, an organization formed for this purpose. Usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57).
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.
ISP	Internet service provider.
LAN	<i>See</i> local area network.
local area network	LAN. 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.
MAC address	Media Access Control address. A unique 48-bit hardware address assigned to every Ethernet node. Usually written in the form 01:23:45:67:89:ab.
Mbps	Megabits per second.
MSB	<i>See</i> Most Significant Bit or Most Significant Byte.
MTU	<i>See</i> Maximum Transmit Unit.
Maximum Transmit Unit	The size in bytes of the largest packet that can be sent or received.
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.
NAT	<i>See</i> Network Address Translation.
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	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	A technique by which several hosts share a single IP address for access to the Internet.
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.
PPP	<i>See</i> Point-to-Point Protocol.
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.
PSTN	Public Switched Telephone Network.
Point-to-Point Protocol	PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.
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	<i>See</i> Routing Information Protocol.
router	A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.
Routing Information Protocol	RIP. A protocol in which routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.
SSID	Service Set Identification. A thirty-two character (maximum) alphanumeric key identifying the 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. <i>See also</i> Wireless Network Name and ESSID.

subnet mask	<i>See</i> netmask.
UPnP	<i>See</i> Universal Plug and Play.
Universal Plug and Play	UPnP. A networking architecture that provides compatibility among networking equipment, software and peripherals of the 400+ vendors that are part of the Universal Plug and Play Forum. 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.
URL	Universal Resource Locator, the global address of documents and other resources on the World Wide Web.
UTP	Unshielded twisted pair. The cable used by 10BASE-T and 100BASE-Tx Ethernet networks.
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.
WAN	<i>See</i> wide area network.
WEB Proxy Server	A Web proxy server is a specialized HTTP server that allows clients access to 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.
WEP	Wired Equivalent Privacy. WEP is a data encryption protocol for 802.11b wireless networks. All wireless nodes and access points on the network are configured with a 64-bit or 128-bit Shared Key for data encryption.
wide area network	WAN. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.
Wi-Fi	<i>See</i> 802.11b. A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standard group promoting interoperability among 802.11b devices.
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 Network Neighborhood.

- Wireless Network Name (SSID)** Wireless Network Name (SSID). The name assigned to a wireless network. This is the same as the SSID or ESSID configuration parameter. There can be multiple wireless networks in a given area. You can connect to only one wireless network at a time. *See also* SSID and ESSID.
- WINS** *See* Windows Internet Naming Service.

Chapter 1 Index

Numerics

3DES 3-6
64 or 128 bit WEP 3-6
802.11b B-12

A

Account Name 2-10, 2-13
ActiveX 4-3
Address Resolution Protocol B-9
ad-hoc mode B-12, B-13
AES 3-6
Auto MDI/MDI-X B-20
Auto Uplink 1-3, B-20

B

backup configuration 6-9
Basic IPsec Wireless Connections 3-13
Basic Wireless Connectivity 3-7
BSSID B-13

C

cables, pinout B-19
Cabling B-19
Cat5 cable 2-1, B-20
Channel 3-4, B-18
configuration
 automatic by DHCP 1-3
 backup 6-9
 erasing 6-10
 router, initial 2-1
Connection Monitor 5-18
content filtering 1-2

conventions
 typography 1-xiii
cookie 4-3
crossover cable 1-3, 8-3, B-20
customer support 1-iii

D

date and time 8-8
Daylight Savings Time 4-9, 8-8
daylight savings time 4-9
Default DMZ Server 7-1
default reset button 8-8
Denial of Service (DoS) protection 1-2, 4-3
denial of service attack B-11
DES 3-6
DHCP 1-3, 7-4, B-10
DHCP Client ID C-17
DHCP Setup field, Ethernet Setup menu 6-2
DMZ Server 7-1
DNS Proxy 1-3
DNS server 2-10, 2-13, C-21
DNS, dynamic 7-7
domain C-21
Domain Name 2-10, 2-13
domain name server (DNS) B-9
DoS attack B-11
Dynamic DNS 1-3, 7-7

E

Encryption Strength 3-5
endpoint B-21

- EnterNet C-19
- EPROM, for firmware upgrade 1-4
- ESSID 3-8, B-13
- Ethernet 1-2
- Ethernet cable B-19

F

- factory settings, restoring 6-10
- features 1-1
- firewall features 1-2
- FLASH memory 6-13
- front panel 1-5

