Reference Manual for the ProSafe VPN Firewall 50 FVS338

NETGEAR

January 2005

Trademarks

NETGEAR is a trademark of Netgear, Inc.

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

Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

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

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

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

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

• Reorient or relocate the receiving antenna.

• Increase the separation between the equipment and receiver.

• Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

• Consult the dealer or an experienced radio/TV technician for help.

EN 55 022 Declaration of Conformance

This is to certify that the FVS338 ProSafe VPN Firewall 50 is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das FVS338 ProSafe VPN Firewall 50 gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

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

Certificate of the Manufacturer/Importer

It is hereby certified that the FVS338 ProSafe VPN Firewall 50 has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

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

Voluntary Control Council for Interference (VCCI) Statement

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

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

Read instructions for correct handling.

Additional Copyrights

AES	Copyright (c) 2001, Dr Brian Gladman <brg@gladman.uk.net>, Worcester, UK. All rights reserved. TERMS Redistribution and use in source and binary forms, with or without modification, are permitted subject to the following conditions: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. The copyright holder's name must not be used to endorse or promote any products derived from this software without his specific prior written permission. This software is provided 'as is' with no express or implied warranties of correctness or fitness for purpose.

Open SSL	Copyright (c) 1998-2000 The OpenSSL Project. All rights reserved.
	Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions * are met:
	1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
	2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
	3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (*http://www.openssl.org/*)"
	4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
	5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
	6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (*http://www.openssl.org/*)"
	THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
	This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

MD5	Copyright (C) 1990, RSA Data Security, Inc. All rights reserved.
	License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function. License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.
	RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.
	These notices must be retained in any copies of any part of this documentation and/or software.
PPP	Copyright (c) 1989 Carnegie Mellon University. All rights reserved.
	Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by Carnegie Mellon University. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.
	THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.
Zlib	zlib.h -- interface of the 'zlib' general purpose compression library version 1.1.4, March 11th, 2002. Copyright (C) 1995-2002 Jean-loup Gailly and Mark Adler.
	This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions: 1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required. 2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software. 3. This notice may not be removed or altered from any source distribution. Jean-loup Gailly: jloup@gzip.org; Mark Adler: madler@alumni.caltech.edu
	The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files ftp://ds.internic.net/rfc/rfc1950.txt (zlib format), rfc1951.txt (deflate format) and rfc1952.txt (gzip format)

January 2005

Product and Publication Details

Model Number:	FVS338
Publication Date:	January 2005
Product Family:	Router
Product Name:	FVS338 ProSafe VPN Firewall 50
Home or Business Product:	Business
Language:	English

Contents

Chapter 4
Connecting the FVS338 to the Internet

**Chapter 10
Troubleshooting**

January 2005

Chapter 1
About This Manual

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

Audience, Scope, Conventions, and Formats

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

This guide uses the following typographical conventions:

Table 1-1.   Typographical Conventions

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

This guide uses the following formats to highlight special messages:

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

This manual is written for the FVS338 VPN firewall according to these specifications.:

Table 1-2.   Manual Scope

Product Version	FVS338 ProSafe VPN Firewall 50
Manual Publication Date	January 2005

> **Note:** Product updates are available on the NETGEAR, Inc. Web site at
> *http://kbserver.netgear.com/products/FVS338.asp*.

How to Use This Manual

The HTML version of this manual includes the following:

- Buttons, `>` and `<`, for browsing forwards or backwards through the manual one page at a time

- A `TOC` button that displays the table of contents and an `Index` button. Double-click on a link in the table of contents or index to navigate directly to where the topic is described in the manual.

- A `Knowledge Base` button to access the full NETGEAR, Inc. online knowledge base for the product model.

- Links to PDF versions of the full manual and individual chapters.

January 2005

How to Print this Manual

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

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

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

- **Printing a Chapter**.

  Use the *PDF of This Chapter* link at the top left of any page.

  – Click the "*PDF of This Chapter*" link at the top right of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.

    Note: Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at *http://www.adobe.com*.

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

    Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

- **Printing the Full Manual**.

  Use the *Complete PDF Manual* link at the top left of any page.

  – Click the *Complete PDF Manual* link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.
  – Click the print icon in the upper left of the window.

    Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Chapter 2
Introduction

This chapter describes the features of the NETGEAR FVS338 ProSafe VPN Firewall 50.

Key Features of the VPN Firewall

The FVS338 ProSafe VPN Firewall 50 with 8 port switch connects your local area network (LAN) to the Internet through an external access device such as a cable modem or DSL modem.

The FVS338 is a complete security solution that protects your network from attacks and intrusions. Unlike simple Internet sharing NAT routers that rely on Network Address Translation for security, the FVS338 uses Stateful Packet Inspection for Denial of Service (DoS) attack protection and intrusion detection. The FVS338 VPN firewall provides you with multiple Web content filtering options, plus browsing activity reporting and instant alerts – both, via e-mail. Network administrators can establish restricted access policies based on time-of-day, Website addresses and address keywords, and share high-speed cable/DSL Internet access for a local network.

With minimum setup, you can install and use the firewall within minutes.

The FVS338 VPN firewall provides the following features:

- One 10/100 Mbps port for an Ethernet connection to a broadband WAN device, such as a cable modem or DSL modem, and one serial port for a dial-up modem connection to the Internet through the public switched telephone network (PSTN).
- Dual WAN ports (one broadband and one serial) provide for increased system reliability.
- Support for up to 50 VPN tunnels.
- Easy, web-based setup for installation and management.
- URL keyword Content Filtering and Site Blocking Security.
- Quality of Service (QoS) support for traffic prioritization.
- Built in 8-port 10/100 Mbps switch.
- Extensive Protocol Support.
- Login capability.

- SNMP for manageability.
- Front panel LEDs for easy monitoring of status and activity.
- Flash memory for firmware upgrade.

Full Routing on Both the Broadband and Serial WAN Ports

You can install, configure, and operate the FVS338 to take full advantage of a variety of routing options on both the serial and broadband WAN ports, including:

- Internet access via either the serial or broadband port.

- Auto fail-over connectivity through an analog modem connected to the serial port
  If the broadband Internet connection fails, after waiting for an amount of time you specify, the FVS338 can automatically establish a backup dial-up Internet connection via the serial port on the firewall.

A Powerful, True Firewall with Content Filtering

Unlike simple Internet sharing NAT routers, the FVS338 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 FVS338 will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the firewall to email the log to you at specified intervals. You can also configure the firewall to send immediate alert messages to your email address or email pager whenever a significant event occurs.

- With its URL keyword filtering feature, the FVS338 prevents objectionable content from reaching your PCs. The firewall allows you to control access to Internet content by screening for keywords within Web addresses. You can configure the firewall to log and report attempts to access objectionable Internet sites.

Security

The FVS338 VPN firewall is equipped with several features designed to maintain security, as described in this section.

- PCs Hidden by NAT
  NAT opens a temporary path to the Internet for requests originating from the local network. Requests originating from outside the LAN are discarded, preventing users outside the LAN from finding and directly accessing the PCs on the LAN.

- Port Forwarding with NAT
  Although NAT prevents Internet locations from directly accessing the PCs on the LAN, the firewall allows you to direct incoming traffic to specific PCs based on the service port number of the incoming request. You can specify forwarding of single ports or ranges of ports.

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

Autosensing Ethernet Connections with Auto Uplink

With its internal 8-port 10/100 switch, the FVS338 can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. Both the LAN and WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

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

Extensive Protocol Support

The FVS338 VPN firewall supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). For further information about TCP/IP, refer to Appendix B, "Network, Routing, Firewall, and Basics."

- IP Address Sharing by NAT
  The FVS338 VPN firewall allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as NAT, allows the use of an inexpensive single-user ISP account.

- Automatic Configuration of Attached PCs by DHCP
  The FVS338 VPN firewall dynamically assigns network configuration information, including IP, gateway, and domain name server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of PCs on your local network.

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

- 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.

Easy Installation and Management

You can install, configure, and operate the FVS338 ProSafe VPN Firewall 50 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 FVS338 VPN firewall automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.

- VPN Wizard
  The FVS338 VPN firewall includes the NETGEAR VPN Wizard to easily configure VPN tunnels according to the recommendations of the Virtual Private Network Consortium (VPNC) to ensure the VPN tunnels are interoperable with other VPNC-compliant VPN routers and clients.

- SNMP
  The FVS338 VPN firewall supports the Simple Network Management Protocol (SNMP) to let you monitor and manage log resources from an SNMP-compliant system manager. The SNMP system configuration lets you change the system variables for MIB2.

- Diagnostic functions
  The firewall incorporates built-in diagnostic functions such as Ping, Trace Route, DNS lookup, and remote reboot.

- Remote management
  The firewall allows you to securely login to the Web Management Interface from a remote location on the Internet. For additional security, you can limit remote management access to a specified remote IP address or range of addresses, and you can choose a nonstandard port number.

- Visual monitoring
  The FVS338 VPN firewall's front panel LEDs provide an easy way to monitor its status and activity.

Maintenance and Support

NETGEAR offers the following features to help you maximize your use of the FVS338 VPN firewall:

- Flash memory for firmware upgrade

- Free technical support seven days a week, twenty-four hours a day

Package Contents

The product package should contain the following items:

- FVS338 ProSafe VPN Firewall 50.
- AC power adapter.
- Category 5 (Cat 5) Ethernet cable.
- *Resource CD for ProSafe VPN Firewall (240-10118-01)*, including:

  — This guide.

  — Application Notes and other helpful information.

  — ProSafe VPN Client Software - one user license.

• Warranty and 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 firewall for repair.

The Router's Front Panel

The FVS338 ProSafe VPN Firewall 50 front panel shown below contains the status LEDs.
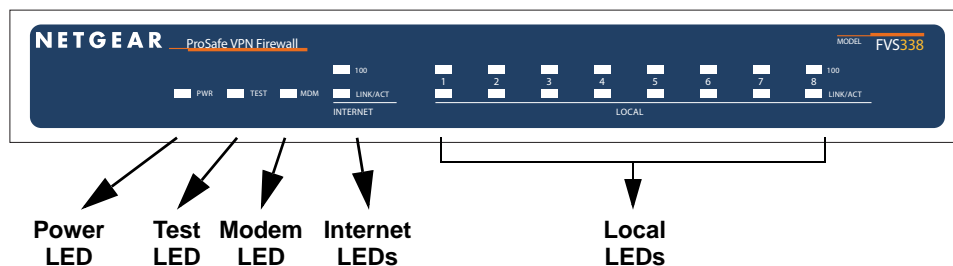
Figure 2-1: FVS338 Front Panel

You can use the LEDs to verify various conditions. Table 2-1 lists and describes each object on the front panel of the router and its operation.

Table 2-1.   Object Descriptions

Object	Activity	Description
Power LED	On (Green) Off	Power is supplied to the router. Power is not supplied to the router.
Test LED	On (Amber) Blinking (Amber) Off	Test mode: The system is initializing or the initialization has failed. Writing to Flash memory (during upgrading or resetting to defaults). The system has booted successfully.
MDM LED	On (Green) Blinking (Green) Off	The serial port detected a link with an attached modem. Server data is being transmitted or received by the serial port. The serial port has no link.

Table 2-1.   Object Descriptions (continued)

Object	Activity	Description

Internet LEDs	Link/Act LED
	     On (Green)
	     Blinking (Green)
	     Off
		The WAN port has detected a link with a connected Ethernet device.
		Data is being transmitted or received by the WAN port.
		The WAN port has no link.

	100 LED
	     On (Green)
	     Off
		The WAN port is operating at 100 Mbps.
		The WAN port is operating at 10 Mbps.

Local LEDs	Link/Act LED
	     On (Green)
	     Blinking (Green)
	     Off
		The LAN port has detected a link with a connected Ethernet device.
		Data is being transmitted or received by the LAN port.
		The LAN port has no link.

	100 LED
	     On (Green)
	     Off
		The LAN port is operating at 100 Mbps.
		The LAN port is operating at 10 Mbps.

The Router's Rear Panel

The rear panel of the FVS338 ProSafe VPN Firewall 50 (Figure 2-1) contains the port connections, modem connector, factory defaults button, On/Off switch, and DC power connection.
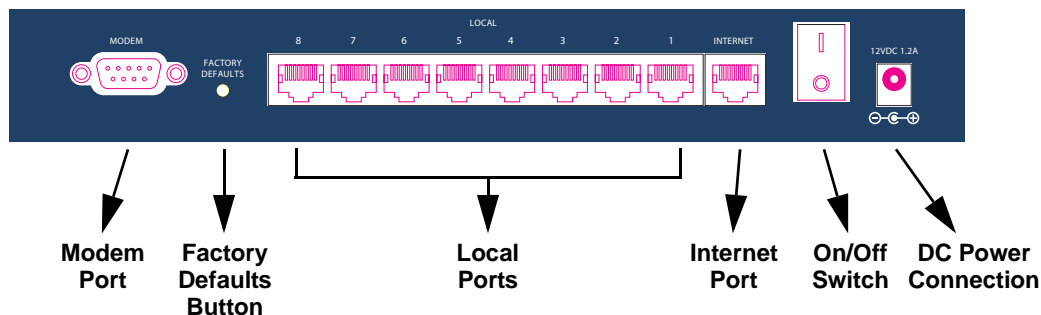
Figure 2-2: FVS338 Rear Panel

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

• Modem port — serves as the WAN2 Internet port through the public switched telephone network (PSTN).

• Factory Defaults push button — see "Default Factory Settings" on page 2-9.

- Local ports — 8-port RJ-45 10/100 Mbps Fast Ethernet Switch, N-way automatic speed negotiation, auto MDI/MDIX.
- Internet port — serves as the WAN1 Internet port. One RJ-45 WAN port, N-way automatic speed negotiation, Auto MDI/MDIX.
- On/Off switch
- DC power in (12 VDC, 1.2A)

The Router's IP Address, Login Name, and Password

Check the label on the bottom of the FVS338's enclosure if you forget the following factory default information:

- IP Address: **http://192.168.1.1** to reach the Web-based GUI from the LAN
- User name: **admin**
- Password: **password**
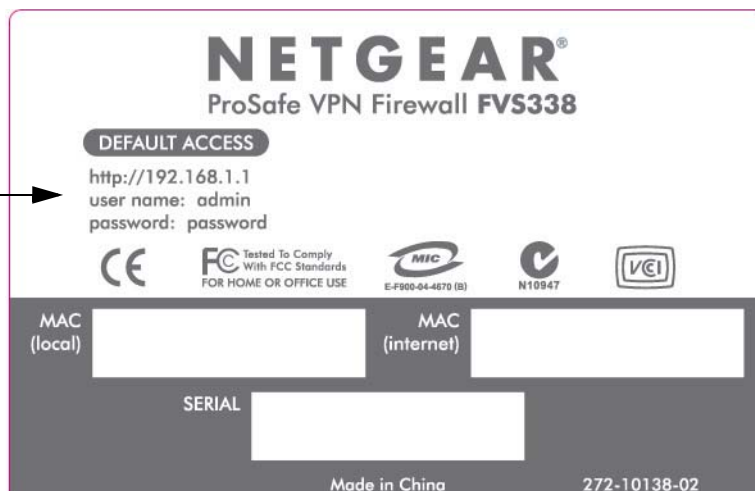
Figure 2-3: FVS338 Bottom Label

Default Factory Settings

When you first receive your FVS338, the default factory settings will be set as shown in Table 2-2 below. You can restore these defaults with the Factory Defaults restore switch on the rear panel — see "The Router's Rear Panel" on page 2-7.

- Pressing this switch for a prolonged period (>10 seconds; until the EST LED begins to blink) causes the router to restore all factory default settings and reboot.

- A shorter press and release causes the router to merely reboot.

Table 2-2.   Factory Default Settings

Feature	Default
User Name (case sensitive)	**admin**
Password (case sensitive)	**password**
Built-in DHCP server	**DHCP server enabled, issues addresses in the default subnet**
IP Configuration	**IP Address: 192.168.1.1** **Subnet Mask: 255.255.255.0**
Time Zone	**GMT**
Time Zone Adjust for Daylight Saving TIme	**Disabled**
SNMP	**Disabled**

NETGEAR Related Products

NETGEAR products related to the FVS338 ProSafe VPN Firewall 50 are as follows:

- FA311 10/100 PCI Adapter
- FA511 10/100 32-bit CardBus Adapter
- GA311 10/100/1000 PCI Adapter
- FVL328 ProSafe VPN Firewall
- FVS318 ProSafe VPN Firewall 8
- FVX538 ProSafe VPN Firewall 200
- FWG114P ProSafe 802.11g Wireless Firewall with USB Print Server
- NMS100 ProSafe Network Management System

- VPN01L and VPN05L ProSafe VPN Client Software
- WG302 ProSafe 802.11g Access Point

January 2005

Chapter 3
Network Planning

This chapter describes the factors to consider when planning a network using a router that has dual WAN ports.

Overview of the Planning Process

The areas that require planning when using a router that has dual WAN ports include:

- Single or multiple exposed hosts
- Virtual private networks (VPNs)

The two WAN ports can be configured to fail over for increased system reliability.

→ **Note:** Exposed hosts are sometimes referred to as DMZ hosts. Unlike hardware-based DMZ ports, however, exposed hosts are implemented in software and do not enjoy the same level of firewall protection that hardware-based DMZ ports do. Use the exposed host feature at your own risk.

Single or Multiple Exposed Hosts

Unrequested incoming traffic can be directed to one or more exposed hosts rather than being discarded. As a result, the IP address of at least one WAN port must always be public.

The mechanism for making the IP address public depends on whether there are single or multiple exposed hosts and whether the dual WAN ports are configured to either fail over or balance the loads. See "Single or Multiple Exposed Hosts" on page 3-2 for further discussion.

Virtual Private Networks (VPNs)

A virtual private network (VPN) tunnel provides a secure communication channel between either two gateway VPN routers or between a remote PC client and gateway VPN router. As a result, the IP address of at least one of the tunnel end points must be known in advance in order for the other tunnel end point to establish (or re-establish) the VPN tunnel. See "Virtual Private Networks (VPNs)" on page 3-5 for further discussion.

January 2005

> **Note:** Once the gateway router WAN port fails over, the VPN tunnel collapses and must be re-established using the new WAN IP address.

The Fail-over Case for Routers With Dual WAN Ports

Failover (Figure 3-1) for the dual WAN port case is different from the single gateway WAN port case when specifying the IP address. Only one WAN port is active at a time and when it fails over, the IP address of the active WAN port always changes. Hence, the use of a fully-qualified domain name is always required, even when the IP address of each WAN port is fixed.

Dual WAN Ports (Before Failover)

WAN1 IP
Router **WAN1 port active**

PSTN
WAN2 port inactive
WAN2 IP (N/A)

Dual WAN Ports (After Failover)

WAN1 IP (N/A)
Router **WAN1 port inactive**

PSTN
WAN2 port active
WAN2 IP

IP address of active WAN port changes after a failover:
o use of fully-qualified domain names always required
o features requiring fixed IP address blocks not supported

Figure 3-1: Dual WAN ports before and after failover

Features such as multiple exposed hosts are not supported in general when using dual WAN port failover because the IP addresses of each WAN port must be in the identical range of fixed addresses.

> **Note:** In certain locales, an ISP has been able to provision the same IP address for the broadband and PSTN service so that the failover to a serial connection would be as seamless as possible.

Single or Multiple Exposed Hosts

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 Incoming Rules menu. Instead of discarding this traffic, you can have it forwarded to one or more LAN hosts on your network. These LAN hosts are called exposed hosts. The addressing of the router's dual WAN port depends on the configuration being implemented:

Table 3-1. **IP addressing requirements for exposed hosts in dual WAN port systems**

Configuration and WAN IP address		Single WAN Port (reference case)	Dual WAN Port Case
			Failover
Single exposed host	Fixed	Allowed (FQDN optional)	FQDN required
	Dynamic	FQDN required	FQDN required
Multiple exposed hosts	Fixed	Address block required	Not allowed*
	Dynamic	Not allowed	Not allowed

*. Not allowed because to do so, the IP addresses of each WAN port would have to be the identical range of fixed addresses. In certain locales, however, an ISP has been able to provision the same IP address for the broadband and PSTN service so that the failover to a serial connection would be as seamless as possible.

Single Exposed Host

The Internet IP address of the router's WAN port must be public so that the public can send incoming traffic to the exposed host when this feature is supported and enabled.

Single Exposed Host: Single WAN Port (Reference Case)

In the single WAN case (Figure 3-2), the WAN's Internet address is either fixed IP or a fully-qualified domain name if the IP address is dynamic.

Figure 3-2: Single WAN port case with exposed host

Single Exposed Host: Dual WAN Ports for Improved System Reliability

In the dual WAN port case with failover (Figure 3-3), the WAN's IP address will always change at failover. A fully-qualified domain name must be used that toggles between the IP addresses of the WAN ports (i.e., WAN1 or WAN2).

January 2005
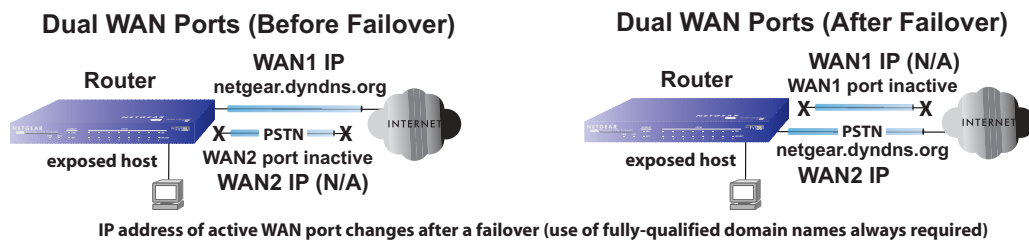
Figure 3-3: Dual WAN port case with exposed host, before and after failover

Multiple Exposed Hosts

The IP address range of the router's WAN port must be both fixed and public so that the public can send incoming traffic to the multiple exposed hosts when this feature is supported and enabled.

Multiple Exposed Hosts: Single WAN Port (Reference Case)

In the single WAN case (Figure 3-4), the WAN port's IP address range must be fixed.
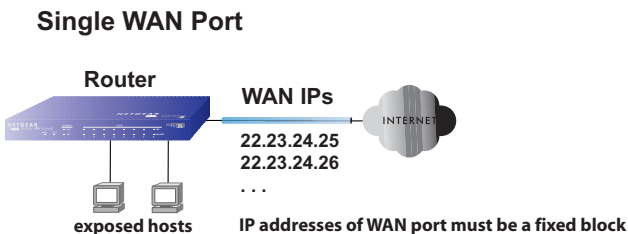
Figure 3-4: Single WAN port case with multiple exposed hosts

Multiple Exposed Hosts: Dual WAN Ports for Improved System Reliability

Using multiple exposed hosts with routers that have dual WAN ports for improved system reliability is a disallowed combination because to do so, the IP addresses of each WAN port would have to be the identical range of fixed addresses. Instead, use additional routers that have dual WAN ports with a single exposed host for improved system reliability.

> **Note:** In certain locales, an ISP has been able to provision the same IP address for the broadband and PSTN service so that the failover to a serial connection would be as seamless as possible.

Virtual Private Networks (VPNs)

When implementing virtual private network (VPN) tunnels, a mechanism must be used for determining the IP addresses of the tunnel end points. The addressing of the router's dual WAN port depends on the configuration being implemented:

Table 3-1.   IP addressing requirements for VPNs in dual WAN port systems

Configuration and WAN IP address		Single WAN Port (reference case)	Dual WAN Port Case
			Failover[*]
VPN Road Warrior (client-to-gateway)	Fixed	Allowed (FQDN optional)	FQDN required
	Dynamic	FQDN required	FQDN required
VPN Gateway-to-Gateway	Fixed	Allowed (FQDN optional)	FQDN required
	Dynamic	FQDN required	FQDN required
VPN Telecommuter (client-to-gateway through a NAT router)	Fixed	Allowed (FQDN optional)	FQDN required
	Dynamic	FQDN required	FQDN required

[*]. All tunnels must be re-established after a failover using the new WAN IP address.

For the single gateway WAN port case, the mechanism is to use a fully-qualified domain name (FQDN) when the IP address is dynamic and to use either an FQDN or the IP address itself when the IP address is fixed. The situation is different when dual gateway WAN ports are used in a failover-based system.

Failover (Figure 3-5) for the dual gateway WAN port case is different from the single gateway WAN port case when specifying the IP address of the VPN tunnel end point. Only one WAN port is active at a time and when it fails over, the IP address of the active WAN port always changes. Hence, the use of a fully-qualified domain name is always required, even when the IP address of each WAN port is fixed.
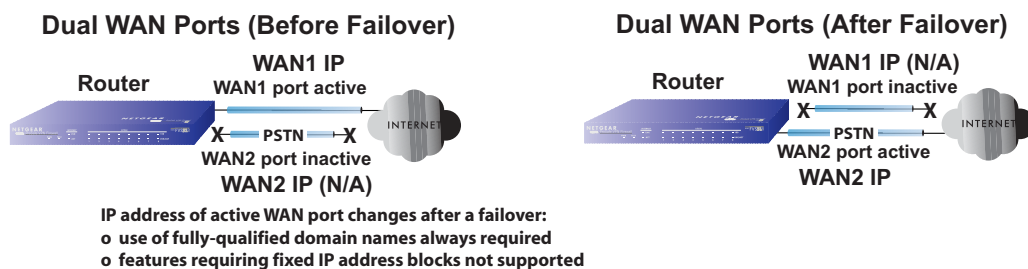
> **Note:** Once the gateway router WAN port fails over, the VPN tunnel collapses and must be re-established using the new WAN IP address.

Dual WAN Ports (Before Failover)   **Dual WAN Ports (After Failover)**

IP address of active WAN port changes after a failover (use of fully-qualified domain names always required)
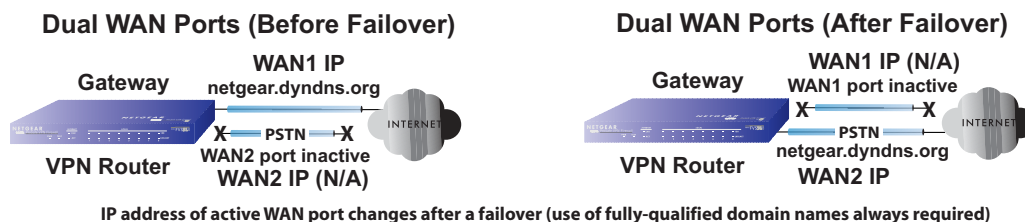
Figure 3-5: Dual gateway WAN ports before and after failover

VPN Road Warrior (Client-to-Gateway)

The following situations exemplify the requirements for a remote PC client with no router to establish a VPN tunnel with a gateway VPN router:

• Single gateway WAN port

• Redundant dual gateway WAN ports for increased system reliability (before and after failover)

VPN Road Warrior: Single Gateway WAN Port (Reference Case)

In the case of the single WAN port on the gateway VPN router (Figure 3-6), the remote PC client initiates the VPN tunnel because the IP address of the remote PC client is not known in advance. The gateway WAN port must act as the responder.
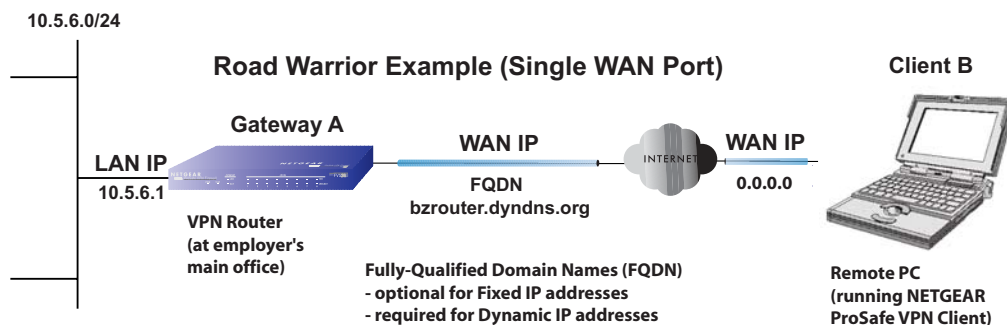
Figure 3-6: Single gateway WAN port case for VPN road warrior

The IP address of the gateway WAN port can be either fixed or dynamic. If the IP address is dynamic, a fully-qualified domain name must be used. If the IP address is fixed, a fully-qualified domain name is optional.

