Model FVL328 ProSafe High-Speed VPN Firewall Reference Manual

NETGEAR

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

SM-FVL328NA-0
November 2002

Trademarks

NETGEAR and Auto Uplink are trademarks or registered trademarks of Netgear, Inc.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders. Portions of this document are copyright Intoto, Inc.

Statement of Conditions

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

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

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

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. 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 FVL328 Prosafe High Speed VPN Firewall is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

Certificate of the Manufacturer/Importer

It is hereby certified that the FVL328 Prosafe High Speed VPN Firewall has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

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

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß dasFVL328 Prosafe High Speed VPN Firewall gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

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

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the second category (information equipment to be used in a residential area or an adjacent area thereto), and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines, aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference.

Read instructions for correct handling.

Technical Support

Refer to the Support Information Card that shipped with your FVL328 Prosafe High Speed VPN Firewall.

World Wide Web

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

Contents

Preface
About This Manual

Chapter 1
Introduction

Chapter 2
Connecting the Firewall to the Internet

Chapter 3
Protecting Your Network

Chapter 4
Virtual Private Networking

Chapter 5
Managing Your Network

Appendix A
Technical Specifications

Appendix B
Networks, Routing, and Firewall Basics

Appendix C
Preparing Your Network

Glossary

Index

List of Procedures

Preface
About This Manual

Thank you for purchasing the NETGEAR™ FVL328 Prosafe High Speed VPN 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.
ALL 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.

Procedure: This format is used to let you know that you are following a sequence of steps required to complete a task.

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.

Technical Support

For help with any technical issues, contact Customer Support at 1-888-NETGEAR, or visit us on the Web at *www.NETGEAR.com*. The NETGEAR Web site includes an extensive knowledge base, answers to frequently asked questions, and a means for submitting technical questions online.

Chapter 1
Introduction

This chapter describes the features of the NETGEAR FVL328 Prosafe High Speed VPN Firewall.

About the FVL328

The FVL328 is a complete security solution that protects your network from attacks and intrusions and enables secure communications using Virtual Private Networks (VPN). Unlike simple Internet sharing routers that rely on Network Address Translation (NAT) for security, the FVL328 uses Stateful Packet Inspection for Denial of Service (DoS) attack protection and intrusion detection. The 8-port FVL328 provides highly reliable Internet access for up to 253 users with up to 100 concurrent VPN tunnels.

Key Features

The FVL328 offers the following features.

A Powerful, True Firewall

Unlike simple Internet sharing NAT routers, the FVL328 is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- DoS protection
  Automatically detects and thwarts DoS attacks such as Ping of Death, SYN Flood, LAND Attack and IP Spoofing.
- Blocks unwanted traffic from the Internet to your LAN.
- Blocks access from your LAN to Internet locations or services that you specify as off-limits.

- Logs security incidents
  The FVL328 will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the firewall to e-mail the log to you at specified intervals. You can also configure the firewall to send immediate alert messages to your e-mail address or e-mail pager whenever a significant event occurs.

Virtual Private Networking

The FVL328 Firewall provides a secure encrypted connection between your local network and remote networks or clients. Its VPN features include:

- Support for 100 simultaneous VPN connections.
- Support for industry standard VPN protocols.
  The FVL328 Prosafe High Speed VPN Firewall supports standard keying methods (Manual or IKE), standard authentication methods (MD5 and SHA-1), and standard encryption methods (DES, 3DES). It is compatible with many other VPN products.
- Support for up to 168 bit encryption (3DES) for maximum security.
- Support for VPN Main Mode, Aggressive mode, or Manual Keying.

Content Filtering

With its content filtering feature, the FVL328 prevents objectionable content from reaching your PCs. The firewall allows you to control access to Internet content by screening for keywords within Web addresses. You can configure the firewall to log and report attempts to access objectionable Internet sites.

Configurable Auto Uplink™ Ethernet Connection

With its internal 8-port 10/100 switch, the FVL328 can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. Both the local LAN and the Internet WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

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

Protocol Support

The FVL328 supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). Appendix B, “Networks, Routing, and Firewall Basics” provides further information on TCP/IP.

- IP Address Sharing by NAT
  The FVL328 allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as NAT, allows the use of an inexpensive single-user ISP account.
- Automatic Configuration of Attached PCs by DHCP
  The FVL328 dynamically assigns network configuration information, including IP, gateway, and domain name server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of PCs on your local network.
- DNS Proxy
  When DHCP is enabled and no DNS addresses are specified, the firewall provides its own address as a DNS server to the attached PCs. The firewall obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.
- PPP over Ethernet (PPPoE)
  PPPoE is a protocol for connecting remote hosts to the Internet over a DSL connection by simulating a dial-up connection. This feature eliminates the need to run a login program such as EnterNet or WinPOET on your PC.
- Point-to-Point Tunneling Protocol 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 many popular Dynamic DNS services to register your dynamic IP address.

Easy Installation and Management

You can install, configure, and operate the FVL328 within minutes after connecting it to the network. The following features simplify installation and management tasks:

- Browser-based management
  Browser-based configuration allows you to easily configure your firewall from almost any type of personal computer, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided and online help documentation is built into the browser-based Web Management Interface.
- Smart Wizard
  The firewall automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- Remote management
  The firewall allows you to login to the Web Management Interface from a remote location via the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses, and you can choose a nonstandard port number.
- Diagnostic functions
  The firewall incorporates built-in diagnostic functions such as Ping, DNS lookup, and remote reboot. These functions allow you to test Internet connectivity and reboot the firewall. You can use these diagnostic functions directly from the FVL328 when your are connected on the LAN or when you are connected over the Internet via the remote management function.
- Visual monitoring
  The firewall’s front panel LEDs provide an easy way to monitor its status and activity.
- Flash EPROM for firmware upgrade
- Regional support, including ISPs like Telstra DSL and BigPond or Deutsche Telekom.

What’s in the Box?

The product package should contain the following items:

- FVL328 Prosafe High Speed VPN Firewall
- AC power adapter
- Category 5 (CAT5) Ethernet cable
- FVL328 *Resource CD*, including:
  - This manual
  - Application notes, tools, and other helpful information
- Warranty and registration card
- Support information card

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

The Firewall’s Front Panel

The front panel of the FVL328 (Figure 1-1) contains status LEDs.

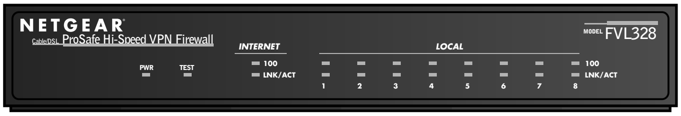


Figure 1-1: FVL328 Front Panel

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

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

Table 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		
100	On/Blinking	The Internet port is operating at 100 Mbps.
LINK/ACT (Activity)	On/Blinking	The port detected a link with the Internet WAN connection and is operating at 10 Mbps. Blinking indicates data transmission.
LOCAL		
100	On/Blinking	The Local port is operating at 100 Mbps.
LINK/ACT (Link/Activity)	On/Blinking	The Local port has detected a link with a LAN connection and is operating at 10 Mbps. Blinking indicates data transmission.

The Firewall's Rear Panel

The rear panel of the FVL328 (Figure 1-2) contains the connections identified below.

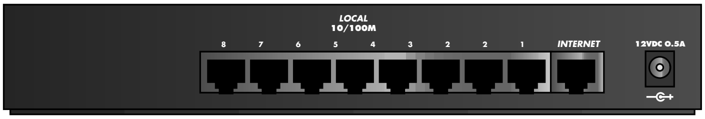


Figure 1-2: FVL328 Rear Panel

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 local computers
- Internet WAN Ethernet RJ-45 port for connecting the firewall to a cable or DSL modem
- AC power adapter input

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 FVL328 Prosafe High Speed VPN Firewall using the Setup Wizard, or how to manually configure your Internet connection.

What You Will Need Before You Begin

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

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

LAN Hardware Requirements

The FVL328 Firewall connects to your LAN via twisted-pair Ethernet cables.

Computer Requirements

To use the FVL328 Firewall on your network, each computer must have an installed Ethernet Network Interface Card (NIC) and an Ethernet cable. If the computer will connect to your network at 100 Mbps, you must use a Category 5 (CAT5) cable such as the one provided with your firewall.

Cable or DSL Modem Requirement

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

LAN Configuration Requirements

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

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

Internet Configuration Requirements

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

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

Where Do I Get the Internet Configuration Parameters?

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

- Your ISP should have provided you with all the information needed to connect to the Internet. If you cannot locate this information, you can ask your ISP to provide it or you can try one of the options below.
- If you have a computer already connected using the active Internet access account, you can gather the configuration information from that computer.
  - For Windows 95/98/Me, open the Network control panel, select the TCP/IP entry for the Ethernet adapter, and click Properties.
  - For Windows 2000/XP, open the Local Area Network Connection, select the TCP/IP entry for the Ethernet adapter, and click Properties.
  - For Macintosh computers, open the TCP/IP or Network control panel.
- You may also refer to the FVL328 *Resource CD* for the NETGEAR Router ISP Guide which provides Internet connection information for many ISPs.

Once you locate your Internet configuration parameters, you may want to record them on the page below according to the instructions in “Recording Your Internet Connection Information” on page 2-3.

Procedure 2-1: Recording Your Internet Connection Information

1. 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: _______________________

Connecting the FVL328 Firewall to Your LAN

This section provides instructions for connecting the FVL328 Prosafe High Speed VPN Firewall to your Local Area Network (LAN).

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

Procedure 2-2: Connecting the Firewall to Your LAN

There are three steps to connecting your firewall:

- Connect the firewall to your network.
- Log in to the firewall.
- Connect to the Internet.

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

1. **Connect the firewall**
   a. Turn off your computer and cable or DSL modem.

b. Disconnect the Ethernet cable (**A)** from your computer which connects to your cable or DSL modem.

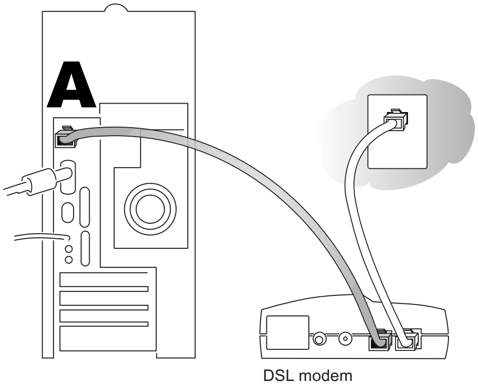


Figure 2-1: Disconnect the cable or DSL modem

c. Connect the Ethernet cable (**A)** from your Cable or DSL modem to the FVL328's Internet port.

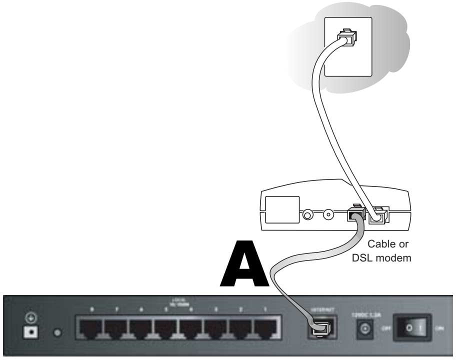


Figure 2-2: Connect the cable or DSL modem to the firewall

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

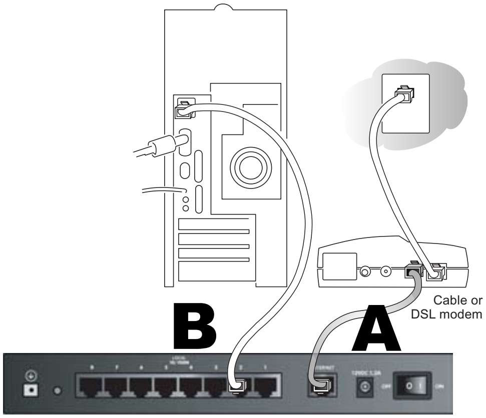


Figure 2-3: Connect the computers on your network to the firewall

Note: The FVL328 Firewall incorporates Auto Uplink™ technology. Each Ethernet port will automatically sense whether the cable plugged into the port should have a 'normal' connection (e.g. connecting to a PC) or an 'uplink' connection (e.g. connecting to a switch or hub). That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

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

2. **Log in to the firewall**

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

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

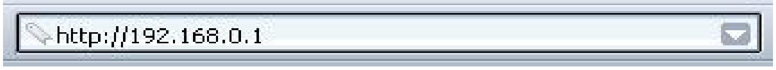
b. Now, turn on your computer.

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

Now that the cable or DSL modem, firewall, and the computer are turned on, verify the following:

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

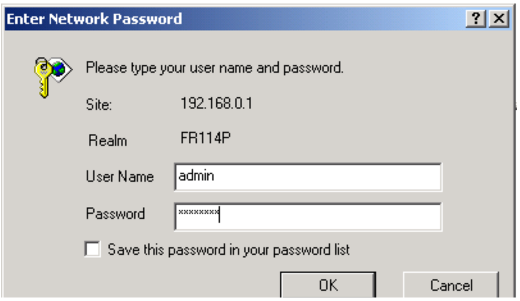
c. Next, use a browser like Internet Explorer or Netscape to log in to the firewall at its default address of *http://192.168.0.1*.



http://192.168.0.1

Figure 2-4: Log in to the firewall

A login window opens as shown in Figure 2-5 below:



Enter Network Password

Please type your user name and password.

Site: 192.168.0.1

Realm FR114P

User Name admin

Password ********

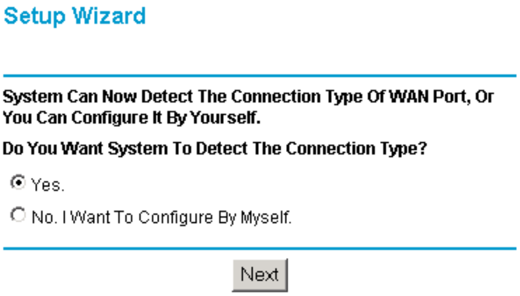
□ Save this password in your password list

Figure 2-5: Login window

d. For security reasons, the firewall has its own user name and password. When prompted, enter **admin** for the firewall User Name and **password** for the firewall Password, both in lower case letters. This default password should be changed later, see, "Protecting Access to Your FVL328 Firewall" on page 3-1.

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

3. **Connect to the Internet**



Setup Wizard

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

Do You Want System To Detect The Connection Type?

● Yes.

○ No. I Want To Configure By Myself.

Next

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. Click the Yes button in the *Setup Wizard*.

b. Please click Next to follow the steps in the Setup Wizard to input the configuration parameters from your ISP to connect to the Internet.

Note: If you were unable to connect to the firewall, please refer to “Basic Functions” on page 7-1.

Connecting the FVL328 Firewall to the Internet

The firewall is now properly attached to your network. You are now ready to configure your firewall to connect to the Internet. There are two ways you can configure your firewall to connect to the Internet:

- Let the FVL328 auto-detect the type of Internet connection you have and configure it.
- Manually choose which type of Internet connection you have and configure it.

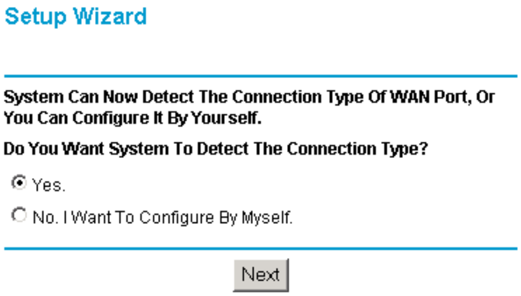
These options are described below. In either case, unless your ISP automatically assigns your configuration automatically via DHCP, you will need the configuration parameters from your ISP you recorded in “Recording Your Internet Connection Information” on page 2-3.

Procedure 2-3: Auto-Detecting Your Internet Connection Type

The Web Configuration Manager built in to the firewall contains a Setup Wizard that can automatically determine your network connection type.

1. If your firewall has not yet been configured, the Setup Wizard shown in Figure 2-7 should launch automatically.

   When the Wizard launches, select Yes in the menu below to allow the firewall to automatically determine your connection.



Setup Wizard

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

Do You Want System To Detect The Connection Type?

● Yes.

○ No. I Want To Configure By Myself.

Figure 2-7: Built-in Web-based Configuration Manager Setup Wizard

Note: If, instead of the Setup Wizard menu, the main menu of the firewall's Configuration Manager as shown in Figure 2-11 appears, click the Setup Wizard link in the upper left to bring up this menu.

2. Click Next.

   The Setup Wizard will now check for the following connection types:

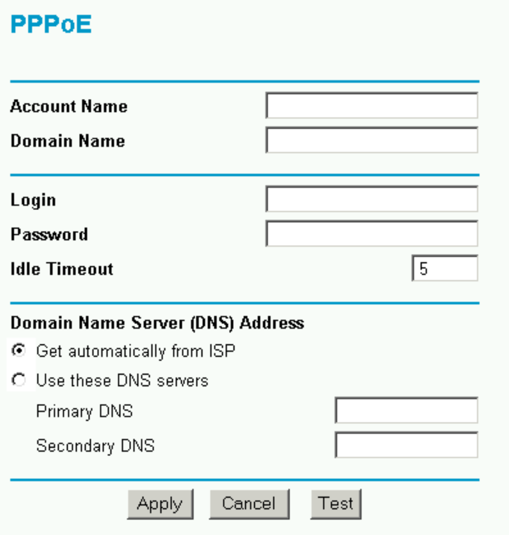
   - Dynamic IP assignment
   - A login protocol such as PPPoE
   - Fixed IP address assignment

   Next, the Setup Wizard will report which connection type it has discovered, and then display 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 modem. When the connection is properly made, the firewall's Internet LED should be on.

