ProSafe VPN Firewall 200 FVX538 Reference Manual

NETGEAR®

NETGEAR, Inc.
350 East Plumeria Drive
San Jose, CA 95134

202-10062-10
v1.0
January 2010

Technical Support

Please refer to the support information card that shipped with your product. By registering your product at *http://www.netgear.com/register*, we can provide you with faster expert technical support and timely notices of product and software upgrades.

NETGEAR, INC. Support Information

Phone: 1-888-NETGEAR, for US & Canada only. For other countries, see your Support information card.

E-mail: support@netgear.com

North American NETGEAR website: *http://www.netgear.com*

Trademarks

NETGEAR and the NETGEAR logo are registered trademarks and ProSafe is a trademark of NETGEAR, Inc. Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

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

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

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

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

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

EU Regulatory Compliance Statement

The ProSafe VPN Firewall 200 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 200 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 200 has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

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

Voluntary Control Council for Interference (VCCI) Statement

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

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

Read instructions for correct handling.

Additional Copyrights

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

Open SSL	Copyright (c) 1998–2000 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (*http://www.openssl.org/*).” 4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, contact openssl-core@openssl.org. 5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project. 6. Redistributions of any form whatsoever must retain the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (*http://www.openssl.org/*).” THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS,” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).
MD5	Copyright (C) 1990, RSA Data Security, Inc. All rights reserved. License to copy and use this software is granted provided that it is identified as the “RSA Data Security, Inc. MD5 Message-Digest Algorithm” in all material mentioning or referencing this software or this function. License is also granted to make and use derivative works provided that such works are identified as “derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm” in all material mentioning or referencing the derived work. RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided “as is” without express or implied warranty of any kind. These notices must be retained in any copies of any part of this documentation and/or software.

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

Product and Publication Details

Model Number:	FVX538
Publication Date:	January 2010
Product Family:	VPN Firewall
Product Name:	ProSafe VPN Firewall 200
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10062-10
Publication Version Number	1.0

Contents

ProSafe VPN Firewall 200 FVX538 Reference Manual

About This Manual

Conventions, Formats and Scope xiii
How to Print This Manual xiv
Revision History xiv

Chapter 1
Introduction

Key Features 1-1
Dual WAN Ports for Increased Reliability or Outbound Load Balancing 1-2
A Powerful, True Firewall with Content Filtering 1-2
Security Features 1-3
Autosensing Ethernet Connections with Auto Uplink 1-3
Extensive Protocol Support 1-4
Easy Installation and Management 1-4
Maintenance and Support 1-5
Package Contents 1-5
VPN Firewall Front and Rear Panels 1-6
Rack Mounting Hardware 1-8
The VPN Firewall's IP Address, Login Name, and Password 1-9
Qualified Web Browsers 1-10

Chapter 2
Connecting the VPN Firewall to the Internet

Understanding the Connection Steps 2-1
Logging into the VPN Firewall 2-2
Configuring the Internet Connections to Your ISPs 2-2
Setting the VPN Firewall's MAC Address 2-5
Manually Configuring Your Internet Connection 2-5
Configuring the WAN Mode (Required for Dual WAN) 2-7
Setting Up Auto-Rollover Mode 2-9

Setting Up Load Balancing 2-11
Configuring Dynamic DNS (Optional) 2-14
Configuring the Advanced WAN Options (Optional) 2-16
Additional WAN Related Configuration 2-17

Chapter 3
LAN Configuration

Choosing the VPN Firewall DHCP Options 3-1
Configuring the LAN Setup Options 3-2
Managing Groups and Hosts (LAN Groups) 3-6
Creating the Network Database 3-6
Viewing the Network Database 3-7
Adding Devices to the Network Database 3-8
Changing Group Names in the LAN Groups Database 3-9
Setting Up DHCP Address Reservation 3-9
Configuring Multi Home LAN IP Addresses 3-10
Configuring and Enabling the DMZ Port 3-11
Configuring Static Routes 3-14
Static Route Example 3-16
Configuring Routing Information Protocol (RIP) 3-16

Chapter 4
Firewall Protection and Content Filtering

About Firewall Protection and Content Filtering 4-1
Using Rules to Block or Allow Specific Kinds of Traffic 4-2
Services-Based Rules 4-3
Viewing Rules and Order of Precedence for Rules 4-7
Configuring LAN WAN Rules 4-9
Configuring DMZ WAN Rules 4-12
Configuring LAN DMZ Rules 4-13
Inbound Rules Examples 4-15
Outbound Rules Example 4-19
Configuring Other Firewall Features 4-19
Attack Checks 4-20
Setting Session Limits 4-22
Managing the Application Level Gateway for SIP Sessions 4-23
Creating Services, QoS Profiles, and Bandwidth Profiles 4-24

Adding Customized Services 4-24
Specifying Quality of Service (QoS) Priorities 4-26
Creating Bandwidth Profiles 4-27
Setting a Schedule to Block or Allow Specific Traffic 4-29
Blocking Internet Sites (Content Filtering) 4-30
Configuring Source MAC Filtering 4-33
Configuring IP/MAC Address Binding 4-35
Configuring Port Triggering 4-37
E-Mail Notifications of Event Logs and Alerts 4-40
Administrator Tips 4-40

Chapter 5
Virtual Private Networking

Considerations for Dual WAN Port Systems 5-1
Using the VPN Wizard for Client and Gateway Configurations 5-3
Creating Gateway to Gateway VPN Tunnels with the Wizard 5-3
Creating a Client to Gateway VPN Tunnel 5-6
Testing the Connections and Viewing Status Information 5-12
NETGEAR VPN Client Status and Log Information 5-12
VPN Firewall VPN Connection Status and Logs 5-14
Managing VPN Policies 5-16
Configuring IKE Policies 5-16
Configuring VPN Policies 5-18
Managing Certificates 5-19
Viewing and Loading CA Certificates 5-21
Viewing Active Self Certificates 5-22
Obtaining a Self Certificate from a Certificate Authority 5-22
Managing your Certificate Revocation List (CRL) 5-25
Extended Authentication (XAUTH) Configuration 5-26
Configuring XAUTH for VPN Clients 5-27
User Database Configuration 5-29
RADIUS Client Configuration 5-30
Assigning IP Addresses to Remote Users (ModeConfig) 5-32
Mode Config Operation 5-32
Configuring Mode Config Operation on the VPN Firewall 5-33
Configuring the ProSafe VPN Client for ModeConfig 5-38

Configuring Keepalives and Dead Peer Detection 5-42
Configuring Keepalives 5-42
Configuring Dead Peer Detection 5-43
Configuring NetBIOS Bridging with VPN 5-44

Chapter 6
VPN Firewall and Network Management

Performance Management 6-1
Bandwidth Capacity 6-1
VPN Firewall Features That Reduce Traffic 6-2
VPN Firewall Features That Increase Traffic 6-4
Using QoS to Shift the Traffic Mix 6-7
Tools for Traffic Management 6-8
Configuring Users, Administrative Settings, and Remote Management 6-8
Changing Passwords and Settings 6-8
Adding External Users 6-10
Configuring an External Server for Authentication 6-11
Enabling Remote Management Access 6-14
Using an SNMP Manager 6-16
Managing the Configuration File 6-18
Configuring Date and Time Service 6-21
Monitoring System Performance 6-23
Activating Notification of Events and Alerts 6-23
Viewing the Logs 6-26
Enabling the Traffic Meter 6-27
Viewing the VPN Firewall Configuration and System Status 6-30
Monitoring VPN Firewall Statistics 6-31
Monitoring WAN Ports Status 6-32
Monitoring Attached Devices 6-33
Monitoring VPN Tunnel Connection Status 6-34
Viewing the VPN Logs 6-35
Viewing the DHCP Log 6-36
Viewing Port Triggering Status 6-36

Chapter 7
Troubleshooting

Basic Functions 7-1

Power LED Not On 7-2
LEDs Never Turn Off 7-2
LAN or Internet Port LEDs Not On 7-2
Troubleshooting the Web Configuration Interface 7-3
Troubleshooting the ISP Connection 7-4
Troubleshooting a TCP/IP Network Using a Ping Utility 7-5
Testing the LAN Path to Your VPN Firewall 7-5
Testing the Path from Your PC to a Remote Device 7-6
Restoring the Default Configuration and Password 7-7
Problems with Date and Time 7-7
Using the Diagnostics Utilities 7-8

Appendix A
Default Settings and Technical Specifications

Appendix B
Network Planning for Dual WAN Ports

What You Will Need to Do Before You Begin B-1
Cabling and Computer Hardware Requirements B-3
Computer Network Configuration Requirements B-3
Internet Configuration Requirements B-3
Where Do I Get the Internet Configuration Parameters? B-4
Internet Connection Information Form B-4
Overview of the Planning Process B-5
Inbound Traffic B-5
Virtual Private Networks (VPNs) B-6
The Roll-over Case for Firewalls With Dual WAN Ports B-6
The Load Balancing Case for Firewalls With Dual WAN Ports B-7
Inbound Traffic B-7
Inbound Traffic to Single WAN Port (Reference Case) B-7
Inbound Traffic to Dual WAN Port Systems B-8
Virtual Private Networks (VPNs) B-9
VPN Road Warrior (Client-to-Gateway) B-11
VPN Gateway-to-Gateway B-14
VPN Telecommuter (Client-to-Gateway Through a NAT Router) B-16

Appendix C
System Logs and Error Messages

System Log Messages C-1
System Startup C-1
Reboot C-2
NTP C-2
Login/Logout C-3
Firewall Restart C-3
IPSec Restart C-4
WAN Status C-4
Web Filtering and Content Filtering Logs C-7
Traffic Metering Logs C-9
Unicast Logs C-9
FTP Logging C-10
Invalid Packet Logging C-10
Routing Logs C-13
LAN to WAN Logs C-14
LAN to DMZ Logs C-14
DMZ to WAN Logs C-14
WAN to LAN Logs C-14
DMZ to LAN Logs C-15
WAN to DMZ Logs C-15

Appendix D
Two Factor Authentication

Why do I need Two-Factor Authentication? D-1
What are the benefits of Two-Factor Authentication? D-1
What is Two-Factor Authentication D-2
NETGEAR Two-Factor Authentication Solutions D-2

Appendix E
Related Documents

Index

About This Manual

The *NETGEAR® ProSafe™ VPN Firewall 200* describes how to install, configure and troubleshoot the ProSafe VPN Firewall 200. 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, file and server names, extensions
Bold	User input, IP addresses, GUI screen text
`Fixed`	Command prompt, CLI text, code
italics	URL links

- **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 200
Manual Publication Date	January 2010

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

Note: Product updates are available on the NETGEAR, Inc. website at *http://kb.netgear.com/app/home*.

How to Print This Manual

To print this manual, 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 website at *http://www.adobe.com*.

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	Date	Description
202-10062-04	1.0	Aug. 2006	Product update: New firmware and a new user interface.
202-10062-05	1.0	Jan. 2007	Remove Trend Micro
202-10062-06	1.0	Jul. 2007	New features: IP/MAC Binding; Bandwidth Limits; Session Limits; IKE Keep Alive; Dead Peer Detection; Oray Support
202-10062-06	1.1	Oct. 2007	Document corrections
202-10062-06	1.2	Oct. 2007	Document additions to Appendix C
202-10062-07	1.0	Mar. 08	Maintenance release

202-10062-09	1.0	Mar. 09	Adds these corrections and topics for the March 2009 firmware maintenance release: • WIKID 2 factor authentication • SIP ALG support • DHCP Relay support • Update VPN configuration procedure topics • Update the Certificate management topic • Correct the firewall scheduling topic
202-10062-10	1.0	January 2010	Added the following new features for the January 2010 firmware maintenance release: • Connection reset and delay options on the WAN ISP Settings screen (see “Manually Configuring Your Internet Connection”). • Support for DNS 3322 in the Dynamic DNS submenu (see “Configuring Dynamic DNS (Optional)”). • Support for an address range for inbound LAN rules on the Add LAN WAN Inbound Service screen (see “Inbound Rules (Port Forwarding)” and “Inbound Rules Examples”). • Support for new log options such as Resolved DNS Names and VPN on the Firewall Logs & E-mail screen (see “Activating Notification of Events and Alerts”). In addition, made the following substantial changes to the book: • Resized all screen captures for better viewing. • Added qualified Web browser information in the “Qualified Web Browsers” and “Computer Network Configuration Requirements” sections. • Updated the WAN1 ISP Settings screen (Figure 2-1) and the ISP Type options in the ”“Manually Configuring Your Internet Connection” section. • Updated the Dynamic DNS Configuration screen (Figure 2-6) and the DDNS providers in the ““Configuring Dynamic DNS (Optional)” section. • Revised the “Enabling the Traffic Meter” section and moved this section from the “Connecting the VPN Firewall to the Internet” chapter to the “VPN Firewall and Network Management” chapter. • Added the “Additional WAN Related Configuration“ section. • Updated the LAN Setup screen (Figure 3-1), added LDAP information and the Enable ARP Broadcast paragraph to the “Configuring the LAN Setup Options” section, and revised this section for more clarity. • Updated the LAN Groups screen (Figure 3-2) and the Network Database Group Name screen (Figure 3-3), and revised the “Managing Groups and Hosts (LAN Groups)” section for more clarity.

202-10062-10 (continued)	1.0	January 2010	(continued) • Updated the LAN Multi-homing screen (Figure 3-4) and revised the "Configuring Multi Home LAN IP Addresses" section for more clarity. • Revised the "Configuring and Enabling the DMZ Port" section for more clarity. • Updated the RIP Configuration screen (Figure 3-8). • Revised the "Viewing Rules and Order of Precedence for Rules" section and updated the LAN WAN Rules screen (Figure 4-2). • Updated the Add LAN WAN Inbound Service screen (Figure 4-3), related screens in the "Inbound Rules Examples" section, and the Inbound Rules table (Table 4-3) to show that a range of IP addresses can be selected for the Send to LAN Server field. • Updated the sections and screens in the "Configuring Other Firewall Features" section and added the "Managing the Application Level Gateway for SIP Sessions" section. • Updated the following sections and screens in the "Firewall Protection and Content Filtering" chapter to show the current user interface: * "Creating Services, QoS Profiles, and Bandwidth Profiles" * "Setting a Schedule to Block or Allow Specific Traffic" * "Blocking Internet Sites (Content Filtering)" * "Configuring Source MAC Filtering" * "Configuring IP/MAC Address Binding" * "Configuring Port Triggering" • Moved the procedures and screens from the "E-Mail Notifications of Event Logs and Alerts" section in the "Firewall Protection and Content Filtering" chapter to the "Activating Notification of Events and Alerts" section in the ""VPN Firewall and Network Management" chapter. • Updated all FVX538 screens and made various corrections and clarifications in the "Virtual Private Networking" chapter. • Revised the "Managing Certificates" section and added the following sections to the "Virtual Private Networking" chapter: * "Configuring Keepalives and Dead Peer Detection" * "Configuring NetBIOS Bridging with VPN" • Revised the following sections in the "VPN Firewall and Network Management" chapter and updated all screens in these sections: * "Configuring Users, Administrative Settings, and Remote Management" * "Monitoring System Performance" • Moved the "Using the Diagnostics Utilities" section from the "VPN Firewall and Network Management" chapter to the "Troubleshooting" chapter.

Chapter 1
Introduction

The ProSafe VPN Firewall 200 FVX538 with eight 10/100 ports and one 1/100/1000 port connects your local area network (LAN) to the Internet through an external access device such as a cable modem or DSL modem.

The FVX538 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.

The FVX538 is a plug-and-play device that can be installed and configured within minutes.

This chapter contains the following sections:

- "Key Features" on this page
- "Package Contents" on page 1-5
- "VPN Firewall Front and Rear Panels" on page 1-6
- "The VPN Firewall's IP Address, Login Name, and Password" on page 1-9
- "Qualified Web Browsers" on page 1-10

Key Features

The VPN firewall provides the following features:

- Dual 10/100 Mbps Ethernet WAN ports for load balancing or failover protection, providing increased system reliability and load balancing. The WAN ports do not respond at all to unsolicited traffic (stealth mode).
- Support for up to 200 simultaneous IPSec VPN tunnels.
- Support for up to 400 internal LAN users (and 50K connections).
- Bundled with the 5-user license of the NETGEAR ProSafe VPN Client software (VPN05L)
- Quality of Service (QoS) and SIP 2.0 support for traffic prioritization, voice, and multimedia.
- Built-in 10/100 Mbps ports plus 1 Gigabit Switch port.

- One console port for local management.
- SNMP Manageable, optimized for the NETGEAR ProSafe Network Management Software (NMS100).
- Easy, web-based setup for installation and management.
- Advanced SPI Firewall and Multi-NAT support.
- Extensive Protocol Support.
- Login capability.
- Front panel LEDs for easy monitoring of status and activity.
- Flash memory for firmware upgrade.
- One U Rack mountable.

Dual WAN Ports for Increased Reliability or Outbound Load Balancing

The FVX538 has two broadband WAN ports, WAN1 and WAN2, each capable of operating independently at speeds of either 10 Mbps or 100 Mbps. The two WAN ports let you connect a second broadband Internet line that can be configured on a mutually-exclusive basis to:

- Provide backup and rollover if one line is inoperable, ensuring you are never disconnected.
- Load balance, or use both Internet lines simultaneously for the outgoing traffic. The VPN firewall balances users between the two lines for maximum bandwidth efficiency.

See "Network Planning for Dual WAN Ports" on page B-1 for the planning factors to consider when implementing the following capabilities with dual WAN port gateways:

- Single or multiple exposed hosts
- Virtual private networks

A Powerful, True Firewall with Content Filtering

Unlike simple Internet sharing NAT routers, the FVX538 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.
- **Secure Firewall**. Blocks unwanted traffic from the Internet to your LAN.
- **Block Sites.** Blocks access from your LAN to Internet locations or services that you specify as off-limits.

- **Logs security incidents.** The FVX538 will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the VPN firewall to e-mail the log to you at specified intervals. You can also configure the VPN firewall to send immediate alert messages to your e-mail address or e-mail pager whenever a significant event occurs.
- **Keyword Filtering.** With its URL keyword filtering feature, the FVX538 prevents objectionable content from reaching your PCs. The VPN firewall allows you to control access to Internet content by screening for keywords within Web addresses. You can configure the VPN firewall to log and report attempts to access objectionable Internet sites.

Security Features

The FVX538 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 VPN 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.
- **DMZ port**. Incoming traffic from the Internet is normally discarded by the VPN 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 FVX538 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 VPN 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 FVX538 supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). For further information about TCP/IP, see the "TCP/IP Networking Basics" document that you can access from the link in "Related Documents" in Appendix E.

- **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 VPN firewall provides its own address as a DNS server to the attached PCs. The VPN firewall obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.
- **PPP over Ethernet (PPPoE)**. PPPoE is a protocol for connecting remote hosts to the Internet over a DSL connection by simulating a dial-up connection. This feature eliminates the need to run a login program such as EnterNet or WinPOET on your PC.

Easy Installation and Management

You can install, configure, and operate the FVX538 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 VPN 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.
- **Auto Detect**. 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 VPN firewall incorporates built-in diagnostic functions such as Ping, Trace Route, DNS lookup, and remote reboot.
- **Remote Management**. The VPN firewall allows you to login to the Web Management Interface from a remote location on the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses, and you can choose a nonstandard port number.
- **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 FVX538:

- Flash memory for firmware upgrade
- Technical support seven days a week, 24 hours a day, according to the terms identified in the Warranty and Support information card provided with your product.

Package Contents

The product package should contain the following items:

- FVX538 ProSafe VPN Firewall 200.
- AC power cable.
- 19-inch rack mounting hardware and rubber feet.
- Category 5 (Cat5) Ethernet cable.
- *Installation Guide, FVX538 ProSafe VPN Firewall 200*
- *Resource CD*, including:
  - Application Notes and other helpful information.
  - ProSafe VPN Client Software – five user licenses.
- 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 VPN firewall for repair.

VPN Firewall Front and Rear Panels

The FVX538 front panel shown below contains the port connections, status LEDs, and the factory defaults reset button.

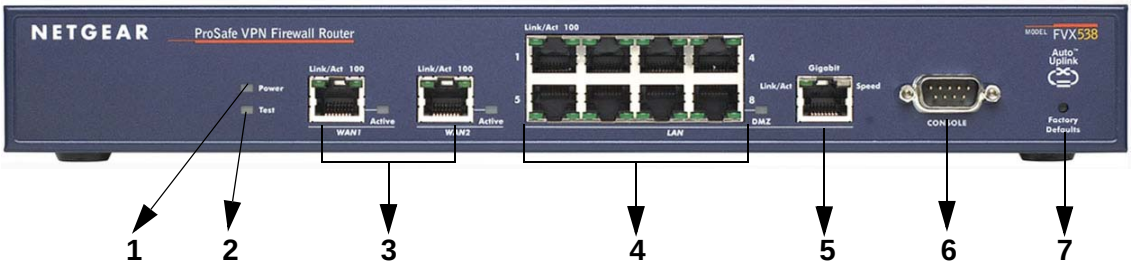


Figure 1-1

Table 1-1 describes each item on the front panel and its operation.

Table 1-1. Object Descriptions

Object	LED Activity		Description
1. Power LED	On (Green)		Power is supplied to the VPN firewall.
	Off		Power is not supplied to the VPN firewall.
2. Test LED	On (Amber)		Test mode: The system is initializing or the initialization has failed.
	Blinking (Amber)		Writing to Flash memory (during upgrading or resetting to defaults).
	Off		The system has booted successfully.
3, WAN Ports and LEDs	Two RJ-45 WAN ports N-way automatic speed negotiation, Auto MDI/MDIX.		
	Link/Act LED	On (Green)	The WAN port has detected a link with a connected Ethernet device.
		Blinking (Green)	Data is being transmitted or received by the WAN port.
		Off	The WAN port has no link.
	100 LED	On (Green)	The WAN port is operating at 100 Mbps.
		Off	The WAN port is operating at 10 Mbps.

Table 1-1. Object Descriptions (continued)

Object	LED Activity		Description
3, WAN Ports and LEDs (continued)	**Active LED**	On (Green)	The WAN port has a valid Internet connection.
		On (Amber)	The Internet connection is down or not being used because the port is available for failover in case the connection on other WAN port fails.
		Off	The WAN port is either not enabled or has no link.
4. LAN Ports and LEDs	8-port RJ-45 10/100 Mbps Fast Ethernet Switch N-way automatic speed negotiation, auto MDI/MDIX.		
	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.
	DMZ LED (port 8)	On (Green)	Port 8 is operating as a dedicated hardware DMZ port.
		Off	Port 8 is operating as a normal LAN port.
5. Gigabit Port and LEDs	Gbit RJ-45 connector. Port for connecting to a Gigabit Ethernet device.		
	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.
	Speed LED	On (Green)	The LAN port is operating at 1,000 Mbps.
		On (Amber)	The LAN port is operating at 100 Mbps.
		Off	The LAN port is operating at 10 Mbps.
6. Console Port	DB9 male connector. Port for connecting to an optional console terminal. Default baud rate is 115.2K; pinouts: (2) Tx, (3) Rx, (5) and (7) Gnd.		
7. Factory Defaults	Push in with a sharp object Factory Defaults reset push button (see Appendix A, “Default Settings and Technical Specifications” for the factory defaults).		

The rear panel of the FVX538 contains the On/Off switch and AC power connection.

Figure 1-2

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

1. AC power in
2. On/Off switch

Rack Mounting Hardware

The FVX538 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).

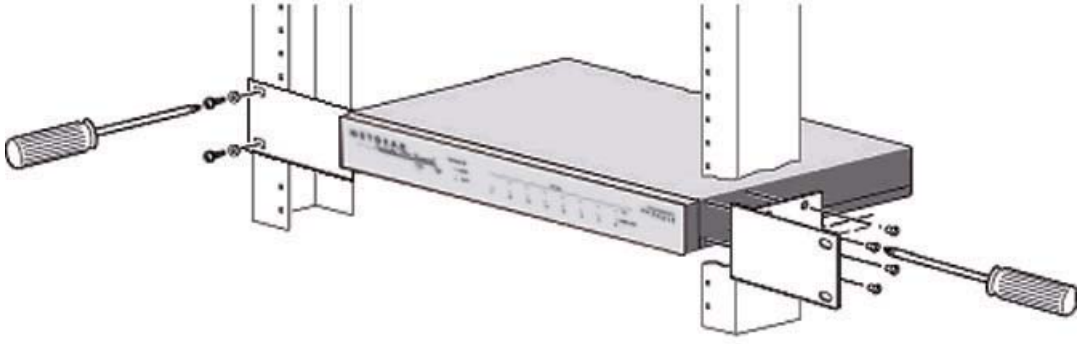


Figure 1-3

The VPN Firewall's IP Address, Login Name, and Password

Check the label on the bottom of the FVX538'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

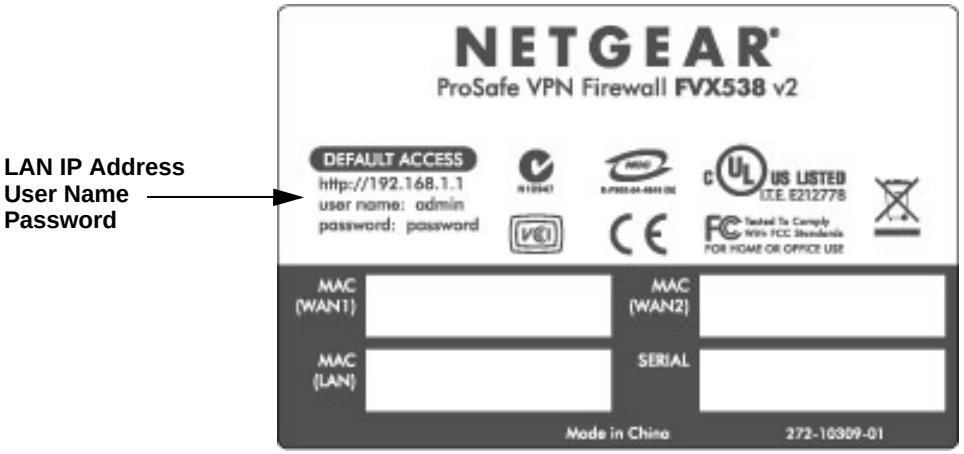


Figure 1-4

To log in to the FVX538 once it is connected, go to **http://192.168.1.1**.