VPN Road Warrior: Dual Gateway WAN Ports for Improved System Reliability

In the case of the dual WAN ports on the gateway VPN router (Figure 3-7), the remote PC client initiates the VPN tunnel with the active gateway WAN port (port WAN1 in this example) because the IP address of the remote PC client is not known in advance. The gateway WAN port must act as a responder.
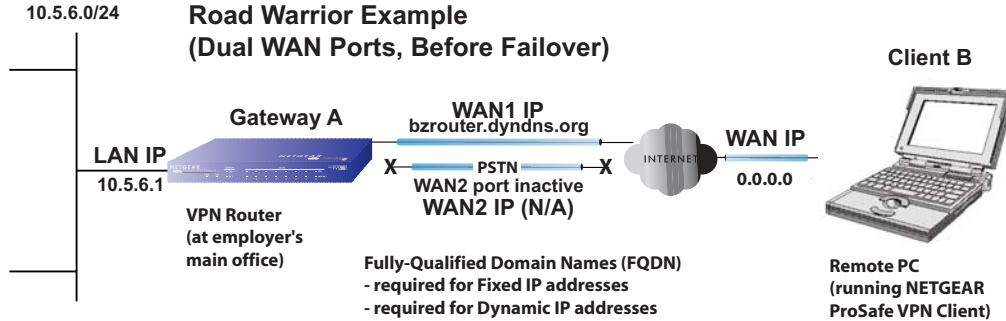
Figure 3-7: Dual gateway WAN ports, before failover, for VPN road warrior

The IP addresses of the gateway WAN ports can be either fixed or dynamic, but a fully-qualified domain name must always be used because the active WAN port could be either WAN1 or WAN2 (i.e., the IP address of the active WAN port is not known in advance).

After a failover of the gateway WAN port (Figure 3-8), the previously inactive gateway WAN port becomes the active port (port WAN2 in this example) and the remote PC client must re-establish the VPN tunnel. The gateway WAN port must act as the responder.

→ | **Note:** Since WAN2 is dial-up, it must be connected before the client can initiate the VPN tunnel.
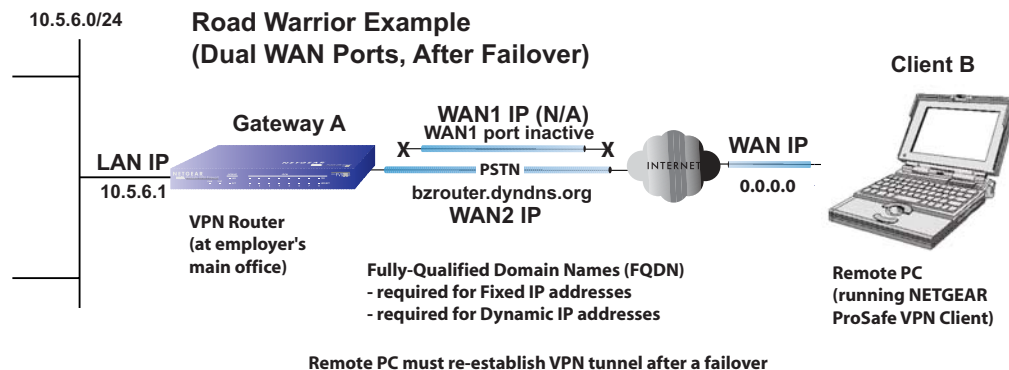
Figure 3-8: Dual gateway WAN ports, after failover, for VPN road warrior

The purpose of the fully-qualified domain name is this case is to toggle the domain name of the gateway router between the IP addresses of the active WAN port (i.e., WAN1 and WAN2) so that the remote PC client can determine the gateway IP address to establish or re-establish a VPN tunnel.

VPN Gateway-to-Gateway

The following situations exemplify the requirements for a gateway VPN router to establish a VPN tunnel with another gateway VPN router:

• Single gateway WAN ports

• Redundant dual gateway WAN ports for increased system reliability (before and after failover)

VPN Gateway-to-Gateway: Single Gateway WAN Ports (Reference Case)

In the case of single WAN ports on the gateway VPN routers (Figure 3-9), either gateway WAN port can initiate the VPN tunnel with the other gateway WAN port because the IP addresses are known in advance.

10.5.6.0/24   **172.23.9.0/24**

Gateway-to-Gateway Example (Single WAN Ports)

Gateway A   **Gateway B**

LAN IP   **WAN IP**   **INTERNET**   **WAN IP**   **LAN IP**

10.5.6.1   **FQDN**   **172.23.9.1**

VPN Router   **netgear.dyndns.org**   **22.23.24.25**   **VPN Router**
(at office A)   **(at office B)**

Fully-Qualified Domain Names (FQDN)
- optional for Fixed IP addresses
- required for Dynamic IP addresses

Figure 3-9: Single gateway WAN ports case for gateway-to-gateway VPN tunnels

The IP address of the gateway WAN ports can be either fixed or dynamic. If an IP address is dynamic, a fully-qualified domain name must be used. If an IP address is fixed, a fully-qualified domain name is optional.

VPN Gateway-to-Gateway: Dual Gateway WAN Ports for Improved System Reliability

In the case of the dual WAN ports on the gateway VPN router (Figure 3-10), either of the gateway WAN ports at one end can initiate the VPN tunnel with the appropriate gateway WAN port at the other end as necessary to balance the loads of the gateway WAN ports because the IP addresses of the WAN ports are known in advance. In this example, port WAN_A1 is active and port WAN_A2 is inactive at Gateway A; port WAN_B1 is active and port WAN_B2 is inactive at Gateway B.

10.5.6.0/24   **Gateway-to-Gateway Example**   **172.23.9.0/24**
                         (Dual WAN Ports, Before Failover)

                         WAN_A1 IP   **WAN_B1 IP**
Gateway A   **netgearA.dyndns.org**   **netgearB.dyndns.org** **Gateway B**

LAN IP   **LAN IP**

10.5.6.1   **X——PSTN——X**   **X——PSTN——X**   **172.23.9.1**
                      WAN_A2 port inactive **WAN_B2 port inactive**
VPN Router   **WAN_A2 IP (N/A)**   **WAN_B2 IP (N/A)**   **VPN Router**
(at office A)   **(at office B)**

Fully-Qualified Domain Names (FQDN)
- required for Fixed IP addresses
- required for Dynamic IP addresses

Figure 3-10: Dual gateway WAN ports, before failover, for gateway-to-gateway VPN tunnels

The IP addresses of the gateway WAN ports can be either fixed or dynamic, but a fully-qualified domain name must always be used because the active WAN ports could be either WAN_A1, WAN_A2, WAN_B1, or WAN_B2 (i.e., the IP address of the active WAN port is not known in advance).

After a failover of a gateway WAN port (Figure 3-11), the previously inactive gateway WAN port becomes the active port (port WAN_A2 in this example) and one of the gateway VPN routers must re-establish the VPN tunnel.
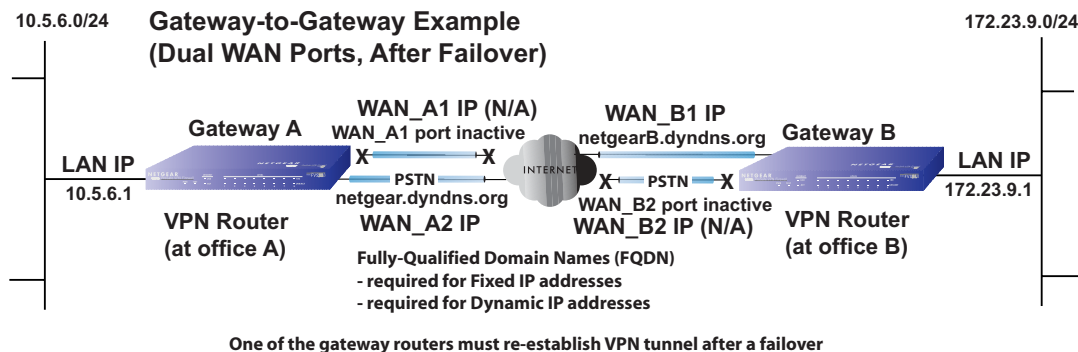
Figure 3-11: Dual gateway WAN ports, after failover, for gateway-to-gateway VPN tunnels

The purpose of the fully-qualified domain names is this case is to toggle the domain name of the failed-over gateway router between the IP addresses of the active WAN port (i.e., WAN_A1 and WAN _A2 in this example) so that the other end of the tunnel has a known gateway IP address to establish or re-establish a VPN tunnel.

VPN Telecommuter (Client-to-Gateway Through a NAT Router)

→ **Note:** The telecommuter case presumes the home office has a dynamic IP address and NAT router for budgetary reasons.

The following situations exemplify the requirements for a remote PC client connected to the Internet with a dynamic IP address through a NAT router to establish a VPN tunnel with a gateway VPN router at the company office:

• Single gateway WAN port

• Redundant dual gateway WAN ports for increased system reliability (before and after failover)

VPN Telecommuter: Single Gateway WAN Port (Reference Case)

In the case of the single WAN port on the gateway VPN router (Figure 3-12), the remote PC client at the NAT router initiates the VPN tunnel because the IP address of the remote NAT router is not known in advance. The gateway WAN port must act as the responder.
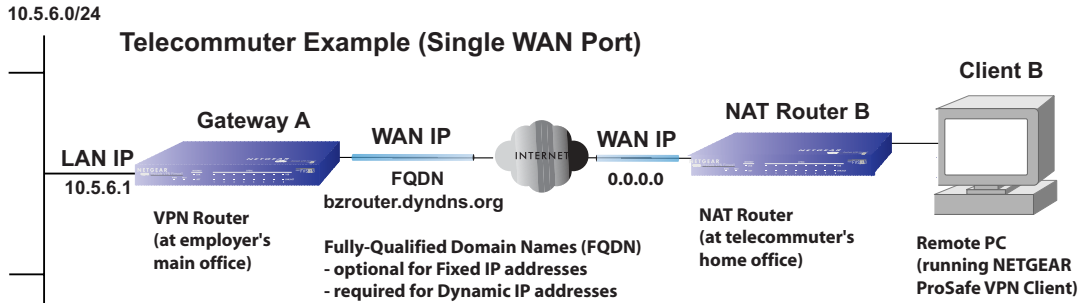
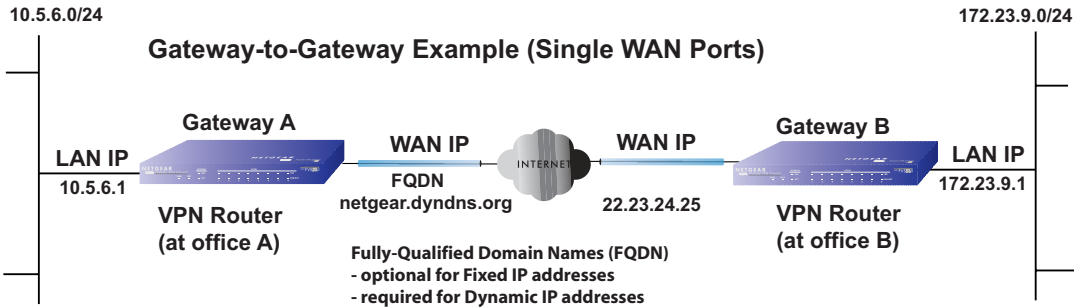**Figure 3-12: Single gateway WAN port case for VPN telecommuter**

The IP address of the gateway WAN port can be either fixed or dynamic. If the IP address is dynamic, a fully-qualified domain name must be used. If the IP address is fixed, a fully-qualified domain name is optional.

VPN Telecommuter: Dual Gateway WAN Ports for Improved System Reliability

In the case of the dual WAN ports on the gateway VPN router (Figure 3-13), the remote PC client initiates the VPN tunnel with the active gateway WAN port (port WAN1 in this example) because the IP address of the remote NAT router is not known in advance. The gateway WAN port must act as the responder.
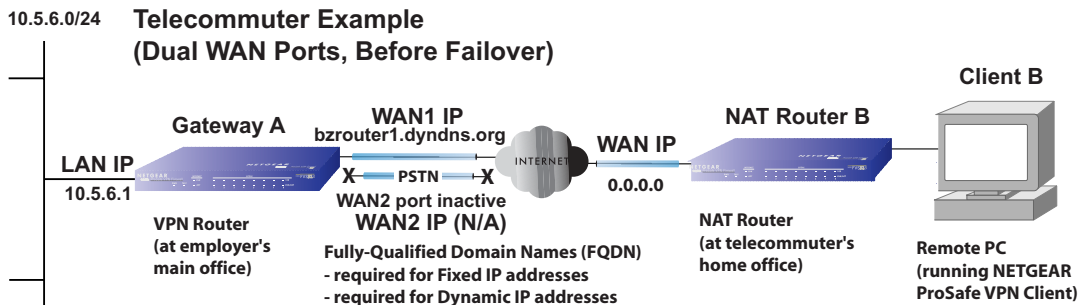
Figure 3-13: Dual gateway WAN ports, before failover, for VPN telecommuter

January 2005

The IP addresses of the gateway WAN ports can be either fixed or dynamic, but a fully-qualified domain name must always be used because the active WAN port could be either WAN1 or WAN2 (i.e., the IP address of the active WAN port is not known in advance).

After a failover of the gateway WAN port (Figure 3-14), the previously inactive gateway WAN port becomes the active port (port WAN2 in this example) and the remote PC must re-establish the VPN tunnel. The gateway WAN port must act as the responder.

> **Note:** Since WAN2 is dial-up, it must be connected before the client can initiate the VPN tunnel.
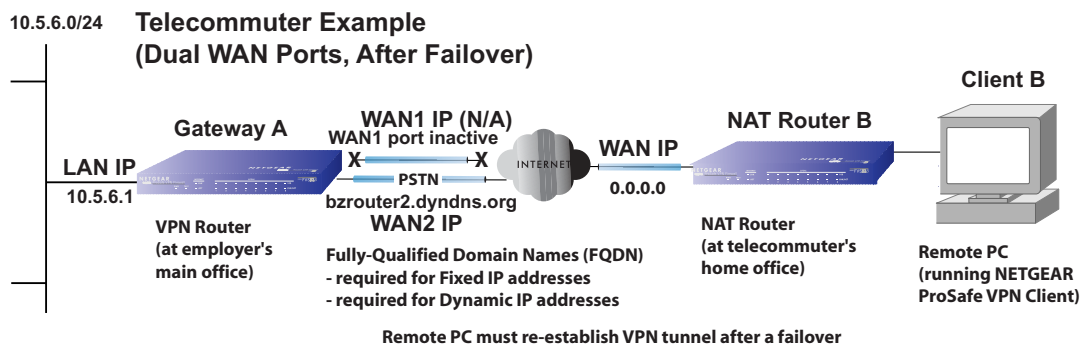
Figure 3-14: Dual gateway WAN ports, after failover, for VPN telecommuter

The purpose of the fully-qualified domain name is this case is to toggle the domain name of the gateway router between the IP addresses of the active WAN port (i.e., WAN1 and WAN2) so that the remote PC client can determine the gateway IP address to establish or re-establish a VPN tunnel.

Chapter 4
Connecting the FVS338 to the Internet

This chapter describes how to set up the firewall on your Local Area Network (LAN) and connect to the Internet. You can perform basic configuration of your FVS338 ProSafe VPN Firewall 50 using the Setup Wizard, or manually configure your Internet connection.

What You Will Need Before You Begin

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

1. A computer properly connected to the VPN 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 account.

LAN Hardware Requirements

To use the FVS338 VPN firewall on your network, each computer must have an installed Ethernet Network Interface Card (NIC) and an Ethernet cable. If the computer will connect to your network at 100 Mbps, you must use a Category 5 (CAT5) cable such as the one provided with your VPN firewall.

The broadband 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 VPN firewall, you will need to connect a computer to the VPN firewall which is set to automatically get its TCP/IP configuration from the VPN firewall via DHCP. The computer you use must have a Web browser such as Internet Explorer v5 or greater or Netscape Communicator v4.7 or greater.

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 VPN 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 FVS338 *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 "Worksheet for Recording Your Internet Connection Information" on page 4-3.

Worksheet for Recording Your Internet Connection Information

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

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

Login Name: _____ Password: _____

Service Name: _____

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

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

Subnet Mask: _____._____._____._____

Gateway IP Address: _____._____._____._____

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

Primary DNS Server IP Address: _____._____._____._____

Secondary DNS Server IP Address: _____._____._____._____

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

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

- If your ISP's mail server is **mail.xxx.yyy.com**, then use **xxx.yyy.com** as the domain name.

ISP Host Name: _____ ISP Domain Name: _____

For Serial Port Internet Access: If you use a dial-up account, record the following:

Account/User Name: _____ Password: _____

Telephone number: _____ Alternative number: _____

Fully Qualified Domain Name: Some organizations use a fully qualified domain name (FQDN) from a dynamic DNS service provider for their IP addresses.

Dynamic DSN Service Provider: _____ FQDN: _____

Connecting the FVS338 to Your LAN

This section provides instructions for connecting the FVS338 ProSafe VPN Firewall 50 to your Local Area Network (LAN).

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

How to Connect the FVS338 to Your LAN

There are three steps to connecting your firewall:

* Connect the VPN firewall to your network.

* Log in to the VPN firewall.

* Connect to the Internet.

Follow the steps below to connect your VPN firewall to your network.

1. **Connect the FVS338.**

    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.

    c. Connect the Ethernet cable (**A**) from your cable or DSL modem to the FVS338's Internet port.

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

       Note: The FVS338 VPN 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 FVS338.

> **Note:** To connect to the VPN 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 VPN firewall and wait for the TEST light to stop blinking.

b. Now, turn on your computer.
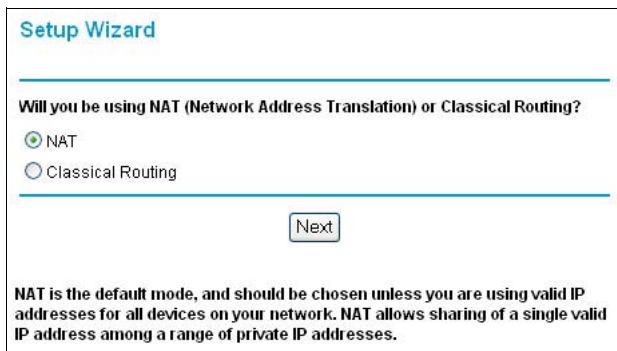
> **Note:** If you usually run software to log in to your Internet connection, do not run that software.

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

– When power on the VPN 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 VPN firewall's LOCAL LINK/ACT lights are lit for any computers that are connected to it.

– The VPN 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 VPN firewall at its default address of *http://192.168.1.1*. A login window opens.

d. For security reasons, the VPN firewall has its own user name and password. When prompted, enter **admin** for the VPN firewall User Name and **password** for the VPN firewall Password, both in lower case letters. This default password should be changed later, as described in "Changing the Administrator Password and Login Timeout" on page 9-8.

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

3. **Connect to the Internet.**

Figure 4-1: Setup Wizard

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

b. Choose NAT or Classical Routing. NAT automatically assigns private IP addresses (192.168.0.x) to LAN connected devices. Classical routing lets you directly manage the IP addresses the FVS338 uses. Classical routing should be selected only by experienced users.

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

   Note: If you choose not to use the Setup Wizard, you can manually configure your Internet connection settings by following the procedure "Manually Configuring Your Internet Connection" on page 4-14.

   Unless your ISP automatically assigns your configuration automatically via DHCP, you will need the configuration parameters from your ISP as you recorded them previously in "Worksheet for Recording Your Internet Connection Information" on page 4-3

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

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

- Connections that require a login using protocols such as PPPoE, Telstra BigPond, or PPTP broadband Internet connections.
- Connections that use dynamic IP address assignment.
- Connections that use fixed IP address assignment.

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

Configuring for a Wizard-Detected Login Account

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 the correct setup menu.

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 VPN 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 want 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 computer in order to access the Internet. When you start an Internet application, the VPN firewall will automatically log you in.

3. Enable or disable NAT (Network Address Translation). NAT allows all LAN computers to gain Internet access via this Router, by sharing this Router's WAN IP address. In most situations, NAT is essential for Internet access via this Router. You should only disable NAT if you are sure you do not require it. When NAT is disabled, only standard routing is performed by this Router.

4. Perform a DNS Lookup. A DNS (Domain Name Server) converts the Internet name (e.g. www.netgear.com) to an IP address. If you need the IP address of a Web, FTP, Mail or other Server on the Internet, you can do a DNS lookup to find the IP address.

   Domain Name Server (DNS) Address: If you know that your ISP does not automatically transmit DNS addresses to the VPN 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 VPN firewall, reboot your computers so that the settings take effect.

5. Enter the Router's MAC Address. Each computer or router on your network has a unique 32-bit local Ethernet address. This is also referred to as the computer's MAC (Media Access Control) address. Usually, select Use default address.

   If your ISP requires MAC authentication, then select either Use this Computer's MAC address to have the router use the MAC address of the computer you are now using, or Use This MAC Address to manually type in the MAC address that your ISP expects.

6. Click Apply to save your settings.

7. Click the Test button to test your Internet connection. If the NETGEAR Web site does not appear within one minute, refer to Chapter 10, "Troubleshooting.

Configuring for a Wizard-Detected Dynamic IP Account

If the Setup Wizard determines that your Internet service account uses Dynamic IP assignment, you will be directed to the correct setup menu.

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 VPN 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 VPN 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 VPN 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 computers after configuring the VPN firewall.

3. The Router's MAC Address is the Ethernet MAC address that will be used by the VPN 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 VPN 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 computer when your account is first opened. They will then only accept traffic from the MAC address of that computer. This feature allows your VPN firewall to masquerade as that computer by using its MAC address.

4. Click Apply to save your settings.

5. Click the Test button to test your Internet connection. If the NETGEAR Web site does not appear within one minute, refer to Chapter 10, "Troubleshooting.

Configuring for a Wizard-Detected Fixed IP (Static) Account

If the Setup Wizard determines that your Internet service account uses Fixed IP assignment, you will be directed to the correct setup menu.

1. Enter your assigned IP Address, Subnet Mask, and the IP Address of your ISP's gateway router. This information should have been provided to you by your ISP. You will need the configuration parameters from your ISP you recorded in "Worksheet for Recording Your Internet Connection Information" on page 4-3.

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 computers after configuring the VPN firewall for these settings to take effect.

3. Click Apply to save the settings.

4. Click the Test button to test your Internet connection. If the NETGEAR Web site does not appear within one minute, refer to Chapter 10, "Troubleshooting.

Configuring a Serial Port as the Primary Internet Connection

Use the procedure below to configure an Internet connection via the serial port of your firewall.

How to Configure the Serial Port for an Internet Connection

There are three steps to configuring the serial port of your firewall for an Internet connection:

1. Connect the firewall to your dial-up analog modem

2. Configure the firewall

3. Connect to the Internet

Follow the steps below to configure a serial port Internet connection on your firewall.

1. **Connect the Firewall to your dial-up modem**

    a. Turn off your modem and connect the cable from the serial port of the FVS338 to the modem.

    b. Turn on the modem and wait about 30 seconds for the lights to stop blinking.

2. **Configure the Serial Port of the Firewall**.

    a. Use a browser to log in to the firewall at http://192.168.1.1 with its default User Name of **admin** and default Password of **password**, or using whatever Password you have set up.

    b. From the Setup Basic Settings menu, click Serial Port.

Figure 4-2: Serial Internet Connection configuration menu

c. Fill in the analog ISP Internet configuration parameters as appropriate:

  • For a Dial-up Account, enter the Account information. Check "Connect as required" to enable the firewall to automatically dial the number. To enable Idle Time disconnect, check the box and enter a time in minutes.
  • To configure the Internet IP settings, fill in the address parameters your ISP provided.

d. Configure the Modem parameters.

Note: You can validate modem string settings by first connecting the modem directly to a PC, establishing a connection to your ISP, and then copying the modem string settings from the PC configuration and pasting them into the FVS338 Modem Properties Initial String field. For more information on this procedure, please refer to the support area of the NETGEAR web site.

- Select the Serial Line Speed. This is the maximum speed the modem will attempt to use. For dial-up modems, 56000 bps would be a typical setting.
- Select the Modem Type.
    - For dial-up, select your modem from the list. "Standard Modem" should work in most cases.
    - If your modem is not on the list, select "User Defined" and enter the Modem Properties.

Note: If you are not using modem from the pre-defined list but are using the "User Defined" Modem Type, you must first use the Serial Port menu Modem link to fill in the Modem Properties settings for your modem.

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

3. **Connect to the Internet to test your configuration.**

a. If you have a broadband connection, disconnect it.

b. From a workstation, open a browser and test your serial port Internet connection.

Note: The response time of your serial port Internet connection will be slower than a broadband Internet connection.

Testing Your Internet Connection

After completing the Internet connection configuration, your can test your Internet connection. Log in to the VPN firewall, then, from the Setup Basic Settings link, click the Test button. If the NETGEAR Web site does not appear within one minute, refer to Chapter 10, "Troubleshooting.

Your VPN firewall is now configured to provide Internet access for your network. Your VPN 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 VPN firewall as needed.

To access the Internet from any computer connected to your VPN firewall, launch a browser such as Microsoft Internet Explorer or Netscape Navigator. You should see the VPN 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 VPN 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   **ISP *Does* Require Login**

Figure 4-3: Browser-based configuration Basic Settings menu

How to Manually Configure the Primary Internet Connection

Use these steps to manually configure the primary Internet connection in the Basic Settings menu.

1. Select your Internet connection type (broadband with or without login, or serial).

   Note: If you are a Telstra BigPond broadband customer, or if you are in an area such as Austria that uses broadband PPTP, login is required. If so, select BigPond or PPTP from the Internet Service Type drop down box.

2. 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.

3. If needed, enter the PPPoE login user name and password provided by your ISP. These fields are case sensitive. To change the login timeout, enter a new value in minutes.