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

Procedure 2-4: Wizard-Detected Login Account Setup

If the Setup Wizard determines that your Internet service account uses a login protocol such as PPP over Ethernet (PPPoE), you will be directed to a menu like the PPPoE menu in Figure 2-8:



PPPoE

Account Name

Domain Name

Login

Password

Idle Timeout 5

Domain Name Server (DNS) Address

● Get automatically from ISP

○ Use these DNS servers

Primary DNS

Secondary DNS

Figure 2-8: Setup Wizard menu for PPPoE login accounts

1. Enter your Account Name (may also be called Host Name) and Domain Name. These parameters may be necessary to access your ISP's services such as mail or news servers. If you leave the Domain Name field blank, the firewall will attempt to learn the domain automatically from the ISP. If this is not successful, you may need to enter it manually.
2. Enter the PPPoE login user name and password provided by your ISP. These fields are case sensitive. If you wish to change the login timeout, enter a new value in minutes.

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

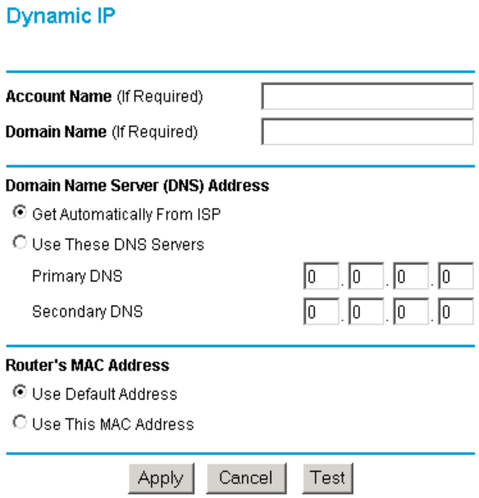
3. Domain Name Server (DNS) Address: If you know that your ISP does not automatically transmit DNS addresses to the firewall during login, select “Use these DNS servers” and enter the IP address of your ISP’s Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

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

4. Click on Apply to save your settings.
5. Click on the Test button to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to Chapter 7, Troubleshooting.

Procedure 2-5: Wizard-Detected Dynamic IP Account Setup

If the Setup Wizard determines that your Internet service account uses Dynamic IP assignment, you will be directed to the menu shown in Figure 2-9 below:



Dynamic IP

Account Name (If Required) [ ]

Domain Name (If Required) [ ]

Domain Name Server (DNS) Address

● Get Automatically From ISP

○ Use These DNS Servers

Primary DNS 0 . 0 . 0 . 0

Secondary DNS 0 . 0 . 0 . 0

Router's MAC Address

● Use Default Address

○ Use This MAC Address

Figure 2-9: Setup Wizard menu for Dynamic IP address

1. Enter your Account Name (may also be called Host Name) and Domain Name. These parameters may be necessary to access your ISP’s services such as mail or news servers. If you leave the Domain Name field blank, the firewall will attempt to learn the domain automatically from the ISP. If this is not successful, you may need to enter it manually.

2. If you know that your ISP does not automatically transmit DNS addresses to the firewall during login, select “Use these DNS servers” and enter the IP address of your ISP’s Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

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

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

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

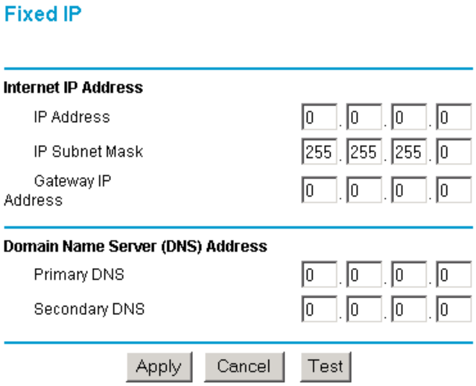
   Note: Some ISPs will register the Ethernet MAC address of the network interface card in your PC when your account is first opened. They will then only accept traffic from the MAC address of that PC. This feature allows your firewall to masquerade as that PC by using its MAC address.

4. Click on Apply to save your settings.

5. Click on the Test button to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to Chapter 7, Troubleshooting.

Procedure 2-6: Wizard-Detected Fixed IP (Static) Account Setup

If the Setup Wizard determines that your Internet service account uses Fixed IP assignment, you will be directed to the menu shown in Figure 2-10 below:



Fixed IP

Internet IP Address

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

Domain Name Server (DNS) Address

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

Figure 2-10: Setup Wizard menu for Fixed IP address

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

   DNS servers are required to perform the function of translating an Internet name such as www.netgear.com to a numeric IP address. For a fixed IP address configuration, you must obtain DNS server addresses from your ISP and enter them manually here. You should reboot your PCs after configuring the firewall for these settings to take effect.
3. Click on Apply to save the settings.
4. Click on the Test button to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to Chapter 7, Troubleshooting.

Testing Your Internet Connection

After completing the Internet connection configuration, your can test your Internet connection. Log in to the firewall, then, from the Setup Basic Settings link, click on the Test button. If the NETGEAR website does not appear within one minute, refer to Chapter 7, Troubleshooting.

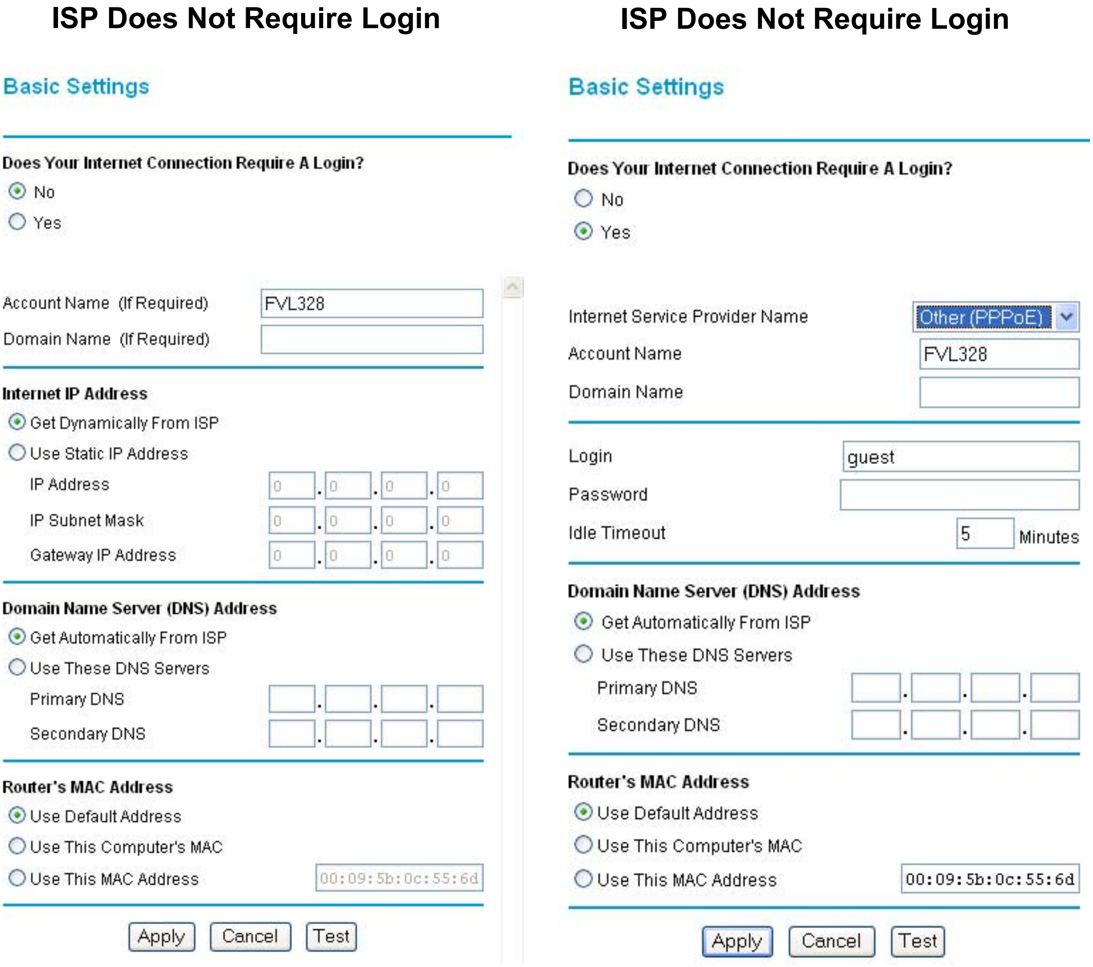
Your firewall is now configured to provide Internet access for your network. Your firewall automatically connects to the Internet when one of your computers requires access. It is not necessary to run a dialer or login application such as Dial-Up Networking or Enternet to connect, log in, or disconnect.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

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

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

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): FVL328
Domain Name (If Required):

Internet IP Address
● Get Dynamically From ISP
○ Use Static IP Address
IP Address: 0 . 0 . 0 . 0
IP Subnet Mask: 0 . 0 . 0 . 0
Gateway IP Address: 0 . 0 . 0 . 0

Domain Name Server (DNS) 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: 00:09:5b:0c:55:6d

ISP Does Not Require Login

Basic Settings

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

Internet Service Provider Name: Other (PPPoE)
Account Name: FVL328
Domain Name:

Login: guest
Password:
Idle Timeout: 5 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: 00:09:5b:0c:55:6d

Figure 2-11: Browser-based configuration Basic Settings menu

Procedure 2-7: Manual Configuration

You can manually configure the firewall in the Basic Settings menu shown in Figure 2-11 using these steps:

1. **Answer the question, "Does Your Internet Connection Require a Login?"**
   - Select Yes if you normally must launch a login program such as Enternet or WinPOET in order to access the Internet.

     Note: If you are a Telstra BigPond cable modem customer, or if you are in an area such as Austria that uses PPTP, login is required. If so, select BigPond or PPTP from the Internet Service Type drop down box.
   - Select No if you do not log in to establish your Internet connection.
2. **If you selected Yes, follow the instructions below.**
   If your Internet connection does not require a login, 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. These fields are case sensitive.
   b. If you wish 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 an Idle Timeout value of zero means never log out.
   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
3. **If you selected No, follow the instructions below.**
   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. The Account Name and Domain Name are not always required.
   b. Internet IP Address (also commonly called the WAN 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.

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

d. Router'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.

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

5. **Click on the Test button to test your Internet connection.**
If the NETGEAR website does not appear within one minute, refer to Chapter 6, Troubleshooting.Select whether your Internet connection requires a login.

Chapter 3
Protecting Your Network

This chapter describes how to use the basic firewall features of the FVL328 Prosafe High Speed VPN Firewall to protect your network.

Protecting Access to Your FVL328 Firewall

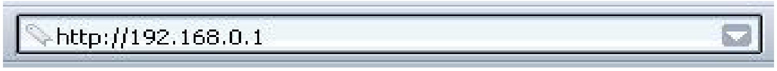
For security reasons, the firewall has its own user name and password. Also, after a period of inactivity for a set length of time, the administrator login will automatically disconnect. When prompted, enter **admin** for the firewall User Name and **password** for the firewall Password. You can use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

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

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

Procedure 3-1: Changing the Built-In Password

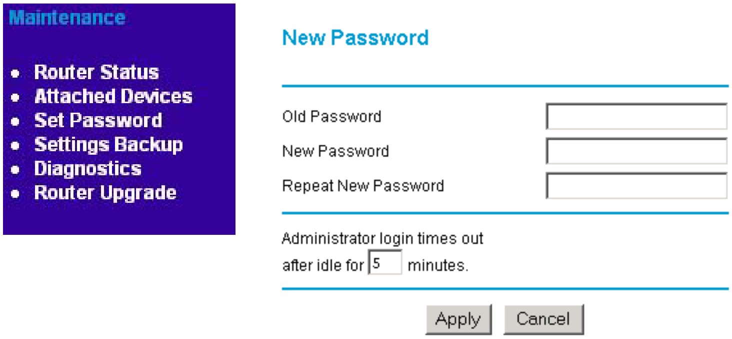
1. Log in to the firewall at its default LAN address of *http://192.168.0.1* with its default User Name of **admin**, default password of **password**, or using whatever password and LAN address you have chosen for the firewall.



http://192.168.0.1

Figure 3-1: Log in to the firewall

2. From the Main Menu of the browser interface, under the Maintenance heading, select Set Password to bring up the menu shown in Figure 3-2.



Administrator login times out after idle for 5 minutes.

Figure 3-2: Set Password menu

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

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

Procedure 3-1: 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 Keywords, Sites, and Services

The firewall provides a variety of options for blocking Internet based content and communications services. With its content filtering feature, the FVL328 Firewall prevents objectionable content from reaching your PCs. The FVL328 allows you to control access to Internet content by screening for keywords within Web addresses. Key content filtering options include:

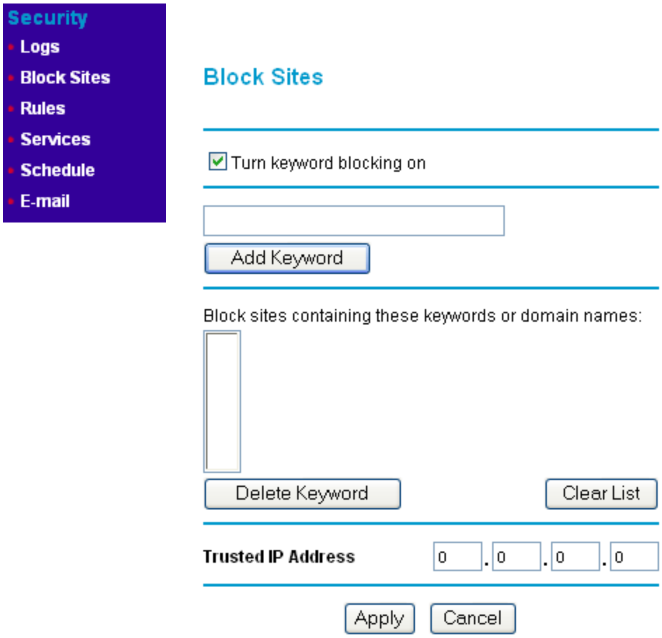
- Blocking access from your LAN to Internet locations that you specify as off-limits.
- Keyword blocking of newsgroup names.
- Outbound services blocking to limit access from your LAN to Internet locations or services that you specify as off-limits.
- Denial of Service (DoS) protection. Automatically 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.

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

Procedure 3-2: Blocking Keywords and Sites

The FVL328 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 on the Block Sites link of the Security menu.



☑ Turn keyword blocking on

Trusted IP Address 0 . 0 . 0 . 0

Figure 3-3: Block Sites menu

3. 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 blocking 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.
- If the keyword "." is entered, all Internet browsing access will be blocked.

Up to 32 entries are supported in the Keyword list.

4. To delete a keyword or domain, select it from the list, click Delete Keyword, then click Apply.
5. 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.
6. Click Apply to save your settings.

Rules

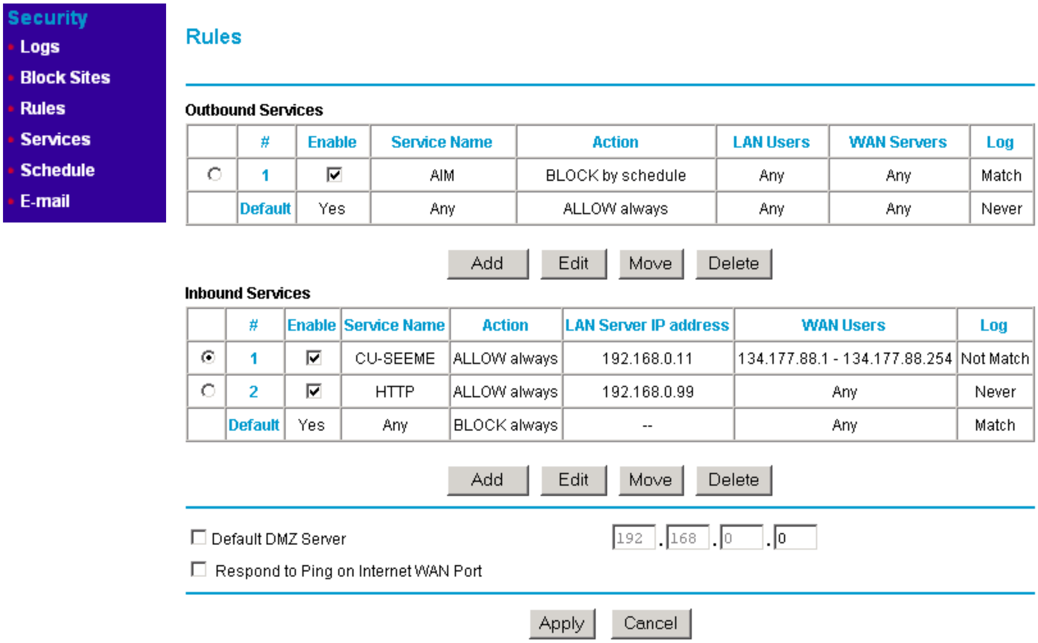
Firewall rules are used to block or allow specific traffic passing through from one side to the other. Inbound rules (WAN to LAN) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Outbound rules (LAN to WAN) determine what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

A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the FVL328 are:

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

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

To access the Rules configuration of the FVL328, click the Rules link on the main menu, then click Add for either an Outbound or Inbound Service.



Rules

Outbound Services

	#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
○	1	☑	AIM	BLOCK by schedule	Any	Any	Match
	Default	Yes	Any	ALLOW always	Any	Any	Never

Inbound Services

	#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
●	1	☑	CU-SEEME	ALLOW always	192.168.0.11	134.177.88.1 - 134.177.88.254	Not Match
○	2	☑	HTTP	ALLOW always	192.168.0.99	Any	Never
	Default	Yes	Any	BLOCK always	--	Any	Match

□ Default DMZ Server 192 . 168 . 0 . 0

□ Respond to Ping on Internet WAN Port

Figure 3-4: Rules menu

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

Inbound Rules (Port Forwarding)

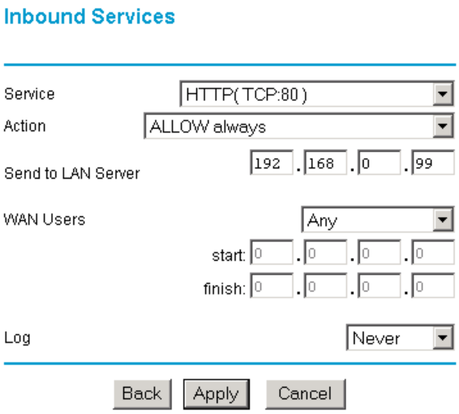
Because the FVL328 uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a web server or game server) visible and available to the Internet. The rule tells the firewall to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as port forwarding.

