FVS338 ProSafe VPN Firewall 50 Reference Manual

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

September 2006
202-10046-03
v1.0

Trademarks

NETGEAR, the NETGEAR logo and ProSafe are trademarks and/or registered trademarks of Netgear, Inc.

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

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

Statement of Conditions

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

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

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

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

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

EU Regulatory Compliance Statement

ProSafe VPN Firewall 50 is compliant with the following EU Council Directives: 89/336/EEC and LVD 73/23/EEC. Compliance is verified by testing to the following standards: EN55022 Class B, EN55024 and EN60950-1.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das 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 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.

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)

Product and Publication Details

Model Number:	FVS338
Publication Date:	September 2006
Product Family:	VPN firewall
Product Name:	ProSafe VPN Firewall 50
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10046-03
Publication Version Number	1.0

Contents

About This Manual

Chapter 1
Introduction

Chapter 2
Connecting the FVS338 to the Internet

Chapter 3
LAN Configuration

Chapter 4
Firewall Protection and Content Filtering

Chapter 5
Virtual Private Networking

Chapter 6
Router and Network Management

About This Manual

The *NETGEAR® ProSafe™ VPN Firewall 50 FVS338 Reference Manual* describes how to install, configure and troubleshoot the ProSafe VPN Firewall 50. The information in this manual is intended for readers with intermediate computer and Internet skills.

Conventions, Formats and Scope

The conventions, formats, and scope of this manual are described in the following paragraphs.

- **Typographical Conventions.** This manual uses the following typographical conventions:

Italics	Emphasis, books, CDs, URL names
Bold	User input
`Fixed`	Screen text, file and server names, extensions, commands, IP addresses

- **Formats.** This manual uses the following formats to highlight special messages:

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

💡	**Tip:** This format is used to highlight a procedure that will save time or resources.

⚠	**Warning:** Ignoring this type of note may result in a malfunction or damage to the equipment.

⚡	**Danger:** This is a safety warning. Failure to take heed of this notice may result in personal injury or death.

- **Scope.** This manual is written for the VPN firewall according to these specifications:

Product Version	ProSafe VPN Firewall 50
Manual Publication Date	September 2006

For more information about network, Internet, firewall, and VPN technologies, see the links to the NETGEAR website in Appendix B, "Related Documents".

Note: Updates to this product are available on the NETGEAR, Inc. website 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 ☰ button that displays the table of contents and an 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 button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

How to Print this Manual

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

- **Printing a Page from HTML**. Each page in the HTML version of the manual is dedicated to a major topic. Select File > Print from the browser menu to print the page contents.
- **Printing from PDF**. 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*.
  - **Printing a PDF 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 left of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.
  - Click the print icon in the upper left of your browser window.
- **Printing a PDF version of the Complete 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 your browser 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.

Revision History

Part Number	Version Number	Description
202-10046-02	1.0	Product update: New firmware and new user Interface

Chapter 1
Introduction

The 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. For example, the FVX538 provides support for Stateful Packet Inspection, Denial of Service (DoS) attack protection and multi-NAT support.The VPN firewall supports 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.

The FVS338 is a plug-and-play device that can be installed and configured within minutes.

Key Features

The 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 rollover connectivity (fail-over) through an analog modem connected to the serial port If the broadband Internet connection fails, after waiting for an pre-specified amount of time 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 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 VPN firewall supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP).

- **IP Address Sharing by NAT.** The 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 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.

Trend Micro Integration

If you have installed the Trend Micro Client/Server/Messaging Suite for SMB on your local network, you can have the firewall enforce its use. When Antivirus Enforcement is selected, local PCs will not be allowed Web access unless they have the Trend Micro OfficeScan client installed and updated with the latest virus definitions.

- The Client/Server/Messaging Suite for Small and Medium Business protects file servers, mail servers, and PCs on your network - and includes antispam capability. The Client/Server Suite for Small and Medium Business protects files servers and PCs.
  - Both products deliver a layered defense against viruses and other malicious code.
  - Unlike competing antivirus products, both products work your NETGEAR VPN Firewall to enforce antivirus policies - end users cannot access the Internet unless they have antivirus protection with current pattern files installed.
  - Both products are specifically built to meet the needs of growing businesses and feature easy installation, automatic transparent updates, and damage cleanup capability.

Activate either product for a free trial.

Easy Installation and Management

You can install, configure, and operate the 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 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 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 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 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 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:

- ProSafe VPN Firewall 50.
- AC power adapter.
- Category 5 Ethernet cable.
- *Resource CD*, including:
  - Application Notes and other helpful information.
  - ProSafe VPN Client Software – one user license.
  - Trend Micro software evaluation.
- 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.

Router Hardware Components

Following is a description of the front and rear panels of the FVS338, including instructions for installing the FVS338 using the rack mounting hardware.

Router Front Panel

The ProSafe VPN Firewall 50 front panel shown below contains the port connections, status LEDs, and the factory defaults reset button.

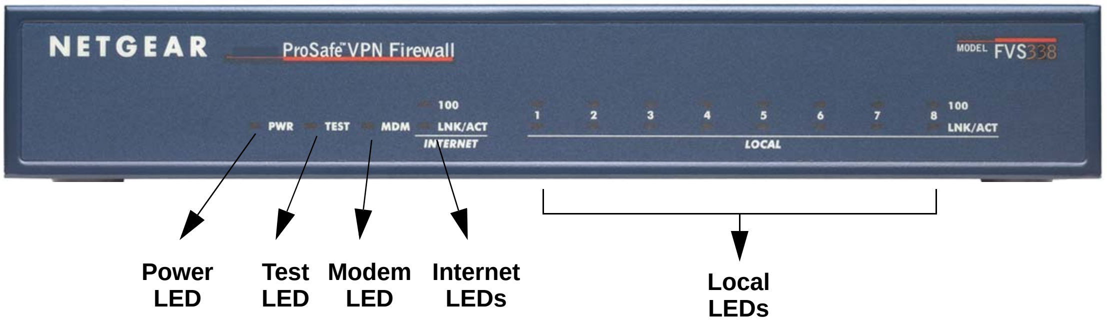


Figure 1-1

The table below describes each item on the front panel and its operation.

Table 1-1. 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 has successfully connected to an ISP and received an IP Address. Server data is being transmitted or received by the serial port. The serial port has no link.
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.

Table 1-1. Object Descriptions (continued)

Object	Activity	Description
Local LEDs	Link/Act LED	
	On (Green)	The LAN port has detected a link with a connected Ethernet device.
	Blinking (Green)	Data is being transmitted or received by the LAN port.
	Off	The LAN port has no link.
	100 LED	
	On (Green)	The LAN port is operating at 100 Mbps.
	Off	The LAN port is operating at 10 Mbps.

Router Rear Panel

The rear panel of the ProSafe VPN Firewall 50 (Figure 1-2) contains the On/Off switch and AC power connection.

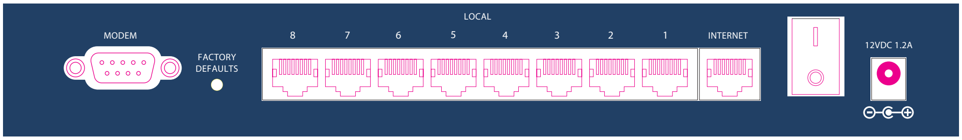


Figure 1-2

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 reset button.
- 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)

Rack Mounting Hardware

The FVS338 can be mounted either on a desktop (using included rubber feet) or in a 19-inch rack (using the included rack mounting hardware illustrated in Figure 1-3).

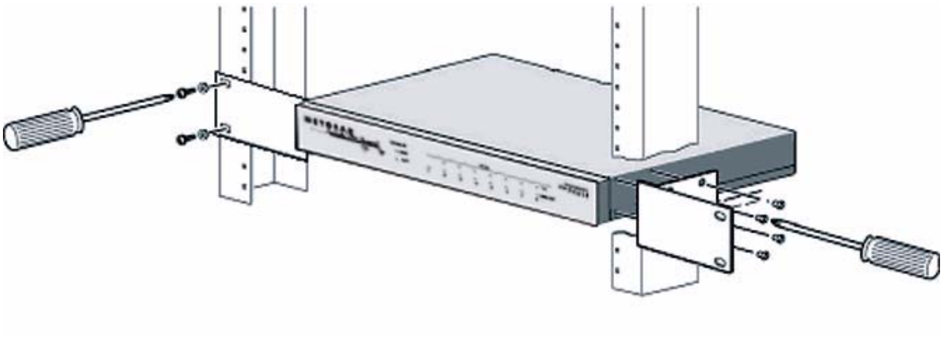


Figure 1-3

Factory Default Login

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**

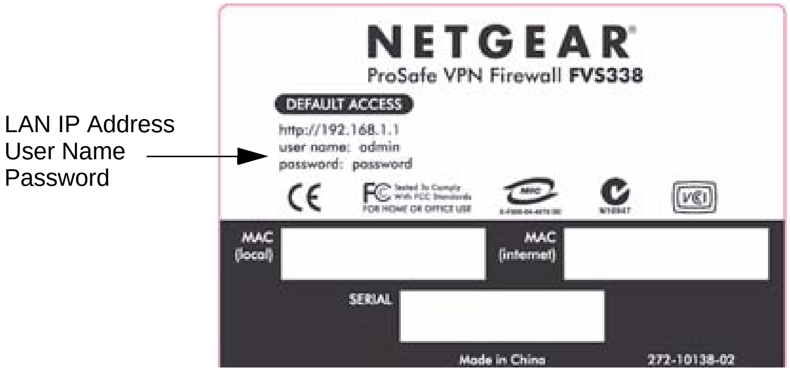
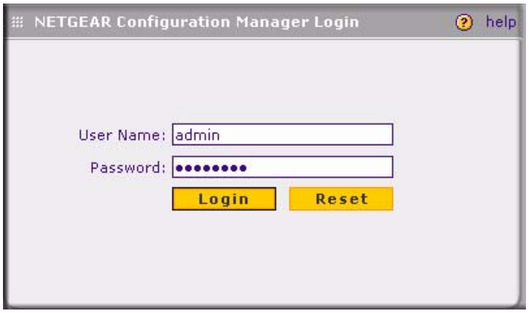


Figure 1-4

To log in to the FVS338 once it is connected:

1. Open a Web browser.
2. Enter **http://192.168.1.1** as the URL.



User Name: admin

Password: ●●●●●●●●

Figure 1-5

3. Once the login screen displays (Figure 1-5), enter the following:
   - **admin** for User Name
   - **password** for Password

Chapter 2
Connecting the FVS338 to the Internet

This section provides instructions for connecting the VPN firewall. Setting up VPN tunnels are covered in Chapter 5, “Virtual Private Networking”:

1. **Connect the firewall physically to your network**. Connect the cables, turn on your router and wait for the Test LED to go out. Make sure your Ethernet and LAN LEDs are lit. (See the *FVS338 ProSafe VPN Firewall 50 Installation Guide* on your Resource CD.)
2. **Log in to the firewall.** After logging in, you are ready to set up and configure your firewall. You can also change your password and enable remote management at this time.
3. **Configure the Internet connections to your ISPs**. During this phase, you will connect to your ISPs. You can also program the WAN traffic meters at this time if desired.
4. **Configure the WAN mode**. Select either **Primary Broadband with Dialup as backup** or **Use only single WAN port**—and select the WAN port from the pull-down menu—either **Broadband** or **Dial-up.**
5. **Configure dynamic DNS on the WAN ports** (if needed). Configure your fully qualified domain names during this phase (if required).
6. **Configure the WAN options** (if needed). Optionally, you can enable each WAN port to respond to a ping. You can also change the factory default MTU size, port speed, and uplink bandwidth. However, these are advanced features and changing them is not usually required.

Connecting the VPN Firewall to Your Network

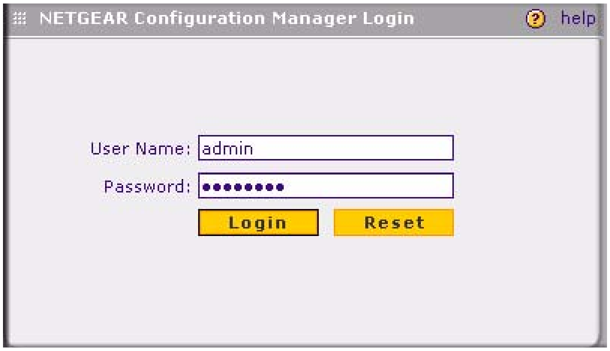
To physically connect your VPN firewall, refer to the I*FVS338 ProSafe VPN Firewall 50 Installation Guide* (a copy is also available on your Resource CD).

Logging in to the VPN Firewall

➡	**Note:** To connect to the firewall, your computer needs to be configured to obtain an IP address automatically via DHCP.

To log in to the VPN firewall:

1. Open a Internet Explorer, Netscape® Navigator, or Firefox browser. In the browser window, enter **http://192.168.1.1** in the address field. The FVS338 login screen will display.



NETGEAR Configuration Manager Login

User Name: admin

Password: ●●●●●●●●

Figure 2-1

2. Enter **admin** for the User Name and **password** for the Password, both in lower case letters.The firewall user name and password are not the same as any user name or password you may use to log in to your Internet connection.
3. Click **Login.** The **Broadband ISP Settings** screen will display.

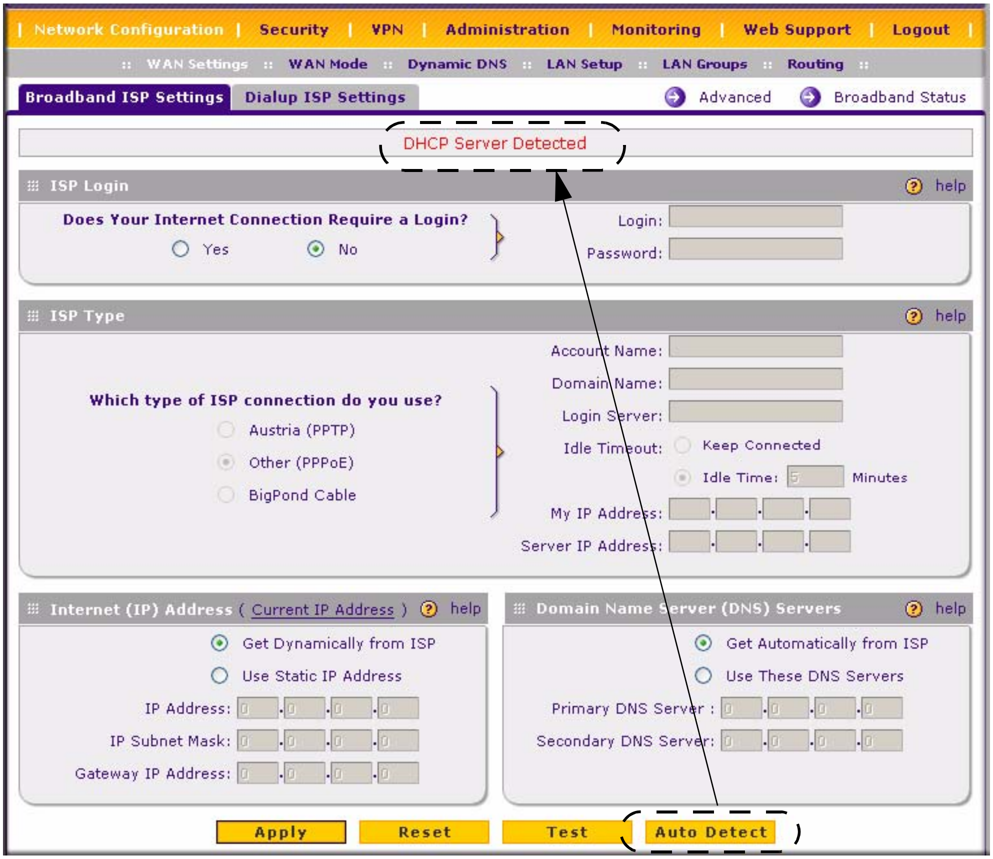
> **Note:** You might want to enable remote management at this time so that you can log in remotely in the future to manage the firewall. See "Enabling Remote Management Access" on page 6-9 for more information. Remote management enable is cleared with a factory default reset. If you enable remote management, you are strongly advised to change your password (see "Changing Passwords and Settings" on page 6-7).

Configuring your Internet Connection

You can configure both Broadband ISP Settings and Dialup ISP Settings.from the WAN Settings menu.

To configure your Broadband ISP Settings:

1. Select **Network Configuration** from the main menu and **WAN Settings** from the submenu. The **Broadband ISP Settings** screen will display.


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
WAN Settings :: WAN Mode :: Dynamic DNS :: LAN Setup :: LAN Groups :: Routing
Broadband ISP Settings
Dialup ISP Settings
Advanced
Broadband Status
help
Apply
Reset
Test
Auto Detect

DHCP Server Detected

ISP Login

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

Login:

Password:

ISP Type

Which type of ISP connection do you use?

○ Austria (PPTP)

● Other (PPPoE)

○ BigPond Cable

Account Name:

Domain Name:

Login Server:

Idle Timeout: ○ Keep Connected

● Idle Time: 5 Minutes

My IP Address: . . .

Server IP Address: . . .

Internet (IP) Address (Current IP Address)

● Get Dynamically from ISP

○ Use Static IP Address

IP Address: 0.0.0.0

IP Subnet Mask: 0.0.0.0

Gateway IP Address: 0.0.0.0

Domain Name Server (DNS) Servers

● Get Automatically from ISP

○ Use These DNS Servers

Primary DNS Server : 0.0.0.0

Secondary DNS Server: 0.0.0.0

Figure 2-2

2. Click **Auto Detect** at the bottom of the screen to automatically detect the type of Internet connection provided by your ISP. Auto Detect will probe for different connection methods and suggest one that your ISP will most likely support.

   When Auto Detect successfully detects an active Internet service, it reports which connection type it discovered. The options are described in the following table.

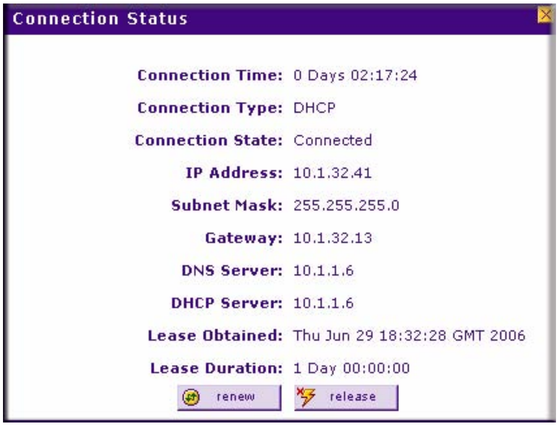
Table 2-1. Internet connection methods

Connection Method	Data Required
PPPoE	Login (Username, Password).
PPTP	Login (Username, Password), Local IP, and PPTP Server IP.
BigPond Cable	Login Username, Password), Account Name, and Server IP.

Table 2-1. Internet connection methods

Connection Method	Data Required
DHCP (Dynamic IP)	No data is required.
Fixed IP	IP address and related data supplied by your ISP.

3. Click **Connection Status** at the top right of the screen to verify your Broadband connection status. Click **Connect** if connection not already present.



Connection Status

Connection Time: 0 Days 02:17:24

Connection Type: DHCP

Connection State: Connected

IP Address: 10.1.32.41

Subnet Mask: 255.255.255.0

Gateway: 10.1.32.13

DNS Server: 10.1.1.6

DHCP Server: 10.1.1.6

Lease Obtained: Thu Jun 29 18:32:28 GMT 2006

Lease Duration: 1 Day 00:00:00

Figure 2-3

If Auto Detect does not find a connection, you will be prompted to check the physical connection between your firewall and the cable or DSL line or to check your Router’s MAC address (see “Setting the Router’s MAC Address (Advanced Options)” on page 2-7).

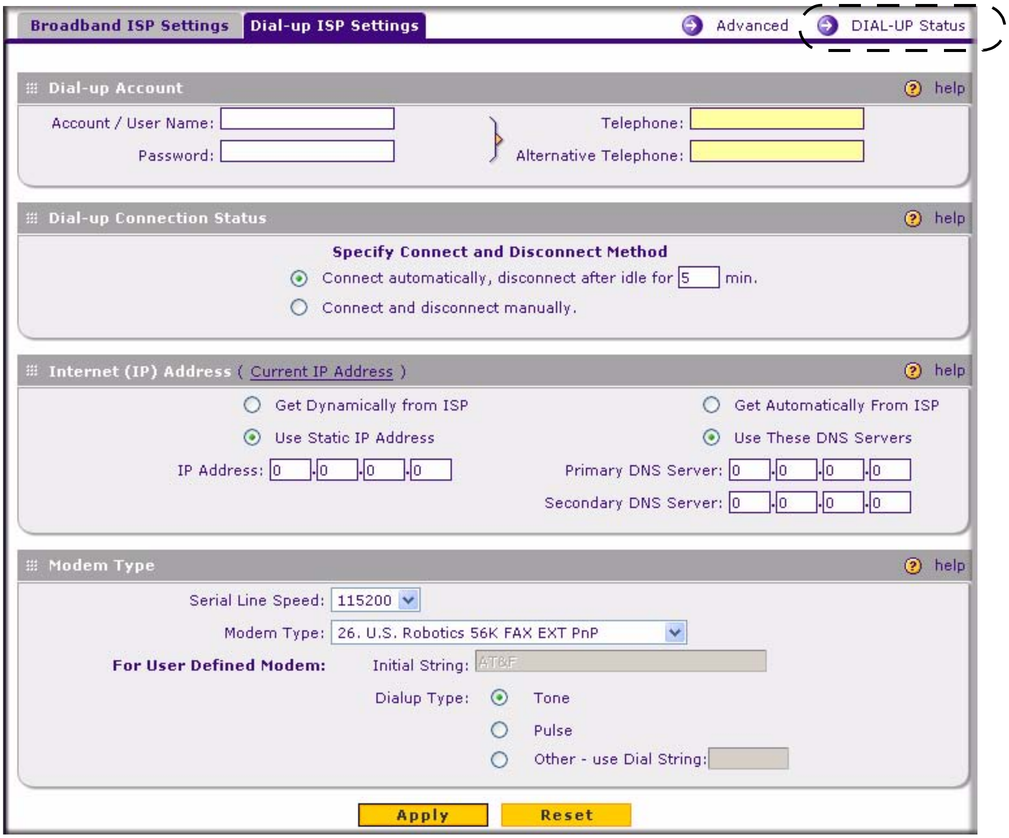
4. Set up the traffic meter for ISP1 if desired. See “Programming the Traffic Meter (if Desired)” on page 2-12.

➡	**Note:** At this point in the configuration process, you are now connected to the Internet through the broadband Ethernet WAN. Optionally, you can continue with the configuration of the dialup ISP serial WAN interface.

The Dialup Settings screen will assist you in setting up the router to access the Internet connection using a dialup modem. Since the Dialup ISP Settings must be configured manually, you will need all of your ISP settings information before you begin.

To configure the Dialup ISP serial WAN port:

1. Select **Network Configuration** from the main menu, **WAN Settings** from the submenu and click the **Dialup ISP Settings** tab to display the Dialup settings screen.



Dial-up Account

Account / User Name:

Password:

Telephone:

Alternative Telephone:

Dial-up Connection Status

Specify Connect and Disconnect Method

● Connect automatically, disconnect after idle for 5 min.

○ Connect and disconnect manually.

Internet (IP) Address (Current IP Address)

○ Get Dynamically from ISP

● Use Static IP Address

IP Address: 0 . 0 . 0 . 0

○ Get Automatically From ISP

● Use These DNS Servers

Primary DNS Server: 0 . 0 . 0 . 0

Secondary DNS Server: 0 . 0 . 0 . 0

Modem Type

Serial Line Speed: 115200

Modem Type: 26. U.S. Robotics 56K FAX EXT PnP

For User Defined Modem: Initial String: AT&F

Dialup Type: ● Tone ○ Pulse ○ Other - use Dial String:

Apply Reset

Figure 2-4

2. Enter the following **Dialup Account** settings:

   a. **Account/User name**: Enter the account name or the user name provided by your ISP. This name will be used to log in to the ISP server.

   b. **Password**: The account password for the dialup ISP

   c. **Telephone**: The telephone number or access number to dial for connectivity. Type in the number using the format described in your modem's user manual.

   d. **Alternative Telephone**: An alternative number which will be dialed if the first is not available (optional).

3. Specify the method to use for your **Dial-up Connection Status.** The VPN firewall can automatically dial to the ISP when a connection is needed or can be configured to wait for manual intervention.:
   a. Check the **Connect automatically disconnect after idle for ___ min.** radios box for the modem to connect automatically. Specify the idle minute amount. The router will connect whenever an outbound connection request is made from a computer on the LAN. The connection will be terminated if there is no data transfer during the specified time interval.
   b. Check the **Connect and disconnect manually** radio box to disable auto dialing and allow manual control over connecting via dial-up. To connect manually, click the **DIAL-Up Status** link at the top and then click **Connect** or **Disconnect**.
4. Internet (IP Address). DialUp ISPs usually assign the IP address automatically when connecting.
   a. The default setting of **Get Dynamically from ISP** will configure the router to accept the ISP assigned IP address.
   b. If your ISP has assigned a static IP address, select the **Use Static IP Address** radio box and enter the IP address in the **IP Address** field.
5. Check the **Get Automatically From ISP** radio box to use ISP assigned DNS server addresses (default). To use different DNS addresses, check the **Use These DNS Servers** radio box and type in the DNS server IP addresses in the **Primary DNS Server** and **Secondary DNS Server** (optional) fields.
6. Click **Apply** to save your settings or **Cancel** to revert to the previous settings.
7. Enter any modem specific parameters to tune the router for different modems:
   c. **Serial Line Speed**: Select the baud rate with which the serial port of the router and the modem connect. Available speeds range from 4.8Kbps to 460.8Kbps.
   d. **Modem Type**: If your modem type is listed in the pull-down menu, select it. For most 56Kbps modems, the U.S. Robotics 56K FAX EXT PnP selection should work. If this does not work, select **User Defined Modem** and type in the Initial String for your modem. The Initial string is usually defined in the modem’s user manual.
   e. **Dial-up Type**: Check the **Tone** radio box if your phone line supports touch tone dialing; select **Pulse** for pulse mode dialing. Select **Other – use Dial String** to configure additional options such as Auto-Answer, etc. (consult your modem manual for dial strings).

Set up the traffic meter for the Dialup ISP if desired (see "Programming the Traffic Meter (if Desired)" on page 2-12).

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

Tip: If you experience connectivity problems with the Dialup ISP, try a different baud rate setting and ensure that the modem parameters you selected match the modem connected to the FVS338.

Setting the Router's MAC Address (Advanced Options)

Each computer or router on your network has a unique 48-bit local Ethernet address. This is also referred to as the computer's MAC (Media Access Control) address. The default is set to **Use Default Address**. If your ISP requires MAC authentication and another MAC address has been previously registered with your ISP, then you must enter that address.

To change the router's default MAC Address:

1. Select **Network Configuration** from the main menu, **Broadband ISP Settings** from the submenu and click the **Advanced** link. Check the radio box for either:

   a. **Use This computer's MAC** address, if this is the address your ISP expects, or

   b. **Use this MAC Address** and enter the MAC address that your ISP expects.

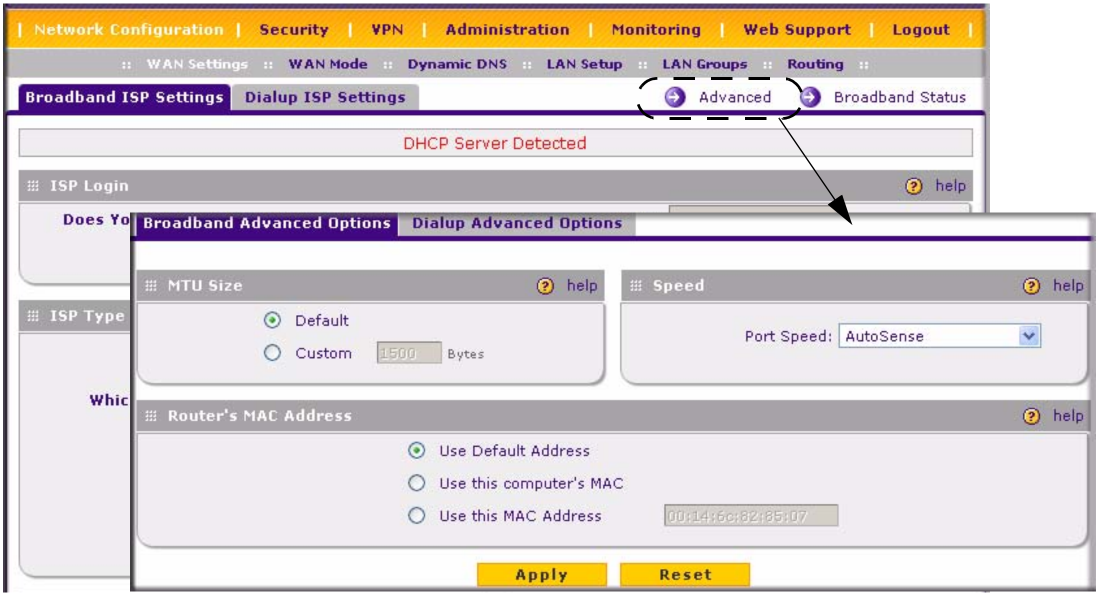
   The format for the MAC address is XX:XX:XX:XX:XX:XX where X is a number from 0 to 9 (inclusive) or an alphabetical letter between A and F (inclusive).

2. Click **Apply** to save your settings or **Cancel** to revert to the previous settings

You may also change the default MTU Size and Port Speed for the Broadband link on this screen, based on the following criteria:

- **MTU Size**. The standard MTU (Maximum Transmit Unit) value for Ethernet networks is either 1500 Bytes or 1492 Bytes for PPPoE connections. Some ISPs may ask you to reduce the MTU, but this is rarely required, and should not be done unless required by your ISP.
- **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.

This could occur on some older broadband modems. If you know that the Ethernet port on your broadband modem supports 100BaseT, select 100BaseT; otherwise, select 10BaseT. Use the half-duplex settings if full-duplex modes do not work.


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
WAN Settings :: WAN Mode :: Dynamic DNS :: LAN Setup :: LAN Groups :: Routing
Broadband ISP Settings
Dialup ISP Settings
Advanced
Broadband Status
ISP Login
help
Does Yo
ISP Type
Whic
Broadband Advanced Options
Dialup Advanced Options
Apply
Reset

DHCP Server Detected

MTU Size

● Default
○ Custom 1500 Bytes

Speed

Port Speed: AutoSense

Router's MAC Address

● Use Default Address
○ Use this computer's MAC
○ Use this MAC Address 00:14:6c:82:85:07

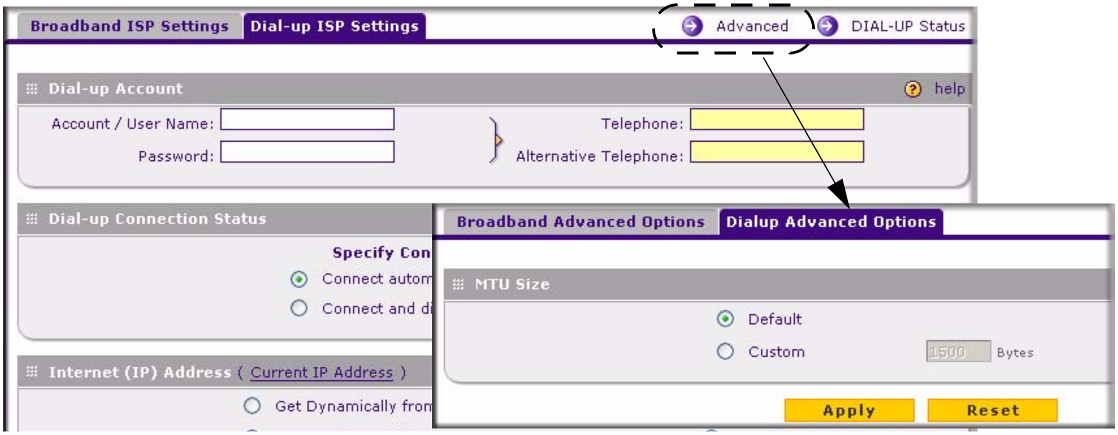
Figure 2-5

You can also change the standard MTU (Maximum Transmit Unit) value for dialup modems from the **Dialup ISP Settings** screen. THe standard value is 576 bytes, but some ISPs may require that you reduce the MTU. However, this is rarely required, and should not be done unless specifically required by the ISP,

To change the MTU value for your dialup modem:

1. Select **Network Configuration** from the main menu, **WAN Settings** from the submenu and the **Dialup ISP Settings** tab. Click the **Advanced** link on the **Dialup ISP Settings** screen.
2. Select the Custom radio box and enter the MTU value, in bytes.
3. Click **Apply** to save your settings.

.



Broadband ISP Settings | Dial-up ISP Settings | Advanced | DIAL-UP Status

Dial-up Account | help

Account / User Name:
Password:
Telephone:
Alternative Telephone:

Dial-up Connection Status

Specify Con
◉ Connect autom
○ Connect and di

Internet (IP) Address (Current IP Address)

○ Get Dynamically from

Broadband Advanced Options | Dialup Advanced Options

MTU Size

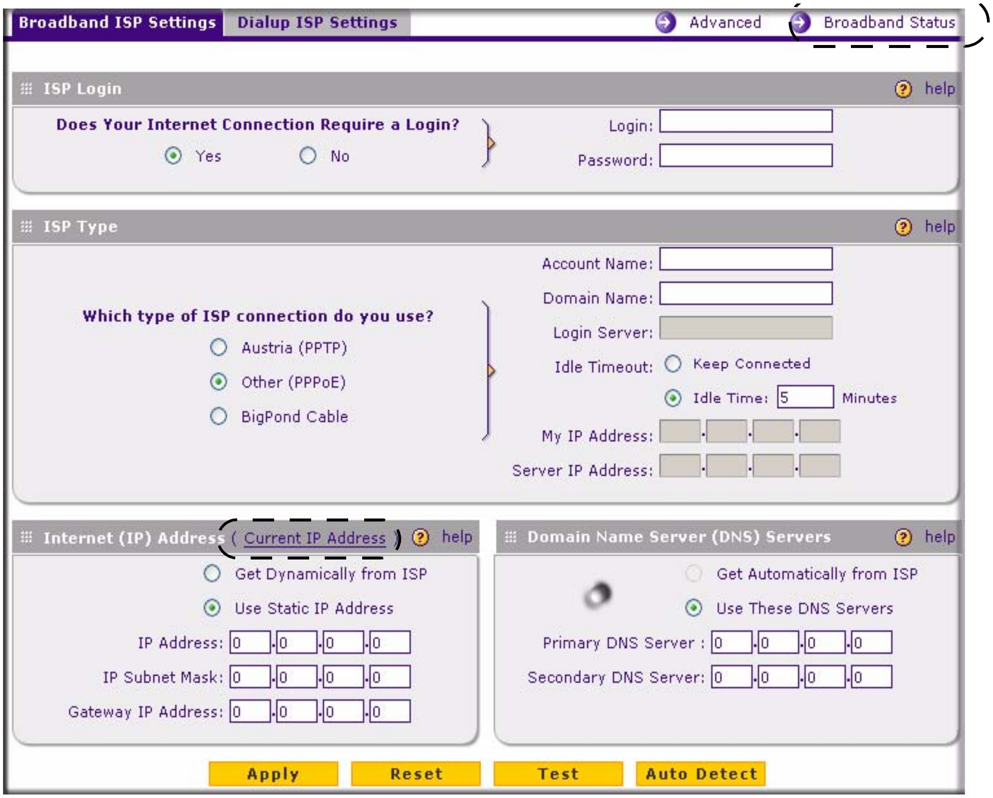
◉ Default
○ Custom 1500 Bytes

Apply | Reset

Figure 2-6

Manually Configuring Your Internet Connection

If you know your Broadband ISP connection type, you can bypass the Auto Detect feature and connect your router manually. Ensure that you have all of the relevant connection information such as IP Addresses, account information, type of ISP connection, etc., before you begin. Unless your ISP automatically assigns your configuration automatically via DHCP, you will need the configuration parameters from your ISP



ISP Login

Does Your Internet Connection Require a Login?

● Yes ○ No

Login:

Password:

ISP Type

Which type of ISP connection do you use?

○ Austria (PPTP)

● Other (PPPoE)

○ BigPond Cable

Account Name:

Domain Name:

Login Server:

Idle Timeout: ○ Keep Connected

● Idle Time: 5 Minutes

My IP Address:

Server IP Address:

Internet (IP) Address (Current IP Address)

○ Get Dynamically from ISP

● Use Static IP Address

IP Address: 0 . 0 . 0 . 0

IP Subnet Mask: 0 . 0 . 0 . 0

Gateway IP Address: 0 . 0 . 0 . 0

Domain Name Server (DNS) Servers

○ Get Automatically from ISP

● Use These DNS Servers

Primary DNS Server : 0 . 0 . 0 . 0

Secondary DNS Server: 0 . 0 . 0 . 0

Figure 2-7

To manually configure your WAN1 ISP settings:

1. **Does your Internet connection require a login**? If you need to enter login information every time you connect to the Internet through your ISP, select Yes. Otherwise, select No.

2. **What type of IPS connection do you use?** If your connection is PPPoE, PPTP or BigPond Cable, then you must login. Check the Yes radio box. The text box fields that require data entry will be highlighted, based on the connection that you selected. If your ISP has not assigned any login information, then choose the No radio box and skip this section. For example:

   - **Austria (PPTP)**: If your ISP is Austria Telecom or any other ISP that uses PPTP for login, select this. Then, fill in the following highlighted fields:

     – **Account Name** (also known as Host Name or System Name): Enter the valid account name for the PPTP connection (usually your email “ID” assigned by your ISP). Some ISPs require entering your full email address here.