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

4. If you want to disable NAT, select the Disable radio button. Before disabling NAT, back up your current configuration settings.

> **Note:** Disabling NAT will reboot the router and reset all the FVS338 configuration settings to the factory default. Disable NAT only if you plan to install the FVS338 in a setting where you will be manually administering the IP address space on the LAN side of the router.

5. Internet IP Address: If your ISP assigned you a permanent, fixed IP address for your PC, select "Use static IP address." Enter the IP address 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.

6. Domain Name Server (DNS) Address: If 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.

   Note: 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.

7. 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.

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

9. Click **Test** to test your Internet connection. If the NETGEAR Web site does not appear within one minute, refer to Chapter 10, "Troubleshooting.

Configure Dynamic DNS (If Needed)

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 allows you to register an extension to its domain, and restores DNS requests for the resulting FQDN to your frequently-changing IP address.

You are going to need a fully qualified domain name to implement features such as exposed hosts and virtual private networks regardless of whether you have a fixed or dynamic 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.

Perform the following steps to configure Dynamic DNS:

1. If you haven't already, log in to the firewall at its default LAN address of *http://192.168.1.1* 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 WAN Setup, click on Dynamic DNS. You will get the screen shown in Figure 4-4.

Figure 4-4: Dynamic DNS screens

Each DNS service provider requires its own parameters (Figure 4-5).

DynDNS Service Screen   **TZO Service Screen**   **Oray Service Screen**

Figure 4-5: Dynamic DNS service provider screens

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.

January 2005

6. Type the entire FQDN name that your dynamic DNS service provider gave you, such as myName.dyndns.org.

7. Type the user name for logging into 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.

Configure the WAN Options (If Needed)

Perform the following steps to configure the WAN options:

1. If you haven't already, log in to the firewall at its default LAN address of *http://192.168.1.1* 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 WAN Setup, click on Options. You will get the screen shown in Figure 4-6.

Figure 4-6: WAN Options Screens

3. Edit the default information you want to change.

   • Respond To Ping On Internet Port—If you want the router to respond to a 'Ping' from the Internet, click this check box. This can be used as a diagnostic tool. You shouldn't check this box unless you have a specific reason to do so.

   • MTU Size—The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 Bytes, or 1492 Bytes for PPPoE connections. For some ISPs you may need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

   • Port Speed—In most cases, your router can automatically determine the connection speed of the Internet (WAN) port. If you cannot establish an Internet connection and the Internet LED blinks continuously, you may need to manually select the port speed.

     If you know that the Ethernet port on your broadband modem supports 100BaseT, select 100M; otherwise, select 10M. Use the half-duplex settings unless you are sure you need full duplex.

   • Uplink Bandwidth—Set Uplink Bandwidth as per your requirements. You need to select a value between 28 kbps to 100 Mbps that represents the maximum speed of your upstream (outbound) connection. If you are unsure, leave it at the default value of 102,400 kbps. It will depend on your WAN connection type and ISP.

January 2005

Chapter 5
Serial Port Configuration

This chapter describes how to configure the serial port options of your FVS338 ProSafe VPN Firewall 50. The FVS338 serial port lets you share the broadband connection of another FVS338, share resources between two LANs, and take advantage of the routing functions on the broadband (WAN), LAN, and serial network interfaces.

Note: If you configure the serial port of the FVS338 as the primary Internet connection, you will not be able to configure the other serial port options. For instructions on configuring the serial port as the primary Internet connection, please see "Configuring a Serial Port as the Primary Internet Connection" on page 4-9.

The FVS338 provides these serial port configuration options:

- **Modem**
  Use this option to configure the serial modem settings for any of the features below.

- **Auto-Rollover**
  Use this option to provide a backup connection for your broadband service. If the broadband service you configured in the Basic Settings menu fails, the FVS338 will automatically connect to the Internet through the serial port. However, you will then be accessing the Internet at a slower speed than you would through your broadband service.

The procedures for these configuration options are presented below.

Configuring a Serial Port Modem

You can configure a serial port modem for any of the features described above.

Be sure you have prepared the basic requirements listed below, then follow the 'how to' procedure.

Basic Requirements for Serial Port Modem Configuration

Configuring a serial port modem requires these elements:

1. A serial analog modem.

---

2. A serial modem cable with a DB9 connector.

3. An active phone line.

How to Configure a Serial Port Modem

Follow the steps below to configure a serial port modem.

1. From the main menu, click **Modem** in the Serial Port section.
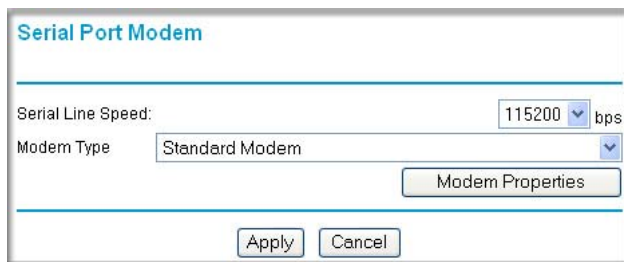
Figure 5-1: Serial Port Modem configuration menu

2. Select the Serial Line Speed.
   This is the maximum speed the modem will attempt to use. For dial-up modems, 56000 bps would be a typical setting.

   — For dial-up, "Standard Modem" should work in most cases. Otherwise, select your modem from the list.

   — If your modem is not on the list, select "User Defined" and enter the Modem Properties.

   If you are using the "User Defined" selection and configuring your own modem stings, fill in the Modem Properties settings.

   Note: You can validate modem string settings by first connecting the modem directly to a PC, establishing a connection to your ISP, and then copying the modem string settings from the PC configuration and pasting them into the FVS338 modem configuration fields. For more information on this procedure, please refer to the support area of the NETGEAR web site.

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

Configuring Auto-Rollover

You can configure the serial port of the FVS338 to provide an auto-rollover backup connection for your broadband service.

Be sure you have prepared the basic requirements listed below, then follow the 'how to' procedure.

Basic Requirements for Auto-Rollover

Auto-Rollover requires these elements:

1. A broadband connection to the FVS338.

2. An analog phone line with an active dial-up ISP account

3. A serial modem properly configured and attached to the DB9 connector on the serial port.

4. The Auto-Rollover settings configured and applied to the FVS338.

How to Configure Auto-Rollover

Follow the steps below to configure a serial port auto-rollover connection.

1. Configure a serial port modem according to the instructions above.

2. From the main menu, click **Auto-rollover** in the Serial Port section.

Figure 5-2: Auto-Rollover configuration menu

3. Configure the Auto-Rollover settings.

4. Click **Apply** for the changes to take effect.

Chapter 6
LAN Configuration

This chapter describes how to configure the advanced features of your FVS338 ProSafe VPN Firewall 50. These features can be found under the Advanced heading in the Main Menu of the browser interface.

- LAN Setup

- DMZ Setup

- Static Routes

Using the LAN IP Setup Options

The LAN IP Setup menu allows configuration of LAN IP services such as DHCP and RIP. From the Main Menu of the browser interface, under Advanced, click on LAN IP Setup to view the LAN IP Setup menu, shown below.

Figure 6-1: LAN IP Setup menu

> **Note:** Once you have completed the LAN IP setup, all outbound traffic is allowed and all inbound traffic is discarded. To change these traffic rules, refer to Chapter 7, "Firewall Protection and Content Filtering.

Configuring LAN TCP/IP Setup Parameters

LAN TCP/IP Setup—The default values are suitable for most users and situations. These are advanced settings that you may configure if you are a network administrator. RIP is applicable if your network contains multiple routers.

• IP Address: Type the IP address of your router (factory default: **192.168.1.1**).

   Make sure that LAN Port IP address and DMZ port IP address are in different subnets.

- IP Subnet Mask: The subnet mask specifies the network number portion of an IP address. Your router will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use 255.255.255.0 as the subnet mask (computed by the router).

- RIP Direction: RIP (Routing Information Protocol, RFC 2453) allows a router to exchange routing information with other routers. The RIP Direction selection controls how the router sends and receives RIP packets. Both is the default.

    – When set to Both or Out Only, the router 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: Multicasting can reduce the load on non-router machines because they do not listen to the RIP multicast address and will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting. For RIP-2B and RIP-2M you can select the type of authentication as NONE or MD5. If MD5 is selected, additional parameters need to be entered.

Use router as DHCP server—By default, the router will function as a DHCP (Dynamic Host Configuration Protocol) server, providing TCP/IP configuration for all computers connected to the router's LAN. If another device on your network will be the DHCP server, or if you will manually configure all devices, select the Disable option under DHCP configuration. Select the DHCP Relay option to configure the router as a DHCP relay.

- DHCP Log - Click this button to see the IP addresses which have been allocated by the DHCP Server to PCs and other DHCP clients.

- Starting IP Address - This box specifies the first of the contiguous addresses in the IP address pool. 192.168.1.2 is the default start address.

- Ending IP Address - This box specifies the last of the contiguous addresses in the IP address pool. 192.168.1.254 is the default ending address.

- WINS Server - This box can specify the Windows NetBios Server IP if one is present in your network.

- Lease Time - This box specifies the Lease time to be given to the DHCP Clients.

> **Note:** If you change the LAN IP address of the firewall while connected through the browser, you will be disconnected. You must then open a new connection to the new IP address and log in again.

Using the Firewall as a DHCP server

By default, the firewall will function as a DHCP (Dynamic Host Configuration Protocol) server, allowing it to assign IP, DNS server, WWS Server, and default gateway addresses to all computers connected to the firewall's LAN. The assigned default gateway address is the LAN address of the firewall. IP addresses will be assigned to the attached PCs from a pool of addresses specified in this menu. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications, the default DHCP and TCP/IP settings of the firewall are satisfactory. See "IP Configuration by DHCP" on page B-10 for an explanation of DHCP and information about how to assign IP addresses for your network.

If another device on your network will be the DHCP server, or if you will manually configure the network settings of all of your computers, clear the 'Use firewall 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 192.168.1.2 and 192.168.1.253, although you may wish to save part of the range for devices with fixed addresses.

The firewall will deliver the following parameters to any LAN device that requests DHCP:

- An IP Address from the range you have defined

- Subnet Mask

- Gateway IP Address (the firewall's LAN IP address)

- Primary DNS Server (if you entered a Primary DNS address in the Basic Settings menu; otherwise, the firewall's LAN IP address)

- Secondary DNS Server (if you entered a Secondary DNS address in the Basic Settings menu)

- WINS Server (if you entered a Secondary DNS address in the Basic Settings menu)

Using Address Reservation

When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time it access the firewall's DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.
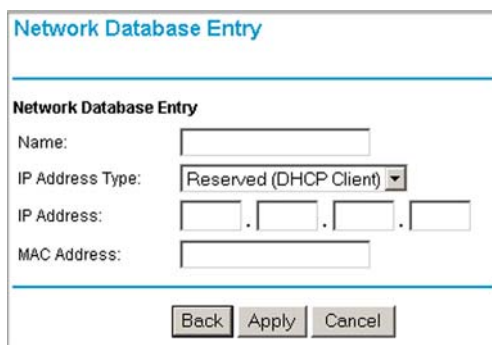
Figure 6-2: Groups and Hosts Entry screen

To reserve an IP address, use the Groups and Hosts Entry screen (see "Managing Groups and Hosts" on page 7-16).

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

Multi Home LAN IPs

Click Multi Home LAN IPs Setup on the LAN IP Setup screen (see Figure 6-1) to invoke the Secondary LAN IP Setup screens. This allows the firewall to act as a gateway to additional logical subnets on your LAN. You can assign the firewall an IP address on each additional logical subnet.

Figure 6-3: Secondary LAN IP Setup screens

DMZ Setup

The DMZ setup screen lets you set up the following features that bypass the standard firewall security used for the LAN:

- **Exposed host (software DMZ)**: Specifying an exposed host allows you to set up a computer or server that is available to anyone on the Internet for services that you haven't defined. There are security issues with doing this, so only do this if you're willing to risk open access. If you do not assign an exposed host, the router discards any incoming service requests that are undefined.

  Note: No firewall security is available for exposed host. Use this feature at your own risk.

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

- **One-to-one NAT mapping**: This feature can only be used if your ISP has allocated you multiple fixed Internet IP addresses.

   Note: No firewall security is available for one-to-one NAT mapping. Use this feature at your own risk.

Exposed Host (Software DMZ)

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

> **Note:** For security, NETGEAR strongly recommends that you avoid using the exposed host feature. When a computer is designated as the exposed host, 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.

From the Main Menu of the browser interface, under Advanced, click on DMZ Setup to view the DMZ Setup menu, shown below.

Figure 6-4: DMZ Setup screen (exposed host setup)

To assign a computer or server to be a exposed host:

1. Click Default DMZ Server.

2. Select the IP address for that PC.

3. Click Apply.

Note: All inbound and outbound traffic is allowed. No firewall protection is available. Use this feature at your own risk.

One-to-One NAT Mapping

> **Note:** You can use the destination address in the inbound rules menu (see "Inbound Rules (Port Forwarding)" on page 7-5) to route additional WAN IP addresses.

If your ISP has given you multiple public IP addresses, this feature allows you to map these additional IP addresses directly to PCs on your LAN or DMZ. (One address has already been entered as your WAN IP and will be used for NAT of all other PCs.) You can define rules for these mappings by entering the assigned public IP address in the Destination Field of the inbound rule.

> → **Note:** For security, NETGEAR strongly recommends that you avoid using the one-to-one NAT mapping feature. When a computer is designated as the destination of one-to-one NAT mapping, it loses much of the protection of the firewall and is exposed to many exploits from the Internet. If compromised, this computer can be used to attack your network.

From the Main Menu of the browser interface, under Advanced, click on DMZ Setup to view the DMZ Setup menu, shown below.

Figure 6-5: DMZ Setup screen (one-to-one NAT mapping setup)

To assign computers or servers for one-to-one NAT mapping:

1. Enable one of the Multi-DMZ checkboxes.

2. To the right of the checkbox, enter the Internet IP address assigned to you by your ISP.

3. Select the PC to be used as the unprotected host for this IP address.

January 2005

4. Click Apply.

Note: All incoming traffic to that IP address will be sent to the selected PC. Out-going traffic from the selected PC will use the IP address you entered, not the default WAN IP address. No firewall protection is available. Use this feature at your own risk.

If you only have one Internet IP address, you cannot use the Multi-DMZ feature. You can only use the Default DMZ Server setting (see "Exposed Host (Software DMZ)" on page 6-7).

Configuring Static Routes

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

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

Figure 6-6. **Static Routes Summary Table and Add screens**

To add or edit a Static Route:

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

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

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

4. Select Active to make this route effective.

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

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

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

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

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

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.

• 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 example:

• The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.

• Private is selected only as a precautionary security measure in case RIP is activated.

Chapter 7
Firewall Protection and Content Filtering

This chapter describes how to use the content filtering features of the FVS338 ProSafe VPN Firewall 50 to protect your network. These features can be found by clicking on the Content Filtering heading in the Main Menu of the browser interface.

Firewall Protection and Content Filtering Overview

The FVS338 ProSafe VPN Firewall 50 provides you with Web content filtering options, plus browsing activity reporting and instant alerts via e-mail. Parents and network administrators can establish restricted access policies based on time-of-day, web addresses and web address keywords. You can also block Internet access by applications and services, such as chat or games.

A firewall is a special category of router that protects one network (the "trusted" network, such as your LAN) from another (the "untrusted" network, such as the Internet), while allowing communication between the two.

A firewall incorporates the functions of a NAT (Network Address Translation) router, while adding features for dealing with a hacker intrusion or attack, and for controlling the types of traffic that can flow between the two networks. Unlike simple Internet sharing NAT routers, a firewall uses a process called stateful packet inspection to protect your network from attacks and intrusions. NAT performs a very limited stateful inspection in that it considers whether the incoming packet is in response to an outgoing request, but true Stateful Packet Inspection goes far beyond NAT.

Using Rules to Block or Allow Specific Kinds of Traffic

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

A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the FVS338 are:

• Inbound: Block all access from outside except responses to requests from the LAN side.

• Outbound: Allow all access from the LAN side to the outside.

These default rules are shown in the Rules table of the Rules menu (under Security on the main menu) in Figure 7-1:

Figure 7-1: Rules menu

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 tailor these rules to your specific needs (see "Administrator Information" on page 7-31).

Note: This feature is for Advanced Administrators only! Incorrect configuration will cause serious problems.

Outbound Services—This lists all existing rules for outbound traffic. If you have not defined any rules, only the default rule will be listed. The default rule allows all outgoing traffic.

- To create a new outbound service rule:

  a. Click the Add button. It does not matter which radio button is selected.

   The Outbound Service screen will be displayed (see "Outbound Rules (Service Blocking)" on page 7-9). This screen has its own help file.

  b. Complete the Outbound Service screen, and save the data. The new rule will be listed in the table when you return to this screen.

- To make changes to an existing outbound service rule:

  a. Click the check box at the beginning of the row and click Apply to disable or Enable the policy.

  b. Click the radio button next to an row in the table.

  c. Click the button for the desired actions:

    – Edit - to make any changes to the rule definition. The Outbound Service screen will be displayed (see "Outbound Rules (Service Blocking)" on page 7-9) with the data for the selected rule.

    – Move - to move the selected rule to a new position in the table. You will be prompted for the new position.

    – Delete - to delete the selected rule.

Inbound Services—This lists all existing rules for inbound traffic. If you have not defined any rules, only the default rule will be listed. The default rule blocks all inbound traffic.

- To create a new inbound service rule:

  a. Click the Add button. It does not matter which radio button is selected.

   The Inbound Service screen will be displayed (see "Inbound Rules (Port Forwarding)" on page 7-5). This screen has its own help file.

  b. Complete the Inbound Service screen and save the data. The new rule will be listed in the table when you return to this screen.

- To make changes to an existing inbound service rule:

  a. Click the radio button next to an row in the table.

  b. Click the button for the desired actions:

       – Edit - to make any changes to the rule definition. The Inbound Service screen will be displayed (see "Inbound Rules (Port Forwarding)" on page 7-5) with the data for the selected rule.

       – Move - to move the selected rule to a new position in the table. You will be prompted for the new position.

       – Delete - to delete the selected rule.

Attack Checks—These check boxes allows you to enable check on various attacks. Select the appropriate checkbox to enable them.

- VPN Passthrough: Enable this to pass the VPN traffic without any filtering, specially used when this box is between two VPN tunnel end points,

- Drop fragmented IP packets: Enable this to drop the fragmented IP packets,

- UDP Flooding: Enable this to limit the number of UDP sessions created from one LAN machine.

- TCP Flooding: Enable this to protect the router from Syn flood attack.

- Enable DNS Proxy: Enable this to allow the incoming DNS queries.

- Enable Stealth Mode: Enable this to set the firewall to operate in stealth mode.

Services-Based Rules

The rules to block traffic are based on the traffic's category of service.

- Inbound rules (port forwarding)—Inbound traffic is normally blocked by the firewall unless the traffic is in response to a request from the LAN side. The firewall can be configured to allow this otherwise blocked traffic.

- Outbound rules (service blocking)—Outbound traffic is normally allowed unless the firewall is configured to disallow it.

- Customized services—Additional services can be added to the list of services in the factory default list. These added services can then have rules defined for them to either allow or block that traffic.

- Quality of service (QoS) priorities—Each service at its own native priority that impacts its quality of performance and tolerance for jitter or delays. You can change this QoS priority if desired to change the traffic mix through the system.

Inbound Rules (Port Forwarding)

Because the FVS338 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.

Figure 7-2: Add Inbound Service Rules screen

→ **Note:** See "Port Triggering" on page 7-24 for yet another way to allow certain types of inbound traffic that would otherwise be blocked by the firewall.

Table 7-1. **Inbound Services**

Item	Description
Services	Select the desired Service or application to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see "Customized Services" on page 7-12).
Action	Select the desired action for packets covered by this rule: • BLOCK always • BLOCK by schedule, otherwise Allow • ALLOW always • ALLOW by schedule, otherwise Block **Note**: Any inbound traffic which is not allowed by rules you create will be blocked by the Default rule.
Select Schedule	Select the desired time schedule (i.e., Schedule1, Schedule2, or Schedule3) that will be used by this rule. • This drop down menu gets activated only when "BLOCK by schedule, otherwise Allow" or "ALLOW by schedule, otherwise Block" is selected as Action. • Use schedule page to configure the time schedules.
LAN users	These settings determine which computers on your network are affected by this rule, based on their IP address. Select the desired IP Address in this field.
WAN Users	These settings determine which Internet locations are covered by the rule, based on their IP address. Select the desired option: • Any - All Internet IP address are covered by this rule. • Single address - Enter the required address in the start fields. • Address range - If this option is selected, you must enter the start and finish fields.
Destination Address	These settings determine the destination IP address for this rule which will be applicable to incoming traffic, this rule will be applied only when the destination IP address of the incoming packet matches the IP address of the WAN interface selected or Specific IP address entered in this field.Selecting ANY enables the rule for any IP in destination field.similarly WAN1 and WAN2 corresponds to respective wan interfaces.
QoS Priority	This setting determines the priority of a service, which in turn, determines the quality of that service for the traffic passing through the firewall. By default, the priority shown is that of the selected service. The user can change it accordingly. If the user does not make a selection (i.e, leaves it as None), then the native priority of the service will be applied to the policy. +5 is the highest priority. See "Quality of Service (QoS) Priorities" on page 7-14.
Log	This determines whether packets covered by this rule are logged. Select the desired action: • Always - always log traffic considered by this rule, whether it matches or not. This is useful when debugging your rules. • Never - never log traffic considered by this rule, whether it matches or not.

> → **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 FVS338 VPN firewall. Only enable those ports that are necessary for your network.

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 7-3:

Figure 7-3: Rule example: A Local Public Web Server

Inbound Rule Example: Allowing Videoconference from Restricted Addresses

If you want to allow incoming videoconferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office, you can create an inbound rule. In the example shown in Figure 7-4, CU-SeeMe connections are allowed only from a specified range of external IP addresses.

Figure 7-4: Rule example: Videoconference from Restricted Addresses

Considerations for Inbound Rules

- If your external IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires. Consider using the Dyamic DNS feature in the Advanced menus so that external users can always find your network.

- If the IP address of the local server PC is assigned by DHCP, it may change when the PC is rebooted. To avoid this, use the Reserved IP address feature in the LAN IP menu to keep the PC's IP address constant.

• Local PCs must access the local server using the PCs' local LAN address (192.168.0.99 in this example). Attempts by local PCs to access the server using the external WAN IP address will fail.

Outbound Rules (Service Blocking)

The FVS338 allows you to block the use of certain Internet services by PCs on your network. This is called service blocking or port filtering.

Figure 7-5: Add Outbound Service Rules screen

→ **Note:** See "Source MAC Filtering" on page 7-23 for yet another way to block outbound traffic from selected PCs that would otherwise be allowed by the firewall.

Table 7-2.   **Outbound Services**

Item	Description
Services	Select the desired Service or application to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see "Customized Services" on page 7-12).
Action	Select the desired action for outgoing connections covered by this rule: • BLOCK always • BLOCK by schedule, otherwise Allow • ALLOW always • ALLOW by schedule, otherwise Block **Note**: Any outbound traffic which is not blocked by rules you create will be allowed by the Default rule. ALLOW rules are only useful if the traffic is already covered by a BLOCK rule. That is, you wish to allow a subset of traffic that is currently blocked by another rule.
Select Schedule	Select the desired time schedule (i.e., Schedule1, Schedule2, or Schedule3) that will be used by this rule. • This drop down menu gets activated only when "BLOCK by schedule, otherwise Allow" or "ALLOW by schedule, otherwise Block" is selected as Action. • Use schedule page to configure the time schedules (see "Using a Schedule to Block or Allow Specific Traffic" on page 7-18).
LAN users	These settings determine which computers on your network are affected by this rule. Select the desired options: • Any - All PCs and devices on your LAN. • Single address - Enter the required address and the rule will be applied to that particular PC. • Address range - If this option is selected, you must enter the start and finish fields. • Groups- Select the Group you wish this rule to apply to. You can use the Network Database screen to assign PCs to Groups. See "Managing Groups and Hosts" on page 7-16.
WAN Users	These settings determine which Internet locations are covered by the rule, based on their IP address. Select the desired option: • Any - All Internet IP address are covered by this rule. • Single address - Enter the required address in the start fields. • Address range - If this option is selected, you must enter the start and finish fields.
QoS Priority	This setting determines the priority of a service, which in turn, determines the quality of that service for the traffic passing through the firewall. By default, the priority shown is that of the selected service. The user can change it accordingly. If the user does not make a selection (i.e, leaves it as None), then the native priority of the service will be applied to the policy. +5 is the highest priority. See "Quality of Service (QoS) Priorities" on page 7-14.

Table 7-2. **Outbound Services**

Item	Description
Log	This determines whether packets covered by this rule are logged. Select the desired action: • Always - always log traffic considered by this rule, whether it matches or not. This is useful when debugging your rules. • Never - never log traffic considered by this rule, whether it matches or not.

Outbound Rule Example: Blocking Instant Messenger

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

Figure 7-6: Rule example: Blocking Instant Messenger

Order of Precedence for Rules

As you define new rules, they are added to the tables in the Rules menu, as shown in Figure 7-7:

Figure 7-7: 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.

Customized Services

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

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application.

Although the FVS338 already holds a list of many service port numbers, you are not limited to these choices. Use the Services menu to add additional services and applications to the list for use in defining firewall rules. The Services menu shows a list of services that you have defined, as shown in Figure 7-8:

Figure 7-8: Services and Add Custom Service screens

To define a new service, first you must determine which port number or range of numbers is used by the application. This information can usually be determined by contacting the publisher of the application or from user groups of newsgroups. When you have the port number information, go the Services menu and click on the Add Custom Service button. The Add Services menu will appear, as shown in Figure 7-8.

To add a service:

1. Enter a descriptive name for the service so that you will remember what it is.

2. Select whether the service uses TCP or UDP as its transport protocol.
   If you can't determine which is used, select both.

3. Enter the lowest port number used by the service.

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

5. Click Apply.
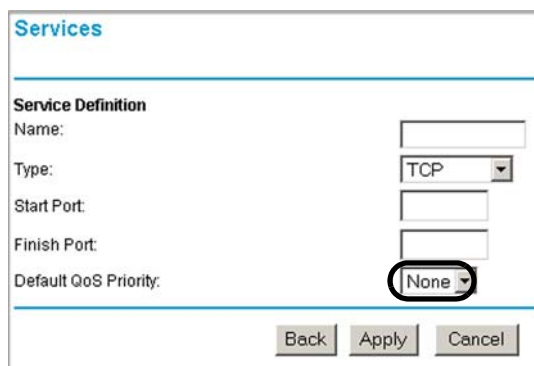
The new service will now appear in the Services menu, and in the Service name selection box in the Rules menu.