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

Remember that allowing inbound services opens holes in your firewall. Only enable those ports that are necessary for your network. Following are two application examples of inbound rules:

Inbound Rule Example: A Local Public Web Server

If you host a public web server on your local network, you can define a rule to allow inbound web (HTTP) requests from any outside IP address to the IP address of your web server at any time of day. This rule is shown in Figure 3-5:



Inbound Services

Service: HTTP(TCP:80)

Action: ALLOW always

Send to LAN Server: 192 . 168 . 0 . 99

WAN Users: Any

start: 0 . 0 . 0 . 0

finish: 0 . 0 . 0 . 0

Log: Never

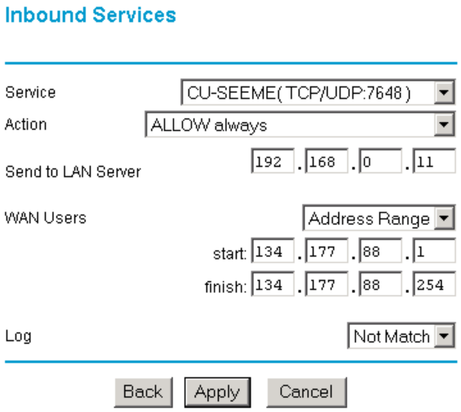
Figure 3-5: Rule example: a local public Web server

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 as seen in Figure 3-4 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.
- Send to LAN Server
  Enter the IP address of the PC or Server on your LAN which will receive the inbound traffic covered by this rule.
- WAN Users
  These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the desired option:
  - Any - All IP addresses are covered by this rule.
  - Address range - If this option is selected, you must enter the "Start" and "Finish" fields.
  - Single address - Enter the required address in the "Start" fields.
- 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.

Inbound Rule Example: Allowing Videoconferencing from Restricted Addresses

If you want to allow incoming videoconferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office, you can create an inbound rule. In the example shown in Figure 3-6, CU-SeeMe connections are allowed only from a specified range of external IP addresses. In this case, we have also specified logging of any incoming CU-SeeMe requests that do not match the allowed parameters.



Inbound Services

Service	CU-SEEME(TCP/UDP:7648)
Action	ALLOW always
Send to LAN Server	192 . 168 . 0 . 11
WAN Users	Address Range
start:	134 . 177 . 88 . 1
finish:	134 . 177 . 88 . 254
Log	Not Match

Figure 3-6: Rule example: Videoconferencing from Restricted Addresses

Considerations for Inbound Rules

- If your external IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires. Consider using the Dynamic DNS feature in the Advanced menus so that external users can always find your network.
- If the IP address of the local server PC is assigned by DHCP, it may change when the PC is rebooted. To avoid this, use the Reserved IP address feature in the LAN IP menu to keep the PC’s IP address constant.
- Local PCs must access the local server using the PCs’ local LAN address (192.168.0.11 in the example in Figure 3-6 above). Attempts by local PCs to access the server using the external WAN IP address will fail.

Outbound Rules (Service Blocking)

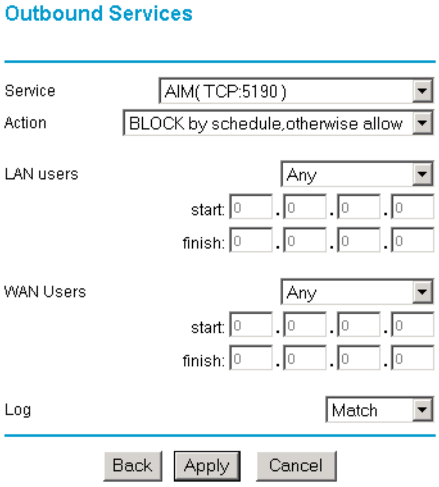
The FVL328 allows you to block the use of certain Internet services by PCs on your network. This is called service blocking or port filtering. You can define an outbound rule to block Internet access from a local PC based on:

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

Following is an application example of outbound rules:

Outbound Rule Example: Blocking Instant Messenger

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



Outbound Services

Service: AIM(TCP:5190)

Action: BLOCK by schedule,otherwise allow

LAN users: Any

start: 0 . 0 . 0 . 0

finish: 0 . 0 . 0 . 0

WAN Users: Any

start: 0 . 0 . 0 . 0

finish: 0 . 0 . 0 . 0

Log: Match

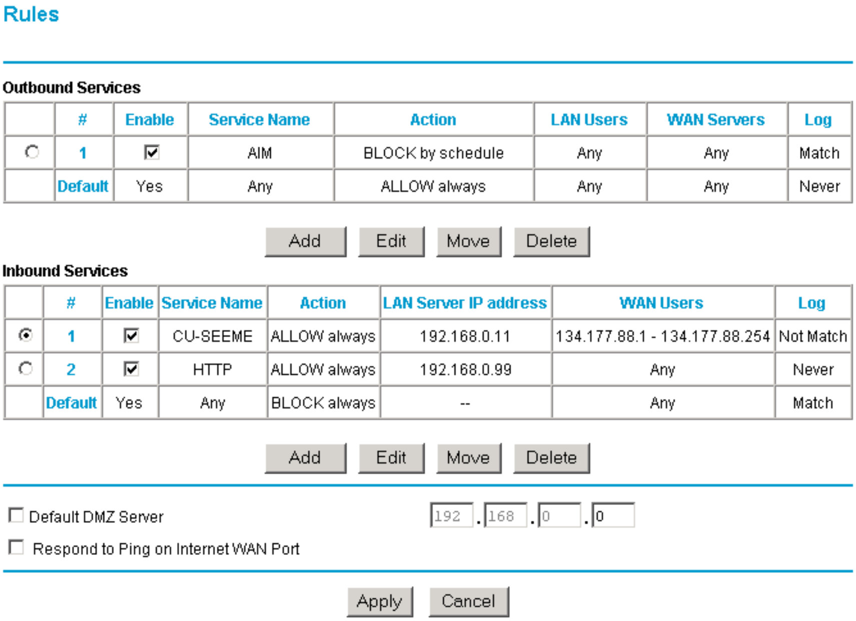
Figure 3-7: Rule example: blocking instant messenger

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 as seen in Figure 3-4 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
  These settings determine which packets are covered by the rule, based on their source LAN IP address. Select the desired option:
  - Any: All IP addresses are covered by this rule.
  - Address range: If this option is selected, you must enter the "Start" and "Finish" fields.
  - Single address: Enter the required address in the "Start" fields.
- WAN Users
  These settings determine which packets are covered by the rule, based on their destination WAN IP address. Select the desired option:
  - Any - All IP addresses are covered by this rule.
  - Address range - If this option is selected, you must enter the "Start" and "Finish" fields.
  - Single address - Enter the required address in the "Start" fields.
- 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.

Order of Precedence for Rules

As you define new rules, they are added to the tables in the Rules menu, as shown in Figure 3-8:



Rules

Outbound Services

	#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
○	1	☑	AIM	BLOCK by schedule	Any	Any	Match
	Default	Yes	Any	ALLOW always	Any	Any	Never

Inbound Services

	#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
●	1	☑	CU-SEEME	ALLOW always	192.168.0.11	134.177.88.1 - 134.177.88.254	Not Match
○	2	☑	HTTP	ALLOW always	192.168.0.99	Any	Never
	Default	Yes	Any	BLOCK always	--	Any	Match

□ Default DMZ Server 192 . 168 . 0 . 0

□ Respond to Ping on Internet WAN Port

Figure 3-8: Rules table with examples

For any traffic attempting to pass through the firewall, the packet information is subjected to the rules in the order shown in the Rules Table, beginning at the top and proceeding to the default rules at the bottom. In some cases, the order of precedence of two or more rules may be important in determining the disposition of a packet. The Move button allows you to relocate a defined rule to a new position in the table.

Services

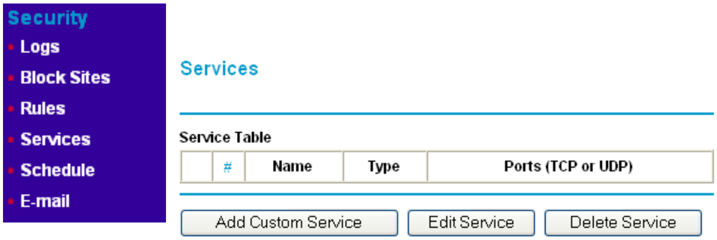
Services are functions performed by server computers at the request of client computers. For example, Web servers serve web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server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

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application. For more information on this topic please see Appendix B, "Networks, Routing, and Firewall Basics.

Although the FVL328 already holds a list of many service port numbers, you are not limited to these choices. Use the procedure below to create your own service definitions.

Procedure 3-3: Defining Services

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 Services link of the Security menu to display the menu shown in Figure 3-9:



Service Table

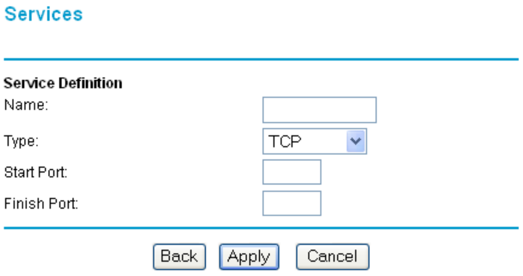
	#	Name	Type	Ports (TCP or UDP)

Figure 3-9: Services menu

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

- When there is an existing service, to edit the service, select the it from the list in the table and click Edit Service.
- To delete an existing Service, select its button on the left side of the table and click Delete.

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



Services

Service Definition

Name:

Type: TCP

Start Port:

Finish Port:

Figure 3-10: Add Services menu

4. Click Apply to save your changes.

Setting Times and Scheduling Firewall Services

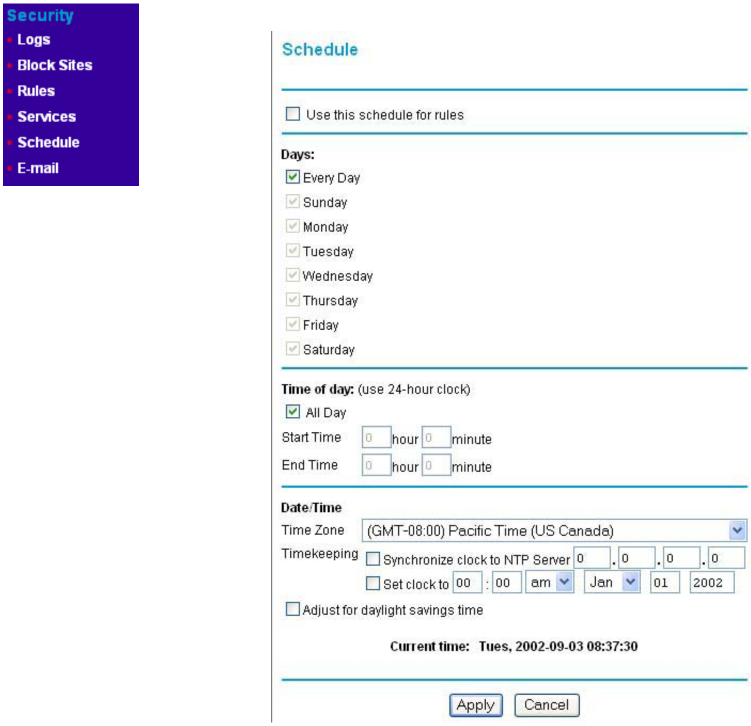
The FVL328 Firewall uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet. In order to localize the time for your log entries, you must select your Time Zone from the list.

Procedure 3-4: 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:

☑ Every Day

☑ Sunday

☑ Monday

☑ Tuesday

☑ Wednesday

☑ Thursday

☑ Friday

☑ Saturday

Time of day: (use 24-hour clock)

☑ All Day

Start Time 0 hour 0 minute

End Time 0 hour 0 minute

Date/Time

Time Zone (GMT-08:00) Pacific Time (US Canada)

Timekeeping □ Synchronize clock to NTP Server 0 . 0 . 0 . 0

□ Set clock to 00 : 00 am Jan 01 2002

□ Adjust for daylight savings time

Current time: Tues, 2002-09-03 08:37:30

Figure 3-11: 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. **Timekeeping** has 2 options:

   - Synchronize to NTP Server - If enabled, the RTC (Real-Time Clock) is updated regularly by contacting this server. If you prefer to use a particular NTP server, enter the server's IP address. If not enabled, the RTC is never changed.

- Set Clock - Use this to set a particular Date/Time to the RTC . This is only useful if “Synchronize to NTP Server” is disabled. Otherwise, your setting will be lost on the next synchronization.

5. Click Apply to save your settings.

Procedure 3-5: 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 is not 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 to display menu shown above in the Schedule Services menu.
3. To block Internet services based on a schedule, select Every Day or select one or more days. If you want to limit access completely for the selected days, select All Day. Otherwise, to limit access during certain times for the selected days, enter Start Blocking and End Blocking times.

   Note: Enter the values as 24-hour time. For example, 10:30 am would be 10 hours and 30 minutes and 10:30 pm would be 22 hours and 30 minutes.
4. Click Apply to save your changes.

Chapter 4
Virtual Private Networking

This chapter describes how to use the virtual private networking (VPN) features of the FVL328 Firewall. VPN tunnels provide secure, encrypted communications between your local network and a remote network or computer.

Overview of FVL328 Policy-Based VPN Configuration

The FVL328 uses state-of-the-art firewall and security technology to facilitate controlled and actively monitored VPN connectivity. Since the FVL328 strictly conforms to IETF standards, it is interoperable with devices from major network equipment vendors.

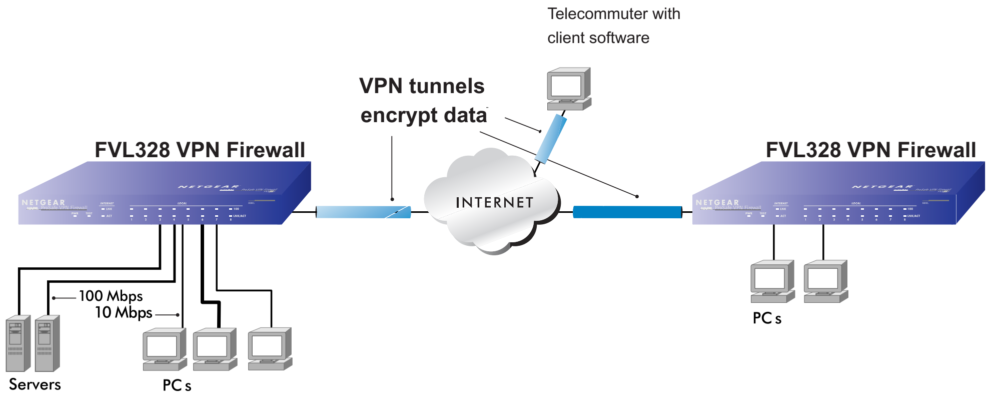


Figure 4-1: Secure access through FVL328 VPN routers

Using Policies to Manage VPN Traffic

You create policy definitions to manage VPN traffic on the FVL328. There are two kinds of policies:

- **IKE Policies**: Define the authentication scheme and automatically generate the encryption keys. As an alternative option, to further automate the process, you can create an IKE policy which uses a trusted certificate authority to provide the authentication while the IKE policy still handles the encryption.
- **VPN Policies**: Apply the IKE policy to specific traffic which requires a VPN tunnel. Or, you can create a VPN policy which does not use an IKE policy but in which you manually enter all the authentication and key parameters.

Since the VPN policies use the IKE policies, you define the IKE policy first. The FVL328 also allows you to manually input the authentication scheme and encryption key values. In the case of manual key management there will not be any IKE policies.

In order to establish secure communication over the Internet with the remote site you need to configure matching VPN policies on both the local and remote FVL328 Firewalls. The outbound VPN policy on one end must match to the inbound VPN policy on other end, and vice versa.

When the network traffic enters into the FVL328 from the LAN network interface, if there is no VPN policy found for a type of network traffic, then that traffic passes through without any change. However, if the traffic is selected by a VPN policy, then the IPSec authentication and encryption rules will be applied to it as defined in the VPN policy.

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

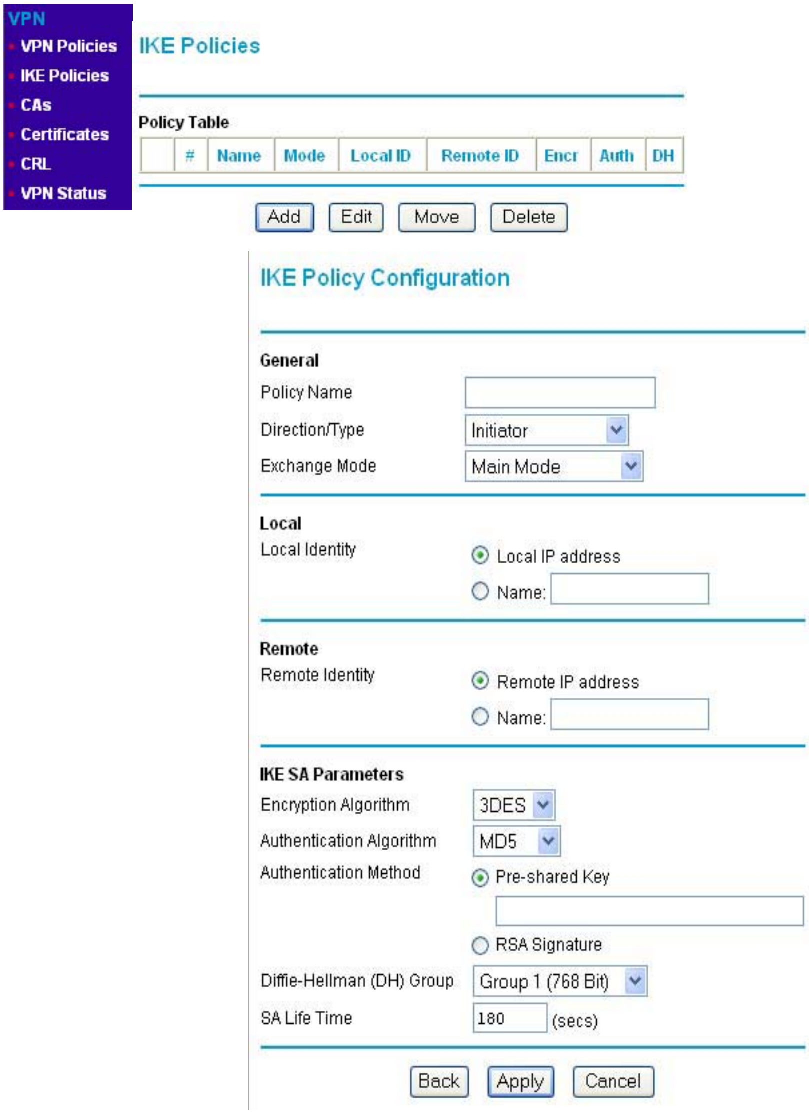
Using Automatic Key Management

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

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

IKE Policies' Automatic Key and Authentication Management

Click the IKE Policies link from the VPN section of the main menu, and then click the Add button of the IKE Policies screen to display the IKE Policy Configuration menu shown in Figure 4-2.