   - **Domain Name**: Your domain name or workgroup name assigned by your ISP, or your ISPs domain name. You may leave this field blank.
   - **Idle Timeout**: Check the Keep Connected radio box to keep the connection always on. To logout after the connection is idle for a period of time, select Idle Time and enter the number of minutes to wait before disconnecting in the timeout field. This is useful if your ISP charges you based on the amount of time you have logged in.
   - **My IP Address:** IP address assigned by the ISP to make the connection with the ISP server.
   - **Server IP Address**: IP address of the PPTP server.
- **Other (PPPoE)**: If you have installed login software such as WinPoET or Enternet, then your connection type is PPPoE. Select this connection and configure the following fields:
   - **Account Name**: Valid account name for the PPPoE connection
   - **Domain Name:** Name of your ISPs domain or your domain name if your ISP has assigned one. You may leave this field blank.
   - **Idle Timeout:** Select Keep Connected, to keep the connection always on. To logout after the connection is idle for a period of time, select Idle Time and enter the number of minutes to wait before disconnecting, in the timeout field.
- **BigPond Cable**: If your ISP is Telstra BigPond Cable, select this option and fill in the Login Server and Idle Timeout fields. The Login Server is the IP address of the local BigPond Login Server in your area. You can find login server information at http://www.netgear.com.sg/support/bigpond.asp

3. If your ISP has assigned a fixed (static or permanent) IP address, select the **Use Static IP Address** radio box and fill in the following fields:
   a. **IP Address:** Static IP address assigned to you. This will identify the router to your ISP.
   b. **Subnet Mask**: This is usually provided by the ISP or your network administrator.
   c. **Gateway IP Address**: IP address of the ISP’s gateway. This is usually provided by the ISP or your network administrator.

   If your ISP has not assigned a Static IP address, select the **Get dynamically from ISP** radio box. The ISP will automatically assign an IP address to the router using DHCP network protocol.

4. If your ISP has not assigned any Domain Name Servers (DNS) addresses, select the **Get dynamically from ISP** radio box. If your ISP has assigned DNS addresses, select the **Use these DNS Servers** radio box. Ensure that you fill in valid DNS server IP addresses in the fields. Incorrect DNS entries may cause connectivity issues.

> **Note:** Domain name servers (DNS) convert Internet names such as www.google.com, www.netgear.com, etc. to Internet addresses called IP addresses. Incorrect settings here will result in connectivity problems.

5. Click **Apply** to save the settings or click **Cancel** to revert to the previous settings.
6. Click **Test** to try and connect to the NETGEAR Web site. If you connect successfully and your settings work, then you may click Logout or go on and configure additional settings.

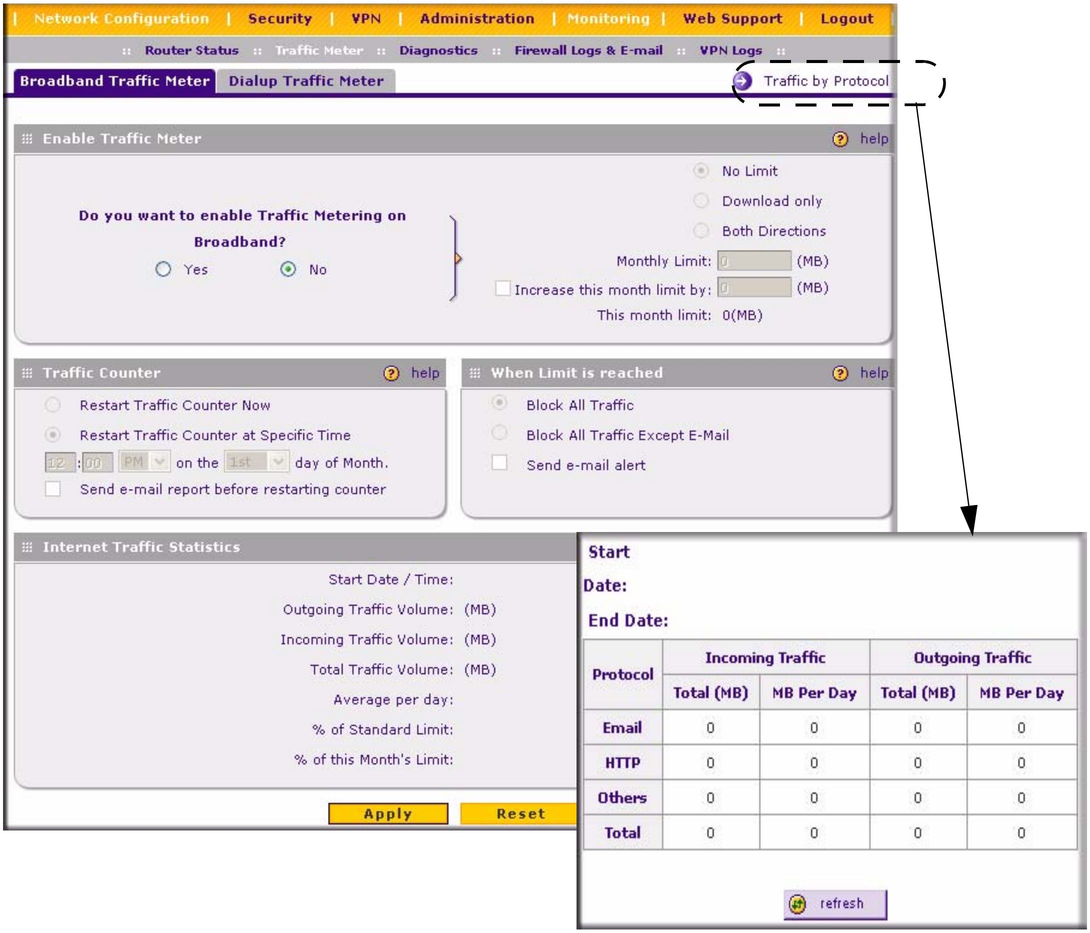
   You can also click on the **Broadband Status** link or the **Current IP Address** link to check on connection status and current IP address.

Programming the Traffic Meter (if Desired)

The traffic meter is useful when an ISP charges by traffic volume over a given period of time or if you want to look at traffic types over a period of time.

To enable the traffic meter:

1. From the primary menu, select **Monitoring**, and then select **Traffic Meter** from the secondary menu. The **Broadband Traffic Meter** screen will display. Fill out the information described in Table 2-2.
2. Click **Apply** to apply the settings or click **Cancel** to return to the previous settings.
3. Select the **Dialup Traffic Meter** tab and repeat steps 1 through 3 to set the Traffic Meter the the Dialup port (if required).


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
:: Router Status :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Broadband Traffic Meter
Dialup Traffic Meter
Traffic by Protocol
help
Apply
Reset
refresh

Enable Traffic Meter

Do you want to enable Traffic Metering on Broadband?

○ Yes ● No

● No Limit

○ Download only

○ Both Directions

Monthly Limit: 0 (MB)

□ Increase this month limit by: 0 (MB)

This month limit: 0(MB)

Traffic Counter

○ Restart Traffic Counter Now

● Restart Traffic Counter at Specific Time

12 : 00 PM on the 1st day of Month.

□ Send e-mail report before restarting counter

When Limit is reached

● Block All Traffic

○ Block All Traffic Except E-Mail

□ Send e-mail alert

Internet Traffic Statistics

Start Date / Time:

Outgoing Traffic Volume: (MB)

Incoming Traffic Volume: (MB)

Total Traffic Volume: (MB)

Average per day:

% of Standard Limit:

% of this Month's Limit:

Start Date:

End Date:

Protocol	Incoming Traffic		Outgoing Traffic	
	Total (MB)	MB Per Day	Total (MB)	MB Per Day
Email	0	0	0	0
HTTP	0	0	0	0
Others	0	0	0	0
Total	0	0	0	0

Figure 2-8

Table 2-2. Traffic Meter Settings

Parameter	Description
Enable Traffic Meter	Check this if you wish to record the volume of Internet traffic passing through the Router's Broadband or Dialup port. Broadband or Dialup can be selected by clicking the appropriate tap; the entire configuration is specific to each interface. • No Limit - If this is selected specified restriction will not be applied when traffic limit is reached. • Download only - If this is selected the specified restriction will be applied to the incoming traffic only • Both Directions - If this is selected the specified restriction will be applied to both incoming and outgoing traffic only
Enable Monthly Limit	Use this if your ISP charges for additional traffic. If enabled, enter the monthly volume limit and select the desired behavior when the limit is reached. **Note**: Both incoming and outgoing traffic are included in the limit.
Increase this month's limit	Use this to temporarily increase the Traffic Limit if you have reached the monthly limit, but need to continue accessing the Internet. Check the checkbox and enter the desired increase. (The checkbox will automatically be cleared when saved so the increase is only applied once.)
This month's limit	This displays the limit for the current month.
Restart traffic counter	This determines when the traffic counter restarts. Choose the desired time and day of the month.
Restart Counter at a Specific Time	Check this radio button to restart the Traffic Counter at a specific time and day of the month. Fill in the time fields and select AM or PM and the day of the month from the pull-down menus.
Send E-mail Report before restarting counter	If checked, an E-mail report will be sent immediately before restarting the counter. You must configure the E-mail screen in order for this function to work (see "E-Mail Notifications of Event Logs and Alerts" on page 4-27).
When limit is reached	Select the desired option: • Block all traffic – all access to and from the Internet will be blocked. • Block all traffic except E-mail – Only E-mail traffic will be allowed. All other traffic will be blocked. • If using this option, you may also select the Send E-mail alert option. You must configure the E-mail screen in order for this function to work.
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 link 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, counter starts only when traffic passed is at least 1MB.

Configuring the WAN Mode

The **WAN Mode** screen allows you to configure how your router uses your external Internet connections; for example, your WAN port or dialup modem connections.

- **NAT.** NAT is the technology which allows all PCs on your LAN to share a single Internet IP address. Viewed from the Internet, the WAN port on the VPN firewall is configured with a single IP address—the “public” address. PCs on your LAN can use any “private” IP address range, and these IP addresses are not visible from the Internet.
  - The Router uses NAT to select the correct PC (on your LAN) to receive any incoming data and hides internal IP addresses from computers on the Internet.
  - If you only have a single Internet IP address, you MUST use NAT.

  NAT is the default setting. Select NAT if your ISP has assigned only one IP address to you. The computers that connect through the router must then be assigned IP addresses from a private subnet (for example: 192.168.1.0).
- **Classical Routing.** In this mode, the Router performs Routing, but without NAT. To gain Internet access, each PC on your LAN must have a valid Internet IP address.

  If your ISP has allocated many IP addresses to you, and you have assigned one of these addresses to each PC, you can choose Classical Routing. Or, you can use Classical Routing for routing private IP addresses within a campus environment. Otherwise, selecting this method will not allow Internet access through this Router.

➡	**Note:** The router will delete all inbound firewall rules when switching between NAT and Classical Routing.

To configure the WAN Mode:

1. Select **Network Configuration** from the main menu and **WAN Mode** from the submenu. The **WAN Mode** screen will display.
2. Check either the **NAT** or **Classical Routing** radio box. NAT is the default.
3. Select the **Port Mode.** The Port Mode settings allow you to configure your router to use only one WAN port or to select the Dialup port as a backup.
   - If you are connected to only one ISP, then check the **Use only single WAN port** and select the WAN port that is connected to your ISP from the pull down menu.

   - If you have both ISP links connected for Internet connectivity, check the **Primary Broadband with Dialup as backup** for auto-rollover**.**

4. The WAN Failure Detection Method must be configured to notify the router of a link failure if you are using Dialup as a backup to engage auto-rollover. The router checks the connection of the primary link at regular intervals to detect its status. Check the radio box of one the following methods to detect link failure:
   - Select **DNS lookup using configured DNS Servers** to detect failure of the Broadband link, using the DNS servers configured in the **Broadband ISP Settings** screen.
   - Select **DNS lookup using this DNS Server** and enter the IP address of the DNS server to specify a DNS server for detecting WAN failure
   - Select **Ping to this IP address** and enter an IP address to detect WAN failure by pinging to an IP address. Ensure that this destination host is reliable.

   If a failure is detected on the primary broadband connection, the secondary dialup connection connects to the Internet. When the primary connection is detected as back online, the secondary dialup connection disconnects.
5. Enter a **Test Period,** in seconds, to tell the router how often it should run the configured detection method. The default is 30 seconds.
6. Enter the number of router failures that should occur before the router rolls-over to the Dialup port. The default is 4.
7. Enter **Apply** to save your settings or **Cancel** to revert to the previous settings.

Configuring Dynamic DNS (If Needed)

> **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 be available since private addresses cannot be routed on the Internet.

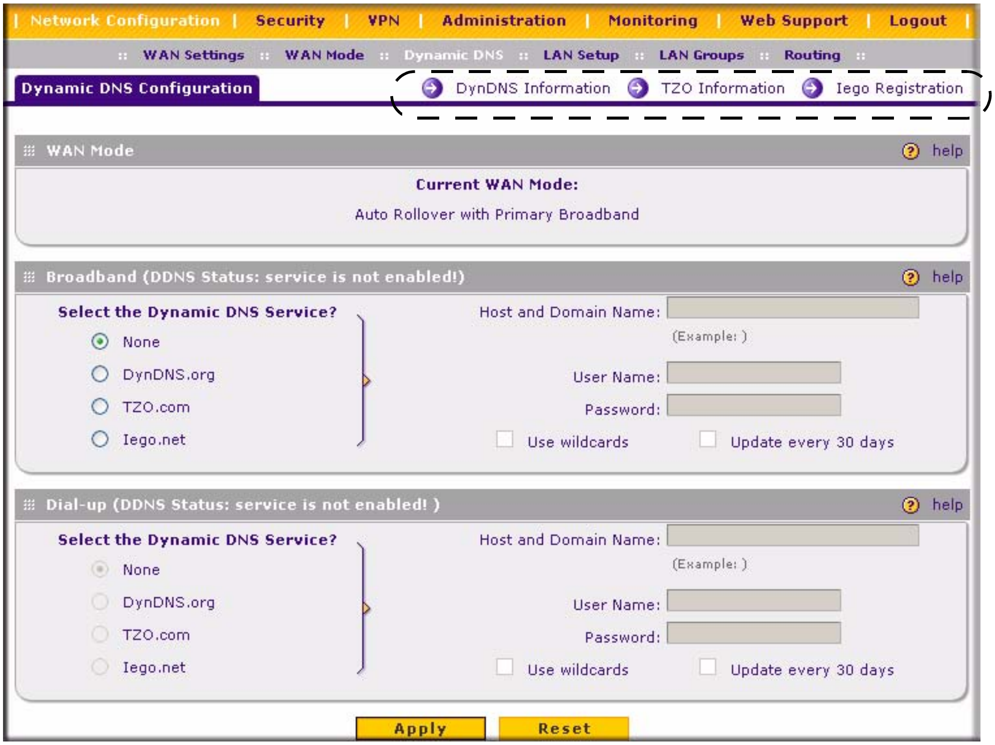
Dynamic DNS (DDNS) is an Internet service that allows routers with varying public IP addresses to be located using Internet domain names. To use DDNS, you must setup an account with a DDNS provider such as DynDNS.org, TZO.com or Iego.net.

Once you have registered your domain name to their IP address, all FQDN traffic will be directed to your frequently-changing IP address. (For rollover mode, you will 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.)

This router firmware includes software that notifies dynamic DNS servers of changes in the WAN IP address, so that the services running on this network can be accessed by others on the Internet. 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.

To configure a Dynamic DNS address:

1. Select **Network Configuration** from the main menu and **Dynamic DNS** from the submenu. The **Dynamic DNS Configuration** screen displays. The **WAN Mode** section displays the currently configured WAN Mode: Single Port or Auto-Rollover.



| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: WAN Mode :: Dynamic DNS :: LAN Setup :: LAN Groups :: Routing ::
DynDNS Information
TZO Information
Iego Registration
help
Apply
Reset

Dynamic DNS Configuration

WAN Mode

Current WAN Mode:

Auto Rollover with Primary Broadband

Broadband (DDNS Status: service is not enabled!)

Select the Dynamic DNS Service?

● None

○ DynDNS.org

○ TZO.com

○ Iego.net

Host and Domain Name:

(Example:)

User Name:

Password:

□ Use wildcards □ Update every 30 days

Dial-up (DDNS Status: service is not enabled!)

Select the Dynamic DNS Service?

● None

○ DynDNS.org

○ TZO.com

○ Iego.net

Host and Domain Name:

(Example:)

User Name:

Password:

□ Use wildcards □ Update every 30 days

Figure 2-9

If you have configured Single Port, choose a DNS service provider, then fill out the DDNS section for that port. If you have enabled Auto-Rollover, choose a service provider and complete both sections. (Only those options that match the configured WAN Mode will be accessible.)

2. Check the Dynamic DNS Service radio box you want to enable. The fields corresponding to the selection you have selected will be highlighted. Each DNS service provider requires its own parameters.
3. Access the Web site of one of the DDNS service providers and set up an account. A link to each DDNS provider is opposite the DNS Configuration screen name.
4. After setting up your account, return to the Dynamic DNS Configuration screen and fill in the required fields for the DDNS service you selected:
   - a. In the Host and Domain Name field, enter the entire FQDN name that your dynamic DNS service provider gave you (for example: <*yourname*>.dyndns.org).
   - b. Enter the User Name, User email Address, or Account Name requested by the DDNS Service to identify you when logging into your DDNS account.
   - c. Enter the Password, or User Key, for your DDNS account.
   - d. If your dynamic DNS provider allows the use of wild cards in resolving your URL, you may check the **Use wildcards** radio 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`
5. Click **Apply** to save your configuration or click **Cancel** your settings and revert to the previous settings.

Chapter 3
LAN Configuration

This chapter describes how to configure LAN Setup, LAN Groups and Routing (Static IP) features of your ProSafe VPN Firewall 50. These features can be found under the **Network Configuration** menu of the router interface.

Configuring Your LAN (Local Area Network)

By default, the firewall will function as a DHCP (Dynamic Host Configuration Protocol) server, allowing it to assign IP, DNS server, WINS Server, and default gateway addresses to all computers connected to the firewall 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.

Using the VPN Firewall as a DHCP Server

For most applications, the default DHCP and TCP/IP settings of the firewall are satisfactory. See the link to "Preparing a Computer for Network Access:" in Appendix B for an explanation of DHCP and information about how to assign IP addresses for your network.

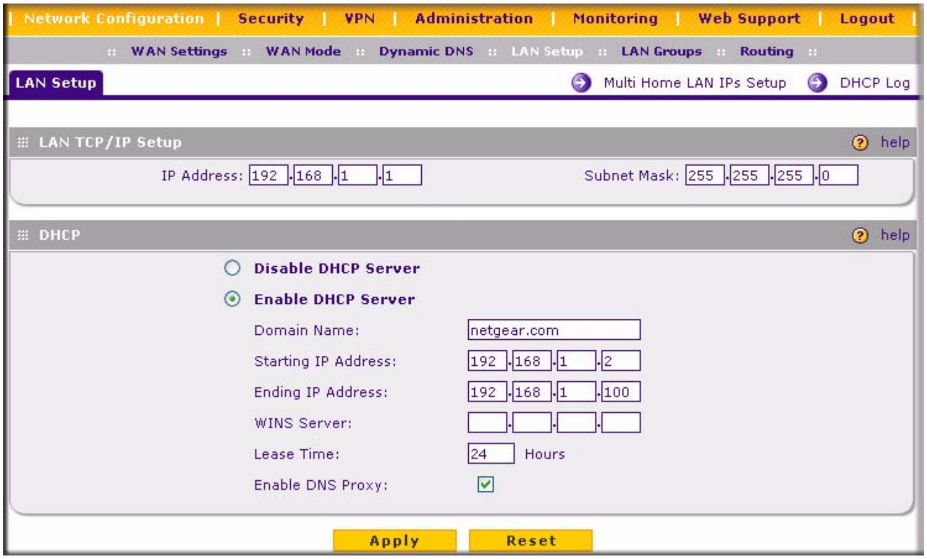
The firewall will deliver the following parameters to any LAN device that requests DHCP:

- An IP Address from the range you have defined
- Subnet Mask
- Gateway IP Address (the firewall's LAN IP address)
- Primary DNS Server (the firewall's LAN IP address)
- WINS Server (if you entered a WINS server address in the DHCP Setup menu)
- Lease Time (date obtained and duration of lease).

The **LAN Setup** screen allows you to configure the LAN on your router. The default values are suitable for most users and situations.

To modify your LAN setup:

1. Select **Network Configuration** from the main menu and **LAN Setup** from the submenu. The **LAN Setup** screen will display.


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: WAN Mode :: Dynamic DNS :: LAN Setup :: LAN Groups :: Routing ::
LAN Setup
Multi Home LAN IPs Setup
DHCP Log
help
help
Apply
Reset

LAN TCP/IP Setup

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

DHCP

○ Disable DHCP Server

● Enable DHCP Server

Domain Name: netgear.com

Starting IP Address: 192 . 168 . 1 . 2

Ending IP Address: 192 . 168 . 1 . 100

WINS Server: . . .

Lease Time: 24 Hours

Enable DNS Proxy: ☑

Figure 3-1

2. Enter the **IP Address** of your router (factory default: **192.168.1.1**). (Always make sure that the LAN Port IP address and DMZ port IP address are in different subnets.)

3. Enter the **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).

4. Check the **Enable DHCP Server** radio button. 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, check the **Disable DHCP Server** radio button. Enable DHCP Server is the default. If Enabled is selected, enter the following parameters:

   a. Enter the **Domain Name** of the router (this is optional).

b. Enter the **Starting IP Address**. This address specifies the first of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN will be assigned an IP address between this address and the Ending IP Address. The IP address 192.168.1.2 is the default start address.

c. Enter the **Ending IP Address**. This address specifies the last of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN will be assigned an IP address between the Starting IP address and this IP address. The IP address 192.168.1.100 is the default ending address.

> ➡ **Note:** The Starting and Ending DHCP addresses should be in the same “network” as the LAN TCP/IP address of the router (the IP Address in **LAN TCP/IP Setup** section).

d. Enter a **WINS Server** IP address. This box can specify the Windows NetBios Server IP if one is present in your network. This field is optional.

e. Enter a **Lease Time.** This specifies the duration for which IP addresses will be leased to clients.

f. Check the **Enable DNS Proxy** radio box. This is optional—the default is enabled. If enabled, the VPN firewall will provide a LAN IP Address for DNS address name resolution.

> ➡ **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. For example, if you change the default IP address **192.168.1.1** to **10.0.0.1**, you must enter **http://10.0.0.1** in your browser to connect to the web management interface.

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

6. Click **Reset** to discard any changes and revert to the previous configuration.

> ➡ **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 4, “Firewall Protection and Content Filtering.”

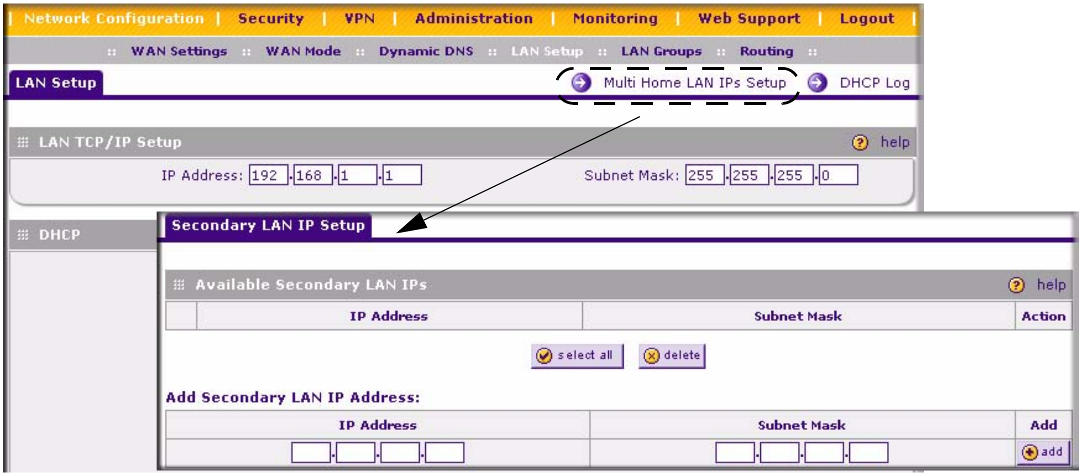
Configuring Multi-Home LAN IPs

If you have computers that are using different IP address ranges in the LAN (for example, 172.16.2.0 or 10.0.0.0), then you can add "aliases" to the LAN port which give computers on those networks access to the Internet. This allows the firewall to act as a gateway to additional logical subnets on your LAN.

To add a secondary LAN IP address:

1. Select **Network Configuration** from the main menu and **LAN Setup** from the secondary menu. Click the **Multi Home LAN IPs Setup** link (see Figure 3-2 on page 3-4) The Secondary LAN IP Setup screen will display.
2. Enter the Secondary IP address and Subnet Mask and click **Add.** The Secondary IP address will be added to the **Available Secondary LAN IPs** table.

Note: Additional IP addresses cannot be configured in the DHCP server. The hosts on the secondary subnets must be manually configured with IP addresses, gateway IP and DNS server IP addresses.


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
WAN Settings :: WAN Mode :: Dynamic DNS :: LAN Setup :: LAN Groups :: Routing
LAN Setup
Multi Home LAN IPs Setup
DHCP Log
LAN TCP/IP Setup
help
DHCP
Secondary LAN IP Setup
Available Secondary LAN IPs
help
select all
delete
Add Secondary LAN IP Address:
add

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

	IP Address	Subnet Mask	Action

IP Address	Subnet Mask	Add

Figure 3-2

Tip: The Secondary LAN IP address will be assigned to the LAN interface of the router and can be used as a gateway by the secondary subnet.

Managing Groups and Hosts

The **Known PCs and Devices** table on the **Groups and Hosts** screen contains a list of all known PCs and network devices, as well as hosts, that are assigned dynamic IP addresses by this router. Collectively, these entries make up the Network Database. The Network Database is created in two ways:

- **Using the DHCP Server.** The router's DHCP server will accept and respond to DHCP client requests from PCs and other network devices. Every computer that is responded to will be added to the Network Database in the **Known PCs and Devices** table.
- **Scanning the Network**. The router will scan the local network periodically, using standard methods such as ARP and NetBIOS, to detect active computers or devices which are not DHCP clients. For computers that do not support the NetBIOS protocol, the name will be displayed in the **known PCs and Devices** table as "Unknown".

Creating the Network Database

The Network Database offers a number of advantages:

- 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 4-2).
  - You can also select the Groups to be covered by the Block Sites feature (see "Setting Block Sites (Content Filtering)" on page 4-21).
  - If necessary, you can also create Firewall Rules to apply to a single PC (see "Enabling Source MAC Filtering" on page 4-23). Because the MAC address is used to identify each PC, users cannot avoid these restrictions by changing their IP address.

- A computer is identified by its MAC address—not its IP address. Hence, changing a computer's IP address does not affect any restrictions applied to that PC.

This **Known PCs and Devices** table lists entries in the Network Database. For each computer or device, the following fields are displayed:

- **Name**: The name of the PC or device. For computers that do not support the NetBIOS protocol, this will be listed as "Unknown" (you can edit the entry manually to add a meaningful name). If the computer was assigned an IP address by the DHCP server, then the Name will be appended by an asterisk.
- **IP Address**: The current IP address of the computer. For DHCP clients of the router, this IP address will not change. If a computer is assigned a static IP addresses, you will need to update this entry manually if the IP address on the computer has been changed.
- **MAC Address**: The MAC address of the PC's network interface.
- **Group**: Each PC or device can be assigned to a single group. By default, a computer is assigned to Group 1, unless a different group is selected from the Group pull-down menu.
- **Action**: Allows modification of the selected entry by clicking Edit.

To add computers to the network database manually:

1. Select **Network Configuration** from the main menu and **LAN Groups** from the submenu. The **Groups and Hosts** screen will display.
2. In the **Add Known PCs and Devices** table, enter the name of the PC or device.
3. Enter the **IP Address Type**. Select **Reserved (DHCP Client)** to direct the router to reserve the IP address for allocation by the DHCP server. Select **Fixed (Set on PC)** if the IP address is statically assigned on the computer.

> **Note:** When specifying a Reserved IP address, make sure that you select an IP address outside of the DHCP Server pool of addresses.

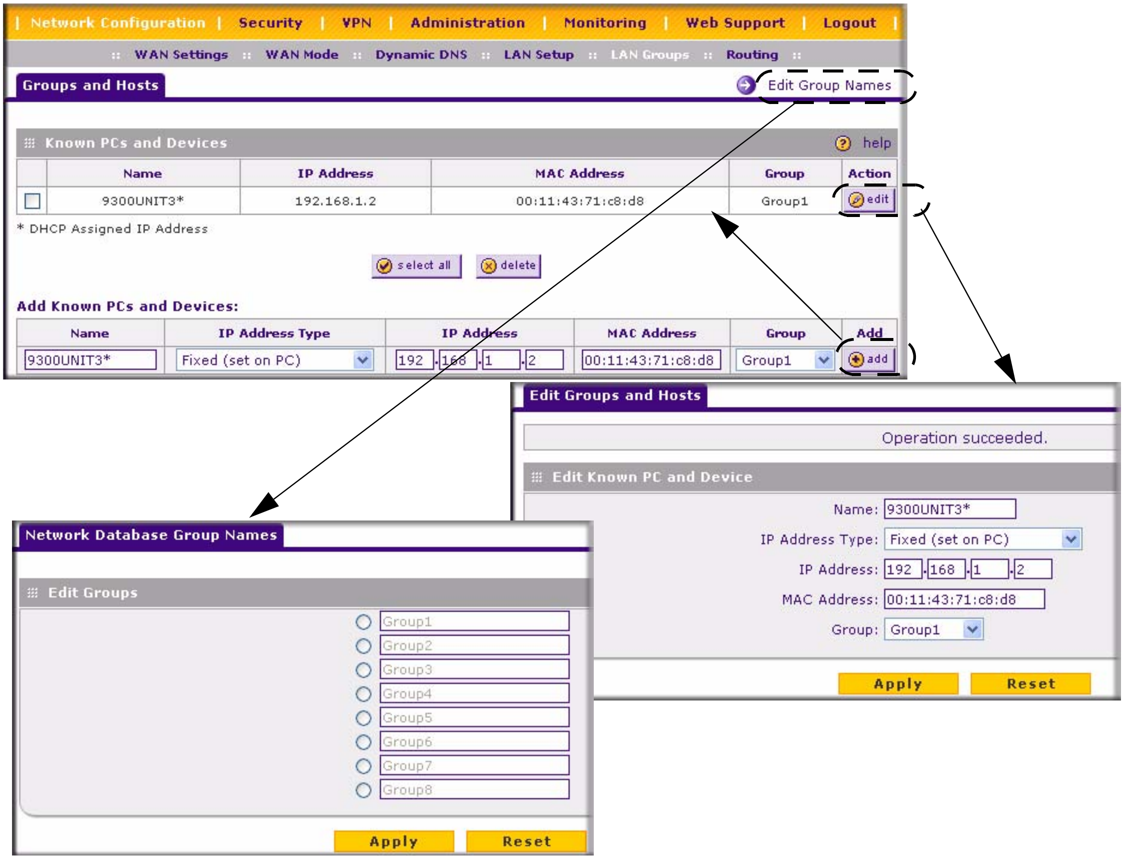
4. Enter the **IP Address** that this computer or device is assigned. If the IP Address Type is Reserved (DHCP Client), the router will reserve the IP address for the associated MAC address.
5. Enter the **MAC Address** of the computer. The MAC address should be in the form: xx:xx:xx:xx:xx:xx (for example: 00:80:48:2a:8b:c0)
6. From the **Group** pull-down menu, select the group to which the computer will be assigned.
7. Click **Add** to add the new entry to the network database in the **Known PCs and Devices** table.

To edit an entry in the **Known PCs and Devices** table:

1. Click **Edit** adjacent to the entry you want to modify. The **Edit Known PCs and Devices** screen will display. Make your modifications to the entry.
2. Click **Apply** to save your settings. The changes will appear the **Known PCs and Devices** table.

To edit a Group Name in the Network Database:

1. On the **Groups and Hosts** screen, click the **Edit Group Names** link.
2. Check the radio button by the group name you want to modify and type in a suitable name.
3. Click Apply to save the settings.


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
WAN Settings :: WAN Mode :: Dynamic DNS :: LAN Setup :: LAN Groups :: Routing
Edit Group Names
help
select all
delete
edit
add

Groups and Hosts

Known PCs and Devices

	Name	IP Address	MAC Address	Group	Action
□	9300UNIT3*	192.168.1.2	00:11:43:71:c8:d8	Group1	edit

* DHCP Assigned IP Address

Add Known PCs and Devices:

Name	IP Address Type	IP Address	MAC Address	Group	Add
9300UNIT3*	Fixed (set on PC)	192 .168 .1 .2	00:11:43:71:c8:d8	Group1	add

Edit Groups and Hosts

Operation succeeded.

Edit Known PC and Device

Name: 9300UNIT3*
IP Address Type: Fixed (set on PC)
IP Address: 192 .168 .1 .2
MAC Address: 00:11:43:71:c8:d8
Group: Group1

Apply Reset

Network Database Group Names

Edit Groups

○ Group1
○ Group2
○ Group3
○ Group4
○ Group5
○ Group6
○ Group7
○ Group8

Apply Reset

Figure 3-3

Setting Up Address Reservation

When you specify a reserved IP address for a device on the LAN (based on the MAC address of the device), that computer or device will always receive the same IP address each time it accesses the firewall’s DHCP server. Reserved IP addresses should be assigned to servers or access points that require permanent IP settings. The Reserved IP address that you select must be outside of the DHCP Server pool.

To reserve an IP address, use the **Groups and Hosts** screen under the **Network Configuration** menu**, LAN Groups** submenu (see “Creating the Network Database” on page 3-5).

➡ **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.

Configuring Static Routes

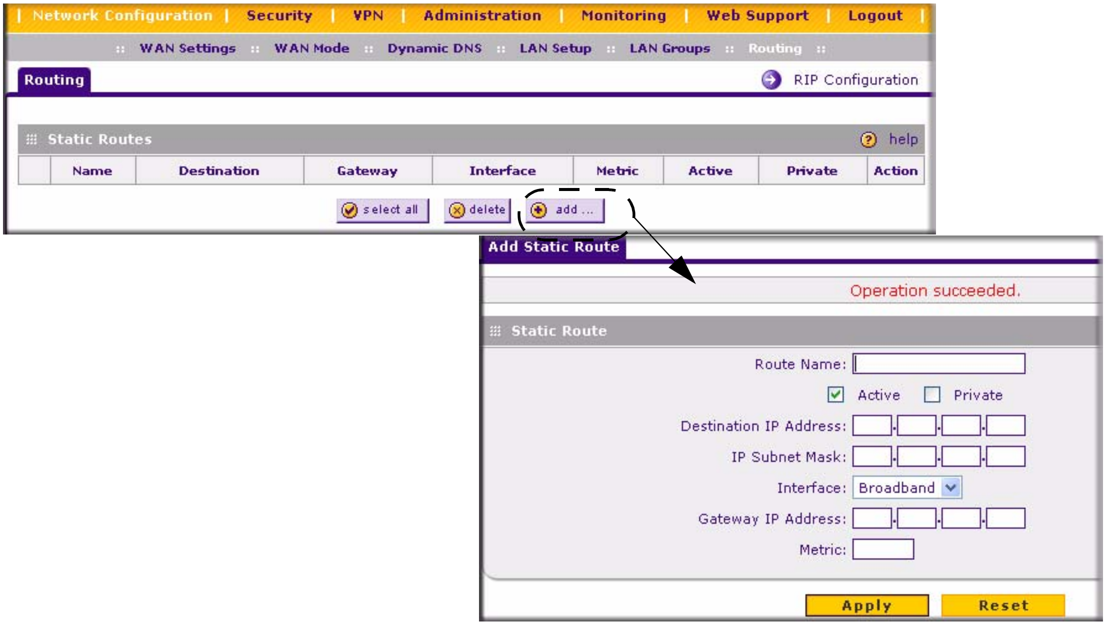
Static Routes provide additional routing information to your firewall. Under normal circumstances, the firewall has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You must configure static routes only for unusual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

To add or edit a Static Route:

1. Select **Network Configuration** from the main menu and **Routing** from the submenu. The **Routing** screen will display.
2. Click **Add.** The **Add Static Route** screen will display.
3. Enter a name for the static route in the **Route Name** field (for identification purpose only).
4. Determine whether the route is
   - **Active** or **Inactive**. A route can be added to the table and made inactive, if not needed. This allows routes to be used as needed without deleting the entry and re-adding it. An inactive route is not broadcast if RIP is enabled. Select the **Active** radio box to make this route effective.
   - **Private**: Determine whether the route can be shared with other routers when RIP is enabled. If Yes, then the route will not be shared in a RIP broadcast or multicast. Check the **Private** radio box if you want to limit access to the LAN only. The static route will not be advertised in RIP.

5. Type the **Destination IP Address** or network of the route's final destination.

6. Enter the **IP Subnet Mask** for this destination. If the destination is a single host, enter 255.255.255.255.


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: WAN Mode :: Dynamic DNS :: LAN Setup :: LAN Groups :: Routing ::
Routing
RIP Configuration
Static Routes
help
select all
delete
add ...
Add Static Route
Static Route
Apply
Reset

	Name	Destination	Gateway	Interface	Metric	Active	Private	Action

Operation succeeded.

Route Name:

☑ Active □ Private

Destination IP Address:

IP Subnet Mask:

Interface: Broadband

Gateway IP Address:

Metric:

Figure 3-4

7. From the **Interface** pull-down menu, selection the physical network interface (Broadband, Dialup, or LAN) through which this route is accessible.

8. Enter the **Gateway IP Address** (which must be a firewall on the same LAN segment as the firewall) of the gateway through which the destination host or network can be reached.

9. Enter the **Metric** value that determines the priority of the route. If multiple routes to the same destination exist, the route with the lowest metric is chosen. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.

10. Click **Apply** to save the static route to the **Static Routes** table.

Static Route Example

For example, a static route is needed if:

- Your primary Internet access is through a cable modem to an ISP.

- You have an ISDN firewall on your home network for connecting to the company where you are employed. This firewall's address on your LAN is 192.168.1.100.
- Your company's network is 134.177.0.0.

When you first configured your firewall, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.1.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your firewall will forward your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company's firewall.