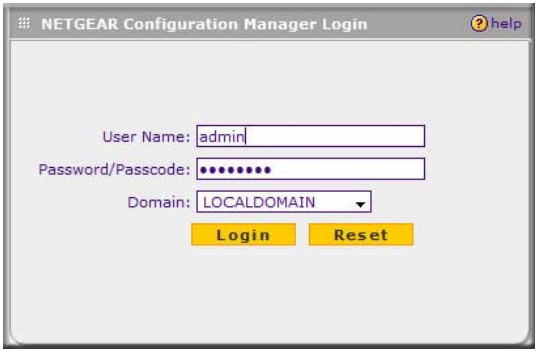


Figure 1-5

Once the login screen displays, enter **admin** for the User Name and the **password** for Password.

Qualified Web Browsers

To configure the FVX538, you must use a Web browser such as Microsoft Internet Explorer 6 or higher, Mozilla Firefox 3 or higher, or Apple Safari 3 or higher with JavaScript, cookies, and you must have SSL enabled.

Chapter 2
Connecting the VPN Firewall to the Internet

This section provides instructions for connecting the ProSafe VPN Firewall 200 FVX538, including these topics:

- "Understanding the Connection Steps" on this page
- "Logging into the VPN Firewall" on page 2-2
- "Configuring the Internet Connections to Your ISPs" on page 2-2
- "Configuring the WAN Mode (Required for Dual WAN)" on page 2-7
- "Configuring Dynamic DNS (Optional)" on page 2-14
- "Configuring the Advanced WAN Options (Optional)" on page 2-16

Setting up VPN tunnels is covered in Chapter 5, "Virtual Private Networking."

Understanding the Connection Steps

Typically, six steps are required to complete the basic Internet connection of your VPN firewall.

1. **Connect the VPN firewall physically to your network**. Connect the cables and restart your network according to the instructions in the installation guide. See the *Installation Guide, FVX538 ProSafe VPN Firewall 200* for complete steps. A PDF of the *Installation Guide* is on the NETGEAR website at: *http://kbserver.netgear.com*.
2. **Log in to the VPN Firewall**. After logging in, you are ready to set up and configure your VPN firewall. You can also change your password and enable remote management at this time. See "Logging into the VPN Firewall" on page 2-2.
3. **Configure the Internet connections to your ISP(s)**. During this phase, you will connect to your ISPs. See "Configuring the Internet Connections to Your ISPs" on page 2-2.
4. **Configure the WAN mode (required for dual WAN operation)**. Select either dedicated (single WAN) mode, auto-rollover mode, or load balancing mode. For load balancing, you can also select any necessary protocol bindings. See "Configuring the WAN Mode (Required for Dual WAN)" on page 2-7.

5. **Configure dynamic DNS on the WAN ports (optional)**. Configure your fully qualified domain names during this phase (if required). See "Configuring Dynamic DNS (Optional)" on page 2-14.
6. **Configure the WAN options (optional)**. Optionally, you can enable each WAN port to respond to a ping, and you can change the factory default MTU size and port speed. However, these are advanced features and changing them is not usually required. See "Configuring the Advanced WAN Options (Optional)" on page 2-16.

Each of these tasks is detailed separately in this chapter. The configuration of firewall and VPN features is described in later chapters.

Logging into the VPN Firewall

To connect to the VPN firewall, your computer needs to be configured to obtain an IP address automatically via DHCP. If you need instructions on how to configure you computer for DHCP, refer to the "Preparing Your Network" document that you can access from the link in Appendix E, "Related Documents."

To log in to the VPN firewall:

1. Connect to the VPN firewall by typing **http://192.168.1.1** in the address field of your browser.
2. When prompted, enter **admin** for the VPN firewall user name and **password** for the VPN firewall password, both in lower case letters. (The VPN 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.**

> **Note:** You might want to enable remote management at this time so that you can log in remotely in the future to manage the VPN firewall (see "Configuring an External Server for Authentication" on page 6-11). If you enable remote management, you are strongly advised to change your password (see "Changing Passwords and Settings" on page 6-8).

Configuring the Internet Connections to Your ISPs

You should first configure your Internet connections to your ISPs on WAN port 1, and then on WAN port 2.

To automatically configure the WAN ports and connect to the Internet:

1. Select the primary menu option **Network Configuration** and the submenu option **WAN Settings**. WAN1 ISP Settings screen will display.

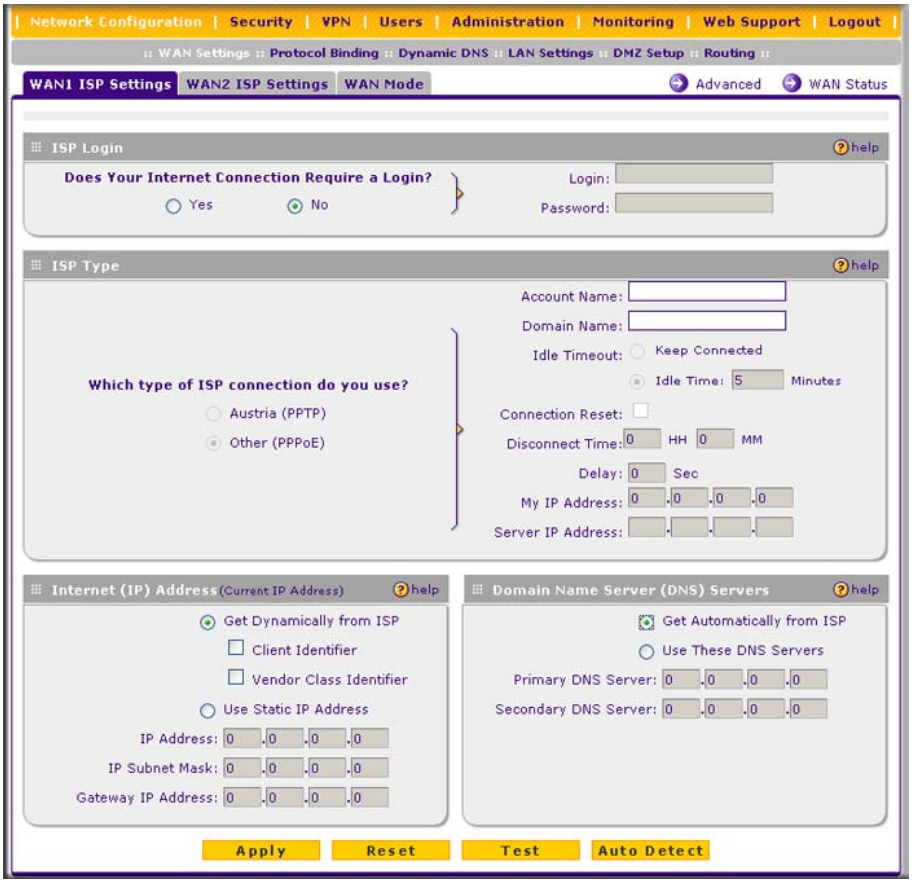


Figure 2-1

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 Table 2-1.

Note: When you click **Auto Detect** while the WAN port already has a connection, you might lose the connection because the VPN firewall will enter its detection mode.

Table 2-1. Internet connection methods

Connection Method	Data Required
PPPoE	Login (Username, Password); Account Name, Domain Name
PPTP	Login (Username, Password), Account Name, Local IP address, and PPTP Server IP address;
DHCP (Dynamic IP)	No data is required.
Fixed (Static) IP	Static IP address, Subnet, and Gateway IP; and related data supplied by your ISP.

If Auto Detect does not find a connection, you will be prompted to check the physical connection between your VPN firewall and the cable or DSL line or to check your VPN firewall's MAC address (see "Setting the VPN Firewall's MAC Address" on page 2-5).

3. Click **WAN Status** at the top right of the screen to verify WAN Port 1 connection status. Click **Connect** if there is no connection.

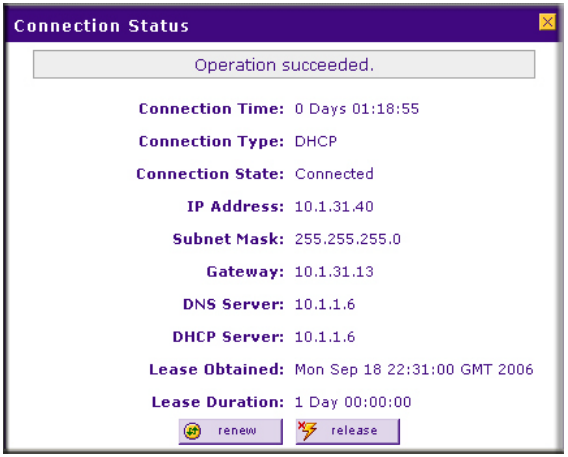


Figure 2-2

4. Set up the traffic meter for WAN 1 ISP if desired. See “Enabling the Traffic Meter” on page 6-27.

> **Note:** At this point of the configuration process, you are now connected to the Internet through WAN port 1. But you must continue with the configuration process to get the complete functionality of the dual WAN interface.

The configure the WAN2 ISP settings:

1. Repeat the above steps to set up the parameters for WAN2 ISP. Start by selecting the **WAN2 ISP Settings** tab. Next click **Auto Detect** on the WAN2 ISP Settings screen and then verify the connection by clicking the **WAN Status** link.
2. Set up the traffic meter for WAN2 ISP, if desired. See “Enabling the Traffic Meter” on page 6-27.

Setting the VPN Firewall’s MAC Address

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. Setting the VPN firewall’s MAC address is controlled through the **Advanced** options on the WAN1 ISP Settings and WAN2 ISP Settings screen (see“Configuring the Advanced WAN Options (Optional)” on page 2-16).

Manually Configuring Your Internet Connection

If you know your ISP connection type, you can bypass the Auto Detect feature and connect your VPN firewall 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 (see Figure 2-1 on page 2-3).

> **Note:** To enable a WAN port to respond to a Ping from the Internet, use the Rules menu (Figure 4-2 on page 4-9).

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:

   - **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 e-mail "ID" assigned by your ISP). Some ISPs require entering your full e-mail 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.
     - **Connection Reset**. Select this checkbox to to specify a time when the PPPoE WAN connection is reset, that is, the connection is disconnected momentarily and then re-established. Enter the hour and minutes in the **Disconnect Time** fields to specify when the connection should be disconnected. Enter the seconds in the **Delay** field to specify the period after which the connection should be re-established.

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:

   - **IP Address**. Static IP address assigned to you. This will identify the VPN firewall to your ISP.
   - **IP Subnet Mask**. This is usually provided by the ISP or your network administrator.
   - **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 VPN firewall using DHCP network protocol.

4. If your ISP has not assigned any Domain Name Servers (DNS) addresses, select the **Get Automatically from ISP** radio box. If your ISP has assigned DNS addresses, select the **Use These DNS Servers** radio box. Ensure that you enter 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 **Reset** to discard any changes and revert to the previous settings.
6. Click **Test** to try and connect to the NETGEAR website. If you connect successfully and your settings work, then you may click Logout or go on and configure additional settings.

To configure your WAN2 ISP settings:

1. Select the **WAN2 ISP Settings** tab. The WAN2 ISP Settings screen will display.
2. Repeat steps 1 through 7 above.

Configuring the WAN Mode (Required for Dual WAN)

The dual WAN ports of the VPN firewall can be configured on a mutually exclusive basis for either auto-rollover (for increased system reliability) or load balancing (for maximum bandwidth efficiency).

The VPN firewall supports the following modes:

- **Auto-Rollover Mode**. In this mode, the selected WAN interface is made primary and the other is the rollover link. As long as the primary link is up, all traffic is sent over the primary link. Once the primary WAN interface goes down, the rollover link is brought up to send the traffic. Traffic will automatically roll back to the original primary link once the original primary link is back up and running again.

  If you want to use a redundant ISP link for backup purposes, select the WAN port that will act as the primary link for this mode. Ensure that the backup WAN port has also been configured and that you configure the **WAN Failure Detection Method** to support Auto-Rollover.

- **Load Balancing Mode**. In this mode the VPN firewall distributes the outbound traffic equally among the WAN interfaces that are functional.

Note: Scenarios could arise when load balancing needs to be bypassed for certain traffic or applications. Here the traffic needs to go on a specific WAN interface. This is done with the protocol binding rules of that WAN interface. The rule should match the desired traffic.

For both alternatives, you must also set up Network Address Translation (NAT):

- **NAT**. NAT is the technology which allows all PCs on your LAN to share a single Internet IP address. From the Internet, there is only a single device (the VPN firewall) and a single IP address. PCs on your LAN can use any private IP address range, and these IP addresses are not visible from the Internet.

  – The VPN firewall uses NAT to select the correct PC (on your LAN) to receive any incoming data.

  – If you only have a single Internet IP address, you MUST use NAT.

  NAT is the default setting.

- **Classical Routing**. In this mode, the VPN firewall 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 VPN firewall.

To learn the status of the WAN ports, you can view the Router Status screen (see "Viewing the VPN Firewall Configuration and System Status" on page 6-30) or look at the LEDs on the front panel (see "VPN Firewall Front and Rear Panels" on page 1-6).

Setting Up Auto-Rollover Mode

If you want to use a redundant ISP link for backup purposes, ensure that the backup WAN port has already been configured. Then you select the WAN port that will act as the primary link for this mode and configure the **WAN Failure Detection Method** to support Auto-Rollover.

When the VPN firewall is configured in Auto-Rollover mode, the VPN firewall uses the **WAN Failure Detection Method** to check the connection of the primary link at regular intervals to detect its status. Link failure is detected in one of the following ways:

- By using DNS queries to a DNS server, or
- By a Ping to an IP address.

For each WAN interface, DNS queries or Ping requests are sent to the specified IP address. If replies are not received, the corresponding WAN interface is considered down.

To configure the dual WAN ports for Auto-Rollover

1. Select **Network Configuration** from the primary menu and **WAN Mode** from the secondary menu. The WAN Mode screen will display.
2. In the **Port Mode** section, check the **Auto-Rollover Using WAN port** radio box.
3. Selection the WAN port that will act as the primary link for this mode from the pull-down menu.
4. From the **WAN Failure detection Method** section, select the detection failure method radio box from one of the following choices:
   - **DNS lookup using configured DNS Servers (ISP DNS Servers)**. In this case, DNS queries are sent to the DNS server configured on the WAN ISP screens (see “Configuring the Internet Connections to Your ISPs” on page 2-2).
   - **DNS lookup using this DNS Server** (for example, a public DNS Server). Enter any public DNS server. DNS queries are sent to this server through the WAN interface being monitored.
   - **Ping to this IP address**. Enter a public IP address that will not reject the ping request or will not consider the traffic abuse. Queries are sent to this server through the WAN interface being monitored.

5. Enter a **Test Period** in seconds. DNS query is sent periodically after every test period. The default test period is 30 seconds.

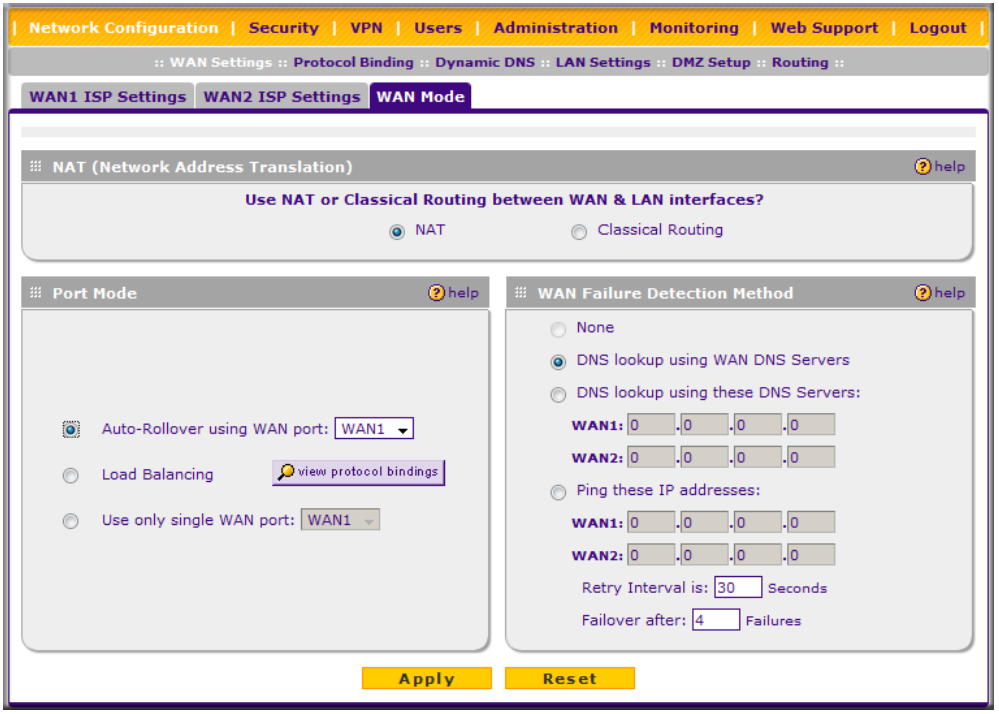


Figure 2-3

6. Enter the **Maximum Failover** amount. The WAN interface is considered down after the configured number of queries have failed to elicit a reply. The rollover link is brought up after this. The Failover default is 4 failures.

   The default time to roll over after the primary WAN interface fails is 2 minutes (a 30-second minimum test period, times a minimum of 4 tests).

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

8. Click **Reset** to revert to the previous settings.

Once a rollover occurs, an alert will be generated (see “Activating Notification of Events and Alerts” on page 6-23). When notified that the failed WAN interface has been restored, you can force traffic back on the original primary WAN interface by reapplying the Auto-Rollover settings in the WAN Port Mode menu.

Setting Up Load Balancing

To use multiple ISP links simultaneously, select Load Balancing. In Load Balancing mode, both links will carry data for the protocols that are bound to them. For example, if the HTTP protocol is bound to WAN1 and the FTP protocol is bound to WAN2, then the VPN firewall will automatically channel FTP data from and to the computers on the LAN through the WAN2 port. All HTTP traffic will be routed through the WAN1 port.

Note: NETGEAR recommends that all specific traffic (for example, HTTP) be configured for the WAN2 port. The only way to make certain traffic goes out one port and all other traffic goes out the other port is to use WAN2 for specified traffic.

Load Balancing can be used to segregate traffic between links that are not of the same speed. High volume traffic can be routed through the port connected to a high speed link and low volume traffic can be routed through the port connected to the low speed link.

To configure the dual WAN ports for load balancing with protocol binding:

1. Check the **Load Balancing** radio button on the WAN Mode screen shown in Figure 2-3 on page 2-10.
2. Click **view protocol bindings** (if protocol binding is needed)**.** The WAN1 Protocol Bindings screen will display.

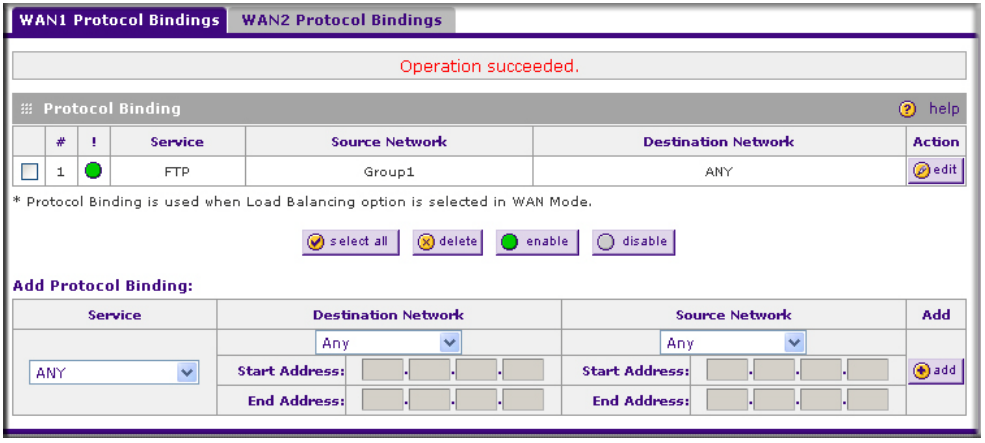


Figure 2-4

3. Enter the following data in the **Add Protocol Binding** section:

   a. **Service** – From the pull-down menu, select 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 4-3).

   b. **Destination Network** – 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.

   c. **Source Network**. 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.
      - **Group 1-Group 8**. If this option is selected, the devices assigned to this group will be affected. (You may also assign a customized name to the group. See **Edit Group Names** on the **Groups and Hosts** menu in the **LAN Groups** submenu.)

4. Click **Add** in the Add column adjacent to the rule**.** The new Protocol Binding Rule will be enabled and added to the Protocol Binding Table for the WAN1 port.

   Select the **WAN2 Protocol Bindings** tab, and repeat steps 1 through 9, to set protocol bindings for the WAN2 port.

To Edit or Add additional Protocol Binding settings:

1. Select **Network Configuration** from the main menu and **Protocol Binding** from the submenu. The WAN1 Protocol Bindings screen will display.

   You can add or edit protocol bindings to either the WAN1 port or click the **WAN2 Protocol Bindings** tab to access the WAN2 Protocol Bindings screen. To add a new protocol binding, following the preceding procedure.

2. Check the radio button adjacent to the protocol binding rule you want to modify. Click **Edit** in the Action column adjacent to the rule. The Edit Protocol Binding screen will display (see Figure 2-5 on page 2-13).

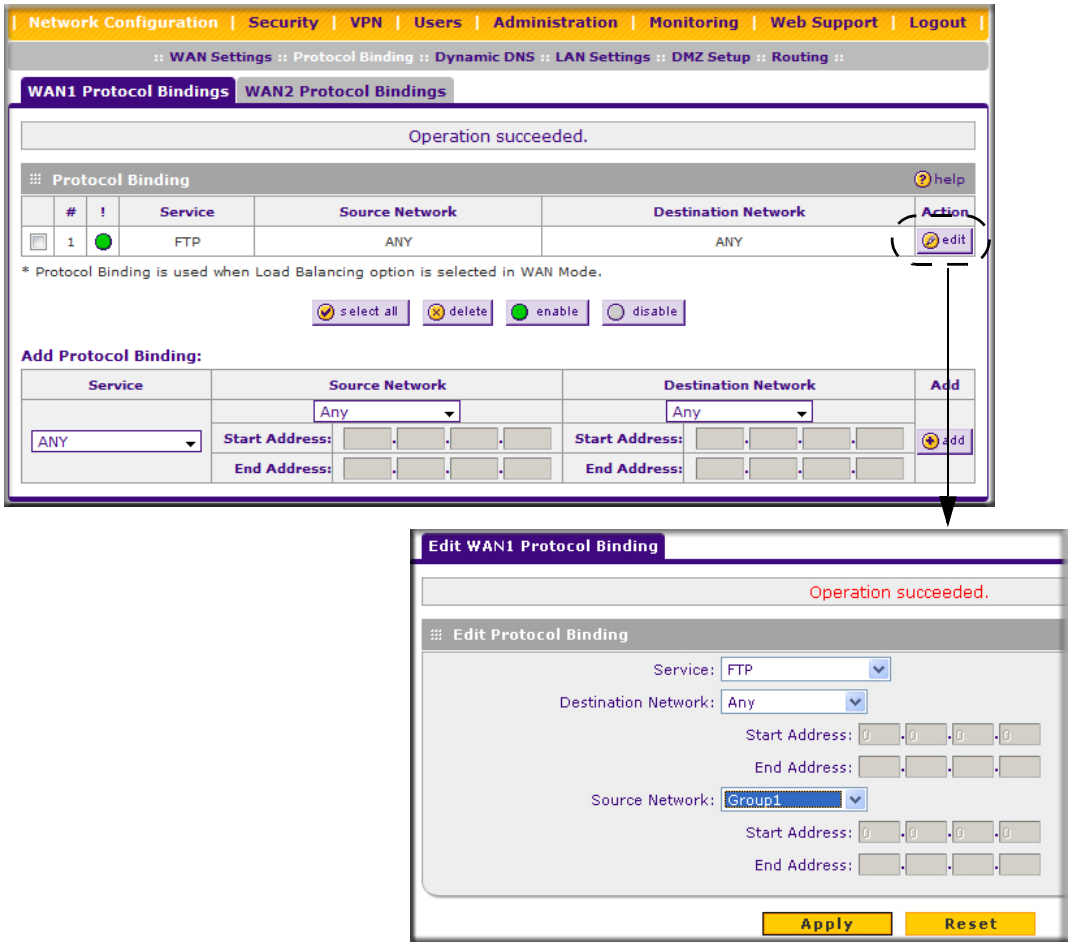


Figure 2-5

3. Modify the parameters for the protocol binding service you selected.
4. Click **Apply.** The modified rule will be enabled and appear in the Protocol Binding table.
5. Click **Reset** to return to the previously configured settings.

Configuring Dynamic DNS (Optional)

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, Oray.net, or 3322.org. Links to DynDNS, TZO, Oray, and 3322 are provided for your convenience on the Dynamic DNS Configuration screen. The VPN firewall 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.

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will not know in advance what your IP address will be, and the address can change frequently—hence, the need for a commercial DDNS service, which allows you to register an extension to its domain, and restores DNS requests for the resulting FQDN to your frequently-changing IP address.

After you have configured your account information in the VPN firewall, whenever your ISP-assigned IP address changes, your VPN firewall will automatically contact your DDNS service provider, log in to your account, and register your new IP address.

- For auto-rollover mode, you will need a fully qualified domain name (FQDN) to implement features such as exposed hosts and virtual private networks regardless of whether you have a fixed or dynamic IP address.
- For load balancing mode, you may still need a fully qualified domain name (FQDN) either for convenience or if you have a dynamic IP address.

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

To configure Dynamic DNS:

1. Select **Network Configuration** from the primary menu and **Dynamic DNS** from the submenu. The Dynamic DNS Configuration screen will display (see Figure 2-6 on page 2-15).

   The **WAN Mode** section displays the currently configured WAN mode (for example, Single Port WAN1, Load Balancing or Auto Rollover). Only those options that match the configured WAN Mode will be accessible.