G

- gateway address C-21

H

- host name 2-10, 2-13

I

- IANA
 - contacting B-2
- IETF B-1
 - Web site address B-7
- IKE 5-7
- IKE Life Time 5-7, 5-11
- infrastructure mode B-12, B-13
- installation 1-4
- Internet account
 - address information C-19
 - establishing C-19
- Internet Service Provider 2-1
- IP addresses C-20, C-21
 - and NAT B-8
 - and the Internet B-2
 - assigning B-2, B-9
 - auto-generated 8-3
 - private B-7
 - translating B-9

- IP configuration by DHCP B-10
- IP networking
 - for Macintosh C-17
 - for Windows C-2, C-7
- IPSec B-21
- IPSec Wireless Connections 3-12
- ISP 2-1

J

- Java 4-3

K

- Key Life 5-7, 5-11

L

- LAN IP Setup Menu 5-5, 7-6
- LEDs
 - description 1-6
 - troubleshooting 8-2
- log
 - sending 6-8
- Log Viewer 5-18

M

- MAC address 8-7, B-9
 - spoofing 2-13, 8-5
- MAC address filter 3-10
- Macintosh C-20
 - configuring for IP networking C-17
 - DHCP Client ID C-17
 - Obtaining ISP Configuration Information C-21
- Manual Keying 5-19
- masquerading C-19
- MD5 authentication 5-21
- MDI/MDI-X B-20
- MDI/MDI-X wiring B-19
- metric 7-10
- MTU 7-4
- multicasting 7-3

N

NAT C-19
NAT. *See* Network Address Translation
netmask
 translation table B-6
Network Address Translation 1-3, B-8, C-19
Network Time Protocol 4-7, 8-8
NTP 4-7, 8-8

O

Open System authentication B-13

P

package contents 1-5
Passphrase 3-7, 3-11
password
 restoring 8-7
PC, using to configure C-22
Perfect Forward Secrecy 5-7, 5-11
ping 7-2
pinout, Ethernet cable B-19
placement 3-1
port forwarding behind NAT B-8
PPP over Ethernet 1-3, C-19
PPPoE 1-3, C-19
PPTP B-21
PreShared Key 5-4, 5-7, 5-9, 5-11, 5-22, 5-23
Primary DNS Server 2-9, 2-10, 2-11, 2-13
protocols
 Address Resolution B-9
 DHCP 1-3, B-10
 Routing Information 1-3, B-2
 support 1-3
 TCP/IP 1-3
publications, related B-1

R

range 3-1

rear panel 1-7
requirements
 hardware 2-1
reserved IP addresses 7-5
reset button, clearing config 8-8
restore factory settings 6-10
Restrict Wireless Access by MAC Address 3-9
RFC
 1466 B-7, B-9
 1597 B-7, B-9
 1631 B-8, B-9
 finding B-7
RIP (Router Information Protocol) 7-3
router concepts B-1
Routing Information Protocol 1-3, B-2

S

SA 5-3, B-21
SafeNet Secure VPN Client 5-8
Secondary DNS Server 2-9, 2-10, 2-11, 2-13
security association 5-3, B-21
Setup Wizard 2-1
SHA-1 authentication 5-21
Shared Key authentication B-13
SMTP 6-8
SPI (Security Parameter Index) 5-20
spooof MAC address 8-5
SSID 3-3, 3-8, 3-9, B-13
stateful packet inspection 1-2, B-11
Static Routes 7-6
subnet addressing B-5
subnet mask B-6, C-20, C-21
Syslog 6-7

T

TCP/IP
 configuring C-1
 network, troubleshooting 8-5
TCP/IP properties

- verifying for Macintosh C-18
- verifying for Windows C-6, C-16
- time of day 8-8
- time zone 4-9
- timeout, administrator login 4-3
- time-stamping 4-9
- troubleshooting 8-1
- Trusted Host 4-5
- Trusted PCs Only 3-4
- tunnel B-21
- typographical conventions 1-xiii

- Wireless Range Guidelines 3-1
- Wireless Security 3-2

U

- Uplink switch B-20
- USB C-19

V

- VPN 1-1

W

- web proxy 4-3
- WEP B-13
- Wi-Fi B-12
- Windows, configuring for IP routing C-2, C-7
- winipcfg utility C-6
- WinPOET C-19
- WINS 7-5
- Wired Equivalent Privacy. *See* WEP
- Wireless Access 2-3
- Wireless Authentication 3-4
- wireless authentication scheme 3-4
- Wireless Card Access List 3-4
- Wireless Encryption 3-4
- Wireless Ethernet B-12
- Wireless IPSec 3-5
- Wireless Network Settings 3-3
- Wireless Performance 3-1