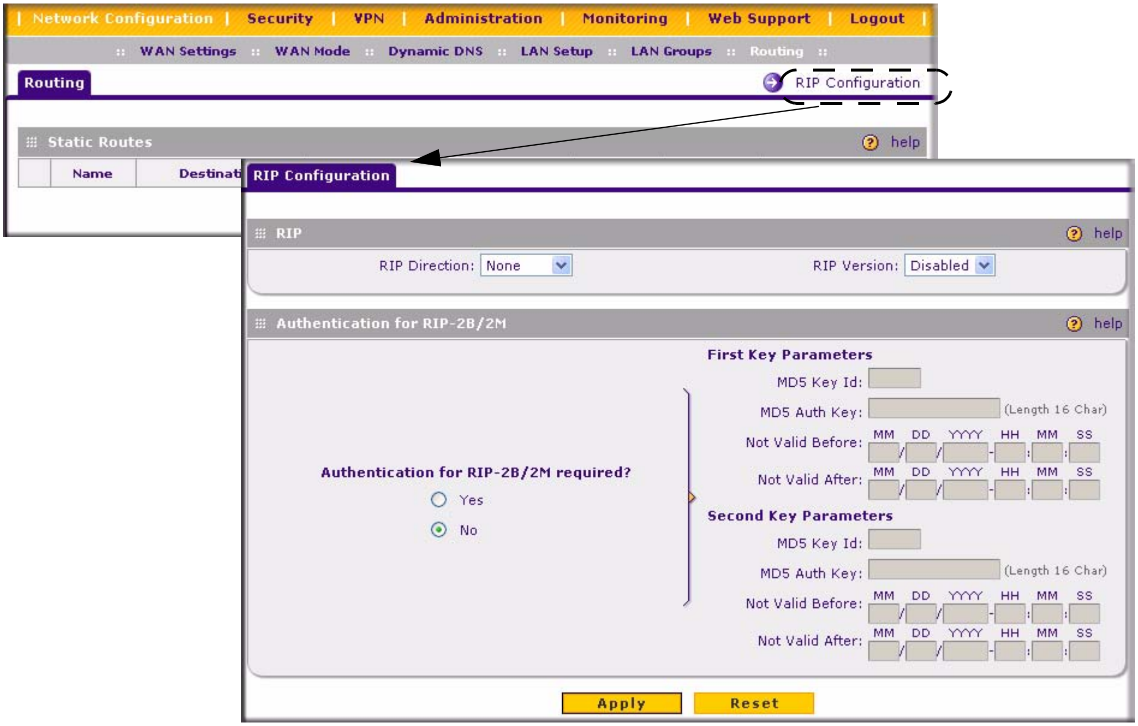
In this case you must define a static route, telling your firewall that 134.177.0.0 should be accessed through the ISDN firewall at 192.168.1.100.

In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Gateway IP Address fields specifies that all traffic for these addresses should be forwarded to the ISDN firewall at 192.168.1.100.
- A Metric value of 1 will work since the ISDN firewall is on the LAN.
- Private is selected only as a precautionary security measure in case RIP is activated.

RIP Configuration

RIP (Routing Information Protocol, RFC 2453) is an Interior Gateway Protocol (IGP) and is commonly used in internal networks. It allows a router to exchange its routing information automatically with other routers, and allows it to dynamically adjust its routing tables and adapt to changes in the network. RIP is disabled by default.


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: WAN Mode :: Dynamic DNS :: LAN Setup :: LAN Groups :: Routing ::
Routing
RIP Configuration
Static Routes
help
Name
Destinati
RIP Configuration
Apply
Reset

RIP

RIP Direction: None

RIP Version: Disabled

Authentication for RIP-2B/2M

Authentication for RIP-2B/2M required?

○ Yes

● No

First Key Parameters

MD5 Key Id:

MD5 Auth Key: (Length 16 Char)

Not Valid Before: MM / DD / YYYY - HH : MM : SS

Not Valid After: MM / DD / YYYY - HH : MM : SS

Second Key Parameters

MD5 Key Id:

MD5 Auth Key: (Length 16 Char)

Not Valid Before: MM / DD / YYYY - HH : MM : SS

Not Valid After: MM / DD / YYYY - HH : MM : SS

Figure 3-5

To enable RIP:

1. Select **Network Configuration** from the main menu and **Routing** from the submenu. The **Routing** screen will display.
2. Click the **RIP Configuration** link. The **RIP Configuration** screen will display.
3. From the **RIP Direction** pull-down menu, select the direction for the router to send and receive RIP packets:
   - **Both** – the router broadcasts its routing table and also processes RIP information received from other routers.
   - **Out Only** – the router broadcasts its routing table periodically but does not accept RIP information from other routers.
   - **In Only** – the router accepts RIP information from other routers, but does not broadcast its routing table.

- **None** – the router neither broadcasts its route table nor does it accept any RIP packets from other routers. This effectively disables RIP.

4. Select the **RIP Version** from the pull-down menu:
   - **RIP-1** – classful routing and does not include subnet information. This is the most commonly supported version.
   - **RIP-2** – supports subnet information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format:
   - **RIP-2B** – uses subnet broadcasting.
   - **RIP-2M** – uses multicasting (see Note below).
5. RIP authentication is disabled by default. To enable authentication for RIP-2B or RIP-2M,
   a. Check the **Yes** radio button.
   b. Input MD5 keys and effective and end dates for the **First Key Parameters** and **Second Key Parameters** for MD5 based authentication between routers.
6. Click **Apply** to save your settings.

➡ **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 you select MD5 then you need to enter additional parameters.

Enabling Trend Micro Antivirus Enforcement

If you have installed the Trend Micro Client/Server Messaging Suite for SMB on your local network, the firewall can enforce antivirus scanning. When Antivirus Enforcement is selected, local PCs will not be allowed web access unless they have the Trend Micro OfficeScan client installed and updated with the latest virus definitions.

To enable Trend Micro Antivirus Enforcement:

1. Select **Security** from the main menu and **Trend Micro** from the submenu. The **Trend Micro** screen sill display.\
2. Check the **Yes** radio box for **Do you want to enable antivirus Enforcement?.**

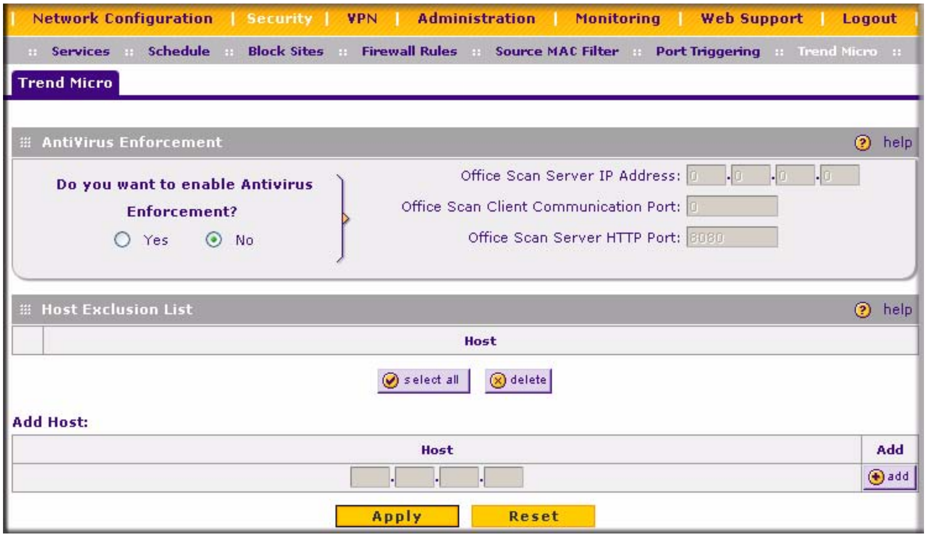
3. Enter the IP address of the **OfficeScan Server** on your local network.
4. Enter the 5-digit port number used for communications between the OfficeScan clients and the server.
5. Click **Apply** to enable Trend Micro.

The Host Exclusion List table lists PCs that are allowed to access the WAN without OfficeScan client.

Note: The OfficeScan Server must appear in the exclusion list.

To allow a PC to access the web without the OfficeScan client:

Enter the IP address of the PC in the **Host** field in the **Add Host** section and click **Add.** The address will be added to the **Host Exclusion List** table.


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
:: Services :: Schedule :: Block Sites :: Firewall Rules :: Source MAC Filter :: Port Triggering :: Trend Micro ::
Trend Micro
help
select all
delete
add
Apply
Reset

AntiVirus Enforcement

Do you want to enable Antivirus Enforcement?

○ Yes ● No

Office Scan Server IP Address: 0 . 0 . 0 . 0

Office Scan Client Communication Port: 0

Office Scan Server HTTP Port: 8080

Host Exclusion List

	Host

Add Host:

Host	Add
. . .	add

Figure 3-6

Note: Follow the instructions in the Trend Micro documentation to complete the installation and configuration of the Trend Micro OfficeScan Server.

Chapter 4
Firewall Protection and Content Filtering

The ProSafe VPN Firewall 50 provides you with Web content filtering options such as Block Sites and Keyword Blocking. 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. It also provides various firewall activity reports and instant alerts via e-mail.

About Firewall Security

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. You can configure up to 600 rules on the FVS338. 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.

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)**. 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.

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.

➡	**Note:** See "Enabling Source MAC Filtering" on page 4-23 for yet another way to block outbound traffic from selected PCs that would otherwise be allowed by the firewall.

Table 4-1. Outbound Rules Fields

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 “Adding Customized Services” on page 4-17).
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 “Setting a Schedule to Block or Allow Traffic” on page 4-20).
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 3-5.
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.

Table 4-1. Outbound Rules Fields (continued)

Item	Description
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. 6 is the highest priority. See "Specifying Quality of Service (QoS) Priorities" on page 4-19.
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.

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.

Whether or not DHCP is enabled and how the PCs will access the server's LAN address impact the Inbound Rules. For example:

- If your external IP address is assigned dynamically by your ISP (DHCP enabled), the IP address may change periodically as the DHCP lease expires. Consider using **Dyamic DNS** (under Network Configuration) so that external users can always find your network (see "Configuring Dynamic DNS (If Needed)" on page 2-16.
- 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 Groups** menu (under Network Configuration) to keep the PC's IP address constant (see "Setting Up Address Reservation" on page 3-8).
- Local PCs must access the local server using the local LAN address of the PC. Attempts by local PCs to access the server using the external WAN IP address will fail.

Note: See "Setting Up Port Triggering" on page 4-24 for yet another way to allow certain types of inbound traffic that would otherwise be blocked by the firewall.

Table 4-2. Inbound Rules Fields

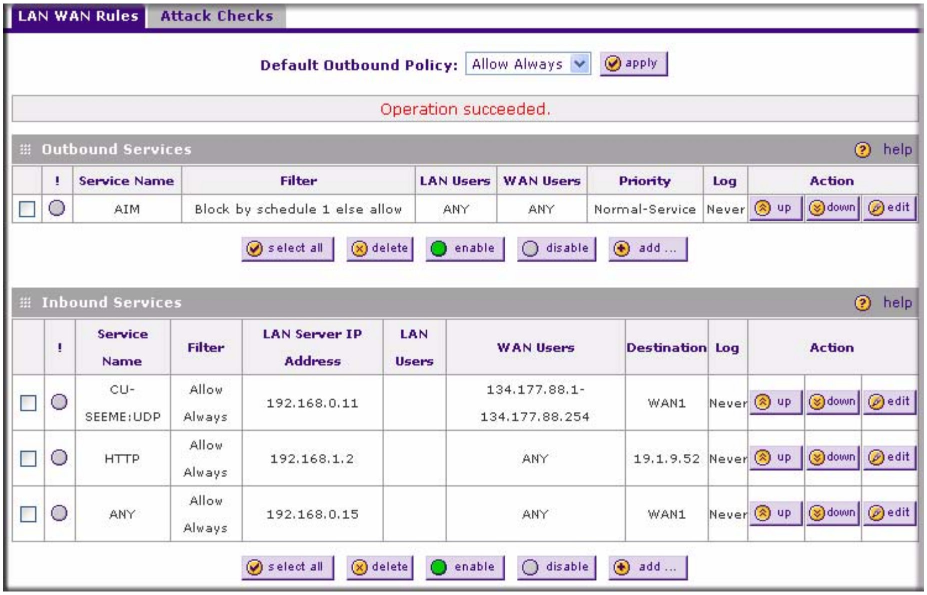
Item	**Description**
Services	Select the desired Service or application to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see "Adding Customized Services" on page 4-17).
Action	Select the desired action for packets 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 Server	This LAN address determines which computer on your network is hosting this service rule. (You can also translate this address to a port number.).
Translate to Port Number	Check the "Translate to Port Number" and enter a port number if you want to assign the LAN Server to a specific port.
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.
WAN Destination IP Address	These settings determine the destination IP address applicable to incoming traffic. This is the public IP address that will map to the internal server; it can either be the address of the WAN1 or WAN2 ports or another public IP address**.**
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. See "Specifying Quality of Service (QoS) Priorities" on page 4-19.
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 VPN firewall. Only enable those ports that are necessary for your network. It is also advisable to turn on the server application security and invoke the user password or privilege levels, if provided.

Order of Precedence for Firewall Rules

As you define new rules, they are added to the tables in the Rules menu, as shown in Figure 4-1



Default Outbound Policy: Allow Always apply

Operation succeeded.

Outbound Services help

	!	Service Name	Filter	LAN Users	WAN Users	Priority	Log	Action
□	○	AIM	Block by schedule 1 else allow	ANY	ANY	Normal-Service	Never	up down edit

Inbound Services help

	!	Service Name	Filter	LAN Server IP Address	LAN Users	WAN Users	Destination	Log	Action
□	○	CU-SEEME:UDP	Allow Always	192.168.0.11		134.177.88.1-134.177.88.254	WAN1	Never	up down edit
□	○	HTTP	Allow Always	192.168.1.2		ANY	19.1.9.52	Never	up down edit
□	○	ANY	Allow Always	192.168.0.15		ANY	WAN1	Never	up down edit

Figure 4-1

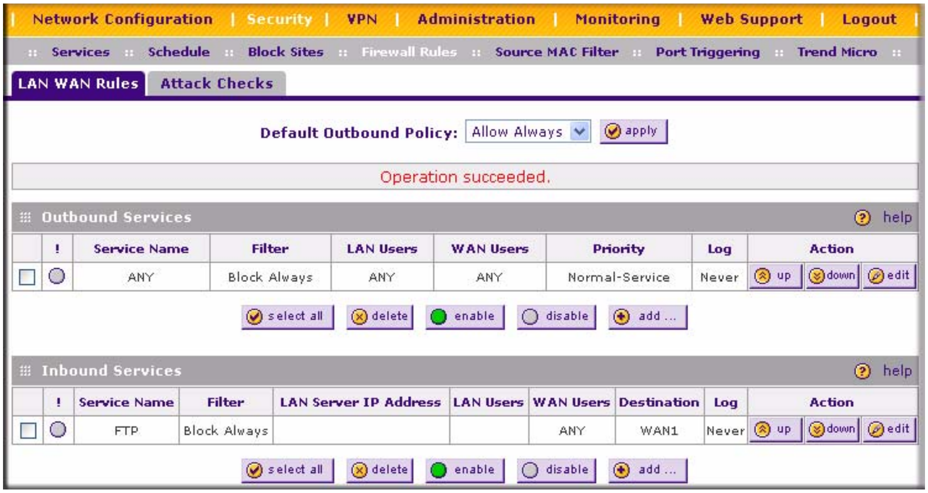
For any traffic attempting to pass through the firewall, the packet information is subjected to the rules in the order shown in the Rules Table, beginning at the top and proceeding to the default rules at the bottom. In some cases, the order of precedence of two or more rules may be important in determining the disposition of a packet. For example, you should place the most strict rules at the top (those with the most specific services or addresses). The **Up** and **Down** buttons allow you to relocate a defined rule to a new position in the table.

Setting LAN WAN Rules

The Default Outbound Policy is to allow all traffic from and to the Internet to pass through. Firewall rules can then be applied to block specific types of traffic from either going out from the LAN to the Internet (Outbound) or coming in from the Internet to the LAN (Inbound). The default policy can be changed to block all outbound traffic and enable only specific services to pass through the router.

To change the Default Outbound Policy:

1. Select **Security** from the main menu and **Firewall Rules** from the submenu. The **LAN WAN Rules** screen will display.
2. Change the **Default Outbound Policy** by selecting Block Always from the drop-down menu and click **Apply**.


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Block Sites :: Firewall Rules :: Source MAC Filter :: Port Triggering :: Trend Micro
LAN WAN Rules
Attack Checks
apply
help
select all
delete
enable
disable
add ...

Default Outbound Policy: Allow Always

Operation succeeded.

Outbound Services

	!	Service Name	Filter	LAN Users	WAN Users	Priority	Log	Action
□	○	ANY	Block Always	ANY	ANY	Normal-Service	Never	up down edit

Inbound Services

	!	Service Name	Filter	LAN Server IP Address	LAN Users	WAN Users	Destination	Log	Action
□	○	FTP	Block Always			ANY	WAN1	Never	up down edit

Figure 4-2

To make changes to an existing outbound or inbound service rule:

1. In the **Action** column adjacent to the rule click:
   - **Edit** – to make any changes to the rule definition of an existing rule. The Outbound Service screen will display containing the data for the selected rule (see Figure 4-3 on page 4-9).
   - **Up** – to move the rule up one position in the table rank.

- **Down** – to move the rule down one position in the table rank.

2. Check the radio box adjacent to the rule and click:
   - Click **Disable** to disable the rule. The “!” Status icon will change from green to grey, indicating that the rule is disabled. (By default, when a rule is added to the table it is automatically enabled.)
   - Click **Delete** to delete the rule.
3. Click **Select All** to select all rules. A check will appear in the radio box for each rule.

LAN WAN Outbound Services Rules

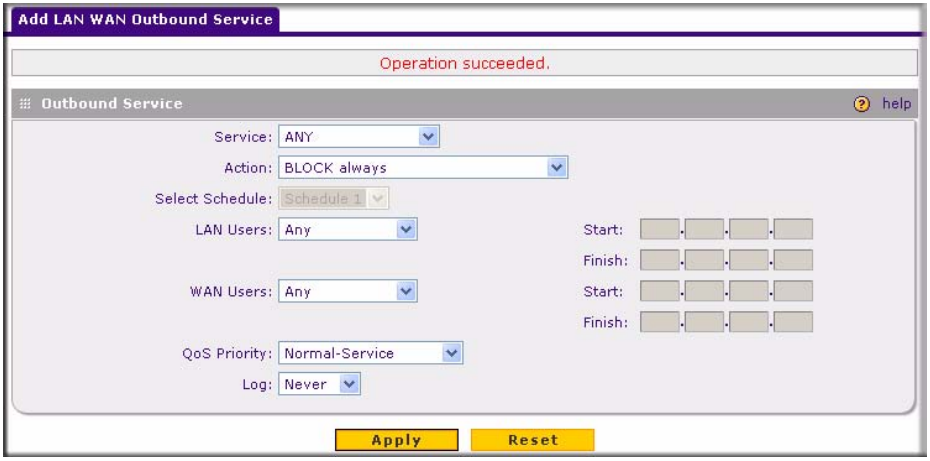
You may define additional rules that will specify exceptions to the default rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day.

You can also tailor these rules to your specific needs (see “Administrator Information” on page 4-31).

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

To create a new outbound service rule:

1. Click **Add** under the Outbound Services Table. The **Add LAN WAN Outbound Service** screen will display.
2. Complete the Outbound Service screen, and save the data (see Table 4-1 on page 4-3).
3. Click **Reset** to cancel your settings and return to the previous settings.
4. Click **Apply** to save your changes and reset the fields on this screen. The new rule will be listed on the **Outbound Services** table.



Add LAN WAN Outbound Service

Operation succeeded.

Outbound Service

Service:	ANY		
Action:	BLOCK always		
Select Schedule:	Schedule 1		
LAN Users:	Any	Start:	. . .
		Finish:	. . .
WAN Users:	Any	Start:	. . .
		Finish:	. . .
QoS Priority:	Normal-Service		
Log:	Never		

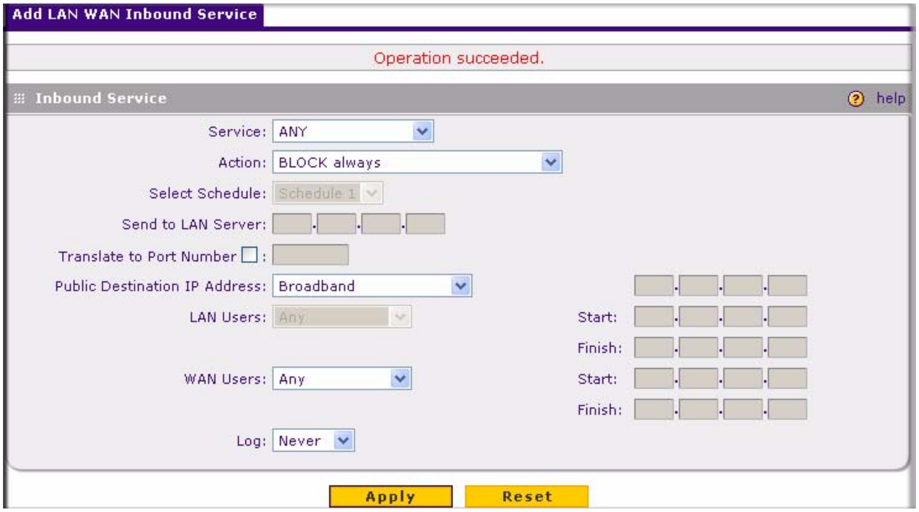
Figure 4-3

LAN WAN Inbound Services Rules

This Inbound Services Rules table lists all existing rules for inbound traffic. If you have not defined any rules, no rules will be listed. By default, all inbound traffic is blocked. **WAN Users**: Whether all WAN addresses or specific IP addresses are included in the rule.

To create a new inbound service rule:

1. Click **Add** under the Inbound Services Table. The **Add LAN WAN Inbound Service** screen will display.
2. Complete the Add WAN LAN Inbound Services screen (see Table 4-2 on page 4-5).
3. Click **Reset** to cancel your settings and return to the previous settings.
4. Click **Apply** to save your changes and reset the fields on this screen. The new rule will be listed on the **Inbound Services** table.
5. Click **Apply** to save your settings. The new rule will be added to the **Inbound Services table.**



Add LAN WAN Inbound Service

Operation succeeded.

Inbound Service

Service: ANY

Action: BLOCK always

Select Schedule: Schedule 1

Send to LAN Server: . . .

Translate to Port Number □ :

Public Destination IP Address: Broadband

LAN Users: Any Start: Finish:

WAN Users: Any Start: Finish:

Log: Never

Figure 4-4

Attack Checks

This screen allows you to specify whether or not the router should be protected against common attacks in the LAN and WAN networks. The various types of attack checks are listed on the **Attack Checks** screen and defined below:

- **WAN Security Checks**
  - **Respond To Ping On Internet Ports**. When enabled, the router will respond to a “Ping” from the Internet. This can be used as a diagnostic tool and shouldn’t be used unless you have a specific diagnostic reason to do so.
  - **Enable Stealth Mode**. If enabled, the router will not respond to port scans from the WAN, thus making it less susceptible to discovery and attacks.
  - **Block TCP Flood.** A SYN flood is a form of denial of service attack in which an attacker sends a succession of SYN requests to a target system. When the system responds, the attacker doesn’t complete the connections, thus leaving the connection half-open and flooding the server with SYN messages. No legitimate connections can then be made.

    When enabled, the router will drop all invalid TCP packets and will be protected from a SYN flood attack.

- **LAN Security Checks.** A UDP flood is a form of denial of service attack that can be initiated when one machine sends a large number of UDP packets to random ports on a remote host. As a result, the distant host will (1) check for the application listening at that port, (2) verify that no application is listening at that port, and then (3) reply with an ICMP Destination Unreachable packet.

  When the victimized system is flooded, it is forced to send many ICMP packets, eventually making it unreachable by other clients. The attacker may also spoof the IP address of the UDP packets, ensuring that the excessive ICMP return packets do not reach him, thus making the attacker's network location anonymous.

  If enabled, the router will not accept more than 20 simultaneous, active UDP connections from a single computer on the LAN.

- **VPN Pass through**. When the router is in NAT mode, all packets going to the Remote VPN Gateway are first filtered through NAT and then encrypted per the VPN policy.

  For example, if a VPN Client or Gateway on the LAN side of this router wants to connect to another VPN endpoint on the WAN (placing this router between two VPN end points), encrypted packets will be sent to this router. Since this router filters the encrypted packets through NAT, the packets will become invalid unless VPN Pass through is enabled.

  When enabled, the VPN tunnel will pass the VPN traffic without any filtering. Tunnels can be

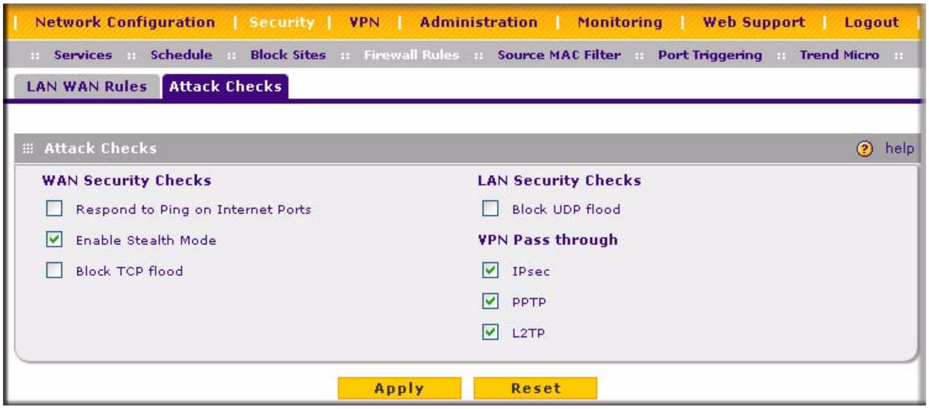
  – IPSec

  – PPTP

  – L2TP

To select the appropriate checkbox for your requirement:

1. Select **Security** from the main menu, **Firewall Rules** from the submenu and then the **Attack Checks** tab. The **Attack Checks** screen will display.
2. Check the radio boxes of the Attack Checks you wish to initiate.
3. Click **Apply** to save your settings


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Block Sites :: Firewall Rules :: Source MAC Filter :: Port Triggering :: Trend Micro
LAN WAN Rules
Attack Checks
help
Apply
Reset

Attack Checks

WAN Security Checks

- □ Respond to Ping on Internet Ports
- ☑ Enable Stealth Mode
- □ Block TCP flood

LAN Security Checks

- □ Block UDP flood

VPN Pass through

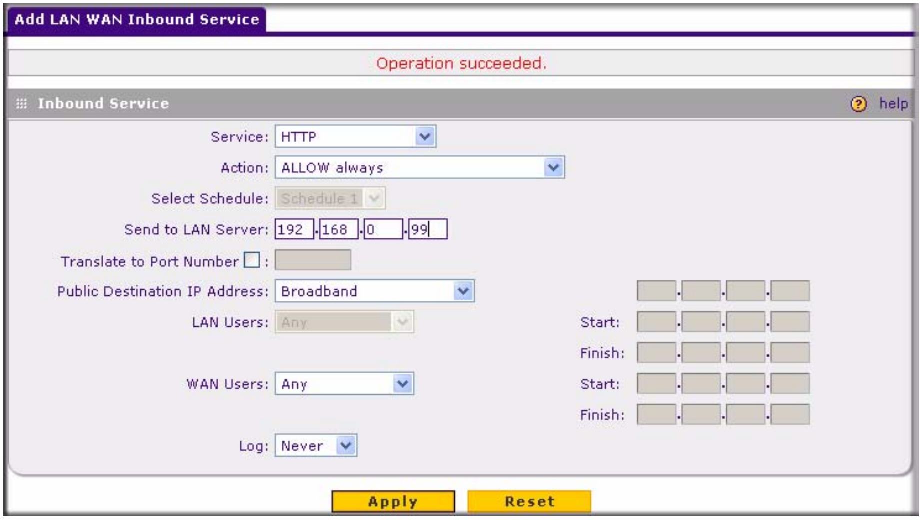
- ☑ IPsec
- ☑ PPTP
- ☑ L2TP

Figure 4-5

Inbound Rules Examples

Hosting 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 4-6:



Operation succeeded.

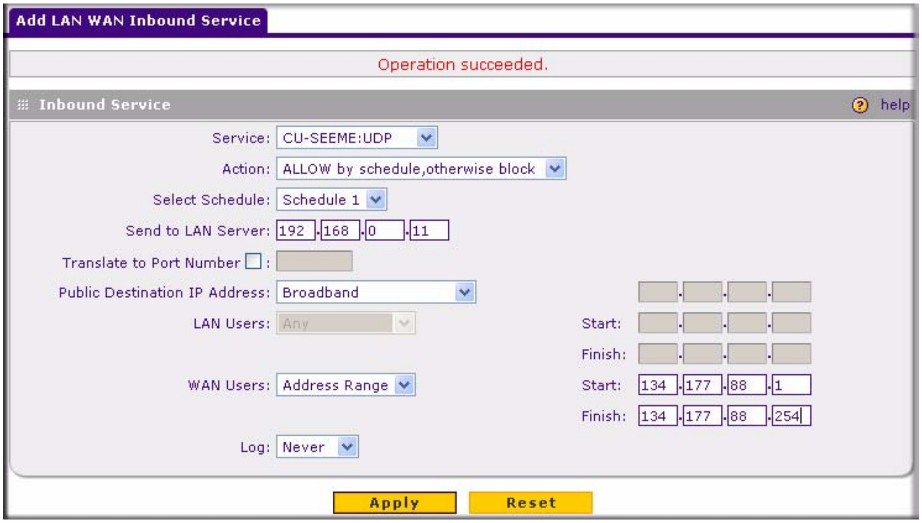
Inbound Service

Service: HTTP
Action: ALLOW always
Select Schedule: Schedule 1
Send to LAN Server: 192.168.0.99
Translate to Port Number □:
Public Destination IP Address: Broadband
LAN Users: Any
Start:
Finish:
WAN Users: Any
Start:
Finish:
Log: Never

Figure 4-6

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 to the right, CU-SeeMe connections are allowed only from a specified range of external IP addresses.



Add LAN WAN Inbound Service

Operation succeeded.

Inbound Service

Service: CU-SEEME:UDP

Action: ALLOW by schedule,otherwise block

Select Schedule: Schedule 1

Send to LAN Server: 192 . 168 . 0 . 11

Translate to Port Number □ :

Public Destination IP Address: Broadband

LAN Users: Any

WAN Users: Address Range

Start: 134 . 177 . 88 . 1

Finish: 134 . 177 . 88 . 254

Log: Never

Figure 4-7

Setting Up One-to-One NAT Mapping

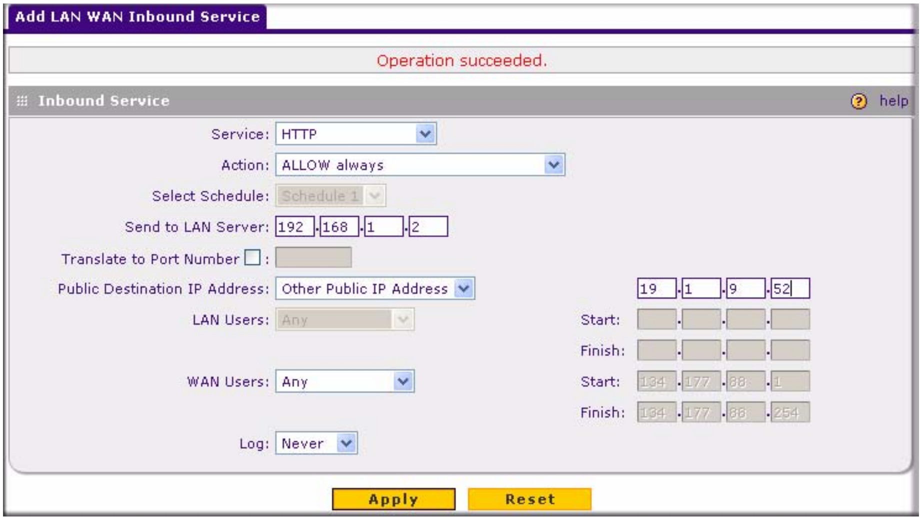
In this example, we will configure multi-NAT to support multiple public IP addresses on one WAN interface. By creating an inbound rule, we will configure the firewall to host an additional public IP address and associate this address with a Web server on the LAN.

> **Tip:** If your ISP allows you to have more than one public IP address for your use, you can use the additional public IP addresses to map to servers on your LAN. One of these public IP addresses will be used as the primary IP address of the router. This address will be used to provide Internet access to your LAN PCs through NAT. The other addresses are available to map to your servers.

To configure the FVS338 for additional IP addresses:

1. Select **Security** from the main menu and **Firewall Rules** from the submenu.
2. Click **Add** under the **Inbound Services** table. The **Add LAN WAN Inbound Service** screen will display.

3. From the service pull-down menu, select the HTTP service for a Web server.
4. From the Action pull-down menu, select Allow Always.
5. In the Send to LAN Server field, enter the local IP address of your Web server PC.
6. From the Public Destination IP Address pull down menu, choose Other Public IP Address.
7. Enter one of your public Internet addresses that will be used by clients on the Internet to reach your Web server.
8. Click **Apply.** The rule will display in the Inbound Services table shown in Figure 4-9.



Add LAN WAN Inbound Service

Operation succeeded.

Inbound Service

Service: HTTP

Action: ALLOW always

Select Schedule: Schedule 1

Send to LAN Server: 192 . 168 . 1 . 2

Translate to Port Number □ :

Public Destination IP Address: Other Public IP Address   19 . 1 . 9 . 52

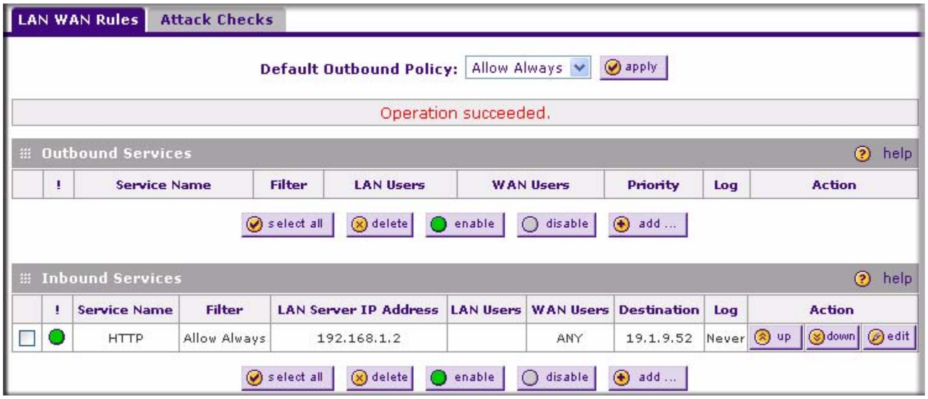
LAN Users: Any   Start: . . .   Finish: . . .

WAN Users: Any   Start: 134 . 177 . 88 . 1   Finish: 134 . 177 . 88 . 254

Log: Never

Figure 4-8

Your rule will now appear in the Inbound Services table of the Rules menu (see Figure 4-9). This rule is different from a normal inbound port forwarding rule in that the Destination box contains an IP Address other than your normal WAN IP Address.



Default Outbound Policy: Allow Always apply

Operation succeeded.

Outbound Services

	!	Service Name	Filter	LAN Users	WAN Users	Priority	Log	Action

Inbound Services

	!	Service Name	Filter	LAN Server IP Address	LAN Users	WAN Users	Destination	Log	Action
□	●	HTTP	Allow Always	192.168.1.2		ANY	19.1.9.52	Never	up down edit

Figure 4-9

To test the connection from a PC on the Internet, type **http://<*IP_address*>**, where **<*IP_address*>** is the public IP address you have mapped to your Web server. You should see the home page of your Web server.

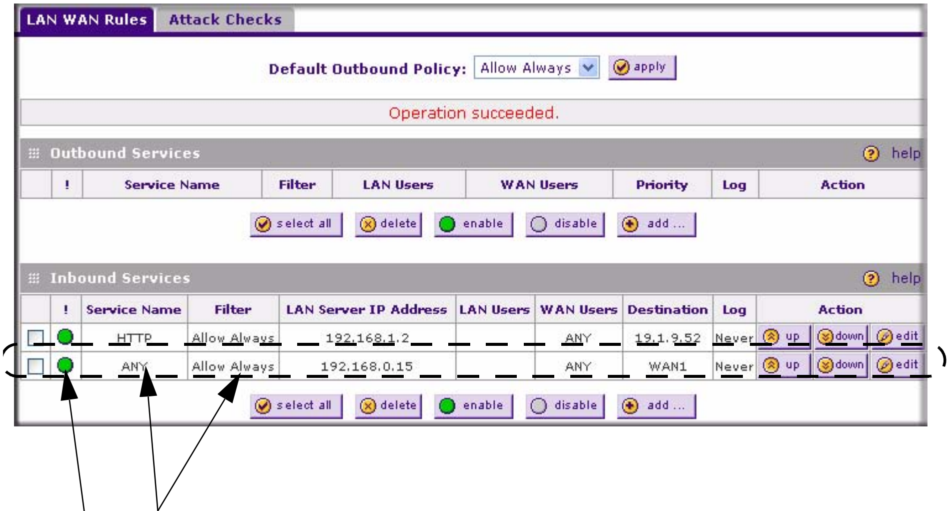
Specifying an Exposed Host

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 have not yet defined.

To expose one of the PCs on your LAN as this host:

1. Create an inbound rule that allows all protocols.
2. Place the rule below all other inbound rules.

> **Note:** For security, NETGEAR strongly recommends that you avoid creating an exposed host. 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.



Default Outbound Policy: Allow Always

Operation succeeded.