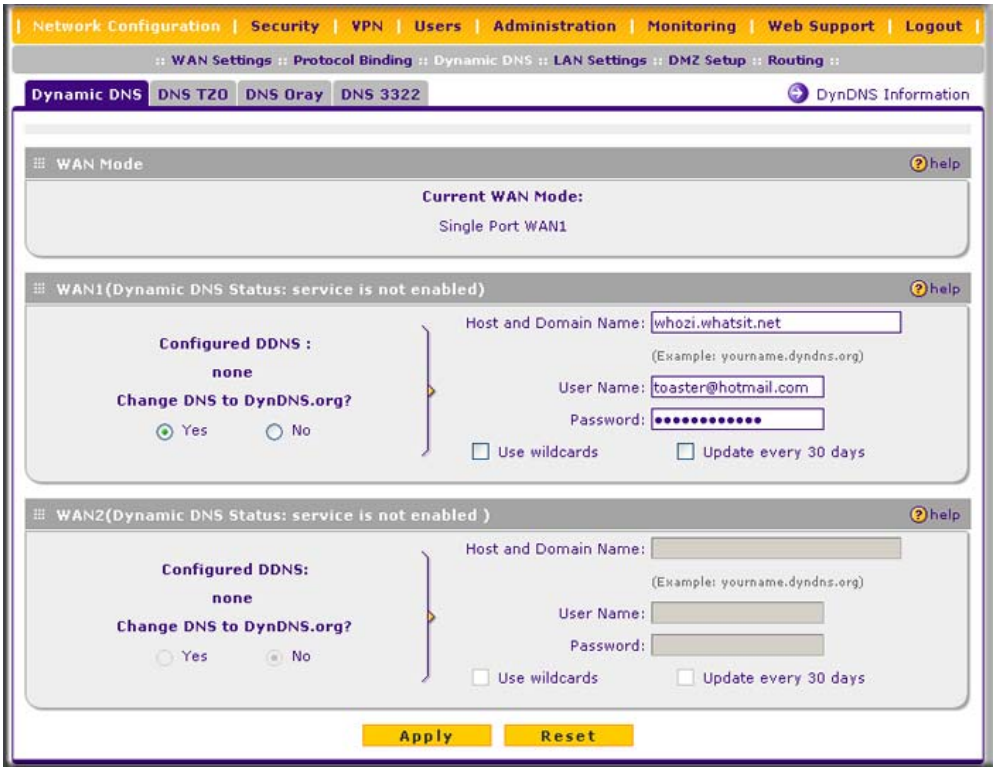


Figure 2-6

2. Click the tab of the Dynamic DNS Service you want to enable. Each DNS service provider requires registration and you then configure its parameters on the corresponding screen.
3. Access the website of one of the DDNS service providers and set up an account. A link to each DDNS provider is to the right of the tabs.
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 e-mail 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.
6. Click **Reset** to return to the previous settings.

Configuring the Advanced WAN Options (Optional)

To configure the advanced WAN options:

1. Select **Network Configuration** from the primary menu and **WAN Settings** from the submenu. The WAN Settings screen will display.
2. Click **Advanced** to access the WAN1 Advanced Options screen.

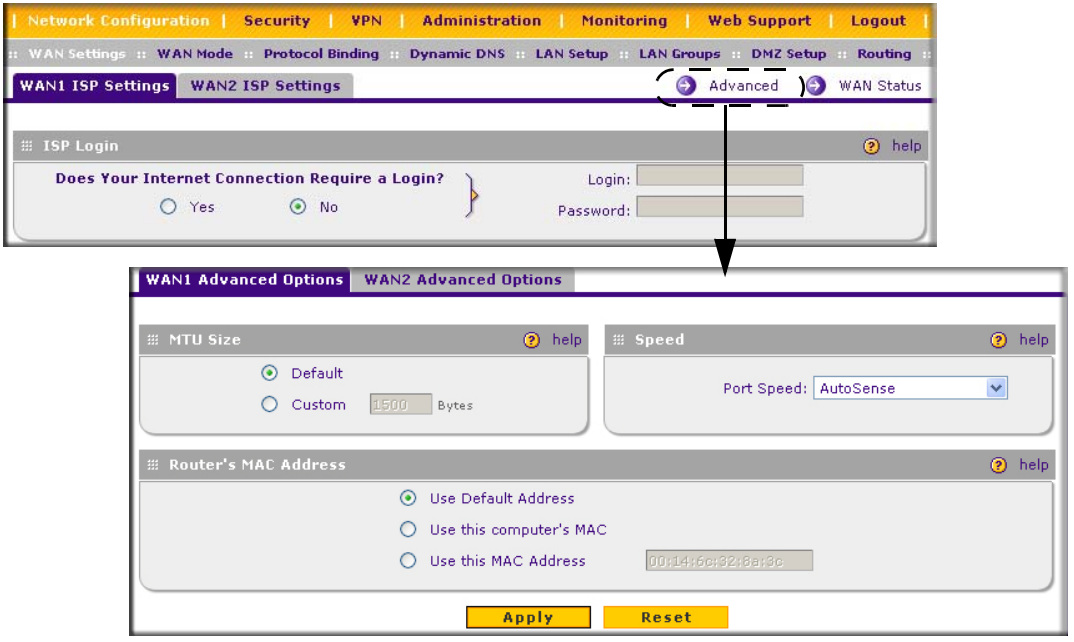


Figure 2-7

3. Edit the default information you want to change.

   - **MTU Size**. The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 Bytes, or 1492 Bytes for PPPoE connections. For some ISPs you may have to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
   - **Port Speed**. In most cases, your VPN firewall 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 have to manually select the port speed. AutoSense is the default.

     If you know that the Ethernet port on your broadband modem supports 100BaseT, select **100BaseT Half_Duplex**; otherwise, select **10BaseT Half_Duplex**. Use the half-duplex settings unless you are sure you need full duplex.
   - **Router's MAC Address**. Each computer or router on your network has a unique 32-bit local Ethernet address. This is also referred to as the computer's MAC (Media Access Control) address. The default is **Use Default Address**. However, if your ISP requires MAC authentication, then select either

     – **Use this Computer's MAC address** to enable the VPN firewall to use the MAC address of the computer you are now using, or

     – **Use This MAC Address** to manually type in the MAC address that your ISP expects.

     The format for the MAC address is XX:XX:XX:XX:XX:XX (numbers 0-9 and either uppercase or lowercase letters A-F). If you select **Use This MAC Address** and then type in a MAC address, your entry will be overwritten.

Additional WAN Related Configuration

- If you want the ability to manage the VPN firewalll remotely, enable remote management at this time (see "Enabling Remote Management Access" on page 6-14). If you enable remote management, NETGEAR strongly recommends that you change your password (see "Changing Passwords and Settings" on page 6-8).
- At this point, you can set up the traffic meter for each WAN, if desired. See "Enabling the Traffic Meter" on page 6-27.

Chapter 3
LAN Configuration

This chapter describes how to configure the advanced LAN features of your ProSafe VPN Firewall 200 FVX538, including the following sections:

- "Choosing the VPN Firewall DHCP Options" on this page
- "Managing Groups and Hosts (LAN Groups)" on page 3-6
- "Managing Groups and Hosts (LAN Groups)" on page 3-6
- "Configuring Multi Home LAN IP Addresses" on page 3-10
- "Configuring and Enabling the DMZ Port" on page 3-11
- "Configuring Static Routes" on page 3-14
- "Configuring Routing Information Protocol (RIP)" on page 3-16

Choosing the VPN Firewall DHCP Options

By default, the VPN 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 VPN firewall LAN. The assigned default gateway address is the LAN address of the VPN firewall. IP addresses will be assigned to the attached PCs from a pool of addresses that you must specify. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN. The DHCP options are available for both the LAN and DMZ settings.

For most applications, the default DHCP and TCP/IP settings of the VPN firewall are satisfactory. See the link to "TCP/IP Networking Basics" in Appendix E, "Related Documents for an explanation of DHCP and information about how to assign IP addresses for your network.

If another device on your network will be the DHCP server, or if you will manually configure the network settings of all of your computers, clear the **Enable DHCP server** radio box by selecting the **Disable DHCP Server** radio box. Otherwise, leave it checked.

Specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the VPN firewall's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.1.2 and 192.168.1.100, although you may wish to save part of the range for devices with fixed addresses.

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

- An IP address from the range that you have defined.
- Subnet mask.
- Gateway IP address (the VPN firewall's LAN IP address).
- Primary DNS server (the VPN firewall's LAN IP address).
- WINS server (if you entered a WINS server address in the **DHCP** section of the LAN Setup screen).
- Lease time (date obtained and duration of lease).

DHCP Relay options allow you to make the VPN firewall a DHCP relay agent. The DHCP Relay Agent makes it possible for DHCP broadcast messages to be sent over routers that do not support forwarding of these types of messages. The DHCP Relay Agent is therefore the routing protocol that enables DHCP clients to obtain IP addresses from a DHCP server on a remote subnet, or which is not located on the local subnet. If you have no configured DHCP Relay Agent, your clients would only be able to obtain IP addresses from the DHCP server which is on the same subnet. To enable clients to obtain IP addresses from a DHCP server on a remote subnet, you have to configure the DHCP Relay Agent on the subnet that contains the remote clients, so that it can relay DHCP broadcast messages to your DHCP server.

When the **DNS Proxy** option is enabled, the VPN firewallwill act as a proxy for all DNS requests and communicate with the ISP's DNS servers (as configured in the WAN settings screen). All DHCP clients will receive the Primary/Secondary DNS IP along with the IP address where the DNS proxy is running, that is, the VPN firewall's LAN IP address. When disabled, all DHCP clients will receive the DNS IP addresses of the ISP excluding the DNS proxy IP address. The feature is particularly useful in Auto Rollover mode. For example, if the DNS servers for each connection are different, then a link failure may render the DNS servers inaccessible. However, when the DNS proxy is enabled, then clients can make requests to the VPN firewall and the VPN firewall, in turn, sends those requests to the DNS servers of the active connection.

Configuring the LAN Setup Options

The LAN Setup screen allows configuration of LAN IP services such as DHCP and allows you to configure a secondary or "multi-home" LAN IP setup in the LAN. The default values are suitable for most users and situations. Disable the DNS Proxy if you are using a dual WAN configuration with route diversity and failover. These are advanced settings most usually configured by a network administrator.

Note: If you enable the DNS Relay feature, you will not use the VPN firewall as a DHCP server but rather as a DHCP relay agent for a DHCP server somewhere else on your network.

To configure the LAN Setup options:

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

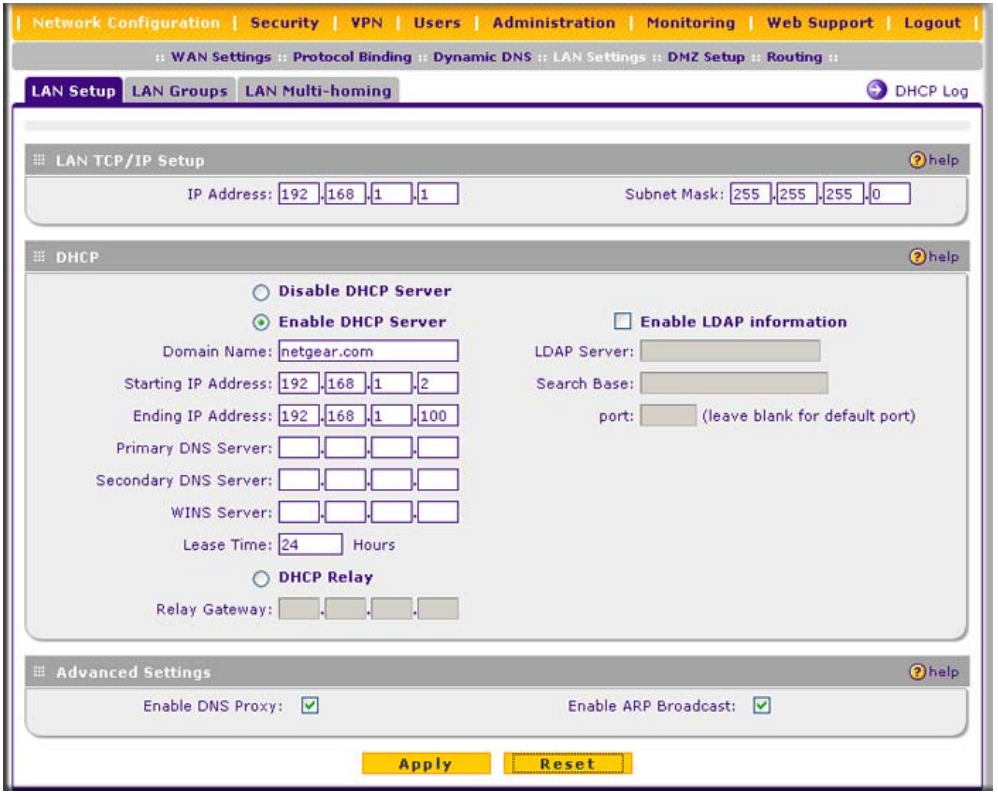


Figure 3-1

2. In the **LAN TCP/IP Setup** section, configure the following settings:
   - **IP Address**. The LAN address of your VPN firewall (factory default: **192.168.1.1**).

> **Note:** If you change the LAN IP address of the VPN 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 now enter **https://10.0.0.1** in your browser to reconnect to the Web Configuration Manager.

- **IP Subnet Mask**. The subnet mask specifies the network number portion of an IP address. Your VPN firewall 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. (Always make sure that the LAN Port IP address and DMZ port IP address are in different subnets.)

3. In the **DHCP** section, select **Disable DHCP Server**, **Enable DHCP Server**, or **DHCP Relay**. By default, the VPN firewall will function as a DHCP server, providing TCP/IP configuration settings for all computers connected to the VPN firewall's LAN. If another device on your network will be the DHCP server, or if you will manually configure all devices, click **Disable DHCP Server**. If the VPN firewall will function as a DHCP relay agent, select **DHCP Relay** and enter the IP address of the DHCP relay gateway in the Relay Gateway field.

   If the DHCP server is enabled, enter the following parameters:

   - **Domain Name.** (Optional) The DHCP will assign the entered domain to DHCP clients.
   - **Starting IP 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.
   - **Ending IP Address**. Specifies the last of the contiguous addresses in the IP address pool. The IP address 192.168.1.100 is the default ending address.

   > **Note:** The starting and ending DHCP addresses should be in the same subnet as the LAN IP address of the VPN firewall (the IP address that is configured in the **LAN TCP/IP Setup** section of the LAN Setup screen).

   - **Primary DNS Server**. (Optional) If an IP address is specified, the VPN firewall will provide this address as the primary DNS server IP address. If no address is specified, the VPN firewall will provide its own LAN IP address as the primary DNS server IP address.
   - **Secondary DNS Server**. (Optional) If an IP address is specified, the VPN firewall will provide this address as the secondary DNS server IP address.

- **WINS Server**. (Optional) Specifies the IP address of a local Windows NetBIOS Server if one is present in your network.
- **Lease Time.** This specifies the duration for which IP addresses will be leased to clients.

If you will use a Lightweight Directory Access Protocol (LDAP) authentication server for network-validated domain-based authentication, select **Enable LDAP Information** to enable the DHCP server to provide LDAP server information. Enter the following parameters:

- **LDAP Server**. Specifies the name or the IP address of the device that hosts the LDAP server.
- **Search Base**. Specifies the distinguished name (dn) at which to start the search, specified as a sequence of relative distinguished names (rdn), connected with commas and without any blank spaces. For most users, the search base is a variation of the domain name. For example, if your domain is yourcompany.com, your search base dn might be as follows: dc=yourcompany,dc=com.
- **port**. Specifies the port number that the LDAP server is using. Leave this field blank for the default port.

4. In the **Advanced Settings** section, configure the following settings:
   - **Enable DNS Proxy**. If the DNS proxy is enabled (which is the default setting), the DHCP server will provide the VPN firewall's LAN IP address as the DNS server for address name resolution. If this box is unchecked, the DHCP server will provide the ISP's DNS server IP addresses. The VPN firewall will still service DNS requests sent to its LAN IP address unless you disable DNS Proxy in the VPN firewall settings (see "Attack Checks" on page 4-20).
   - **Enable ARP Broadcast**. If ARP broadcast is enabled (which is the default setting), the Address Resolution Protocol (ARP) is broadcasted on the LAN so that IP addresses can be mapped to physical addresses (that is, MAC addresses).
5. Click **Apply** to save your settings or 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."

Managing Groups and Hosts (LAN Groups)

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 VPN firewall. Collectively, these entries make up the Network Database.

The Network Database is updated by these methods:

- **DHCP Client Requests**. By default, the DHCP server in this VPN firewall 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.
- **Manual Entry**. You can manually enter information about a network device.

Creating the Network Database

Some advantages of the Network Database are:

- 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 address on PCs. Because the address allocated by the DHCP Server will never change, you do not need to assign a fixed IP address 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 "Using Rules to Block or Allow Specific Kinds of Traffic" on page 4-2).
  - You can also select the groups to be covered by the Block Sites feature (see "Blocking Internet Sites (Content Filtering)" on page 4-30).

– If necessary, you can also create firewall rules to apply to a single PC (see "Configuring Source MAC Filtering" on page 4-33). 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.

Viewing the Network Database

To view the Network Database, follow these steps:

1. Select **Network Configuration** from the primary menu and **LAN Settings** from the submenu. The LAN Setup screen will display.
2. Click the **LAN Groups** tab. The LAN Groups screen will display.

Figure 3-2

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

- **Name**. The name of the computer or device. Computers that do not support the NetBIOS protocol will be listed as Unknown. In this case, the name can be edited manually for easier management. If the computer was assigned an IP address by the DHCP server, then an asterisk is be appended to the name.
- **IP Address**. The current IP address of the computer. For DHCP clients of the VPN firewall, this IP address will not change. If a computer is assigned a static IP address, you must to update this entry manually when the IP address of the computer changes.

- **MAC Address**. The MAC address of the computer's network interface.
- **Group**. Each PC or device can be assigned to a single group. By default, a computer is assigned to the first group (Group 1). To change the group assignment by selecting the **Edit** link in the **Action** column.
- **Action/Edit**. Allows modification of the selected entry.

Adding Devices to the Network Database

To add devices manually to the Network Database:

1. To add computers to the network database manually, fill in the following fields:
   - **Name**: The name of the PC or device.
   - **IP Address Type**. From the pull-down menu, choose how this device receives its IP address:
     - Select **Fixed (Set on PC)** if the IP address is statically assigned on the computer.
     - Select **Reserved (DHCP Client)** to direct the VPN firewall to reserve the IP address for allocation by the DHCP server (see "Setting Up DHCP Address Reservation" on page 3-9).

     Note: When assigning a reserved IP address to a client, the IP address selected must be outside the range of addresses allocated to the DHCP server pool.

   - **IP Address**. The IP address that this computer or device is assigned. If the IP Address Type is **Reserved (DHCP Client)**, the VPN firewall will reserve the IP address for the associated MAC address.
   - **MAC Address**. The MAC address of the computer's network interface. The MAC address format is six colon-separated pairs of hexadecimal characters (0-9 and A-F), such as 01:23:45:67:89:AB.
   - **Group**. The group to which the computer has to be assigned. (Group 1 is the default group.)
2. Click **Add** to add the new entry to the network database.
3. As an optional step: To enable DHCP address reservation for the entry that you just added to the Known PCs and Devices table, select the checkbox for the table entry and click **Save Binding** to bind the IP address to the MAC address for DHCP assignment.

Changing Group Names in the LAN Groups Database

By default, the LAN Groups are named Group1 through Group8. You can rename these group names to be more descriptive, such as Engineering or Marketing.

To edit the names of any of the eight available groups:

1. From the **LAN Groups** screen, click the **Edit Group Names** link to the right of the tabs. The Network Database Group Names screen appears.

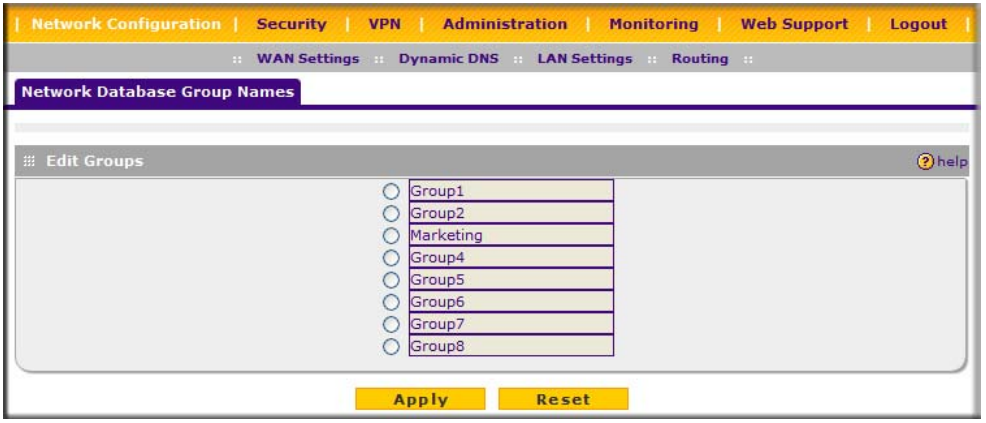


Figure 3-3

2. Select the radio button next to any group name to make that name active for editing.
3. Type a new name in the field.
4. Select and edit other group names if desired.
5. Click **Apply** to save your settings.

Setting Up DHCP 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 VPN 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, manually enter the device on the LAN Groups screen, specifying **Reserved (DHCP Client)**, as described in “Adding Devices to the Network Database” on page 3-8.

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

Configuring Multi Home LAN IP Addresses

If you have computers on your LAN using different IP address ranges (for example, 172.16.2.0 or 10.0.0.0), you can add “aliases” to the LAN port, giving computers on those networks access to the Internet through the VPN firewall. This allows the VPN firewall to act as a gateway to additional logical subnets on your LAN. You can assign the VPN firewall an IP address on each additional logical subnet.

To add a secondary LAN IP address:

1. Select **Network Configuration** from the primary menu and **LAN Settings** from the submenu. The LAN Setup screen will display.
2. Click the **LAN Multi-homing** tab. The LAN Multi-homing screen will display.

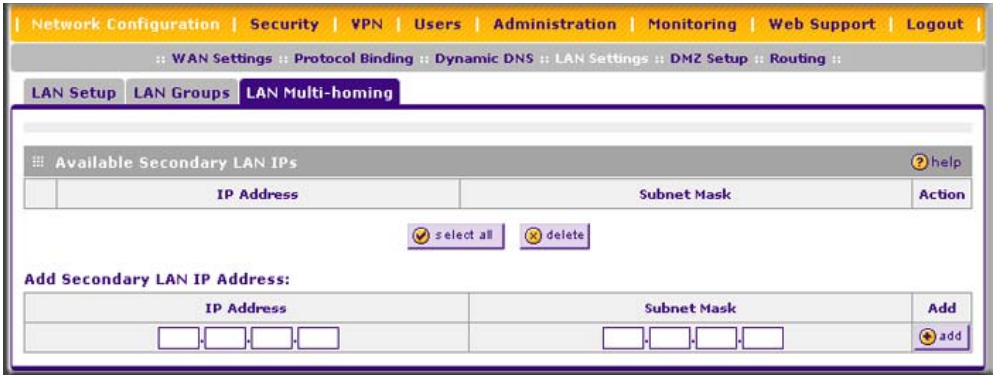


Figure 3-4

The Available Secondary LAN IPs table lists the secondary LAN IP addresses added to the VPN firewall.

- **IP Address**. The IP address alias added to the LAN port of the VPN firewall. This is the gateway for computers that need to access the Internet.
- **Subnet Mask**. IPv4 Subnet Mask.
- **Action**. The Edit link allows you to make changes to the selected entry.
- **Select All**. Selects all the entries in the Available Secondary LAN IPs table.
- **Delete**. Deletes selected entries from the Available Secondary LAN IPs table.

3. Type in the IP Address and the Subnet Mask in the respective text fields.
4. Click **Add**. The Secondary LAN IP address will be added to the 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 the IP addresses, gateway IP and DNS server IPs.

Warning: Make sure the secondary IP addresses are different from the LAN, WAN, DMZ, and any other subnet attached to this VPN firewall.
For example:
WAN1 IP address: 10.0.0.1 with subnet 255.0.0.0
WAN2 IP address: 20.0.0.1 with subnet 255.0.0.0
DMZ IP address: 192.168.10.1 with subnet 255.255.255.0
LAN IP address: 192.168.1.1 with subnet 255.255.255.0
Secondary LAN IP: 192.168.20.1 with subnet 255.255.255.0

Configuring and Enabling the DMZ Port

The De-Militarized Zone (DMZ) is a network which, when compared to the LAN, has fewer firewall restrictions, by default. This zone can be used to host servers (such as a web server, ftp server, or e-mail server, for example) and give public access to them. The eighth LAN port on the VPN firewall can be dedicated as a hardware DMZ port for safely providing services to the Internet, without compromising security on your LAN.

The DMZ port feature is also helpful when using some online games and videoconferencing applications that are incompatible with NAT. The VPN firewall is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, local PCs can run the application properly if those PCs are used on the DMZ port.

Note: A separate firewall security profile is provided for the DMZ port that is hardware independent of the standard firewall security used for the LAN.

The DMZ Setup screen allows you to set up the DMZ port. It permits you to enable or disable the hardware DMZ port (LAN port 8, see "VPN Firewall Front and Rear Panels" on page 1-6) and configure an IP address and Mask for the DMZ port.

To enable and configure the DMZ port:

1. From the main menu, select **Network Configuration** and then select **DMZ Setup** from the submenu. The DMZ Setup screen will display.
2. Check the **Do you want to enable DMA Port?** radio box.
3. Enter an IP address and the subnet mask for the DMZ port. Make sure that the DMZ port IP address and LAN Port IP address are in different subnets (for example, an address outside the LAN Address pool, such as 192.168.1.101).

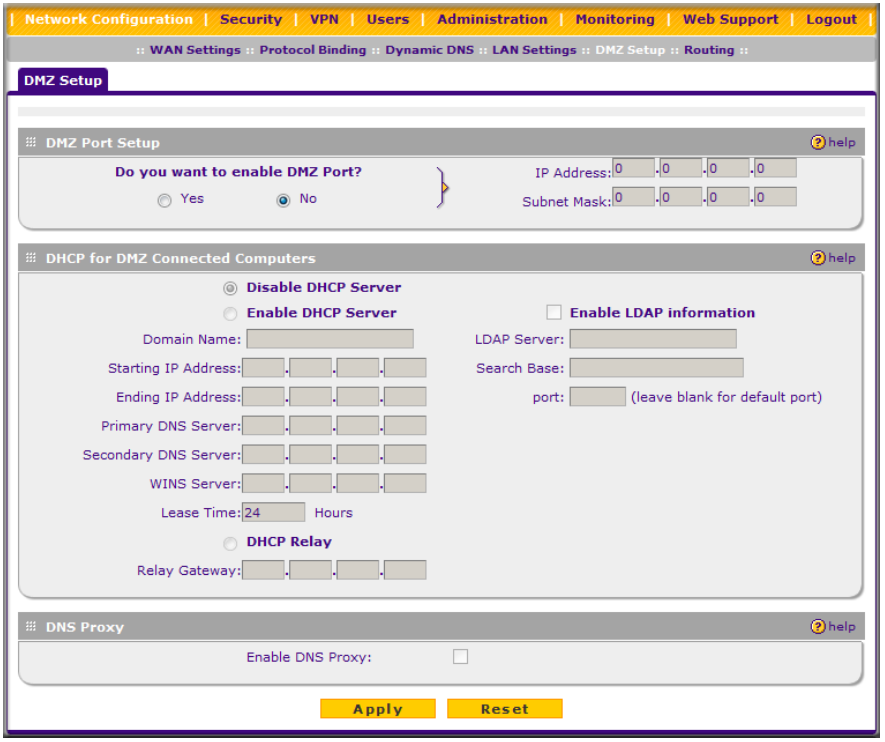


Figure 3-5

If desired, select **Enable DHCP Server**, which will provide TCP/IP configuration for all computers connected to the VPN firewall's DMZ network. If another device on your DMZ network will be the DHCP server, or if you will manually configure all devices, leave the **Disable DHCP Server** radio box selected, which is the default setting.