Quality of Service (QoS) Priorities

This setting determines the priority of a service, which in turn, determines the quality of that service for the traffic passing through the firewall. The user can change this priority:

• At the services definition screen for customized services

• On the inbound rules screen

• On the outbound rules screen

Services Add Screen
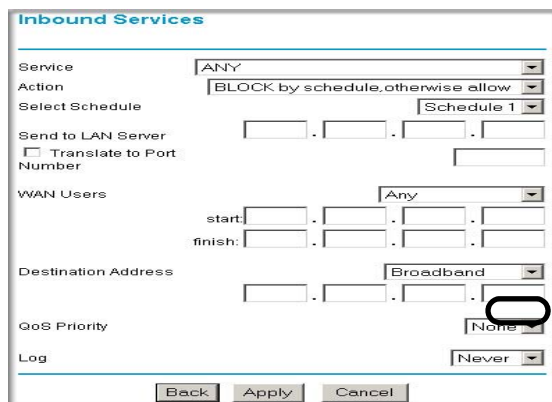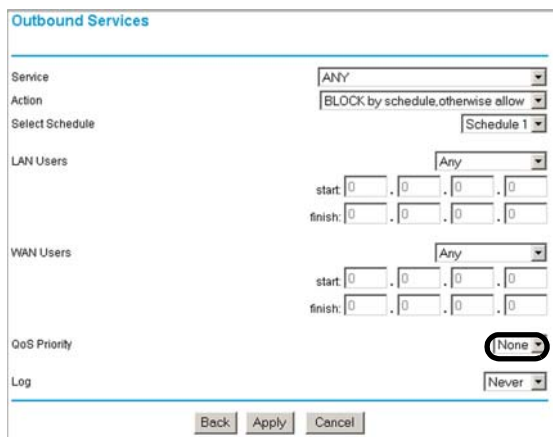
Inbound Rules Add Screen   **Outbound Rules Add Screen**

Figure 7-9: Setting and Overriding QoS priorities

The QoS priority definition for a service determines the queue that is used for its traffic passing through the FVS338 VPN firewall as follows:

Table 7-3.   Traffic queue to be used for a service

Native ToS Setting[*]	Netgear QoS Setting[†]					
	None	**6**	**5**	**4**	**3**	**2**
7 (highest)	7	6	5	4	3	2
6	6	6	5	4	3	2
5	5	6	5	4	3	2
4	4	6	5	4	3	2
3	3	6	5	4	3	2
2	2	6	5	4	3	2
1 (default)	1	6	5	4	3	2
0 (lowest)	0	6	5	4	3	2

[*] IEEE 802.1D-1998 (formerly 802.1p) standard.

[†] Specifies which output queue in the FVS338 to use for that service's traffic. The three type-of-service bits in the traffic frame remain unchanged.

Example 1 (priority unchanged): If the native ToS setting for a service is 3 and the Netgear QoS setting for this service is None, then the traffic for this service is placed in the queue that handles priority 3 traffic. The priority of this service through the FVS338 VPN firewall has not changed.

Example 2 (priority increased): If the native ToS setting for a service is 3 and the Netgear QoS setting for this service is 4, then the traffic for this service is placed in the queue that handles priority 4 traffic rather than the queue that handles priority 3 traffic. The priority of this service through the FVS338 VPN firewall has been increased.

Example 3 (priority decreased): If the native ToS setting for a service is 3 and the Netgear QoS setting for this service is 2, then the traffic for this service is placed in the queue that handles priority 2 traffic rather than the queue that handles priority 3 traffic. The priority of this service through the FVS338 VPN firewall has been decreased.

Managing Groups and Hosts

The Network Database is an automatically-maintained list of all known PCs and network devices. PCs and devices become known by the following methods:

- DHCP Client Requests—By default, the DHCP server in this Router is enabled, and will accept and respond to DHCP client requests from PCs and other network devices. These requests also generate an entry in the Network Database. Because of this, leaving the DHCP Server feature (on the LAN screen) enabled is strongly recommended.

- Scanning the Network—The local network is scanned using standard methods such as arp. This will detect active devices which are not DHCP clients. However, sometimes the name of the PC or device cannot be accurately determined, and will be shown as Unknown.

Advantages of the Network Database are as follows:

- Generally, you do not need to enter either IP address or MAC addresses. Instead, you can just select the desired PC or device.

- No need to reserve an IP address for a PC in the DHCP Server. All IP address assignments made by the DHCP Server will be maintained until the PC or device is removed from the database, either by expiry (inactive for a long time) or by you.

- No need to use a Fixed IP on PCs. Because the address allocated by the DHCP Server will never change, you don't need to assign a fixed IP to a PC to ensure it always has the same IP address.

- MAC-level Control over PCs. The Network Database uses the MAC address to identify each PC or device. So changing a PC's IP address does not affect any restrictions on that PC.

- Group and Individual Control over PCs

  – You can assign PCs to Groups and apply restrictions to each Group using the Firewall Rules screen (see "Services-Based Rules" on page 7-4).

  – You can also select the Groups to be covered by the Block Sites feature (see "Block Sites" on page 7-20).

  – If necessary, you can also create Firewall Rules to apply to a single PC (see "Source MAC Filtering" on page 7-23). Because the MAC address is used to identify each PC, users cannot avoid these restrictions by changing their IP address.

Network Database

Known PCs and Devices

	Name	IP Address	MAC Address	Group
○	Eng-temp	192.168.1.2	00:08:02:11:28:31	default ▼

Add Edit Delete

Apply Cancel Refresh Edit Group Names

Network Database Entry

Network Database Entry

Name: _____

IP Address Type: Reserved (DHCP Client) ▼

IP Address: ___ . ___ . ___ . ___

MAC Address: _____

Back Apply Cancel

Network Database Group Names

Group 1 default

Group 2 Marketing

Group 3 Sales

Group 4 Warehouse

Group 5 Support

Group 6 Lab1

Group 7 Lab2

Group 8 Others

Back Apply Cancel

Figure 7-10: Groups and Hosts screens

Table 7-4.   Groups and hosts

Item	Description
Known PCs and Devices	This table lists all current entries in the Network Database. For each PC or device, the following data is displayed. • Radio button—Use this to select a PC for editing or deletion. • Name—The name of the PC or device. Sometimes, this can not be determined, and will be listed as Unknown. In this case, you can edit the entry to add a meaningful name. • IP Address—The current IP address. For DHCP clients, where the IP address is allocated by the DHCP Server in this device, this IP address will not change. Where the IP address is set on the PC (as a fixed IP address), you may need to update this entry manually if the IP address on the PC is changed. • MAC Address—The MAC address of the PC. The MAC address is a low-level network identifier which is fixed at manufacture. • Group—Each PC or device must be in a single group. The Group column indicates which group each entry is in. By default, all entries are in the Default group (the D column.)
Operations	• Group Assignment —You can select a group for any entry by selecting the desired group from the drop down menu in the Group column. Click Apply • Adding a new Entry—If a PC is not connected, using a fixed IP, or a different LAN segment, it may not be listed. In this case, you can add it by clicking the Add button. • Editing an Entry—You can edit an entry by selecting its radio button, and clicking the Edit button. • Deleting an Entry—If a PC or device has been removed from your network, you can delete it from the database by selecting its radio button, and clicking the Delete button. • Edit Group Names—The Group names can be edited by clicking Edit Group Names button. By default the group names are Default, Marketing, Sales, Warehouse, Support, Lab1, Lab2, and Others.

Using a Schedule to Block or Allow Specific Traffic

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

Figure 7-11: Schedule menu

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

Note: 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.

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

Time Zone

The FVS338 VPN firewall uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet. In order to localize the time for your log entries, you must specify your Time Zone:

• Time Zone. Select your local time zone. This setting will be used for the blocking schedule and for time-stamping log entries.

• Daylight Savings Time. Check this box for daylight savings time.

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

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

Block Sites

If you want to reduce incoming traffic by preventing access to certain sites on the Internet, you can use the VPN firewall's content and Web component filtering feature. By default, this feature is disabled; all requested traffic from any Web site is allowed. When users try to access a blocked site, they will get a message: Blocked by NETGEAR.

• Keyword (and domain name) blocking—You can specify up to 32 words that, should they appear in the website name (i.e., URL) or in a newsgroup name, will cause that site or newsgroup to be blocked by the VPN firewall.

   You can apply the keywords to one or more groups. Requests from the PCs in the groups for which keyword blocking has been enabled will be blocked. Blocking does not occur for the PCs that are in the groups for which keyword blocking has not been enabled.

   You can bypass keyword blocking for trusted domains by adding the exact matching domain to the list of Trusted Domains. Access to the domains on this list by PCs even in the groups for which keyword blocking has been enabled will still be allowed without any blocking.

• Web component blocking—You can block the following Web component types: Proxy, Java, ActiveX, and Cookies. Sites on the Trusted Domains list are still subject to Web component blocking when the blocking of a particular Web component has been enabled.

The Block Sites menu is shown in :

Block Sites

Web Components
- ☐ Proxy
- ☐ ActiveX
- ☐ Java
- ☐ Cookies

Keyword Blocking
☐ Turn keyword blocking on

[   ]

Add Keyword

Block sites containing these keywords or domain names:

[   ]

Delete Keyword   Delete All

Apply Keyword Blocking to:
- ☑ default
- ☐ Marketing
- ☐ Sales
- ☐ Warehouse
- ☐ Support
- ☐ Lab1
- ☐ Lab2
- ☐ Others

Trusted Domains

[   ]

Add Trusted Domain

Allow these domains without any filtering:

[   ]

Delete Trusted Domain   Delete All

Apply   Cancel

Figure 7-12: Block Sites menu

Table 7-5. **Block Sites**

Item	Description
Web Component Blocking	Select Proxy, Java, ActiveX and Cookies to enable respective content filtering. **Example**: By enabling Java filtering *.java files will be blocked. **Note**: Keywords are always blocked.
To block keywords or Internet domains:	• Select the Turn keyword blocking on check box. • Type a keyword or domain name in the Add Keyword box, click Add Keyword button. The word or domain name appears in the list below. Any number of domain names and keywords can be added to the list. • To delete a keyword or domain name: Select the word or domain name in the list, click Delete Keyword button. • To delete all keywords: Click Delete All button to delete all the Keywords from the list.
Groups	Select the groups specified below the Apply Keyword blocking to tab to enable keyword blocking for those groups. The Request from the PC's that are in the group for which Keyword filtering is enabled will undergo the Filtering process. Otherwise the filtering does not apply. See "Managing Groups and Hosts" on page 7-16.
Trusted Domains	• In the Trusted Domains box, enter the exact matching domain name for which the keyword filtering will be bypassed. **Example**: Enter www.netgear.com to bypass URL keyword filtering for this domain. The domains in this list will be allowed without any filtering, web component filtering still applies. Click on Add Trusted Domains button. The domain name appears in the list below. Any number of domain names can be added to the list. • To delete a Domain name: Select the word or domain name in the list. Click Delete Trusted Domain button. • To delete all domain names: Click Delete All button.

Keyword application examples:

• If the keyword "XXX" is specified, the URL <http://www.badstuff.com/xxx.html> is blocked, as is the newsgroup alt.pictures.XXX.

• If the keyword ".com" is specified, only websites with other domain suffixes (such as .edu or .gov) can be viewed.

• If you wish to block all Internet browsing access, enter the keyword ".".

Source MAC Filtering

Source MAC Filter will drop the Internet-bound traffic received from the PCs with the specified MAC address.

- By default, the source MAC address filter is disabled. All the traffic received from PCs with any MAC address is allowed by default.

- When enabled, Internet-bound traffic will be dropped from the PCs that have the configured MAC addresses.

Figure 7-13: Source MAC Filter screens

→ **Note:** For additional ways of restricting outbound traffic, see "Outbound Rules (Service Blocking)" on page 7-9.

Table 7-6.   **Source MAC address filter**

Item	Description
Activation	• Enable the source MAC filter by ticking the check box. • Press APPLY.

Add	• Now add the MAC Addresses from which the traffic should be dropped by clicking on ADD button.
	   Each time one MAC Address entry can be added.
	   MAC Address input should be entered with ':' seperator. A valid MAC address will have 0 to 9 and A to F.
	   Example: 00:e0:4c:69:0a:11
	• Press APPLY.
	   Now the traffic from the specified MAC addresses will be dropped.

Disable	• To Disable Source MAC Filter, uncheck Source MAC Filter Enable check box. The list of the MAC Addresses can be kept in the database. • If the filter has to be avoided for a specific MAC address in the database, select the MAC address entry and click on Delete button.

Port Triggering

Port triggering allows some applications to function correctly that would otherwise be partially blocked by the firewall. Using this feature requires that you know the port numbers used by the Application.

Once configured, operation is as follows:

• A PC makes an outgoing connection using a port number defined in the Port Triggering table.

• This Router records this connection, opens the additional INCOMING port or ports associated with this entry in the Port Triggering table, and associates them with the PC.

• The remote system receives the PCs request and responds using the different port numbers that you have now opened.

• This Router matches the response to the previous request, and forwards the response to the PC.

   Without Port Triggering, this response would be treated as a new connection request rather than a response. As such, it would be handled in accordance with the Port Forwarding rules.

• Only 1 PC can use a Port Triggering application at any time.

• After a PC has finished using a Port Triggering application, there is a Time-out period before the application can be used by another PC. This is required because this Router cannot be sure when the application has terminated.

> **Note:** For additional ways of allowing inbound traffic, see "Inbound Rules (Port Forwarding)" on page 7-5.

Figure 7-14: Port Triggering screens

Table 7-7. **Port Triggering**

Item	Description
Port Triggering Rules	• Enable - Indicates if the rule is enabled or disabled. Generally, there is no need to disable a rule unless it interferes with some other function such as Port Forwarding. • Name - The name for this rule. • Outgoing Ports - The port or port range for outgoing traffic. An outgoing connection using one of these ports will trigger this rule. • Incoming Ports - The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC which triggered this rule.
Adding a new Rule	• To add a new rule, click the Add and enter the following data on the resulting screen. • Name - enter a suitable name for this rule (e.g., the name of the application) • Enable/Disable - select the desired option. • Outgoing (Trigger) Port Range - enter the range of port numbers used by the application when it generates an outgoing request. • Incoming (Response) Port Range - enter the range of port numbers used by the remote system when it responds to the PC's request.
Modifying or Deleting an existing Rule:	• Select the desired rule by clicking the radio button beside the rule. • Click Edit or Delete as desired.
Checking Operation and Status	To see which rules are currently being used, click the Status button. The following data will be displayed: • Rule - the name of the Rule. • LAN IP Address - The IP address of the PC currently using this rule. • Open Ports - the Incoming ports which are associated the this rule. Incoming traffic using one of these ports will be sent to the IP address above. • Time Remaining - The time remaining before this rule is released, and thus available for other PCs. This timer is restarted whenever incoming or outgoing traffic is received.

Getting E-Mail Notifications of Event Logs and Alerts

Your router will log security-related events such as denied incoming service requests, hacker probes, and administrator logins, according to your settings on this screen.

If you have set up content filtering on the Block Sites page (see "Block Sites" on page 7-20), you can also log when someone on your network tried to access a blocked site.

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

Figure 7-15: Logs and E-mail screens

Click on View Log button to view various log messages generated by the Router.

- In view log window To delete all log entries: Click Clear Log.

- To see the most recent entries: Click Refresh.

- To E-mail the log messages now: Click Send Log.

Log Identifier is a mandatory field to identify the log messages. This ID appended to log messages.

Items to include in the log:

- Use these checkboxes to determine which events are included in the log. Selecting all events will increase the size of the log, so it is good practice to disable any events which are not really required.

- Selecting an event under Include In Log will enable logging of messages pertaining to that event. Ex: Selecting Admin Login, will enable generation of log messages whenever Admin logs in.

- Selecting an event under Include In Alerts will enable logging of messages pertaining to that event. This category typically contains Internet Attack events. Ex: Selecting SYN Flood, will enable generation of Alert messages whenever SYN Flood occurs.

Emailing logs:

- If you have Email Logs enabled, you'll receive these logs in an Email message.

- To receive alerts and logs by e-mail you have to enable Email Logs option.

  – In the Respond to Identd from SMTP Server check this box to respond to IDENT protocol.

  – In the Email Server address Enter E-mail outgoing SMTP mail server of your ISP (for example, 172.16.1.10).

  – If you leave this box blank, no alerts or logs will be sent to you.

  – In the Return Email Address box, type the user's e-mail address.

  – In the Log / Alert Email box, type the e-mail address where the logs and alerts will be sent. Use a full e-mail address (for example, ChrisXY@myISP.com).

  – In the Authenticate with SMTP server Check this box to enable authentication for alerts and logs.

  – In the User Name Box, fill the user name for SMTP authentication.

  – In the Password Box, fill the password for SMTP authentication.

Syslog—Enable or disable as required:

- Disable - Select this if you don't have a Syslog server.

- Enable - Syslog server IP address - If your Syslog server has a fixed IP address, select this option, and enter the IP address of your Syslog server and select appropriate syslog facility.

Message length and frequency:

- In the Log Queue Length box, set the logs queue length.

- In the Log Threshold Time box, set the logs Threshold time.

- In the Alert Queue Length box, set the alerts queue length.

Click Apply to have your changes take effect.

Syslog

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

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

Viewing Logs of Web Access or Attempted Web Access

The firewall will log security-related events such as denied incoming and outgoing service requests, hacker probes, and administrator logins.

- If you enable content filtering in the Block Sites menu, the Log page will also show you when someone on your network tried to access a blocked site.

- If you enabled e-mail notification, you'll receive these logs in an e-mail message.

- If you don't have e-mail notification enabled, you can view the logs here.

An example is shown in Figure 7-16. Log entries are described in Table 7-8 and log action buttons are described in Table 7-9.
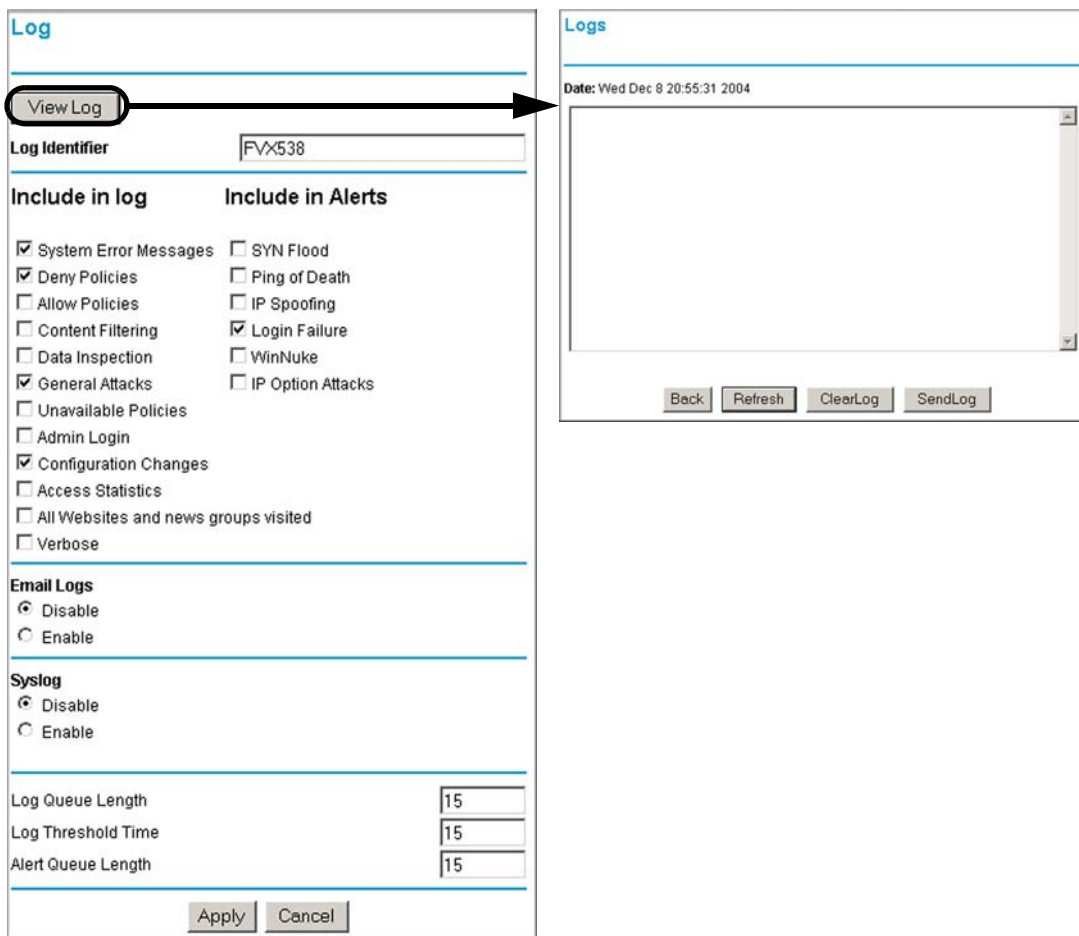
Figure 7-16: Firewall Logs menu

Table 7-8.   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.

Table 7-8. **Log entry descriptions**

Field	Description
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.

Table 7-9. **Log action buttons**

Field	Description
Refresh	Click this button to refresh the log screen.
Clear Log	Click this button to clear the log entries.
Send Log	Click this button to email the log immediately.

Administrator Information

Consider the following operational items:

1. As an option, you can enable remote management if you have to manage distant sites from a central location (see "Enabling Remote Management Access" on page 9-9).

2. Although rules (see "Using Rules to Block or Allow Specific Kinds of Traffic" on page 7-1) is the basic way of managing the traffic through your system, you can further refine your control with the following optional features of the FVS338 VPN firewall:

   – Groups and hosts (see "Managing Groups and Hosts" on page 7-16)

   – Services (see "Services-Based Rules" on page 7-4)

   – Schedules (see "Using a Schedule to Block or Allow Specific Traffic" on page 7-18)

   – Block sites (see "Block Sites" on page 7-20)

   – Source MAC filtering (see "Source MAC Filtering" on page 7-23)

   – Port triggering (see "Port Triggering" on page 7-24)

Chapter 8
Virtual Private Networking

This chapter describes how to use the virtual private networking (VPN) features of the FVS338 VPN firewall. VPN tunnels provide secure, encrypted communications between your local network and a remote network or computer.

Tip: When using dual WAN port networks, use the VPN Wizard to configure the basic parameters and them edit the VPN and IKE Policy screens for the various VPN scenarios.

Fully Qualified Domain Names

See "Configure Dynamic DNS (If Needed)" on page 4-16 for the procedure on how to select and configure the Dynamic DNS service.

Creating a VPN Connection: Between FVX538 and FVS338

This section describes how to configure a VPN connection between a NETGEAR FVX538 VPN Firewall and a NETGEAR FVS338 VPN Firewall.
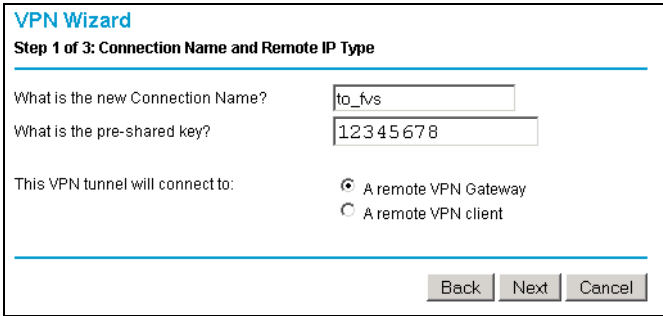
Using each firewall's VPN Wizard, we will create a set of policies (IKE and VPN) that will allow the two firewalls to connect from locations with fixed IP addresses. Either firewall can initiate the connection.

This procedure was developed and tested using:

- Netgear FVX538 VPN Firewall with version 1.6.11 firmware
    - WAN1 IP address is 10.1.0.118
    - LAN IP address subnet is 192.168.1.1 255.255.255.0
- Netgear FVS338 VPN Firewall with version 1.6.7 firmware
    - WAN IP address is 10.1.1.150
    - LAN IP address subnet is 192.168.2.1 255.255.255.0

January 2005

Configuring the FVX538
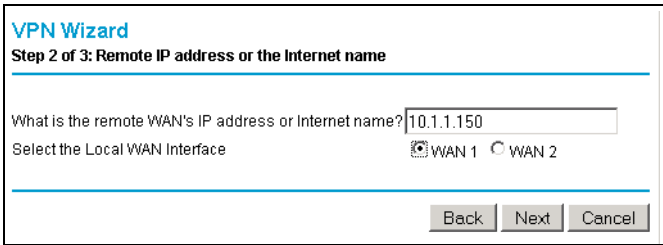
1. Select the VPN Wizard

2. Give the client connection a name, such as **to_fvs**.

3. Enter a value for the pre-shared key.

4. Select 'a remote VPN gateway'.

VPN Wizard

Step 1 of 3: Connection Name and Remote IP Type

What is the new Connection Name?   to_fvs

What is the pre-shared key?   12345678

This VPN tunnel will connect to: ⦿ A remote VPN Gateway

                                        ○ A remote VPN client

Back   Next   Cancel

Figure 8-1: VPN Wizard start page

5. Click Next.

6. Enter the WAN IP address of the remote FVS338.

7. Click WAN1 to bind this connection to the WAN1 port.

VPN Wizard

Step 2 of 3: Remote IP address or the Internet name

What is the remote WAN's IP address or Internet name? 10.1.1.150

Select the Local WAN Interface   ⦿ WAN 1   ○ WAN 2

Back   Next   Cancel

Figure 8-2: WAN IP address of remote FVS338

8. Click Next.

January 2005

9. Enter the LAN IP address and subnet mask of the remote FVS338.

VPN Wizard
Step 3 of 3: Secure Connection Remote Accessibility

What is the **remote** LAN IP address and Subnet Mask?

IP Address: 192 . 168 . 2 . 0
Subnet Mask: 255 . 255 . 255 . 0

Back   Next   Cancel

Figure 8-3: LAN IP address and subnet mask of remote FVX538

10. Click Next.

11. Click Done to create the 'to_fvs' IKE and VPN policies.

In the IKE Policies menu, the 'to_fvs' IKE policy will appear in the table.

IKE Policies

Policy Table

	#	Name	Mode	Local ID	Remote ID	Encr	Auth	DH
○	1	to_fvs	Main	10.1.0.118	10.1.1.150	3DES	SHA1	Group 2 (1024 Bit)

Add   Edit   Delete

Figure 8-4: IKE Policies

12. You can view the IKE parameters by selecting 'to_fvs' and clicking Edit. It should not be necessary to make any changes.

Figure 8-5: FVX538-to-FVS338 IKE screen

13. In the VPN Policies menu, the 'to_fvs' VPN policy will appear in the table.

Figure 8-6: FVX538 VPN Policies screen

14. You can view the VPN parameters by selecting 'to_fvs' and clicking Edit. It should not be necessary to make any changes.