Outbound Services

	!	Service Name	Filter	LAN Users	WAN Users	Priority	Log	Action

Inbound Services

	!	Service Name	Filter	LAN Server IP Address	LAN Users	WAN Users	Destination	Log	Action
□	●	HTTP	Allow Always	192.168.1.2		ANY	19.1.9.52	Never	up down edit
□	●	ANY	Allow Always	192.168.0.15		ANY	WAN1	Never	up down edit

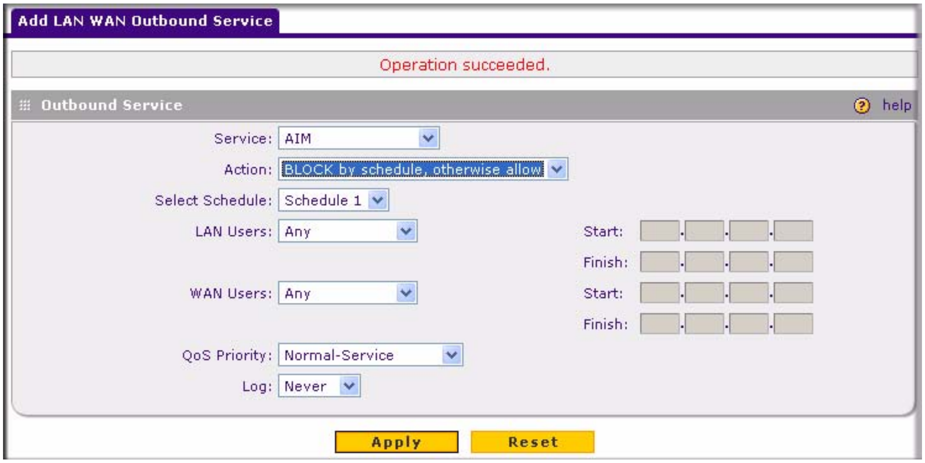
1. Select All protocols and ALLOW Always (or Allow by Schedule)
2. Place rule below all other inbound rules

Figure 4-10

Outbound Rules Example – Blocking Instant Messenger

Outbound rules let you prevent users from using applications such as AOL Instant Messenger, Real Audio or other non-essential sites.

If you want to block AOL 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.


Add LAN WAN Outbound Service

Operation succeeded.

Outbound Service

Service: AIM

Action: BLOCK by schedule, otherwise allow

Select Schedule: Schedule 1

LAN Users: Any

Start:

Finish:

WAN Users: Any

Start:

Finish:

QoS Priority: Normal-Service

Log: Never

Figure 4-11

Adding Customized Services

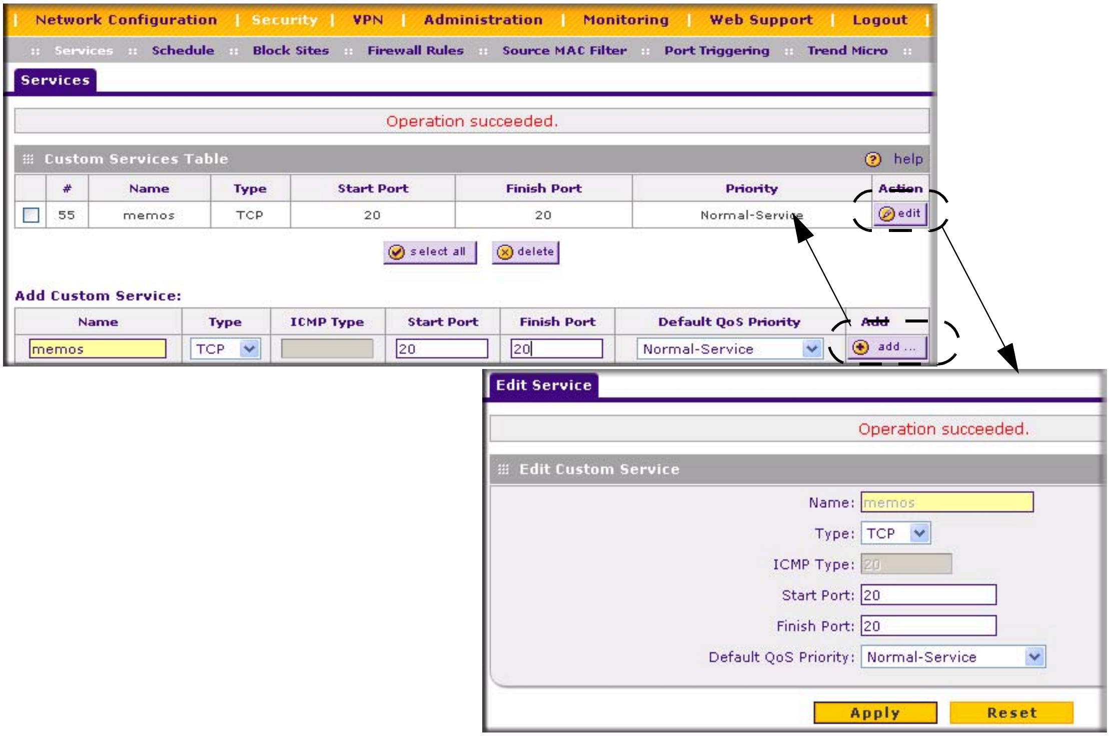
Services are functions performed by server computers at the request of client computers. You can configure up to 125 custom services.

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 Internet Protocol 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 4-12.

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, you can enter it on the Services screen.


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Block Sites :: Firewall Rules :: Source MAC Filter :: Port Triggering :: Trend Micro ::
Services
help
select all
delete
Edit Service
Apply
Reset

Operation succeeded.

Custom Services Table

	#	Name	Type	Start Port	Finish Port	Priority	Action
□	55	memos	TCP	20	20	Normal-Service	edit

Add Custom Service:

Name	Type	ICMP Type	Start Port	Finish Port	Default QoS Priority	Add
memos	TCP		20	20	Normal-Service	add ...

Operation succeeded.

Edit Custom Service

Name: memos
Type: TCP
ICMP Type: 20
Start Port: 20
Finish Port: 20
Default QoS Priority: Normal-Service

Figure 4-12

To add a service:

1. Select **Security** from the main menu and **Services** from the submenu. The **Services** screen will display.
2. In the **Add Custom Service** table, enter a descriptive name for the service (this is for your convenience).
3. Select the Layer 3 Protocol that the service uses as its transport protocol. It can be TCP, UDP or ICMP.
4. Enter the first TCP or UDP port of the range that the service uses. If the service uses only one port, then the Start Port and the Finish Port will be the same.
5. Enter the last port of the range that the service uses. If the service only uses a single port number, enter the same number in both fields.
6. Click **Add**. The new custom service will be added to the Custom Services Table.

To edit the parameters of a service:

1. In the Custom Services Table, click the **Edit** icon adjacent to the service you want to edit. The **Edit Service** screen will display.
2. Modify the parameters you wish to change.
3. Click **Reset** to cancel the changes and restore the previous settings.
4. Click **Apply** to confirm your changes. The modified service will display in the Custom Services Table.

Specifying Quality of Service (QoS) Priorities

The Quality of Service (QoS) Priorities 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:

- On the **Services** screen in the Customer Services Table for customized services (see Figure 4-12).
- On the **LAN WAN Outbound Services** screen (see Figure 4-11).

The QoS priority definition for a service determines the queue that is used for the traffic passing through the VPN firewall. A priority is assigned to IP packets using this service. Priorities are defined by the “Type of Service (ToS) in the Internet Protocol Suite” standards, RFC 1349. A ToS priority for traffic passing through the VPN firewall is one of the following:

- **Normal-Service:** No special priority given to the traffic. The IP packets for services with this priority are marked with a ToS value of 0.
- **Minimize-Cost:** Used when data has to be transferred over a link that has a lower “cost”. The IP packets for services with this priority are marked with a ToS value of 1.
- **Maximize-Reliability:** Used when data needs to travel to the destination over a reliable link and with little or no retransmission. The IP packets for services with this priority are marked with a ToS value of 2.
- **Maximize-Throughput**: Used when the volume of data transferred during an interval is important even if the latency over the link is high. The IP packets for services with this priority are marked with a ToS value of 4.
- **Minimize-Delay:** Used when the time required (latency) for the packet to reach the destination must be low. The IP packets for services with this priority are marked with a ToS value of 8.

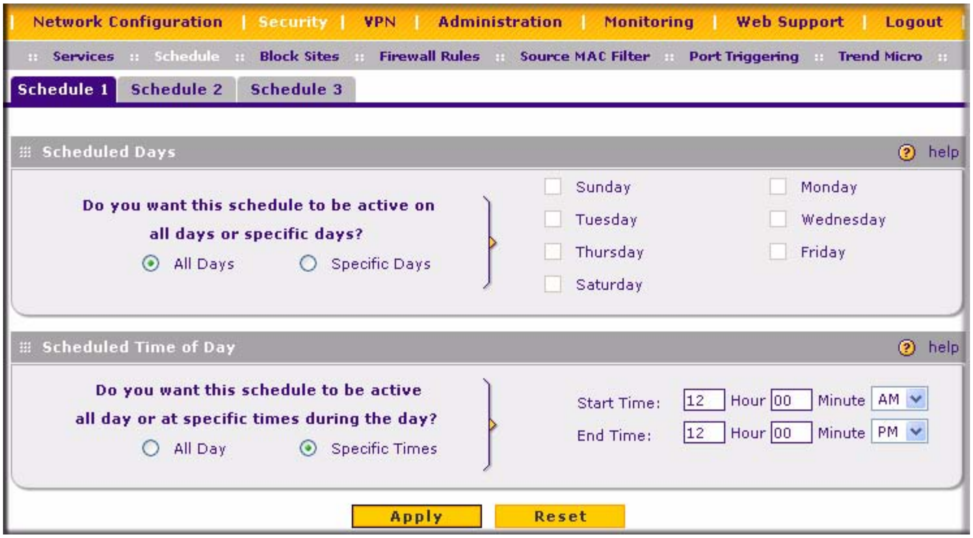
Setting a Schedule to Block or Allow Traffic

If you defined an outbound or inbound 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 one of the Schedules—Schedule 1, Schedule 2 or Schedule 3.

To invoke rules and block keywords or Internet domains based on a schedule:

1. Select **Security** from the main menu and **Schedule** from the sub-menu. The **Schedule 1** screen will display.
2. Check the radio button for All Days or Specific Days. If you chose Specific Days, check the radio button for each day you want the schedule to be in effect.
3. Check the radio button to schedule the time of day: All Day, or Specific Times. If you chose Specific Times, enter the Start Time and End Time fields (Hour, Minute, AM/PM), which will limit access during certain times for the selected days.
4. Click **Reset** to cancel your settings and revert to the previous settings.
5. Click **Apply** to save your settings to **Schedule 1.**

Repeat these 5 steps to set to a schedule for **Schedule 2** and **Schedule 3.**



Scheduled Days

Do you want this schedule to be active on all days or specific days?

● All Days ○ Specific Days

□ Sunday □ Monday
□ Tuesday □ Wednesday
□ Thursday □ Friday
□ Saturday

Scheduled Time of Day

Do you want this schedule to be active all day or at specific times during the day?

○ All Day ● Specific Times

Start Time: 12 Hour 00 Minute AM
End Time: 12 Hour 00 Minute PM

Figure 4-13

Setting Block Sites (Content Filtering)

If you want restrict internal LAN users from access to certain sites on the Internet, you can use the VPN firewall's Content Filtering and Web Components filtering. By default, these features are disabled; all requested traffic from any Web site is allowed. If you enable one or more of these features and users try to access a blocked site, they will see a "Blocked by NETGEAR" message.

Several types of blocking are available:

- **Web Components** blocking. You can block the following Web component types: Proxy, Java, ActiveX, and Cookies. Even sites on the Trusted Domains list will be subject to Web Components blocking when the blocking of a particular Web component is enabled.
- **Keyword** (and domain name) blocking. You can specify up to 32 words that, should they appear in the Web site name (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 or keywords on this list by PCs, even those in the groups for which keyword blocking has been enabled, will still be allowed without any blocking.

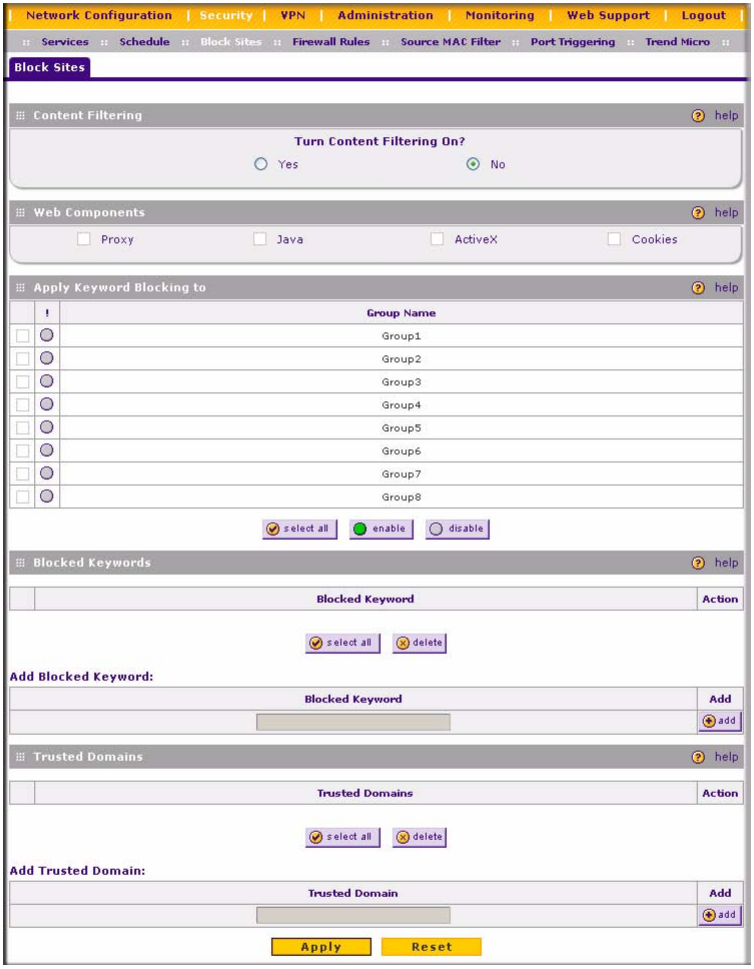
Keyword Blocking application examples:

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

To enable Content Filtering:

1. Select **Security** from the main menu and **Block Sites** from the sub-menu. The **Block Sites** screen will display.
2. Check the **Yes** radio button to enable Content Filtering.
3. Check the radio boxes of any Web Components you wish to block.
4. Check the radio buttons of the groups to which you wish to apply Keyword Blocking. Click **Enable** to activate Keyword blocking (or disable to deactivate Keyword Blocking).

5. Build your list of blocked Keywords or Domain Names in the **Blocked Keyword** fields. After each entry, click **Add.** The Keyword or Domain name will be added to the **Blocked Keywords** table. (You can also edit an entry by clicking **Edit** in the Action column adjacent to the entry.)
6. Build a list of Trusted Domains in the **Trusted Domains** fields. After each entry, click **Add.** The Trusted Domain will appear in the **Trusted Domains** table. (You can also edit any entry by clicking **Edit** in the Action column adjacent to the entry.)
7. Click **Reset** to cancel your changes and revert to the previous settings.
8. Click **Apply** to save your settings.



Content Filtering

Turn Content Filtering On?

○ Yes ● No

Web Components

□ Proxy □ Java □ ActiveX □ Cookies

Apply Keyword Blocking to

	!	Group Name
□	○	Group1
□	○	Group2
□	○	Group3
□	○	Group4
□	○	Group5
□	○	Group6
□	○	Group7
□	○	Group8

Blocked Keywords

	Blocked Keyword	Action

Add Blocked Keyword:

Blocked Keyword	Add
	add

Trusted Domains

	Trusted Domains	Action

Add Trusted Domain:

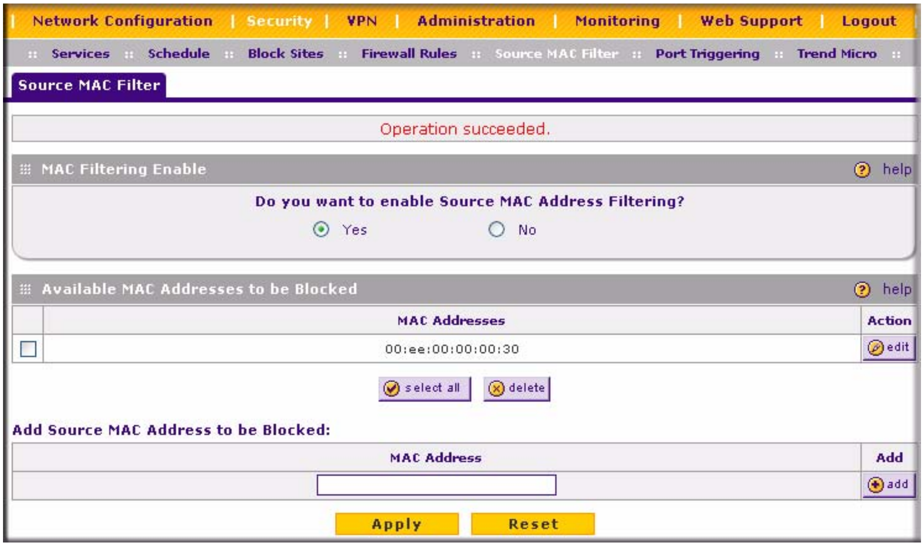
Trusted Domain	Add
	add

Figure 4-14

Enabling Source MAC Filtering

Source MAC Filter allows you to filter out traffic coming from certain known machines or devices.

- 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, traffic will be dropped coming from any computers or devices whose MAC addresses are listed in **Available MAC Addresses to be Blocked** table.


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
:: Services :: Schedule :: Block Sites :: Firewall Rules :: Source MAC Filter :: Port Triggering :: Trend Micro ::
Source MAC Filter

Operation succeeded.

MAC Filtering Enable

Do you want to enable Source MAC Address Filtering?

● Yes ○ No

Available MAC Addresses to be Blocked

	MAC Addresses	Action
□	00:ee:00:00:00:30	edit

Add Source MAC Address to be Blocked:

MAC Address	Add
	add

Figure 4-15

Note: For additional ways of restricting outbound traffic, see "LAN WAN Outbound Services Rules" on page 4-8.

To enable MAC filtering and add MAC addresses to be blocked:

1. Select **Security** from the main menu and **Source MAC Filter** from the sub-menu. The **Source MAC Filter** screen will display.
2. Check the Yes radio box in the **MAC Filtering Enable** section.

3. Build your list of Source MAC Addresses to be block by entering the first MAC address in the **MAC Address** field in the form xx:xx:xx:xx:xx:xx where x is a numeric (0 to 9) or an alphabet between and a and f (inclusive), for example: 00:e0:4c:69:0a:

4. Click **Add.** The Mac Address will be added to the **Available MAC Addresses to be Blocked** table. (You can edit the MAC address by clicking **Edit** in the Action column adjacent to the MAC Address.)

5. Click **Reset** to cancel a MAC address entry before adding it to the table.

6. When you have completed adding MAC addresses, click **Apply** to save your settings

Setting Up Port Triggering

Port triggering allows some applications running on a LAN network to be available to external applications 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, Port Triggering operates as follows:

1. A PC makes an outgoing connection using a port number defined in the Port Triggering table.
2. The VPN firewall records this connection, opens the an INCOMING port or ports associated with this entry in the Port Triggering table, and associates them with the PC.
3. The remote system receives the PCs request and responds using the different port numbers that you have now opened.
4. The VPN firewall 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 this Router cannot be sure when the application has terminated.

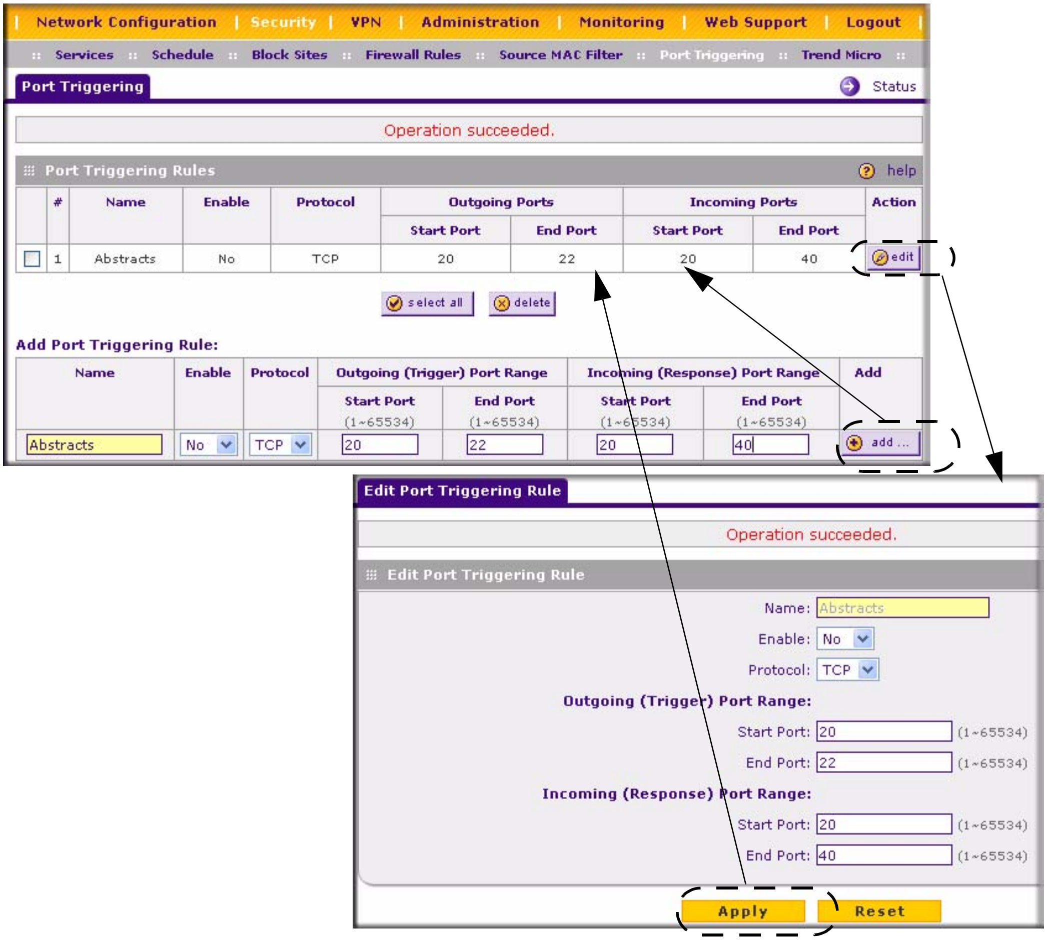
➡ **Note:** For additional ways of allowing inbound traffic, see "LAN WAN Inbound Services Rules" on page 4-9.

To add a Port triggering rule:

1. Select **Security** from the main menu and **Port Triggering** from the submenu. The **Port Triggering** screen will display.

1. Enter a user-defined name for this rule in the **Name** field.

2. From the **Enable** pull-down menu, indicate if the rule is enabled or disabled.



Operation succeeded.

Port Triggering Rules

	#	Name	Enable	Protocol	Outgoing Ports		Incoming Ports		Action
					Start Port	End Port	Start Port	End Port	
□	1	Abstracts	No	TCP	20	22	20	40	edit

Add Port Triggering Rule:

Name	Enable	Protocol	Outgoing (Trigger) Port Range		Incoming (Response) Port Range		Add
			Start Port (1~65534)	End Port (1~65534)	Start Port (1~65534)	End Port (1~65534)	
Abstracts	No	TCP	20	22	20	40	add ...

Edit Port Triggering Rule

Operation succeeded.

Edit Port Triggering Rule

Name: Abstracts

Enable: No

Protocol: TCP

Outgoing (Trigger) Port Range:

Start Port: 20 (1~65534)

End Port: 22 (1~65534)

Incoming (Response) Port Range:

Start Port: 20 (1~65534)

End Port: 40 (1~65534)

Figure 4-16

3. From the **Protocol** pull-down menu, select either TCP or UDP protocol.

4. In the **Outgoing (Trigger) Port Range** fields;

   a. Enter the **Start Port** range (1 - 65534).

   b. Enter the **End Port** range (1 - 65534).

5. In the **Incoming (Response) Port Range** fields:

   a. Enter the **Start Port** range (1 - 65534).

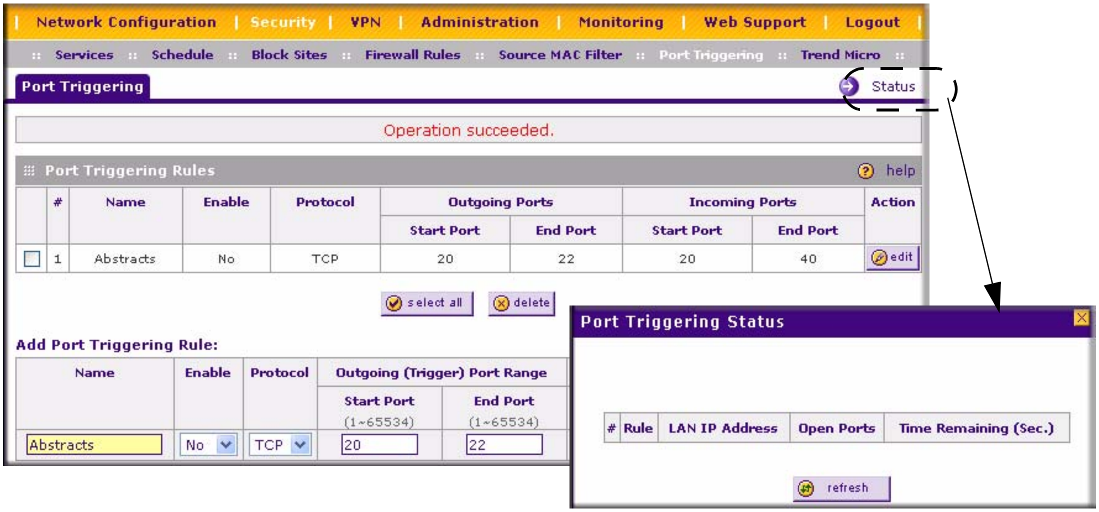
   b. Enter the **End Port** range (1 - 65534).

6. Click **Add.** The Port Triggering Rule will be added to the **Port Triggering Rules** table.

To edit or modify a rule:

1. Click **Edit** in the Action column opposite the rule you wish to edit. The **Edit Port Triggering Rule** screen will display.
2. Modify any of the fields for this rule.
3. Click **Reset** to cancel any changes and return to the previous settings.
4. Click **Apply** to save your modifications. Your changes will appear in the **Port Triggering Rules** table.

To check the status of the Port Triggering rules, click the **Status** link on the **Port Triggering** screen..


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
Services :: Schedule :: Block Sites :: Firewall Rules :: Source MAC Filter :: Port Triggering :: Trend Micro
Port Triggering
Status
help
select all
delete
refresh

Operation succeeded.

Port Triggering Rules

	#	Name	Enable	Protocol	Outgoing Ports		Incoming Ports		Action
					Start Port	End Port	Start Port	End Port	
□	1	Abstracts	No	TCP	20	22	20	40	edit

Add Port Triggering Rule:

Name	Enable	Protocol	Outgoing (Trigger) Port Range	
			Start Port (1~65534)	End Port (1~65534)
Abstracts	No	TCP	20	22

Port Triggering Status

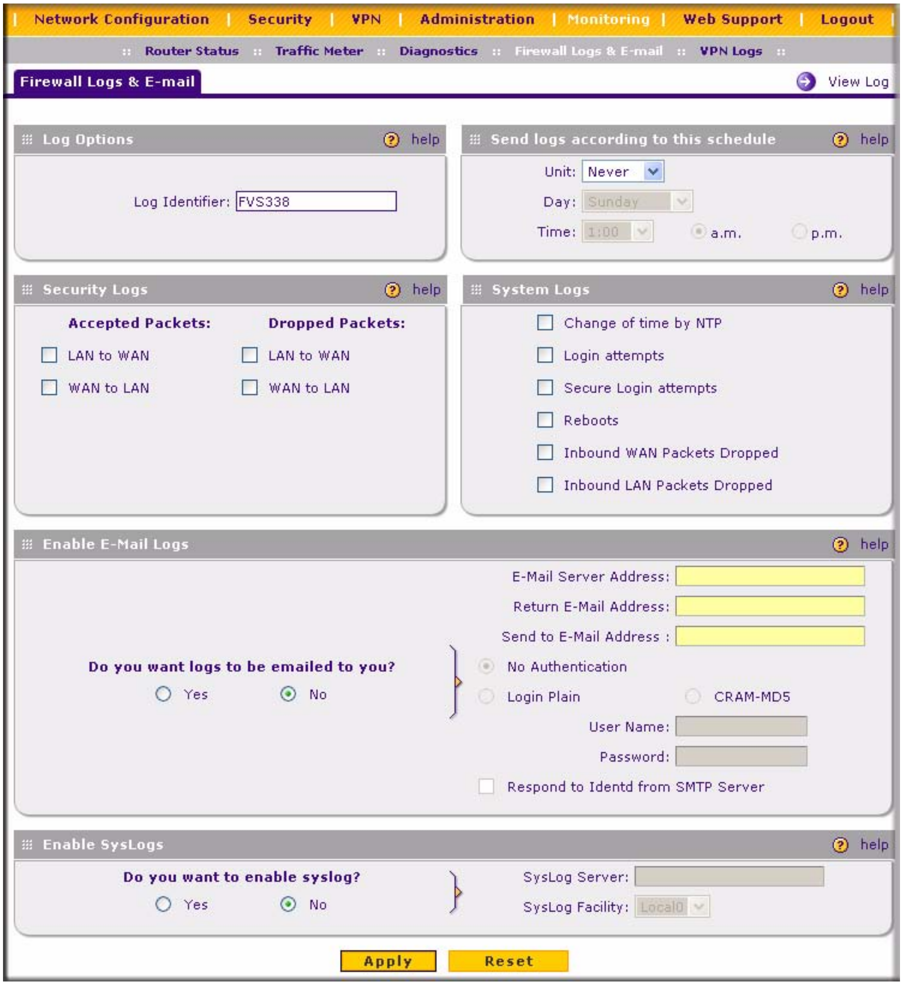
#	Rule	LAN IP Address	Open Ports	Time Remaining (Sec.)

Figure 4-17

E-Mail Notifications of Event Logs and Alerts

The Firewall Logs can be configured to log and then e-mail denial of access, general attack information, and other information to a specified email address. For example, your VPN firewall will log security-related events such as: accepted and dropped packets on different segments of your LAN; denied incoming and outgoing service requests; hacker probes and Login attempts; and other general information based on the settings you input on the **Firewall Logs & E-mail** screen. In addition, if you have set up Content Filtering on the Block Sites screen (see "Setting Block Sites (Content Filtering)" on page 4-21), a log will be generated when someone on your network tries to access a blocked site.

You must have e-mail notification enabled to receive the logs in an e-mail message. If you don't have e-mail notification enabled, you can view the logs on the **Logs** screen (see Figure 4-18 on page 4-28). Selecting all events will increase the size of the log, so it is good practice to select only those events which are required.


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
Router Status :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs
Firewall Logs & E-mail
View Log
help
Apply
Reset

Log Options

Log Identifier: FVS338

Send logs according to this schedule

Unit: Never

Day: Sunday

Time: 1:00 ● a.m. ○ p.m.

Security Logs

Accepted Packets:

□ LAN to WAN

□ WAN to LAN

Dropped Packets:

□ LAN to WAN

□ WAN to LAN

System Logs

□ Change of time by NTP

□ Login attempts

□ Secure Login attempts

□ Reboots

□ Inbound WAN Packets Dropped

□ Inbound LAN Packets Dropped

Enable E-Mail Logs

Do you want logs to be emailed to you? ○ Yes ● No

E-Mail Server Address:

Return E-Mail Address:

Send to E-Mail Address :

● No Authentication

○ Login Plain ○ CRAM-MD5

User Name:

Password:

□ Respond to Identd from SMTP Server

Enable SysLogs

Do you want to enable syslog? ○ Yes ● No

SysLog Server:

SysLog Facility: Local0

Figure 4-18

To set up Firewall Logs and E-mail alerts:

1. Select **Monitoring** from the main menu and then **Firewall Logs & E-mail** from the submenu. The **Firewall Logs & E-mail** screen will display.
2. Enter the name of the log in the **Log Identifier** field. Log Identifier is a mandatory field used to identify the log messages. The ID appended to log messages.
3. Enter a **Schedule** for sending the logs. From the **Unit** pull-down menu, select: Never, Hourly, Daily, or Weekly. Then fill in the Day and Time fields that correspond to your selection.

4. In the **Security Logs** section, check the network segments radio box for which you would like logs to be sent (for example, LAN to WAN under Dropped Packets).
5. In the **System Logs** section, check the radio box for the type of system events to be logged.
6. Check the **Yes** radio box to enable E-mail Logs. Then enter:
   a. **E-mail Server address** – Enter the outgoing E-mail SMTP mail server address of your ISP (for example, 172.16.1.10). If you leave this box blank, no logs will be sent to you.

   b. **Return E-mail Address** – Enter the e-mail address of the user.

   c. **Send To E-mail Address** – Enter the e-mail address where the logs and alerts should be sent. You must use the full e-mail address (for example, ChrisXY@myISP.com).
7. The **No Authentication** radio box is checked by default. If your SMTP server authenticates users, uncheck the radio box by selecting the authentication type—either **Login Plain** or **CRAM-MD5**—based on your SMTP server requirements. Then enter the user name and password to be used for authentication.
8. If you want to respond to IDENT protocol, check the **Respond to Identd from SMTP Server** radio box. The Ident Protocol is an Internet protocol that helps identify the user of a particular TCP connection (a common daemon program for providing the ident service is identd).
9. You can configure the firewall to send system logs to an external PC that is running a syslog logging program. Click the **Yes** radio box to enable SysLogs and send messages to the syslog server, then:
   a. Enter your **Syslog Server** IP address

   b. Select the appropriate syslog facility from the **SysLog Facility** pull-down menu. he SysLog Facility levels of severity are described in Table 4-3 below.
10. Click **Reset** to cancel your changes and return to the previous settings.
11. Click **Apply** to save your settings.

Table 4-3. SysLog Facility Message Levels

Numerical Code	Severity
0	Emergency: System is unusable
1	Alert: Action must be taken immediately
2	Critical: Critical conditions
3	Error: Error conditions
4	Warning: Warning conditions

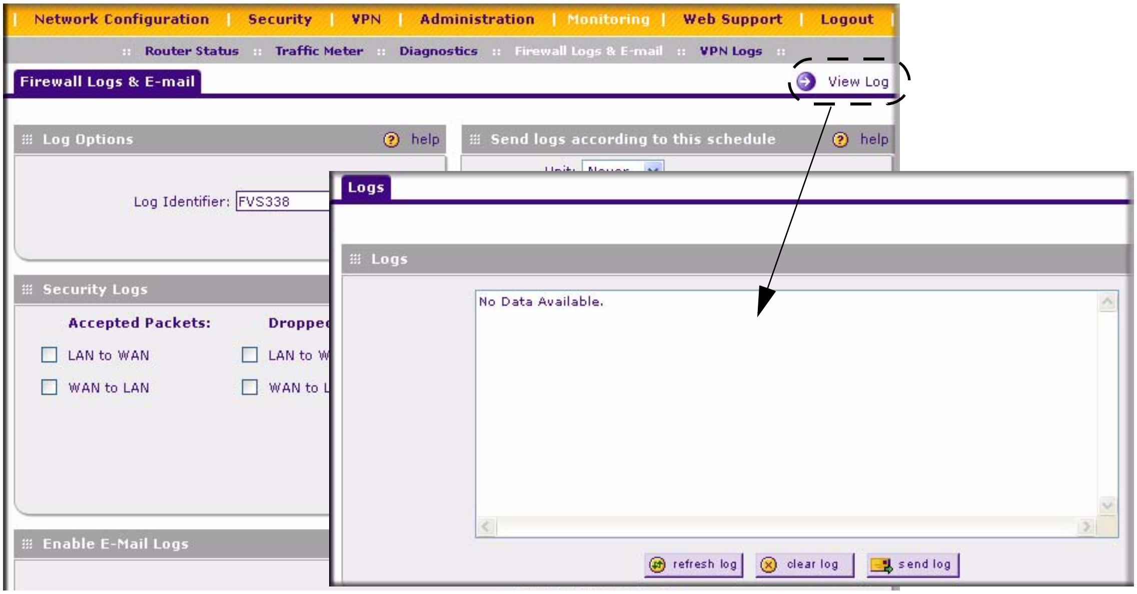
Table 4-3. SysLog Facility Message Levels (continued)

Numerical Code	Severity
5	Notice: Normal but significant conditions
6	Informational: Informational messages
7	Debug: Debug level messages

To view the Firewall logs:

1. Click on the **View Log** icon opposite the **Firewall Logs & E-mail** tab. The **Logs** screen will display.
2. If the E-mail Logs options as been enabled, you can send a copy of the log by clicking **send log.**
3. Click **refresh log** to retrieve the latest update; and click **clear log** to delete all entries.

Log entries are described in Table 4-4.


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Firewall Logs & E-mail
View Log
Log Options
help
Send logs according to this schedule
help
Security Logs
Accepted Packets:
Droppe
LAN to WAN
WAN to LAN
LAN to W
WAN to L
Enable E-Mail Logs
Logs
Logs
refresh log
clear log
send log

Log Identifier: FVS338

No Data Available.

Figure 4-19

Table 4-4. Log Entry Descriptions

Field	Description
Date and Time	The date and time the log entry was recorded.
Description or Action	The type of event and what action was taken if any.
Source IP	The IP address of the initiating device for this log entry.
Source port and interface	The service port number of the initiating device, and whether it originated from the LAN, WAN or DMZ.
Destination	The name or IP address of the destination device or Web site.
Destination port and interface	The service port number of the destination device, and whether it's on the LAN, WAN or DMZ.

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 6-9).
2. Although setting firewall rules (see "Using Rules to Block or Allow Specific Kinds of Traffic" on page 4-1) is the basic way of managing the traffic through your system, you can further refine your control with the following features of the VPN firewall:
   - Groups and hosts (see "Managing Groups and Hosts" on page 3-5)
   - Services (see "Services-Based Rules" on page 4-2)
   - Schedules (see "Setting a Schedule to Block or Allow Traffic" on page 4-20)
   - Block sites (see "Setting Block Sites (Content Filtering)" on page 4-21)
   - Source MAC filtering (see "Enabling Source MAC Filtering" on page 4-23)
   - Port triggering (see "Setting Up Port Triggering" on page 4-24)

Chapter 5
Virtual Private Networking

This chapter describes how to use the Virtual Private Networking (VPN) features of the 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 then edit the VPN and IKE Policy screens for the various VPN scenarios.