If the DHCP server is enabled, enter the following parameters:

- **Domain Name.** (Optional) The DHCP will assign the entered domain to DHCP clients.
- **Starting IP 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.
- **Ending IP Address**. Specifies the last of the contiguous addresses in the IP address pool. The IP address 192.168.1.100 is the default ending address.

Note: The Starting and Ending DHCP addresses should be in the same subnet as the LAN IP address of the VPN firewall (the IP Address configured in the **LAN TCP/IP Setup** section).

- **Primary DNS Server**. (Optional) If an IP address is specified, the VPN firewall will provide this address as the primary DNS server IP address. If no address is specified, the VPN firewall will provide its own LAN IP address as the primary DNS server IP address.
- **Secondary DNS Server**. (Optional) If an IP address is specified, the VPN firewall will provide this address as the secondary DNS server IP address.
- **WINS Server**. (Optional) Specifies the IP address of a local Windows NetBIOS Server if one is present in your network.
- **Lease Time.** This specifies the duration for which IP addresses will be leased to clients.

If you will use a Lightweight Directory Access Protocol (LDAP) authentication server for network-validated domain-based authentication, select **Enable LDAP Information** to enable the DHCP server to provide LDAP server information. Enter the following parameters:

- **LDAP Server**. Specifies the name or the IP address of the device that hosts the LDAP server.
- **Search Base**. Specifies the distinguished name (dn) at which to start the search, specified as a sequence of relative distinguished names (rdn), connected with commas and without any blank spaces. For most users, the search base is a variation of the domain name. For example, if your domain is yourcompany.com, your search base dn might be as follows: dc=yourcompany,dc=com.

- **port**. Specifies the port number that the LDAP server is using. Leave this field blank for the default port.

4. In the **Advanced Settings** section, select **Enable DNS Proxy** if you want to enabled the DNS proxy, which is the default setting. The DHCP server will provide the VPN firewall's LAN IP address as the DNS server for address name resolution. If this box is unchecked, the DHCP server will provide the ISP's DNS server IP addresses. The VPN firewall will still service DNS requests sent to its LAN IP address unless you disable DNS Proxy in the VPN firewall's settings (see "Attack Checks" on page 4-20).
5. Click **Apply** to save your settings or click **Reset** to discard any changes and revert to the previous configuration. The DMZ LED next to LAN port 8 (see "VPN Firewall Front and Rear Panels" on page 1-6) will light up indicating that the DMZ port has been enabled.

To define the DMZ WAN Rules and LAN DMZ Rules, see "Configuring DMZ WAN Rules" on page 4-12 and "Configuring LAN DMZ Rules" on page 4-13, respectively.

Configuring Static Routes

Static Routes provide additional routing information to your VPN firewall. Under normal circumstances, the VPN firewall has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You should 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.

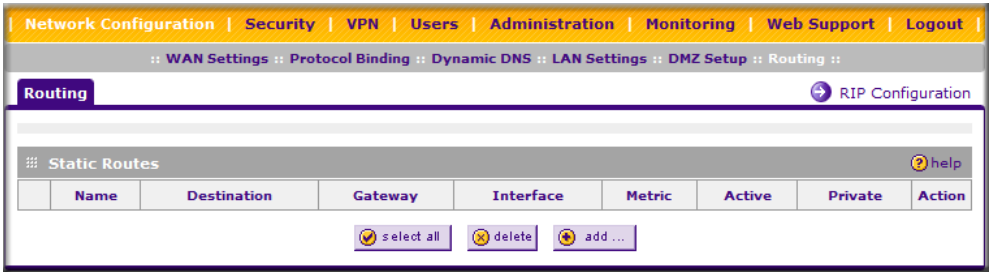


Figure 3-6

2. Click **Add**. The Add Static Route screen will display.

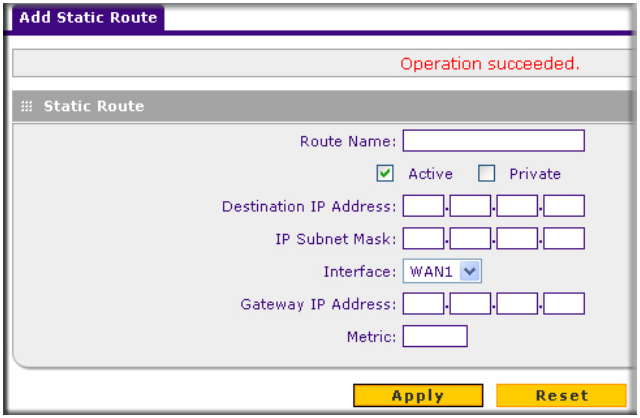


Figure 3-7

3. Enter a route name for this static route in the **Route Name** field (for identification and management).
4. Select **Active** to make this route effective.
5. Select **Private** if you want to limit access to the LAN only. The static route will not be advertised in RIP.
6. Enter the destination IP Address to the host or network to which the route leads.
7. Enter the IP subnet mask for this destination. If the destination is a single host, enter 255.255.255.255.
8. Select the physical network interface (WAN1, WAN2, or LAN) through which this route is accessible.
9. Enter the gateway IP address through which the destination host or network can be reached (must be a device on the same LAN segment as the VPN firewall).
10. Enter the metric priority for this route. If multiple routes to the same destination exit, the route with the lowest metric is chosen. (value must be between 1 and 15),
11. Click **Reset** to discard any changes and revert to the previous settings or click **Apply** to save your settings.

    The new static route will be added to Static Routes table.

You can edit the route's settings by clicking **Edit** in the Action column adjacent to the route.

Static Route Example

For example, you may require a static route 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 VPN 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 VPN 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 VPN 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.

Configuring Routing Information Protocol (RIP)

RIP (Routing Information Protocol, RFC 2453) is an Interior Gateway Protocol (IGP) that is commonly used in internal networks (LANs). 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.

To configure RIP:

1. Select **Network Configuration** from the main menu and **Routing** from the submenu. The Routing screen will display (see Figure 3-6 on page 3-14).

2. Click **RIP Configuration** link to the right of the Routing tab**.** The RIP Configuration screen will display.

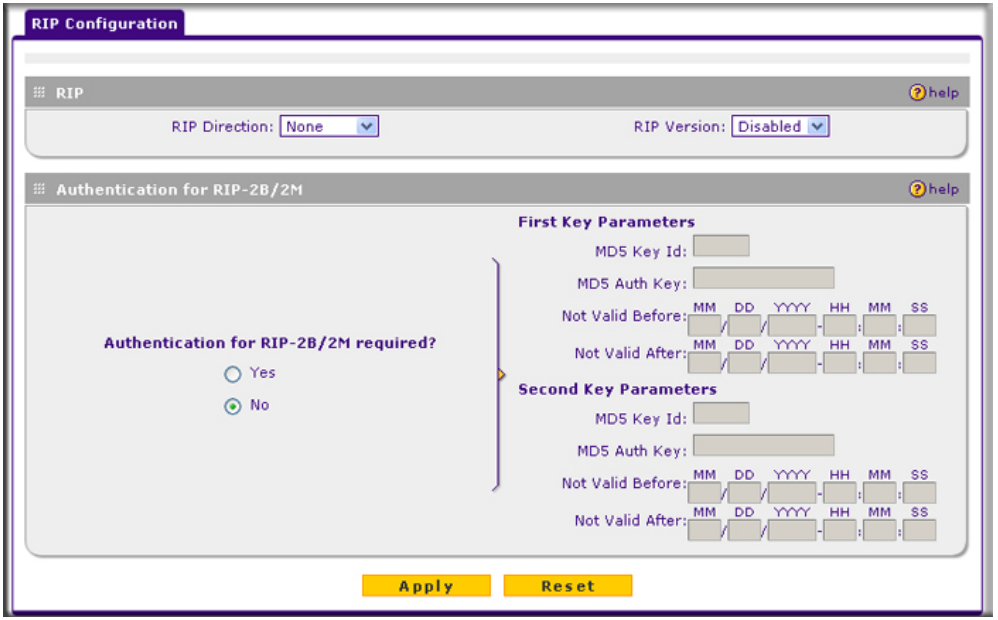


Figure 3-8

3. From the **RIP Direction** pull-down menu, select the direction in which the VPN firewall will send and receives RIP packets. The choices are:

   - **None**. The VPN firewall neither broadcasts its route table nor does it accept any RIP packets from other routers. This effectively disables RIP.
   - **Both**. The VPN firewall broadcasts its routing table and also processes RIP information received from other routers.
   - **Out Only**. The VPN firewall broadcasts its routing table periodically but does not accept RIP information from other routers.
   - **In Only**. The VPN firewall accepts RIP information from other routers, but does not broadcast its routing table.

4. From the **RIP Version** pull-down menu, select the version:

   - **Disabled**. The default section disables RIP versions.
   - **RIP-1**. A class-based routing that does not include subnet information. This is the most commonly supported version.

- **RIP-2**. This includes all the functionality of RIPv1 plus it supports subnet information. Though the data is sent in RIP-2 format for both RIP-2B and RIP-2M, the modes in which packets are sent are different.
  - **RIP-2B**. Sends the routing data in RIP-2 format and uses subnet broadcasting.
  - **RIP-2M**. Sends the routing data in RIP-2 format and uses multicasting.

5. **Authentication for RIP2B/2M required?** If you selected RIP-2B or RIP-2M, check the **Yes** radio box to enable authentication, and enter the MD-5 keys to authenticate between devices in the **First Key Parameters** and **Second Key Parameters** sections on the screen.
6. Click **Reset** to discard any changes and revert to the previous settings or click **Apply** to save your settings.

Chapter 4
Firewall Protection and Content Filtering

This chapter describes how to use the content filtering features of the ProSafe VPN Firewall 200 FVX538 to protect your network.

This chapter includes the following sections:

- "About Firewall Protection and Content Filtering" on this page
- "Using Rules to Block or Allow Specific Kinds of Traffic" on page 4-2
- "Configuring Other Firewall Features" on page 4-19
- "Creating Services, QoS Profiles, and Bandwidth Profiles" on page 4-24
- "Setting a Schedule to Block or Allow Specific Traffic" on page 4-29
- "Blocking Internet Sites (Content Filtering)" on page 4-30
- "Configuring Source MAC Filtering" on page 4-33
- "Configuring IP/MAC Address Binding" on page 4-35
- "Configuring Port Triggering" on page 4-37
- "Administrator Tips" on page 4-40

About Firewall Protection and Content Filtering

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

A firewall is a special category of router that protects one network (the "trusted" network, such as your LAN) from another (the untrusted network, such as the Internet), while allowing communication between the two. You can further segment keyword blocking to certain known groups (see "Managing Groups and Hosts (LAN Groups)" on page 3-6 to set up LAN Groups).

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

This section includes the following topics:

- "Services-Based Rules" on this page
- "Viewing Rules and Order of Precedence for Rules" on page 4-7
- "Configuring LAN WAN Rules" on page 4-9
- "Configuring DMZ WAN Rules" on page 4-12
- "Configuring LAN DMZ Rules" on page 4-13
- "Inbound Rules Examples" on page 4-15
- "Outbound Rules Example" on page 4-19

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 VPN firewall. 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 VPN firewall 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.

The firewall rules for blocking/allowing traffic on the VPN firewall can be applied to LAN/WAN traffic, DMZ/WAN traffic and LAN/DMZ traffic.

Table 4-1. Supported FIrewall Rule Configurations

Traffic Rule	Outbound Rules	Inbound Rules
LAN WAN	50	50
DMZ WAN	50	50
LAN DMZ	50	50

Services-Based Rules

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

- **Outbound Rules (service blocking)**. Outbound traffic is normally allowed unless the VPN firewall is configured to disallow it.
- **Inbound Rules (port forwarding)**. Inbound traffic is normally blocked by the VPN firewall unless the traffic is in response to a request from the LAN side. The VPN firewall can be configured to allow this otherwise blocked traffic.
- **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 (see "Adding Customized Services" on page 4-24).
- **Quality of Service (QoS) priorities**. Each service has its own native priority that impacts its quality of performance and tolerance for jitter or delays. You can change the QoS priority which will change the traffic mix through the system (see "Specifying Quality of Service (QoS) Priorities" on page 4-26).

Outbound Rules (Service Blocking)

The VPN firewall 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 "Configuring Source MAC Filtering" on page 4-33 for yet another way to block outbound traffic from selected PCs that would otherwise be allowed by the VPN firewall.

Table 4-2. Outbound Rules

Item	Description
Service	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 4-24).
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 that 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.

Table 4-2. Outbound Rules (continued)

Item	Description
Select Schedule	Select the desired time schedule (Schedule1, Schedule2, or Schedule3) that will be used by this rule. • This pull-down menu gets activated only when “BLOCK by schedule, otherwise Allow” or “ALLOW by schedule, otherwise Block” is selected as Action. • Use schedule screen to configure the time schedules (see “Setting a Schedule to Block or Allow Specific Traffic” on page 4-29).
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 to which this rule will apply. Use the LAN Groups screen (under Network Configuration) to assign PCs to Groups. See “Managing Groups and Hosts (LAN Groups)” on page 3-6.
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 field. • Address range – If this option is selected, you must enter the start and end fields.
DMZ Users	These settings determine which DMZ computers on the DMZ network are affected by this rule. Select the desired options. • Any – All PCs and devices on your DMZ network. • Single address – Enter the required address and the rule will be applied to that particular PC on the DMZ network. • Address range – If this option is selected, you must enter the start and finish fields of the DMZ computers.
QoS Priority	Specifies the priority of a service which, in turn, determines the quality of that service for the traffic passing through the VPN 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 (leaves it as Normal-Service), then the native priority of the service will be applied to the policy. See “Specifying Quality of Service (QoS) Priorities” on page 4-26.
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.

Table 4-2. Outbound Rules (continued)

Item	Description
Bandwidth Profile	Bandwidth Limiting determines the way in which the data is sent to/from your host. The purpose of bandwidth limiting is to provide a solution for limiting the outgoing/incoming traffic, thus preventing the LAN users for consuming all the bandwidth of our internet link. Bandwidth Limiting for outbound traffic will be done on the available WAN interface in the single port and Auto-Failover modes. The limiting will be done on the user-specified interface in Load Balancing mode. The bandwidth limiting for inbound traffic will be done on the LAN interface for all WAN modes. Bandwidth Limiting will not apply to the DMZ interface. See "Creating Bandwidth Profiles" on page 4-27.
NAT IP	Specifies whether the source IP address of the outgoing packets should be the WAN interface address or a specified address, which should belong to the WAN subnet.
NAT Single IP Is On (interface)	Specifies to which WAN interface the NAT IP address belongs. All outgoing packets will be routed through the specified WAN interface only.

Inbound Rules (Port Forwarding)

Because the VPN firewall 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 VPN 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, how the PCs will access the server's LAN address impacts 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 dynamic DNS so that external users can always find your network (see "Configuring Dynamic DNS (Optional)" on page 2-14).
- 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 to keep the PC's IP address constant (see "Setting Up DHCP Address Reservation" on page 3-9).
- Local PCs must access the local server using the PCs' local LAN address. Attempts by local PCs to access the server using the external WAN IP address will fail.

Note: See "Configuring Port Triggering" on page 4-37 for yet another way to allow certain types of inbound traffic that would otherwise be blocked by the VPN firewall.

Table 4-3. Inbound Rules

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 screen (see "Adding Customized Services" on page 4-24).
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 (that is, Schedule1, Schedule2, or Schedule3) that will be used by this rule (see "Setting a Schedule to Block or Allow Specific Traffic" on page 4-29). • This pull-down menu gets activated only when "BLOCK by schedule, otherwise Allow" or "ALLOW by schedule, otherwise Block" is selected as Action. • Use the schedule screen to configure the time schedules.
Send to LAN Server	This field appears only with NAT routing (not classical routing). This LAN address or range of LAN addresses determines which computer or computers on your network are hosting this service rule. (You can also translate these addresses to a port number.)
Send to DMZ Server	The DMZ server 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 Destination IP Address	This setting determines the destination IP address applicable to incoming traffic. This is the public IP address that will map to the internal LAN server; it can either be the address of the WAN1 or WAN2 ports or another public IP address**.**
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 to which this rule will apply. Use the LAN Groups screen (under Network Configuration) to assign PCs to Groups. See "Managing Groups and Hosts (LAN Groups)" on page 3-6.
WAN Users	These settings determine which Internet locations are covered by the rule, based on their IP addresses. Select the desired option: • Any – All Internet IP address are covered by this rule. • Single address – Enter the required address in the start field. • Address range – If this option is selected, you must enter the start and end fields.

Table 4-3. Inbound Rules (continued)

Item	Description
Log	This determines whether packets covered by this rule are logged. Select the desired action: • Always – Always log traffic considered by this rule, whether it matches or not. This is useful when debugging your rules. • Never – Never log traffic considered by this rule, whether it matches or not.
Bandwidth Profile	Bandwidth Limiting determines the way in which the data is sent to/from your host. The purpose of bandwidth limiting is to provide a solution for limiting the outgoing/incoming traffic, thus preventing the LAN users for consuming all the bandwidth of our internet link. Bandwidth Limiting for outbound traffic will be done on the available WAN interface in the single port and Auto-Failover modes. The limiting will be done on the user-specified interface in Load Balancing mode. The bandwidth limiting for inbound traffic will be done on the LAN interface for all WAN modes. Bandwidth Limiting will not apply to the DMZ interface. See “Creating Bandwidth Profiles” on page 4-27.

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.

Viewing Rules and Order of Precedence for Rules

To view the firewall rules, select **Security** from the main menu and **Firewall** from the submenu. The LAN WAN Rules screen appears (Figure 4-1 on page 4-8 shows some examples). As you define new rules, they are added to the tables in the Rules menu as the last item in the list.

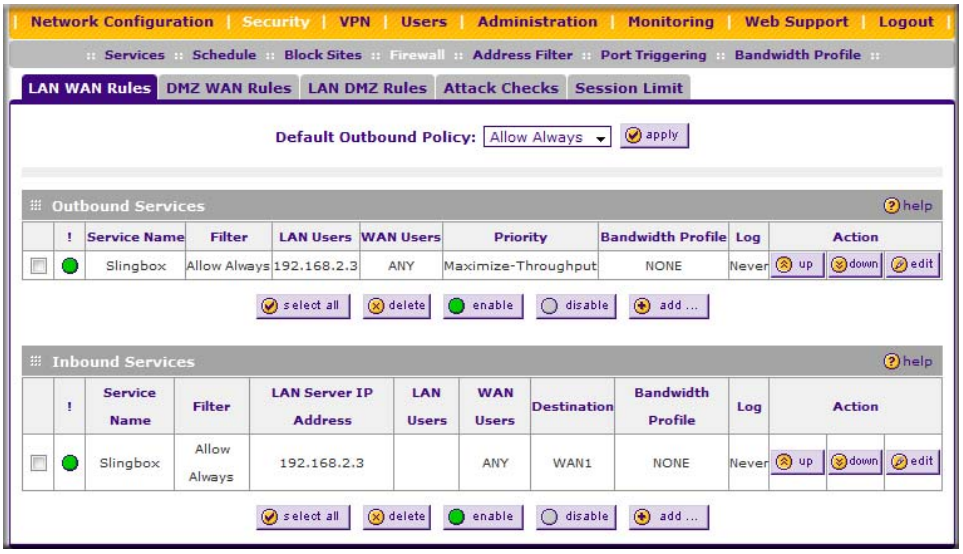


Figure 4-1

For LAN WAN rules, DMZ WAN rules, and LAN DMZ rules, for any traffic attempting to pass through the VPN firewall, the packet information is subjected to the rules in the order shown in the **Outbound Services** and **Inbound Services** rules tables rules tables, beginning at the top and proceeding to 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** button allows you to relocate a defined rule to a new position in the table (see below).

To make changes to an existing outbound or inbound service rule on the the LAN WAN Rules, DMZ WAN Rules, or LAN DMZ Rules screen, in the Action column to the right of to the rule, click on of the following table buttons:

- **edit**. Allows you to make any changes to the rule definition of an existing rule. Depending on your selection, either an Edit Outbound Service screen or Edit Inbound Service screen displays, containing the data for the selected rule.
- **up**. Moves the rule up one position in the table rank.
- **down**. Moves the rule down one position in the table rank.

To enable, disable, or delete one or more rules on the LAN WAN Rules, DMZ WAN Rules, or LAN DMZ Rules screen:

1. Select the checkbox to the left of the rule that you want to delete or disable or click the **select all** table button to select all rules.

2. Click one of the following table buttons:

   - **enable**. Enables the rule or rules. The "!" status icon changes from a grey circle to a green circle, indicating that the rule is or rules are enabled. (By default, when a rule is added to the table, it is automatically enabled.)
   - **disable**. Disables the rule or rules. The "!" status icon changes from a green circle to a grey circle, indicating that the rule is or rules are disabled.
   - **delete**. Deletes the rule or rules.

To add a new rule, click **Add**. For more information, see "Configuring LAN WAN Rules" on this page, "Configuring DMZ WAN Rules" on page 4-12, and "Configuring LAN DMZ Rules" on page 4-13.

Configuring LAN WAN Rules

The default outbound policy is to allow all traffic to the Internet to pass through. Firewall rules can then be applied to block specific types of traffic from going out from the LAN to the Internet (outbound). The default policy of Allow Always can be changed to block all outbound traffic which then allows you to enable only specific services to pass through the VPN firewall.

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.

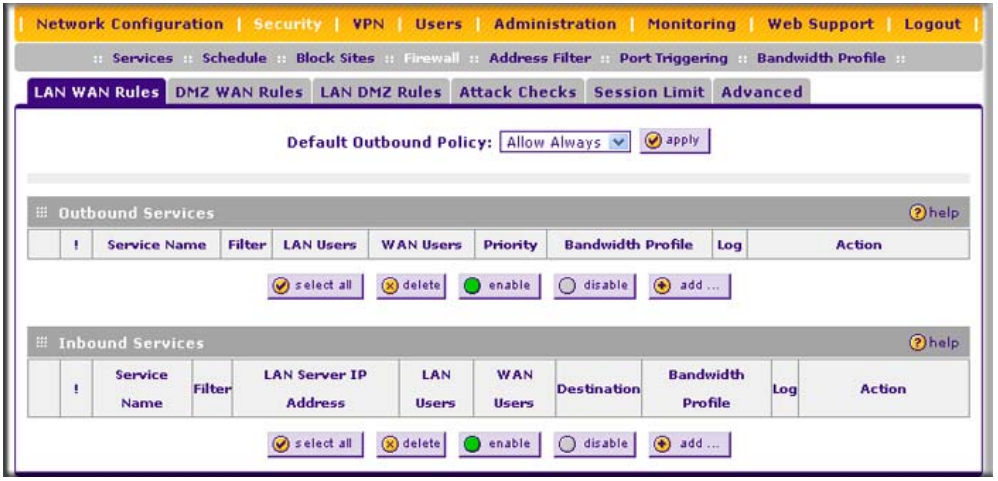


Figure 4-2

2. Change the **Default Outbound Policy** by selecting **Block Always** from the pull-down menu.

3. Click **Apply**.

LAN WAN Outbound Services Rules

You may define 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. The outbound rule will block the selected application from any internal IP LAN address to any external WAN IP address according to the schedule created in the Schedule menu.

You can also tailor these rules to your specific needs (see "Administrator Tips" on page 4-40).

Note: This feature is for advanced administrators only! Incorrect configuration will cause serious problems.

To create a new LAN WAN outbound service rule:

1. In the LAN WAN Rules screen, click **Add** under the **Outbound Services** table. The Add LAN WAN Outbound Service screen will display...

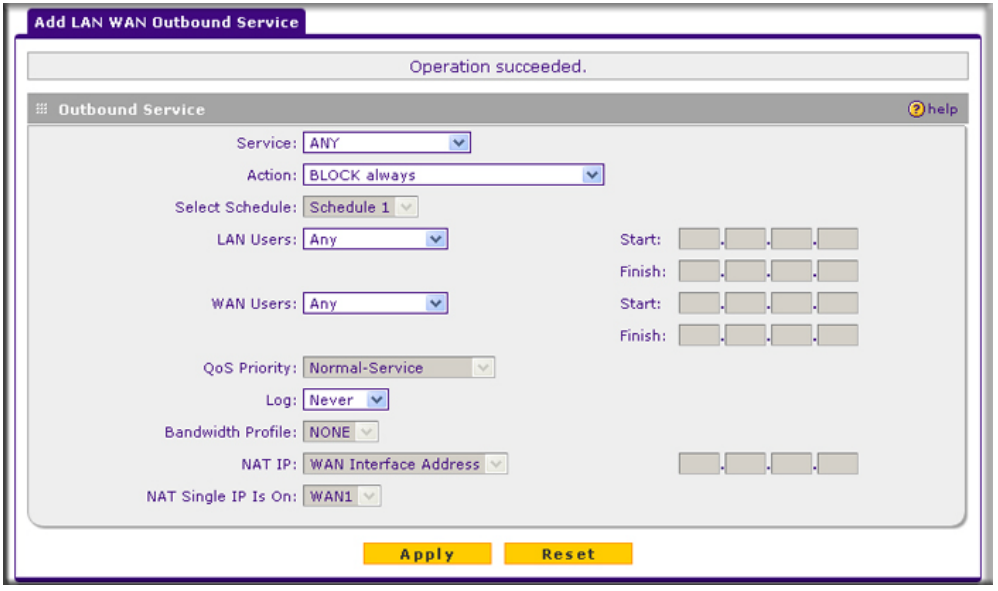


Figure 4-3

2. Configure the parameters based on the descriptions in Table 4-2 on page 4-3.

3. Click **Apply** to save your changes and reset the fields on this screen. The new rule will be listed in the **Outbound Services** table.