Figure 8-7: FVX538-to-FVS338 VPN screen

Configuring the FVS338

1. Select the VPN Wizard

2. Give the client connection a name, such as **to_fvx**.

3. Enter a value for the pre-shared key.
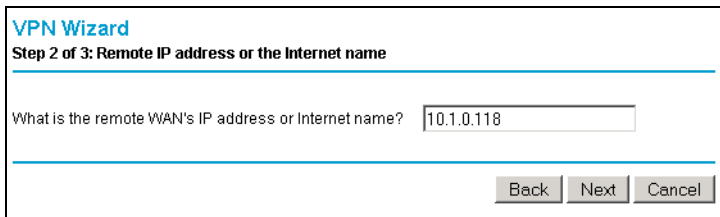
4.   Select 'a remote VPN gateway'.

VPN Wizard

Step 1 of 3: Connection Name and Remote IP Type

What is the new Connection Name?   to_fvx

What is the pre-shared key?   12345678

This VPN tunnel will connect to: ◉ A remote VPN Gateway
                                          ○ A remote VPN client

                                          Back   Next   Cancel

Figure 8-8: VPN Wizard start page

5.   Click Next.

6.   Enter the WAN IP address of the remote FVX538.
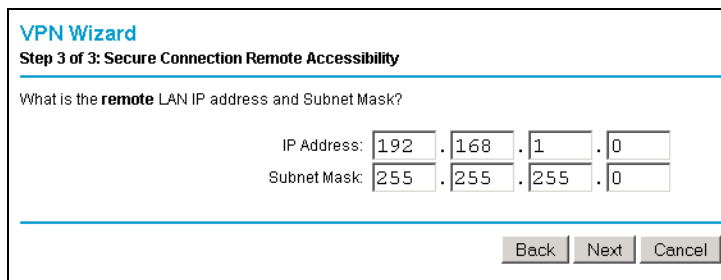
VPN Wizard

Step 2 of 3: Remote IP address or the Internet name

What is the remote WAN's IP address or Internet name?   10.1.0.118

                                          Back   Next   Cancel

Figure 8-9: WAN IP address of remote FVX538

7.   Click Next.

January 2005

8. Enter the LAN IP address and subnet mask of the remote FVX538.

VPN Wizard
Step 3 of 3: Secure Connection Remote Accessibility

What is the **remote** LAN IP address and Subnet Mask?

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

Back | Next | Cancel

Figure 8-10: LAN IP address and subnet mask of remote FVX538

9. Click Next.

10. Click Done to create the 'to_fvx' IKE and VPN policies.

Testing the Connection

1. From a PC on either firewall's LAN, try to ping a PC on the other firewall's LAN. Establishing the VPN connection may take several seconds.

2. For additional status and troubleshooting information, view the VPN log and status menu in the FVX538 or FVS338.

Creating a VPN Connection: Netgear VPN Client to FVS338

This section describes how to configure a VPN connection between a Windows PC and the FVS338 VPN firewall.

Using the FVS338's VPN Wizard, we will create a single set of policies (IKE and VPN) that will allow up to 50 remote PCs to connect from locations in which their IP addresses are unknown in advance. The PCs may be directly connected to the Internet or may be behind NAT routers. If more PCs are to be connected, an additional policy or policies must be created.
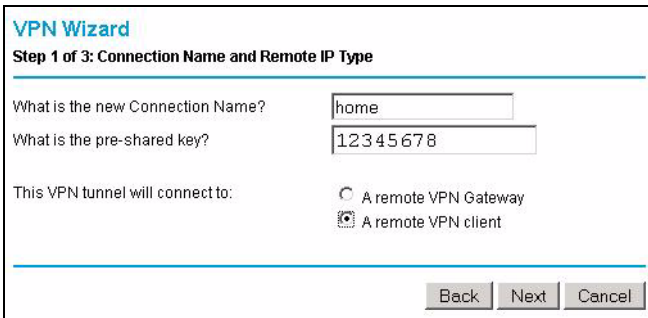
Each PC will use Netgear's VPN Client. Since the PC's IP address is assumed to be unknown, the PC must always be the Initiator of the connection.

This procedure was developed and tested using:

- Netgear FVS338 ProSafe VPN Firewall 50 with version 1.6.11 firmware
- Netgear VPN Client version 10.3.5 (Build 6)
- NAT router: Netgear FR114P with version 1.5_09 firmware

Configuring the FVS338

1. Select the VPN Wizard
2. Give the client connection a name, such as **home**.
3. Enter a value for the pre-shared key.
4. Select 'a remote VPN client'.

Figure 8-11: VPN Wizard

5. Click Next to go to the summary page.
6. Click Done to create the 'home' IKE and VPN policies.

Configuring the VPN Client

1. Right-click on the VPN client icon ⬛ in your Windows toolbar and select the Security Policy Editor.

2. In the upper left of the Policy Editor window, click the New Document icon to open a New Connection.
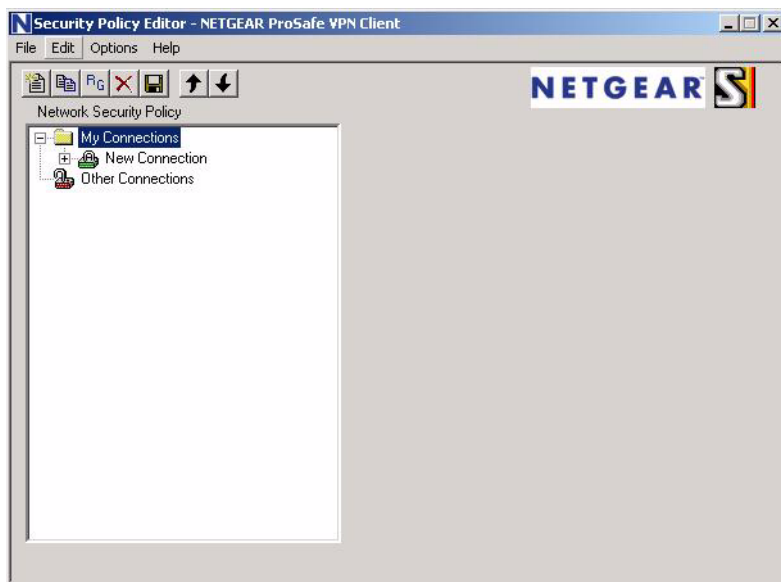
Figure 8-12: New Client Connection screen

January 2005

3. Give the New Connection a name, such as **to_FVS**.
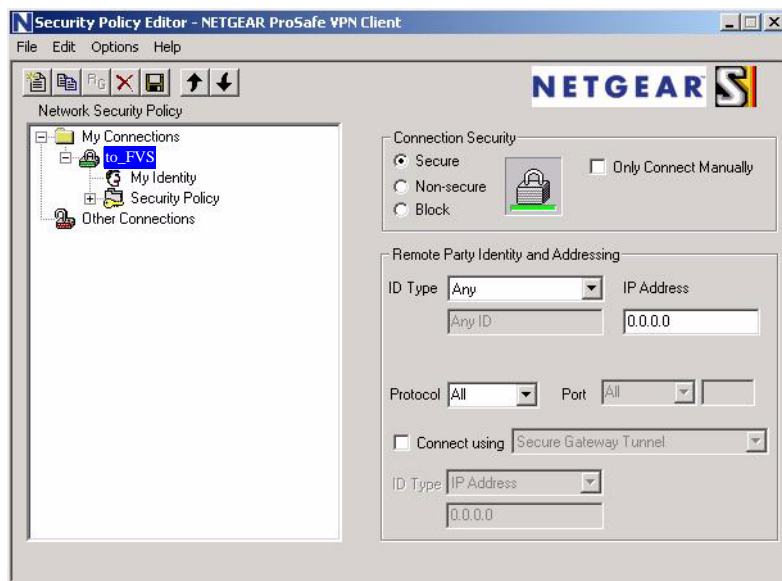
Figure 8-13: New connection named

4. In the Remote Party Identity section, select ID Type of IP Subnet.

5. Enter the LAN IP Subnet Address and Subnet Mask of the FVS338's LAN.

6. Select 'Connect using Secure Gateway Tunnel'.

7. Under ID Type, select 'Domain Name' and 'Gateway IP Address'.

8. For Domain Name, enter 'fvs_local.com' and enter the WAN IP Address of the FVS338.
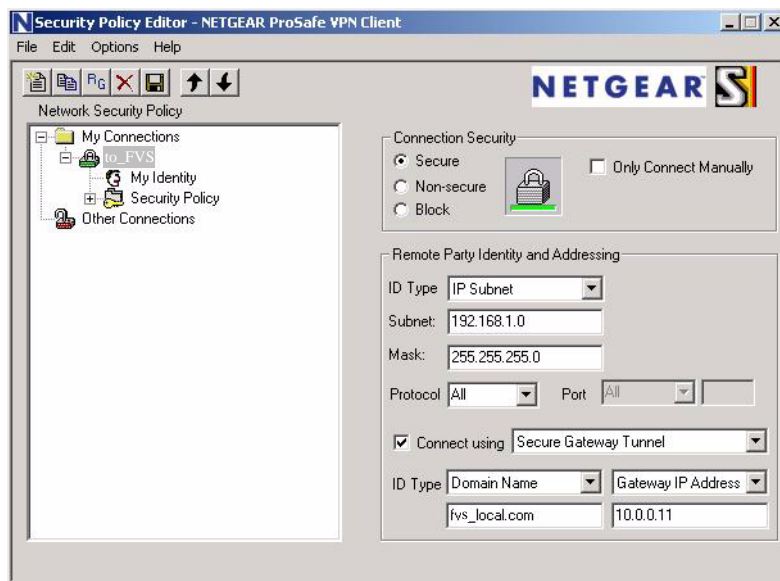
Figure 8-14: Remote client info

9. In the left frame, click on My Identity.

10. Select Certificate = None.

11. Under ID Type, select 'Domain Name'.

   The value entered under Domain Name will be of the form '<name><XY>.fvs_remote.com', where each user must use a different variation on the Domain Name entered here. The <name> is the policy name used in the FVS338 configuration. In this example, it is 'home'. X and Y are an arbitrary pair of numbers chosen for each user.

   Note: X may not be zero!

   In this example, we have entered home11.fvs_remote.com. Up to fifty user variations can be served by one policy.

12. Leave Virtual Adapter disabled, and select your computer's Network Adapter. Your current IP address will appear.
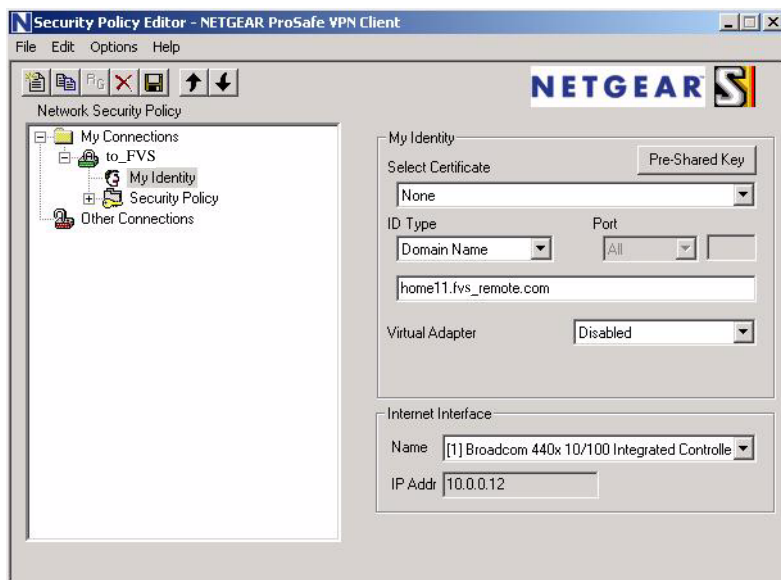
Figure 8-15: My Identity screen

13. Before leaving the My Identity menu, click the Pre-Shared Key button.

14. Click Enter Key, type your preshared key, and click OK.

This key will be shared by all users of the FVS338 policy "home".

Figure 8-16: Pre-shared key

15. In the left frame, click on Security Policy.

16. Select Phase 1 Negotiation Mode = Aggressive Mode.

PFS should be disabled, and Replay Detection should be enabled.
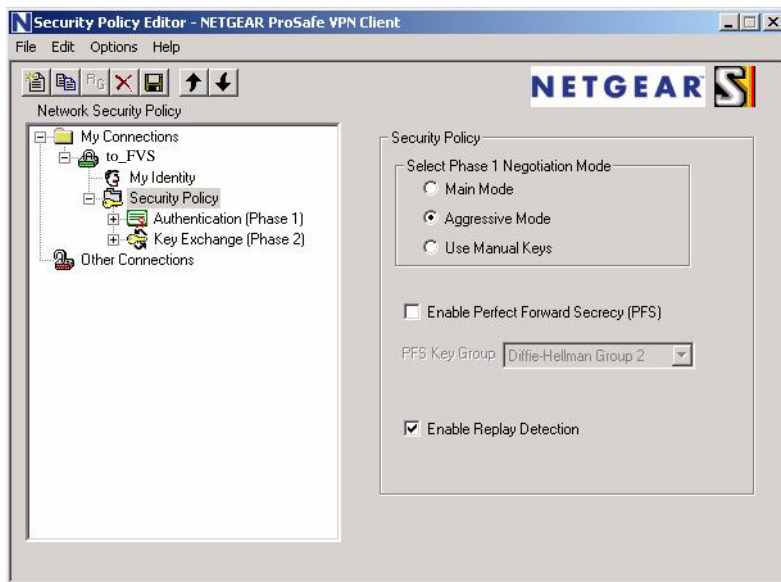
Figure 8-17: Client Security Policy screen

17. In the left frame, expand Authentication and select Proposal 1.

Compare with the figure below. No changes should be necessary.
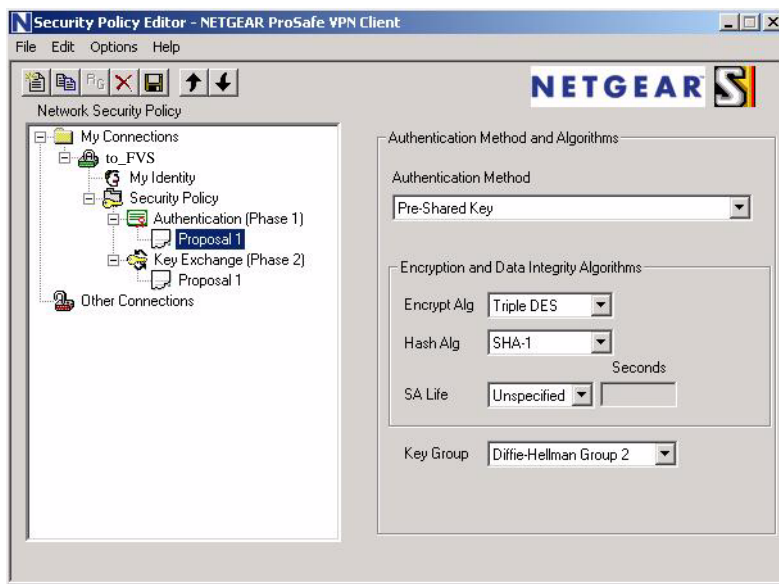
Figure 8-18: Client Authorization screen

18. In the left frame, expand Key Exchange and select Proposal 1.

Compare with the figure below. No changes should be necessary.
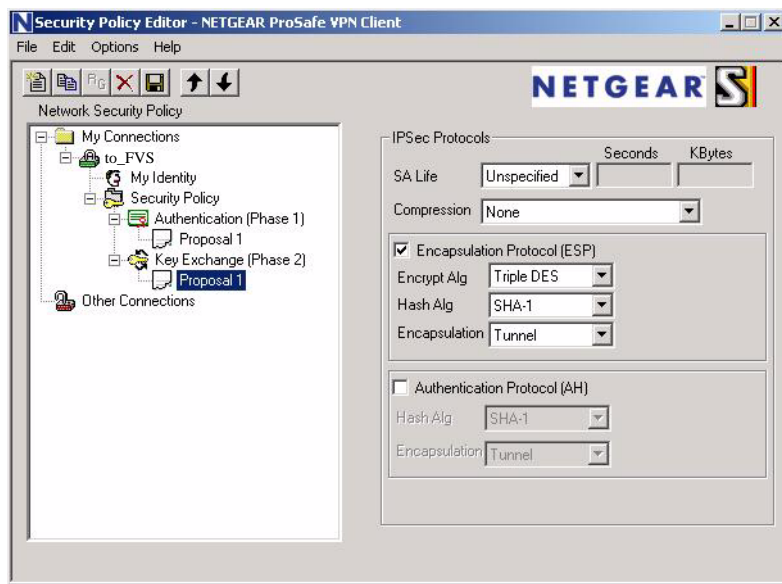
Figure 8-19: Client Key Exchange screen

19. In the upper left of the window, click the disk icon to save the policy.

Testing the Connection

20. Right-click on the VPN client icon ⛊ in your Windows toolbar and select "Connect...", then "My Connections\to_FVS".

Within 30 seconds you should receive a message "Successfully connected to My Connections\to_FVS" and the VPN client icon in the toolbar should say On: ⛊

21. For additional status and troubleshooting information, right-click on the VPN client icon ⑤ in your Windows toolbar and select "Connection Monitor" or "Log Viewer", or view the VPN log and status menu in the FVS338.
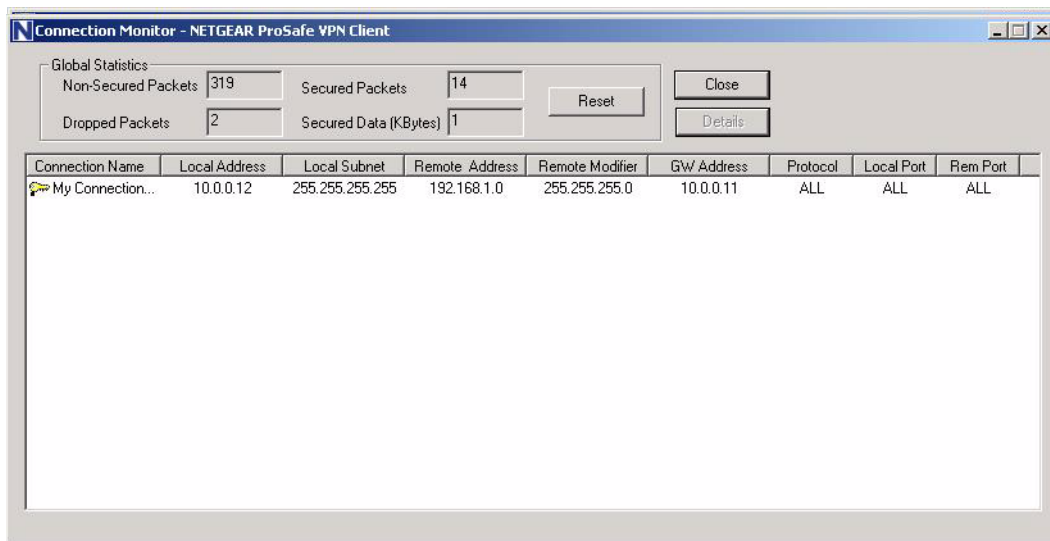
Figure 8-20: Client Connection Monitor screen

Chapter 9
Router and Network Management

This chapter describes how to use the network management features of your FVS338 ProSafe VPN Firewall 50. These features can be found by clicking on the appropriate heading in the Main Menu of the browser interface.

The FVS338 ProSafe VPN Firewall 50 offers many tools for managing the network traffic to optimize its performance. You can also control administrator access, be alerted to important events requiring prompt action, monitor the firewall status, perform diagnostics, and manage the firewall configuration file.

Performance Management

Performance management consists of controlling the traffic through the FVS338 VPN firewall so that the necessary traffic gets through when there is a bottleneck and either reducing unnecessary traffic or rescheduling some traffic to low-peak times to prevent bottlenecks from occurring in the first place. The FVS338 VPN firewall has the necessary features and tools to help the network manager accomplish these goals.

Bandwidth Capacity

The maximum bandwidth capacity of the FVS338 VPN firewall in each direction is as follows:

*   LAN side: 800 Mbps (eight LAN ports at 100 Mbps each)

*   WAN side: 100 Mbps (rollover mode, active broadband WAN port at 100 Mbps)

In practice, the WAN side bandwidth capacity will be much lower when DSL or cable modems are used to connect to the Internet. At 1.5 Mbps, the broadband WAN port will support a traffic rate of 1.5 Mbps (active broadband WAN port at 1.5 Mbps). After a rollover, the serial dial-up WAN port bandwidth will be much lower.

As a result and depending on the traffic being carried, the WAN side of the firewall will be the limiting factor to throughput for most installations.

January 2005

VPN Firewall Features That Reduce Traffic

Features of the VPN firewall that can be called upon to decrease WAN-side loading are as follows:

• Service blocking
• Block sites
• Source MAC filtering

Service Blocking

Note: This feature is for Advanced Administrators only! Incorrect configuration will cause serious problems.

You can control specific outbound traffic (i.e., from LAN to WAN and from DMZ to WAN). Outbound Services lists all existing rules for outbound traffic. If you have not defined any rules, only the default rule will be listed. The default rule allows all outgoing traffic.

Each rule lets you specify the desired action for the connections covered by the rule:

• BLOCK always
• BLOCK by schedule, otherwise Allow
• ALLOW always
• ALLOW by schedule, otherwise Block

As you define your firewall rules, you can further refine their application according to the following criteria:

• LAN users—These settings determine which computers on your network are affected by this rule. Select the desired options:

    – Any: All PCs and devices on your LAN.

    – Single address: The rule will be applied to the address of a particular PC.

    – Address range: The rule is applied to a range of addresses.

    – Groups: The rule is applied to a Group (you use the Network Database to assign PCs to Groups—see "Groups and Hosts" on page 9-3).

• WAN Users—These settings determine which Internet locations are covered by the rule, based on their IP address.

    – Any: The rule applies to all Internet IP address.

    – Single address: The rule applies to a single Internet IP address.

– Address range: The rule is applied to a range of Internet IP addresses.

• Services—You can specify the desired Services or applications to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see "Services" on page 9-3).

• Schedule—You can specify whether the rule is to be applied on the Schedule 1, Schedule 2, or Schedule 3 time schedule (see "Schedule" on page 9-3).

See "Using Rules to Block or Allow Specific Kinds of Traffic" on page 7-1 for the procedure on how to use this feature.

Services

The Rules menu contains a list of predefined Services for creating firewall rules. If a service does not appear in the predefined Services list, you can define the service. The new service will then appear in the Rules menu's Services list.

See "Services-Based Rules" on page 7-4 for the procedure on how to use this feature.

Groups and Hosts

You can apply these rules selectively to groups of PCs to reduce the outbound or inbound traffic. The Network Database is an automatically-maintained list of all known PCs and network devices. PCs and devices become known by the following methods:

• DHCP Client Request—By default, the DHCP server in this Router is enabled, and will accept and respond to DHCP client requests from PCs and other network devices. These requests also generate an entry in the Network Database. Because of this, leaving the DHCP Server feature (on the LAN screen) enabled is strongly recommended.

• Scanning the Network—The local network is scanned using standard methods such as arp. This will detect active devices which are not DHCP clients. However, sometimes the name of the PC or device cannot be accurately determined, and will be shown as Unknown.

See "Managing Groups and Hosts" on page 7-16 for the procedure on how to use this feature.

Schedule

If you have set firewall rules on the Rules screen, you can configure three different schedules (i.e., schedule 1, schedule 2, and schedule 3) for when a rule is to be applied. Once a schedule is configured, it affects all Rules that use this schedule. You specify the days of the week and time of day for each schedule.

See "Using a Schedule to Block or Allow Specific Traffic" on page 7-18 for the procedure on how to use this feature.

Block Sites

If you want to reduce traffic by preventing access to certain sites on the Internet, you can use the VPN firewall's filtering feature. By default, this feature is disabled; all requested traffic from any Web site is allowed.

- Keyword (and domain name) blocking—You can specify up to 32 words that, should they appear in the website name (i.e., URL) or in a newsgroup name, will cause that site or newsgroup to be blocked by the VPN firewall.

  You can apply the keywords to one or more groups. Requests from the PCs in the groups for which keyword blocking has been enabled will be blocked. Blocking does not occur for the PCs that are in the groups for which keyword blocking has not been enabled.

  You can bypass keyword blocking for trusted domains by adding the exact matching domain to the list of Trusted Domains. Access to the domains on this list by PCs even in the groups for which keyword blocking has been enabled will still be allowed without any blocking.

- Web component blocking—You can block the following Web component types: Proxy, Java, ActiveX, and Cookies. Sites on the Trusted Domains list are still subject to Web component blocking when the blocking of a particular Web component has been enabled.

See "Block Sites" on page 7-20 for the procedure on how to use this feature.

Source MAC Filtering

If you want to reduce outgoing traffic by preventing Internet access by certain PCs on the LAN, you can use the source MAC filtering feature to drop the traffic received from the PCs with the specified MAC addresses. By default, this feature is disabled; all traffic received from PCs with any MAC address is allowed.

See "Source MAC Filtering" on page 7-23 for the procedure on how to use this feature.

VPN Firewall Features That Increase Traffic

Features that tend to increase WAN-side loading are as follows:

- Port forwarding
- Port triggering
- Exposed hosts

• VPN tunnels

Port Forwarding

The firewall always blocks DoS (Denial of Service) attacks. A DoS attack does not attempt to steal data or damage your PCs, but overloads your Internet connection so you can not use it (i.e., the service is unavailable). You can also create additional firewall rules that are customized to block or allow specific traffic.

Note: This feature is for Advanced Administrators only! Incorrect configuration will cause serious problems.

You can control specific inbound traffic (i.e., from WAN to LAN and from WAN to DMZ). Inbound Services lists all existing rules for inbound traffic. If you have not defined any rules, only the default rule will be listed. The default rule blocks all inbound traffic.

Each rule lets you specify the desired action for the connections covered by the rule:

• BLOCK always
• BLOCK by schedule, otherwise Allow
• ALLOW always
• ALLOW by schedule, otherwise Block

You can also enable a check on special rules:

• VPN Passthrough—Enable this to pass the VPN traffic without any filtering, specially used when this firewall is between two VPN tunnel end points.

• Drop fragmented IP packets—Enable this to drop the fragmented IP packets.

• UDP Flooding—Enable this to limit the number of UDP sessions created from one LAN machine.

• TCP Flooding—Enable this to protect the router from Syn flood attack.

• Enable DNS Proxy—Enable this to allow the incoming DNS queries.

• Enable Stealth Mode—Enable this to set the firewall to operate in stealth mode.

As you define your firewall rules, you can further refine their application according to the following criteria:

• LAN users—These settings determine which computers on your network are affected by this rule. Select the desired IP Address in this field.

- WAN Users—These settings determine which Internet locations are covered by the rule, based on their IP address.

  – Any: The rule applies to all Internet IP address.

  – Single address: The rule applies to a single Internet IP address.

  – Address range: The rule is applied to a range of Internet IP addresses.

- Destination Address—These settings determine the destination IP address for this rule which will be applicable to incoming traffic, this rule will be applied only when the destination IP address of the incoming packet matches the IP address of the WAN interface selected or Specific IP address entered in this field.Selecting ANY enables the rule for any IP in destination field.similarly WAN1 and WAN2 corresponds to respective wan interfaces.

- Services—You can specify the desired Services or applications to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see "Services" on page 9-3).

- Schedule—You can specify whether the rule is to be applied on the Schedule 1, Schedule 2, or Schedule 3 time schedule (see "Schedule" on page 9-3).