Dual WAN Port Systems

The dual WAN ports in the VPN firewall can be configured for rollover mode for increased system reliability by specifying the Broadband connection with the Dialup connection as backup. This WAN mode choice then impacts how the VPN features must be configured.

Table 5-1. IP Addressing Requirements for VPN in Dual WAN Port Systems

Configuration and WAN IP address		Rollover Mode[a]	Dedicated Mode
VPN Road Warrior (client-to-gateway)	Fixed	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required
VPN Gateway-to-Gateway	Fixed	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required
VPN Telecommuter (client-to-gateway through a NAT router)	Fixed	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required

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

The use of fully qualified domain names is mandatory when the WAN ports are in rollover mode ("Configuring the WAN Mode" on page 2-15); also required for the VPN tunnels to fail over. When using rollover mode, you must configure a Dynamic DNS service (see "Configuring Dynamic DNS (If Needed)" on page 2-16 to select and configure the Dynamic DNS service).

Setting up a VPN Connection using the VPN Wizard

Setting up a VPN tunnel connection requires that all settings and parameters on both sides of the VPN tunnel match or mirror each other precisely, which can be a daunting task. The VPN Wizard can assist in guiding you through the setup procedure by asking you a series of questions that will determine the IPSec keys and VPN policies it sets up. It also will set the parameters for the network connection: Security Association, traffic selectors, authentication algorithm, and encryption. The parameters used by the VPN wizard are based on the VPNC recommendations.

Creating a VPN Tunnel to a Gateway

You can set up multiple Gateway VPN tunnel policies through the VPN Wizard. You can also set up multiple remote VPN Client policies through the VPN Wizard. A remote client policy can support up to 25 clients.

To create a VPN tunnel gateway policy using the VPN Wizard:

1. Select **VPN** from the main menu and **VPN Wizard** from the submenu. The **VPN Wizard** screen will display.
2. Select **Gateway** as your **VPN tunnel connection**. The wizard needs to know if you are planning to connect to a remote Gateway or setting up the connection for a remote client/PC to establish a secure connection to this device.
3. Select a **Connection Name**. Enter an appropriate name for the connection. This name is not supplied to the remote VPN Endpoint. It is used to help you manage the VPN settings.
4. Enter a **Pre-shared Key**. The key must be entered both here and on the remote VPN Gateway, or the remote VPN Client. This key length should be minimum 8 characters and should not exceed 49 characters. This method does not require using a CA (Certificate Authority).
5. Enter the **Remote WAN IP Address or Internet Name** of the gateway you want to connect to.

   Both the remote WAN address and the your local WAN address are required. When choosing these addresses, follow the guidelines in Table 5-1 above.

   The remote WAN IP address of the Gateway must be a public address or the Internet name of the Gateway. The *Internet name* is the Fully Qualified Domain Name (FQDN) as setup in a Dynamic DNS service. Both local and remote ends should be defined as either IP addresses or Internet Names (FQDN). A combination of IP address and Internet Name is not permissible.
6. Enter your **Local WAN IP Address or Internet Name**.

The Local WAN IP address is the address used in the IKE negotiation phase. Automatically, the WAN IP address assigned by your ISP may display. You can modify the address to use your FQDN; required if the WAN Mode you selected is auto-rollover.

7. Enter the **Remote LAN IP Address and Subnet Mask** of the remote gateway.

   The information entered here must match the Local LAN IP and Subnet Mask of the remote gateway; otherwise the secure tunnel will fail to connect.The IP address range used on the remote LAN must be different from the IP address range used on the local LAN.

8. Click **Apply** to save your settings. the **VPN Policies** table will display showing your VPN policy. You can click the IKE Policies tab to view the corresponding IKE Policy.

Creating a VPN Tunnel Connection to a VPN Client

You can set up multiple Gateway VPN tunnel policies through the VPN Wizard. Multiple remote VPN Client policies can also be set up through the VPN Wizard by changing the default End Point Information settings. A remote client policy can support up to 25 clients. The remote clients must configure the “Local Identity” field in their policy as “PolicyName<*X*>.fvs_remote.com”, where *X* stands for a number from 1 to 25.

As an example, if the client-type policy on the router is configured with “home” as the policy name, and if two users are required to connect using this policy, then the “Local Identity” in their policy should be configured as “home1.fvs_remote.com” and “home2.fvs_remote.com”, respectively.

To create a VPN Client Policy using the VPN Wizard:

1. Select **VPN** from the main menu and **VPN Wizard** from the submenu. The **VPN Wizard** screen will display.
2. Select **VPN Client** as your **VPN tunnel connection**. The wizard needs to know if you are planning to connect to a remote Gateway or setting up the connection for a remote client/PC to establish a secure connection to this device.
3. Select a **Connection Name**. Enter an appropriate name for the connection. This name is not supplied to the remote VPN Endpoint. It is used to help you manage the VPN settings.
4. Enter a **Pre-shared Key**. The key must be entered both here and on the remote VPN Gateway, or the remote VPN Client. This key length should be minimum 8 characters and should not exceed 49 characters. This method does not require using a CA (Certificate Authority).
5. The **Remote Identifier Information** and the **Local Identifier Information** will display with the default IKE Client Policy values: **fvs_remote.com** for the remote end point and **fvs_local.com** for the local end point.

6. Click **Apply**. The **VPN Client** screen will display showing that the VPN Client has been enabled. Click the IKE Policies tab to view the corresponding IKE Client Policy.

IKE Policies

The IKE (Internet Key Exchange) protocol performs negotiations between the two VPN Gateways, and provides automatic management of the Keys used in IPSec. It is important to remember that:

- “Auto” generated VPN policies must use the IKE negotiation protocol.
- “Manual” generated VPN policies cannot use the IKE negotiation protocol.

IKE Policy Operation

IKE Policies are activated when:

1. The VPN Policy Selector determines that some traffic matches an existing VPN Policy. If the VPN policy is of type “Auto”, then the **Auto Policy Parameters** defined in the VPN Policy are accessed which specify which IKE Policy to use.
2. If the VPN Policy is a “Manual” policy, then the **Manual Policy Parameters** defined in the VPN Policy are accessed and the first matching IKE Policy is used to start negotiations with the remote VPN Gateway.
   - If negotiations fail, the next matching IKE Policy is used.
   - If none of the matching IKE Policies are acceptable to the remote VPN Gateway, then a VPN tunnel cannot be established.
3. An IKE session is established, using the SA (Security Association) parameters specified in a matching IKE Policy:
   - Keys and other parameters are exchanged.
   - An IPsec SA (Security Association) is established, using the parameters in the VPN Policy.

The VPN tunnel is then available for data transfer.

IKE Policy Table

When you use the VPN Wizard to set up a VPN tunnel, an IKE Policy is established and populated in the Policy Table and is given the same name as the new VPN connection name. You can also edit exiting policies or add new IKE policies directly on the Policy Table Screen. Each policy contains the following data:

- **Name**. Uniquely identifies each IKE policy. The name is chosen by you and used for the purpose of managing your policies; it is not supplied to the remote VPN Server. If the Policy is a Client Policy, it will be prepended by an "*".
- **Mode**. Two modes are available: either "Main" or "Aggressive".
  - Main Mode is slower but more secure.
  - Aggressive mode is faster but less secure. (If specifying either a FQDN or a User FQDN name as the Local ID/Remote ID, aggressive mode is automatically selected.)
- **Local ID**. The IKE/ISAKMP identify of this device. (The remote VPN must have this value as their "Remote ID".)
- **Remote ID**. The IKE/ISAKMP identify of the remote VPN Gateway. (The remote VPN must have this value as their "Local ID".)
- **Encr**. Encryption Algorithm used for the IKE SA. The default setting using the VPN Wizard is 3DES. (This setting must match the Remote VPN.)
- **Auth**. Authentication Algorithm used for the IKE SA. The default setting using the VPN Wizard is SHA1. (This setting must match the Remote VPN.)
- **DH**.
- Diffie-Hellman Group. The Diffie-Hellman algorithm is used when exchanging keys. The DH Group sets the number of bits. The VPN Wizard default setting is Group 2. (This setting must match the Remote VPN.)

  To gain a more complete understanding of the encryption, authentication and DH algorithm technologies, see Appendix B, "Related Documents".

VPN Policies

You can create two types of VPN Policies. When using the VPN Wizard to create a VPN policy, only the Auto method is available.

- **Manual**. All settings (including the keys) for the VPN tunnel are manually input at each end (both VPN endpoints). No third party server or organization is involved.
- **Auto**. Some parameters for the VPN tunnel are generated automatically by using the IKE (Internet Key Exchange) protocol to perform negotiations between the two VPN endpoints (the Local ID Endpoint and the Remote ID Endpoint).

In addition, a CA (Certificate Authority) can also be used to perform authentication (see "Certificates" on page 5-33). To use a CA, each VPN Gateway must have a Certificate from the CA. For each Certificate, there is both a "Public Key" and a "Private Key". The "Public Key" is freely distributed, and is used to encrypt data. The receiver then uses their "Private Key" to decrypt the data (without the Private Key, decryption is impossible). CAs can be beneficial since using them reduces the amount of data entry required on each VPN Endpoint.

VPN Policy Operation

The VPN Policies screen allows you to add additional policies—either Auto or Manual—and to manage the VPN policies already created. You can edit policies, enable or disable them, or delete them entirely. The rules for VPN policy use conform to:

1. Traffic covered by a policy will automatically be sent via a VPN tunnel.
2. The VPN tunnel is created according to the parameters in the SA (Security Association).
3. The remote VPN Endpoint must have a matching SA, or it will refuse the connection.

VPN Policy Table

When you use the VPN Wizard to set up a VPN tunnel, both a VPN Policy and an IKE Policy is established and populated in both Tables on the VPN Policies screen. The name you selected as the VPN Tunnel connection name during Wizard setup identifies both the VPN Policy and IKE Policy. You can also edit exiting policies, add new VPN policies directly or change the policy hierarchy to the Policy Table. The Policy Table contains the following fields:

- **! (Status)**. Indicates whether the policy is enabled (green circle) or disabled (grey circle). To Enable or Disable a Policy, check the radio box adjacent to the circle and click **Enable** or **Disable**, as required.
- **Name**. Each policy is given a unique name (the Connection Name when using the VPN Wizard). Client Policies are annotated by an "*".
- **Type**. The Type is "Auto" or "Manual" as described previously (Auto is used during VPN Wizard configuration).

- **Local**. IP address (either a single address, range of address or subnet address) on your local LAN. Traffic must be from (or to) these addresses to be covered by this policy. (Subnet address is the default IP address when using the VPN Wizard).
- **Remote**. IP address or address range of the remote network. Traffic must be to (or from) these addresses to be covered by this policy. (The VPN Wizard default requires the remote LAN IP address and subnet mask for a gateway policy).
- **AH**. Authentication Header. This specifies the authentication protocol for the VPN header (VPN Wizard default is disabled).
- **ESP**. Encapsulating Security Payload. This specifies the encryption protocol used for the VPN data (VPN Wizard default is enabled).

VPN Tunnel Connection Status

Recent VPN tunnel activity is shown on the **IPSec Connection Status** screen (accessed by selecting **VPN** from the main menu and **Connection Status** from the submenu).You can set a Poll Interval (in seconds) to check the connection status of all active IKE Policies to obtain the latest VPN tunnel activity. The Active IPSec (SA)s table also lists current data for each active IPSec SA (Security Association):

- **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.
- **Tx (Packets).** The number of packets transmitted over this SA.
- **State**. The current state of the SA. Phase 1 is “Authentication phase” and Phase 2 is “Key Exchange phase”.
- **Action**. Allows you to terminate or build the SA (connection), if required.

Creating a VPN Gateway Connection: Between FVS338 and FVX538

This section describes how to configure a VPN connection between a NETGEAR FVS338 VPN Firewall and a NETGEAR FVX538 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.

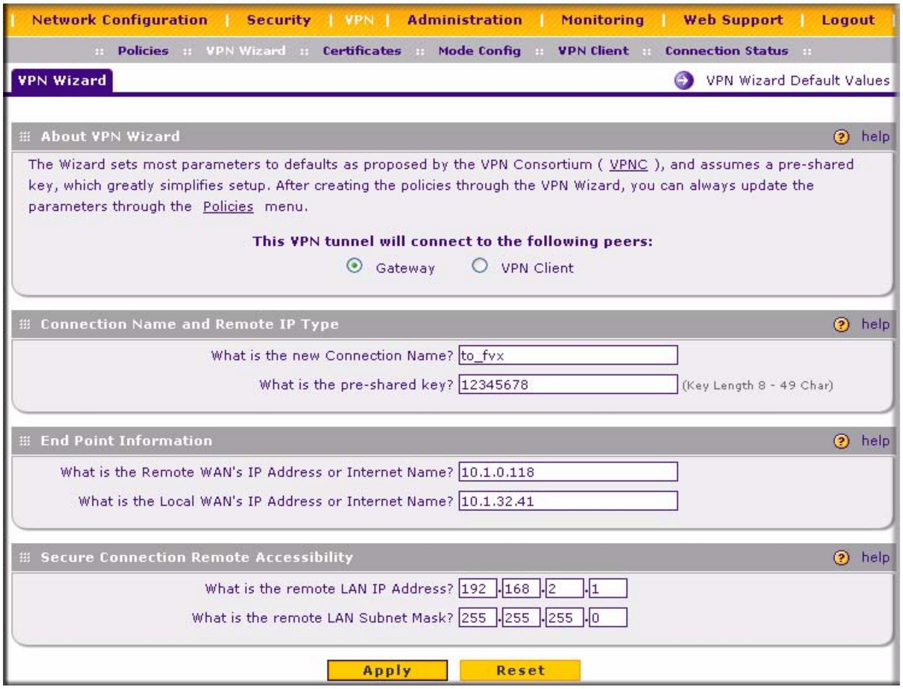
This procedure was developed and tested using:

- Netgear FVS338 VPN Firewall
  - WAN IP address: 10.1.32.41
  - LAN IP address subnet:192.168.1.1/255.255.255.0
- Netgear FVX538 VPN Firewall
  - WAN1 IP address: 10.1.0.118
  - LAN IP address subnet: 192.168.2.1/255.255.255.0

Configuring the FVS338

To configure the FVS338 using the VPN Wizard:

1. Select **VPN** from the main menu and **VPN Wizard** from the submenu. The **VPN Wizard** screen will display.
2. Check the **Gateway** radio box to establish a gateway-to-gateway VPN tunnel.
3. Give the new connection a name such as **to_fvx.**
4. Enter a value for the pre-shared key.
5. Enter the WAN IP address or Internet name of the remote WAN and the WAN IP Address or Internet name of the local WAN. The address type must match.
6. Enter the remote LAN IP address and subnet mask.
7. Click **Apply** to create the IKE and VPN policies.


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
:: Policies :: VPN Wizard :: Certificates :: Mode Config :: VPN Client :: Connection Status ::
VPN Wizard
VPN Wizard Default Values
help
Apply
Reset

About VPN Wizard

The Wizard sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a pre-shared key, which greatly simplifies setup. After creating the policies through the VPN Wizard, you can always update the parameters through the Policies menu.

This VPN tunnel will connect to the following peers:
● Gateway ○ VPN Client

Connection Name and Remote IP Type

What is the new Connection Name? to_fvx
What is the pre-shared key? 12345678 (Key Length 8 - 49 Char)

End Point Information

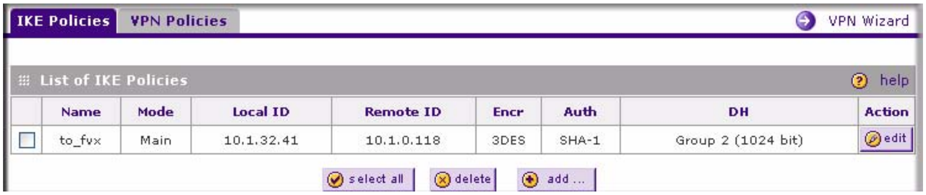
What is the Remote WAN's IP Address or Internet Name? 10.1.0.118
What is the Local WAN's IP Address or Internet Name? 10.1.32.41

Secure Connection Remote Accessibility

What is the remote LAN IP Address? 192 .168 .2 .1
What is the remote LAN Subnet Mask? 255 .255 .255 .0

Figure 5-1

The **IKE Policies** screen will display showing the new “to_fvx” policy.

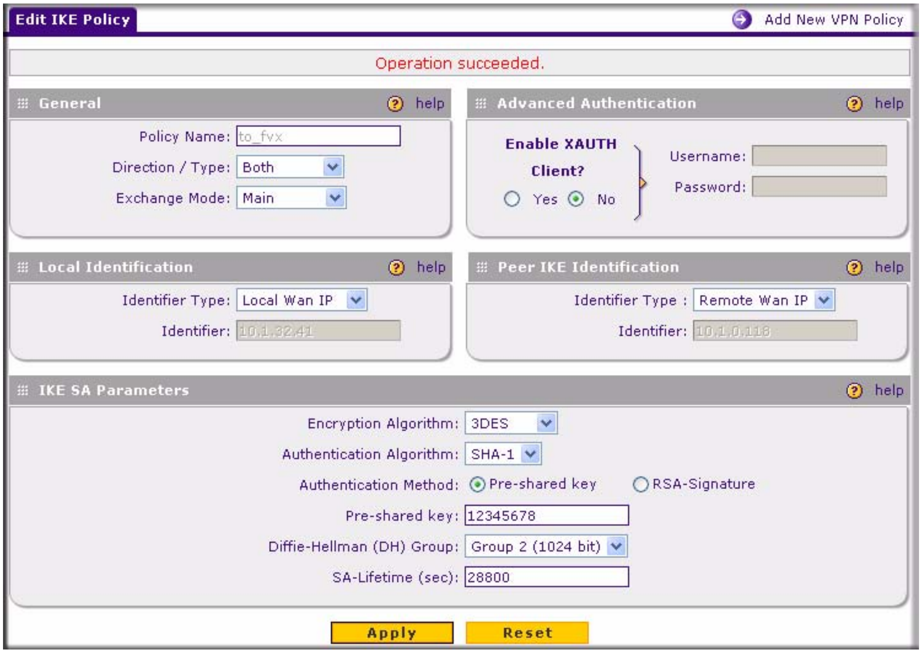


List of IKE Policies

	Name	Mode	Local ID	Remote ID	Encr	Auth	DH	Action
□	to_fvx	Main	10.1.32.41	10.1.0.118	3DES	SHA-1	Group 2 (1024 bit)	edit

Figure 5-2

You can view the IKE parameters by clicking **Edit** in the **Action** column adjacent to the “to-fvs” policy. It should not be necessary to make any changes.



Edit IKE Policy — Add New VPN Policy

Operation succeeded.

General

Policy Name: to_fvx

Direction / Type: Both

Exchange Mode: Main

Advanced Authentication

Enable XAUTH Client? ○ Yes ● No

Username:

Password:

Local Identification

Identifier Type: Local Wan IP

Identifier: 10.1.32.41

Peer IKE Identification

Identifier Type : Remote Wan IP

Identifier: 10.1.0.118

IKE SA Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

Authentication Method: ● Pre-shared key ○ RSA-Signature

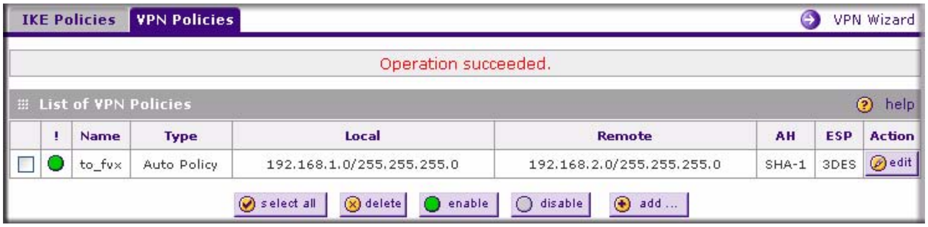
Pre-shared key: 12345678

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

SA-Lifetime (sec): 28800

Figure 5-3

Click the **IKE Policies** tab to view the corresponding IKE Policy. The **IKE Policies** screen will display.



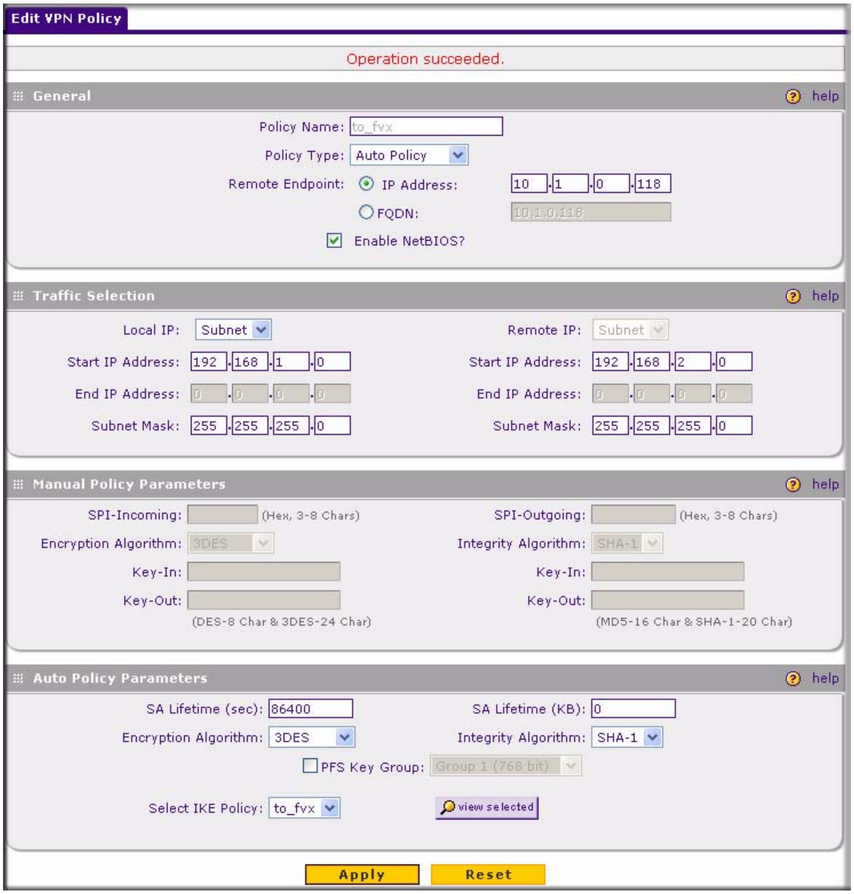
Operation succeeded.

List of VPN Policies

	!	Name	Type	Local	Remote	AH	ESP	Action
□	●	to_fvx	Auto Policy	192.168.1.0/255.255.255.0	192.168.2.0/255.255.255.0	SHA-1	3DES	edit

Figure 5-4

You can view the VPN parameters by clicking **Edit** in the **Actions** column adjacent to “to_fvx”. It should not be necessary to make any changes



Edit VPN Policy

Operation succeeded.

General — help

Policy Name: to_fvx

Policy Type: Auto Policy

Remote Endpoint: ● IP Address: 10 . 1 . 0 . 118

○ FQDN: 10.1.0.118

☑ Enable NetBIOS?

Traffic Selection — help

Local IP:	Subnet	Remote IP:	Subnet
Start IP Address:	192 . 168 . 1 . 0	Start IP Address:	192 . 168 . 2 . 0
End IP Address:	0 . 0 . 0 . 0	End IP Address:	0 . 0 . 0 . 0
Subnet Mask:	255 . 255 . 255 . 0	Subnet Mask:	255 . 255 . 255 . 0

Manual Policy Parameters — help

SPI-Incoming:	(Hex, 3-8 Chars)	SPI-Outgoing:	(Hex, 3-8 Chars)
Encryption Algorithm:	3DES	Integrity Algorithm:	SHA-1
Key-In:		Key-In:	
Key-Out:		Key-Out:	
	(DES-8 Char & 3DES-24 Char)		(MD5-16 Char & SHA-1-20 Char)

Auto Policy Parameters — help

SA Lifetime (sec):	86400	SA Lifetime (KB):	0
Encryption Algorithm:	3DES	Integrity Algorithm:	SHA-1

□ PFS Key Group: Group 1 (768 bit)

Select IKE Policy: to_fvx — view selected

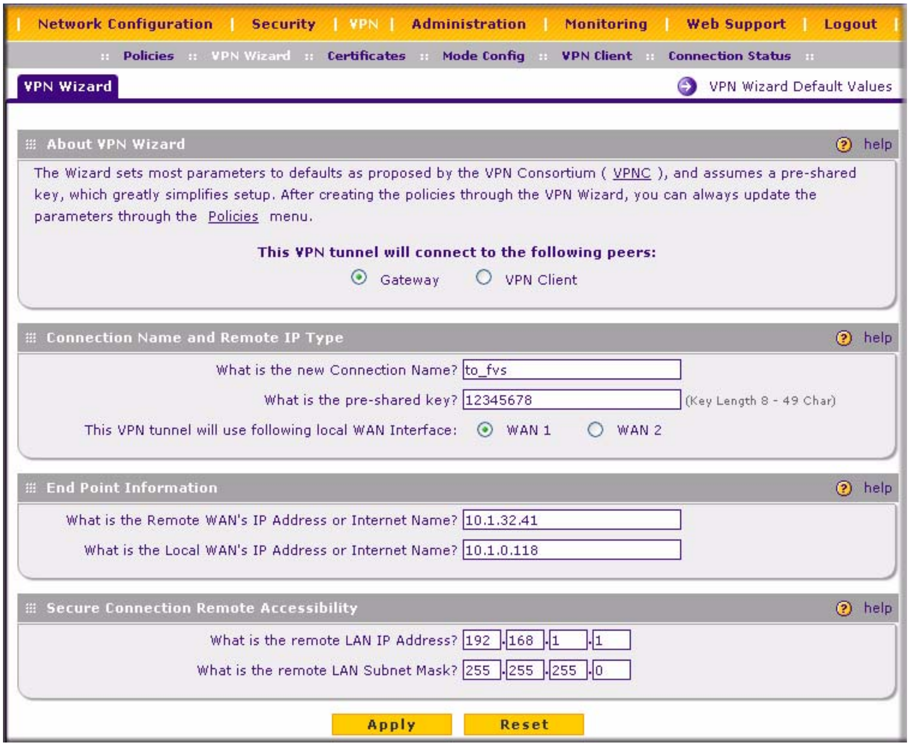
Figure 5-5

Configuring the FVX538

To configure the FVX538 using the VPN Wizard:

1. Select **VPN** from the main menu. The **Policies** screen will display. Click the **VPN Wizard** link. The **VPN Wizard** screen will display.
2. Check the **Gateway** radio box to establish a remote VPN gateway.
3. Give the new connection a name such as **to_fvs.**
4. Enter a value for the pre-shared key.
5. Enter the WAN IP address or Internet name of the remote WAN.

6. Enter the remote LAN IP address and subnet mask.
7. Click **Apply** to create the “to_fvs” IKE and VPN policies.


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Policies :: VPN Wizard :: Certificates :: Mode Config :: VPN Client :: Connection Status ::
VPN Wizard
VPN Wizard Default Values
help

About VPN Wizard

The Wizard sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a pre-shared key, which greatly simplifies setup. After creating the policies through the VPN Wizard, you can always update the parameters through the Policies menu.

This VPN tunnel will connect to the following peers: ● Gateway ○ VPN Client

Connection Name and Remote IP Type

What is the new Connection Name? to_fvs
What is the pre-shared key? 12345678 (Key Length 8 - 49 Char)
This VPN tunnel will use following local WAN Interface: ● WAN 1 ○ WAN 2

End Point Information

What is the Remote WAN's IP Address or Internet Name? 10.1.32.41
What is the Local WAN's IP Address or Internet Name? 10.1.0.118

Secure Connection Remote Accessibility

What is the remote LAN IP Address? 192 .168 .1 .1
What is the remote LAN Subnet Mask? 255 .255 .255 .0

Figure 5-6

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 Client Connection: VPN Client to FVS338

This section describes how to configure a VPN connection between a Windows PC (the client) installed with the NETGEAR ProSafe VPN Client and the VPN firewall.

Using the FVS338 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 the NETGEAR 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:

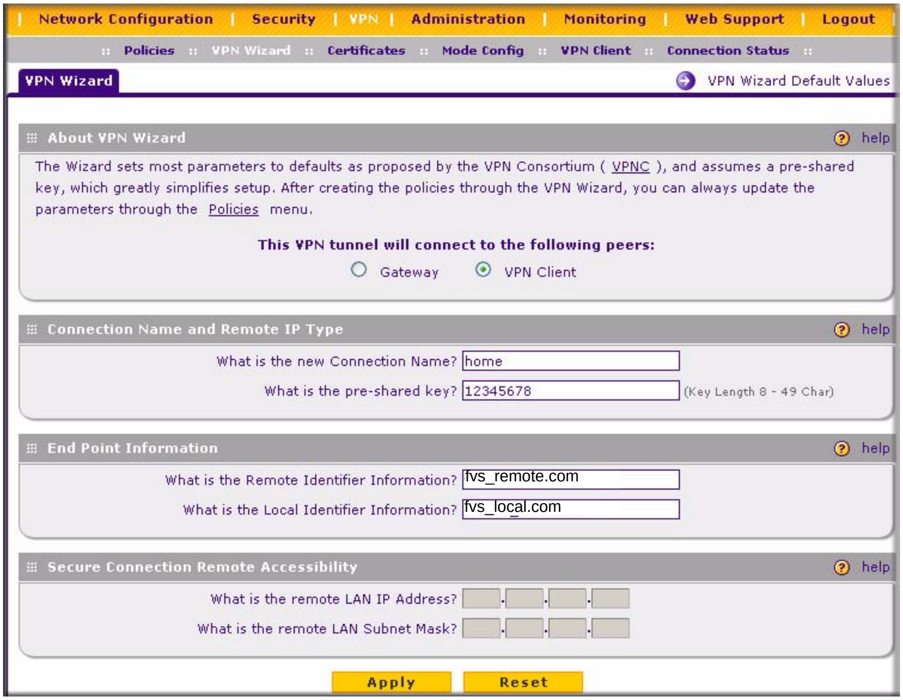
- NETGEAR ProSafe VPN Firewall 50 FVS338
- NETGEAR ProSafe VPN Client
- NAT router: NETGEAR FR114P

Configuring the FVS338

To configure the FVS338 using the VPN Wizard:

1. Select **VPN** from the main menu. The **Policies** screen will display. Click the **VPN Wizard** link. The **VPN Wizard** screen will display.
2. Check the **VPN Client** radio box to establish a remote VPN client.
3. Give the new connection a name such as **home.**
4. Enter a value for the pre-shared key.
5. Click **Apply.** The **VPN Policies** screen will display showing a VPN Client policy named home. Select the **VPN Policies** tab to display the corresponding "home" VPN Policy.

> **Note:** When XAuthentication (XAUTH) is enabled, incoming VPN connections are authenticated against the FVS338 Network Database first, then, if configured, a RADIUS server is checked.


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Policies :: VPN Wizard :: Certificates :: Mode Config :: VPN Client :: Connection Status ::
VPN Wizard
VPN Wizard Default Values
help
Apply
Reset

About VPN Wizard

The Wizard sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a pre-shared key, which greatly simplifies setup. After creating the policies through the VPN Wizard, you can always update the parameters through the Policies menu.

This VPN tunnel will connect to the following peers:

○ Gateway ● VPN Client

Connection Name and Remote IP Type

What is the new Connection Name? home

What is the pre-shared key? 12345678 (Key Length 8 - 49 Char)

End Point Information

What is the Remote Identifier Information? fvs_remote.com

What is the Local Identifier Information? fvs_local.com

Secure Connection Remote Accessibility

What is the remote LAN IP Address? . . .

What is the remote LAN Subnet Mask? . . .

Figure 5-7

Configuring the VPN Client

On a remote PC that has a NETGEAR ProSafe VPN Client installed, configure the client using the FVS338 VPN Client default parameters (displayed in both the IKE Policy table and the VPN Policy table of the FVS338 under the name “home”):

- Local FQDN (the router): fvs_local.com
- Remote FQDN (the client): fvs_remote.com
- Encryption Algorithm: 3DES
- Authentication Algorithm: SHA-1
- Pre-shared key: 12345678 (defined by user)
- Diffie-Hellman (DH) Group: Group 2 (1024 bit)
- SA Life Time: unspecified
- Remote LAN IP subnet: 192.168.1.0/255.255.255.0

To configure the VPN Client:

1. Right-click on the VPN client icon in your Windows toolbar and select the **Security Policy Editor**. The **Security Policy Editor** screen will display.
2. In the upper left of the Policy Editor window, click the New Document icon to open a New Connection.

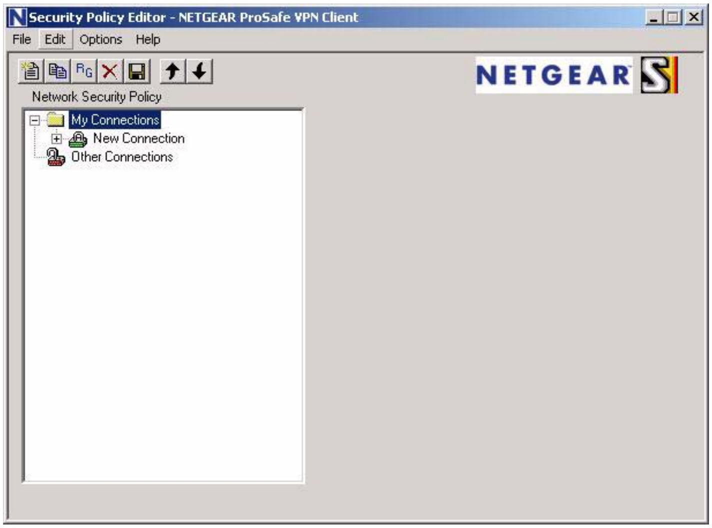
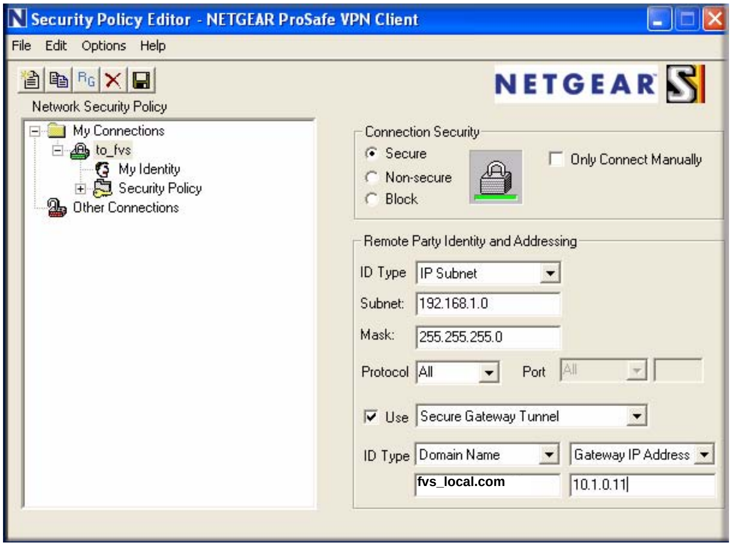


Figure 5-8

3. Give the New Connection a name, such as **`to_FVS`** (shown in Figure 5-9)**.**
4. In the Remote Party Identity section, from the **ID Type** pull-down menu, select **IP Subnet**.
5. Enter the LAN IP Subnet Address and Subnet Mask of the FVS338 LAN.
6. Check **Connect using** radio box and select **Connect using Secure Gateway Tunnel** from the pull-down menu.
7. From the **ID Type** pull-down menu, select **Domain Name** and **Gateway IP Address**.

3. For the Domain Name, enter **`fvs_local.com`** and enter the WAN IP Address of the FVS338.



Connection Security

● Secure
○ Non-secure
○ Block

□ Only Connect Manually

Remote Party Identity and Addressing

ID Type: IP Subnet

Subnet: 192.168.1.0

Mask: 255.255.255.0

Protocol: All   Port: All

☑ Use Secure Gateway Tunnel

ID Type: Domain Name   Gateway IP Address

fvs_local.com   10.1.0.11

Figure 5-9

8. In the left frame, click on **My Identity** (shown in Figure 5-10).

9. From the **Select Certificate** pull-down menu, select **None**.

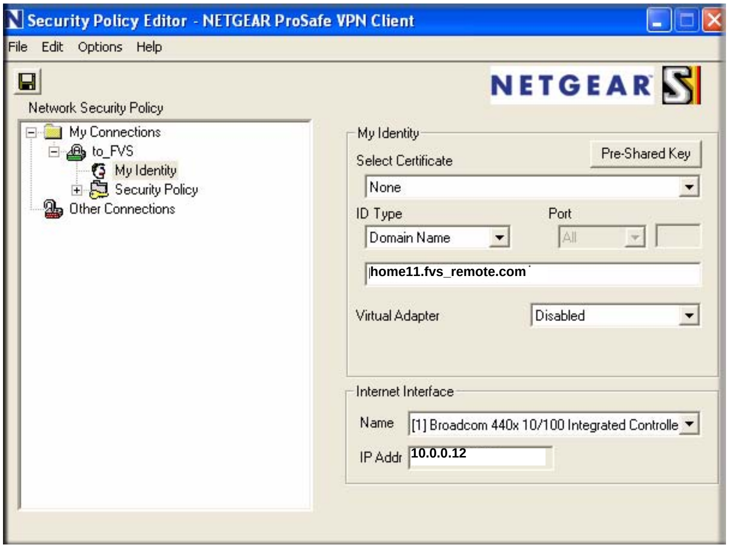
10. From the **ID Type** pull-down menu, select **Domain Name**.

    The value entered under Domain Name will be in 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 entered "home11.fvs_remote.com". Up to 25 user variations can be served by one policy.