LAN WAN Inbound Services Rules

This **Inbound Services** 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. Remember that allowing inbound services opens holes in your VPN firewall. Only enable those ports that are necessary for your network.

To create a new LAN WAN inbound service rule:

1. In the LAN WAN Rules screen, click **Add** under the **Inbound Services** table. The Add LAN WAN Inbound Service screen will display.

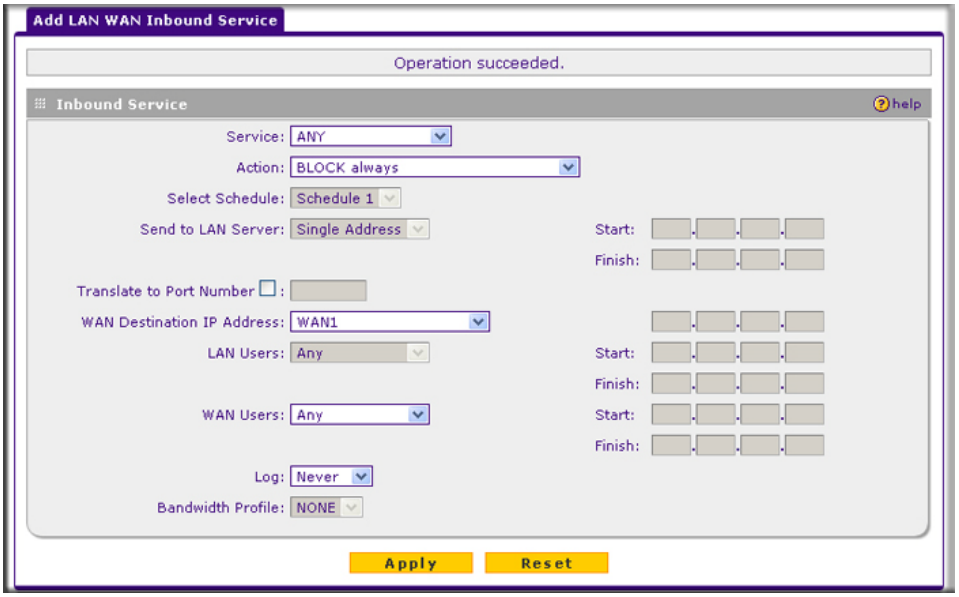


Figure 4-4

2. Configure the parameters based on the descriptions in Table 4-3 on page 4-6.
3. Click **Apply** to save your changes and reset the fields on this screen. The new rule will be listed in the **Inbound Services** table.

Configuring DMZ WAN Rules

The firewall rules for traffic between the DMZ and the WAN/Internet are configured on the **DMZ WAN Rules** screen. 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 DMZ to the Internet (outbound) or coming in from the Internet to the DMZ (inbound). The default outbound policy can be changed to block all outbound traffic and enable only specific services to pass through the VPN firewall by adding an outbound services rule.

To create a new DMZ WAN outbound service policy:

1. Select **Security** from the main menu and **Firewall Rules** from the submenu. The LAN WAN Rules screen will display.
2. Select the **DMZ WAN Rules** tab. The DMZ WAN Rules screen will display.

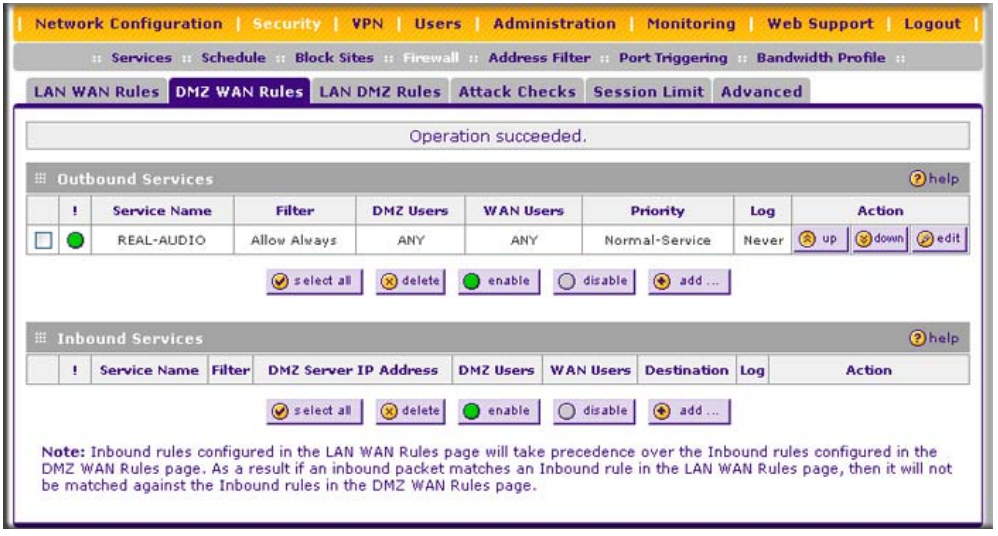


Figure 4-5

3. Click **Add** under the **Outbound Services** table. The Add DMZ WAN Outbound Services screen will display (see Figure 4-6 on page 4-13).

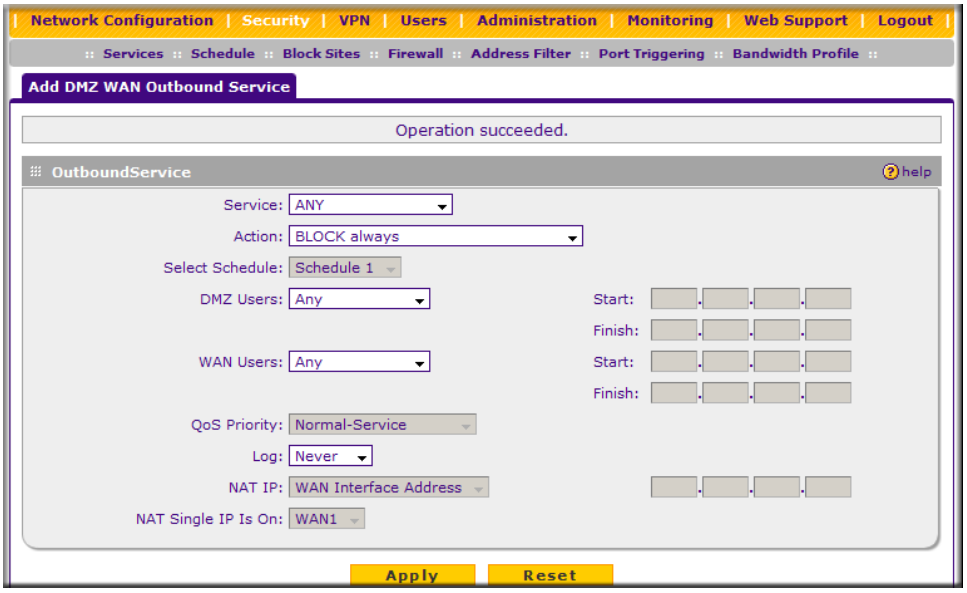


Figure 4-6

4. Configure the parameters based on the descriptions in Table 4-2 on page 4-3.
5. Click **Apply.** The new rule will appear in the **Outbound Services** table. The rule is automatically enabled.

The procedure to add a new DMZ WAN inbound service policy is similar to the procedure described above with the exception that you click **Add** under the **Inbound Services** table, you configure the parameters based on the descriptions in Table 4-3 on page 4-6, and the policy is added to the **Inbound Services** table.

Configuring LAN DMZ Rules

The LAN DMZ Rules screen allows you to create rules that define the movement of traffic between the LAN and the DMZ. The Default Outbound and Inbound Policies is to allow all traffic between the local LAN and DMZ network. Firewall rules can then be applied to block specific types of traffic from either going out from the LAN to the DMZ (outbound) or coming in from the DMZ to the LAN (inbound).

To create a new LAN DMZ outbound service policy:

1. Select **Security** from the main menu and **Firewall Rules** from the submenu. The LAN WAN Rules screen will display.

2. Select the **LAN DMZ Rules** tab. The LAN DMZ Rules screen will display.

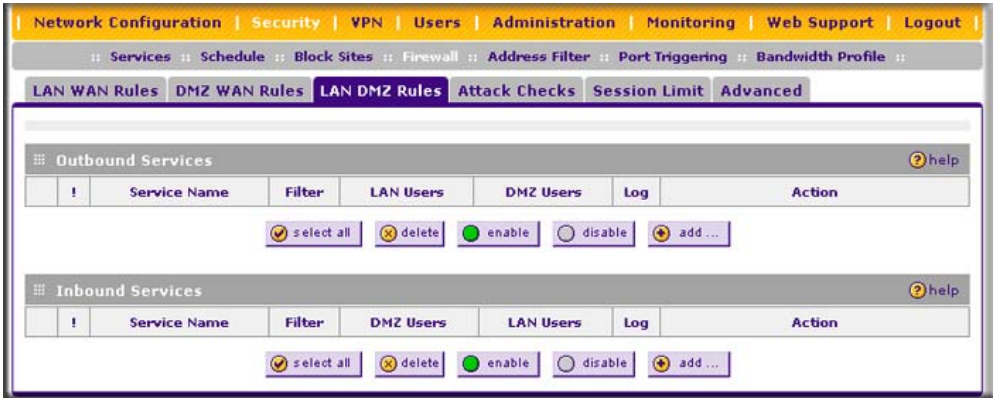


Figure 4-7

3. Click **Add** under the Outbound Services Table. The Add LAN DMZ Outbound Service screen will display.

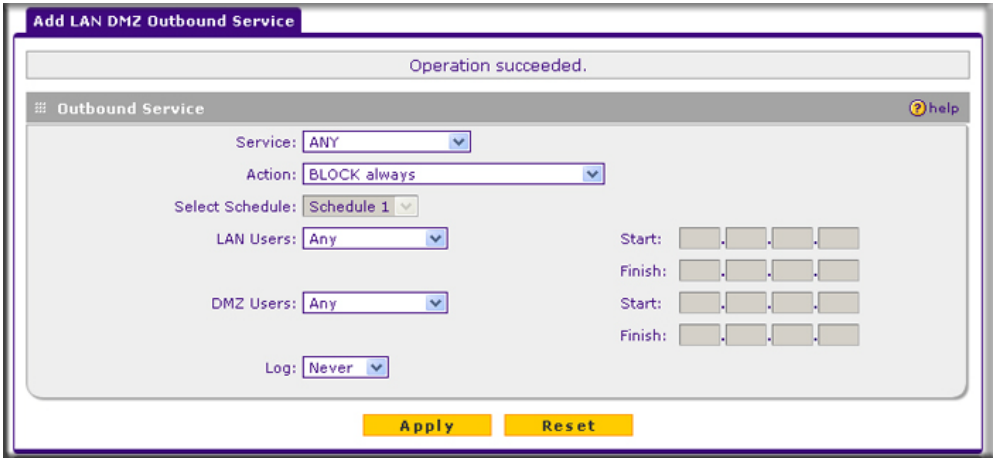


Figure 4-8

4. Configure the parameters based on the descriptions in Table 4-2 on page 4-3.
5. Click **Apply.** The new rule will appear in the **Outbound Services** table. The rule is automatically enabled.

The procedure to add a new LAN DMZ inbound service policy is similar to the procedure described above with the exception that you click **Add** under the **Inbound Services** table, you configure the parameters based on the descriptions in Table 4-3 on page 4-6, and the policy is added to the **Inbound Services** table.

Inbound Rules Examples

LAN WAN Inbound Rule: 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.

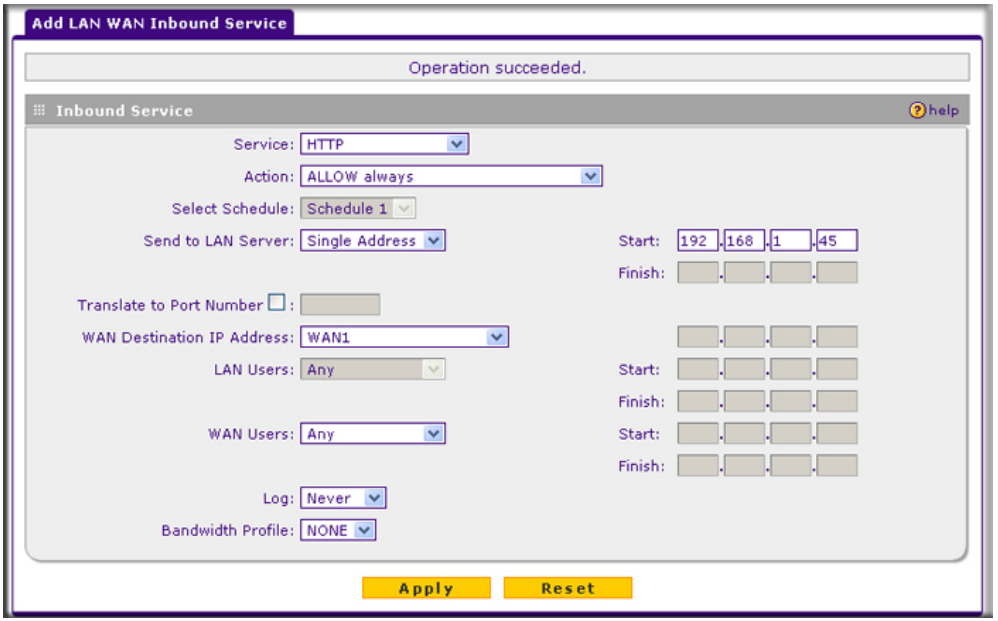


Figure 4-9

LAN WAN Inbound Rule: 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.

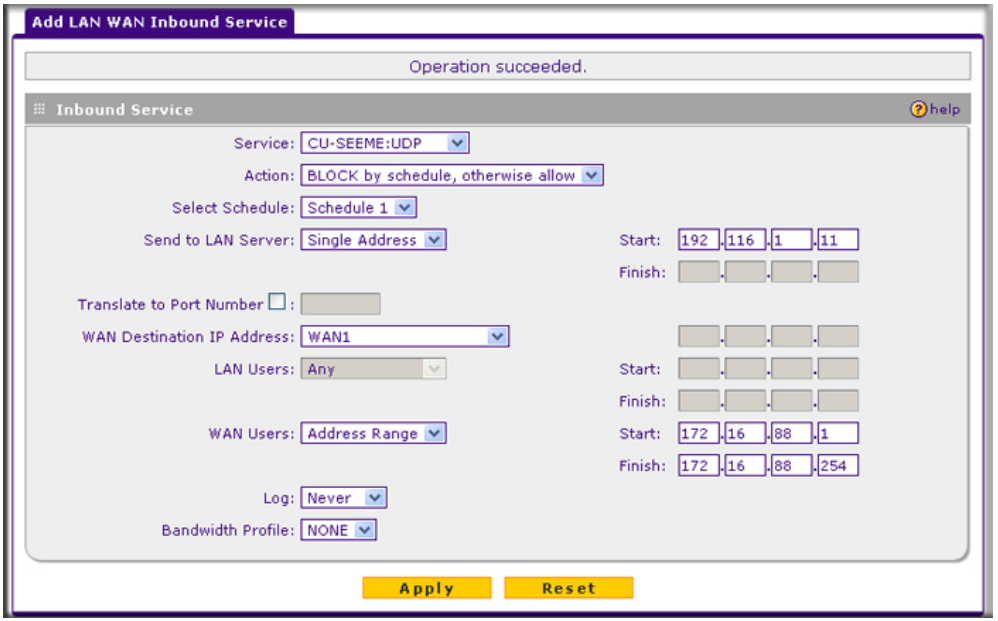


Figure 4-10

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

LAN WAN or DMZ WAN Inbound Rule: Setting Up One-to-One NAT Mapping

If you arrange with your ISP 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 or DMZ. One of these public IP addresses will be used as the primary IP address of the VPN firewall. 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.

In the example shown in Figure 4-11 on page 4-17, we have configured multi-NAT to support multiple public IP addresses on one WAN interface. The inbound rule instructs the VPN firewall to host an additional public IP address (10.1.0.5) and to associate this address with the Web server on the LAN (at 192.168.1.1). We also instruct the VPN firewall to translate the incoming HTTP port number (port 80) to a different port number (port 8080).

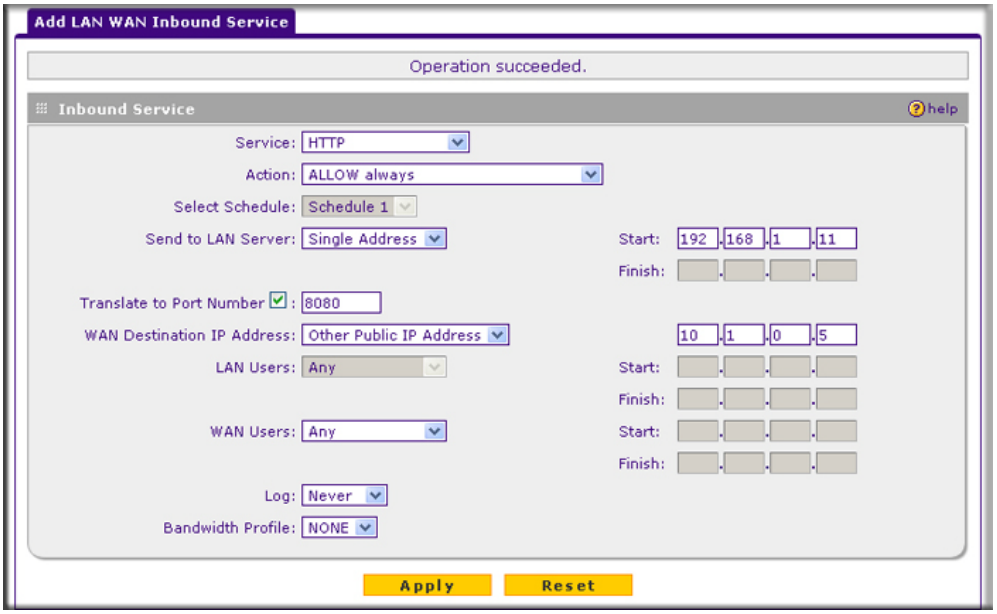


Figure 4-11

The following addressing scheme is used in this example:

- VPN firewall FVX538
  - WAN1 primary public IP address: 10.1.0.1
  - WAN1 additional public IP address: 10.1.0.5
  - LAN IP address 192.168.1.1
- Web server PC on the VPN firewall's LAN
  - LAN IP address: 192.168.1.11
  - Port number for Web service: 8080

To test the connection from a PC on the WAN side, type **http://10.1.0.5.** The home page of the Web server should appear.

LAN WAN or DMZ WAN Inbound Rule: 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 or DMZ 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.

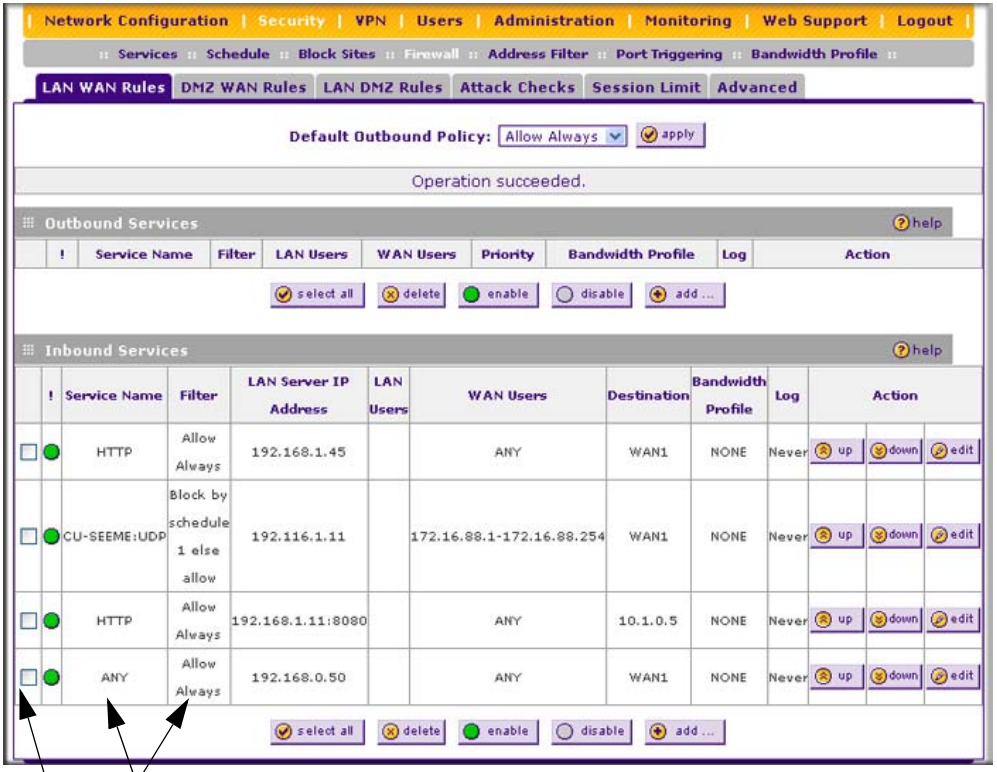


Figure 4-12

Outbound Rules Example

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

LAN WAN Outbound Rule: Blocking Instant Messenger

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

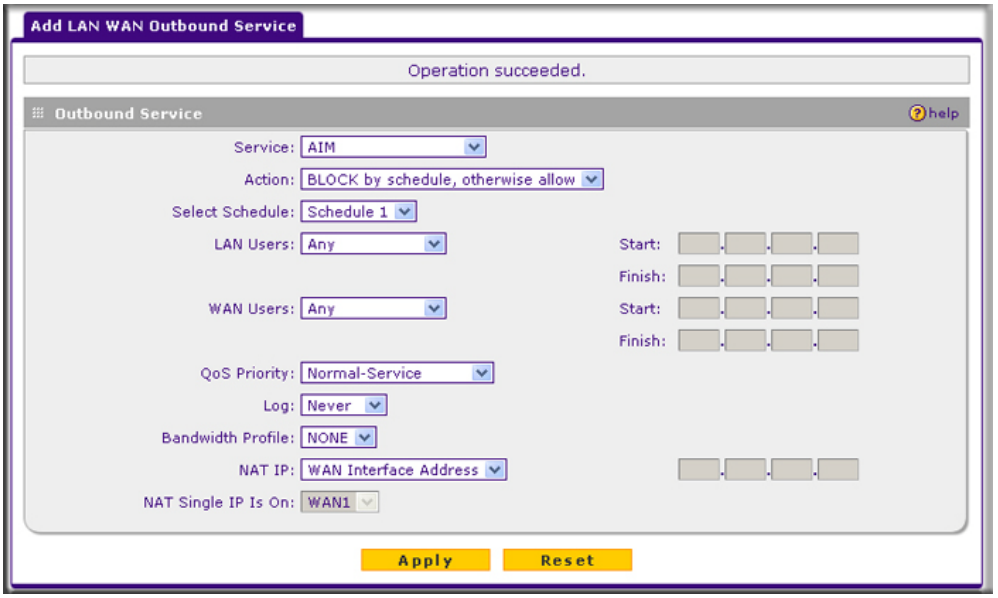


Figure 4-13

You can also have the VPN firewall log any attempt to use Instant Messenger during that blocked period.

Configuring Other Firewall Features

You can configure attack checks, set session limits, and manage the Application Level Gateway (ALG) for SIP sessions.

Attack Checks

The Attack Checks screen allows you to specify whether or not the VPN firewall should be protected against common attacks in the DMZ, LAN and WAN networks. To enable the appropriate attack checks for your environment:

1. Select **Security** from the main menu and **Firewall Rules** from the submenu. The LAN WAN Rules screen will display.
2. Click the **Attack Checks** tab. The Attack Checks screen will display.

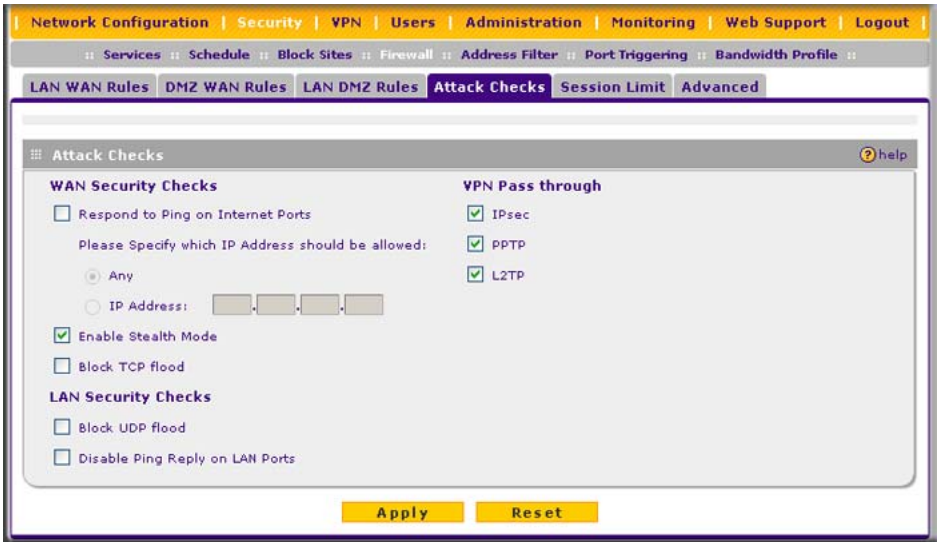


Figure 4-14

3. Check the boxes for the Attack Checks you wish to monitor. The various types of attack checks are listed and defined below.
4. Click **Apply** to save your settings.

The various types of attack checks listed on the Attack Checks screen are:

- **WAN Security Checks**
  - **Respond To Ping On Internet Ports**. By default, the VPN firewall responds to an ICMP Echo (ping) packet coming from the Internet or WAN side. Responding to a ping can be a useful diagnostic tool when there are connectivity problems. If the ping option is enabled, you can allow either any IP address or a specific IP address only to respond to a ping. You can disable the ping option to prevent hackers from easily discovering the VPN firewall via a ping.

  - **Enable Stealth Mode**. In stealth mode, the VPN firewall will not respond to port scans from the WAN or Internet, which makes 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 does not complete the connection, thus saturating the server with half-open connections. No legitimate connections can then be made.

    When blocking is enabled, the VPN firewall will limit the lifetime of partial connections and will be protected from a SYN flood attack.

- **LAN Security Checks**
  - **Block UDP flood**. A UDP flood is a form of denial of service attack in which the attacking machine sends a large number of UDP packets to random ports to the victim host. As a result, the victim host will check for the application listening at that port, see that no application is listening at that port, and 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, making the attacker's network location anonymous.