See "Using Rules to Block or Allow Specific Kinds of Traffic" on page 7-1 for the procedure on how to use this feature.

Port Triggering

Port triggering allows some applications to function correctly that would otherwise be partially blocked by the firewall. Using this feature requires that you know the port numbers used by the Application.

Once configured, operation is as follows:

- A PC makes an outgoing connection using a port number defined in the Port Triggering table.

- This Router records this connection, opens the additional INCOMING port or ports associated with this entry in the Port Triggering table, and associates them with the PC.

- The remote system receives the PCs request and responds using the different port numbers that you have now opened.

- This Router matches the response to the previous request and forwards the response to the PC. Without Port Triggering, this response would be treated as a new connection request rather than a response. As such, it would be handled in accordance with the Port Forwarding rules.

  – Only one PC can use a Port Triggering application at any time.

– After a PC has finished using a Port Triggering application, there is a time-out period before the application can be used by another PC. This is required because the firewall cannot be sure when the application has terminated.

See "Port Triggering" on page 7-24 for the procedure on how to use this feature.

Exposed Hosts

The exposed host feature can only be used if your ISP has allocated you multiple fixed Internet IP addresses.

> **Note:** Exposed hosts are sometimes referred to as DMZ hosts. Unlike hardware-based DMZ ports, however, exposed hosts are implemented in software and do not enjoy the same level of firewall protection that hardware-based DMZ ports do. Use the exposed host feature at your own risk.

In this situation, you can define a separate DMZ server for each internet IP address.

• All incoming traffic to that IP address will be sent to the selected PC.

• Out-going traffic from the selected PC will use the IP address you entered, not the default WAN IP address.

See "Single or Multiple Exposed Hosts" on page 3-2 for the conditions when you can use exposed hosts in dual WAN port networks.

See "One-to-One NAT Mapping" on page 6-8 for the procedure on how to use this feature.

VPN Tunnels

The VPN firewall permits up to 200 VPN tunnels at a time. Each tunnel requires extensive processing for encryption and authentication.

See Chapter 8, "Virtual Private Networking" for the procedure on how to use this feature.

Using QoS to Shift the Traffic Mix

The QoS priority settings determine the priority and, in turn, the quality of service for the traffic passing through the firewall. The QoS is set individually for each service.

• You can accept the default priority defined by the service itself by not changing its QoS setting.

- You can change the priority to a higher or lower value than its default setting to give the service higher or lower priority than it otherwise would have.

The QoS priority settings conform to the IEEE 802.1D-1998 (formerly 802.1p) standard for class of service tag.

You will not change the WAN bandwidth used by changing any QoS priority settings. But you will change the mix of traffic through the WAN ports by granting some services a higher priority than others. The quality of a service is impacted by its QoS setting, however.

See "Quality of Service (QoS) Priorities" on page 7-14 for the procedure on how to use this feature.

Tools for Traffic Management

The FVS338 ProSafe VPN Firewall 50 includes several tools that can be used to monitor the traffic conditions of the firewall and control who has access to the Internet and the types of traffic they are allowed to have. See "Monitoring" on page 9-14 for a discussion of the tools.

Administrator Access Authorization

You can change the administrator password, administrator login timeout, and enable remote management.

Changing the Administrator Password and Login Timeout

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

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

Figure 9-1: Set Password menu

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

Note: If you make the administrator login timeout value too large, you will have to wait a long time before you are able to log back into the router if your previous login was disrupted (i.e., you did not click **Logout** on the Main Menu bar to log out).

The password and timeout value you enter will be changed back to **password** and **5** minutes, respectively, after a factory defaults reset.

Enabling Remote Management Access

Using the Remote Management page, you can allow an administrator on the Internet to configure, upgrade, and check the status of your FVS338 VPN firewall. You must be logged in locally to enable remote management.

> **Note:** Be sure to change the firewall's default configuration password to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both upper and lower case), numbers, and symbols. Your password can be up to 30 characters. See "Changing the Administrator Password and Login Timeout" on page 9-8 for the procedure on how to do this.

Figure 9-2 shows the **Remote Management** screen that is invoked by clicking **Remote Management** under **Management** on the Main Menu bar.

Figure 9-2: Remote Management screen

To configure your firewall for Remote Management:

1. Select the Turn Remote Management On check box.

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

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

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

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

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

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

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

4. Click Apply to have your changes take effect.

5. When accessing your firewall from the Internet, the Secure Sockets Layer (SSL) will be enabled. You will enter *https://* and type your firewall's WAN IP address into your browser, followed by a colon (:) and the custom port number. For example, if your WAN IP address is 134.177.0.123 and you use port number 8080, type the following in your browser:

    https://134.177.0.123:8080

The router's remote login URL is *https://IP_address:port_number* or *https://FullyQualifiedDomainName:port_number*.

If you do not use the SSL *https://address*, but rather use *http://address*, the FVS338 will automatically attempt to redirect to *https://address.*

Note: The first time you remotely connect the FVS338 with a browser via SSL, you may get a message regarding the SSL certificate. If you are using a Windows computer with Internet Explorer 5.5 or higher, simply click Yes to accept the certificate.

Tip: If you are using a dynamic DNS service such as TZO, you can always identify the IP address of your FVS338 by running TRACERT from the Windows Start menu Run option. For example, **tracert yourFVS338.mynetgear.ne**t and you will see the IP address your ISP assigned to the FVS338.

Event Alerts

You can be alerted to important events such as WAN port rollover, WAN traffic limits reached, and login failures and attacks.

WAN Port Rollover

You can request an email alert when the WAN port rolls over if the WAN mode is configured for rollover.

Traffic Limits Reached

Figure 9-3 shows the **Internet Traffic** screen that is invoked by clicking **Internet Traffic** under **WAN Setup** on the Main Menu bar. The WAN1 and WAN2 ports are programmed separately. A WAN port shuts down once its traffic limit is reached when this feature is enabled.

Traffic Meter

WAN1 ▾ ◄──────────────────────── **Each WAN port is programmed separately.**

Internet Traffic Meter

☐ Enable Traffic Meter

   ⦿ No limit

   ○ Download only

   ○ Both Directions

Monthly Limit   [   ] (MBytes)

☐ Increase this month's limit by   [0] (MBytes)

   This month's limit: (MBytes)

Traffic counter

   Restart traffic counter at [ ] : [ ] [am ▾] on the [▾] day of each month

   ☐ Send E-mail Report before restarting counter

                                     [Restart Counter Now]

When Limit is reached:

⦿ Block all traffic

   Block all traffic except E-mail

   ☐ Send E-mail alert ◄──────────── **WAN port shuts down once the traffic limit is reached. An email alert can be sent when this shutdown happens.**

Internet Traffic Statistics

Start Date/Time: 00:00:00 00:00:00

Outgoing Traffic Volume: (MBytes)

Incoming Traffic Volume: (MBytes)

Total Traffic Volume: (MBytes)

Average per day

% of Standard Limit:

% of this Month's Limit:

                                       [Traffic by Protocol]

                   [Apply]   [Cancel]

Figure 9-3: Traffic Limit Reached alert

Login Failures and Attacks

Figure 9-3 shows the **Log** screen that is invoked by clicking **Logs and Email** under **Security** on the Main Menu bar.

Figure 9-4: Logs and email screen

Monitoring

You can view status information about the firewall, WAN ports, LAN ports, and VPN tunnels and program SNMP connections.

Viewing VPN Firewall Status and Time Information

Firewall Status

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

Router Status

System Name	FVS 338
Firmware Version	
Primary	V1.6.7
Secondary	V1.2.8

LAN Port

MAC Address	00:00:84:60:50:02
IP Address	192.168.1.1
DHCP	enable
IP Subnet Mask	255.255.255.0

Broadband Configuration

WAN Mode	active
NAT (Network Address Translation)	enabled
Connection Type	DHCP
State	Connected
IP Address	10.1.0.47
Subnet Mask	255.255.254.0
Gateway	10.1.1.13
Domain Name Server	10.1.1.7
MAC Address	00:03:47:DF:50:12

Dial-up Configuration

WAN Mode	passive
NAT (Network Address Translation)	enabled
Connection Type	Dial-Up
State	---
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
Domain Name Server	0.0.0.0

Show Statistics

System Up Time 0 Days 2:32:08

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN1	Up	223365	488536	0	24856844	502866347	0 Days 2:32:08
WAN2	Up	402	0	0	131052	0	0 Days 2:32:08
LAN	Up	380551	222308	0	494760415	24898751	0 Days 2:32:08

Poll Interval: 5 (secs)   Set Interval   Stop

Figure 9-5: Router Status screen

Table 9-1.   **Router Status**

Item	Description
System Name	This is the Account Name that you entered in the Basic Settings page.
Firmware Version	This is the current software the router is using. This will change if you upgrade your router.
LAN Port Information	These are the current settings for MAC address, IP address, DHCP role and Subnet Mask that you set in the LAN IP Setup page. DHCP can be either Server or None.
WAN Port Information	This indicates whether NAT is Enabled or Disabled. It also displays the current settings for MAC address, IP address, DHCP role and Subnet Mask that you set in the Basic Settings page. DHCP can be either Client or None.

Note: The Router Status page displays current settings and statistics for your router. As this information is read-only, any changes must be made on other pages.

Time Information

Time information is found on the Schedules screen.

Figure 9-6: Time information on the Schedule screen

If supported for your region, you can check Automatically adjust for Daylight Savings Time.

Table 9-1.   Current date and time

Item	Description
Use Default NTP Servers (Network Time Protocol)	If enabled, the system clock is updated regularly by contacting a Default Netgear NTP Server on the Internet.
Use Custom NTP Servers	If you prefer to use a particular NTP server, enable this and enter the name or IP address of an NTP Server in the Server 1 Name/IP Address field. If required, you can also enter the address of another NTP server in the Server 2 Name/IP Address field.If you select this option and leave either Server 1 or Server 2 fields empty, they get set to Default Netgear NTP servers

WAN Ports

You can monitor the status of the WAN connections, Dynamic DNS services, and Internet traffic information.

WAN Port Connection Status

Invoke the Connection Status screen from WAN ISP Basic Settings screens by clicking on WAN Status to view the current connection state of the WAN port.

Connection Status

IP Address	10.1.1.148
Subnet Mask	255.255.254.0
Default Gateway	10.1.1.13
DHCP Server	10.1.1.7
DNS Server	10.1.1.6
Lease Obtained	Wed Dec 8 19:31:39 2004
Lease Duration	0 Days 4:00:00

Release   Renew

Close Window

Figure 9-7: Connection Status screen

Dynamic DNS Status

Invoke the Dynamic DNS Status screen from Dynamic DNS screen by clicking Show Status to see the current DDNS Status in a sub-window.
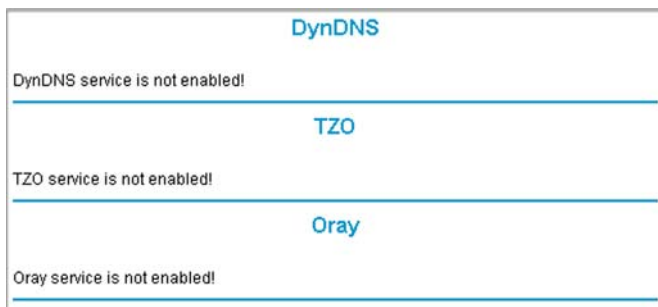
Figure 9-8: Dynamic DNS Status screen

Internet Traffic Information

The Internet Traffic screen provides the following information:

• Internet Traffic Statistics—This displays statistics on Internet Traffic via the WAN port. If you have not enabled the Traffic Meter, these statistics are not available.

• Traffic by Protocol —Click this button if you want to know more details of the Internet Traffic. The volume of traffic for each protocol will be displayed in a sub-window. Traffic counters are updated in MBytes scale and the counter starts only when traffic passed is at least 1 MB.

Figure 9-9: Internet Traffic information

LAN Ports and Attached Devices

Known PCs and 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 Security heading, select Groups and Hosts to view the table, shown below.

Network Database

Known PCs and Devices

	Name	IP Address	MAC Address	Group
○	Eng-temp	192.168.1.2	00:08:02:11:28:31	default ▾

Add   Edit   Delete

Apply   Cancel   Refresh   Edit Group Names

Figure 9-10: Network Database screen

The Network Database is an automatically-maintained list of all known PCs and network devices. PCs and devices become known by the following methods:

• DHCP Client Requests—By default, the DHCP server in this Router is enabled, and will accept and respond to DHCP client requests from PCs and other network devices. These requests also generate an entry in the Network Database. Because of this, leaving the DHCP Server feature (on the LAN screen) enabled is strongly recommended.

• Scanning the Network—The local network is scanned using standard methods such as arp. This will detect active devices which are not DHCP clients. However, sometimes the name of the PC or device cannot be accurately determined and will be shown as Unknown.

The Known PCs and Devices table lists all current entries in the Network Database. For each PC or device, the following data is displayed.

Table 9-1.   Known PCs and Devices table

Item	Description
Name	The name of the PC or device. Sometimes, this can not be determined, and will be listed as Unknown. In this case, you can edit the entry to add a meaningful name.
IP Address	The current IP address. For DHCP clients, where the IP address is allocated by the DHCP Server in this device, this IP address will not change. Where the IP address is set on the PC (as a fixed IP address), you may need to update this entry manually if the IP address on the PC is changed.
MAC Address	The MAC address of the PC. The MAC address is a low-level network identifier which is fixed at manufacture.
Group	Each PC or device must be in a single group. The Group column indicates which group each entry is in. By default, all entries are in the Default group.

Note: 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.

DHCP Log

You can view the DHCP log. Invoke the DHCP Log from LAN IP Setup screen.
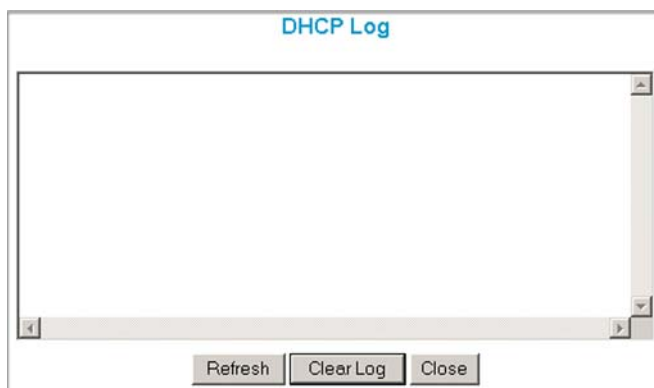
Figure 9-11: DHCP Log

Port Triggering Status

You can view the status of port triggering. Invoke the Port Triggering Status screen from Port Triggering screen.

Figure 9-12: Port Triggering Status screen

Table 9-1.   **Port Triggering Status data**

Item	Description
Rule	The name of the Rule.
LAN IP Address	The IP address of the PC currently using this rule.
Open Ports	The Incoming ports which are associated the this rule. Incoming traffic using one of these ports will be sent to the IP address above.
Time Remaining	The time remaining before this rule is released, and thus available for other PCs. This timer is restarted whenever incoming or outgoing traffic is received.

Firewall

You can view the log of the firewall activities.

Figure 9-3 shows the **Log** screen that is invoked by clicking **Logs and Email** under **Security** on the Main Menu bar.

Figure 9-13: Logs and email screen

Invoke the Firewall Log screen from Logs and Email screen.
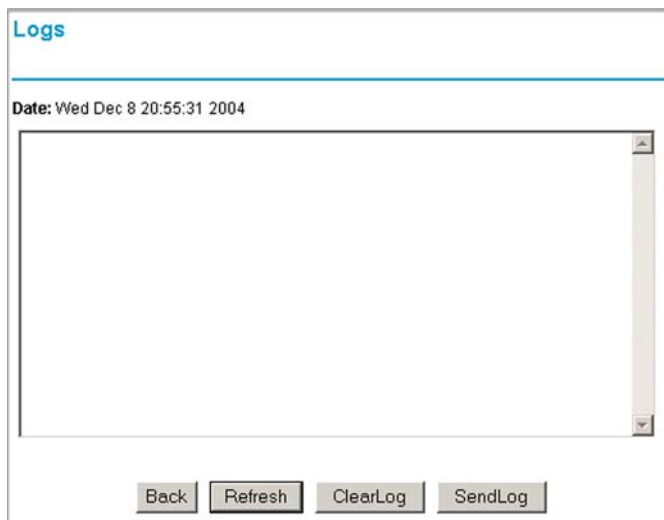
Figure 9-14: Firewall Log screen (invoked from Logs and Email screen)

VPN Tunnels

You can view the status of the VPN tunnels.

January 2005
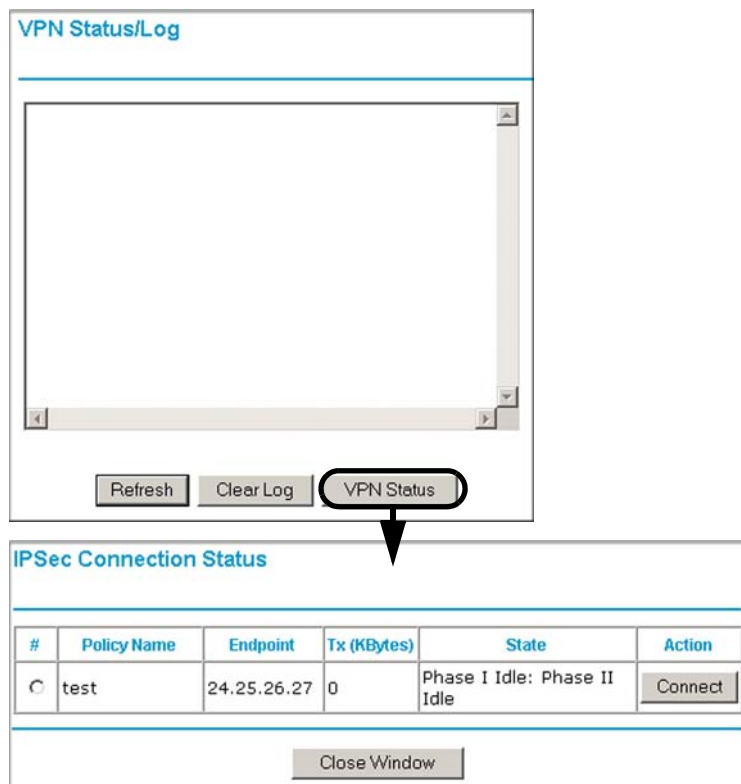
Figure 9-15: VPN Status/Log and IPSec Connection Status screens

Table 9-1.   VPN Status data

Item	Description
Policy Name	The name of the VPN policy associated with this SA.
Endpoint	The IP address on the remote VPN Endpoint.
Tx (KBytes)	The amount of data transmitted over this SA.
State	The current status of the SA.Phase 1 is Authentication phase and Phase 2 is Key Exchange phase.
Action	Use this button to terminate/build the SA (connection) if required.

SNMP

SNMP lets you monitor and manage log resources from an SNMP-compliant system manager. SNMP system configuration lets you to change the system variables for MIB2.

Figure 9-16: SNMP Configuration screens

Diagnostics

You can perform diagnostics such as pinging an IP address, perform a DNS lookup, display the routing table, reboot the firewall, and capture packets.

Note: For normal operation, diagnostics are not required.

Figure 9-17: Diagnostics screen

Table 9-1.   Diagnostics

Item	Description
Ping or Trace an IP address	Ping—Use this to send a ping packet request to the specified IP address. This is often used to test a connection. If the request times out (no reply is received), this usually means the destination is unreachable. However, some network devices can be configured not to respond to a ping. The ping results will be displayed in a new screen; click Back to return to the Diagnostics screen.
	Trace—Often called Trace Route, this will list all Routers between the source (this device) and the destination IP address. The Trace Route results will be displayed in a new screen; click Back to return to the Diagnostics screen.
Perform a DNS Lookup	A DNS (Domain Name Server) converts the Internet name (e.g. www.netgear.com) to an IP address. If you need the IP address of a Web, FTP, Mail or other Server on the Internet, you can do a DNS lookup to find the IP address.
Display the Routing Table	This operation will display the internal routing table. This information is used by Technical Support and other staff who understand Routing Tables.

Table 9-1.   Diagnostics

Item	Description
Reboot the Router	Use this button to perform a remote reboot (restart). You can use this if the Router seems to have become unstable or is not operating normally.
	Note: Rebooting will break any existing connections either to the Router (such as this one) or through the Router (for example, LAN users accessing the Internet). However, connections to the Internet will automatically be re-established when possible.
Packet Trace	Click Packet Trace button to Select the interface and start the packet capture on that interface.

Configuration File Management

The configuration settings of the FVS338 VPN firewall are stored within the firewall in a configuration file. This file can be saved (backed up) to a user's PC, retrieved (restored) from the user's PC, or cleared to factory default settings. You can also upgrade the firewall software with the latest version from Netgear.

From the Main Menu of the browser interface, under the Management heading, select the Settings Backup heading to bring up the menu shown below.
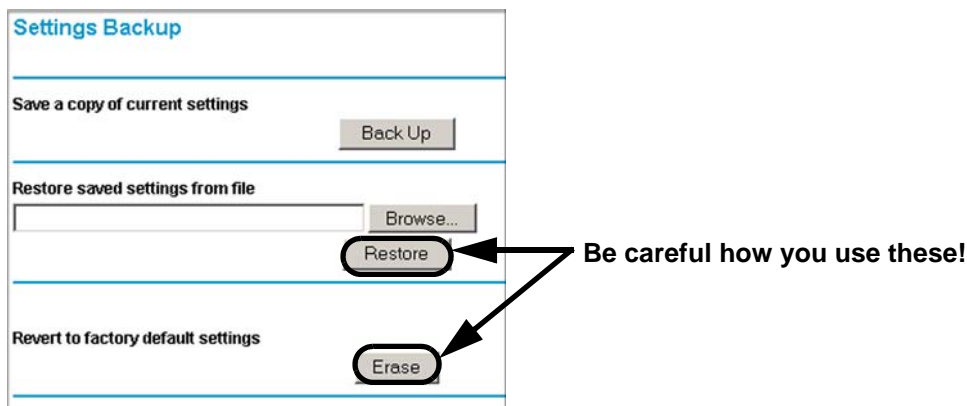
Figure 9-18: Settings Backup menu

The options are described in the following sections.

Restoring and Backing Up the Configuration

IMPORTANT! Once you start restoring settings or erasing the router, do NOT try to go online, turn off the router, shutdown the computer or do anything else to the router until it finishes restarting! This should only take a minute or so. When the Test light turns off, wait a few more seconds before doing anything with the router.

The Restore and Backup options in the Settings Backup menu allow you to save and retrieve a file containing your firewall's configuration settings.

• To save your settings, select the Backup tab. Click the Backup button. Your browser will extract the configuration file from the firewall and will prompt you for a location on your PC to store the file. You can give the file a meaningful name at this time, such as pacbell.cfg.

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

An Alert page appears showing the status of restore operation.You need to manually restart the router to make the restored settings effective.

IMPORTANT! Do not try to go online, turn off the router, shutdown the computer or do anything else to the router until it finishes restarting! When the Test light turns off, wait a few more seconds before doing anything with the router.

Upgrading the Firewall Software

The routing software of the FVS338 VPN firewall is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR. Upgrade files can be downloaded from Netgear's website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.TRX) file before sending it to the firewall. The upgrade file can be sent to the firewall using your browser.

Note: The Web browser used to upload new firmware into the FVS338 VPN firewall must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer or Netscape Navigator 3.0 or above.

From the Main Menu of the browser interface, under the Management heading, select the Router Upgrade heading to display the menu shown below.

Firmware Upgrade

Locate and Select the Upgrade File from your Hard Disk:

[   ] Browse...   **Be careful how you use this!**

Upload   Cancel
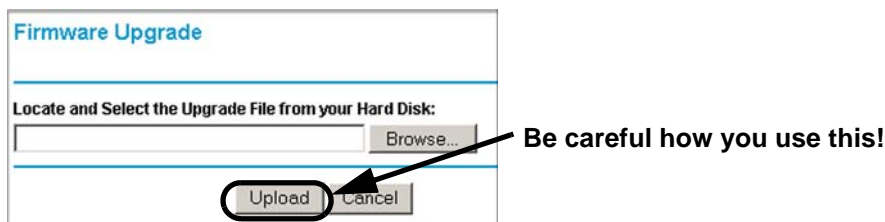
Figure 9-19: Router Upgrade menu

To upload new firmware:

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

2. In the Router Upgrade menu, click the Browse button and browse to the location of the binary (.BIN) upgrade file

3. Click Upload.

   Note: When uploading software to the FVS338 VPN firewall, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it may corrupt the software. When the upload is complete, your firewall will automatically restart. The upgrade process will typically take about one minute.

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

Erasing the Configuration (Factory Defaults Reset)

It is sometimes desirable to restore the firewall to a known blank condition. This can be done by using the Erase function, which will restore all factory settings. After an erase, the firewall's password will be **password**, the LAN IP address will be 192.168.1.1, and the firewall's DHCP client will be enabled.

• To erase the configuration and reset the router to the original factory default settings, click the Erase button (see Figure 9-18).

   IMPORTANT! Do not try to go online, turn off the router, shutdown the computer or do anything else to the router until the router finishes restarting! When the Test light turns off, wait a few more seconds before doing anything with the router.

   You need to manually restart the router to make the default settings effective.After rebooting, the router's password will be password, the LAN IP address will be 192.168.1.1 and the router will act as a DHCP server on the LAN and act as a DHCP client to the Internet.

• To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the front panel of the firewall (see "The Router's Front Panel" on page 2-6). Also see "Restoring the Default Configuration and Password" on page 10-7.

Chapter 10
Troubleshooting

This chapter gives information about troubleshooting your FVS338 ProSafe VPN Firewall 50. After each problem description, instructions are provided to help you diagnose and solve the problem.

Basic Functioning

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

1. When power is first applied, verify that the PWR LED is on.

2. After approximately 10 seconds, verify that:

    a. The TEST LED is not lit.

    b. The LAN port LEDs are lit for any local ports that are connected.

    c. The Internet port LED is lit.

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

If any of these conditions does not occur, refer to the appropriate following section.

Power LED Not On

If the Power and other LEDs are off when your firewall is turned on:

- Make sure that the power cord is properly connected to your firewall and that the power supply adapter is properly connected to a functioning power outlet.

- Check that you are using the 12 V DC power adapter supplied by NETGEAR for this product.

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

LEDs Never Turn Off

When the firewall is turned on, the LEDs turns on for about 10 seconds and then turn off. If all the LEDs stay on, there is a fault within the firewall.

If all LEDs are still on one minute after power up:

- Cycle the power to see if the firewall recovers.

- Clear the firewall's configuration to factory defaults. This will set the firewall's IP address to 192.168.1.1. This procedure is explained in "Restoring the Default Configuration and Password" on page 10-7.

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

LAN or Internet Port LEDs Not On

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

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

- Make sure that power is turned on to the connected hub or workstation.

- Be sure you are using the correct cable:

  When connecting the firewall's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

Troubleshooting the Web Configuration Interface

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

- Check the Ethernet connection between the PC and the firewall as described in the previous section.