11. Leave Virtual Adapter disabled, and select your computer's Network Adapter. Your current IP address will appear.



Select Certificate: None

ID Type: Domain Name

Port: All

home11.fvs_remote.com

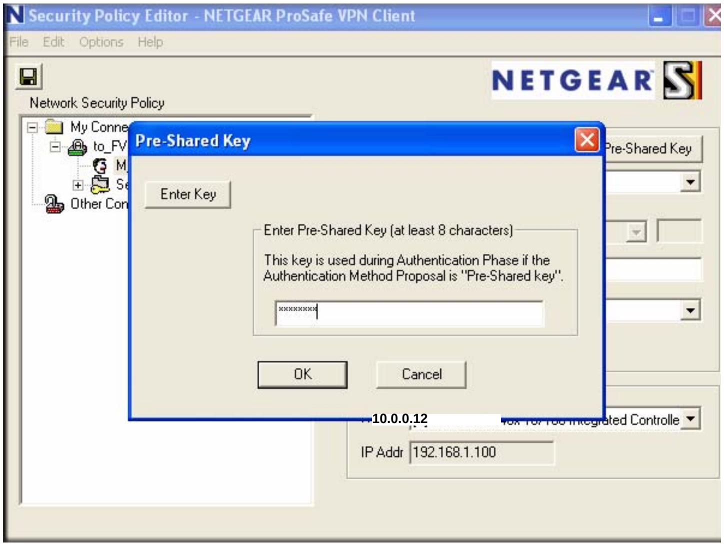
Virtual Adapter: Disabled

Name: [1] Broadcom 440x 10/100 Integrated Controlle

IP Addr: 10.0.0.12

Figure 5-10

12. Before leaving the My Identity menu, click **Pre-Shared Key**.
13. Click **Enter Key**, and type your preshared key. Click **OK**. This key will be shared by all users of the FVS338 policy “home”.



Enter Pre-Shared Key (at least 8 characters)

This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".

****

10.0.0.12

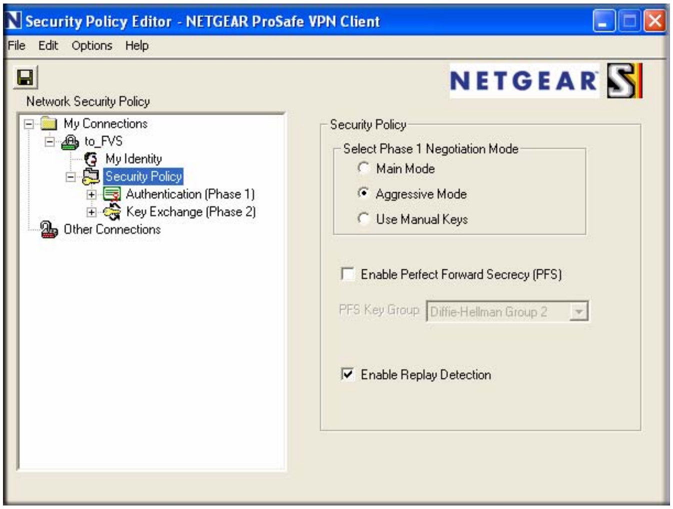
IP Addr: 192.168.1.100

Figure 5-11

14. In the left frame, click **Security Policy** (shown in Figure 5-12).

15. Select **Phase 1 Negotiation Mode** by checking the **Aggressive Mode** radio box.

16. **PFS Key Group** should be disabled, and **Enable Replay Detection** should be enabled.



Security Policy

Select Phase 1 Negotiation Mode

○ Main Mode

● Aggressive Mode

○ Use Manual Keys

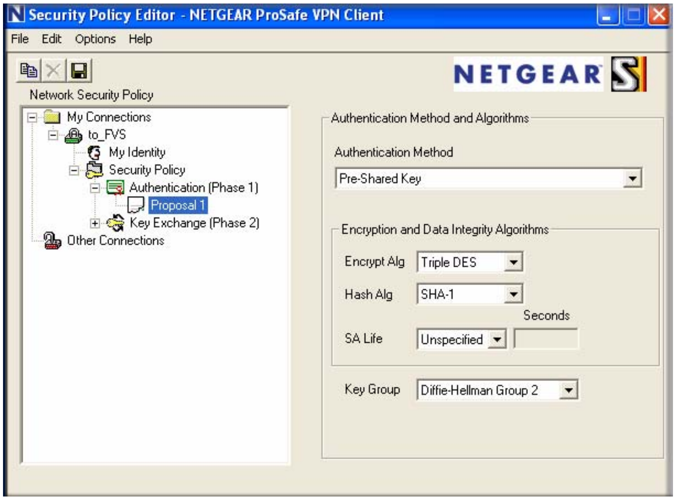
☐ Enable Perfect Forward Secrecy (PFS)

PFS Key Group: Diffie-Hellman Group 2

☑ Enable Replay Detection

Figure 5-12

17. In the left frame, expand **Authentication (Phase 1)** and select **Proposal 1**. Compare with the figure below. No changes should be necessary.



Authentication Method and Algorithms

Authentication Method: Pre-Shared Key

Encryption and Data Integrity Algorithms

Encrypt Alg: Triple DES

Hash Alg: SHA-1

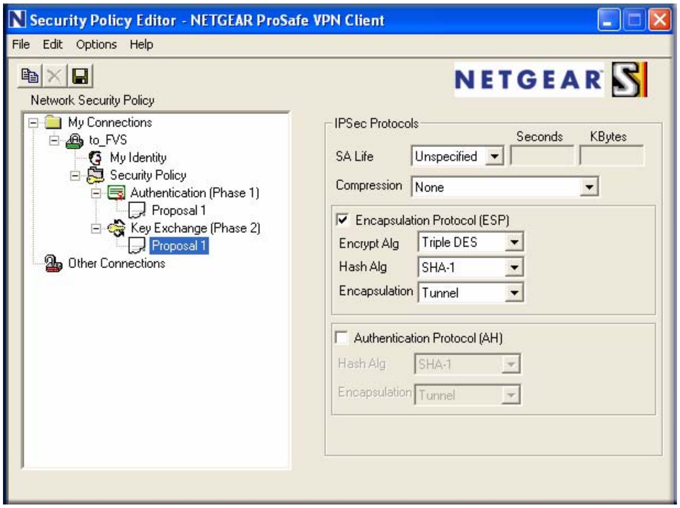
SA Life: Unspecified Seconds

Key Group: Diffie-Hellman Group 2

Figure 5-13

18. In the left frame, expand **Key Exchange (Phase 2)** and select **Proposal 1**. Compare with the figure below. No changes should be necessary.

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



SA Life: Unspecified

Compression: None

☑ Encapsulation Protocol (ESP)

Encrypt Alg: Triple DES

Hash Alg: SHA-1

Encapsulation: Tunnel

☐ Authentication Protocol (AH)

Hash Alg: SHA-1

Encapsulation: Tunnel

Figure 5-14

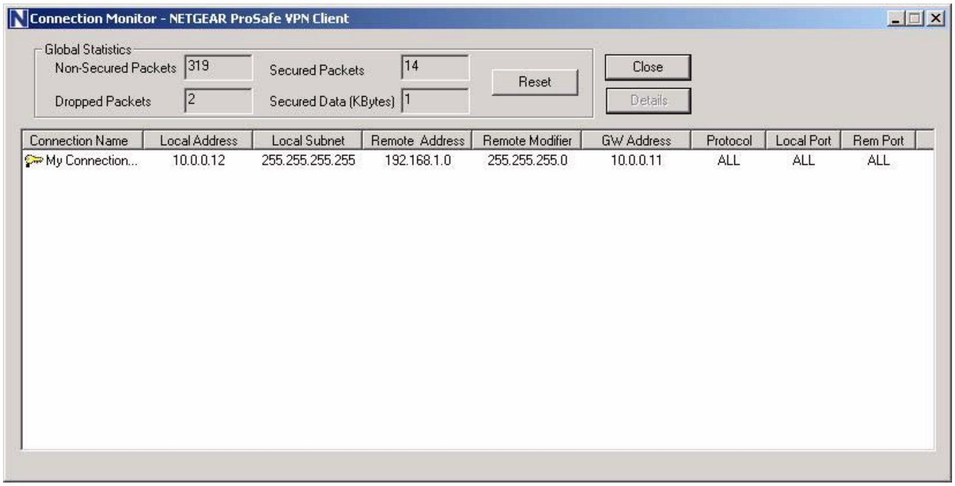
Testing the Connection

To test your VPN connection:

1. Right-click the VPN client icon in your Windows toolbar and select **Connect...**, and then select **My Connections\to_FVS**.

   Within 30 seconds you should receive the message “Successfully connected to My Connections\to_FVS” and the VPN client icon in the toolbar should display On:

2. For additional status and troubleshooting information, right-click the VPN client icon in your Windows toolbar and select **Connection Monitor** or **Log Viewer**; or view the VPN Logs and VPN Connection Status of the FVS338.



Global Statistics

Non-Secured Packets	319	Secured Packets	14
Dropped Packets	2	Secured Data (KBytes)	1

Connection Name	Local Address	Local Subnet	Remote Address	Remote Modifier	GW Address	Protocol	Local Port	Rem Port
My Connection...	10.0.0.12	255.255.255.255	192.168.1.0	255.255.255.0	10.0.0.11	ALL	ALL	ALL

Figure 5-15

Extended Authentication (XAUTH) Configuration

When connecting many VPN clients to a VPN gateway router, an administrator may want a unique user authentication method beyond relying on a single common preshared key for all clients. Although the administrator could configure a unique VPN policy for each user, it is more convenient for the VPN gateway router to authenticate users from a stored list of user accounts. XAUTH provides the mechanism for requesting individual authentication information from the user, and a local User Database or an external authentication server, such as a RADIUS server, provides a method for storing the authentication information centrally in the local network.

XAUTH is enabled when adding or editing an IKE Policy. Two types of XAUTH are available:

- **Edge Device.** If this is selected, the router is used as a VPN concentrator where one or more gateway tunnels terminate. If this option is chosen, you must specify the authentication type to be used in verifying credentials of the remote VPN gateways: User Database, RADIUS-PAP, or RADIUS-CHAP.
- **IPSec Host.** If you want authentication by the remote gateway, enter a User Name and Password to be associated with this IKE policy. If this option is chosen, the remote gateway must specify the user name and password used for authenticating this gateway.

Note: If a RADIUS-PAP server is enabled for authentication, XAUTH will first check the local User Database for the user credentials. If the user account is not present, the router will then connect to a RADIUS server.

Configuring XAUTH for VPN Clients

Once the XAUTH has been enabled, you must establish user accounts on the Local Database to be authenticated against XAUTH, or you must enable a RADIUS-CHAP or RADIUS-PAP server.

Note: If you are modifying an existing IKE Policy to add **XAUTH**, if it is in use by a VPN Policy, the VPN policy must be disabled before you can modify the IKE Policy.

To enable and configure XAUTH:

1. Select **VPN** from the main menu and **Policies** from the submenu. The **IKE Policies** screen will display.
2. You can either modify an existing IKE Policy by clicking **Edit** adjacent to the policy, or create a new IKE Policy by clicking **Add.**

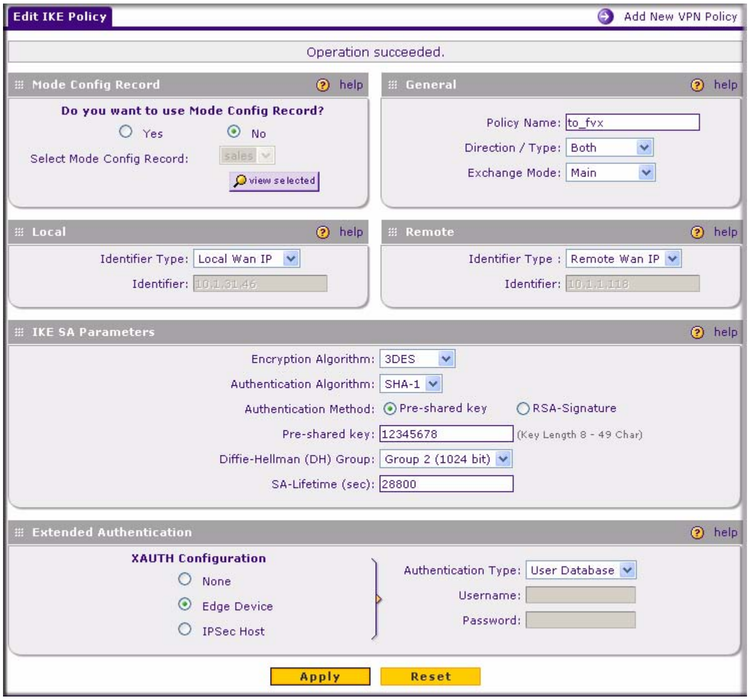
   Note: If the IKE policy is in use by a VPN Policy, you must either disable or delete the VPN policy before making changes to the IKE Policy.

3. In the **Extended Authentication** section, select the **Authentication Type** from the pull-down menu which will be used to verify user account information. Select
   - **Edge Device** to use this router as a VPN concentrator where one or more gateway tunnels terminate. When this option is chosen, you will need to specify the authentication type to be used in verifying credentials of the remote VPN gateways.
     – **User Database** to verify against the router’s user database. Users must be added through the User Database screen (see “User Database Configuration” on page 5-22).

     – **RADIUS–CHAP** or **RADIUS–PAP** (depending on the authentication mode accepted by the RADIUS server) to add a RADIUS server. If RADIS–PAP is selected, the router will first check in the User Database to see if the user credentials are available. If the user account is not present, the router will then connect to the RADIUS server (see “RADIUS Client Configuration” on page 5-23).

- **IPSec Host** if you want to be authenticated by the remote gateway. In the adjacent **Username** and **Password** fields, type in the information user name and password associated with the IKE policy for authenticating this gateway (by the remote gateway).

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



Operation succeeded.

Mode Config Record

Do you want to use Mode Config Record? ○ Yes ● No

Select Mode Config Record: sales

General

Policy Name: to_fvx

Direction / Type: Both

Exchange Mode: Main

Local

Identifier Type: Local Wan IP

Identifier: 10.1.31.46

Remote

Identifier Type : Remote Wan IP

Identifier: 10.1.1.118

IKE SA Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

Authentication Method: ● Pre-shared key ○ RSA-Signature

Pre-shared key: 12345678 (Key Length 8 - 49 Char)

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

SA-Lifetime (sec): 28800

Extended Authentication

XAUTH Configuration

○ None

● Edge Device

○ IPSec Host

Authentication Type: User Database

Username:

Password:

Figure 5-16

User Database Configuration

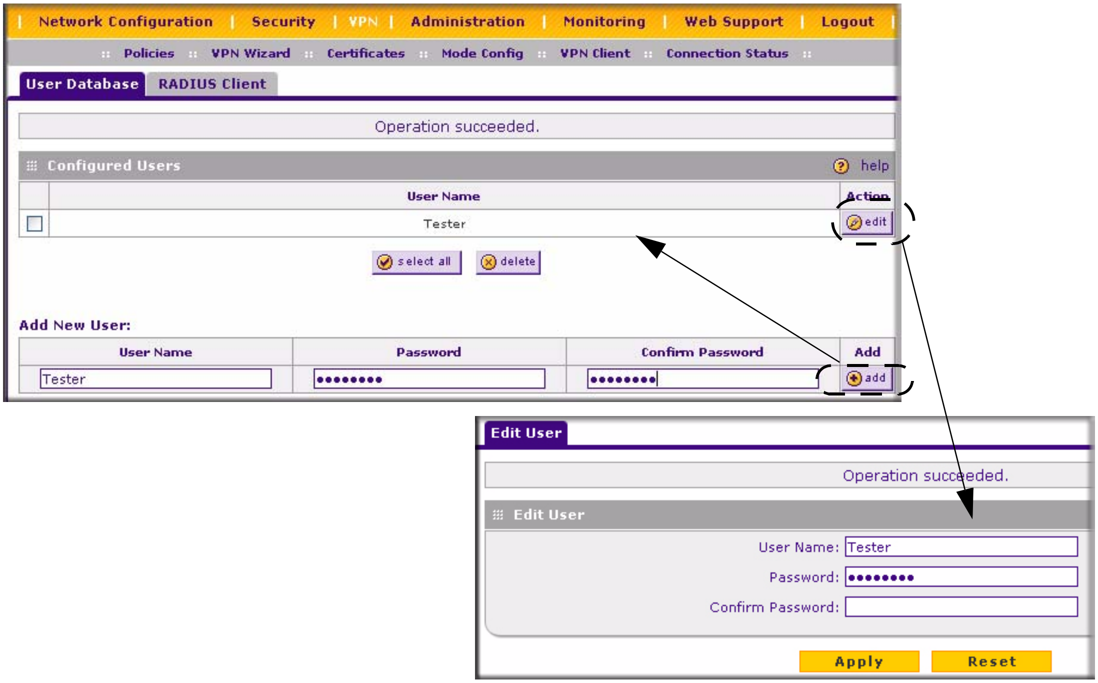
The User Database Screen is used to configure and administer VPN Client users for use by the XAUTH server. Whether or not you use an external RADIUS server, you may want to have some users authenticated locally. These users must be added to the **User Database** Configured Users table.

To add a new user:

1. Select **VPN** from the main menu and **VPN Client** from the submenu. The **User Database** screen will display.

2. Enter a **User Name**. This is the unique ID of a user which will be used in the User Name field of the VPN client.

3. Enter a **Password** for the user, and reenter the password in the **Confirm Password** field.
4. Click **Add.** The User Name will be added to the Configured Hosts table.


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
Policies :: VPN Wizard :: Certificates :: Mode Config :: VPN Client :: Connection Status
User Database
RADIUS Client
help
select all
delete
edit
add
Apply
Reset

Operation succeeded.

Configured Users

	User Name	Action
□	Tester	edit

Add New User:

User Name	Password	Confirm Password	Add
Tester	••••••••	••••••••	add

Edit User

Operation succeeded.

Edit User

User Name:	Tester
Password:	••••••••
Confirm Password:	

Figure 5-17

To edit the user name or password:

1. Click **Edit** opposite the user’s name. The **Edit User** screen will display.
2. Make the required changes to the User Name or Password and click **Apply** to save your settings or **Reset** to cancel your changes and return to the previous settings**.** The modified user name and password will display in the Configured Users table.

RADIUS Client Configuration

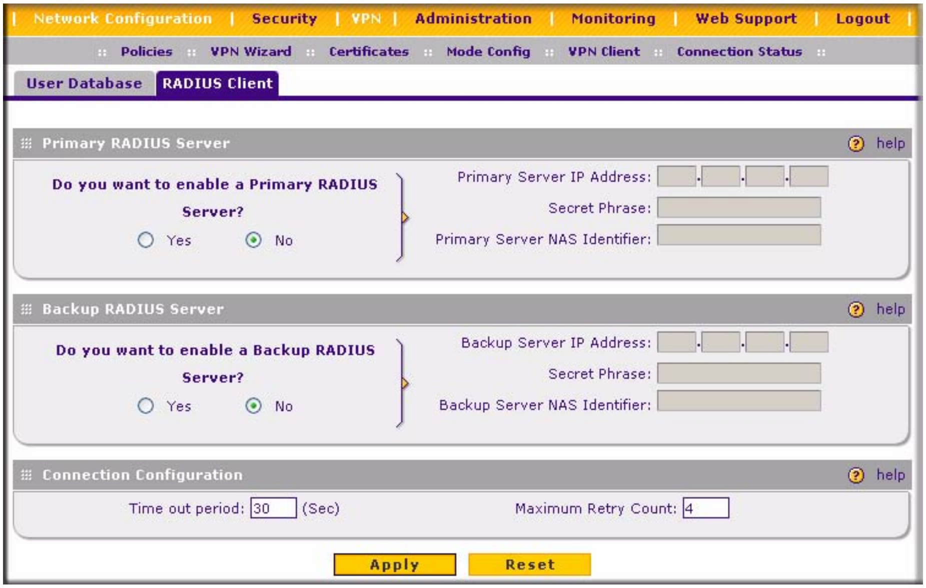
RADIUS (Remote Authentication Dial In User Service, RFC 2865) is a protocol for managing Authentication, Authorization and Accounting (AAA) of multiple users in a network. A RADIUS server will store a database of user information, and can validate a user at the request of a gateway or server in the network when a user requests access to network resources. During the establishment of a VPN connection, the VPN gateway can interrupt the process with an XAUTH (eXtended AUTHentication) request. At that point, the remote user must provide authentication information such as a username/password or some encrypted response using his username/password information. The gateway will try and verify this information first against a local User Database (if RADIUS-PAP is enabled) and then by relaying the information to a central authentication server such as a RADIUS server.

To configure the Primary RADIUS Server:

1. Select **VPN** from the main menu, **VPN Client** from the submenu and then select the **RADIUS Client** tab. The **RADIUS Client** screen will display.
2. Enable the Primary RADIUS server by checking the **Yes** radio box.
3. Enter the Primary **RADIUS Server IP address**.
4. Enter a **Secret Phrase**. Transactions between the client and the RADIUS server are authenticated using a shared secret phrase, so the same Secret Phrase must be configured on both client and server.
5. Enter the **Primary Server NAS Identifier** (Network Access Server). This Identifier MUST be present in a RADIUS request. Ensure that NAS Identifier is configured as the same on both client and server.

   The FVS338 is acting as a NAS (Network Access Server), allowing network access to external users after verifying their authentication information. In a RADIUS transaction, the NAS must provide some NAS Identifier information to the RADIUS Server. Depending on the configuration of the RADIUS Server, the router's IP address may be sufficient as an identifier, or the Server may require a name, which you would enter here. This name would also be configured on the RADIUS Server, although in some cases it should be left blank on the RADIUS Server.
6. Enable a Backup RADIUS Server (if required) by following steps 2 through 5.
7. Set the **Time Out Period**, in seconds, that the router should wait for a response from the RADIUS server.
8. Set the **Maximum Retry Count.** This is the number of tries the router will make to the RADIUS server before giving up.
9. Click **Reset** to cancel any changes and revert to the previous settings.
10. Click **Apply** to save the settings.

➡	**Note:** The Authentication Protocol, usually PAP or CHAP, is configured in the XAUTH section of the VPN Client screen.


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
Policies :: VPN Wizard :: Certificates :: Mode Config :: VPN Client :: Connection Status
User Database
RADIUS Client
help
Apply
Reset

Primary RADIUS Server

Do you want to enable a Primary RADIUS Server?

○ Yes ● No

Primary Server IP Address:

Secret Phrase:

Primary Server NAS Identifier:

Backup RADIUS Server

Do you want to enable a Backup RADIUS Server?

○ Yes ● No

Backup Server IP Address:

Secret Phrase:

Backup Server NAS Identifier:

Connection Configuration

Time out period: 30 (Sec)

Maximum Retry Count: 4

Figure 5-18

Manually Assigning IP Addresses to Remote Users (ModeConfig)

To simply the process of connecting remote VPN clients to the FVS338, the ModeConfig module can be used to assign IP addresses to remote users, including a network access IP address, subnet mask, and name server addresses from the router. Remote users are given IP addresses available in secured network space so that remote users appear as seamless extensions of the network.

In the following example, we configured the VPN firewall using ModeConfig, and then configured a PC running ProSafe VPN Client software using these IP addresses.

- NETGEAR ProSafe VPN Firewall 50
  - WAN IP address: 172.21.4.1
  - LAN IP address/subnet: 192.168.2.1/255.255.255.0
- NETGEAR ProSafe VPN Client software IP address: 192.168.1.2

ModeConfig Operation

After IKE Phase 1 is complete, the VPN connection initiator (remote user/client) asks for IP configuration parameters such as IP address, subnet mask and name server addresses. The ModeConfig module will allocate an IP address from the configured IP address pool and will activate a temporary IPSec policy using the template security proposal information configured in the ModeConfig record.

> **Note:** After configuring a Mode Config record, you must go to the IKE Policies menu and configure an IKE policy using the newly-created Mode Config record as the Remote Host Configuration Record. The VPN Policies menu does not need to be edited.

Setting Up ModeConfig

Two menus must be configured—the ModeConfig menu and the IKE Policies menu.

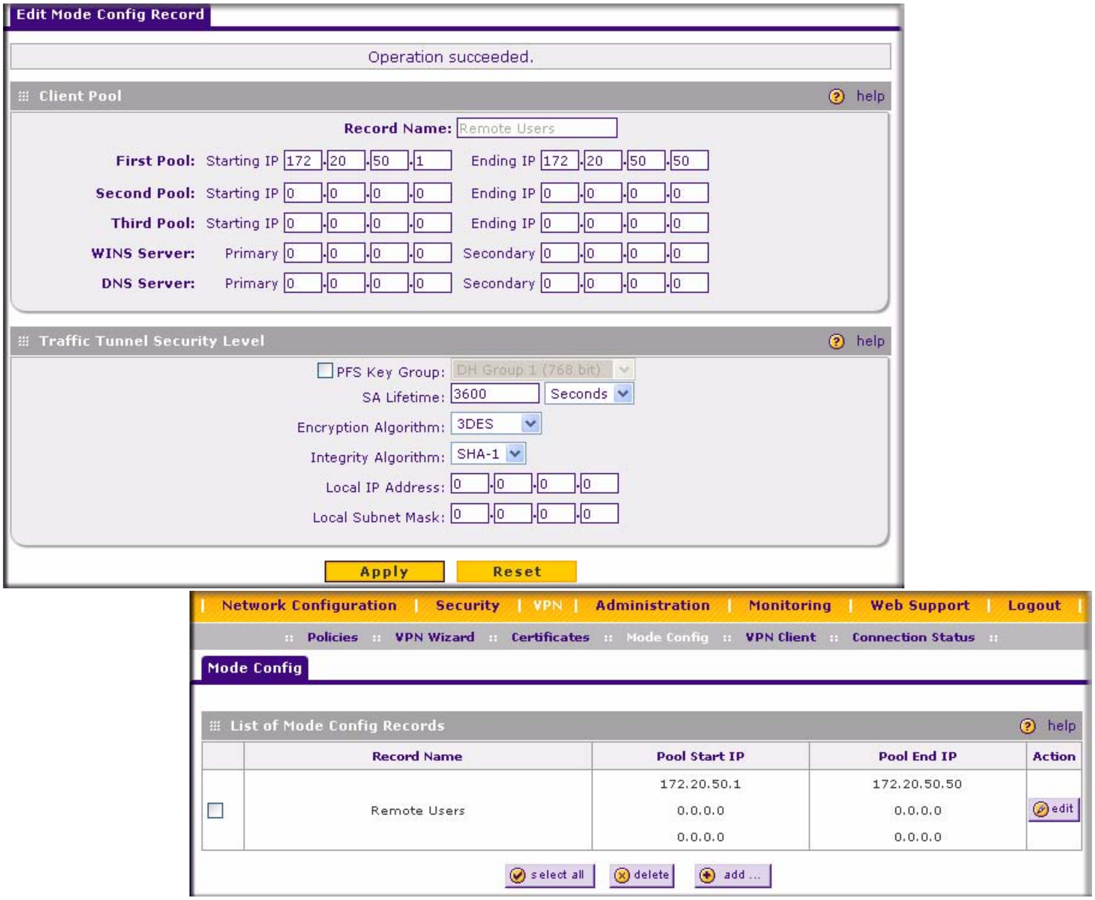
To configure the ModeConfig menu:

1. Select **VPN** from the main menu and **Mode Config** from the submenu. The **Mode Config** screen will display.
2. Click **Add.** The **Add Mode Config Record** screen will display.
3. Enter a descriptive **Record Name** such as “Remote Users”.
4. Assign at least one range of IP Pool addresses in the First IP Pool field to give to remote VPN clients.

   > **Note:** The IP Pool should not be within your local network IP addresses. Use a different range of private IP addresses such as 172.20.xx.xx.

5. If you have a WINS Server on your local network, enter its IP address.
6. Enter one or two DNS Server IP addresses to be used by remote VPN clients.
7. If you enable Perfect Forward Secrecy (PFS), select DH Group 1 or 2. This setting must match exactly the configuration of the remote VPN client,
8. Specify the Local IP Subnet to which the remote client will have access. Typically, this is your router’s LAN subnet, such as 192.168.2.1/255.255.255.0. (If not specified, it will default to the LAN subnet of the device.)

9. Specify the VPN policy settings. These settings must match the configuration of the remote VPN client. Recommended settings are:
   - SA Lifetime: 3600 seconds
   - Authentication Algorithm: SHA-1
   - Encryption Algorithm: 3DES
10. Click **Apply**. The new record should appear in the VPN Remote Host Mode Config Table (a sample record is shown below).



Edit Mode Config Record

Operation succeeded.

Client Pool

Record Name: Remote Users

First Pool:	Starting IP	172.20.50.1	Ending IP	172.20.50.50
Second Pool:	Starting IP	0.0.0.0	Ending IP	0.0.0.0
Third Pool:	Starting IP	0.0.0.0	Ending IP	0.0.0.0
WINS Server:	Primary	0.0.0.0	Secondary	0.0.0.0
DNS Server:	Primary	0.0.0.0	Secondary	0.0.0.0

Traffic Tunnel Security Level

□ PFS Key Group: DH Group 1 (768 bit)

SA Lifetime: 3600 Seconds

Encryption Algorithm: 3DES

Integrity Algorithm: SHA-1

Local IP Address: 0.0.0.0

Local Subnet Mask: 0.0.0.0

help
help
Apply
Reset
Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
Policies :: VPN Wizard :: Certificates :: Mode Config :: VPN Client :: Connection Status
Mode Config

List of Mode Config Records

	Record Name	Pool Start IP	Pool End IP	Action
□	Remote Users	172.20.50.1 0.0.0.0 0.0.0.0	172.20.50.50 0.0.0.0 0.0.0.0	edit

Figure 5-19

To configure an IKE Policy:

1. From the main menu, select **VPN**. The **IKE Policies** screen will display showing the current policies in the List of IKE Policies Table.

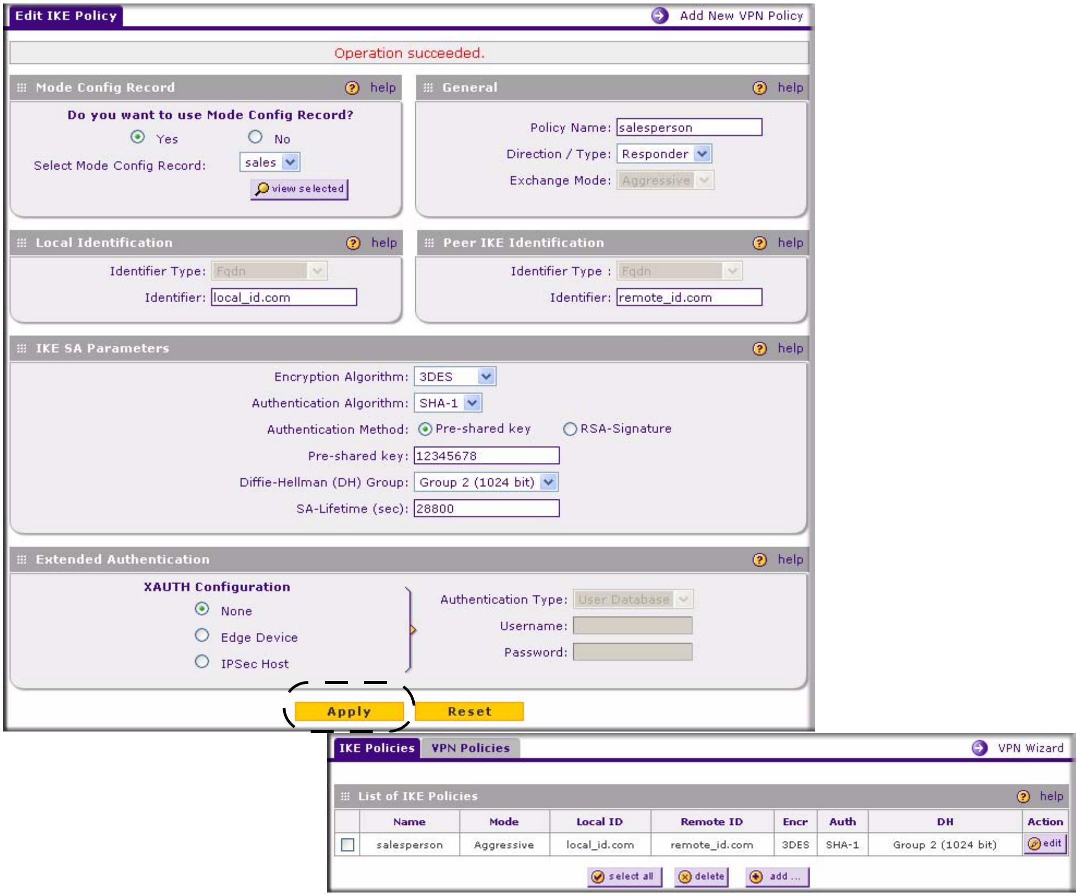
2. Click **Add** to configure a new IKE Policy. The **Add IKE Policy** screen will display.
3. Enable **Mode Config** by checking the **Yes** radio box and selecting the Mode Config record you just created from the pull-down menu. (You can view the parameters of the selected record by clicking the **View selected** radio box.)

   Mode Config works only in Aggressive Mode, and Aggressive Mode requires that both ends of the tunnel be defined by a FQDN.
4. In the **General** section:
   - **a.** Enter a description name in the Policy Name Field such as "salesperson". This name will be used as part of the remote identifier in the VPN client configuration.
   - **b.** Set Direction/Type to Responder.
   - **c.** By default, the Exchange Mode is set to Aggressive.
5. For Local information:
   - **d.** Select Fully Qualified Domain Name for the Local Identity Type.
   - **e.** Enter an identifier in the Remote Identity Data field that is not used by any other IKE policies. This identifier will be used as part of the local identifier in the VPN client configuration.
6. Specify the IKE SA parameters. These settings must be matched in the configuration of the remote VPN client. Recommended settings are:
   - Encryption Algorithm: 3DES
   - Authentication Algorithm: SHA-1
   - Diffie-Hellman: Group 2
   - SA Lifetime: 3600 seconds
7. Enter a Pre-Shared Key that will also be configured in the VPN client.
8. XAUTH is disabled by default. To enable XAUTH, select:
   - the **Edge Device** radio button to use this router as a VPN concentrator where one or more gateway tunnels terminate. (If selected, you must specify the **Authentication Type** to be used in verifying credentials of the remote VPN gateways.)
   - the **IPsec Host** radio button if you want this gateway to be authenticated by the remote gateway. Enter a Username and Password to be associated with the IKE policy. When this option is chosen, you will need to specify the user name and password to be used in authenticating this gateway (by the remote gateway).

9. If Edge Device was enabled, select the **Authentication Type** from the pull down menu which will be used to verify account information: User Database, RADIUS-CHAP or RADIUS-PAP. Users must be added thorough the User Database screen (see "User Database Configuration" on page 5-22 or "RADIUS Client Configuration" on page 5-23).

> **Note:** If RADIUS-PAP is selected, the router will first check the User Database to see if the user credentials are available. If the user account is not present, the router will then connect to the RADIUS server.

10. Click **Apply.** The new policy will appear in the IKE Policies Table (a sample policy is shown below)



Edit IKE Policy — Add New VPN Policy

Operation succeeded.

Mode Config Record — help

Do you want to use Mode Config Record? ● Yes ○ No

Select Mode Config Record: sales — view selected

General — help

Policy Name: salesperson

Direction / Type: Responder

Exchange Mode: Aggressive

Local Identification — help

Identifier Type: Fqdn

Identifier: local_id.com

Peer IKE Identification — help

Identifier Type : Fqdn

Identifier: remote_id.com

IKE SA Parameters — help

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

Authentication Method: ● Pre-shared key ○ RSA-Signature

Pre-shared key: 12345678

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

SA-Lifetime (sec): 28800

Extended Authentication — help

XAUTH Configuration

● None

○ Edge Device

○ IPSec Host

Authentication Type: User Database

Username:

Password:

Apply — Reset

IKE Policies — VPN Policies — VPN Wizard

List of IKE Policies — help

	Name	Mode	Local ID	Remote ID	Encr	Auth	DH	Action
□	salesperson	Aggressive	local_id.com	remote_id.com	3DES	SHA-1	Group 2 (1024 bit)	edit

select all — delete — add ...

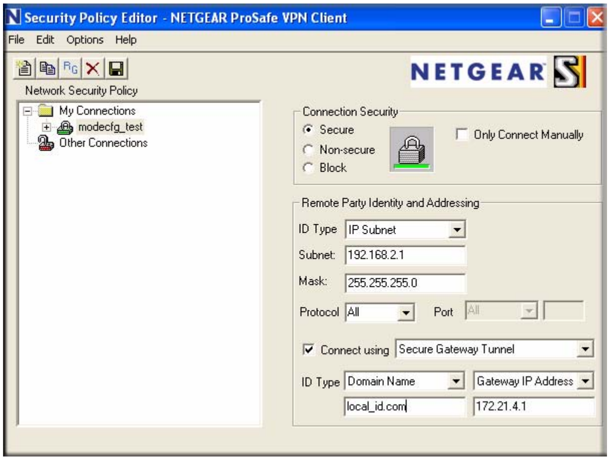
Figure 5-20

Configuring the ProSafe VPN Client for ModeConfig

From a client PC running NETGEAR ProSafe VPN Client software, configure the remote VPN client connection.

To configure the client PC:

1. Right-click the VPN client icon in the Windows toolbar. In the upper left of the Policy Editor window, click the New Policy editor icon.
   a. Give the connection a descriptive name such as “modecfg_test” (this name will only be used internally).
   b. From the ID Type pull-down menu, select IP Subnet.
   c. Enter the IP Subnet and Mask of the VPN firewall (this is the LAN network IP address of the gateway).
   d. Check the Connect using radio button and select Secure Gateway Tunnel from the pull-down menu.
   e. From the ID Type pull-down menu, select Domain name and enter the FQDN of the VPN firewall; in this example it is “local_id.com”.
   f. Select Gateway IP Address from the second pull-down menu and enter the WAN IP address of the VPN firewall; in this example it is “172.21.4.1”.



Network Security Policy
- My Connections
  - modecfg_test
- Other Connections

Connection Security
● Secure
○ Non-secure
○ Block
□ Only Connect Manually

Remote Party Identity and Addressing
ID Type: IP Subnet
Subnet: 192.168.2.1
Mask: 255.255.255.0
Protocol: All
Port: All
☑ Connect using: Secure Gateway Tunnel
ID Type: Domain Name | Gateway IP Address
local_id.com | 172.21.4.1

Figure 5-21

2. From the left side of the menu, click My Identity and enter the following information:
   a. Click **Pre-Shared Key** and enter the key you configured in the FVS338 IKE menu.