    If flood checking is enabled, the VPN firewall will not accept more than 20 simultaneous, active UDP connections from a single computer on the LAN.
  - **Disable Ping Reply on LAN Ports**. To prevent the VPN firewall from responding to ping requests from the LAN, click this checkbox.
- **VPN Pass through**. When the VPN firewall functions in NAT mode, all packets going to the Remote VPN Gateway are first filtered through NAT and then encrypted per the VPN policy.

  If a VPN client or gateway on the LAN side of the VPN firewall wants to connect to another VPN endpoint on the WAN, with the VPN firewall between the two VPN end points, all encrypted packets will be sent to the VPN firewall. Since the VPN firewall filters the encrypted packets through NAT, the packets become invalid.

  IPSec, PPTP, and L2TP represent different types of VPN tunnels that can pass through the VPN firewall. To allow the VPN traffic to pass through without filtering, enable those options for the type of tunnel(s) that will pass through the VPN firewall.

Setting Session Limits

Session Limit allows you to specify the total number of sessions allowed, per user, over an IP (Internet Protocol) connection across the VPN firewall. This feature is enabled on the Session Limit screen and shown below in Figure 4-15. Session Limit is disabled by default.

To set session limits:

1. Select **Security** from the main menu and **Firewall Rules** from the submenu. The LAN WAN Rules screen will display.
2. Click the **Session Limit** tab. The Session Limit screen will display..

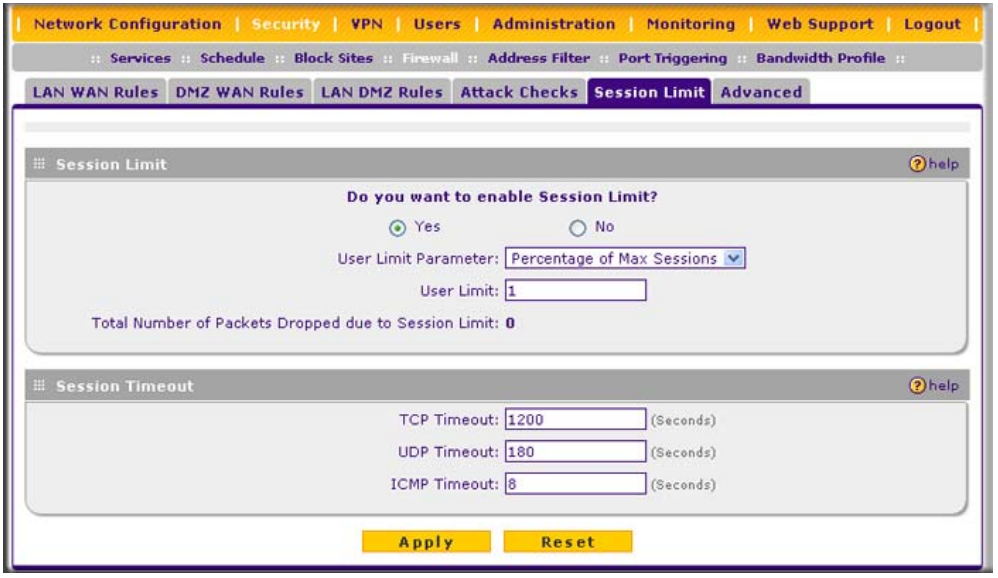


Figure 4-15

3. Click the **Yes** radio button under **Do you want to enable Session Limit?**
4. From the **User Limit Parameter** pull-down menu, define the maximum number of sessions per IP either as a percentage of maximum sessions or as an absolute.

   The percentage is computed on the total connection capacity of the device.
5. Enter the **User Limit**. If the User Limit Parameter is set to **Percentage of Max Sessions**, this is the maximum number of sessions allowed from a single source machine as a percentage of the total connection capacity. (Session Limit is per machine based.) Otherwise, if the User Limit Parameter is set to **Number of Sessions**, the user limit is an absolute value.

Note: Some protocols (such as FTP or RSTP) create two sessions per connection which should be considered when configuring Session Limiting.

The **Total Number of Packets Dropped due to Session Limit** field shows total number of packets dropped when session limit is reached.

6. In the **Session Timeout** section, modify the TCP, UDP and ICMP timeout values as you require. A session will expire if no data for the session is received for the duration of the timeout value. The default timeout values are 1200 seconds for TCP sessions, 180 seconds for UDP sessions, and 8 seconds for ICMP sessions.
7. Click **Apply** to save your settings.

Managing the Application Level Gateway for SIP Sessions

The Application Level Gateway (ALG) facilitates multimedia sessions such as voice over IP (VoIP) sessions that use the Session Initiation Protocol (SIP) across the firewall and provides support for multiple SIP clients. ALG support for SIP is disabled by default.

To enable ALG for SIP:

1. Select **Security** from the main menu and **Firewall Rules** from the submenu. The LAN WAN Rules screen will display.
2. Click the **Advanced** tab. The Advanced screen will display.

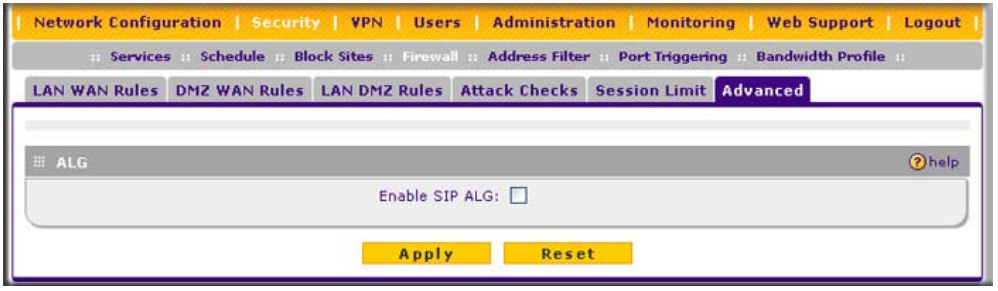


Figure 4-16

3. Select the **Enable SIP ALG** checkbox.
4. Click **Apply** to save your settings.

Creating Services, QoS Profiles, and Bandwidth Profiles

When you create inbound and outbound firewall rules, you use firewall objects such as services, QoS profiles, bandwidth profiles, and schedules to narrow down the firewall rules:

- **Services**. A service narrows down the firewall rule to an application and a port number. For information about adding services, see "Adding Customized Services" on page 4-24.
- **QoS profiles**. A quality of service (QoS) profile defines the relative priority of an IP packet for traffic that matches the firewall rule. For information about creating QoS profiles, see "Specifying Quality of Service (QoS) Priorities" on page 4-26.
- **Bandwidth Profiles**. A bandwidth profile allocates and limits traffic bandwidth for the LAN users to which a firewall rule is applied. For information about creating bandwidth profiles, see "Creating Bandwidth Profiles" on page 4-27.

Note: A schedule narrows down the period during which a firewall rule is applied. For information about specifying schedules, see "Setting a Schedule to Block or Allow Specific Traffic" on page 4-29.

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 Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application.

Although the VPN firewall already holds a list of many service port numbers, you are not limited to these choices. Use the Services screen to add additional services and applications to the list for use in defining firewall rules. The Services screen shows a list of services that you have defined, as shown in Figure 4-17 on page 4-25.

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.

To add a customized service:

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

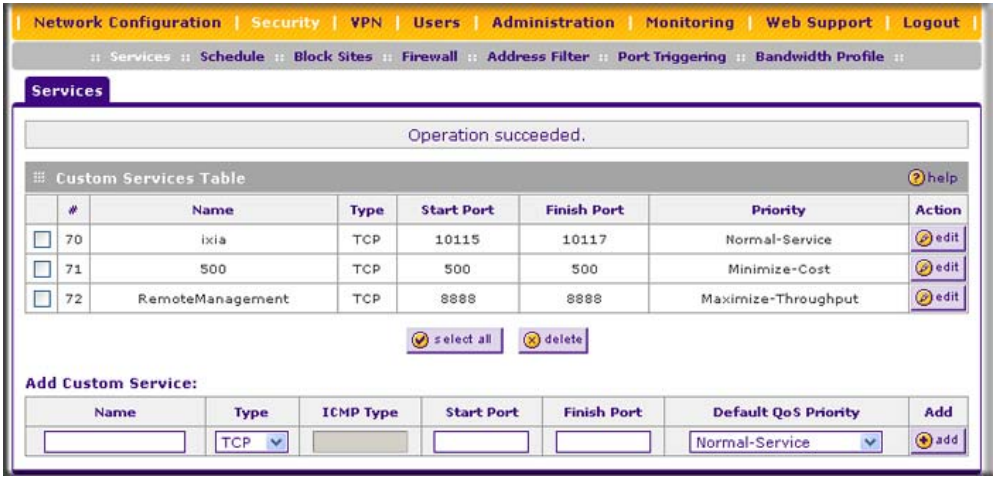


Figure 4-17

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.

Modifying a Service

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.

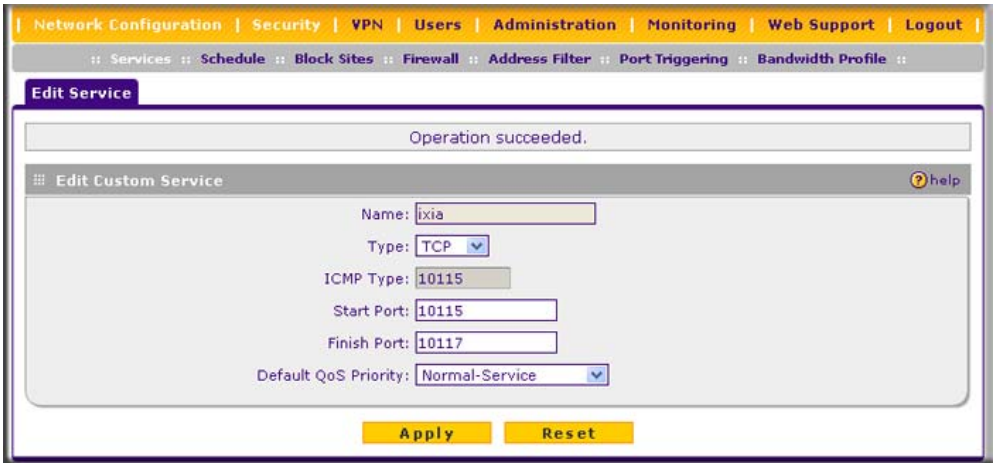


Figure 4-18

2. Modify the parameters you wish to change.
3. Click **Reset** to cancel the changes and restore the previous settings or 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 Custom Services Table for customized services (see Figure 4-17).
- On the Add LAN WAN Outbound Services screen (see Figure 4-3 on page 4-10).
- On the Add DMZ WAN Outbound Services screen (see Figure 4-6 on page 4-13).

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.

Creating Bandwidth Profiles

Bandwidth limiting determines the way in which data is communicated with your host. The purpose of bandwidth limiting is to provide a method for limiting traffic, thus preventing LAN users from consuming all the bandwidth on your WAN link.

- Bandwidth limiting is done on the available WAN interface in both the single port and Auto-Failover modes. Bandwidth limiting is handled on the user-specified interface in Load Balancing mode.
- Bandwidth limiting does not apply to the DMZ interface.

For example, when a new connection is established by a device, the device will locate the firewall rule corresponding to the connection.

- If the rule has a bandwidth profile specification, then the device will create a bandwidth class in the kernel.
- If multiple connections correspond to the same firewall rule, they will share the same class.

An exception occurs for an individual bandwidth profile if the classes are per source IP. The source IP is the IP of the first packet of the connection:

The class is deleted when all the connections using the class expire.

To add a bandwidth profile:

1. Select **Security** from the main menu and **Bandwidth Profile** from the submenu. The Bandwidth Profile screen will display (see Figure 4-19 on page 4-28).

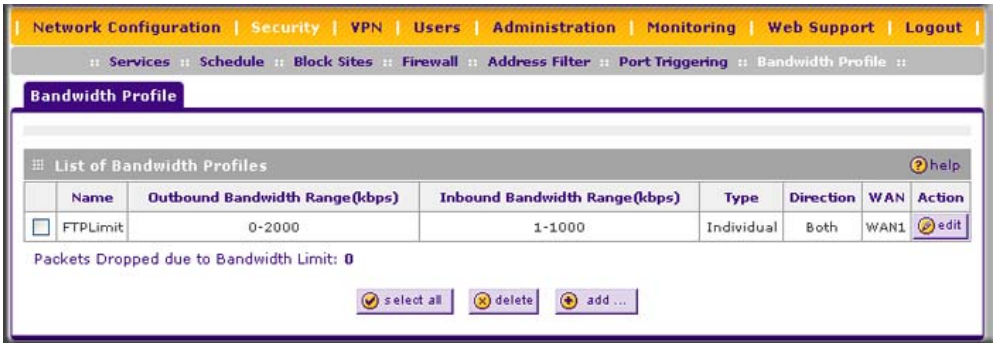


Figure 4-19

2. Click **Add** to add a new bandwidth profile. The Add New Bandwidth Profile screen displays.

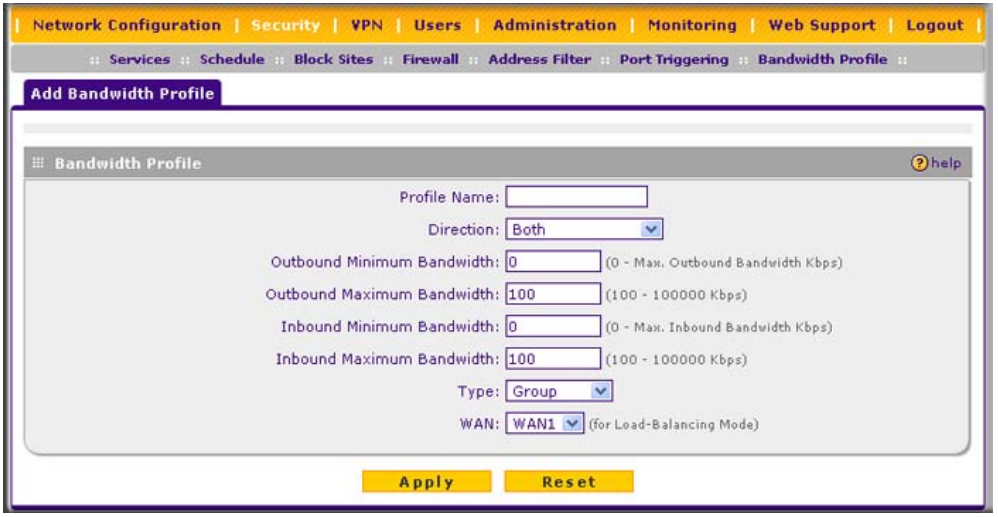


Figure 4-20

3. Enter the following information:

a. Enter a **Profile Name**. This name will become available in the firewall rules definition menus.

b. From the **Direction** pull-down box, select whether the profile will apply to outbound, inbound, or both outbound and inbound traffic.

c. Depending on the direction that you selected, enter the minimum and maximum bandwidths to be allowed:

- Enter the **Outbound Minimum Bandwidth** and **Outbound Maximum Bandwidth** in Kbps.
- Enter the **Inbound Minimum Bandwidth** and **Inbound Maximum Bandwidth** in Kbps.

The minimum bandwidth can range from 0 Kbps to the maximum bandwidth that you specify. The maximum bandwidth can range from 100 Kbps to 100,000 Kbps.

d. From the **Type** pull-down box, select whether the profile will apply to a group or individual.

e. From the **WAN** pull-down box, specify the WAN interface (if in Load Balancing Mode) for the profile.

- Click **Apply**. The new bandwidth profile will be added to the **List of Bandwidth Profiles** table.

To edit a bandwidth profile:

1. Click the **Edit** link adjacent to the profile you want to edit. The Edit Bandwidth Profile screen is displayed. (This screen shows the same fields as the Add New Bandwidth Profile screen.)
2. Modify the settings that you wish to change.
3. Click **Apply**. Your modified profile will display in the **Bandwidth Profile** table.

To remove an entry from the table, select the profile and click **delete**.

To remove all the profiles, click **select All** and then click **delete**.

Setting a Schedule to Block or Allow Specific Traffic

Schedules define the timeframes under which firewall rules may be applied.

Three schedules, Schedule 1, Schedule 2 and Schedule3 can be defined, and any one of these can be selected when defining firewall rules.

To invoke rules based on a schedule, follow these steps:

1. Select **Security** from the main menu and **Schedule** from the submenu. The Schedule 1 screen will display (see Figure 4-21 on page 4-30).

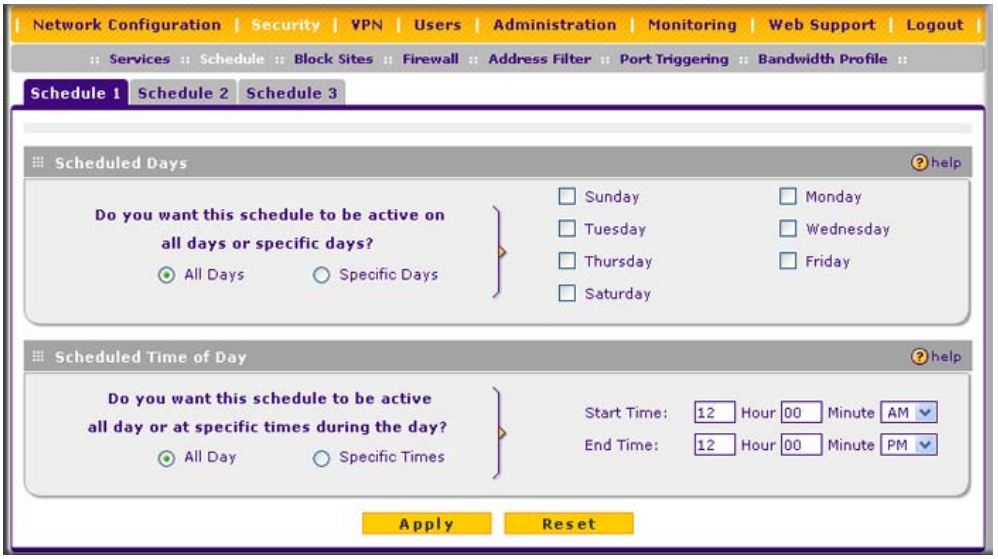


Figure 4-21

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 **Apply** to save your settings to Schedule 1.

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

Blocking Internet Sites (Content Filtering)

If you want to 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 website 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. Some of these components are can be used by malicious Websites to infect computers that access them. Even sites on the Trusted Domains list will be subject to Web Components blocking when the blocking of a particular Web component is enabled.
  - **Proxy**. A proxy server (or simply, proxy) allows computers to route connections to other computers through the proxy, thus circumventing certain firewall rules. For example, if connections to a specific IP address are blocked by a firewall rule, the requests can be routed through a proxy that is not blocked by the rule, rendering the restriction ineffective. Enabling this feature blocks proxy servers.
  - **Java**. Blocks java applets from being downloaded from pages that contain them. Java applets are small programs embedded in web pages that enable dynamic functionality of the page. A malicious applet can be used to compromise or infect computers. Enabling this setting blocks Java applets from being downloaded.
  - **ActiveX**. Similar to Java applets, ActiveX controls install on a Windows computer running Internet Explorer. A malicious ActiveX control can be used to compromise or infect computers. Enabling this setting blocks ActiveX applets from being downloaded.
  - **Cookies**. Cookies are used to store session information by websites that usually require login. However, several websites use cookies to store tracking information and browsing habits. Enabling this option filters out cookies from being created by a website..

    Note: Many websites require that cookies be accepted in order for the site to be accessed properly. Blocking cookies may interfere with useful functions provided by these websites.

- **Keyword Blocking** (Domain Name Blocking). You can specify up to 32 words that, should they appear in the website 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 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 submenu. The Block Sites screen will display.

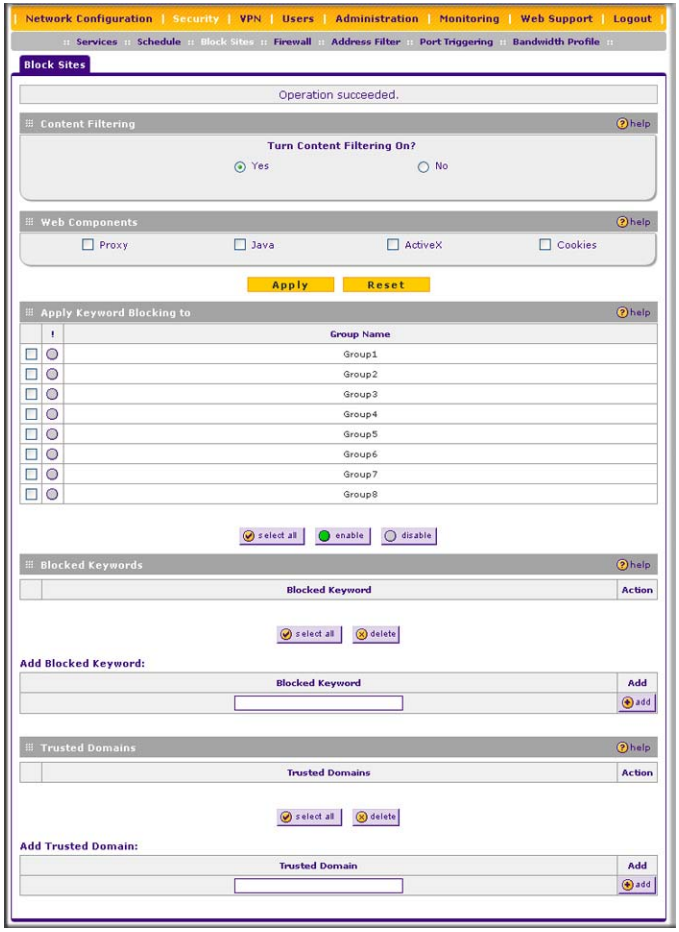


Figure 4-22

2. Check the **Yes** radio button to enable content filtering.
3. Click **Apply** to activate the screen controls.
4. Check the radio boxes of any web components you wish to block.
5. 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).
6. 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.)
7. 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.)

Configuring Source MAC Filtering

Source MAC filtering 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.
- 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.

Note: For additional ways of restricting outbound traffic, see “Outbound Rules (Service Blocking)” on page 4-3.

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

1. Select **Security** from the main menu and **Address Filter** from the submenu. The Source MAC Filter screen will display (see Figure 4-23 on page 4-34).

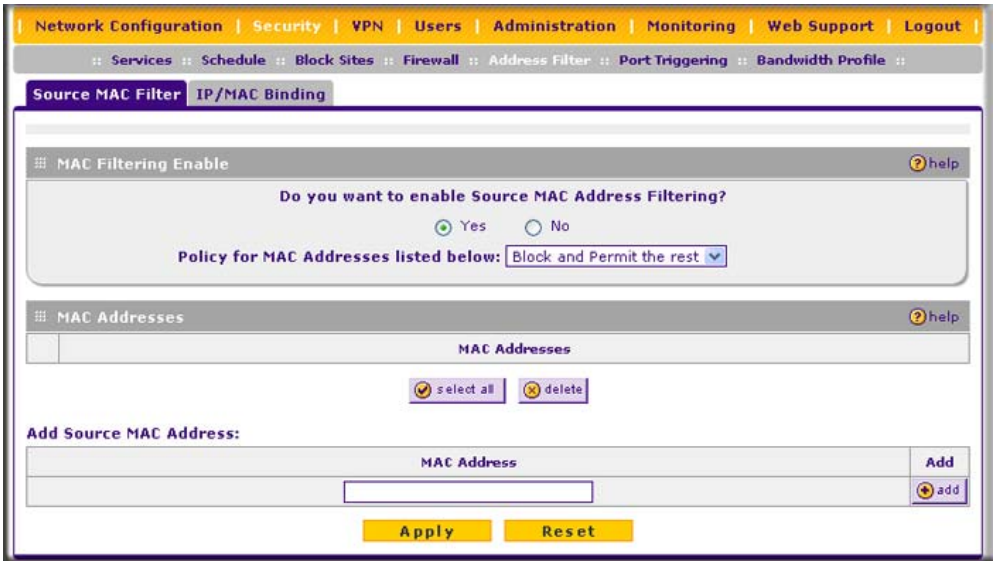


Figure 4-23

2. Check the Yes radio box in the **MAC Filtering Enable** section.
3. Select the action to be taken on outbound traffic from the listed MAC addresses:
   - Block this list and permit all other MAC addresses.
   - Permit this list and block all other MAC addresses.
4. Enter a MAC Address in the **Add Source MAC Address** checkbox and click **Add**. The MAC address will appear in the **MAC Addresses** table. Repeat this process to add additional MAC addresses.

   A valid MAC address is six colon-separated pairs of hexadecimal digits (0 to 9 and a to f). For example: 01:23:45:ab:cd:ef.
5. Click **Reset** to cancel a MAC address entry before adding it to the table or click **Apply** to save your settings.

You can edit the MAC address by clicking **Edit** in the Action column adjacent to the MAC Address.

To remove an entry from the table, select the MAC address entry and click **Delete**.

To select all the list of MAC addresses, click **Select All**. A checkmark will appear in the box to the left of each MAC address in the **MAC Addresses** table.

Configuring IP/MAC Address Binding

IP/MAC binding allows you to bind an IP address to a MAC address and the other way around. Some devices are configured with static addresses. To prevent users from changing their static IP addresses, IP/MAC binding must be enabled on the VPN firewall. If the VPN firewall detects packets with a matching IP address, but with the inconsistent MAC address (or the other way around), it will drop these packets. If users have enabled the logging option for IP/MAC binding, these packets will be logged before they are dropped. The VPN firewallwill then display the total number of dropped packets that violated either the IP-to-MAC binding or the MAC-to-IP binding.

Following is an example:

Assume that three computers on the LAN are set up as follows:

- Host1: MAC address (00:01:02:03:04:05) and IP address (192.168.10.10)
- Host2: MAC address (00:01:02:03:04:06) and IP address (192.168.10.11)
- Host3: MAC address (00:01:02:03:04:07) and IP address (192.168.10.12)

If all the above host entries are added to the **IP/MAC Binding** table, the following scenarios indicate the possible outcome.

- Host1: Matching IP address and MAC address in the **IP/MAC Bindings** table.
- Host2: Matching IP address but inconsistent MAC address in the **IP/MAC Bindings** table.
- Host3: Matching MAC address but inconsistent IP address in the **IP/MAC Bindings** table.

The VPN firewall will block the traffic coming from Host2 and Host3, but allow the traffic coming from Host1 to any external network. The total count of dropped packets will be displayed.

To enable IP/MAC Binding and add IP and MAC address for binding:

1. Select **Security** from the main menu and **Address Filter** from the submenu.
2. Select the **IP/MAC Binding** tab. The IP/MAC Binding screen will display (see Figure 4-24 on page 4-36).