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

  Note: If your PC's IP address is shown as 169.254.x.x: Recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the PC to the firewall and reboot your PC.

- If your firewall's IP address has been changed and you don't know the current IP address, clear the firewall's configuration to factory defaults. This will set the firewall's IP address to 192.168.1.1. This procedure is explained in "Restoring the Default Configuration and Password" on page 10-7.

- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded.

- Try quitting the browser and launching it again.

- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

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

- When entering configuration settings, be sure to click the APPLY button before moving to another menu or tab, or your changes are lost.

- Click the Refresh or Reload button in the Web browser. The changes may have occurred, but the Web browser may be caching the old configuration.

Troubleshooting the ISP Connection

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

To check the WAN IP address:

1. Launch your browser and select an external site such as www.netgear.com

2. Access the Main Menu of the firewall's configuration at http://192.168.1.1

3. Under the Management 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.

If your firewall can obtain an IP address, but your PC is unable to load any web pages from the Internet:

• Your PC may not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. 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.

Troubleshooting a TCP/IP Network Using a Ping Utility

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

Testing the LAN Path to Your Firewall

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

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

1. From the Windows toolbar, click 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 192.168.1.1`

3. Click on OK.

   You should see a message like this one:

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

   If the path is working, you see this message:

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

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

Request timed out

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

- Wrong physical connections

  — Make sure the LAN port LED is on. If the LED is off, follow the instructions in "LAN or Internet Port LEDs Not On" on page 10-2.

  — Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and firewall.

- Wrong network configuration

  — Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.

  — Verify that the IP address for your firewall and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your PC to a Remote Device

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

PING -n 10 *<IP address>*

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

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

  — Check that your PC has the IP address of your firewall listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC's Network Control Panel.

  — 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.

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 192.168.1.1. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the firewall (see "Erasing the Configuration (Factory Defaults Reset)" on page 9-31).

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

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

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 FVS338 VPN firewall uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000. Cause: The firewall has not yet successfully reached a Network Time Server. Check that your Internet access settings are configured correctly. If you have just completed configuring the firewall, wait at least five minutes and check the date and time again.

- Time is off by one hour. Cause: The firewall does not automatically sense Daylight Savings Time. In the E-Mail menu, check or uncheck the box marked "Adjust for Daylight Savings Time".

January 2005

Appendix A
Technical Specifications

This appendix provides technical specifications for the FVS338 ProSafe VPN Firewall 50.

Network Protocol and Standards Compatibility

Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP
	PPP over Ethernet (PPPoE)

Power Adapter

North America:	120V, 60 Hz, input
United Kingdom, Australia:	240V, 50 Hz, input
Europe:	230V, 50 Hz, input
Japan:	100V, 50/60 Hz, input
All regions (output):	12 V DC @ 1.2 A output, 18W maximum

Physical Specifications

Dimensions:	28 x 175 x 118 mm (1.1 x 6.89 x 4.65 in.)
Weight:	0.3 kg (0.66 lb)

Environmental Specifications

Operating temperature:	0° to 40° C (32º to 104º F)
Operating humidity:	90% maximum relative humidity, noncondensing

Electromagnetic Emissions

Meets requirements of:	FCC Part 15 Class B
	VCCI Class B
	EN 55 022 (CISPR 22), Class B

Interface Specifications

LAN:	10BASE-T or 100BASE-Tx, RJ-45
WAN:	10BASE-T or 100BASE-Tx

Appendix B
Network, Routing, Firewall, and Basics

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

Related Publications

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

Basic Router Concepts

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

January 2005

What is a Router?

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

Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connection they support. The FVS338 ProSafe VPN Firewall 50 is a small office router that routes the IP protocol over a single-user broadband connection.

Routing Information Protocol

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

The FVS338 VPN firewall supports both the older RIP-1 and the newer RIP-2 protocols. Among other improvements, RIP-2 supports subnet and multicast protocols. RIP is not required for most home applications.

IP Addresses and the Internet

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

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

For example, the following binary address:

```
11000011  00100010  00001100  00000111
```

is normally written as:

```
195.34.12.7
```

Network, Routing, Firewall, and Basics

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.

Class A

Network   Node

Class B

          Network   Node

Class C
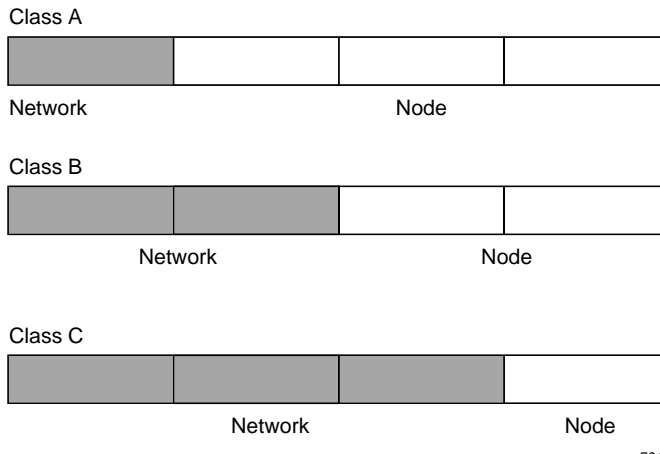
          Network   Node

Figure 10-1: 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)
```

Network, Routing, Firewall, and Basics

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.

Class B

Network		Subnet	Node

Figure 10-2: 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 10-1.   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 10-2.   Netmask Formats

Dotted-Decimal	Masklength
255.0.0.0	/8
255.255.0.0	/16

Table 10-2.　　**Netmask Formats**

255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31
255.255.255.255	/32

Configure all hosts on a LAN segment to use the same netmask for the following reasons:

• So that hosts recognize local IP broadcast packets

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

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

Private IP Addresses

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