IKE Policies

Policy Table

	#	Name	Mode	Local ID	Remote ID	Encr	Auth	DH

IKE Policy Configuration

General

Policy Name

Direction/Type: Initiator

Exchange Mode: Main Mode

Local

Local Identity: ● Local IP address ○ Name:

Remote

Remote Identity: ● Remote IP address ○ Name:

IKE SA Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: MD5

Authentication Method: ● Pre-shared Key ○ RSA Signature

Diffie-Hellman (DH) Group: Group 1 (768 Bit)

SA Life Time: 180 (secs)

Figure 4-2: IKE - Policy Configuration Menu

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

Table 4-1. IKE Policy Configuration Fields

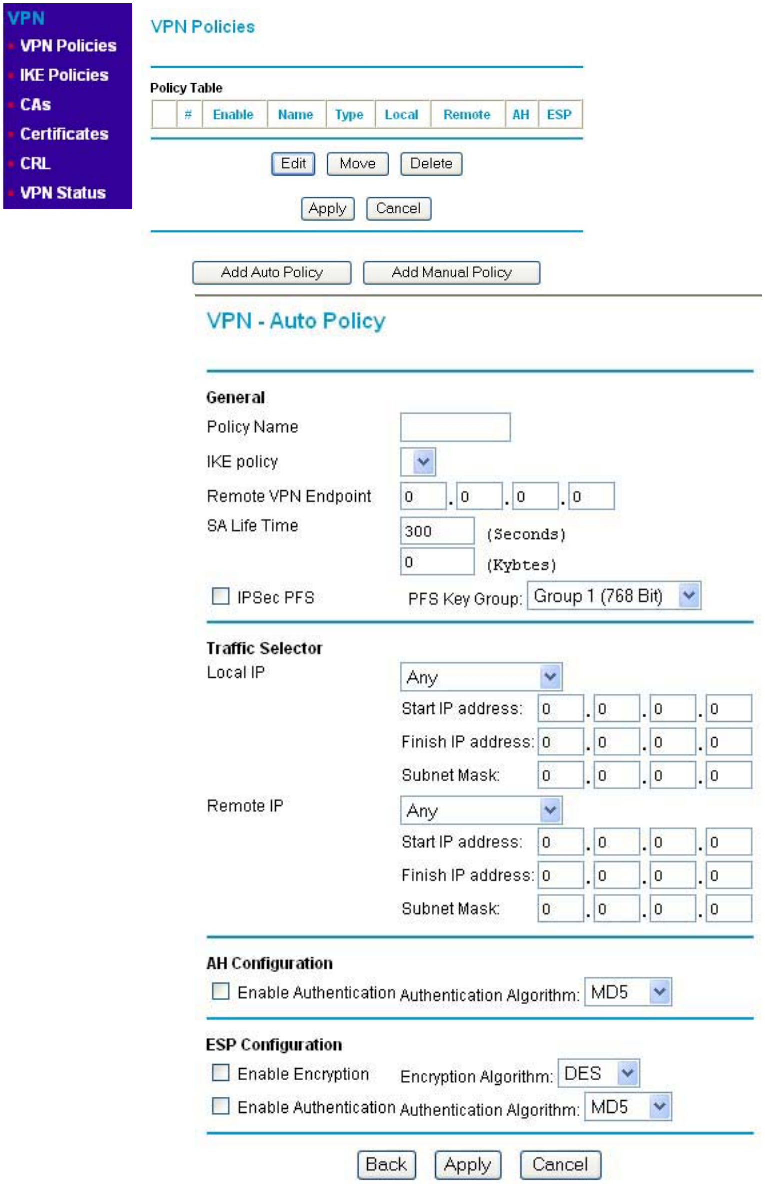
Field	Description
General	These settings identify this policy and determine its major characteristics.
Policy Name	The descriptive name of the IKE policy. Each policy should have a unique policy name. This name is not supplied to the remote VPN endpoint. It is only used to help you identify IKE policies.
Direction/Type	This setting is used when determining if the IKE policy matches the current traffic. The drop-down menu includes the following: • Initiator – Outgoing connections are allowed, but incoming are blocked. • Responder – Incoming connections are allowed, but outgoing are blocked. • Both Directions – Both outgoing and incoming connections are allowed. • Remote Access – This is to allow only incoming client connections, where the IP address of the remote client is unknown. If Remote Access is selected, the "Exchange Mode" MUST be "Aggressive," and the 'Identities' below (both Local and Remote) MUST be "Name." On the matching VPN Policy, the IP address of the remote VPN endpoint should be set to 0.0.0.0.
Exchange Mode	Main Mode or Aggressive Mode. This setting must match the setting used on the remote VPN endpoint. • Main Mode is slower but more secure. Also, the "Identity" below must be established by IP address. • Aggressive Mode is faster but less secure. The "Identity" below can be by name (host name, domain name, email address, etc.) instead of by IP address.
Local Local Identity	These parameters apply to the Local FVL328 firewall.
Local IP Address	Use this field to identify the local FVL328 by its Internet (WAN) port IP address.
Name	This field lets you identify the local FVL328 by name.

Table 4-1. IKE Policy Configuration Fields

Field	Description
Remote Remote Identity	These parameters apply to the target remote FVL328 firewall.
Remote IP Address	Use this field to identify the remote FVL328 by its Internet (WAN) port IP address.
Name	This field lets you identify the target remote FVL328 by name.
IKE Security Association (SA) Parameters	These parameters determine the properties of the IKE Security Association.
Encryption Algorithm	Choose the encryption algorithm for this IKE policy: • DES is the default • 3DES is more secure
Authentication Algorithm	If you enable Authentication Header (AH), this menu lets you to select from these authentication algorithms: • MD5 - the default • SHA-1 - more secure
Authentication Method	You may select Pre-Shared Key or RSA Signature.
Pre-Shared Key	Specify the key according to the requirements of the Authentication Algorithm you selected. • For MD5, the key length should be 16 bytes. • For SHA-1, the key length should be 20 bytes.
RSA Signature	RSA Signature requires a certificate.
Diffie-Hellman (D-H) Group	The DH Group setting determines the bit size used in the key exchange. This must match the value used on the remote gateway.
SA Life Time	The amount of time in seconds before the Security Association expires; over an hour (3600) is common.

VPN Policy Configuration for Auto Key Negotiation

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



VPN Policies

Policy Table

	#	Enable	Name	Type	Local	Remote	AH	ESP

VPN - Auto Policy

General

Policy Name

IKE policy

Remote VPN Endpoint 0 . 0 . 0 . 0

SA Life Time 300 (Seconds)

0 (Kybtes)

□ IPSec PFS PFS Key Group: Group 1 (768 Bit)

Traffic Selector

Local IP Any

Start IP address: 0 . 0 . 0 . 0

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Remote IP Any

Start IP address: 0 . 0 . 0 . 0

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

AH Configuration

□ Enable Authentication Authentication Algorithm: MD5

ESP Configuration

□ Enable Encryption Encryption Algorithm: DES

□ Enable Authentication Authentication Algorithm: MD5

Figure 4-3: VPN - Auto Policy Menu

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

Table 4-1. VPN Auto Policy Configuration Fields

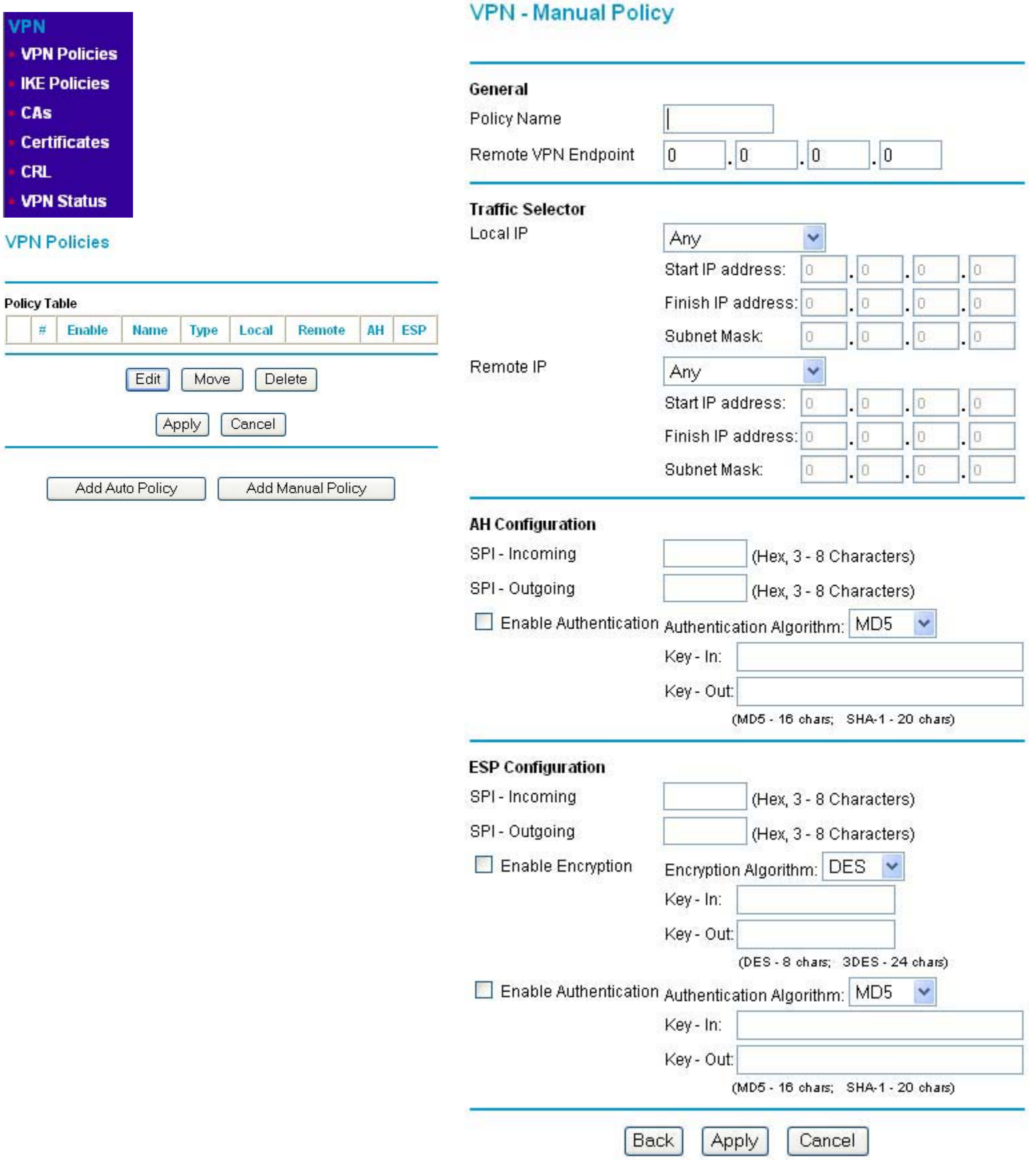
Field	Description
General	These settings identify this policy and determine its major characteristics.
Policy Name	The descriptive name of the VPN policy. Each policy should have a unique policy name. This name is not supplied to the remote VPN endpoint. It is only used to help you identify VPN policies.
IKE Policy	The existing IKE policies are presented in a drop-down list. **Note:** Create the IKE policy BEFORE creating a VPN - Auto policy.
Remote VPN Endpoint	The WAN Internet IP address of the remote VPN firewall or client to which you wish to connect. The remote VPN endpoint must have this FVL328's WAN Internet IP address entered as its "Remote VPN Endpoint."
SA Life Time	The duration of the Security Association before it expires. • Seconds - the amount of time before the SA expires. Over an hour is common (3600). • Kbytes - the amount of traffic before the SA expires. One of these can be set without setting the other.
IPSec PFS	If enabled, security is enhanced by ensuring that the key is changed at regular intervals. Also, even if one key is broken, subsequent keys are no easier to break. Each key has no relationship to the previous key.
PFS Key Group	If PFS is enabled, this setting determines the DH group bit size used in the key exchange. This must match the value used on the remote gateway.
Traffic Selector	These settings determine if and when a VPN tunnel will be established. If network traffic meets *all* criteria, then a VPN tunnel will be created.
Local IP	The drop-down menu allows you to configure the source IP address of the outbound network traffic for which this VPN policy will provide security. Usually, this address will be from your network address space. The choices are: • ANY for all valid IP addresses in the Internet address space • Single IP Address • Range of IP Addresses • Subnet Address

Table 4-1. VPN Auto Policy Configuration Fields

Field	Description
Remote IP	The drop-down menu allows you to configure the destination IP address of the outbound network traffic for which this VPN policy will provide security. Usually, this address will be from the remote site's corporate network address space. The choices are: • ANY for all valid IP addresses in the Internet address space • Single IP Address • Range of IP Addresses • Subnet Address
Authenticating Header (AH) Configuration	AH specifies the authentication protocol for the VPN header. These settings must match the remote VPN endpoint.
Enable Authentication	Use this checkbox to enable or disable AH for this VPN policy.
Authentication Algorithm	If you enable AH, then select the authentication algorithm: • MD5 - the default • SHA1 - more secure
Encapsulated Security Payload (ESP) Configuration	ESP provides security for the payload (data) sent through the VPN tunnel. Generally, you will want to enable both Encryption and Authentication. Two ESP modes are available: • Plain ESP encryption • ESP encryption with authentication These settings must match the remote VPN endpoint.
Enable Encryption	Use this checkbox to enable or disable ESP Encryption.
Encryption Algorithm	If you enable ESP encryption, then select the encryption algorithm: • DES - the default • 3DES - more secure
Enable Authentication	Use this checkbox to enable or disable ESP transform for this VPN policy. You can select the ESP mode also with this menu. Two ESP modes are available: • Plain ESP • ESP with authentication
Authentication Algorithm	If you enable AH, then use this menu to select which authentication algorithm will be employed. The choices are: • MD5 - the default • SHA1 - more secure

VPN Policy Configuration for Manual Key Exchange

With Manual Key Management, you will not use an IKE policy. You must manually type in all the required key information. Click the VPN Policies link from the VPN section of the main menu to display the menu shown in Figure 4-4.



Policy Table

	#	Enable	Name	Type	Local	Remote	AH	ESP

General

Policy Name

Remote VPN Endpoint 0 . 0 . 0 . 0

Traffic Selector

Local IP: Any
Start IP address: 0 . 0 . 0 . 0
Finish IP address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0

Remote IP: Any
Start IP address: 0 . 0 . 0 . 0
Finish IP address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0

AH Configuration

SPI - Incoming (Hex, 3 - 8 Characters)
SPI - Outgoing (Hex, 3 - 8 Characters)
□ Enable Authentication Authentication Algorithm: MD5
Key - In:
Key - Out:
(MD5 - 16 chars; SHA-1 - 20 chars)

ESP Configuration

SPI - Incoming (Hex, 3 - 8 Characters)
SPI - Outgoing (Hex, 3 - 8 Characters)
□ Enable Encryption Encryption Algorithm: DES
Key - In:
Key - Out:
(DES - 8 chars; 3DES - 24 chars)
□ Enable Authentication Authentication Algorithm: MD5
Key - In:
Key - Out:
(MD5 - 16 chars; SHA-1 - 20 chars)

Figure 4-4: VPN - Manual Policy Menu

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

Table 4-1. VPN Manual Policy Configuration Fields

Field	Description
General	These settings identify this policy and determine its major characteristics.
Policy Name	The name of the VPN policy. Each policy should have a unique policy name. This name is not supplied to the remote VPN Endpoint. It is used to help you identify VPN policies.
Remote VPN Endpoint	The WAN Internet IP address of the remote VPN firewall or client to which you wish to connect. The remote VPN endpoint must have this FVL328's WAN Internet IP address entered as its "Remote VPN Endpoint."
Traffic Selector	These settings determine if and when a VPN tunnel will be established. If network traffic meets *all* criteria, then a VPN tunnel will be created.
Local IP	The drop down menu allows you to configure the source IP address of the outbound network traffic for which this VPN policy will provide security. Usually, this address will be from your network address space. The choices are: • ANY for all valid IP addresses in the Internet address space • Single IP Address • Range of IP Addresses • Subnet Address
Remote IP	The drop down menu allows you to configure the destination IP address of the outbound network traffic for which this VPN policy will provide security. Usually, this address will be from the remote site's corporate network address space. The choices are: • ANY for all valid IP addresses in the Internet address space • Single IP Address • Range of IP Addresses • Subnet Address

Table 4-1. VPN Manual Policy Configuration Fields

Field	Description
Authenticating Header (AH) Configuration	AH specifies the authentication protocol for the VPN header. These settings must match the remote VPN endpoint. **Note:** The "Incoming" settings here must match the "Outgoing" settings on the remote VPN endpoint, and the "Outgoing" settings here must match the "Incoming" settings on the remote VPN endpoint.
SPI - Incoming	Enter a Hex value (3 - 8 chars). Any value is acceptable, provided the remote VPN endpoint has the same value in its "Outgoing SPI" field.
SPI - Outgoing	Enter a Hex value (3 - 8 chars). Any value is acceptable, provided the remote VPN endpoint has the same value in its "Incoming SPI" field.
Enable Authentication	Use this checkbox to enable or disable AH. Authentication is often not used. In this case, leave the checkbox unchecked.
Authentication Algorithm	If you enable AH, then select the authentication algorithm: • MD5 - the default • SHA1 - more secure Enter the keys in the fields provided. For MD5, the keys should be 16 characters. For SHA-1, the keys should be 20 characters.
Key - In	Enter the keys. • For MD5, the keys should be 16 characters. • For SHA-1, the keys should be 20 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Authentication Algorithm "Key - Out" field.
Key - Out	Enter the keys in the fields provided. • For MD5, the keys should be 16 characters. • For SHA-1, the keys should be 20 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Authentication Algorithm "Key - In" field.
Encapsulated Security Payload (ESP) Configuration	ESP provides security for the payload (data) sent through the VPN tunnel. Generally, you will want to enable both encryption and authentication. when you use ESP. Two ESP modes are available: • Plain ESP encryption • ESP encryption with authentication These settings must match the remote VPN endpoint.