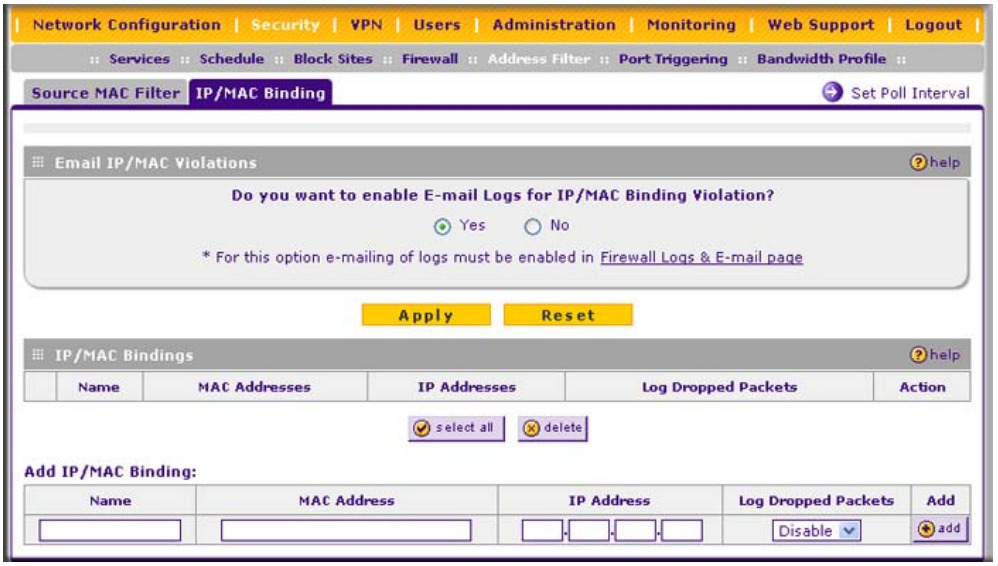


Figure 4-24

3. Select the **Yes** radio box and click **Apply**. Make sure that you have enabled the e-maling of logs (see "Activating Notification of Events and Alerts" on page 6-23).
4. Add an IP/MAC Bind rule by entering:
   a. **Name**. Specify an easily identifiable name for this rule.
   b. **MAC Address**. Specify the MAC Address for this rule.
   c. **IP Addresses**. Specify the IP Address for this rule.
   d. **Log Dropped Packets**. Select the logging option for this rule from the pull-down menu.
5. Click **Add.** The new IP/MAC rule will be appear the **IP/MAC Binding** table.

   The IP/MAC Binding Table lists the currently defined IP/MAC Bind rules:
   - **Name**. Displays the user-defined name for this rule.
   - **MAC Addresses**. Displays the MAC Addresses for this rule.
   - **IP Addresses**. Displays the IP Addresses for this rule.
   - **Log Dropped Packets**. Displays the logging option for this rule.

To edit an IP/MAC Bind rule, click **Edit** adjacent to the entry. The following fields of an existing IP/MAC Bind rule can be modified:

- **MAC Address**. Specify the MAC Address for this rule.
- **IP Addresses**. Specify the IP Address for this rule.
- **Log Dropped Packets**. Specify the logging option for this rule.

To remove an entry from the table, select the IP/MAC Bind entry and click **Delete**.

To see the counter that shows the packets that were dropped because of IP-MAC binding violations and to set the poll interval, click the **Set Poll Interval** link at the top of the IP/MAC Binding screen.

Configuring Port Triggering

Port triggering allows some applications to function correctly that would otherwise be partially blocked by the VPN firewall when it functions in NAT mode. Some applications require that when external devices connect to them, they receive data on a specific port or range of ports. The VPN firewall must send all incoming data for that application only on the required port or range of ports. Using this feature requires that you know the port numbers used by the application.

Port triggering allows computers on the private network (LAN) to request that one or more ports be forwarded to them. Unlike basic port forwarding which forwards ports to only one preconfigured IP address, port triggering waits for an outbound request from the private network on one of the defined outgoing ports. It then automatically sets up forwarding to the IP address that sent the request. When the application ceases to transmit data over the port, the VPN firewall waits for a timeout interval and then closes the port or range of ports, making them available to other computers on the private network.

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 additional 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.

Note these restrictions with port triggering:

- 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 VPN firewall cannot detect when the application has terminated.

> **Note:** For additional ways of allowing inbound traffic, see "Inbound Rules (Port Forwarding)" on page 4-5.

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.

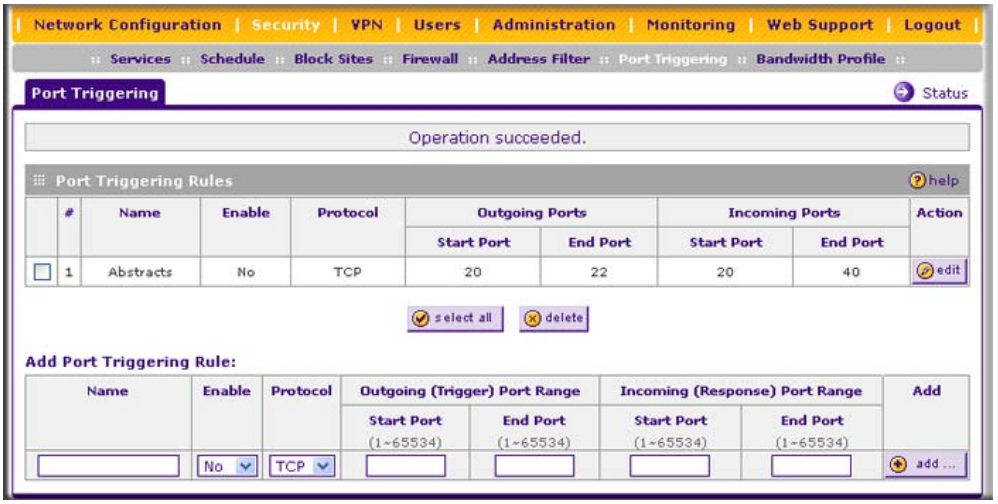


Figure 4-25

2. Enter a user-defined name for this rule in the **Name** field.
3. From the **Enable** pull-down menu, indicate if the rule is enabled or disabled.
4. From the **Protocol** pull-down menu, select either the TCP or UDP protocol.
5. In the **Outgoing (Trigger) Port Range** fields:
   a. Enter the **Start Port** range (1 - 65534).
   b. Enter the **End Port** range (1 - 65534).

6. In the **Incoming (Response) Port Range** fields:
   a. Enter the **Start Port** range (1 - 65534).
   b. Enter the **End Port** range (1 - 65534).
7. 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.

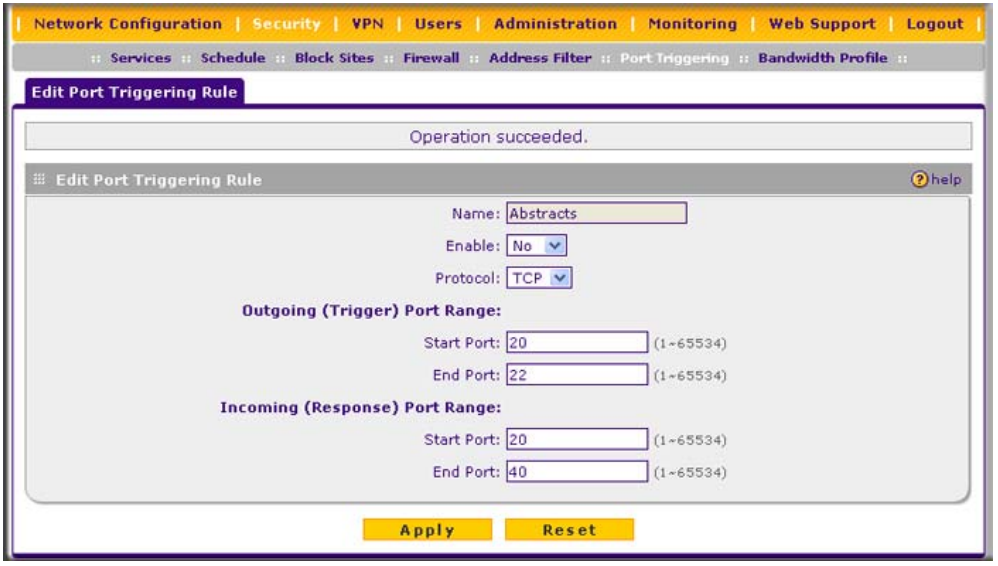


Figure 4-26

2. Modify any of the fields for this rule.
3. Click **Reset** to cancel any changes and return to the previous settings or 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.

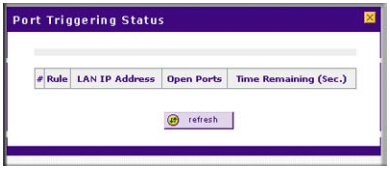


Figure 4-27

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 e-mail 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 that you enter on the Firewall Logs & E-mail screen. In addition, if you have set up content filtering on the Block Sites screen (see "Blocking Internet Sites (Content Filtering)" on page 4-30), a log will be generated when someone on your network tries to access a blocked site.

To configure e-mail or syslog notification, or to view the logs, see "Activating Notification of Events and Alerts" on page 6-23.

Administrator Tips

Consider the following operational items:

- As an option, you can enable remote management if you have to manage distant sites from a central location (see "Configuring an External Server for Authentication" on page 6-11).
- Although rules (see "Using Rules to Block or Allow Specific Kinds of Traffic" on page 4-2) is the basic way of managing the traffic through your system, you can further refine your control with the following optional features of the VPN firewall:
  - Groups and hosts (see "Managing Groups and Hosts (LAN Groups)" on page 3-6)
  - Services (see "Services-Based Rules" on page 4-3)
  - Schedules (see "Setting a Schedule to Block or Allow Specific Traffic" on page 4-29)
  - Block sites (see "Blocking Internet Sites (Content Filtering)" on page 4-30)
  - Source MAC filtering (see "Configuring Source MAC Filtering" on page 4-33)
  - Port triggering (see "Configuring Port Triggering" on page 4-37)

Chapter 5
Virtual Private Networking

This chapter describes how to use the virtual private networking (VPN) features of the ProSafe VPN Firewall 200 FVX538.

This chapter includes the following sections:

- "Considerations for Dual WAN Port Systems" on this page
- "Using the VPN Wizard for Client and Gateway Configurations" on page 5-3
- "Testing the Connections and Viewing Status Information" on page 5-12
- "Managing VPN Policies" on page 5-16
- "Managing Certificates" on page 5-19
- "Extended Authentication (XAUTH) Configuration" on page 5-26
- "Assigning IP Addresses to Remote Users (ModeConfig)" on page 5-32
- "Configuring Keepalives and Dead Peer Detection" on page 5-42
- "Configuring NetBIOS Bridging with VPN" on page 5-44

Considerations for Dual WAN Port Systems

If both of the WAN ports of the VPN firewall are configured, you can enable either Auto-Rollover mode for increased system reliability or Load Balancing mode for optimum bandwidth efficiency. This WAN mode choice impacts how the VPN features must be configured.

The use of fully qualified domain names in VPN policies is mandatory when the WAN ports are in load balancing or rollover mode; and is also required for the VPN tunnels to fail over. FQDN is optional when the WAN ports are in load balancing mode if the IP addresses are static but mandatory if the WAN IP addresses are dynamic.

Refer to "Virtual Private Networks (VPNs)" on page B-9 for more on the IP addressing requirements for VPN in the dual WAN modes. For instructions on how to select and configure a dynamic DNS service for resolving FQDNs, see "Configuring Dynamic DNS (Optional)" on page 2-14. For instructions on WAN mode configuration, see "Configuring the WAN Mode (Required for Dual WAN)" on page 2-7.

The diagrams and table below show how the WAN mode selection relates to VPN configuration.

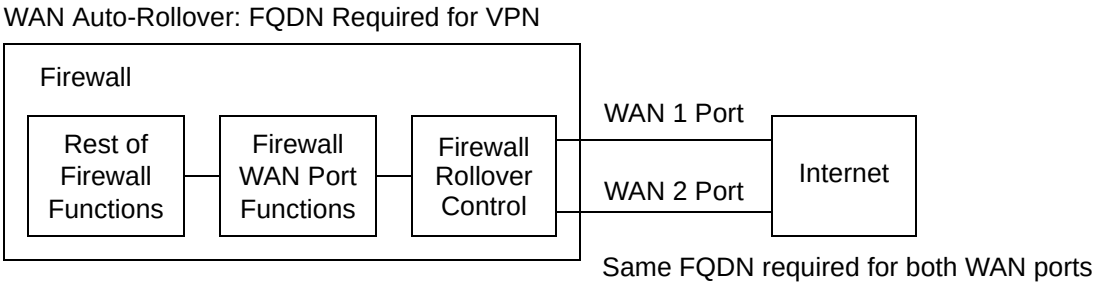


Figure 5-1

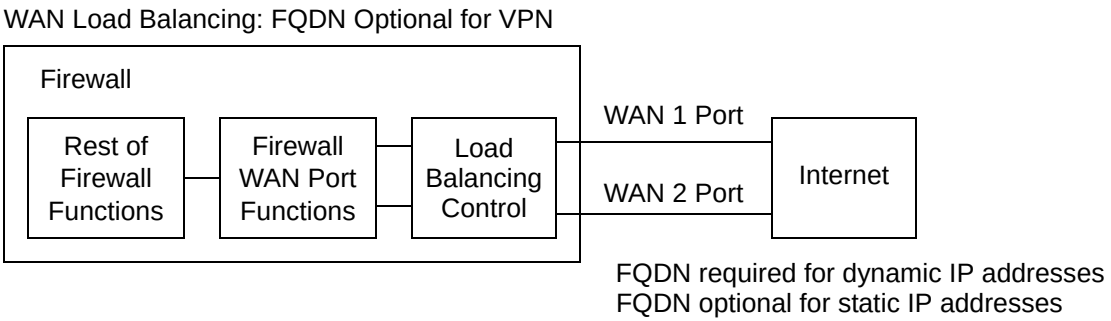


Figure 5-2

Table 5-1 summarizes the WAN addressing requirements (FQDN or IP address) for your VPN tunnel in either dual WAN mode.

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

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

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

Using the VPN Wizard for Client and Gateway Configurations

You use the VPN Wizard to configure multiple gateway or client VPN tunnel policies.

The section below provides wizard and NETGEAR *VPN Client* configuration procedures for the following scenarios:

- Using the wizard to configure a VPN tunnel between 2 VPN gateways
- Using the wizard to configure a VPN tunnel between a VPN gateway and a VPN client

Configuring 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 efficiently guides you through the setup procedure with a series of questions that will determine the IPsec keys and VPN policies it sets up. The VPN Wizard will also 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 recommendations of the VPN Consortium (VPNC), an organization that promotes multi-vendor VPN interoperability.

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

Creating Gateway to Gateway VPN Tunnels with the Wizard

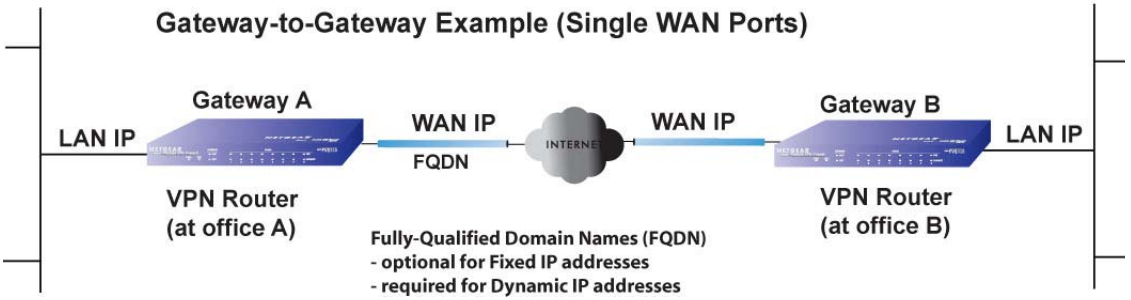


Figure 5-3

Follow these steps to set up a gateway VPN tunnel using the VPN Wizard.

1. Select **VPN** from the main menu and **VPN Wizard** from the submenu. The VPN Wizard screen will display. To view the wizard default settings, click the **VPN Wizard Default Values** link. You can modify these settings after completing the wizard.

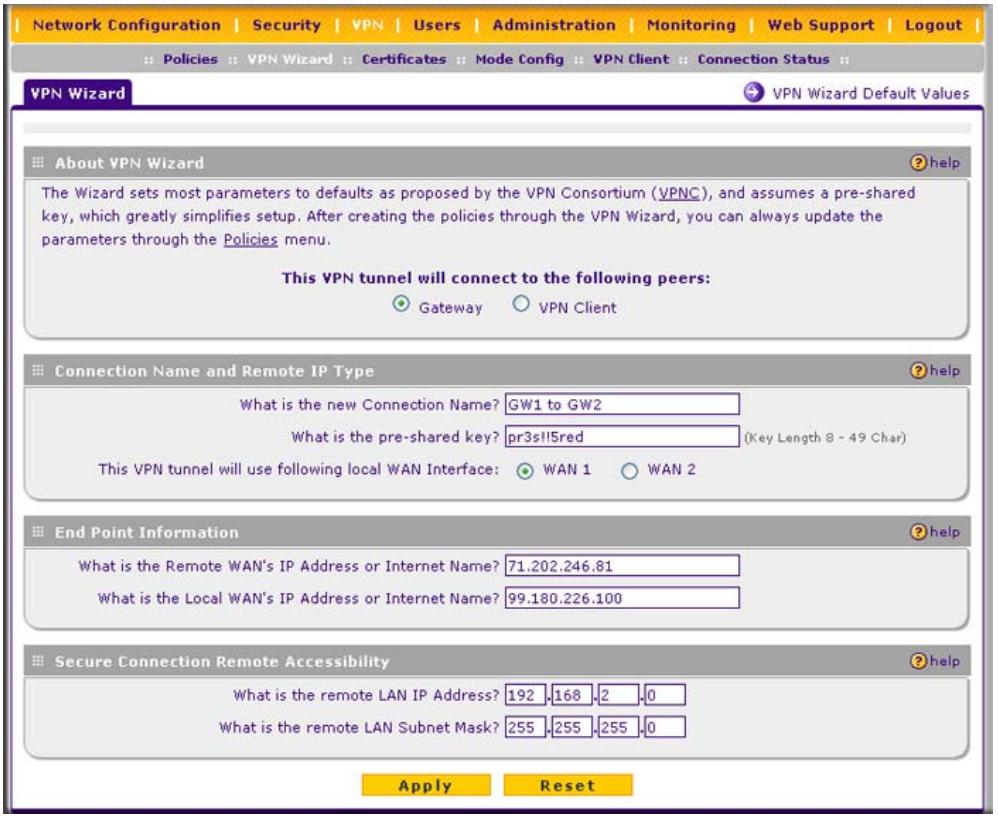


Figure 5-4

2. Select **Gateway** as your connection type.
3. Create a **Connection Name**. Enter a descriptive name for the connection. This name used to help you manage the VPN settings; is not supplied to the remote VPN endpoint.
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 must be a minimum of 8 characters and should not exceed 49 characters.
5. Choose which WAN port to use as the VPN tunnel end point.

	**Note:** If you are using a dual WAN rollover configuration, after completing the wizard, you must manually update the VPN policy to enable VPN rollover. This allows the VPN tunnel to roll over when the WAN Mode is set to Auto Rollover. The wizard will not set up the VPN policy with rollover enabled.

6. Enter the **Remote and Local WAN IP Addresses or Internet Name**s of the gateways which will connect.
   - Both the remote WAN address and your local WAN address are required.

> **Tip:** To assure tunnels stay active, after completing the wizard, manually edit the VPN policy to enable keepalive which periodically sends ping packets to the host on the peer side of the network to keep the tunnel alive.

   - The remote WAN IP address must be a public address or the Internet name of the remote gateway. The *Internet name* is the Fully Qualified Domain Name (FQDN) as registered in a Dynamic DNS service. Both local and remote endpoints should be defined as either FQDN or IP addresses. A combination of IP address and FQDN is not allowed.

> **Tip:** For DHCP WAN configurations, first, set up the tunnel with IP addresses. Once you validate the connection, use the wizard to create new policies using FQDN for the WAN addresses.

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

> **Note:** The Remote LAN IP address *must* be in a different subnet than the Local LAN IP address. For example, if the local subnet is 192.168.1.x, then the remote subnet could be 192.168.10.x. but *could not* be 192.168.1.x. If this information is incorrect, the tunnel will fail to connect.

8. Click **Apply** to save your settings. The VPN Policies screen shows that the policy is now enabled.

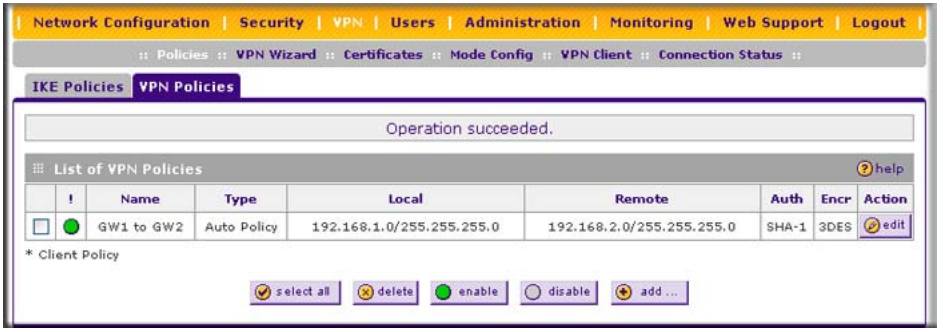


Figure 5-5

9. If you are connecting to another NETGEAR VPN firewall, use the VPN Wizard to configure the second VPN firewall to connect to the one you just configured.

To display the status of your VPN connections, select **VPN** from the main menu and **Connection Status** from the submenu. The Connection Status screen will display.

Figure 5-6

The tunnel will automatically establish when both the local and target gateway policies are appropriately configured and enabled,

	Note: When using FQDN, if the dynamic DNS service is slow to update their servers when your DHCP WAN address changes, the VPN tunnel will fail because the FQDN does not resolve to your new address. If you have the option to configure the update interval, set it to an appropriately short time.

Creating a Client to Gateway VPN Tunnel

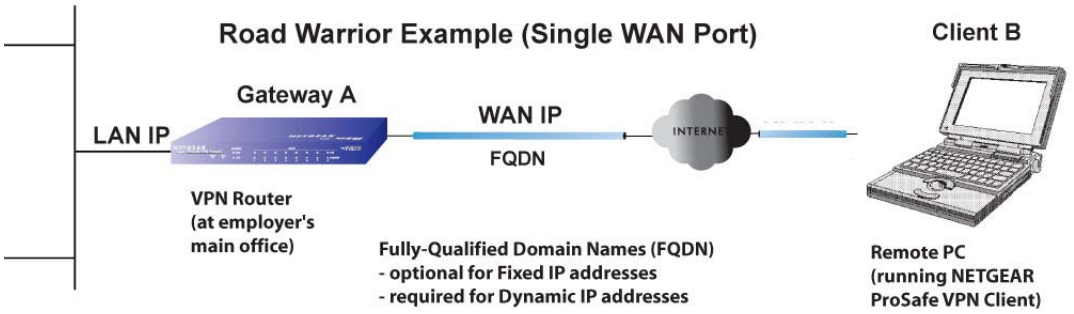


Figure 5-7

Follow these steps to configure the a VPN client tunnel:

- Configure the client policies on the gateway.
- Configure the VPN client to connect to the gateway.

Use the VPN Wizard Configure the Gateway for a Client Tunnel

1. Select **VPN** from the main menu and **VPN Wizard** from the submenu. The VPN Wizard screen will display. To view the wizard default settings, click the **VPN Wizard Default Values** link. You can modify these settings after completing the wizard.

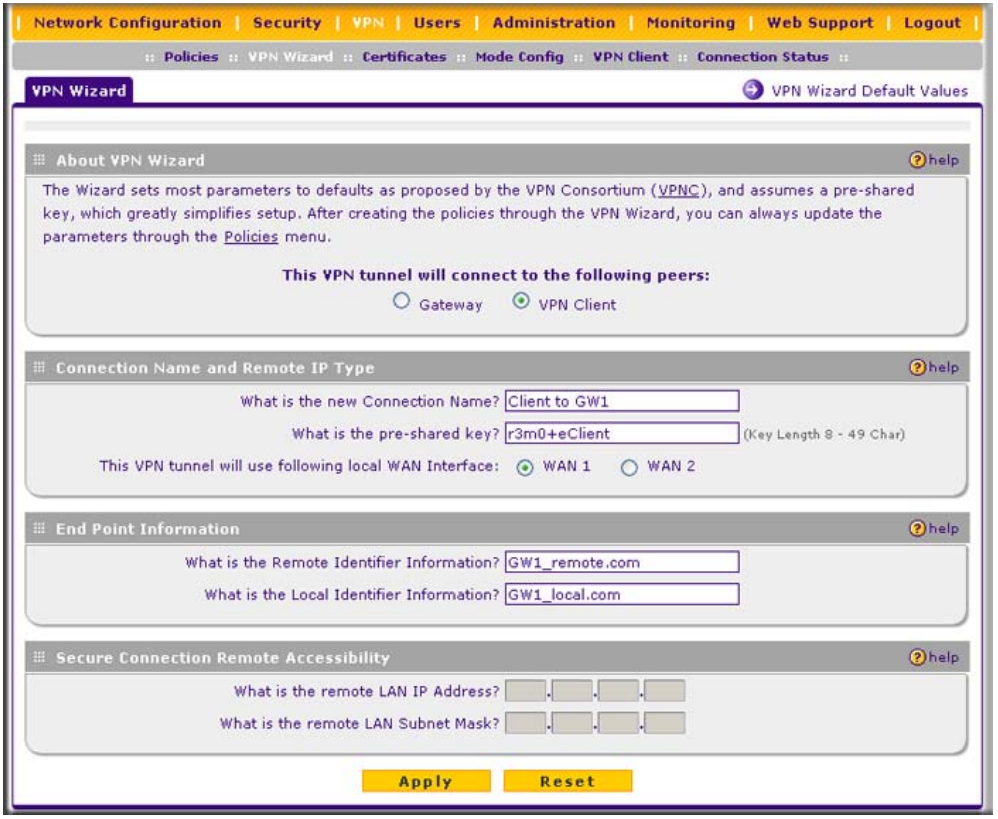


Figure 5-8

2. Select **VPN Client** as your VPN tunnel connection.
3. Create a **Connection Name** such as “Client to GW1”.

   This descriptive name is not supplied to the remote VPN client; it is only for your reference.