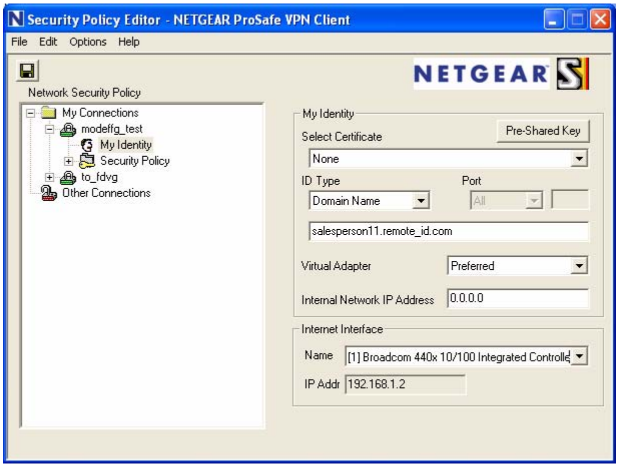
b. From the Select Certificate pull-down menu, select None.

c. From the ID Type pull-down menu, select Domain Name and create an identifier based on the name of the IKE policy you created; for example “salesperson11.remote_id.com”.

d. Under Virtual Adapter pull-down menu, select Preferred. The Internal Network IP Address should be 0.0.0.0.

> ➡ **Note:** If no box is displayed for Internal Network IP Address, go to Options/Global Policy Settings, and check the box for “Allow to Specify Internal Network Address.”

e. Select your Internet Interface adapter from the Name pull-down menu.



My Identity

Select Certificate: None

ID Type: Domain Name

Port: All

salesperson11.remote_id.com

Virtual Adapter: Preferred

Internal Network IP Address: 0.0.0.0

Internet Interface

Name: [1] Broadcom 440x 10/100 Integrated Controlle

IP Addr: 192.168.1.2

Figure 5-22

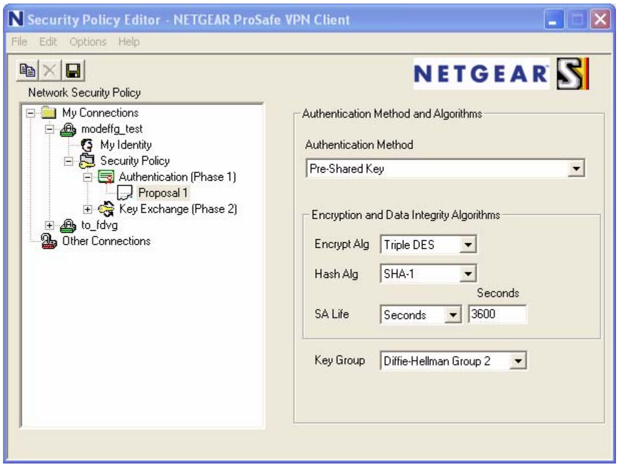
3. On the left-side of the menu, select Security Policy.

a. Under Security Policy, Phase 1 Negotiation Mode, check the Aggressive Mode radio button.

b. Check the Enable Perfect Forward Secrecy (PFS) radio button, and select the Diffie-Hellman Group 2 from the PFS Key Group pull-down menu.

c. Enable Replay Detection should be checked.

4. Click on Authentication (Phase 1) on the left-side of the menu and select Proposal 1. Enter the Authentication values to match those in the VPN firewall ModeConfig Record menu.



Authentication Method and Algorithms

Authentication Method: Pre-Shared Key

Encryption and Data Integrity Algorithms

Encrypt Alg: Triple DES

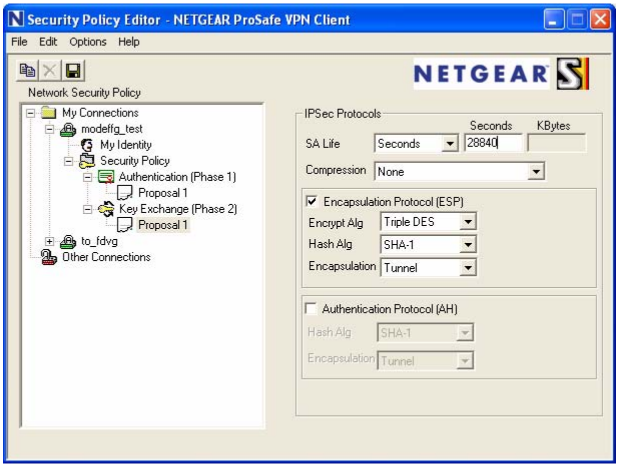
Hash Alg: SHA-1

SA Life: Seconds, 3600 Seconds

Key Group: Diffie-Hellman Group 2

Figure 5-23

5. Click on Key Exchange (Phase 2) on the left-side of the menu and select Proposal 1. Enter the values to match your configuration of the VPN firewall ModeConfig Record menu. (The SA Lifetime can be longer, such as 8 hours (28800 seconds)).



IPSec Protocols

SA Life: Seconds, 28840 Seconds, KBytes

Compression: None

☑ Encapsulation Protocol (ESP)

Encrypt Alg: Triple DES

Hash Alg: SHA-1

Encapsulation: Tunnel

☐ Authentication Protocol (AH)

Hash Alg: SHA-1

Encapsulation: Tunnel

Figure 5-24

6. Click the Save icon to save the Security Policy and close the VPN ProSafe VPN client.

To test the connection:

1. Right-click on the VPN client icon in the Windows toolbar and select Connect. The connection policy you configured will appear; in this case “My Connections\modecfg_test”.
2. Click on the connection. Within 30 seconds the message “Successfully connected to MyConnections/modecfg_test will display and the VPN client icon in the toolbar will read “On”.
3. From the client PC, ping a computer on the VPN firewall LAN.

Certificates

Digital Certificates (also known as X509 Certificates) are used to authenticate the identity of users and systems, and are issued by various CAs (Certification Authorities). Digital Certificates are used by this router during the IKE (Internet Key Exchange) authentication phase as an alternative authentication method. Trusted Certificates are issued to you by various CAs (Certification Authorities).

Trusted Certificates (CA Certificates)

Trusted Certificates are used to verify the validity of certificates issued to an organization and signed by the issuing CA authority. When a certificate is generated, it is signed by a publicly-known authority called the Certificate Authority.

The Trusted Certificates table shows the Trusted Certificates issued by the various CAs (Certification Authorities). For each Certificate, the following data is listed in the **Trusted Certificates** table:

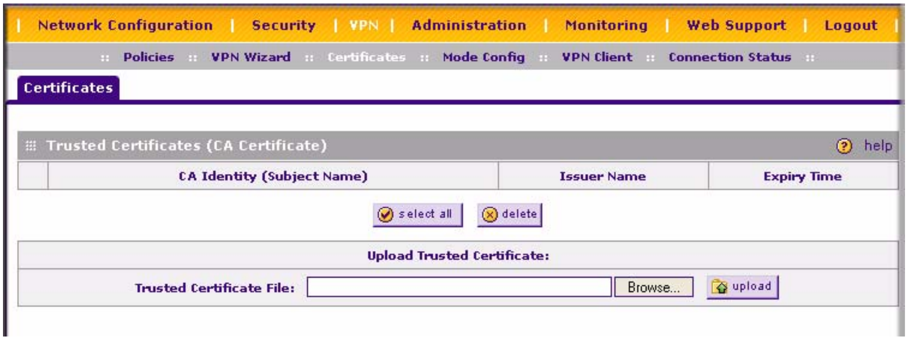
- **CA Identity (Subject Name)**. The organization or name to whom the certificate has been issued.
- **Issuer Name.** The name of the CA that issued the certificate.
- **Expiry Time.** The date when the certificate becomes invalid.

New certificates can be uploaded to the router when they are received.

To upload a Trusted Certificate:

1. Select **VPN** from the main menu and **Certificates** from the submenu. The **Certificates** screen will display.

2. Click **Browse** to locate the trusted certificate on your computer and then click **Upload**. The certificate will be stored on the router and will display in the **Trusted Certificates** table.



	CA Identity (Subject Name)	Issuer Name	Expiry Time

Figure 5-25

Self Certificates

Active Self certificates are certificates issued to you by the various Certificate Authorities (CAs) that are available for presentation to peer IKE servers. Each active self certificate is listed in the **Active Self Certificates** table. The data consists of:

- **Name.** A unique given by you to identify the certificate.
- **Subject Name**. The name which other organizations will see as the Holder (owner) of this Certificate. This should be your registered business name or official company name. Generally, all Certificates should have the same value in the Subject field.
- **Serial Number**. This is the serial number maintained by the CA. It is used to identify the certificate with in the CA.
- **Issuer Name.** The name of the CA which issued the Certificate.
- **Expiry Time**. The date on which the Certificate expires. You should renew the Certificate before it expires.

To use a Certificate, you must first generate and request the certificate from the CA from the computer or device that will be using the CA. The **Certificate Signing Request (CSR)** file must be filled out and submitted to the CA who will then generate a certificate for this device.

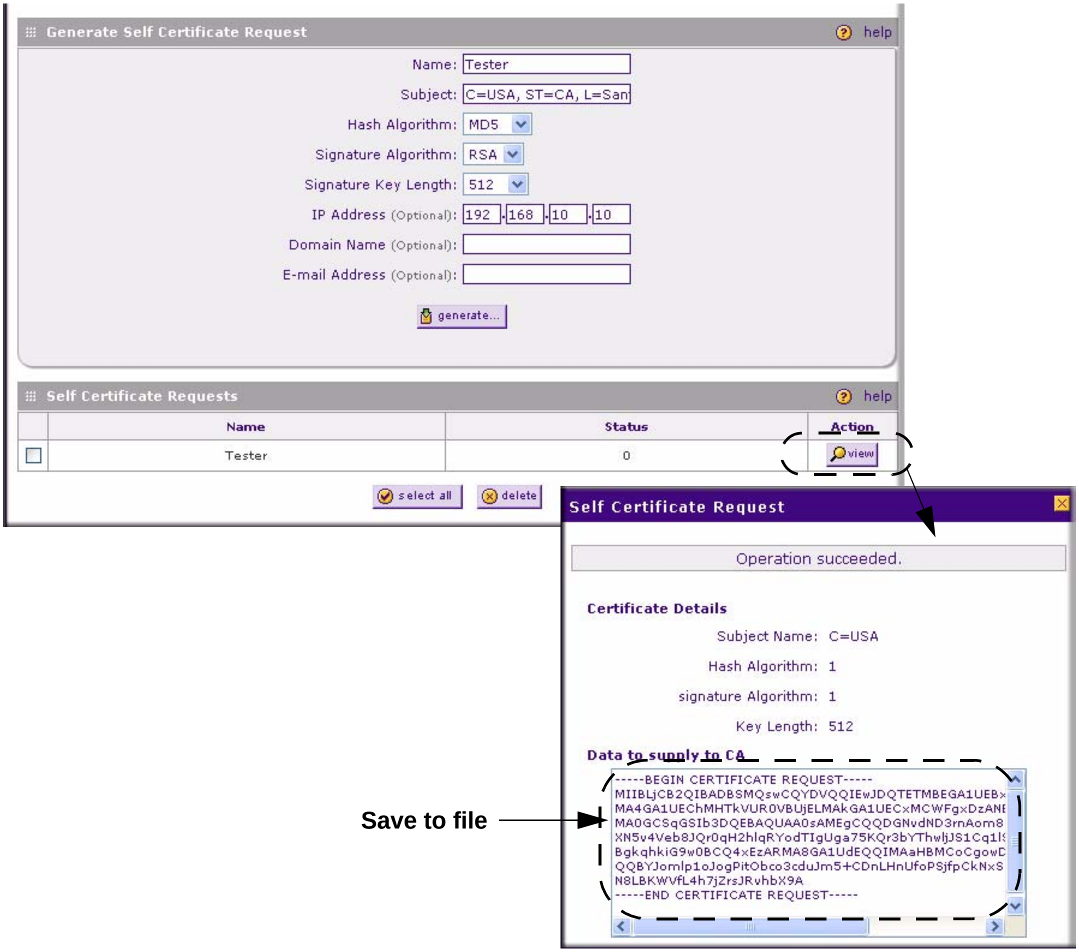
To request a Certificate from the CA:

1. From the main menu under **VPN**, select the **Certificates** submenu. The **Certificates** screen will display.
2. In the **Generate Self Certificate Request,** enter the required data:

- **Name** – Enter a name that will identify this Certificate.
- **Subject** – This is the name which other organizations will see as the Holder (owner) of the Certificate. Since this name will be seen by other organizations, you should use your registered business name or official company name.

  This information must be submitted in the following format: C=<*country*>, ST=<*state*>, L=<*city*>, O=<*organization*>, OU=<*department*>, CN=<*device name*>. In the following example: C=USA, ST=CA, L=Santa Clara, O=NETGEAR, OU=XX, CN=FVS338)
- From the pull-down menus, select the following values:
  - Hash Algorithm: MD5 or SHA2.
  - Signature Algorithm: RSA.
  - Signature Key Length: 512, 1024, 2048. (Larger key sizes may improve security, but may also impact performance.)

3. Complete the Optional fields, if desired, with the following information:
   - **IP Address** – If you have a fixed IP address, you may enter it here. Otherwise, you should leave this field blank.
   - **Domain Name** – If you have a Domain name, you can enter it here. Otherwise, you should leave this field blank.
   - **E-mail Address**– Enter your e-mail address in this field.
4. Click **Generate**. Your request will display in the **Self Certificate Requests** table.
5. View the request by clicking **View** in the Action column. The **Self Certificate Request** screen will display.
6. The Self Certificate Request data screen will display the data required for submission to the CA. Copy the data in the **Data to supply to CA** field data into a file, including all of the data contained in “----BEGIN CERTIFICATE REQUEST---” and “---END CERTIFICATE REQUEST---”
7. Following the instructions of the CA to complete the certificate request process.



Name:	Tester
Subject:	C=USA, ST=CA, L=San
Hash Algorithm:	MD5
Signature Algorithm:	RSA
Signature Key Length:	512
IP Address (Optional):	192 .168 .10 .10
Domain Name (Optional):	
E-mail Address (Optional):	

	Name	Status	Action
□	Tester	0	view

Operation succeeded.