Table 4-1. VPN Manual Policy Configuration Fields

Field	Description
SPI - Incoming	Enter a Hex value (3 - 8 chars). Any value is acceptable, provided the remote VPN endpoint has the same value in its "Outgoing SPI" field.
SPI - Outgoing	Enter a Hex value (3 - 8 chars). Any value is acceptable, provided the remote VPN endpoint has the same value in its "Incoming SPI" field.
Enable Encryption	Use this checkbox to enable or disable ESP Encryption.
Encryption Algorithm	If you enable ESP Encryption, then select the Encryption Algorithm: • DES - the default • 3DES -more secure
Key - In	Enter the key in the fields provided. • For DES, the key should be 8 characters. • For 3DES, the key should be 24 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Encryption Algorithm "Key - Out" field.
Key - Out	Enter the key in the fields provided. • For DES, the key should be 8 characters. • For 3DES, the key should be 24 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Encryption Algorithm "Key - In" field.
Enable Authentication	Use this checkbox to enable or disable ESP authentication for this VPN policy.
Authentication Algorithm	If you enable authentication, then use this menu to select the algorithm: • MD5 - the default • SHA1 - more secure
Key - In	Enter the key. • For MD5, the key should be 16 characters. • For SHA-1, the key should be 20 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Authentication Algorithm "Key - Out" field.
Key - Out	Enter the key in the fields provided. • For MD5, the key should be 16 characters. • For SHA-1, the key should be 20 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Authentication Algorithm "Key - In" field.

Using Digital Certificates for IKE Auto-Policy Authentication

Digital certificates are strings generated using encryption and authentication schemes which cannot be duplicated by anyone without access to the different values used in the production of the string. They are issued by Certification Authorities (CAs) to authenticate a person or a workstation uniquely. The CAs are authorized to issue these certificates by Policy Certification Authorities (PCAs), who are in turn certified by the Internet Policy Registration Authority (IPRA). The FVL328 is able to use certificates to authenticate users at the end points during the IKE key exchange process.

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

Each CA has its own certificate. The certificates of a CA are added to the FVL328 and can then be used to form IKE policies for the user. Once a CA certificate is added to the FVL328 and a certificate is created for a user, the corresponding IKE policy is added to the FVL328. Whenever the user tries to send traffic through the FVL328, the certificates are used in place of pre-shared keys during initial key exchange as the authentication and key generation mechanism. Once the keys are established and the tunnel is set up the connection proceeds according to the VPN policy.

Certificate Revocation List (CRL)

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

Whenever an IKE policy receives the certificate from a peer, it checks for this certificate in the CRL on the FVL328 obtained from the corresponding CA. If the certificate is not present in the CRL it means that the certificate is not revoked. IKE can then use this certificate for authentication. If the certificate is present in the CRL it means that the certificate is revoked, and the IKE will not authenticate the client.

You must manually update the FVL328 CRL regularly in order for the CA-based authentication process to remain valid.

Walk-Through of Configuration Scenarios on the FVL328

There are a variety of configurations you might implement with the FVL328. The scenarios listed below illustrate typical configurations you might use in your organization.

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

- VPN Consortium Scenarios without Any Product Implementation Details
- VPN Consortium Scenarios Based on the FVL328 User Interface

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

> **Note:** NETGEAR will publish additional interoperability scenarios with various gateway and client software products. Look on the NETGEAR web site at www.netgear.com for the HTML version of this manual. The scenarios will be published as an additional section of the on-line version of this reference manual.

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

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

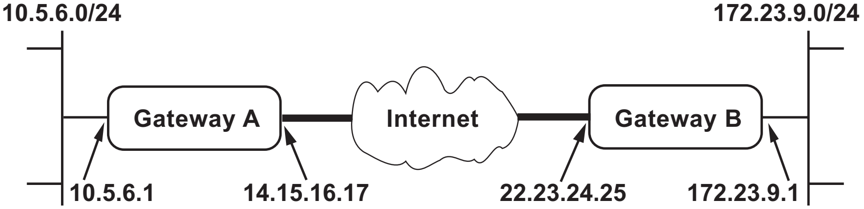


Figure 4-5: VPN Consortium Scenario 1

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

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

The IKE Phase 1 parameters used in Scenario 1 are:

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

The IKE Phase 2 parameters used in Scenario 1 are:

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

FVL328 Scenario 1: FVL328 to Gateway B with IKE and VPN Policies

Note: This scenario assumes all ports are open on the FVL328. You can verify this by reviewing the security settings as seen in the "Rules menu" on page 3-6.

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

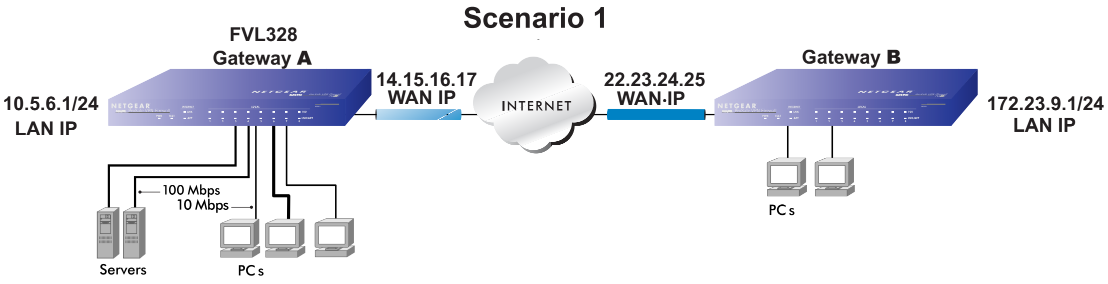


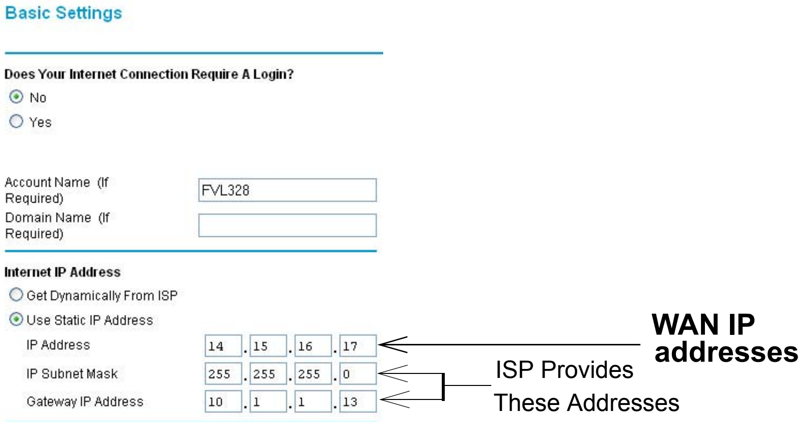
Figure 4-6: LAN to LAN VPN access from an FVL328 to an FVL328

1. Log in to the FVL328 labeled Gateway A as in the illustration.

   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.

2. Configure the WAN (Internet) and LAN IP addresses of the FVL328.

   a. From the main menu Setup section, click on the Basic Setup link.



Basic Settings

Does Your Internet Connection Require A Login?

● No

○ Yes

Account Name (If Required)	FVL328
Domain Name (If Required)	

Internet IP Address

○ Get Dynamically From ISP

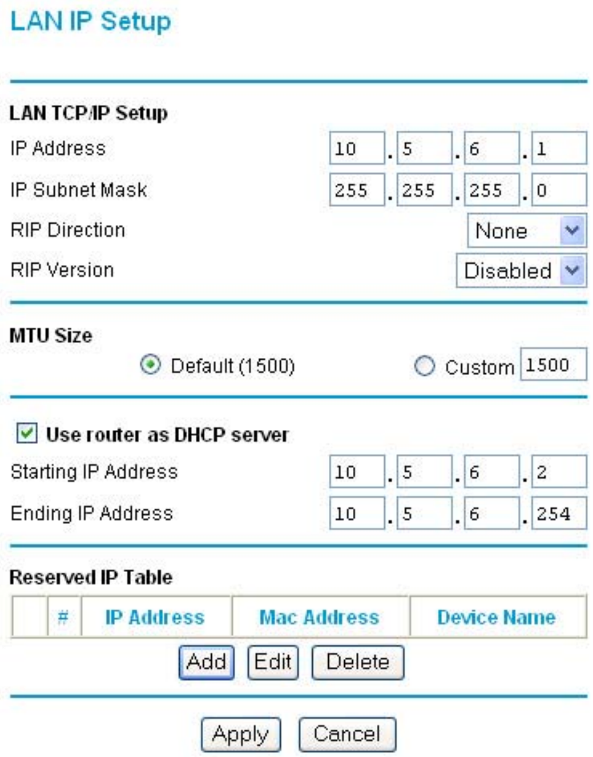
● Use Static IP Address

IP Address	14 . 15 . 16 . 17
IP Subnet Mask	255 . 255 . 255 . 0
Gateway IP Address	10 . 1 . 1 . 13

Figure 4-7: FVL328 Internet IP Address menu

b. Configure the WAN Internet Address according to the settings in Figure 4-6 above and click Apply to save your settings. For more information on configuring the WAN IP settings in the Basic Setup topics, please see "Manual Configuration" on page 2-16.

c. From the main menu Advanced section, click on the LAN IP Setup link.



LAN IP Setup

LAN TCP/IP Setup

IP Address 10 . 5 . 6 . 1

IP Subnet Mask 255 . 255 . 255 . 0

RIP Direction None

RIP Version Disabled

MTU Size

● Default (1500) ○ Custom 1500

☑ Use router as DHCP server

Starting IP Address 10 . 5 . 6 . 2

Ending IP Address 10 . 5 . 6 . 254

Reserved IP Table

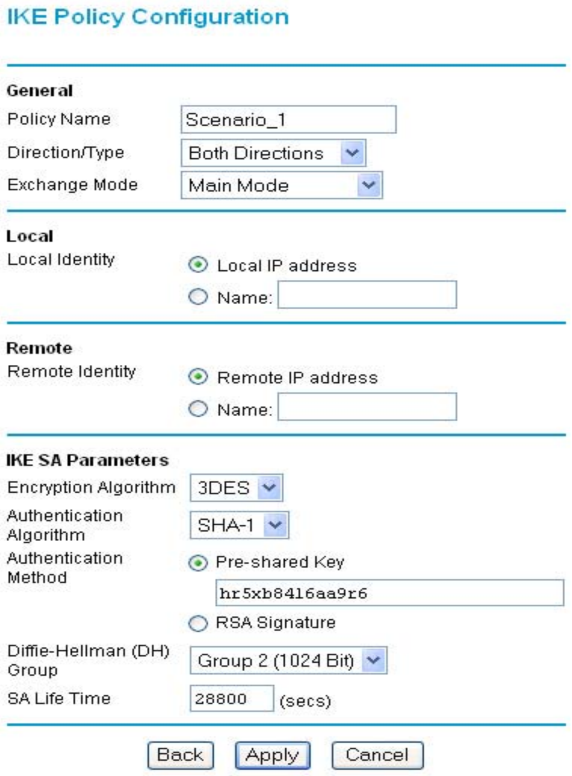
	#	IP Address	Mac Address	Device Name

d. Configure the LAN IP address according to the settings in Figure 4-6 above and click Apply to save your settings. For more information on LAN TCP/IP setup topics, please see "Configuring LAN TCP/IP Setup" on page 6-5.

Note: After you click Apply to change the LAN IP address settings, your workstation will be disconnected from the FVL328. You will have to log on with *http://10.5.6.1* which is now the address you use to connect to the built-in web-based configuration manager of the FVL328.

3. **Set up the IKE Policy illustrated below on the FVL328.**

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



IKE Policy Configuration

General

Policy Name: Scenario_1

Direction/Type: Both Directions

Exchange Mode: Main Mode

Local

Local Identity: ● Local IP address ○ Name:

Remote

Remote Identity: ● Remote IP address ○ Name:

IKE SA Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

Authentication Method: ● Pre-shared Key hr5xb84l6aa9r6 ○ RSA Signature

Diffie-Hellman (DH) Group: Group 2 (1024 Bit)

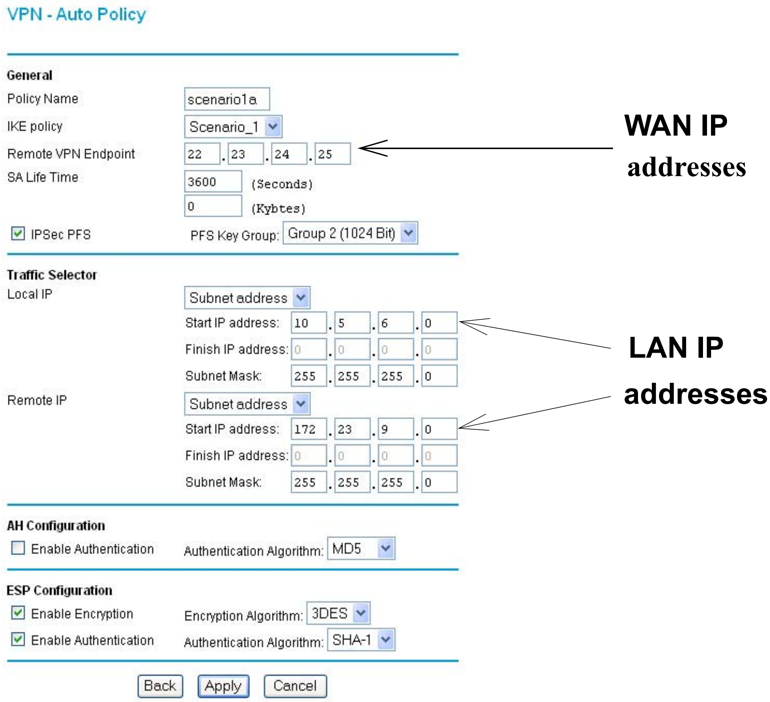
SA Life Time: 28800 (secs)

Figure 4-8: Scenario 1 IKE Policy

   b. Configure the IKE Policy according to the settings in the illustration above and click Apply to save your settings. For more information on IKE Policy topics, please see "IKE Policies' Automatic Key and Authentication Management" on page 4-3.

4. Set up the FVL328 VPN -Auto Policy illustrated below.

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



VPN - Auto Policy

General

Policy Name: scenario1a

IKE policy: Scenario_1

Remote VPN Endpoint: 22 . 23 . 24 . 25

SA Life Time: 3600 (Seconds)

0 (Kybtes)

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

Traffic Selector

Local IP: Subnet address

Start IP address: 10 . 5 . 6 . 0

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Remote IP: Subnet address

Start IP address: 172 . 23 . 9 . 0

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

AH Configuration

☐ Enable Authentication — Authentication Algorithm: MD5

ESP Configuration

☑ Enable Encryption — Encryption Algorithm: 3DES

☑ Enable Authentication — Authentication Algorithm: SHA-1

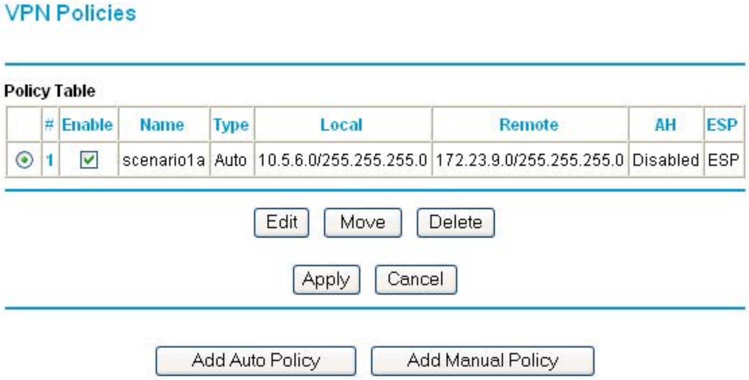
WAN IP addresses

LAN IP addresses

Figure 4-9: Scenario 1 VPN - Auto Policy

   b. Configure the IKE Policy according to the settings in the illustration above and click Apply to save your settings. For more information on IKE Policy topics, please see "IKE Policies' Automatic Key and Authentication Management" on page 4-3.

5. After applying these changes, you will see a table entry like the one below.



VPN Policies

Policy Table

	#	Enable	Name	Type	Local	Remote	AH	ESP
●	1	☑	scenario1a	Auto	10.5.6.0/255.255.255.0	172.23.9.0/255.255.255.0	Disabled	ESP

Figure 4-10: VPN Policies table

Now all traffic from the range of LAN IP addresses specified on FVL328 A and FVL328 B will flow over a secure VPN tunnel.