```
10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255
```

Choose your private network number from this range. The DHCP server of the FVS338 VPN firewall is preconfigured to automatically assign private addresses.

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

Single IP Address Operation Using NAT

In the past, if multiple PCs on a LAN needed to access the Internet simultaneously, you had to obtain a range of IP addresses from the ISP. This type of Internet account is more costly than a single-address account typically used by a single user with a modem, rather than a router. The FVS338 VPN firewall employs an address-sharing method called Network Address Translation (NAT). This method allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your ISP.

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

The following figure illustrates a single IP address operation.
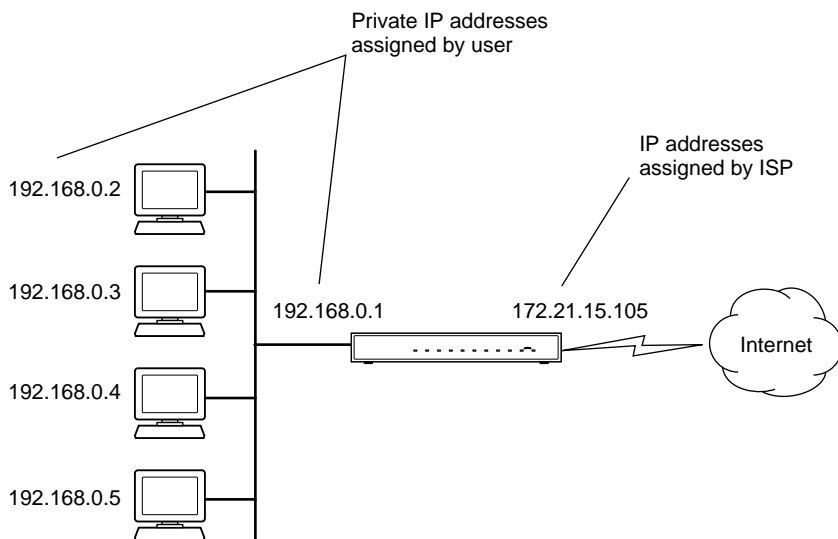
Figure 10-3: Single IP Address Operation Using NAT

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)*.

January 2005

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 FVS338 VPN firewall has the capacity to act as a DHCP server.

The FVS338 VPN firewall also functions as a DHCP client when connecting to the ISP. The firewall can automatically obtain an IP address, subnet mask, DNS server addresses, and a gateway address if the ISP provides this information by DHCP.

Internet Security and Firewalls

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

What is a Firewall?

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

Stateful Packet Inspection

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

Denial of Service Attack

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

Ethernet Cabling

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

.

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

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

Category 5 Cable Quality

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

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

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

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

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

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

Inside Twisted Pair Cables

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

Figure B-1 illustrates straight-through twisted pair cable.
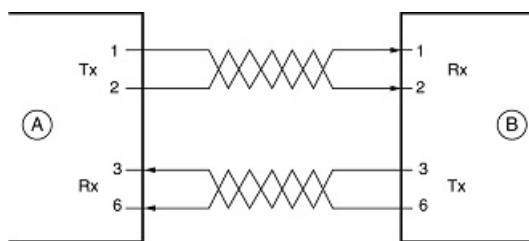
Key:
A = UPLINK OR MDI PORT (as on a PC)
B = Normal or MDI-X port (as on a hub or switch)
1, 2, 3, 6 = Pin numbers

Figure B-1: Straight-Through Twisted-Pair Cable

Figure B-2 illustrates crossover twisted pair cable.
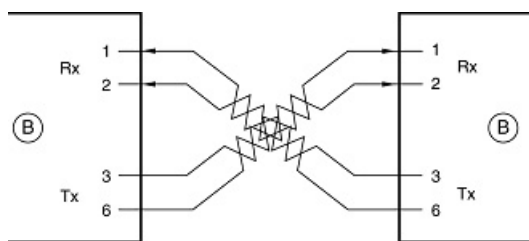
Key:
B = Normal or MDI-X port (as on a hub or switch)
1, 2, 3, 6 = Pin numbers

Figure B-2: Crossover Twisted-Pair Cable

January 2005

Key:
1 = RJ-45 plug
2 = Category 5 UTP patch cable

5525.1
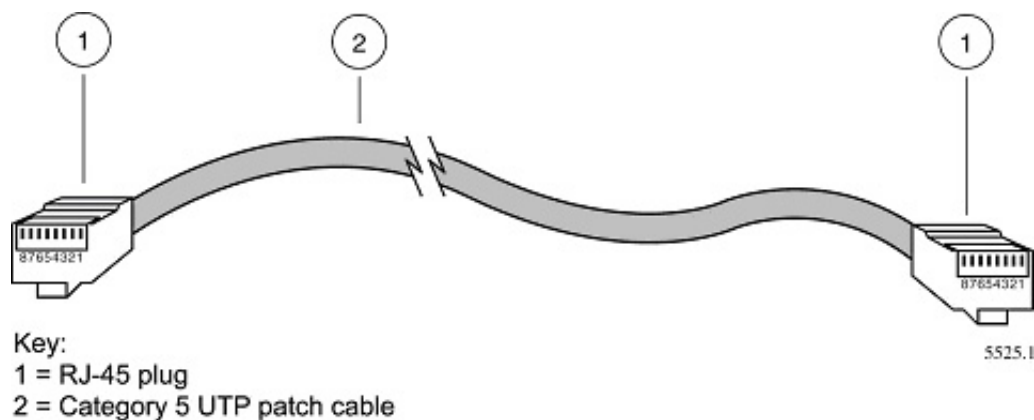
Figure B-3: Category 5 UTP Cable with Male RJ-45 Plug at Each End

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

Uplink Switches, Crossover Cables, and MDI/MDIX Switching

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

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

The FVS338 VPN firewall incorporates Auto Uplink™ technology (also called MDI/MDIX). Each LOCAL Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a normal connection (e.g. connecting to a PC) or an uplink connection (e.g. connecting to a router, switch, or hub). That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink™ will accommodate either type of cable to make the right connection.

Appendix C
Preparing Your Network

This appendix describes how to prepare your network to connect to the Internet through the FVS338 ProSafe VPN Firewall 50 and how to verify the readiness of broadband Internet service from an Internet service provider (ISP).

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

Preparing Your Computers for TCP/IP Networking

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

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

- Windows® 95 or later includes the software components for establishing a TCP/IP network.

- Windows 3.1 does not include a TCP/IP component. You need to purchase a third-party TCP/IP application package such as NetManage Chameleon.

- Macintosh Operating System 7 or later includes the software components for establishing a TCP/IP network.

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

January 2005

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

The FVS338 VPN firewall is shipped preconfigured as a DHCP server. The firewall assigns the following TCP/IP configuration information automatically when the PCs are rebooted:

- PC or workstation IP addresses—192.168.0.2 through 192.168.0.254
- Subnet mask—255.255.255.0
- Gateway address (the firewall)—192.168.1.1

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

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

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

Install or Verify Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.

2. Double-click the Network icon.

   The Network window opens, which displays a list of installed components:
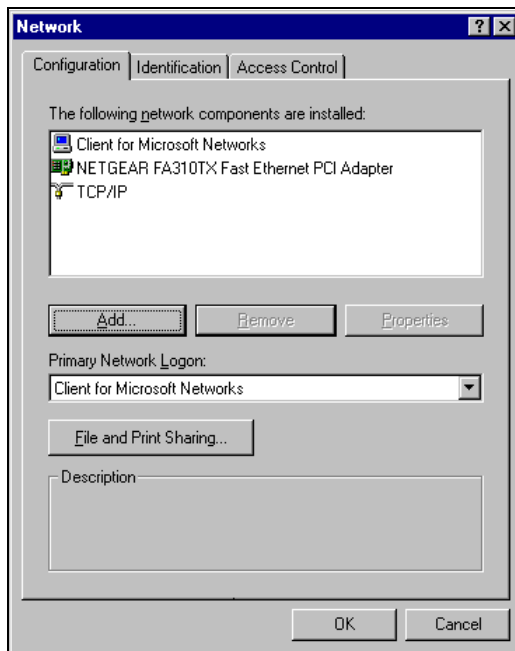
You must have an Ethernet adapter, the TCP/IP protocol, and Client for Microsoft Networks.

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

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

a. Click the Add button.

b. Select Adapter, and then click Add.

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

If you need TCP/IP:

a. Click the Add button.

b. Select Protocol, and then click Add.

c. Select Microsoft.

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

If you need Client for Microsoft Networks:

    a.   Click the Add button.

    b.   Select Client, and then click Add.

    c.   Select Microsoft.

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

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

Enabling DHCP to Automatically Configure TCP/IP Settings

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

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

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

1

Locate your **Network Neighborhood** icon.

- If the Network Neighborhood icon is on the Windows desktop, position your mouse pointer over it and right-click your mouse button.

- If the icon is not on the desktop,

  - Click **Start** on the task bar located at the bottom left of the window.

  - Choose **Settings**, and then **Control Panel**.

  - Locate the **Network Neighborhood** icon and click on it. This will open the Network panel as shown below.

2

Verify the following settings as shown:

- Client for Microsoft Network exists

- Ethernet adapter is present

- TCP/IP is present

- **Primary Network Logon** is set to Windows logon

Click on the **Properties** button. The following TCP/IP Properties window will display.

Network ? ✕

Configuration | Identification | Access Control |

The following network components are installed:

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

[Add...] [Remove] [Properties]

Primary Network Logon:

[Client for Microsoft Networks ▼]
Client for Microsoft Networks
Windows Logon

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

[OK] [Cancel]

January 2005

3

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

- Verify the following:

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

- Click **OK** to continue.

Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.
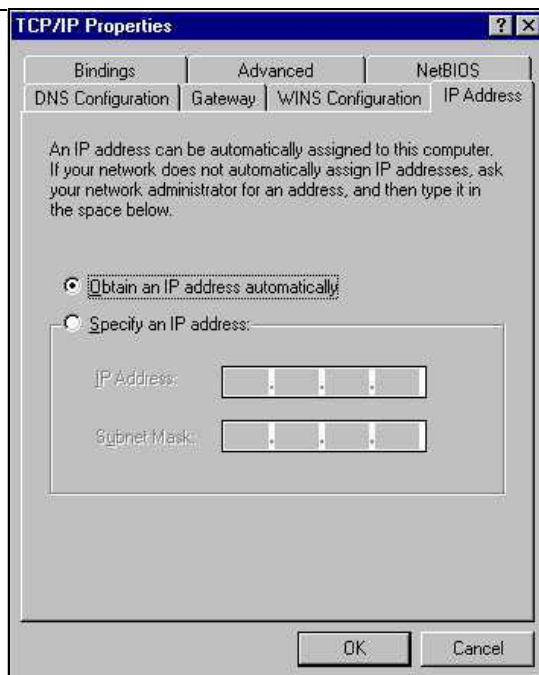
Selecting Windows' Internet Access Method

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.

2. Double-click the Internet Options icon.

3. Select "I want to set up my Internet connection manually" or "I want to connect through a Local Area Network" and click Next.

4. Select "I want to connect through a Local Area Network" and click Next.

5. Uncheck all boxes in the LAN Internet Configuration screen and click Next.

6. Proceed to the end of the Wizard.

Verifying TCP/IP Properties

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

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

January 2005

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

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

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

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

   • The IP address is between 192.168.0.2 and 192.168.0.254

   • The subnet mask is 255.255.255.0

   • The default gateway is 192.168.1.1

Configuring Windows NT4, 2000 or XP for IP Networking

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

Install or Verify Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.

2. Double-click the Network and Dialup Connections icon.

3. If an Ethernet adapter is present in your PC, you should see an entry for Local Area Connection. Double-click that entry.

4. Select Properties.

5. Verify that 'Client for Microsoft Networks' and 'Internet Protocol (TCP/IP)' are present. If not, select Install and add them.

6. Select 'Internet Protocol (TCP/IP)', click Properties, and verify that "Obtain an IP address automatically is selected.

7. Click OK and close all Network and Dialup Connections windows.

8. Then, restart your PC.

Enabling DHCP to Automatically Configure TCP/IP Settings

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

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

DHCP Configuration of TCP/IP in Windows XP

1

Locate your **Network Neighborhood** icon.

• Select **Control Panel** from the Windows XP new Start Menu.

• Select the **Network Connections** icon on the Control Panel. This will take you to the next step.

2

• Now the Network Connection window displays.

The Connections List that shows all the network connections set up on the PC, located to the right of the window.

• Right-click on the **Connection** you will use and choose **Status**.

January 2005
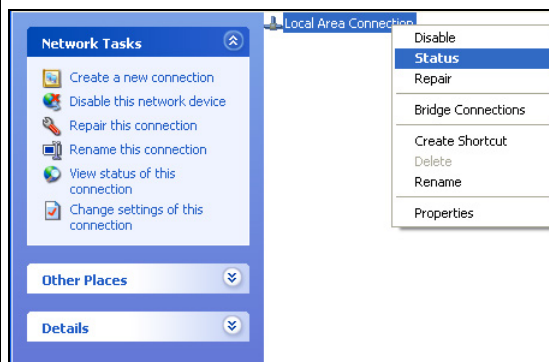
3	**Local Area Connection Status**
• Now you should be at the Local Area Network Connection Status window. This box displays the connection status, duration, speed, and activity statistics. • Administrator logon access rights are needed to use this window. • Click the **Properties button** to view details about the connection.	General tab: Support Connection Status: Connected Duration: 01:40:23 Speed: 100.0 Mbps Activity Sent — Received Packets: 138,143 | 243,057 Properties Disable Close
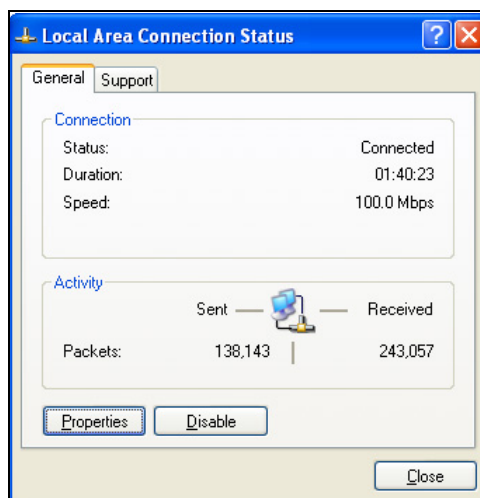
4	**Local Area Connection Properties**
• The TCP/IP details are presented on the Support tab page. • Select **Internet Protocol,** and click **Properties** to view the configuration information**.**	General Authentication Advanced Connect using: Intel(R) PRO/100 VE Network Connection Configure... This connection uses the following items: ☑ Client for Microsoft Networks ☑ File and Printer Sharing for Microsoft Networks ☐ QoS Packet Scheduler ☑ Internet Protocol (TCP/IP) Install... Uninstall Properties Description Allows your computer to access resources on a Microsoft network. ☑ Show icon in notification area when connected OK Cancel

January 2005

5

- Verify that the **Obtain an IP address automatically** radio button is selected.

- Verify that **Obtain DNS server address automatically** radio button is selected.

- Click the **OK** button.

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

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

Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

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

○ Obtain an IP address automatically
○ Use the following IP address:

    IP address:

    Subnet mask:

    Default gateway:

○ Obtain DNS server address automatically
○ Use the following DNS server addresses:

    Preferred DNS server:

    Alternate DNS server:

Advanced...

OK | Cancel

DHCP Configuration of TCP/IP in Windows 2000

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

1

• Click on the **My Network Places** icon on the Windows desktop. This will bring up a window called Network and Dial-up Connections.

• Right click on **Local Area Connection** and select **Properties**.

2

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

• Verify that you have the correct Ethernet card selected in the **Connect using:** box.

• Verify that at least the following two items are displayed and selected in the box of "Components checked are used by this connection:"

• Client for Microsoft Networks and

• Internet Protocol (TCP/IP)

• Click **OK**.

Local Area Connection Properties

General

Connect using:

3Com 10/100 Mini PCI Ethernet Adapter

Configure

Components checked are used by this connection:

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

Install...   Uninstall   Properties

Description

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

☑ Show icon in taskbar when connected

OK   Cancel

January 2005

3

- With Internet Protocol (TCP/IP) selected, click on **Properties** to open the Internet Protocol (TCP/IP) Properties dialogue box.

- Verify that

  - **Obtain an IP address automatically** is selected.

  - **Obtain DNS server address automatically** is selected.

- Click **OK** to return to Local Area Connection Properties.
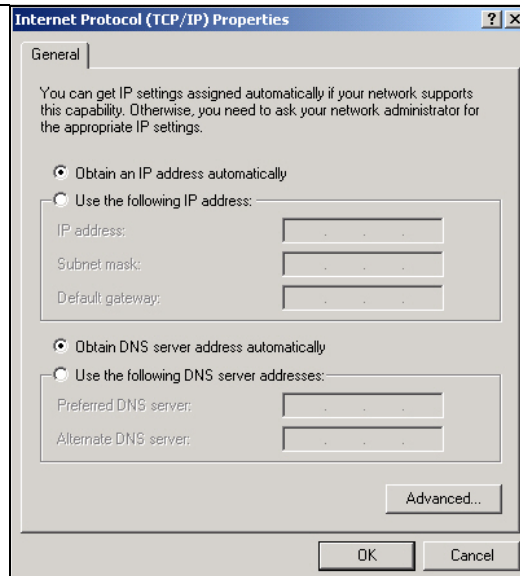
4

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

Restart the PC.

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

Preparing Your Network

January 2005
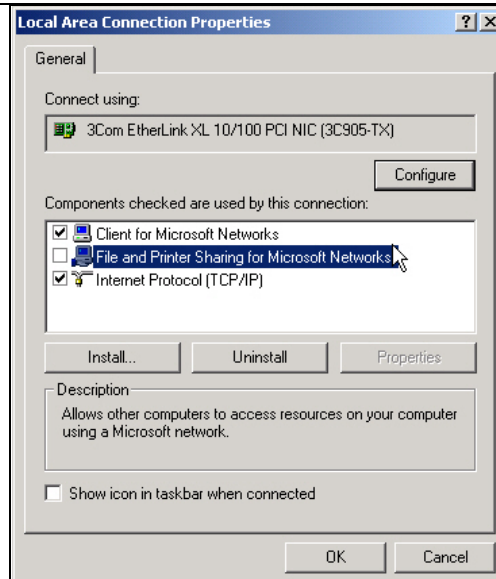
DHCP Configuration of TCP/IP in Windows NT4

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

1

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

2

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

The Network panel will display.

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

January 2005
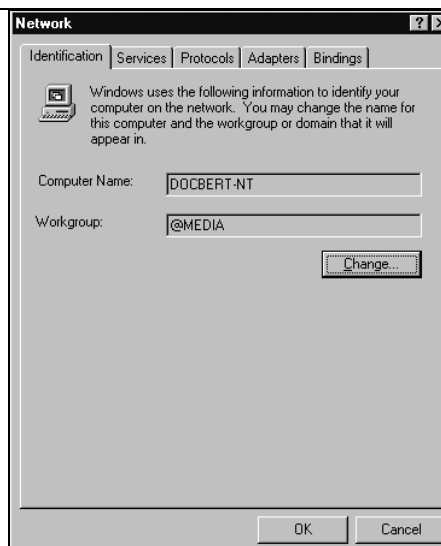
3

• Highlight the **TCP/IP Protocol** in the **Network Protocols** box, and click on the **Properties** button.
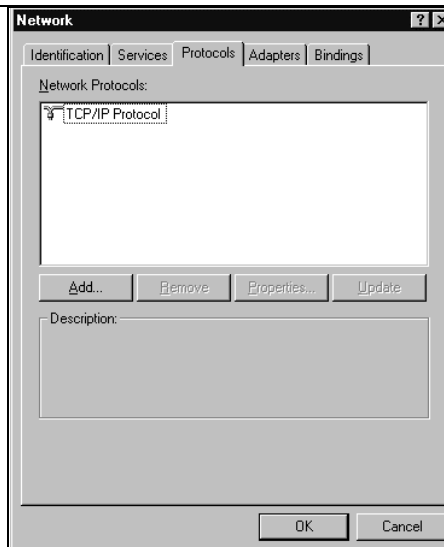
4

- The **TCP/IP Properties** dialog box now displays.

- Click the **IP Address** tab**.**

- Select the radio button marked **Obtain an IP address from a DHCP server.**

- Click **OK**. This completes the configuration of TCP/IP in Windows NT.

Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.
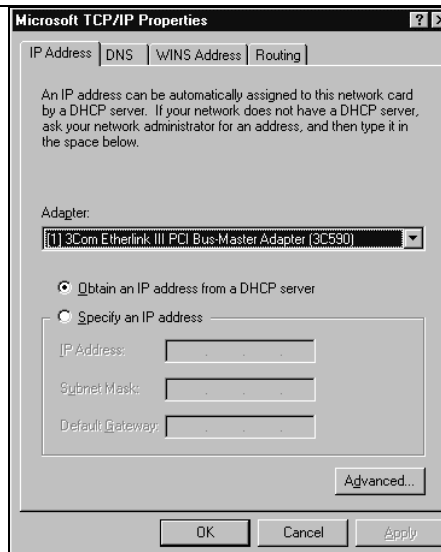
Verifying TCP/IP Properties for Windows XP, 2000, and NT4

To check your PC's TCP/IP configuration:

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

   The Run window opens.

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

   A command window opens

3. Type **ipconfig /all**

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

   • The IP address is between 192.168.0.2 and 192.168.0.254

   • The subnet mask is 255.255.255.0

January 2005

- The default gateway is 192.168.1.1

4. Type **exit**

Configuring the Macintosh for TCP/IP Networking

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

MacOS 8.6 or 9.x

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

   The TCP/IP Control Panel opens:
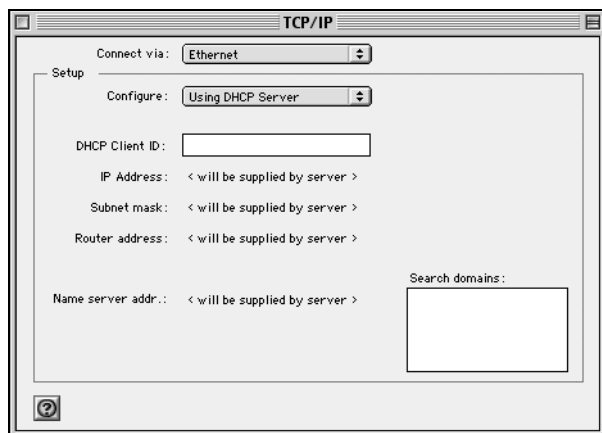
2. From the "Connect via" box, select your Macintosh's Ethernet interface.

3. From the "Configure" box, select Using DHCP Server.

   You can leave the DHCP Client ID box empty.

4. Close the TCP/IP Control Panel.

5. Repeat this for each Macintosh on your network.

MacOS X

1. From the Apple menu, choose System Preferences, then Network.

2. If not already selected, select Built-in Ethernet in the Configure list.

3. If not already selected, Select Using DHCP in the TCP/IP tab.

4. Click Save.

Verifying TCP/IP Properties for Macintosh Computers

After your Macintosh is configured and has rebooted, you can check the TCP/IP configuration by returning to the TCP/IP Control Panel. From the Apple menu, select Control Panels, then TCP/IP.
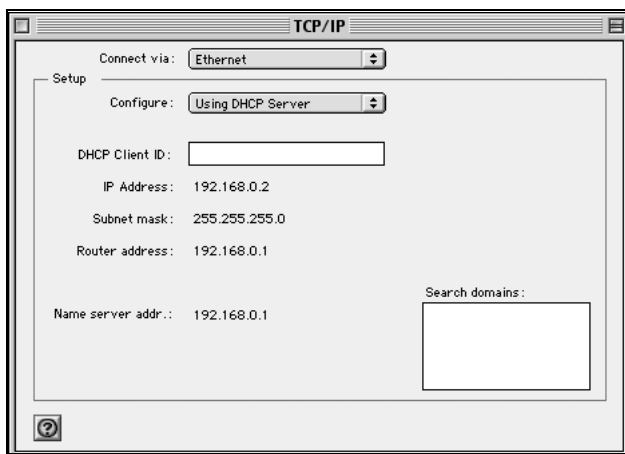
The panel is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

- The IP Address is between 192.168.0.2 and 192.168.0.254

- The Subnet mask is 255.255.255.0

- The Router address is 192.168.1.1

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

Verifying the Readiness of Your Internet Account

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

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

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

Are Login Protocols Used?

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

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

What Is Your Configuration Information?

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

- An IP address and subnet mask

- A gateway IP address, which is the address of the ISP's router

- One or more domain name server (DNS) IP addresses

- Host name and domain suffix

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

    `mail.xxx.yyy.com`

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

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

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

Obtaining ISP Configuration Information for Windows Computers

As mentioned above, you may need to collect configuration information from your PC so that you can use this information when you configure the FVS338 VPN firewall. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

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

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.

2. Double-click the Network icon.

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

3. Select TCP/IP, and then click Properties.

    The TCP/IP Properties dialog box opens.

4. Select the IP Address tab.

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

5. Select the Gateway tab.

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

6. Select the DNS Configuration tab.

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

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

    You are returned to the Network window.

8. Click OK.

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

Obtaining ISP Configuration Information for Macintosh Computers

As mentioned above, you may need to collect configuration information from your Macintosh so that you can use this information when you configure the FVS338 VPN firewall. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

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

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

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

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

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

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

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

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

7. Close the TCP/IP Control Panel.

Restarting the Network

Once you've set up your computers to work with the firewall, you must reset the network for the devices to be able to communicate correctly. Restart any computer that is connected to the FVS338 VPN firewall.

After configuring all of your computers for TCP/IP networking and restarting them, and connecting them to the local network of your FVS338 VPN firewall, you are ready to access and configure the firewall.

January 2005

Appendix D
Virtual Private Networking

There have been many improvements in the Internet including Quality of Service, network performance, and inexpensive technologies, such as DSL. But one of the most important advances has been in Virtual Private Networking (VPN) Internet Protocol security (IPSec). IPSec is one of the most complete, secure, and commercially available, standards-based protocols developed for transporting data.

What is a VPN?

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

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

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

VPNs are traditionally used for:

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

- **Remote Access:** Remote access enables telecommuters and mobile workers to access e-mail and business applications. A dial-up connection to an organization's modem pool is one method of access for remote workers, but is expensive because the organization must pay the associated long distance telephone and service costs. Remote access VPNs greatly reduce expenses by enabling mobile workers to dial a local Internet connection and then set up a secure IPSec-based VPN communications to their organization.

- **Extranets**: Extranets are secure connections between two or more organizations. Common uses for extranets include supply-chain management, development partnerships, and subscription services. These undertakings can be difficult using legacy network technologies due to connection costs, time delays, and access availability. IPSec-based VPNs are ideal for extranet connections. IPSec-capable devices can be quickly and inexpensively installed on existing Internet connections.

What Is IPSec and How Does It Work?

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

IPSec Security Features

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

- **Authentication:** Verifies that the packet received is actually from the claimed sender.

- **Integrity:** Ensures that the contents of the packet did not change in transit.

- **Confidentiality:** Conceals the message content through encryption.

IPSec Components

IPSec contains the following elements:

- **Encapsulating Security Payload (ESP)**: Provides confidentiality, authentication, and integrity.

- **Authentication Header (AH)**: Provides authentication and integrity.

- **Internet Key Exchange (IKE)**: Provides key management and Security Association (SA) management.

Encapsulating Security Payload (ESP)

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

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

ESP also provides all encryption services in IPSec. Encryption translates a readable message into an unreadable format to hide the message content. The opposite process, called decryption, translates the message content from an unreadable format to a readable message. Encryption/ decryption allows only the sender and the authorized receiver to read the data. In addition, ESP has an option to perform authentication, called ESP authentication. Using ESP authentication, ESP provides authentication and integrity for the payload and not for the IP header.
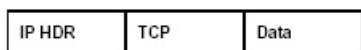
Figure 10-4: Original packet and packet with IPSec Encapsulated Security Payload

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

Authentication Header (AH)

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

Although AH protects the packet's origin, destination, and contents from being tampered with, the identity of the sender and receiver is known. In addition, AH does not protect the data's confidentiality. If data is intercepted and only AH is used, the message contents can be read. ESP protects data confidentiality. For added protection in certain cases, AH and ESP can be used together. In the following table, IP HDR represents the IP header and includes both source and destination IP addresses.
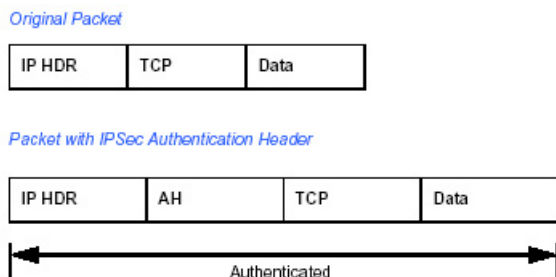
Figure 10-5: Original packet and packet with IPSec Authentication Header

IKE Security Association

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

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

Mode

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

*   **Transport Mode:** The transport mode IPSec implementation encapsulates only the packet's payload. The IP header is not changed. After the packet is processed with IPSec, the new IP packet contains the old IP header (with the source and destination IP addresses unchanged) and the processed packet payload. Transport mode does not shield the information in the IP header; therefore, an attacker can learn where the packet is coming from and where it is going to. The previous packet diagrams show a packet in transport mode.

*   **Tunnel Mode:** The tunnel mode IPSec implementation encapsulates the entire IP packet. The entire packet becomes the payload of the packet that is processed with IPSec. A new IP header is created that contains the two IPSec gateway addresses. The gateways perform the encapsulation/decapsulation on behalf of the hosts. Tunnel mode ESP prevents an attacker from analyzing the data and deciphering it, as well as knowing who the packet is from and where it is going.

Note: AH and ESP can be used in both transport mode or tunnel mode.
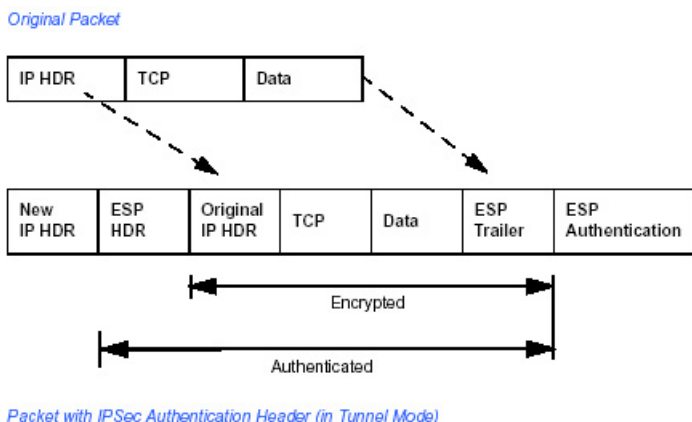
Figure 10-6: Original packet and packet with IPSec ESP in Tunnel mode

Key Management

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

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

Understand the Process Before You Begin

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

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

It is a good idea to gather all the necessary information required to establish a VPN before you begin the configuration process. You should understand whether the firmware is up to date, all of the addresses that will be necessary, and all of the parameters that need to be set on both sides. Try to understand any incompatibilities before you begin, so that you minimize any potential complications which may arise from normal firewall or WAN processes.

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

• The NETGEAR VPN Tutorial – http://www.netgear.com/planetvpn/pvpn_2.html

• The VPN Consortium – http://www.vpnc.org/

• The VPN bibliography in "Additional Reading" on page D-11.

VPN Process Overview

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

Network Interfaces and Addresses

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

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

Interface Addressing

This TechNote uses example addresses provided the VPN Consortium. It is important to understand that you will be using addresses specific to the devices that you are attempting to connect via IPSec VPN.
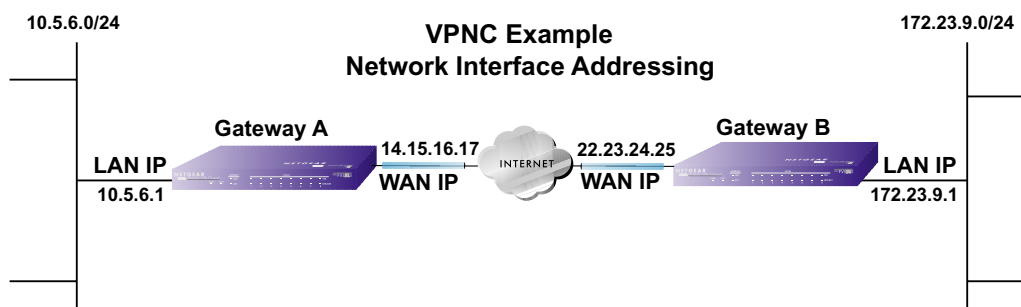
Figure 10-7: VPNC Example Network Interface Addressing

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

Table 10-1.   WAN (Internet/Public) and LAN (Internal/Private) Addressing

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

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

Table 10-2.   Subnet Addressing

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

Firewalls

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

Setting Up a VPN Tunnel Between Gateways

A SA, frequently called a tunnel, is the set of information that allows two entities (networks, PCs, routers, firewalls, gateways) to "trust each other" and communicate securely as they pass information over the Internet.
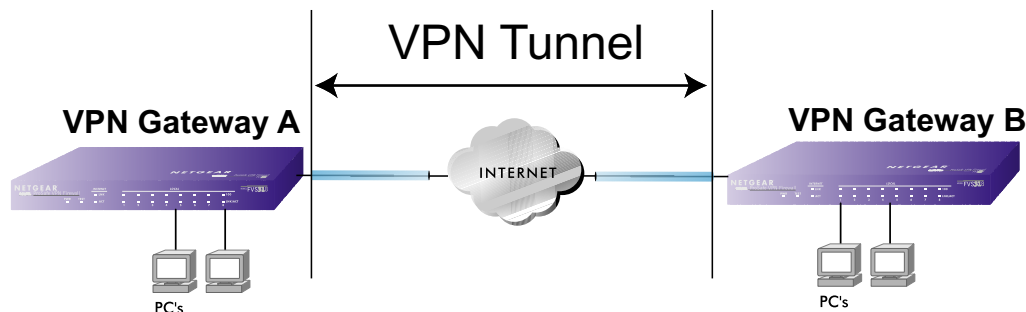
Figure 10-8: VPN Tunnel SA

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

Each gateway must negotiate its Security Association with another gateway using the parameters and processes established by IPSec. As illustrated below, the most common method of accomplishing this process is via the Internet Key Exchange (IKE) protocol which automates some of the negotiation procedures. Alternatively, you can configure your gateways using manual key exchange, which involves manually configuring each paramter on both gateways.
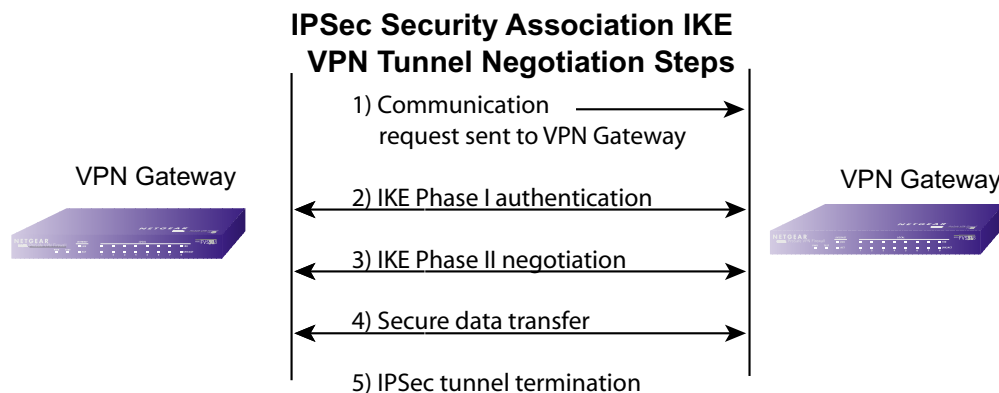
Figure 10-9: IPSec SA negotiation

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

2. **IKE Phase I.**

   a. The two parties negotiate the encryption and authentication algorithms to use in the IKE SAs.

   b. The two parties authenticate each other using a predetermined mechanism, such as preshared keys or digital certificates.

   c. A shared master key is generated by the Diffie-Hellman Public key algorithm within the IKE framework for the two parties. The master key is also used in the second phase to derive IPSec keys for the SAs.

3. **IKE Phase II.**

   a. The two parties negotiate the encryption and authentication algorithms to use in the IPSec SAs.

   b. The master key is used to derive the IPSec keys for the SAs. Once the SA keys are created and exchanged, the IPSec SAs are ready to protect user data between the two VPN gateways.

4. **Data transfer.** Data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.

5. **IPSec tunnel termination.** IPSec SAs terminate through deletion or by timing out.

VPNC IKE Security Parameters

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

VPNC IKE Phase I Parameters

The IKE Phase 1 parameters used:

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

VPNC IKE Phase II Parameters

The IKE Phase 2 parameters used in Scenario 1 are:

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

Testing and Troubleshooting

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

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

*   Parameters may be configured differently on Gateway A vs. Gateway B.

*   Two LANs set up with similar or overlapping addressing schemes.

*   So many required configuration parameters mean errors such as mistyped information or mismatched parameter selections on either side are more likely to happen.

Additional Reading

*   *Building and Managing Virtual Private Networks*, Dave Kosiur, Wiley & Sons; ISBN: 0471295264

*   *Firewalls and Internet Security: Repelling the Wily Hacker*, William R. Cheswick and Steven M. Bellovin, Addison-Wesley; ISBN: 0201633574

*   *VPNs A Beginners Guide*, John Mains, McGraw Hill; ISBN: 0072191813

*   [FF98] Floyd, S., and Fall, K., Promoting the Use of End-to-End Congestion Control in the Internet. IEEE/ACM Transactions on Networking, August 1999.

Relevant RFCs listed numerically:

- [RFC 791] *Internet Protocol DARPA Internet Program Protocol Specification*, Information Sciences Institute, USC, September 1981.

- [RFC 1058] *Routing Information Protocol*, C Hedrick, Rutgers University, June 1988.

- [RFC 1483] *Multiprotocol Encapsulation over ATM Adaptation Layer 5*, Juha Heinanen, Telecom Finland, July 1993.

- [RFC 2401] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol, RFC 2401, November 1998.

- [RFC 2407] D. Piper, The Internet IP Security Domain of Interpretation for ISAKMP, November 1998.

- [RFC 2474] K. Nichols, S. Blake, F. Baker, D. Black, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998.

- [RFC 2475] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, An Architecture for Differentiated Services, December 1998.

- [RFC 2481] K. Ramakrishnan, S. Floyd, A Proposal to Add Explicit Congestion Notification (ECN) to IP, January 1999.

- [RFC 2408] D. Maughan, M. Schertler, M. Schneider, J. Turner, Internet Security Association and Key Management Protocol (ISAKMP).

- [RFC 2409] D. Harkins, D.Carrel, Internet Key Exchange (IKE) protocol.

- [RFC 2401] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol.

Glossary

List of Glossary Terms

Use the list below to find definitions for technical terms used in this manual.

Numeric

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.

802.1x

802.1x defines port-based, network access control used to provide authenticated network access and automated data encryption key management. The IEEE 802.1x draft standard offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1x uses a protocol called EAP (Extensible Authentication Protocol) and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication. For details on EAP specifically, refer to IETF's RFC 2284.

802.11a

IEEE specification for wireless networking at 54 Mbps operating in unlicensed radio bands over 5GHz.

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 2.4-2.5GHz.

802.11g

A soon to be ratified IEEE specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz. 802.11g is backwards compatible with 802.11b.

A

Access Control List (ACL)

An ACL is a database that an Operating System uses to track each user's access rights to system objects (such as file directories and/or files).

Ad-hoc Mode

An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an access point (AP). Ad-hoc mode is also referred to as peer-to-peer mode or an Independent Basic Service Set (IBSS). Ad-hoc mode is useful for establishing a network where wireless infrastructure does not exist or where services are not required.

ADSL

Short for asymmetric digital subscriber line, a technology that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate). ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

ARP

Address Resolution Protocol, a TCP/IP protocol used to convert an IP address into a physical address (called a DLC address), such as an Ethernet address. A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address. There is also Reverse ARP (RARP) which can be used by a host to discover its IP address. In this case, the host broadcasts its physical address and a RARP server replies with the host's IP address.

Auto Uplink

Auto Uplink™ technology (also called MDI/MDIX) eliminates the need to worry about crossover vs. straight-through Ethernet cables. Auto Uplink™ will accommodate either type of cable to make the right connection.

B

Bandwidth

The information capacity, measured in bits per second, that a channel could transmit. Bandwidth examples include 10 Mbps for Ethernet, 100 Mbps for Fast Ethernet, and 1000 Mbps (I Gbps) for Gigabit Ethernet.

Baud

The signaling rate of a line, that is, the number of transitions (voltage or frequency changes) made per second. Also known as line speed.

Broadcast

A packet sent to all devices on a network.

C

Class of Service

A term to describe treating different types of traffic with different levels of service priority. Higher priority traffic gets faster treatment during times of switch congestion

CA

A Certificate Authority is a trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs.

Cat 5

Category 5 unshielded twisted pair (UTP) cabling. An Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or Cat 5 or Cat V, by the Electronic Industry Association (EIA). This rating will be printed on the cable jacket. Cat 5 cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

Certificate Authority

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

D

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.

DMZ

Specifying a Default DMZ Server allows you to set up a computer or server that is available to anyone on the Internet for services that you haven't defined. There are security issues with doing this, so only do this if you'll willing to risk open access.

DNS
Short for Domain Name System (or Service), an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Domain Name
A descriptive name for an address or group of addresses on the Internet. Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as .com, .edu, .uk, etc. For example, in the address mail.NETGEAR.com, mail is a server name and NETGEAR.com is the domain.

DSL
Short for digital subscriber line, but is commonly used in reference to the asymmetric version of this technology (ADSL) that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).
ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

DSLAM
DSL Access Multiplexor. The piece of equipment at the telephone company central office that provides the ADSL signal.

Dynamic Host Configuration Protocol
DHCP. 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.

E

EAP
Extensible Authentication Protocol is a general protocol for authentication that supports multiple authentication methods. EAP, an extension to PPP, supports such authentication methods as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards. In wireless communications using EAP, a user requests connection to a WLAN through an AP, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks

the AP for proof of identity, which the AP gets from the user and then sends back to the server to complete the authentication. EAP is defined by RFC 2284.

ESSID

The Extended Service Set Identification (ESSID) is a thirty-two character (maximum) alphanumeric key identifying the wireless local area network.

Ethernet

A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks transmit packets at a rate of 10 Mbps.

G

Gateway

A local device, usually a router, that connects hosts on a local network to other networks.

I

ICMP

See "Internet Control Message Protocol"

IEEE

Institute of Electrical and Electronics Engineers. This American organization was founded in 1963 and sets standards for computers and communications.

IETF

Internet Engineering Task Force. An organization responsible for providing engineering solutions for TCP/IP networks. In the network management area, this group is responsible for the development of the SNMP protocol.

IKE

Internet Key Exchange. An automated method for exchanging and managing encryption keys between two VPN devices.

Infrastructure Mode

An 802.11 networking framework in which devices communicate with each other by first going through an Access Point (AP). In infrastructure mode, wireless devices can communicate with each other or can communicate with a wired network. When one AP is connected to wired network and a set of wireless stations it is referred to as a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or more

BSSs that form a single subnetwork. Most corporate wireless LANs operate in infrastructure mode because they require access to the wired LAN in order to use services such as file servers or printers.

Internet Control Message Protocol

ICMP is an extension to the Internet Protocol (IP) that supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

Internet Protocol

The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it among all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the Internet. Packets can arrive in a different order than they were sent. The Internet Protocol just delivers them. It's up to another protocol, the Transmission Control Protocol (TCP) to put them back in the right order. IP is a connectionless protocol, which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (The reason the packets do get put in the right order is because of TCP, the connection-oriented protocol that keeps track of the packet sequence in a message.) In the Open Systems Interconnection (OSI) communication model, IP is in Layer 3, the Networking Layer. The most widely used version of IP today is IP version 4 (IPv4). However, IP version 6 (IPv6) is also beginning to be supported. IPv6 provides for much longer addresses and therefore for the possibility of many more Internet users. IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.

IP

See "Internet Protocol"

IP Address

A four-byte number uniquely defining each host on the Internet, usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57). Ranges of addresses are assigned by Internic, an organization formed for this purpose.

ISP

Internet service provider.

L

LAN

See "Local Area Network"

Local Area Network

A communications network serving users within a limited area, such as one floor of a building. A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers and is limited to a distance of 1,500 feet. LANs can be connected together, but if modems and telephones connect two or more LANs, the larger network constitutes what is called a WAN or Wide Area Network.

M

MAC

(1) Medium Access Control. In LANs, the sublayer of the data link control layer that supports medium-dependent functions and uses the services of the physical layer to provide services to the logical link control (LLC) sublayer. The MAC sublayer includes the method of determining when a device has access to the transmission medium. (2) Message Authentication Code. In computer security, a value that is a part of a message or accompanies a message and is used to determine that the contents, origin, author, or other attributes of all or part of the message are as they appear to be. (*IBM Glossary of Computing Terms*)

MAC address

The Media Access Control address is a unique 48-bit hardware address assigned to every network interface card. Usually written in the form 01:23:45:67:89:ab.

Maximum Receive Unit

The size in bytes of the largest packet that can be sent or received.

Maximum Transmit Unit

The size in bytes of the largest packet that can be sent or received.

Mbps

Megabits per second.

MDI/MDIX

In cable wiring, the concept of transmit and receive are from the perspective of the PC, which is wired as a Media Dependant Interface (MDI). In MDI wiring, a PC transmits on pins 1 and 2. At the hub, switch,

January 2005

router, or access point, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X).

MTU

The size in bytes of the largest packet that can be sent or received.

P

packet

A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.

Point-to-Point Protocol

PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.

PPP

A protocol allowing a computer using TCP/IP to connect directly to the Internet.

PPPoA

PPPoA. PPP over ATM is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPPoE

PPPoE. PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPP over ATM

PPPoA. PPP over ATM is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPP over Ethernet

PPPoE. PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPTP

Point-to-Point Tunneling Protocol. A method for establishing a virtual private network (VPN) by embedding Microsoft's network protocol into Internet packets.

Protocol

A set of rules for communication between devices on a network.

PSTN
Public Switched Telephone Network.

Q

QoS
See "Quality of Service"

Quality of Service
QoS is a networking term that specifies a guaranteed level of throughput. Throughput is the amount of data transferred from one device to another or processed in a specified amount of time - typically, throughputs are measured in bytes per second (Bps).

R

RADIUS
Short for Remote Authentication Dial-In User Service, RADIUS is an authentication system. Using RADIUS, you must enter your user name and password before gaining access to a network. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.

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*.

router
A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

S

SSID
A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name. *See also* Wireless Network Name and ESSID.

Segment

A section of a LAN that is connected to the rest of the network using a switch, bridge, or repeater.

Subnet Mask

Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.

T

TCP/IP

The main internetworking protocols used in the Internet. The Internet Protocol (IP) used in conjunction with the Transfer Control Protocol (TCP) form TCP/IP.

U

Universal Plug and Play

UPnP. A networking architecture that provides compatibility among networking technology. UPnP compliant routers provide broadband users at home and small businesses with a seamless way to participate in online games, videoconferencing and other peer-to-peer services.

UTP

Unshielded twisted pair is the cable used by 10BASE-T and 100BASE-Tx Ethernet networks.

W

WAN

See "Wide Area Network"

Web

Also known as World-Wide Web (WWW) or W3. An Internet client-server system to distribute information, based upon the hypertext transfer protocol (HTTP).

WEB Proxy Server

A Web proxy server is a specialized HTTP server that allows clients access to the Internet from behind a firewall. The proxy server listens for requests from clients within the firewall and forwards these requests to remote Internet servers outside the firewall. The proxy server reads responses from the external servers and then sends them to internal client clients.

WEP

Wired Equivalent Privacy 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

A WAN is a computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

Wi-Fi

A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see *http://www.wi-fi.net*), an industry standards group promoting interoperability among 802.11b devices.

Windows Internet Naming Service

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using the Windows Network Neighborhood feature.

WINS

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

Wireless Network Name (SSID)

Wireless Network Name (SSID) is the name assigned to a wireless network. This is the same as the SSID or ESSID configuration parameter.

WPA

Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancements that increase the level of data protection and access control for existing and future wireless LAN systems.