Certificate Details

Subject Name:	C=USA
Hash Algorithm:	1
signature Algorithm:	1
Key Length:	512

Data to supply to CA

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBLjCB2QIBADBSMQswCQYDVQQIEwJDQTETMBEGA1UEBx
MA4GA1UEChMHTkVUR0VBUjELMAkGA1UECxMCWFgxDzANE
MA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDGNvdND3rnAom8
XN5v4Veb8JQr0qH2hlqRYodTIgUga75KQr3bYThwljJS1Cq1l
BgkqhkiG9w0BCQ4xEzARMA8GA1UdEQQIMAaHBMCoCgowD
QQBYJomlp1oJogPitObco3cduJm5+CDnLHnUfoPSjfpCkNxS
N8LBKWVfL4h7jZrsJRvhbX9A
-----END CERTIFICATE REQUEST-----
```

Figure 5-26

To submit your Self Certificate request to a CA:

1. Connect to the web site of the CA.
2. Start the Self Certificate request procedure.
3. When prompted for the requested data, copy the data from your saved data file (including “----BEGIN CERTIFICATE REQUEST---” and “---END CERTIFICATE REQUEST’).
4. Submit the CA form. If no problems ensue, the Certificate will be issued.

When you obtain the certificate from the CA, you can then upload it to your computer. Click **Browse** to locate the **Certificate file** and then click **Upload.** The certificate will display in the **Active Self Certificates** table (see Figure 5-25).

Certificates are updated by their issuing CA authority on a regular basis. You should track all of your CAs to ensure that you have the latest version and/or that your certificate has not been revoked. To track your CAs, you must upload the Certificate Identify for each CA to the CRL.

Managing your Certificate Revocation List (CRL)

CRL (Certificate Revocation List) files show Certificates which are active and certificates which have been revoked, and are no longer valid. Each CA issues their own CRLs.

It is important that you keep your CRLs up-to-date. You should obtain the CRL for each CA regularly.

The CRL table lists your active CAs and their critical release dates:

- **CA Identity** – The official name of the CA which issued this CRL.
- **Last Update** – The date when this CRL was released.
- **Next Update** – The date when the next CRL will be released.

To upload a Certificate Identity to the CRL:

1. Click **Browse**, and then locate the file you previously downloaded from a CA.
2. Select the Certificate Identity file. The name will appear in the “File to upload” field. Click **Upload.** The new Certificate Identity will appear in the **Certification Revocation Lists** table. If you have a previous CA Identity from the same CA, it should now be deleted.

.

Chapter 6
Router and Network Management

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

The 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 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 VPN firewall has the necessary features and tools to help the network manager accomplish these goals.

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

You can control specific outbound traffic (for example., from LAN 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.

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

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 "Managing Groups and Hosts" on page 3-5).
- **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-Based Rules" on page 4-2).
- **Schedule** – You can specify whether the rule is to be applied on the Schedule 1, Schedule 2, or Schedule 3 time schedule (see "Setting a Schedule to Block or Allow Traffic" on page 4-20).

See “Using Rules to Block or Allow Specific Kinds of Traffic” on page 4-1 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 4-2 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 3-5for 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 “Setting a Schedule to Block or Allow Traffic” on page 4-20 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 Web site name (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 "Setting Block Sites (Content Filtering)" on page 4-21 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 "Enabling Source MAC Filtering" on page 4-23 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
- DMZ port
- 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.

⚠	**Warning:** 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 "Adding Customized Services" on page 4-17).
- **Schedule** – You can specify whether the rule is to be applied on the Schedule 1, Schedule 2, or Schedule 3 time schedule (see "Setting a Schedule to Block or Allow Traffic" on page 4-20).

See "Using Rules to Block or Allow Specific Kinds of Traffic" on page 4-1 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 "Setting Up Port Triggering" on page 4-24 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 5, "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 "Specifying Quality of Service (QoS) Priorities" on page 4-19 for the procedure on how to use this feature.

Tools for Traffic Management

The 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 "Viewing Router Configuration and System Status" on page 6-22 for a discussion of the tools.

Administration

You can change the administrator and guest passwords and settings, configure an SNMP manager, backup settings and upgrade firmware, and enable remote management. Administrator access is read/write and guest access is read-only.

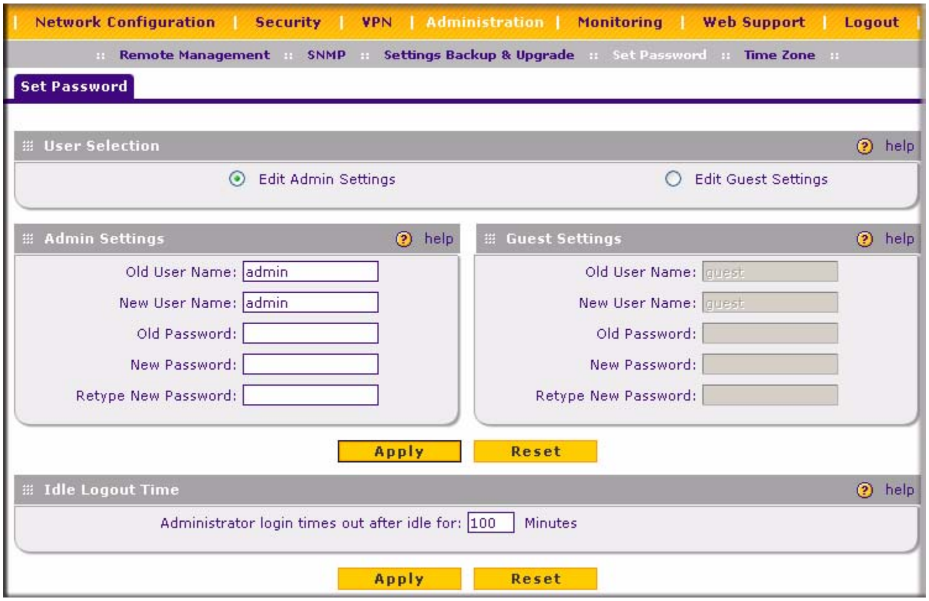
Changing Passwords and Settings

The default passwords for the firewall's Web Configuration Manager is **password**. Netgear recommends that you change this password to a more secure password. You can also configure a separate password for guests.

To modify User or Admin settings:

1. Select **Administration** from the main menu and **Set Password** from the submenu. The **Set Password** screen will display.
2. Select the Settings you wish to edit by checking either the **Edit Admin Settings** or **Edit Guest Settings** radio box.
3. Change the password by first entering the old password, and then entering the new password twice.
4. Click **Apply** to save your settings or **Cancel** to return to your previous settings.
5. Change the **Idle Logout Time** field to the number of minutes you require. The default is 5 minutes.
6. Click **Apply** to save this setting.

➡	**Note:** If you make the administrator login time-out 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).



User Selection

● Edit Admin Settings ○ Edit Guest Settings

Admin Settings

Old User Name:	admin
New User Name:	admin
Old Password:	
New Password:	
Retype New Password:	

Guest Settings

Old User Name:	guest
New User Name:	guest
Old Password:	
New Password:	
Retype New Password:	

Idle Logout Time

Administrator login times out after idle for: 100 Minutes

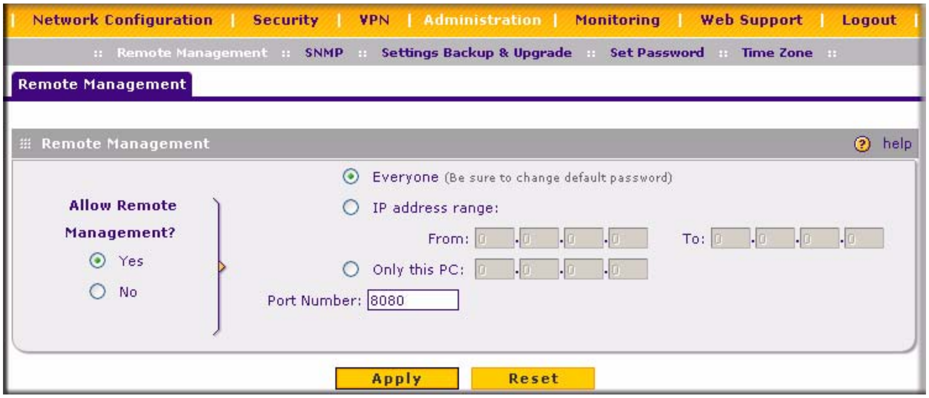
Figure 6-1

Note: The password and time-out 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 VPN firewall. You must be logged in locally to enable remote management (see "Logging in to the VPN Firewall" on page 2-1).

Note: Be sure to change the firewall 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 Passwords and Settings" on page 6-7 for the procedure on how to do this.


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Set Password :: Time Zone ::
Remote Management
help
Apply
Reset

Remote Management

Allow Remote Management?
● Yes
○ No

● Everyone (Be sure to change default password)
○ IP address range:
From: 0.0.0.0 To: 0.0.0.0
○ Only this PC: 0.0.0.0
Port Number: 8080

Figure 6-2

To configure your firewall for Remote Management:

1. Select the Turn Remote Management On check box.

a. 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.

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

c. 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.

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

2. 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.

3. Click **Apply** to have your changes take effect.

When accessing your firewall from the Internet, the Secure Sockets Layer (SSL) will be enabled. You will enter *https://* and type the WAN IP address of your firewall 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, enter the following in your browser:

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

The remote URL login of the router 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.

Note: 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 Run menu. For example, renter `tracert yourFVS338.mynetgear.net` and you will see the IP address your ISP assigned to the FVS338.

Using a SNMP Manager

Simple Network Management Protocol (SNMP) lets you monitor and manage your router from an SNMP Manager. It provides a remote means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

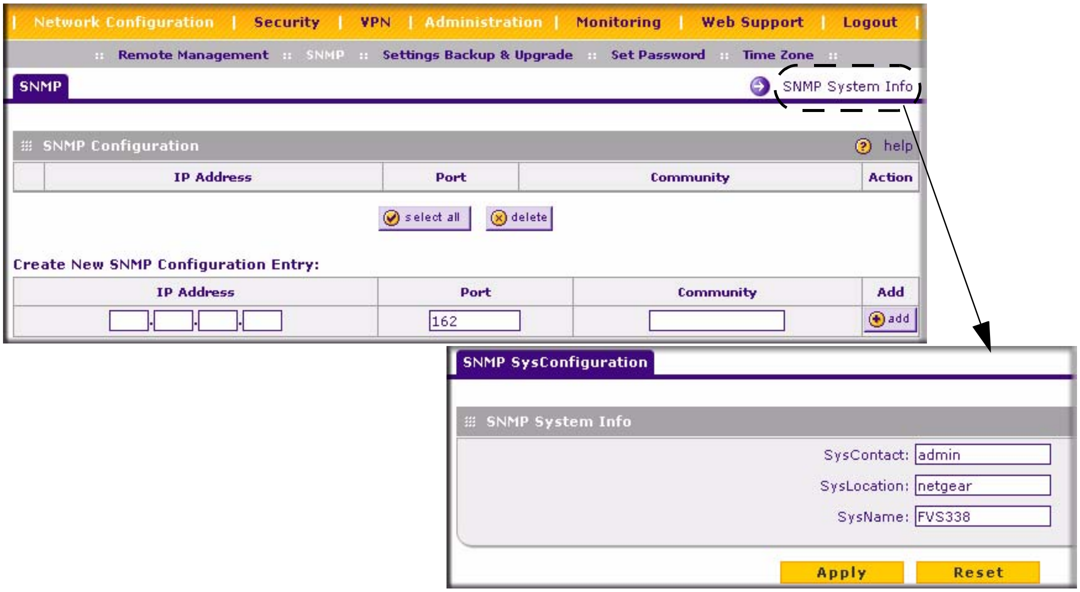
The SNMP Configuration table lists the SNMP configurations by:

- **IP Address**: The IP address of the SNMP manager.
- **Port**: The trap port of the configuration.
- **Community**: The trap community string of the configuration.

To create a new SNMP configuration entry:

1. Select **Administration** from the main menu and **SNMP** from the submenu. The **SNMP** screen will display.
2. Under **Create New SNMP Configuration Entry,** enter the IP Address of the SNMP manager in the **IP Address** field and the Subnet Mask in the **Subnet Mask** field.
   - If you want to allow only the host address to access the VPN firewall and receive traps (for example, see Figure 6-3), enter an IP Address of, for example, 192.168.1.100 with a Subnet Mask of 255.255.255.**255**.
   - If you want to allow a subnet access to the VPN firewall through SNMP, enter an IP address of, for example,192.168.1.100 with a Subnet Mask of 255.255.255.**0**. The traps will still be received on 192.168.1.100, but the entire subnet will have access through the community string.
   - If you want to make the VPN firewall globally accessible using the community string, but still receive traps on the host, enter 0.0.0.0 as the Subnet Mask and an IP Address for where the traps will be received.
3. Enter the trap port number of the configuration in the **Port** field. The default is 162.
4. Enter the trap community string of the configuration in the **Community** field.
5. Click **Add** to create the new configuration. The entry will display in the **SNMP Configuration** table.

6. Click **Edit** in the **Action** column adjacent to the entry to modify or change the selected configuration.


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
Remote Management :: SNMP :: Settings Backup & Upgrade :: Set Password :: Time Zone
SNMP
SNMP System Info
SNMP Configuration
help
select all
delete
Create New SNMP Configuration Entry:
add
SNMP SysConfiguration
SNMP System Info
Apply
Reset

	IP Address	Port	Community	Action

IP Address	Port	Community	Add
. . .	162		add

SysContact: admin

SysLocation: netgear

SysName: FVS338

Figure 6-3

The **SNMP System Info** link displays the VPN firewall identification information available to the SNMP Manager. System Contact, System Location, and System name.

To modify the SNMP System contact information:

1. Click the **SNMP System Info** link. The **SNMP SysConfiguration** screen will display.
2. Modify any of the contact information that you want the SNMP Manager to use.
3. Click **Apply** to save your settings.

Settings Backup and Firmware Upgrade

Once you have installed the VPN firewall and have it working properly, you should back up a copy of your setting so that it is if something goes wrong. When you backup the settings, they are saved as a file on your computer. You can then restore the VPN firewall settings from this file. The **Settings Backup & Upgrade** screen allows you to:

- Back up and save a copy of your current settings
- Restore saved settings from the backed-up file.

- Revert to the factory default settings.
- Upgrade the VPN firewall firmware from a saved file on your hard disk to use a different firmware version.

Backup and Restore Settings

To backup and restore settings:

1. Select **Administration** from the main menu and **Settings Backup & Upgrade** from the submenu. THe **Settings Backup and Firmware Upgrade** screen will display.
2. Click **backup** to save a copy of your current settings.

   If your browser isn’t set up to save downloaded files automatically, locate where you want to save the file, specify file name, and click Save. If you have your browser set up to save downloaded files automatically, the file will be saved to your browser's download location on the hard disk.

⚠	**Warning:** Once you start restoring settings or erasing the router, do NOT interrupt the process. Do not try to go online, turn off the router, shutdown the computer or do anything else to the router until it finishes restarting!

To restore settings from a backup file:

1. Click **Browse**. Locate and select the previously saved backup file (by default, netgear.cfg).
2. When you have located the file, click **restore**.

   An Alert page will appear indicating the status of the restore operation. You must manually restart the VPN firewall for the restored settings to take effect.

To reset the router to the original factory default settings, click **default**

You must manually restart the VPN firewall in order for the default settings to take effect. After rebooting, the router's password will be **password** and the LAN IP address will be **192.168.1.1.** The VPN firewall will act as a DHCP server on the LAN and act as a DHCP client to the Internet.

⚠	**Warning:** When you click **default,** your router settings will be erased. All firewall rules, VPN policies, LAN/WAN settings and other settings will be lost. Please backup your settings if you intend on using them!

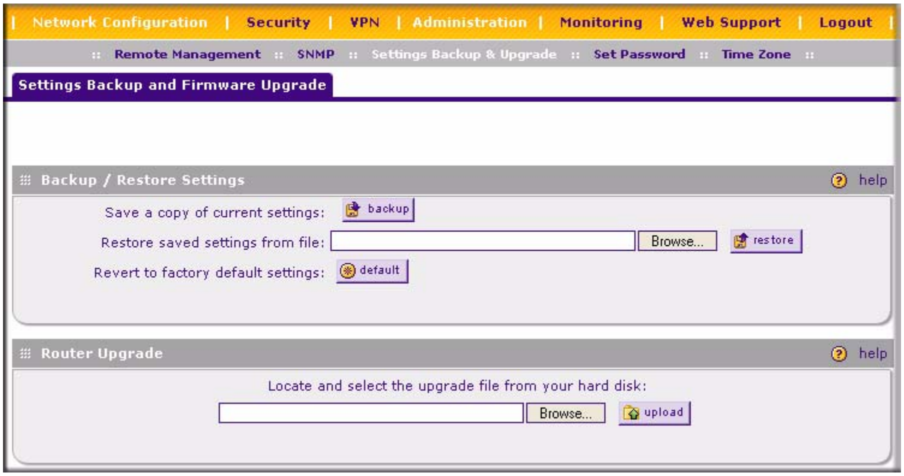

| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Set Password :: Time Zone ::
Settings Backup and Firmware Upgrade
Backup / Restore Settings
help
Save a copy of current settings:
backup
Restore saved settings from file:
Browse...
restore
Revert to factory default settings:
default
Router Upgrade
help
Locate and select the upgrade file from your hard disk:
Browse...
upload

Figure 6-4

Router Upgrade

You can install a different version of the VPN firewall firmware from the **Settings Backup & Upgrade** screen. To view the current version of the firmware that your VPN firewall is running, select **Monitoring** from the main menu. The **Router Status** screen on the will display all of the VPN firewall router statistics. When you upgrade your firmware, the Firmware Version will change to reflect the new version.

To download a firmware version:

1. Go to the NETGEAR Web site at *http://www.netgear.com/support* and click on **Downloads.**
2. From the **Product Selection** pull-down menu, select your product. Select the software version and follow the **To Install** steps to download your software.

   After downloading an upgrade file, you may need to unzip (uncompress) it before upgrading the router. If Release Notes are included in the download, read them before continuing.

⚠ **Warning:** Once you click **Upload** do NOT interrupt the router!

To upgrade router software:

1. Select **Administration** from the main menu and **Settings Backup & Upgrade** from the submenu. The **Settings Backup and Firmware Upgrade** screen will display.

2. Click **Browse** in the **Router Upgrade** section.
3. Locate the downloaded file and click **upload.** This will start the software upgrade to your VPN firewall router. This may take some time. At the conclusion of the upgrade, your router will reboot.

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

4. After the VPN firewall has rebooted, select **Monitoring** and confirm the new firmware version to verify that your router now has the new software installed.

> **Note:** In some cases, such as a major upgrade, it may be necessary to erase the configuration and manually reconfigure your router after upgrading it. Refer to the Release Notes included with the software to find out if this is required.

Setting the Time Zone

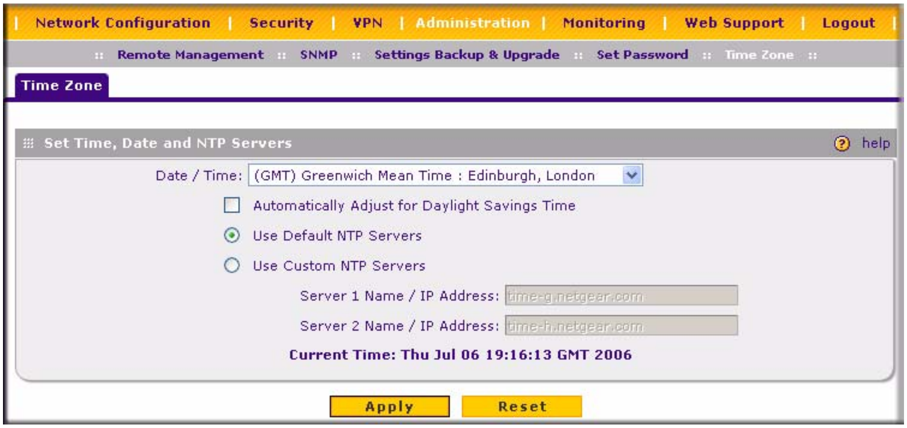
Date, time and NTP Server designations can be input on the **Time Zone** screen. Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock times in a network of computers.

To set Time, Date and NTP servers:

1. Select **Administration** from the main menu and **Time Zone** from the submenu. The **Time Zone** screen will display.
2. From the **Date/Time** pull-down menu, select the Local Time Zone. This is required in order for scheduling to work correctly. The VPN firewall includes a Real-Time Clock (RTC), which it uses for scheduling.
3. If supported in your region, check the **Automatically Adjust for Daylight Savings Time** radio box.
4. Select a NTP Server option by checking one of the following radio boxes:
   - **Use Default NTP Servers**: If this is enabled, then the RTC (Real-Time 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 instead 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 the Server 1 or Server 2 fields empty, they will be set to the Default Netgear NTP servers.

5. Click **Apply** to save your settings or click **Cancel** to revert to your previous settings.


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Remote Management :: SNMP :: Settings Backup & Upgrade :: Set Password :: Time Zone ::
Time Zone
Set Time, Date and NTP Servers
help
Apply
Reset

Date / Time: (GMT) Greenwich Mean Time : Edinburgh, London

□ Automatically Adjust for Daylight Savings Time

● Use Default NTP Servers

○ Use Custom NTP Servers

Server 1 Name / IP Address: time-g.netgear.com

Server 2 Name / IP Address: time-h.netgear.com

Current Time: Thu Jul 06 19:16:13 GMT 2006

Figure 6-5

Monitoring the Router

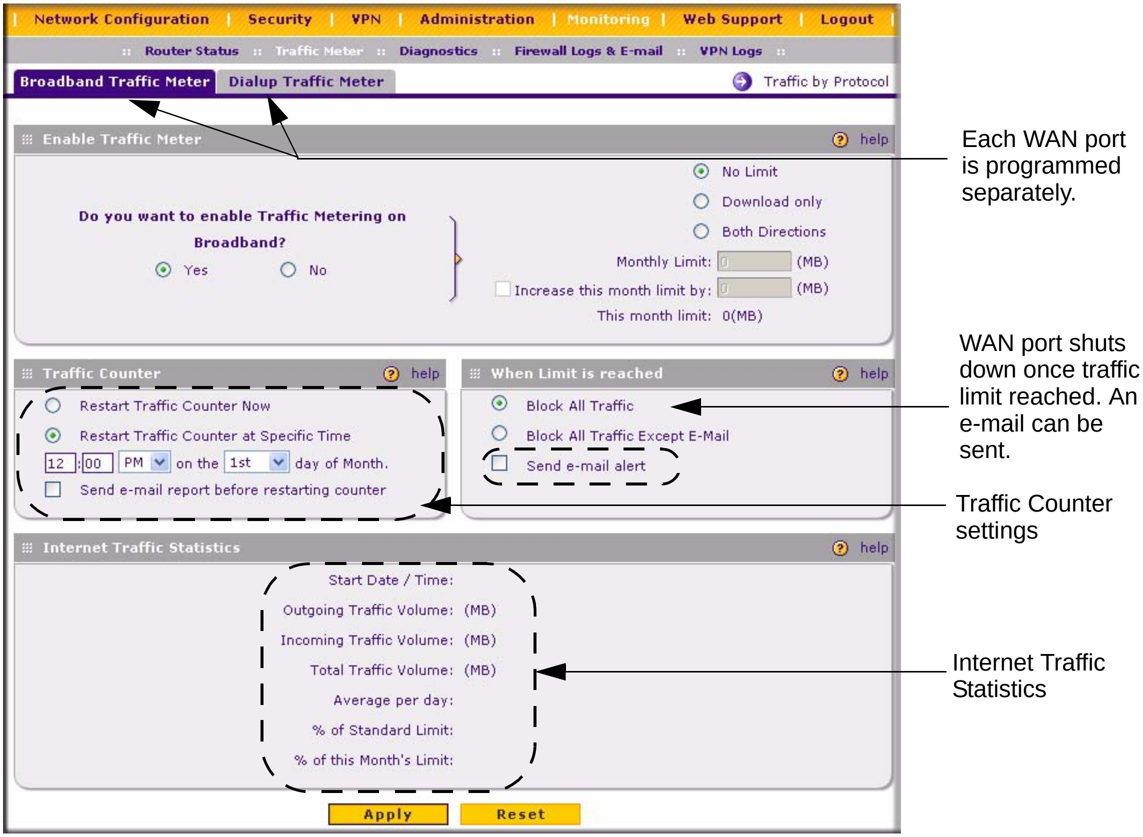
You can be alerted to important events such as WAN port rollover, WAN traffic limits reached, and login failures and attacks. You can also view status information about the firewall, WAN ports, LAN ports, and VPN tunnels.

Enabling the Traffic Meter

To monitor traffic limits on each of the WAN ports, select **Administration** from the main menu and **Traffic Meter** from the submenu. The **Broadband Traffic Meter** screen will display. (The Broadband and Dialup ports are programmed separately.) A WAN port shuts down once its traffic limit is reached if the **Block all traffic** feature is enabled.

The Traffic Meter screen also provides the following information:

- **Internet Traffic Statistics** – Displays statistics on Internet Traffic via the WAN port. If you have not enabled the Traffic Meter, these statistics are not available.



| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Broadband Traffic Meter
Dialup Traffic Meter
Traffic by Protocol
help
Apply
Reset

Enable Traffic Meter

Do you want to enable Traffic Metering on Broadband?

● Yes ○ No

● No Limit

○ Download only

○ Both Directions

Monthly Limit: 0 (MB)

□ Increase this month limit by: 0 (MB)

This month limit: 0(MB)

Traffic Counter

○ Restart Traffic Counter Now

● Restart Traffic Counter at Specific Time

12 : 00 PM on the 1st day of Month.

□ Send e-mail report before restarting counter

When Limit is reached

● Block All Traffic

○ Block All Traffic Except E-Mail

□ Send e-mail alert

Internet Traffic Statistics

Start Date / Time:

Outgoing Traffic Volume: (MB)

Incoming Traffic Volume: (MB)

Total Traffic Volume: (MB)

Average per day:

% of Standard Limit:

% of this Month's Limit:

Each WAN port is programmed separately.

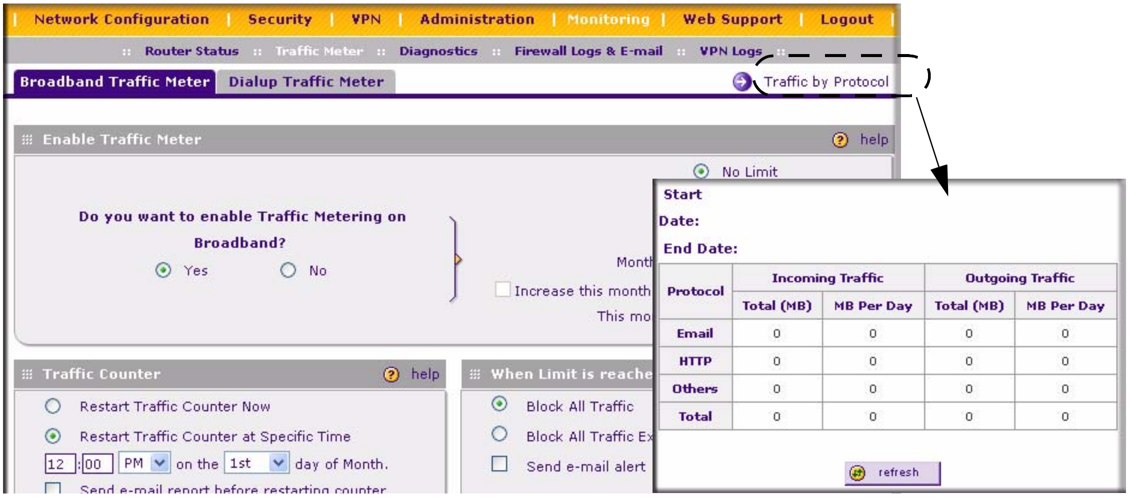
WAN port shuts down once traffic limit reached. An e-mail can be sent.

Traffic Counter settings

Internet Traffic Statistics

Figure 6-6

- **Traffic by Protocol** – Click this button to display Internet Traffic details. 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



Do you want to enable Traffic Metering on Broadband?

● Yes ○ No

● No Limit

Month

□ Increase this month

This mo

○ Restart Traffic Counter Now

● Restart Traffic Counter at Specific Time

12 :00 PM on the 1st day of Month.

□ Send e-mail report before restarting counter

● Block All Traffic

○ Block All Traffic Ex

□ Send e-mail alert

Start Date:

End Date:

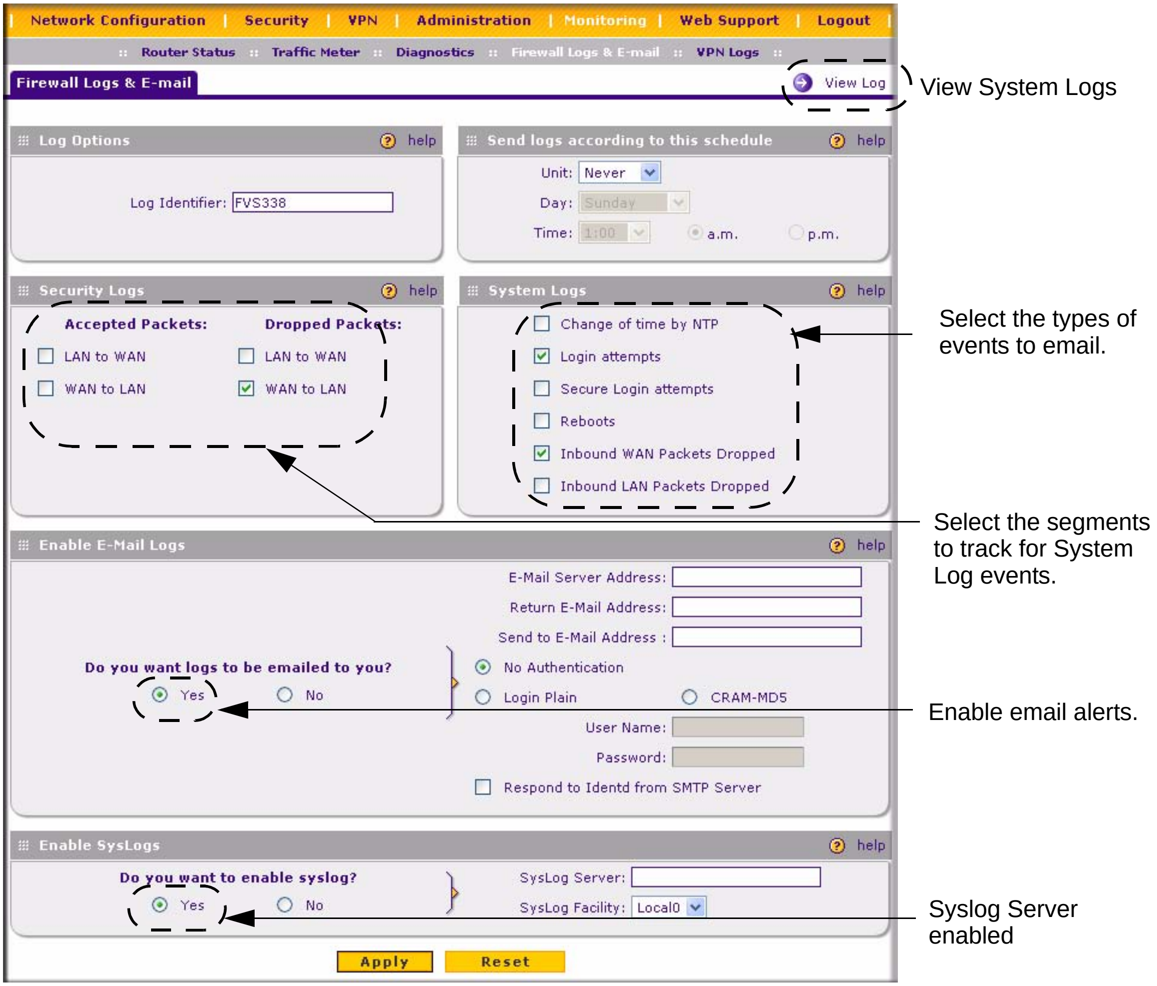
Protocol	Incoming Traffic		Outgoing Traffic	
	Total (MB)	MB Per Day	Total (MB)	MB Per Day
Email	0	0	0	0
HTTP	0	0	0	0
Others	0	0	0	0
Total	0	0	0	0

Figure 6-7

Setting Login Failures and Attacks Notification

Figure 6-8 shows the **Firewall Logs & E-mail** screen that is invoked by selecting **Monitoring** from the main menu and selecting **Firewall Logs & E-mail** from the submenu.

You can send a System log of firewall activities to an email address or a log of the firewall activities can be viewed, saved to a syslog server, and then sent to an email address. You can view the logs by clicking **View Logs.**



Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
:: Router Status :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
View Log
help
Apply
Reset

Firewall Logs & E-mail

Log Options

Log Identifier: FVS338

Send logs according to this schedule

Unit: Never

Day: Sunday

Time: 1:00 ● a.m. ○ p.m.

Security Logs

Accepted Packets:	Dropped Packets:
□ LAN to WAN	□ LAN to WAN
□ WAN to LAN	☑ WAN to LAN

System Logs

- □ Change of time by NTP
- ☑ Login attempts
- □ Secure Login attempts
- □ Reboots
- ☑ Inbound WAN Packets Dropped
- □ Inbound LAN Packets Dropped

Enable E-Mail Logs

E-Mail Server Address:

Return E-Mail Address:

Send to E-Mail Address :

Do you want logs to be emailed to you? ● Yes ○ No

● No Authentication

○ Login Plain ○ CRAM-MD5

User Name:

Password:

□ Respond to Identd from SMTP Server

Enable SysLogs

Do you want to enable syslog? ● Yes ○ No

SysLog Server:

SysLog Facility: Local0

View System Logs

Select the types of events to email.

Select the segments to track for System Log events.

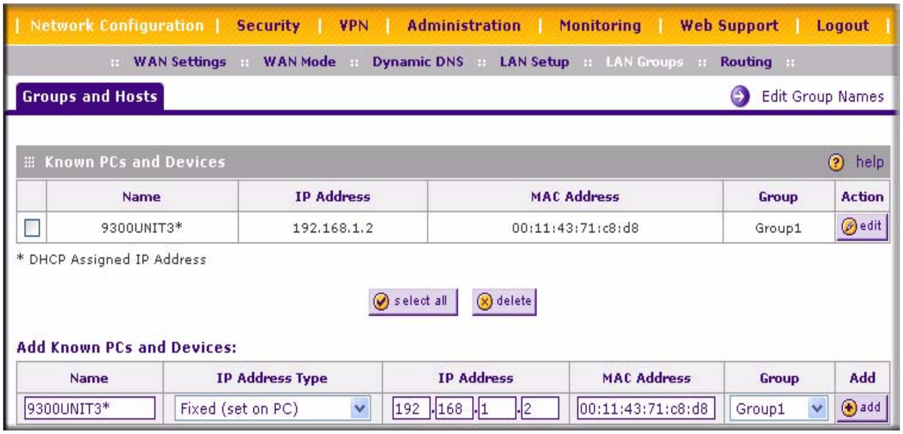
Enable email alerts.

Syslog Server enabled

Figure 6-8

Monitoring Attached Devices

The **Groups and Hosts** menu contains a table of all IP devices that the VPN firewall has discovered on the local network. Select **Network Configuration** from the main menu and **LAN Groups** from the submenu. The **Groups and Hosts** screen will display.


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: WAN Mode :: Dynamic DNS :: LAN Setup :: LAN Groups :: Routing ::
Groups and Hosts
Edit Group Names
Known PCs and Devices
help
select all
delete
edit
add

	Name	IP Address	MAC Address	Group	Action
□	9300UNIT3*	192.168.1.2	00:11:43:71:c8:d8	Group1	edit

* DHCP Assigned IP Address

Add Known PCs and Devices:

Name	IP Address Type	IP Address	MAC Address	Group	Add
9300UNIT3*	Fixed (set on PC)	192.168.1.2	00:11:43:71:c8:d8	Group1	add

Figure 6-9

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 enabled (on the LAN Setup screen) 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.

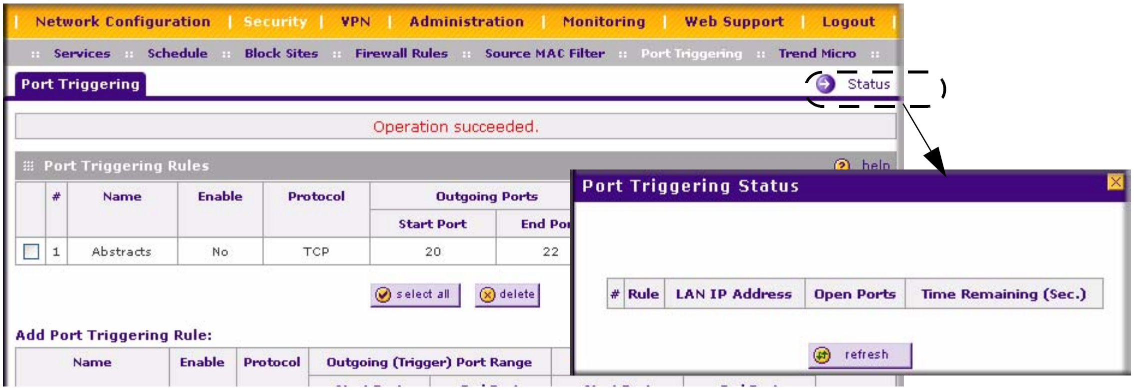
Table 6-1. Known PCs and Devices

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 Group1.

Note: If the VPN firewall is rebooted, the table data is lost until the VPN firewall rediscovers the devices.

Viewing Port Triggering Status

You can view the status of Port Triggering by selecting **Security** from the main menu and **Port Triggering** from the submenu. When the **Port Triggering** screen display, click the **Status** link.


| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Services :: Schedule :: Block Sites :: Firewall Rules :: Source MAC Filter :: Port Triggering :: Trend Micro ::
Port Triggering
Status
help
select all
delete
refresh

Operation succeeded.

Port Triggering Rules

	#	Name	Enable	Protocol	Outgoing Ports	
					Start Port	End Por
□	1	Abstracts	No	TCP	20	22

Add Port Triggering Rule:

Name	Enable	Protocol	Outgoing (Trigger) Port Range

Port Triggering Status

#	Rule	LAN IP Address	Open Ports	Time Remaining (Sec.)

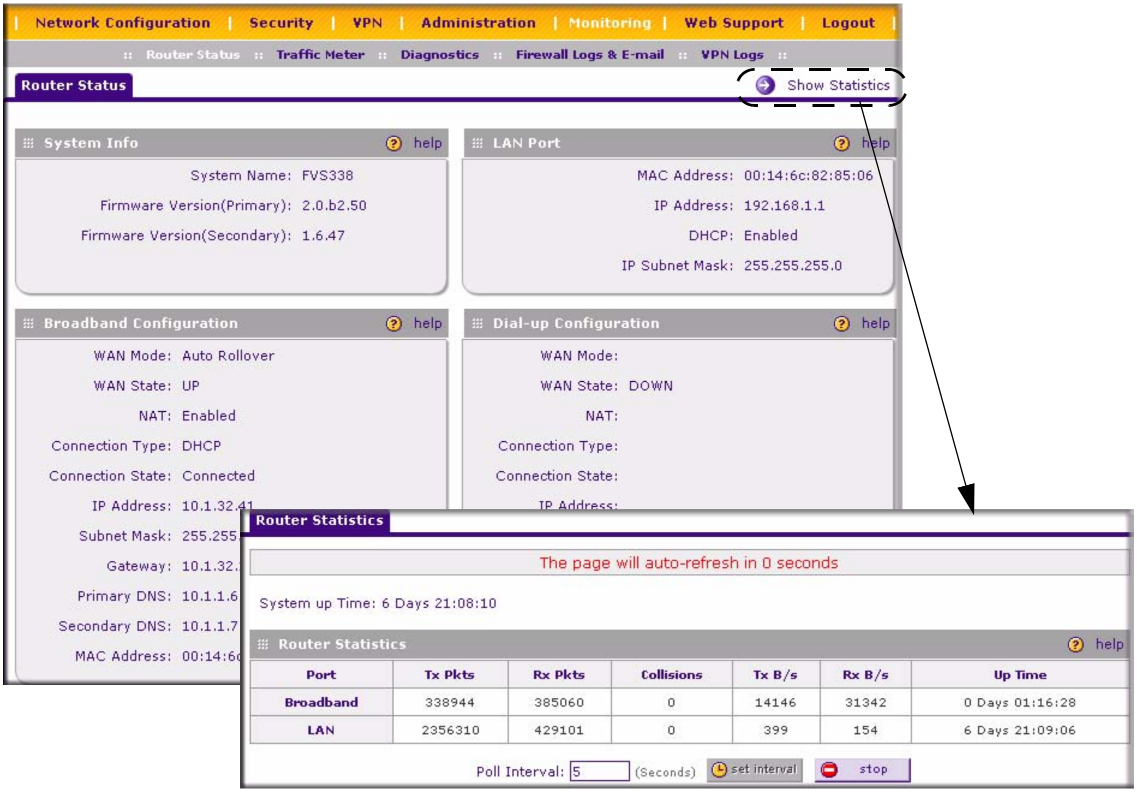
Figure 6-10

Table 6-2. 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.

Viewing Router Configuration and System 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**, The **Router Status** screen will display.



System Name: FVS338
Firmware Version(Primary): 2.0.b2.50
Firmware Version(Secondary): 1.6.47

MAC Address: 00:14:6c:82:85:06
IP Address: 192.168.1.1
DHCP: Enabled
IP Subnet Mask: 255.255.255.0

WAN Mode: Auto Rollover
WAN State: UP
NAT: Enabled
Connection Type: DHCP
Connection State: Connected
IP Address: 10.1.32.41
Subnet Mask: 255.255
Gateway: 10.1.32.
Primary DNS: 10.1.1.6
Secondary DNS: 10.1.1.7
MAC Address: 00:14:6

WAN Mode:
WAN State: DOWN
NAT:
Connection Type:
Connection State:
IP Address:

The page will auto-refresh in 0 seconds

System up Time: 6 Days 21:08:10

Port	Tx Pkts	Rx Pkts	Collisions	Tx B/s	Rx B/s	Up Time
Broadband	338944	385060	0	14146	31342	0 Days 01:16:28
LAN	2356310	429101	0	399	154	6 Days 21:09:06

Poll Interval: 5 (Seconds)

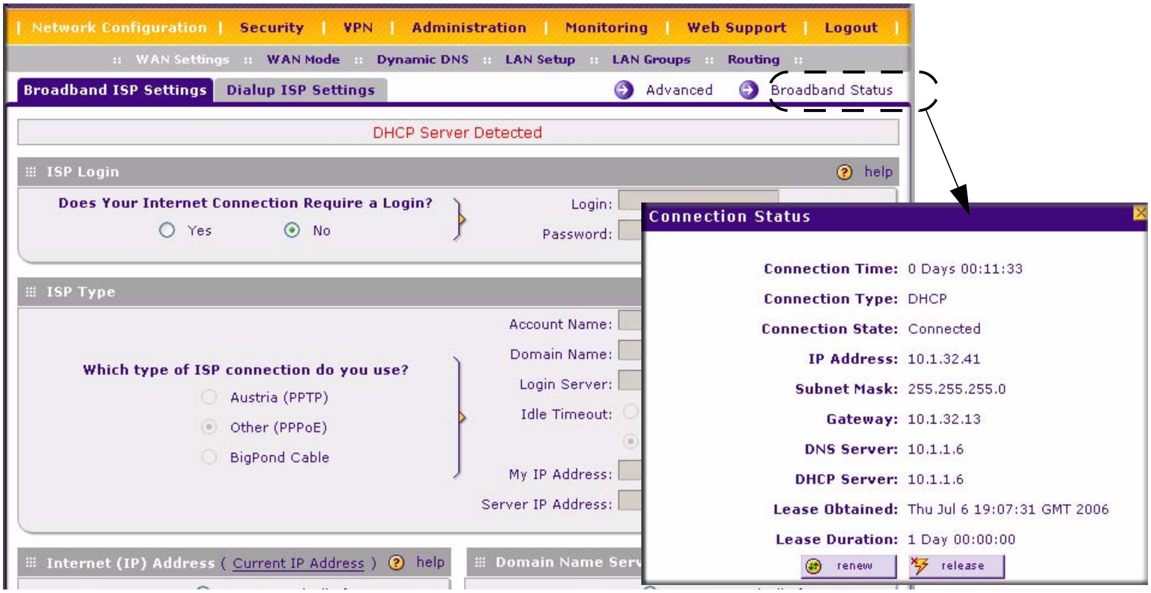
Figure 6-11

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	Displays the current settings for MAC address, IP address, DHCP role and IP Subnet Mask that you set in the LAN IP Setup page. DHCP can be either Server or None.
Broadband Configuration	Indicates whether the WAN Mode is Single or Rollover, and whether the WAN State is UP or DOWN. If the WAN State is up, it also displays • NAT: Enabled or Disabled. • Connection Type: DHCP enabled or disabled. • Connection State: Connected or Disconnected • WAN IP Address • Subnet Mask • Gateway Address • Primary and Secondary DNS Server Addresses • MAC Address.
Dialup Configuration	Displays the same details as for WAN1 Configuration.

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

Monitoring WAN Ports Status

You can monitor the status of both of the WAN connections, the Dynamic DNS Server connections, and the DHCP Server connections. Select **Network Configuration** from the main menu and **WAN Settings** from the submenu. The **Broadband ISP Settings** screen will display. Click the **Broadband Status** link to obtain status on the Broadband port. Select the **Dialup ISP Settings** tab and click the **Dialup Status** link to obtain status on the Dialup port.

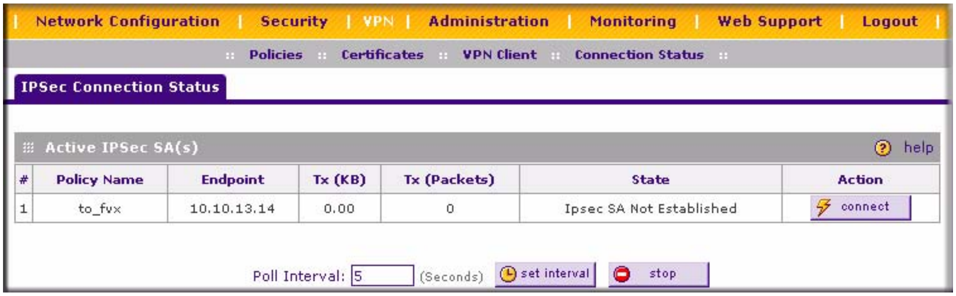


Connection Time: 0 Days 00:11:33
Connection Type: DHCP
Connection State: Connected
IP Address: 10.1.32.41
Subnet Mask: 255.255.255.0
Gateway: 10.1.32.13
DNS Server: 10.1.1.6
DHCP Server: 10.1.1.6
Lease Obtained: Thu Jul 6 19:07:31 GMT 2006
Lease Duration: 1 Day 00:00:00

Figure 6-12

Monitoring VPN Tunnel Connection Status

You can view the status of the VPN tunnels by selecting **VPN** from the main menu and **Connection Status** from the submenu. The **IPSec Connection Status** screen will display.


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
Policies :: Certificates :: VPN Client :: Connection Status
IPSec Connection Status
Active IPSec SA(s)
help
set interval
stop

#	Policy Name	Endpoint	Tx (KB)	Tx (Packets)	State	Action
1	to_fvx	10.10.13.14	0.00	0	Ipsec SA Not Established	connect

Poll Interval: 5 (Seconds)

Figure 6-13

Table 6-3. IPSec Connection Status Fields

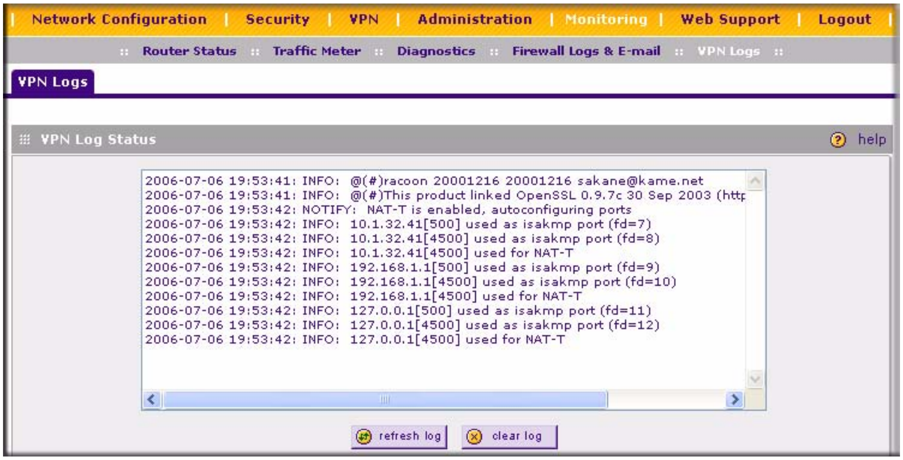
Item	Description
Policy Name	The name of the VPN policy associated with this SA.
Endpoint	The IP address on the remote VPN Endpoint.

Table 6-3. IPSec Connection Status Fields (continued)

Item	Description
Tx (KB)	The amount of data transmitted over this SA.
Tx (Packets)	The number of IP packets 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.

VPN Logs

The **VPN Logs** screen gives log details for recent VPN activity. Select **Monitoring** from the main menu and **VPN Logs** from the submenu to view the VPN Logs. You can refresh the log display to view the most recent entries, or clear the log display to delete all the log entries.

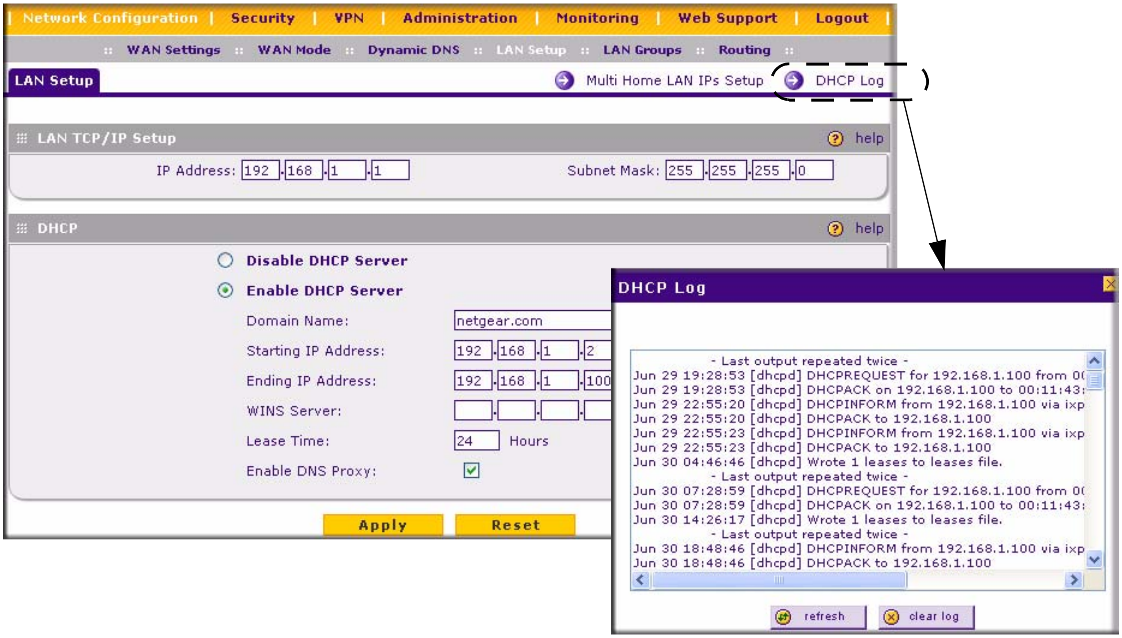

| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Router Status :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
VPN Logs
VPN Log Status
help
refresh log
clear log

```
2006-07-06 19:53:41: INFO:  @(#)racoon 20001216 20001216 sakane@kame.net
2006-07-06 19:53:41: INFO:  @(#)This product linked OpenSSL 0.9.7c 30 Sep 2003 (http
2006-07-06 19:53:42: NOTIFY:  NAT-T is enabled, autoconfiguring ports
2006-07-06 19:53:42: INFO:  10.1.32.41[500] used as isakmp port (fd=7)
2006-07-06 19:53:42: INFO:  10.1.32.41[4500] used as isakmp port (fd=8)
2006-07-06 19:53:42: INFO:  10.1.32.41[4500] used for NAT-T
2006-07-06 19:53:42: INFO:  192.168.1.1[500] used as isakmp port (fd=9)
2006-07-06 19:53:42: INFO:  192.168.1.1[4500] used as isakmp port (fd=10)
2006-07-06 19:53:42: INFO:  192.168.1.1[4500] used for NAT-T
2006-07-06 19:53:42: INFO:  127.0.0.1[500] used as isakmp port (fd=11)
2006-07-06 19:53:42: INFO:  127.0.0.1[4500] used as isakmp port (fd=12)
2006-07-06 19:53:42: INFO:  127.0.0.1[4500] used for NAT-T
```

Figure 6-14

DHCP Log

You can view the DHCP log from the **LAN Setup** screen. Select **Network Configuration** from the main menu and **Lan Setup** from the submenu. When the **LAN Setup** screen displays, click the **DHCP Log** link.


Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
:: WAN Settings :: WAN Mode :: Dynamic DNS :: LAN Setup :: LAN Groups :: Routing ::
LAN Setup
Multi Home LAN IPs Setup
DHCP Log
help
help
Apply
Reset
refresh
clear log

LAN TCP/IP Setup

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

DHCP

○ Disable DHCP Server
● Enable DHCP Server

Domain Name: netgear.com
Starting IP Address: 192 . 168 . 1 . 2
Ending IP Address: 192 . 168 . 1 . 100
WINS Server:
Lease Time: 24 Hours
Enable DNS Proxy: ☑

DHCP Log

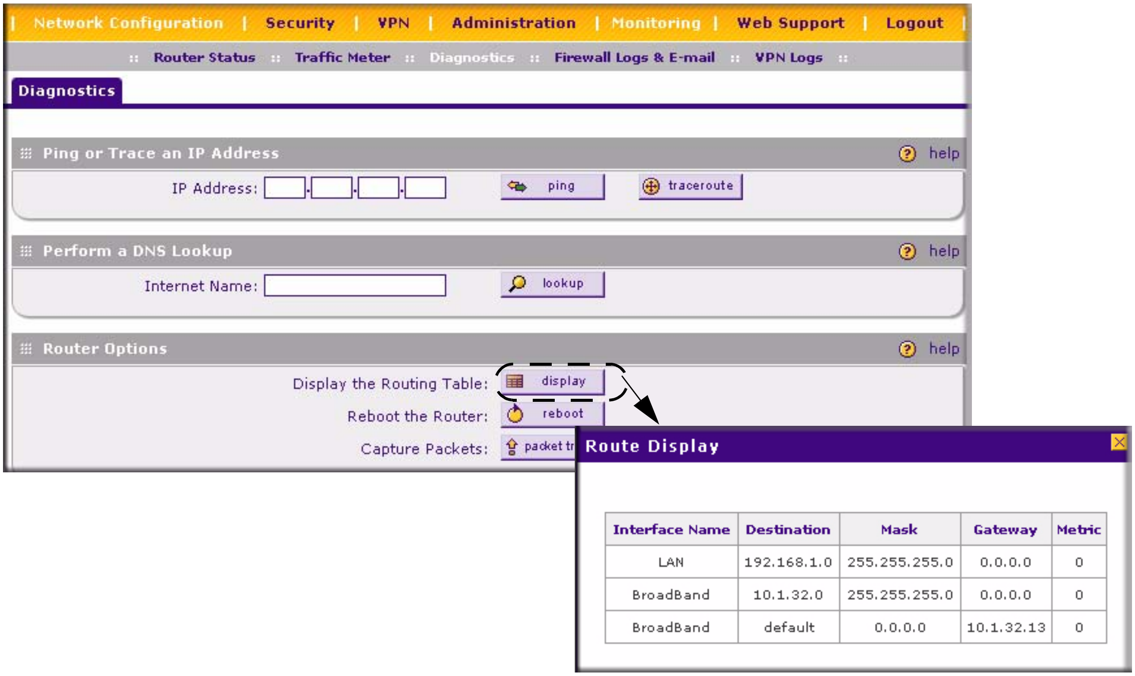
```
               - Last output repeated twice -
Jun 29 19:28:53 [dhcpd] DHCPREQUEST for 192.168.1.100 from 0(
Jun 29 19:28:53 [dhcpd] DHCPACK on 192.168.1.100 to 00:11:43:
Jun 29 22:55:20 [dhcpd] DHCPINFORM from 192.168.1.100 via ixp
Jun 29 22:55:20 [dhcpd] DHCPACK to 192.168.1.100
Jun 29 22:55:23 [dhcpd] DHCPINFORM from 192.168.1.100 via ixp
Jun 29 22:55:23 [dhcpd] DHCPACK to 192.168.1.100
Jun 30 04:46:46 [dhcpd] Wrote 1 leases to leases file.
               - Last output repeated twice -
Jun 30 07:28:59 [dhcpd] DHCPREQUEST for 192.168.1.100 from 0(
Jun 30 07:28:59 [dhcpd] DHCPACK on 192.168.1.100 to 00:11:43:
Jun 30 14:26:17 [dhcpd] Wrote 1 leases to leases file.
               - Last output repeated twice -
Jun 30 18:48:46 [dhcpd] DHCPINFORM from 192.168.1.100 via ixp
Jun 30 18:48:46 [dhcpd] DHCPACK to 192.168.1.100
```

Figure 6-15

Performing Diagnostics

You can perform diagnostics such as pinging an IP address, performing a DNS lookup, displaying the routing table, rebooting the firewall, and capturing packets. Select **Monitoring** from the main menu and **Diagnostics** from the submenu. The **Diagnostics** screen will display.

➡	**Note:** For normal operation, diagnostics are not required.



Interface Name	Destination	Mask	Gateway	Metric
LAN	192.168.1.0	255.255.255.0	0.0.0.0	0
BroadBand	10.1.32.0	255.255.255.0	0.0.0.0	0
BroadBand	default	0.0.0.0	10.1.32.13	0

Figure 6-16

Table 6-4. Diagnostics Fields

Item	Description
Ping or Trace an IP address	Ping – Used to send a ping packet request to a specified IP address—most often, to test a connection. If the request times out (no reply is received), it usually means that 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” on the Windows menu bar to return to the Diagnostics screen.
	Traceroute (often called Trace Route) – Lists 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” on the Windows menu bar 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, most often, by Technical Support.

Table 6-4. Diagnostics Fields

Item	Description
Reboot the Router	Used 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	Packet Trace selects the interface and starts the packet capture on that interface.

Chapter 7
Troubleshooting

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

Basic Functions

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

1. When power is first applied, verify that the 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 7-7.

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 7-7.

Tip: If you don't want to revert to the factory default settings and lose your configuration settings, you can reboot the router and use sniffer to capture packets sent during the reboot. Look at the ARP packets to locate the router's LAN interface address.

- 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 Monitoring menu, 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 the Internet, and may check for your PC’s MAC address. In this case:
  – Inform your ISP that you have bought a new network device, and ask them to use the firewall’s MAC address; or

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

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 7-2.
  - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and firewall.
- Wrong network configuration
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
  - Verify that the IP address for your firewall and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your PC to a Remote Device

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

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

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

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

- Check that your PC has the IP address of your firewall listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC's Network Control Panel.
- Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your PC, enter that host name as the Account Name in the Basic Settings menu.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your firewall to "clone" or "spoof" the MAC address from the authorized PC. Refer to "Manually Configuring Your Internet Connection" on page 2-9.

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 "Backup and Restore Settings" on page 6-13).
- Use the 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 reset button on the rear panel of the firewall.

1. Press and hold the reset button until the Test LED turns on and begins to blink (about 10 seconds).
2. Release the reset button and wait for the firewall to reboot.

Problems with Date and Time

The E-Mail menu in the Content Filtering section displays the current date and time of day. The VPN firewall uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

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

Appendix A
Default Settings and Technical Specifications

You can use the reset button located on the front of your device to reset all settings to their factory defaults. This is called a hard reset.

- To perform a hard reset, push and hold the reset button for approximately 5 seconds (until the TEST LED blinks rapidly). Your device will return to the factory configuration settings shown in Table A-1 below.
- Pressing the reset button for a shorter period of time will simply cause your device to reboot.

Table A-1. FVS338 Default Settings

Feature		**Default Behavior**
Router Login		
	User Login URL	http://192.168.1.1
	User Name (case sensitive)	admin
	Login Password (case sensitive)	password
Internet Connection		
	WAN MAC Address	Use Default address
	WAN MTU Size	1500
	Port Speed	AutoSense
Local Network (LAN)		
	Lan IP	192.168.1.1
	Subnet Mask	255.255.255.0
	RIP Direction	None
	RIP Version	Disabled
	RIP Authentication	Disabled
	DHCP Server	Enabled
	DHCP Starting IP Address	192.168.1.2
	DHCP Ending IP Address	192.168.1.100
	DMZ	Disabled

Table A-1. FVS338 Default Settings (continued)

Feature		Default Behavior
	Time Zone	GMT
	Time Zone Adjusted for Daylight Saving Time	Disabled
	SNMP	Disabled
	Remote Management	Disabled
Firewall		
	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the http port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled
	Stealth Mode	Enabled

Technical Specifications for the ProSafe VPN Firewall 50 are listed in the following table.

Table A-2. VPN firewall Default Technical Specifications

Feature		Specification
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
Physical Specifications		
	Dimensions:	1.1 x 6.89 x 4.65 in.
	Weight:	0.3 kg (0.66 lb)

Table A-2. VPN firewall Default Technical Specifications

Feature		Specification
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, and 9-pin DIN Serial

Appendix B
Related Documents

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
Internet Networking and TCP/IP Addressing:	*http://documentation.netgear.com/reference/enu/tcpip/index.htm*
Wireless Communications:	*http://documentation.netgear.com/reference/enu/wireless/index.htm*
Preparing a Computer for Network Access:	*http://documentation.netgear.com/reference/enu/wsdhcp/index.htm*
Virtual Private Networking (VPN):	*http://documentation.netgear.com/reference/enu/vpn/index.htm*
Glossary:	*http://documentation.netgear.com/reference/enu/glossary/index.htm*

Index