Procedure 4-1: Checking VPN Connections

You can test connectivity and view VPN status information on the FVL328.

1. To test connectivity between the Gateway A FVL328 LAN and the Gateway B LAN, follow these steps:
   a. Using our example, from a PC attached to the FVL328 on LAN A, on a Windows PC click the Start button on the taskbar and then click Run.
   b. Type **`ping -t 172.23.9.1`**, and then click OK.
   c. This will cause a continuous ping to be sent to the LAN interface of Gateway B. After between several seconds and two minutes, the ping response should change from “timed out” to “reply.”
   d. At this point the connection is established.

2. To test connectivity between the FVL328 Gateway A and Gateway B WAN ports, follow these steps:

   a. Using our example, log in to the FVL328 on LAN A, go to the main menu Maintenance section and click the Diagnostics link.

   b. To test connectivity to the WAN port of Gateway B, enter **`22.23.24.25`**, and then click Ping.

   c. This will cause a ping to be sent to the WAN interface of Gateway B. After between several seconds and two minutes, the ping response should change from “timed out” to “reply.” You may have to run this test several times before you get the “reply” message back from the target FVL328.

   d. At this point the connection is established.

   Note: If you want to ping the FVL328 as a test of network connectivity, be sure the FVL328 is configured to respond to a ping on the Internet WAN port by checking the checkbox seen in “Rules menu” on page 3-6. However, to preserve a high degree of security, you should turn off this feature when you are finished with testing.

3. To view the FVL328 event log and status of Security Associations, follow these steps:

   a. Go to the FVL328 main menu VPN section and click the VPN Status link.

   b. The log screen will display a history of the VPN connections, and the IPSec SA and IKE SA tables will report the status and data transmission statistics of the VPN tunnels for each policy.

VPN Consortium Scenario 2: Gateway-to-Gateway with Certificates

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

The sequence of steps for using the PKIX certificates include:

1. Generating a new public/private key pair.
2. Creating a certificate request for this gateway; including the fields which must or must not be included in the certificate.
3. Transmitting that request to a Trusted Root CA.
4. Receiving the certificate back from the Trusted Root CA.
5. Installing the new user certificate.
6. Installing the trusted CA certificate for the Trusted Root CA.
7. Associating the new end entity certificate and the Trusted Root CA certificate with the SA for Gateway B.
8. Setting up CRL checking.

FVL328 Scenario 2: FVL328 to FVL328 with RSA Certificates

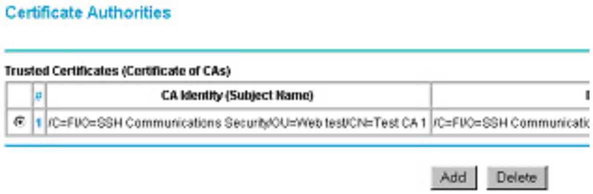
Note: Before completing this configuration scenario, make sure the correct Time Zone is set on the FVL328. For instructions on this topic, please see, "Setting Your Time Zone" on page 3-14.

1. Generate a new public/private key pair.
   a. Obtain a certificate from a Certificate Authority (CA)

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

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

2. Install the trusted CA certificate for the Trusted Root CA.
   a. Log in to the FVL328, and upload the *trust.txt* certificate file.
   b. From the main menu VPN section, click on the CA link.
   c. Click Add to add a CA.
   d. Click Browse to locate the *trust.txt* file.
   e. Click Upload.



Certificate Authorities

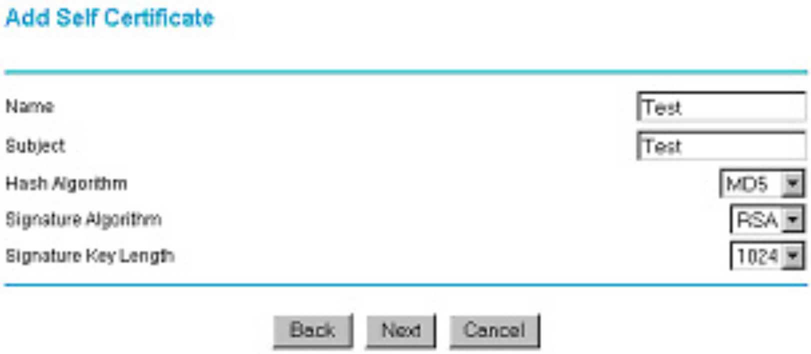
Trusted Certificates (Certificate of CAs)

	#	CA Identity (Subject Name)	I
●	1	/C=FI/O=SSH Communications Security/OU=Web test/CN=Test CA 1	/C=FI/O=SSH Communicatio

Figure 4-11: VPN Policies table

You will now see a screen such as the one above showing that the Certificate Authority is now registered with the FVL328.

3. Create a certificate request for the FVL328.
   a. From the main menu VPN section, click on the Certificates link and click Add.
   b. Fill in the requested fields on the Add Self Certificate screen.

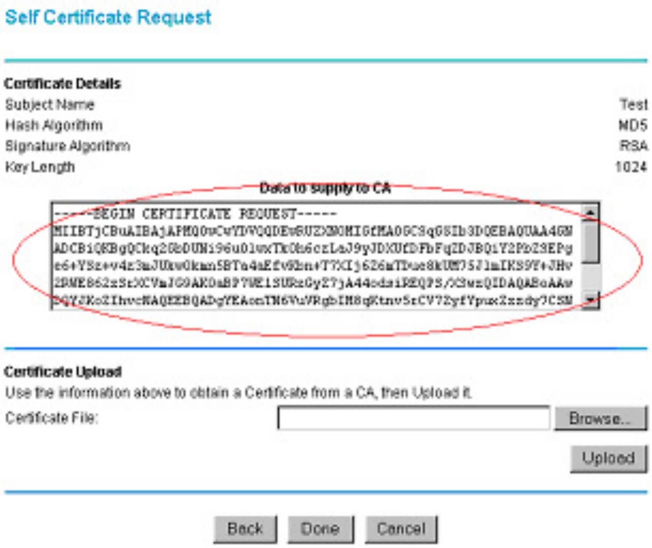


Add Self Certificate

Name	Test
Subject	Test
Hash Algorithm	MD5
Signature Algorithm	RSA
Signature Key Length	1024

Figure 4-12: Add Self Certificates required fields

c. Click Next to continue. The FVL328 generates a Self Certificate Request as shown below.



Self Certificate Request

Certificate Details

Subject Name	Test
Hash Algorithm	MD5
Signature Algorithm	RSA
Key Length	1024

Data to supply to CA

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBTjCBuAIBAjAPMQ0wCwYDVQQDEwRUZXN0MIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQCkq2GbDUNi96u0lwxTk0h6czLaJ9yJDXUfDFbFqZDJBQiY2PbZ3EPg
e6+YSz+v4z3mJUkw0kmn5BTa4aEfv9bn+T7XIj626mTDue8kUM75J1mIKS9Y+JHv
2RME862zSzXCVmJG9AK0aBP7WE1SURzGyZ7jA44odziREQPS/XCwzQIDAQABoAAw
DQYJKoZIhvcNAQEEBQADgYEAomTN6VuVRgbIM8qKtnv5zCV7ZyfYpuxZzzdy7CSM
```

Certificate Upload

Use the information above to obtain a Certificate from a CA, then Upload it.

Certificate File:

Figure 4-13: Self Certificate Request data

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

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

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

5. Receive the certificate back from the Trusted Root CA.

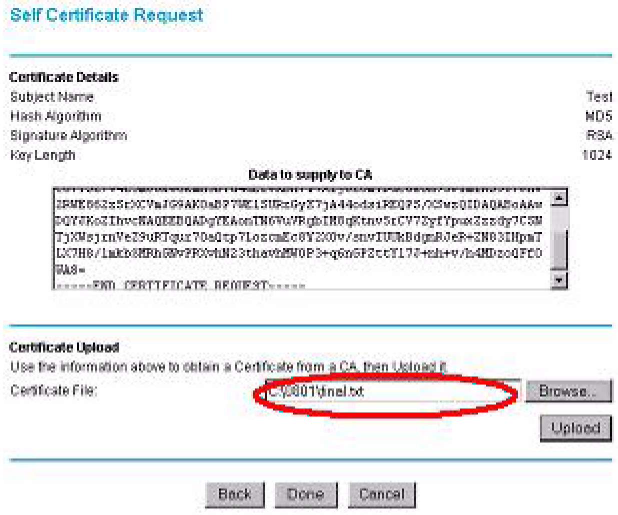
   Note: In the case of a Windows 2000 internal CA, the CA administrator might simply email it to back to you. Follow the procedures of your CA. Save the certificate you get back from the CA as a text file called *final.txt*.

6. Install the new certificate.

   a. From the main menu VPN section, click on the Certificates link and click Add.

   b. If you closed the menu from the previous session, fill in the requested fields on the Add Self Certificate screen exactly as you did earlier.

c. Click Next to continue.



Self Certificate Request

Certificate Details

Subject Name	Test
Hash Algorithm	MD5
Signature Algorithm	RSA
Key Length	1024

Data to supply to CA

```
2RWE862zSrXCVaJG9AKDaB77WE15URzGyZ7jA44odz1REQ75/XSwzQIDAQABoAAw
DQYJKoZIhvcNAQEEBQADgYEAonTN6VuVRgbIN8gKtnv5rCV7ZyfYpwxZzzdy7C5M
TjXMsjrnVe29uRTqur70aQtp7LozcmEc0Y2X0v/snvIUUkBdgmRJeR+ZN03IHpmT
LX7H8/1mkb8MRhGWv9RX+hN23thavhMW0P3+q6nGFZccY17J+mh+v/h4MDzoQFC0
WA8=
-----END CERTIFICATE REQUEST-----
```

Certificate Upload

Use the information above to obtain a Certificate from a CA, then Upload it.

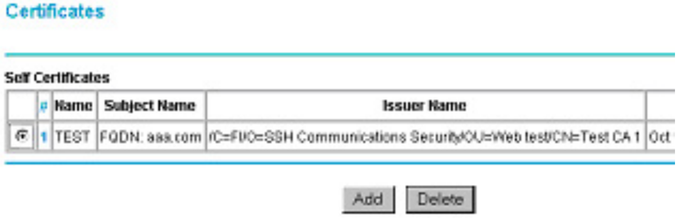
Certificate File: C:\j801\final.txt

Figure 4-14: Certificate Upload

d. Click Browse to locate the *final.txt* file you saved earlier which contains the certificate from the CA.

e. Click Upload.

f. Click Done when the upload is complete. You will now see this entry in the Self Certificates table as illustrated below.



Certificates

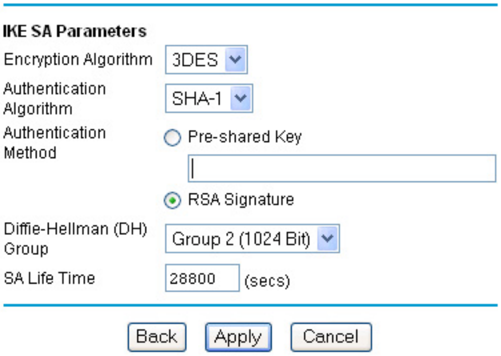
Self Certificates

	#	Name	Subject Name	Issuer Name	
◉	1	TEST	FQDN: aaa.com	/C=FI/O=SSH Communications Security/OU=Web test/CN=Test CA 1	Oct

Figure 4-15: Self Certificates table

7. Associate the new certificate and the Trusted Root CA certificate on the FVL328.

a. Create a new IKE policy called **Scenario_2** with all the same properties of **Scenario_1** (see "Scenario 1 IKE Policy" on page 4-18) except now use the RSA Signature instead of the shared key.



IKE SA Parameters

Encryption Algorithm	3DES
Authentication Algorithm	SHA-1
Authentication Method	○ Pre-shared Key ● RSA Signature
Diffie-Hellman (DH) Group	Group 2 (1024 Bit)
SA Life Time	28800 (secs)

Figure 4-16: IKE policy using RSA Signature

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

Now, the traffic from devices within the range of the LAN subnet addresses on FVL328 A and Gateway B will be authenticated using the certificates rather than via a shared key.

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

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

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

b. From the main menu VPN section, click on the CRL link.

c. Click Add to add a CRL.

d. Click Browse to locate the CRL file.

e. Click Upload.

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

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

Chapter 5
Managing Your Network

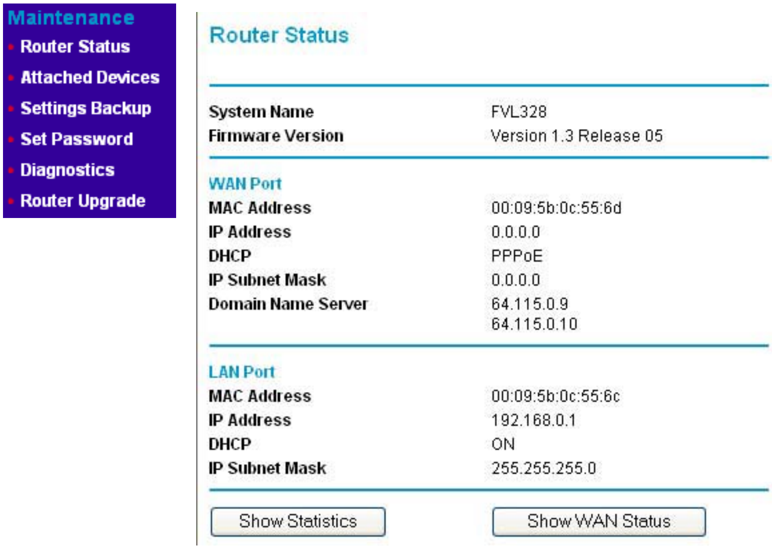
This chapter describes how to perform network management tasks with your FVL328 Prosafe High Speed VPN Firewall.

Network Management Information

The FVL328 provides a variety of status and usage information which is discussed below.

Viewing Router Status and Usage Statistics

From the Main Menu, under Maintenance, select Router Status to view the screen in Figure 5-1.



Router Status

System Name	FVL328
Firmware Version	Version 1.3 Release 05
WAN Port	
MAC Address	00:09:5b:0c:55:6d
IP Address	0.0.0.0
DHCP	PPPoE
IP Subnet Mask	0.0.0.0
Domain Name Server	64.115.0.9 64.115.0.10
LAN Port	
MAC Address	00:09:5b:0c:55:6c
IP Address	192.168.0.1
DHCP	ON
IP Subnet Mask	255.255.255.0

Figure 5-1: Router Status screen

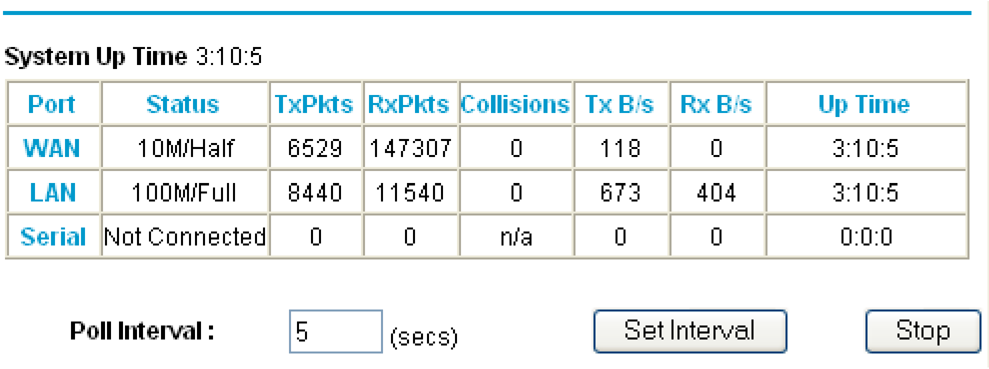
The Router Status menu provides a limited amount of status and usage information. From the Main Menu of the browser interface, under Maintenance, select Router Status to view the status screen, shown in Figure 5-1.

This screen shows the following parameters:

Table 5-1. 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 Servers (DNS)	This field displays the DNS Server IP addresses being used by the firewall. These addresses are usually obtained dynamically from the ISP.
LAN Port	These parameters apply to the Local (WAN) port of the firewall.
MAC Address	This field displays the Ethernet MAC address being used by the Local (LAN) port of the firewall.
IP Address	This field displays the IP address being used by the Local (LAN) port of the firewall. The default is 192.168.0.1
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 5-2 below:



System Up Time 3:10:5

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

Poll Interval : 5 (secs)

Figure 5-2. Router Statistics screen

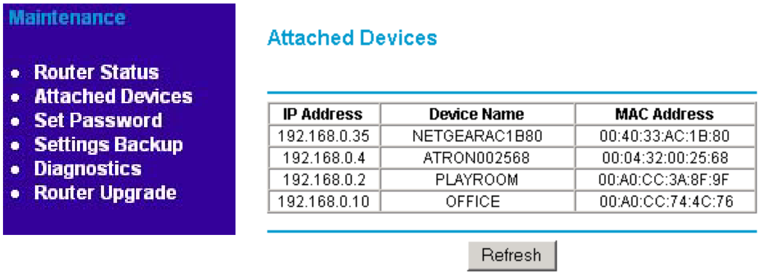
This screen shows the following statistics:

Table 5-2. Router Statistics Fields

Field	Description
System up Time	The time elapsed since the last power cycle or reset.
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.
Rx B/s	The average line utilization —average CLU for this port.
Up Time	The time elapsed since this port acquired the link.
Poll Interval	Specifies the intervals at which the statistics are updated in this window. Click on Stop to freeze the display. Click on Set Interval to set the polling refresh interval.

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 5-3



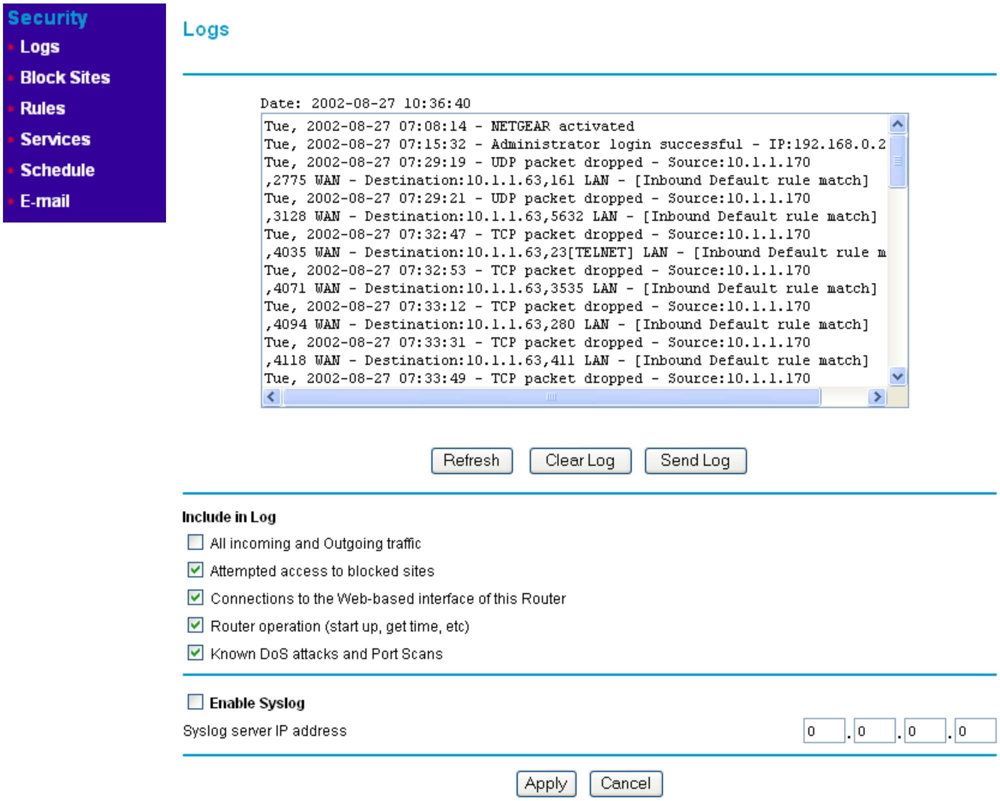
IP Address	Device Name	MAC Address
192.168.0.35	NETGEARAC1B80	00:40:33:AC:1B:80
192.168.0.4	ATRON002568	00:04:32:00:25:68
192.168.0.2	PLAYROOM	00:A0:CC:3A:8F:9F
192.168.0.10	OFFICE	00:A0:CC:74:4C:76

Figure 5-3: Attached Devices menu

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

Viewing, Selecting, and Saving Logged Information

The firewall will log security-related events such as denied incoming service requests, hacker probes, and administrator logins. If you enabled content filtering in the Block Sites menu, the Logs page shows you when someone on your network tried to access a blocked site. If you enabled e-mail notification, you'll receive these logs in an e-mail message. If you don't have e-mail notification enabled, you can view the logs here. An example is shown below.



Logs

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

Include in Log

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

□ **Enable Syslog**

Syslog server IP address 0 . 0 . 0 . 0

Figure 5-4: Security Logs menu

Log entries are described below:

Table 5-5: 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 below:

Table 5-6: 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 e-mail the log immediately.
Apply	Click this button to apply any changed settings.
Cancel	Click this button to clear any changed settings.

Changing the Include in Log Settings

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 the Syslog Feature

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

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 e-mailed.]

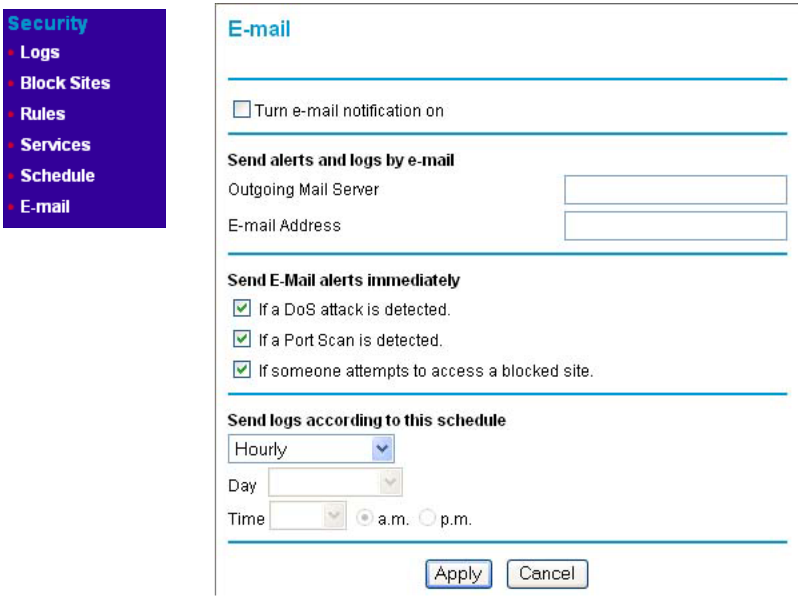
Dropped Packets

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

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

Enabling Security Event E-mail Notification

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



E-mail

□ Turn e-mail notification on

Send alerts and logs by e-mail

Outgoing Mail Server

E-mail Address

Send E-Mail alerts immediately

☑ If a DoS attack is detected.

☑ If a Port Scan is detected.

☑ If someone attempts to access a blocked site.

Send logs according to this schedule

Hourly

Day

Time ● a.m. ○ p.m.

- 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 FVL328 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.

Procedure 5-2: Backing Up the Configuration to a File

1. Log in to the firewall at its default LAN address of *http://192.168.0.1* with its default User Name of **admin**, default password of **password**, or using whatever password and LAN address you have chosen for the firewall.

2. From the Maintenance heading of the Main Menu, select the Settings Backup menu as seen in Figure 5-7.

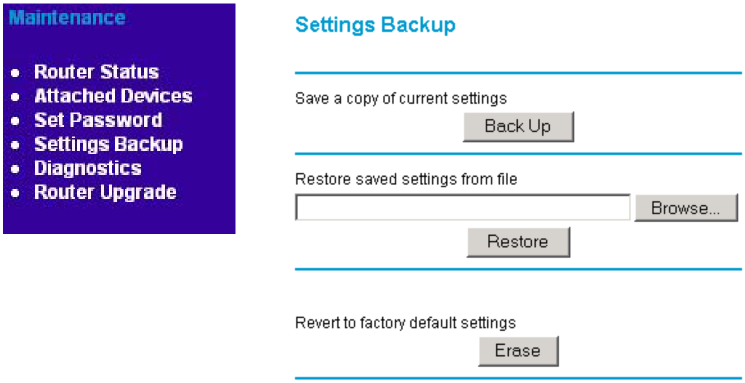


Figure 5-7: Settings Backup menu

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

Procedure 5-3: Restoring a Configuration from a File

1. Log in to the firewall at its default LAN address of *http://192.168.0.1* with its default user name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the firewall.
2. From the Maintenance heading of the Main Menu, select the Settings Backup menu as seen in Figure 5-7.
3. Under Restore Saved Settings from File, enter the full path to the file on your network or click the Browse button to browse to the file.
4. When you have located the `.cfg` file, click the Restore button to upload the file to the firewall.
5. The firewall will then reboot automatically.

Procedure 5-4: Erasing 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 Settings Backup menu, click the Erase button under Revert to factory default settings.
2. The firewall will then reboot automatically.

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

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

Running Diagnostic Utilities and Rebooting the Router

The FVL328 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.

Note: If you are troubleshooting a network connectivity problem and want to Ping the FVL328, be sure it is configured to respond to a Ping on the Internet WAN port by checking the checkbox seen in "Rules menu" on page 3-6. However, to preserve a high degree of security, you should turn off this feature when you are finished with your diagnostic testing.

From the Main Menu of the browser interface, under the Maintenance heading, select the Router Diagnostics heading to display the menu shown below. Then select the function you wish to activate.

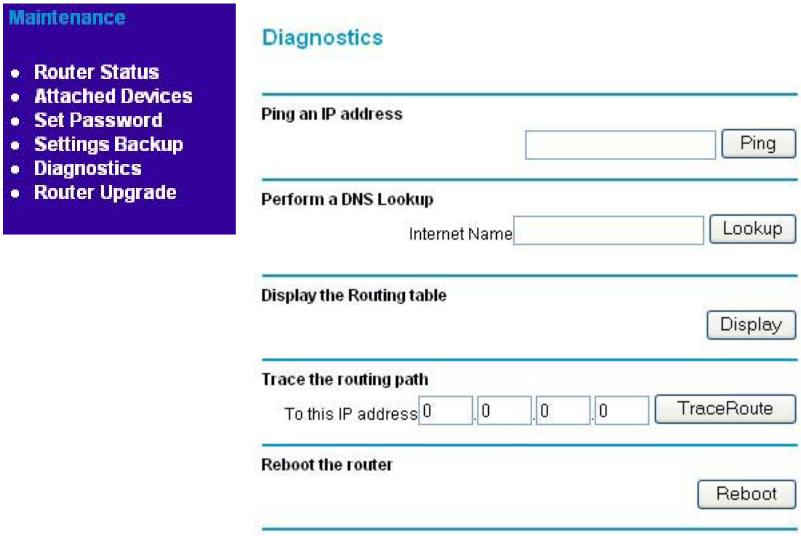


Figure 5-8: Diagnostics menu

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 5-5: Configuring 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.

   Note: For security reasons, 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, the Secure Sockets Layer (SSL) will be enabled. You will enter *https://* and 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:

```
        https://134.177.0.123:8080
```

Upgrading the Router’s Firmware

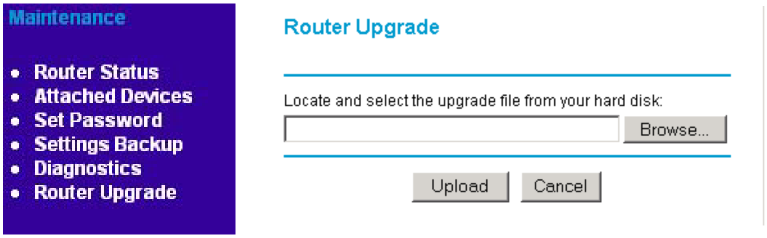
The software of the FVL328 Firewall is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR.

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

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

Procedure 5-1: Upgrading the Router

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, select the Router Upgrade heading to display the menu shown in Figure 5-9.



Locate and select the upgrade file from your hard disk:

Figure 5-9: Router Upgrade menu

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

Note: When uploading software to the firewall, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it may corrupt the software. When the upload is complete, your firewall will automatically restart. The upgrade process will typically take about one minute. In some cases, you may need to clear the configuration and reconfigure the firewall after upgrading.

Chapter 6
Advanced Configuration

This chapter describes how to configure the advanced features of your FVL328 Prosafe High Speed VPN Firewall.

Configuring Advanced Security

The FVL328 Prosafe High Speed VPN 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:** For security, you should avoid using the default DMZ server feature. When a computer is designated as the default DMZ server, it loses much of the protection of the firewall, and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

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.

Procedure 6-1: Assigning a Default DMZ Server

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

Responding 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.

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.

DHCP

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.

Using the Router as a DHCP Server

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 addresses 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.

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 accesses the firewall's DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.

To reserve an IP address:

1. Click the Add button.
2. In the IP Address box, type the IP address to assign to the PC or server.
   Choose an IP address from the 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.

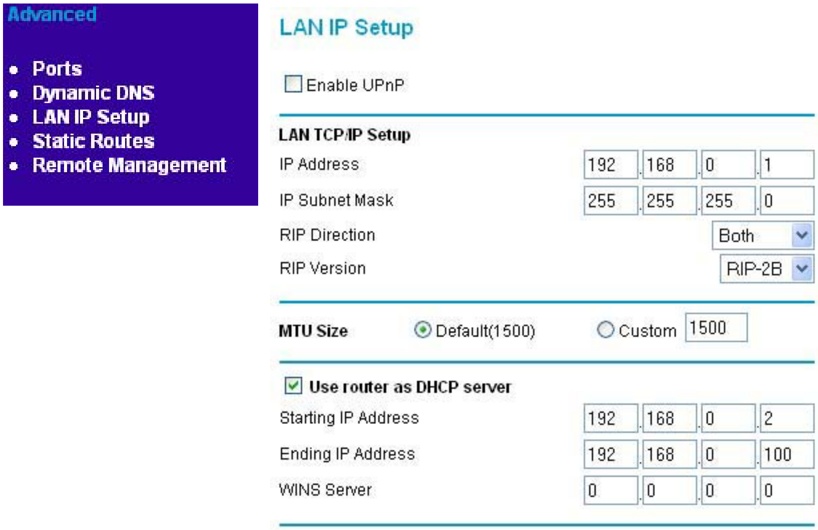
To edit or delete a reserved address entry:

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

Procedure 6-2: Configuring LAN TCP/IP Setup

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 in Figure 6-1



LAN IP Setup

□ Enable UPnP

LAN TCP/IP Setup

IP Address 192 . 168 . 0 . 1

IP Subnet Mask 255 . 255 . 255 . 0

RIP Direction Both

RIP Version RIP-2B

MTU Size ● Default(1500) ○ Custom 1500

☑ Use router as DHCP server

Starting IP Address 192 . 168 . 0 . 2

Ending IP Address 192 . 168 . 0 . 100

WINS Server 0 . 0 . 0 . 0

Figure 6-1: LAN IP Setup Menu

3. Enter the 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, which will allow you to register your domain to their IP address, and will forward traffic directed to your domain to your frequently-changing IP address.

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

Procedure 6-3: 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.

Static Route Example

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

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.0.100.
- Your company's network is 134.177.0.0.

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

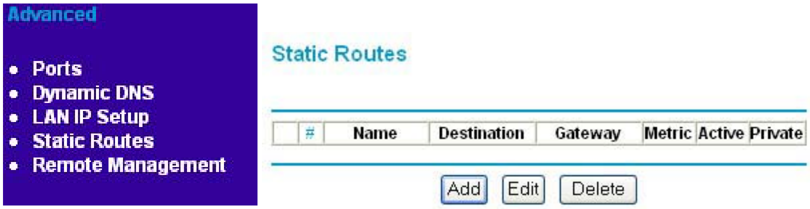
In this case you must define a static route, telling your firewall that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100. The static route would look like Figure 6-3.

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 6-4: Configuring Static Routes

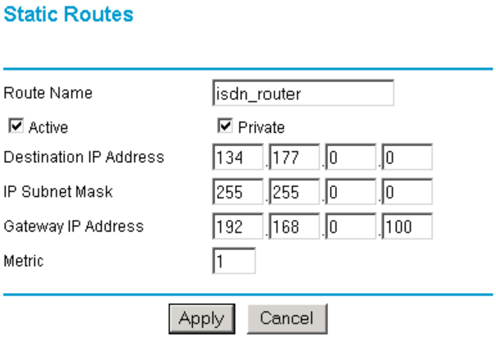
1. Log in to the firewall at its default LAN address of *http://192.168.0.1* with its default user name of **admin**, default password of **password**, or using whatever password and LAN address you have chosen for the firewall.
2. From the Main Menu of the browser interface, under Advanced, click on Static Routes to view the Static Routes menu, shown in Figure 6-2.



	#	Name	Destination	Gateway	Metric	Active	Private

Figure 6-2: Static Routes Table

3. To add or edit a Static Route:
   a. Click the Edit button to open the Edit Menu, shown below.



Route Name	isdn_router
☑ Active	☑ Private
Destination IP Address	134 . 177 . 0 . 0
IP Subnet Mask	255 . 255 . 0 . 0
Gateway IP Address	192 . 168 . 0 . 100
Metric	1

Figure 6-3: 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. Select Active to make this route effective.

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

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

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

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

h. Type a number between 1 and 15 as the Metric value.
This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.

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

Chapter 7
Troubleshooting

This chapter gives information about troubleshooting your FVL328 Prosafe High Speed VPN Firewall. For the common problems listed, go to the section indicated.

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

  Go to "Basic Functions" on page 7-1.

- I can't access the firewall's configuration with my browser.

  Go to "Troubleshooting the Web Configuration Interface" on page 7-3.

- I've configured the firewall but I can't access the Internet.

  Go to "Troubleshooting the ISP Connection" on page 7-4.

- I can't remember the firewall's configuration password, or I want to clear the configuration and start over again.

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

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 7-7.

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

Local or Internet Port Link LEDs Not On

If either the Local or Internet Port Link LEDs do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the firewall and at the hub or PC.

- Make sure that power is turned on to the connected hub or PC.
- Be sure you are using the correct cable:
  - — When connecting the firewall's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

Troubleshooting the Web Configuration Interface

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

- Check the Ethernet connection between the PC and the firewall as described in the previous section.
- Make sure your PC's IP address is on the same subnet as the firewall. If you are using the recommended addressing scheme, your PC's address should be in the range of 192.168.0.2 to 192.168.0.254. Refer to "Verifying TCP/IP Properties" on page C-5 or "Configuring the Macintosh for TCP/IP Networking" on page C-6 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 7-7.
- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

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

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

Troubleshooting the ISP Connection

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

To check the WAN IP address:

1. Launch your browser and select an external site such as *www.netgear.com.*
2. Access the Main Menu of the firewall's configuration at *http://192.168.0.1*.
3. Under the Maintenance heading, select Router Status.
4. Check that an IP address is shown for the WAN Port.
   If 0.0.0.0 is shown, your firewall has not obtained an IP address from your ISP.

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

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

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

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

- Your ISP may check for your PC's host name.
  Assign the PC Host Name of your ISP account as the Account Name in the Basic Settings menu.
- Your ISP only allows one Ethernet MAC address to connect to Internet, and may check for your PC's MAC address. In this case:

  Inform your ISP that you have bought a new network device, and ask them to use the firewall's MAC address.

  OR

  Configure your firewall to spoof your PC's MAC address. This can be done in the Basic Settings menu. Refer to "Manually Configuring Your Internet Connection" on page 2-15.

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 "Verifying TCP/IP Properties" on page C-6. 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 "Verifying TCP/IP Properties" on page C-6.

Troubleshooting a TCP/IP Network Using a Ping Utility

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

Testing the LAN Path to Your Firewall

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

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

1. From the Windows toolbar, click on the Start button and select Run.
2. In the field provided, type Ping followed by the IP address of the firewall, as in this example:

```
ping 192.168.0.1
```

3. Click on OK.

   You should see a message like this one:

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

   If the path is working, you see this message:

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

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

```
Request timed out
```

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

   - Wrong physical connections
     — Make sure the LAN port LED is on. If the LED is off, follow the instructions in "Local or Internet Port Link LEDs Not On" on page 7-2.
     — Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and firewall.
   - Wrong network configuration
     — Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
     — Verify that the IP address for your firewall and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your PC to a Remote Device

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

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

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

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

- — Check that your PC has the IP address of your firewall listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC's Network Control Panel. Verify that the IP address of the firewall is listed as the default gateway as described in "Verifying TCP/IP Properties" on page C-5.
- — 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 2-15.

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 5-9).
- 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.

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.

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.

Problems with Date and Time

The E-Mail menu in the Content Filtering section displays the current date and time of day. The FVL328 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 FVL328 Prosafe High Speed VPN Firewall.

Network Protocol and Standards Compatibility	
Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP PPP over Ethernet (PPPoE)
Power Adapter	
North America:	120V, 60 Hz, input
United Kingdom, Australia:	240V, 50 Hz, input
Europe:	230V, 50 Hz, input
Japan:	100V, 50/60 Hz, input
All regions (output):	12 V DC @ 1.2A output, 20W maximum
Physical Specifications	
Dimensions:	H: 1.56 in (3.96 cm) W: 10.0 in (25.4 cm) D: 9.0 in (17.8 cm)
Weight:	2.72 lb. (1.23 Kg)

Environmental Specifications	
Operating temperature:	32°-140° F (0° to 40° C)
Operating humidity:	90% maximum relative humidity, noncondensing
Electromagnetic Emissions	
Meets requirements of:	FCC Part 15 Class B
	VCCI Class B
	EN 55 022 (CISPR 22), Class B
Interface Specifications	
Local:	10BASE-T or 100BASE-Tx, RJ-45
Internet:	10BASE-T or 100BASE-Tx, RJ-45

Appendix B
Networks, Routing, and Firewall Basics

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

Related Publications

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

Basic Router Concepts

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

What is a Router?

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

Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connection they support.

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 FVL328 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.

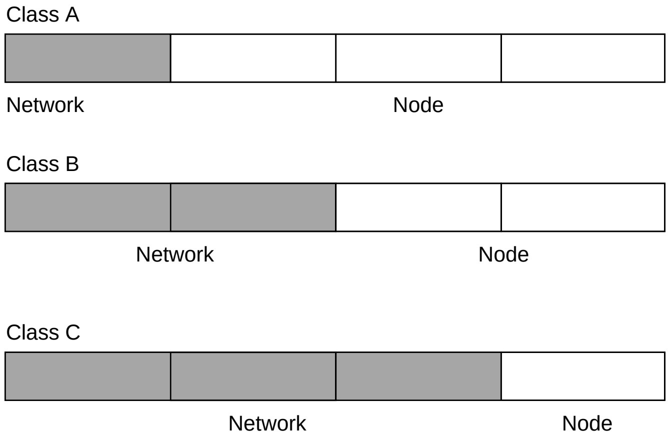


Figure 7-1: Three Main Address Classes

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.

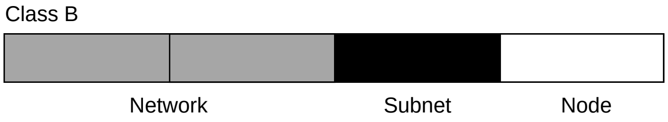


Figure 7-2: Example of Subnetting a Class B Address

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

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

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

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

Table 7-1. 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 7-2. Netmask Formats

Dotted-Decimal	Masklength
255.0.0.0	/8
255.255.0.0	/16

Table 7-2. 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

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

- So that hosts recognize local IP broadcast packets.

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

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

Private IP Addresses

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

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

NETGEAR recommends that you choose your private network number from this range. The DHCP server of the FVL328 Firewall is preconfigured to automatically assign private addresses.

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

Single IP Address Operation Using NAT

In the past, if multiple PCs on a LAN needed to access the Internet simultaneously, you had to obtain a range of IP addresses from the ISP. This type of Internet account is more costly than a single-address account typically used by a single user with a modem, rather than a router. The FVL328 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.

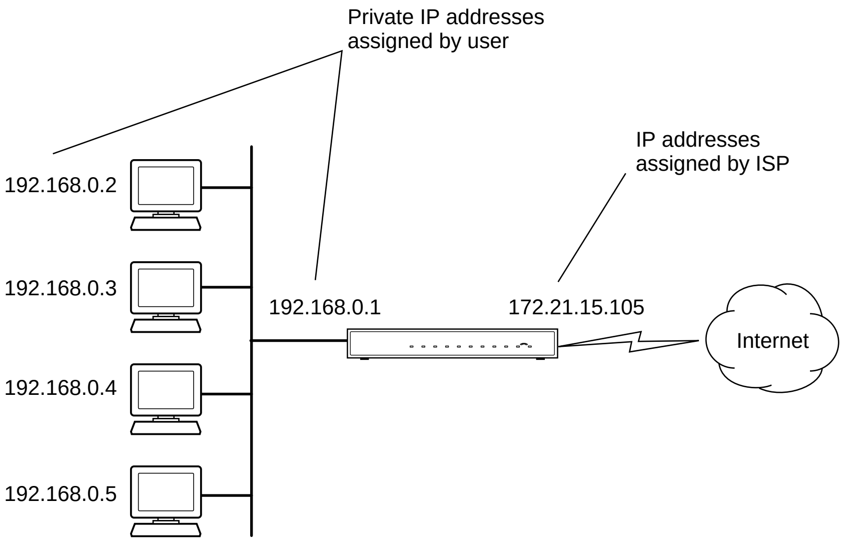


Figure 7-3: Single IP Address Operation Using NAT

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 FVL328 Firewall has the capacity to act as a DHCP server.

The FVL328 Firewall also functions as a DHCP client when connecting to the ISP. The firewall can automatically obtain an IP address, subnet mask, DNS server addresses, and a gateway address if the ISP provides this information by DHCP.

Internet Security and Firewalls

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

What is a Firewall?

A firewall is a device that protects one network from another, while allowing communication between the two. A firewall incorporates the functions of the NAT router, while adding features for dealing with a hacker intrusion or attack. Several known types of intrusion or attack can be recognized when they occur. When an incident is detected, the firewall can log details of the attempt, and can optionally send e-mail 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 be rejected.

Denial of Service Attack

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

Ethernet Cabling

Although Ethernet networks originally used thick or thin coaxial cable, most installations currently use unshielded twisted pair (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. A normal "straight-through" UTP Ethernet cable follows the EIA568B standard wiring as described in Table 7-1.

Table 7-1. UTP Ethernet cable wiring, straight-through

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

Uplink Switches and Crossover Cables

In the wiring table, the concept of transmit and receive are from the perspective of the PC. For example, the PC transmits on pins 1 and 2. At the hub, the perspective is reversed, and the hub receives on pins 1 and 2. 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.

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", 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.

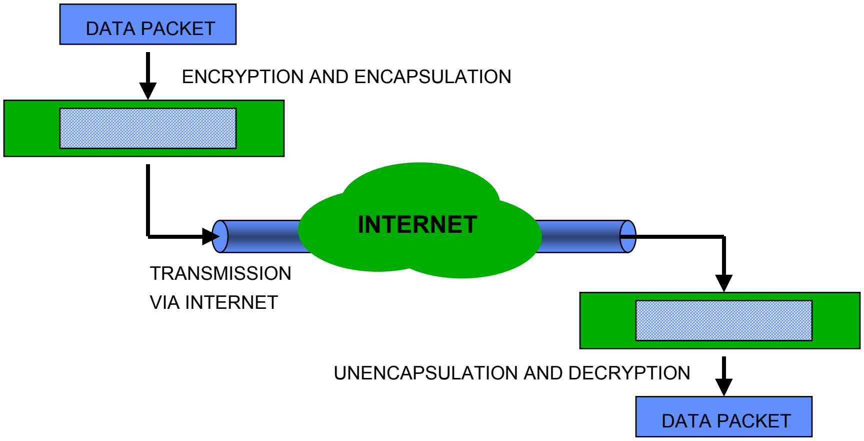


Figure 7-4: VPN overview

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 FVL328 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. The FVL328 is capable of 100 SAs.

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.

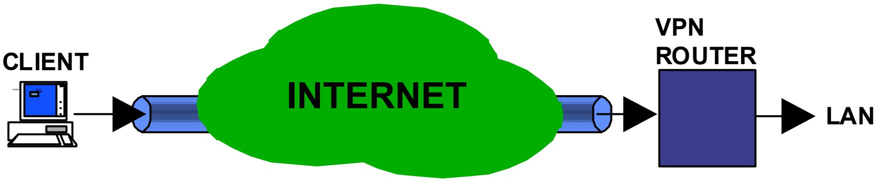


Figure 7-5: Client to LAN access through VPN router

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

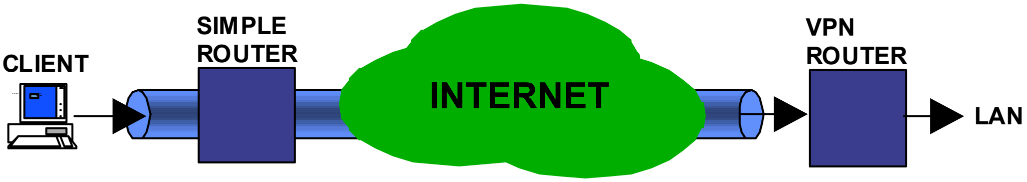


Figure 7-6: Client to LAN access through simple router to VPN router

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

For a PC to act as a tunnel endpoint to your FVL328 Firewall, the PC must run a VPN client program based on the IPSec protocol. NETGEAR recommends that you use the SafeNet SoftRemote (or Soft-PK) VPN client program, which is available from SafeNet (*www.safenet-inc.com*).

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

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.

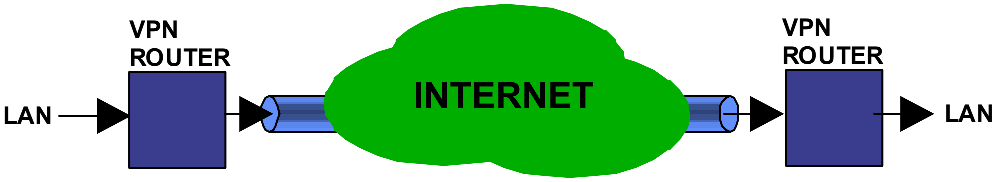


Figure 7-7: LAN to LAN access through VPN router to VPN router

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 FVL328 Prosafe High Speed VPN Firewall and how to verify the readiness of broadband Internet service from an Internet service provider (ISP).

> **Note:** If an ISP technician configured your computer during the installation of a broadband modem, or if you configured it using instructions provided by your ISP, you may need to copy the current configuration information for use in the configuration of your firewall. Write down this information before reconfiguring your computers. Refer to "Obtaining ISP Configuration Information for Windows Computers" on page C-10 or "Obtaining ISP Configuration Information for Macintosh Computers" on page C-11 for further information.

Preparing Your Computers for TCP/IP Networking

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

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

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

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

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

The FVL328 Firewall is shipped preconfigured as a DHCP server. The firewall assigns the following TCP/IP configuration information automatically when the PCs are rebooted:

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

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

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

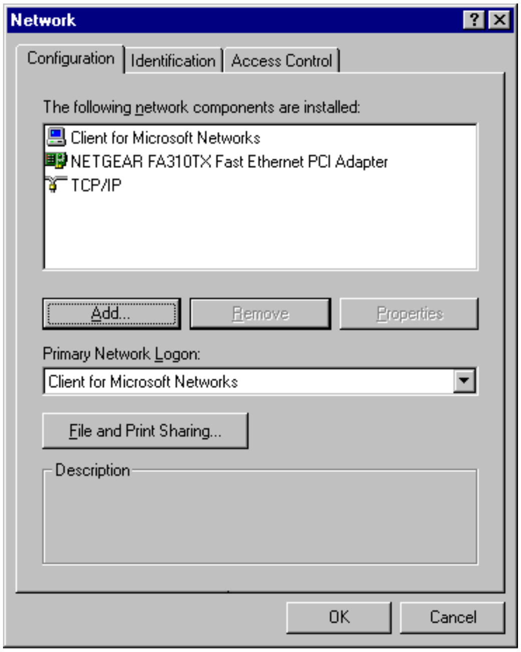
As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Install or Verify Windows Networking Components

To install or verify the necessary components for IP networking:

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

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



The following network components are installed:

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

Primary Network Logon: Client for Microsoft Networks

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

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

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

a. Click the Add button.

b. Select Adapter, and then click Add.

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

If you need TCP/IP:

a. Click the Add button.

b. Select Protocol, and then click Add.

c. Select Microsoft.

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

If you need Client for Microsoft Networks:

a. Click the Add button.

b. Select Client, and then click Add.

c. Select Microsoft.

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

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

Enabling DHCP to Automatically Configure TCP/IP Settings

After the TCP/IP protocol components are installed, each PC must be assigned specific information about itself and resources that are available on its network. The simplest way to configure this information is to allow the PC to obtain the information from the internal DHCP server of the FVL328 Firewall. To use DHCP with the recommended default addresses, follow these steps:

1. Connect all PCs to the firewall, then restart the firewall and allow it to boot.
2. On each attached PC, open the Network control panel (refer to the previous section) and select the Configuration tab.
3. From the components list, select TCP/IP->(your Ethernet adapter) and click Properties.
4. In the IP Address tab, select “Obtain an IP address automatically”.
5. Select the Gateway tab.
6. If any gateways are shown, remove them.
7. Click OK.
8. Restart the PC.

Repeat steps 2 through 8 for each PC 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 *winipcfg.exe*:

1. On the Windows taskbar, click the Start button, and then click Run.
2. Type **`winipcfg`**, and then click OK.

   The IP Configuration window opens, which lists (among other things), your IP address, subnet mask, and default gateway.
3. From the drop-down box, select your Ethernet adapter.

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

   - 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 NT, 2000 or XP for 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.

Installing or Verifying 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. Make sure your PC is connected to the firewall, then reboot your PC.

Verifying TCP/IP Properties

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:
   - The IP address is between 192.168.0.2 and 192.168.0.254
   - The subnet mask is 255.255.255.0
   - The default gateway is 192.168.0.1
4. Type `exit`

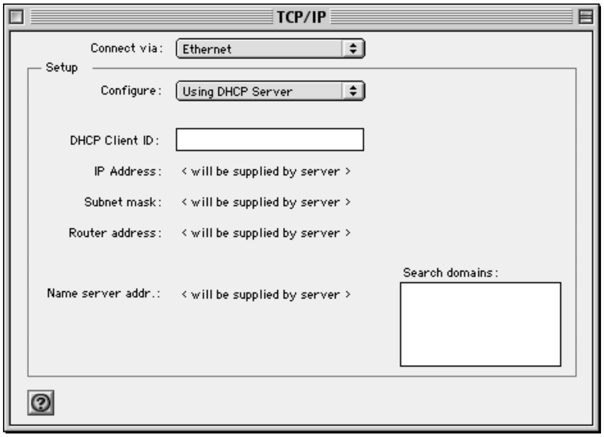
Configuring the Macintosh for TCP/IP Networking

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

MacOS 8.6 or 9.x

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

The TCP/IP Control Panel opens:



Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Search domains:

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

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

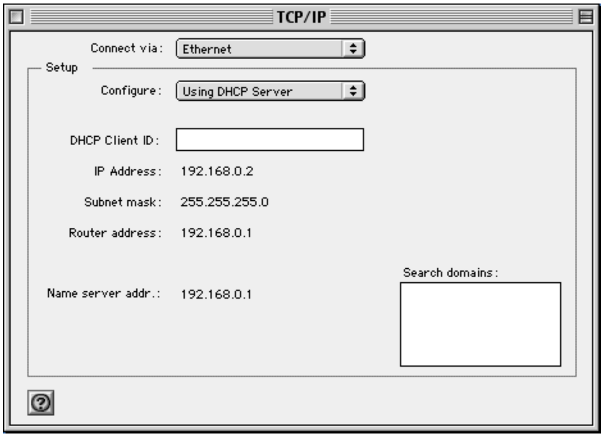
   You can leave the DHCP Client ID box empty.
4. Close the TCP/IP Control Panel.
5. Repeat this for each Macintosh on your network.

MacOS X

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

Verifying TCP/IP Properties for Macintosh Computers

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



TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: 192.168.0.2

Subnet mask: 255.255.255.0

Router address: 192.168.0.1

Name server addr.: 192.168.0.1

Search domains:

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 uses 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 FVL328 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 FVL328 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 have 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 FVL328 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

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.

AH Authentication Header

CA Certificate Authority. A trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be. Usually, this means that the CA has an arrangement with a financial institution, such as a credit card company, which provides it with information to confirm an individual's claimed identity. CAs are a critical component in data security and electronic_commerce because they guarantee that the two parties exchanging information are really who they claim to be.

CRL Certificate Revocation List. Each Certificate Authority (CA) maintains a revoked certificates list.

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. *See* also 3DES.

DH Deffie Helman shared secret algorithm.

DHCP *See* 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

See 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.

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.

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
See local area network.

LDAP
Lightweight Directory Access Protocol. A set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access. Because it's a simpler version of X.500, LDAP is sometimes called *X.500-lite.*

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
See Most Significant Bit or Most Significant Byte.

MTU
See 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
See Network Address Translation.

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 *See* 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 *See* 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.

subnet mask *See* netmask.

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 *See* wide area network.

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.

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.

WINS *See* Windows Internet Naming Service.

Index