4. Enter a **Pre-shared Key**; in this example, we are using r3m0+eC1ient**,** which must also be entered in the VPN client software. The key length must be 8 characters minimum and cannot exceed 49 characters.

5. Choose which WAN port to use as the VPN tunnel end point.

> **Note:** If you are using a dual WAN rollover configuration, after completing the wizard, you must manually update the VPN policy to enable VPN rollover. This allows the VPN tunnel to roll over when the WAN Mode is set to Auto Rollover. The wizard will not set up the VPN policy with rollover enabled.

6. The public **Remote and Local Identifier** are automatically filled in by pre-pending the first several letters of the model number of your gateway to form FQDNs used in the VPN policies. In this example, we are using GW1_remote.com, and GW1_local.com.

> **Tip:** To assure tunnels stay active, after completing the wizard, manually edit the VPN policy to enable keepalive which periodically sends ping packets to the host on the peer side of the network to keep the tunnel alive.

7. Click **Apply** to save your settings. The VPN Policies screen shows that the policy is now enabled. (To view or modify the VPN policy, see "Managing VPN Policies" on page 5-16.)

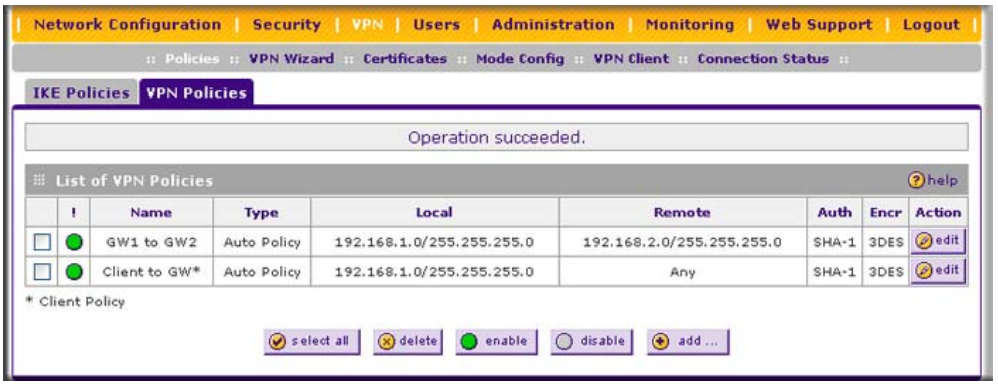


Figure 5-9

Use the NETGEAR VPN Client Security Policy Editor to Create a Secure Connection

From a PC with the NETGEAR ProSafe VPN Client installed, configure a VPN client policy to connect to the VPN firewall.

Follow these steps to configure your VPN client.

1. Right-click on the VPN client icon in your Windows toolbar, choose **Security Policy Editor,** and verify that the **Options** > **Secure** > **Specified Connections** selection is enabled.

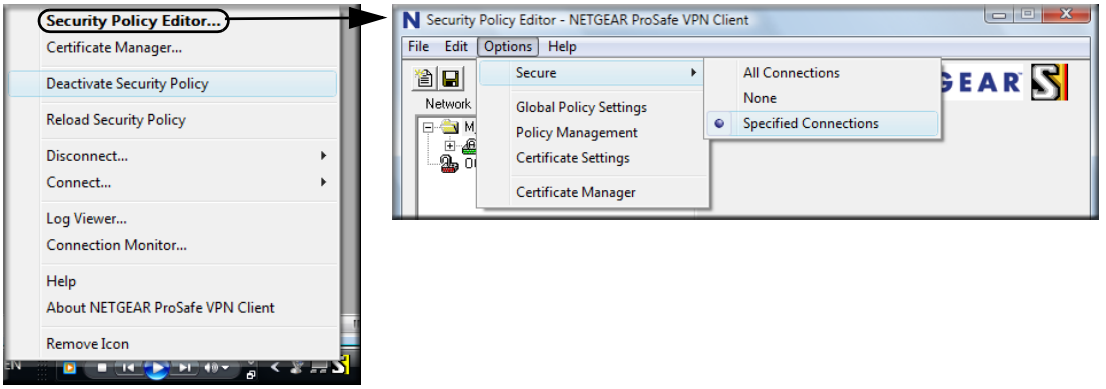


Figure 5-10

2. In the upper left of the Policy Editor window, click the New Document icon (the first on the left) to open a New Connection. Give the New Connection a name; in this example, we are using **gw1**.

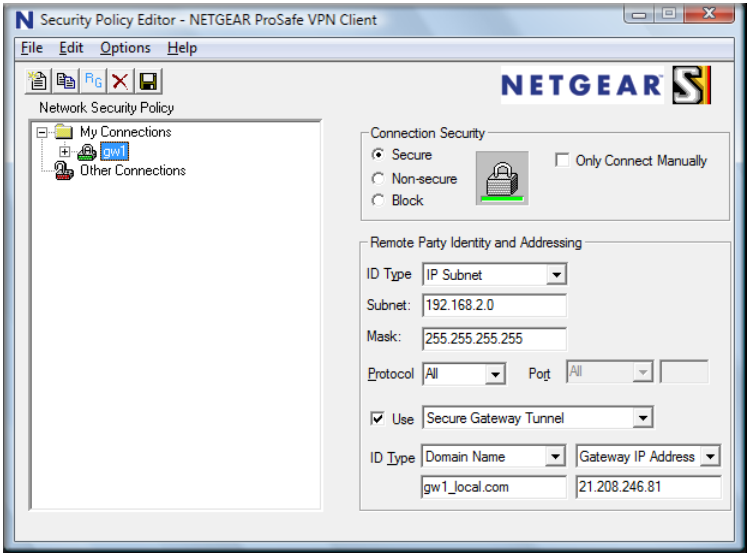


Figure 5-11

Fill in the other options according to the instructions below.

- Under Connection Security, verify that the Secure radio button is selected.
- From the **ID Type** pull-down menu, choose **IP Subnet**.
- Enter the LAN IP **Subnet Address** and **Subnet Mask** of the VPN firewall LAN; in this example, we are using 192.168.2.0.
- Check the **Use** checkbox and choose **Secure Gateway Tunnel** from the pull-down menu.
- From the first **ID Type** pull-down menus, choose **Domain Name.** Enter the FQDN address which the VPN firewall VPN Wizard provided; in this example, we are using gw1_local.com.
- From the second **ID Type** pull-down menu, choose **Gateway IP Address** and enter the WAN IP Gateway address of the VPN firewall; in this example, we are using 21.208.216.81.

3. In the left frame, click **My Identity**. Fill in the options according to the instructions below.

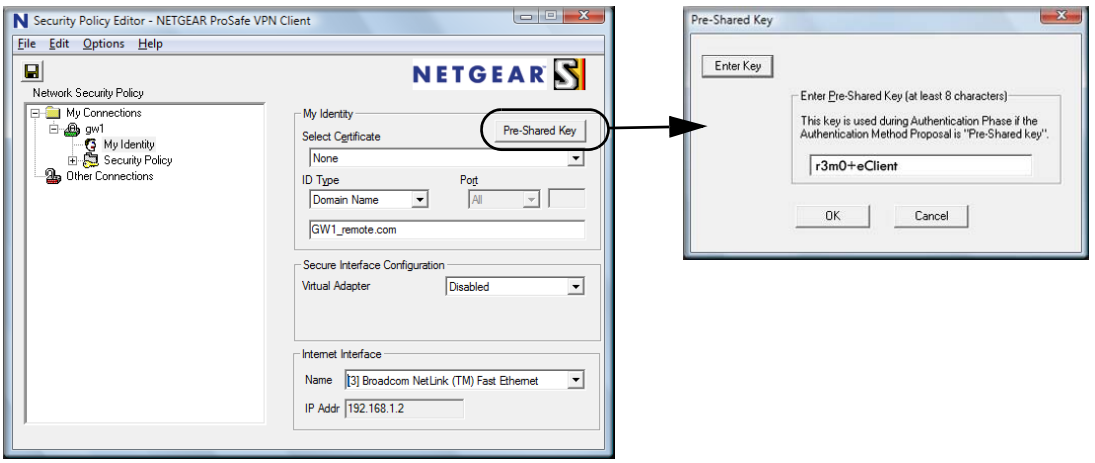


Figure 5-12

- From the **Select Certificate** pull-down menu, choose **None**.
- Click **Pre-Shared Key** to enter the key you provided in the VPN Wizard; in this example, we are using “r3m0+eC1ient.”
- From the ID Type pull-down menu, choose **Domain Name.**
- Leave **Virtual Adapter** disabled.
- In **Network Adapter** select the adapter you will use; the IP address of the selected adapter will display.

4. Verify the Security Policy settings; no changes are needed.

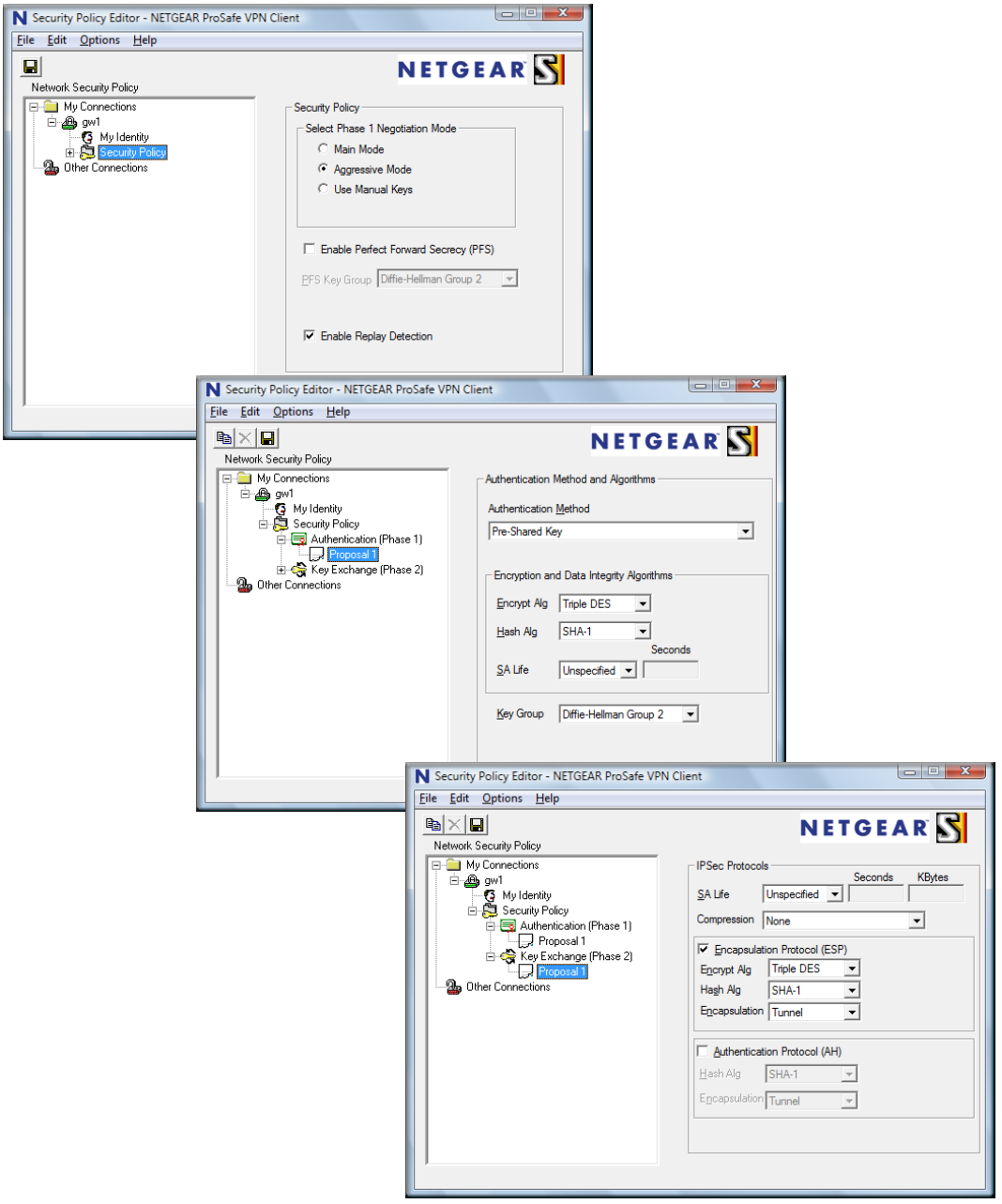

Security Policy Editor - NETGEAR ProSafe VPN Client
File Edit Options Help
NETGEAR
Network Security Policy
My Connections
gw1
My Identity
Security Policy
Other Connections
Security Policy
Select Phase 1 Negotiation Mode
Main Mode
Aggressive Mode
Use Manual Keys
Enable Perfect Forward Secrecy (PFS)
PFS Key Group
Diffie-Hellman Group 2
Enable Replay Detection
Security Policy Editor - NETGEAR ProSafe VPN Client
File Edit Options Help
NETGEAR
Network Security Policy
My Connections
gw1
My Identity
Security Policy
Authentication (Phase 1)
Proposal 1
Key Exchange (Phase 2)
Other Connections
Authentication Method and Algorithms
Authentication Method
Pre-Shared Key
Encryption and Data Integrity Algorithms
Encrypt Alg
Triple DES
Hash Alg
SHA-1
Seconds
SA Life
Unspecified
Key Group
Diffie-Hellman Group 2
Security Policy Editor - NETGEAR ProSafe VPN Client
File Edit Options Help
NETGEAR
Network Security Policy
My Connections
gw1
My Identity
Security Policy
Authentication (Phase 1)
Proposal 1
Key Exchange (Phase 2)
Proposal 1
Other Connections
IPSec Protocols
Seconds
KBytes
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 5-13

- On the left, click **Security Policy** to view the settings: no changes are needed.
- On the left, expand **Authentication (Phase 1)** and click **Proposal 1**: no changes are needed.
- On the left, expand **Key Exchange (Phase 2)** and click **Proposal 1**. No changes are needed.

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

Testing the Connections and Viewing Status Information

Both the NETGEAR VPN Client and the VPN firewall provide VPN connection and status information. This information is useful for verifying the status of a connection and troubleshooting problems with a connection.

NETGEAR VPN Client Status and Log Information

To test a client connection and view the status and log information, follow these steps.

1. To test the client connection, from your PC, right-click on the VPN client icon in your Windows toolbar and choose **Connect...**, then **My Connections\gw1**.

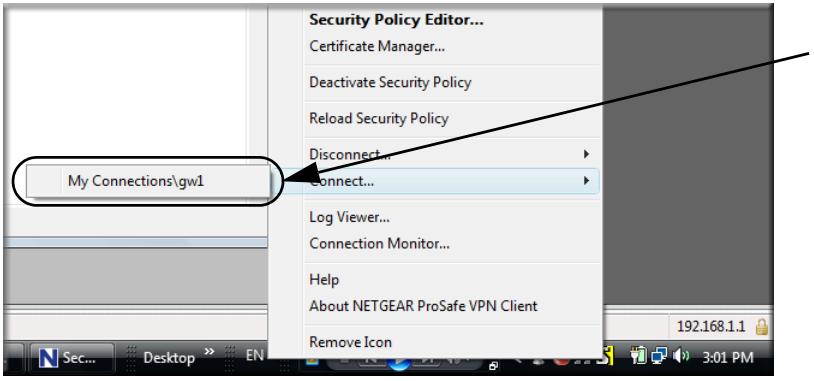


Figure 5-14

Within 30 seconds you should receive the message “Successfully connected to My Connections\gw1”.

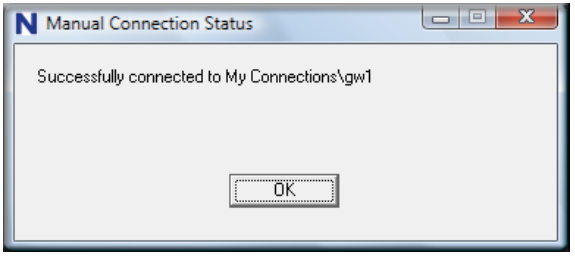


Figure 5-15

The VPN client icon in the system tray should state On: 

2. To view more detailed additional status and troubleshooting information from the NETGEAR VPN client, follow these steps.

- Right-click the VPN Client icon in the system tray and select Log Viewer.

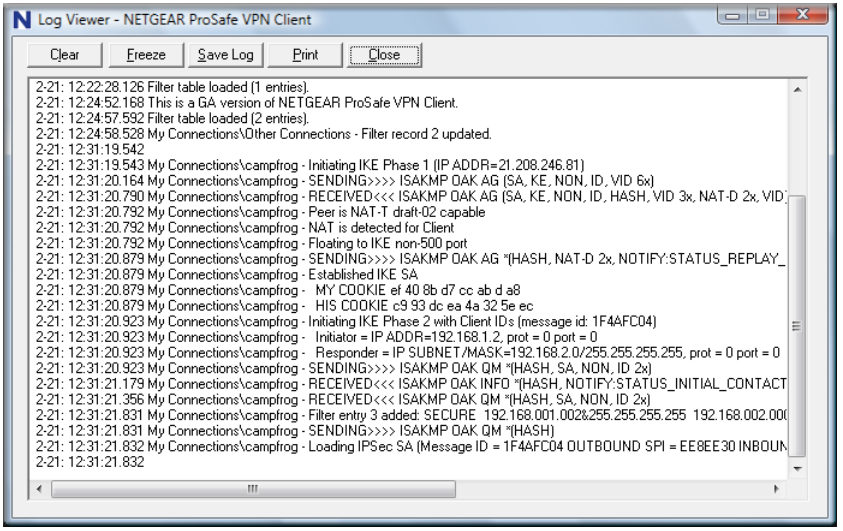


Figure 5-16

- Right-click the VPN Client icon in the system tray and select Connection Monitor.

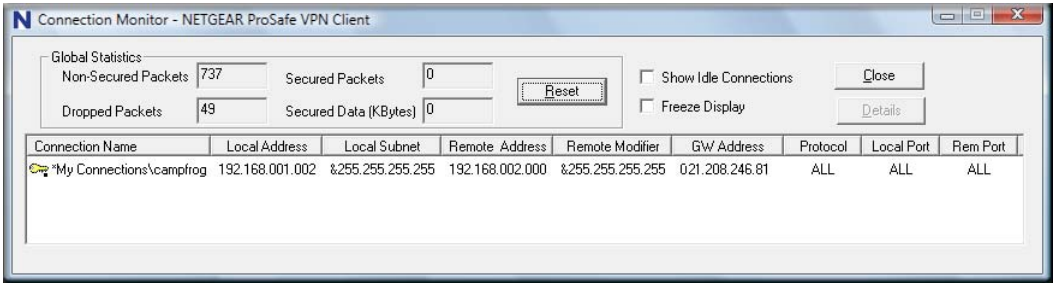


Figure 5-17

The VPN client system tray icon provides a variety of status indications, which are listed below.

Table 5-2.

System Tray Icon	Status
	The client policy is deactivated.
	The client policy is deactivated but not connected.
	The client policy is activated and connected. A flashing vertical bar indicates traffic on the tunnel.

VPN Firewall VPN Connection Status and Logs

To view VPN firewall VPN connection status, select **VPN** from the main menu and **Connection Status** from the submenu. The VPN Connection Status screen will display.

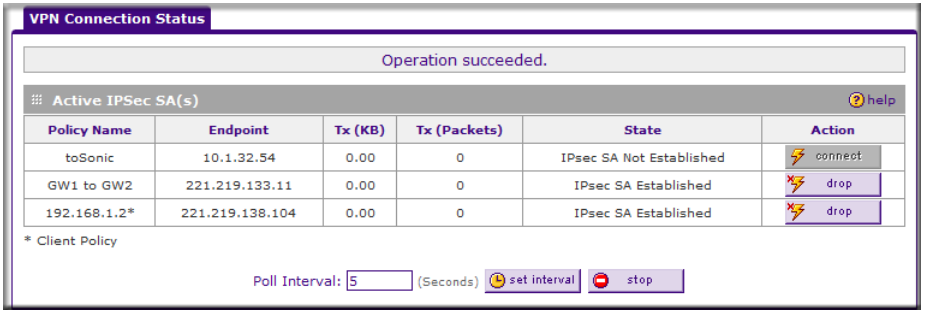


Figure 5-18

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.

To view VPN firewall VPN logs, select **Monitoring** from the main menu and **VPN Logs** from the submenu. The VPN Logs screen will display.

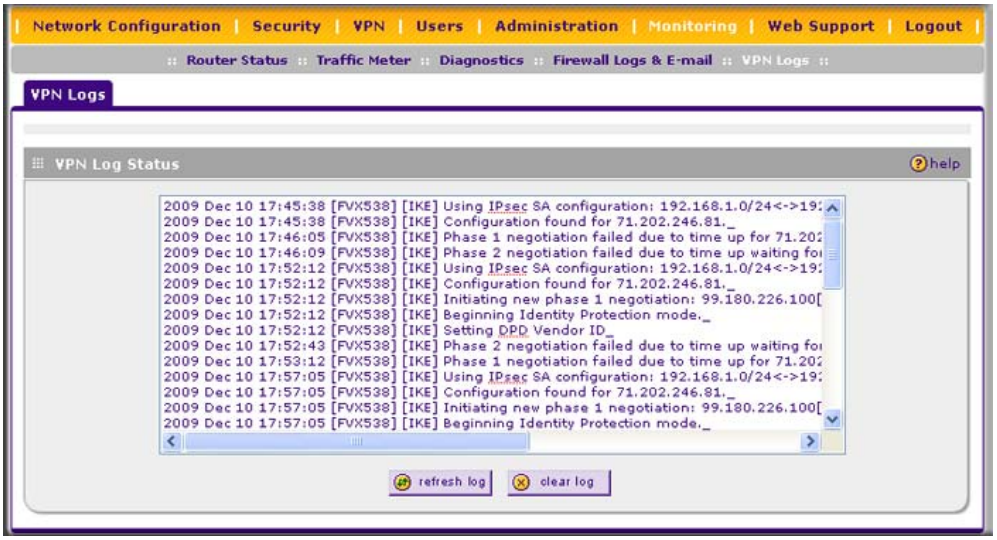


Figure 5-19

Managing VPN Policies

When you use the VPN Wizard to set up a VPN tunnel, both a VPN policy and an IKE policy are established and populated in both policy tables. The name you selected as the VPN Tunnel connection name during Wizard setup identifies both the VPN policy and IKE policy. You can edit existing policies, or add new VPN and IKE policies directly in the policy tables.

Note: You cannot modify an IKE policy that is associated with an enabled VPN policy. To modify the IKE policy, first disable the VPN policy. After you have modified and saved the IKE policy, you can then re-enable the VPN policy.

Configuring 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 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.

The IKE Policies Screen

When you use the VPN Wizard to set up a VPN tunnel, an IKE Policy is established and populated in the **List of IKE Policies** table on the IKE Policies screen 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 IKE Policies screen.

To view the IKE Policies screen, select **VPN** from the main menu and **Policies** from the submenu. The IKE Policies screen will display.

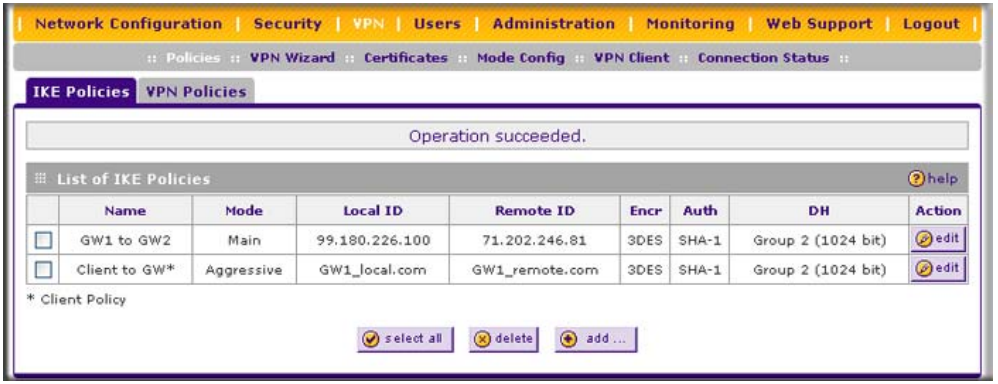


Figure 5-20

Each policy that is listed in the **List of IKE Policies** table 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.
- **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 identifier of this device. (The remote VPN must have this value as their “Remote ID”.)
- **Remote ID**. The IKE/ISAKMP identifier 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.)
- **Enable Dead Peer Detection**: Dead Peer Detection is used to detect whether the peer is alive or not. If the peer is detected as dead, the IPSec and IKE Security Association are deleted.

  To gain a more complete understanding of the encryption, authentication and DH algorithm technologies, see Appendix E, "Related Documents" for a link to the NETGEAR website.

Configuring 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 entered 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 "Managing Certificates" on page 5-19). 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 by any sender to encrypt data intended for the receiver (the key owner). The receiver then uses its private key to decrypt the data (without the private key, decryption is impossible). The use of certificates for authentication reduces the amount of data entry required on each VPN endpoint.

The VPN Policies Screen

The VPN Policies screen (see Figure 5-9 on page 5-8) 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 policies, or delete them entirely. The rules for VPN policy use are:

1. Traffic covered by a policy will automatically be sent via a VPN tunnel.
2. When traffic is covered by two or more policies, the first matching policy will be used. (In this situation, the order of the policies is important. However, if you have only one policy for each remote VPN Endpoint, then the policy order is not important.)
3. The VPN tunnel is created according to the parameters in the SA (Security Association).

4. The remote VPN Endpoint must have a matching SA, or it will refuse the connection.

Only one client policy may configured at a time (noted by an "*" next to the policy name). The **List of VPN Policies** 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).
- **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. (The subnet address is supplied as 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).
- **AH**. Authentication Header. The default setting using the VPN Wizard is SHA1. (This setting must match the remote VPN.)
- **ESP**. Encapsulating Security Payload. The default setting using the VPN Wizard is 3DES. (This setting must match the remote VPN.)
- **Action.** Allows you to access individual policies to make any changes or modifications.

Managing Certificates

Digital Self 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 VPN firewall during the IKE (Internet Key Exchange) authentication phase as an alternative authentication method.

The VPN firewall uses Digital Certificates (also known as X509 Certificates) during the Internet Key Exchange (IKE) authentication phase to authenticate connecting VPN gateways or clients, or to be authenticated by remote entities. The same Digital Certificates are extended for secure web access via SSL VPN connections over HTTPS.

Digital Certificates can be either self signed or can be issued by Certification Authorities (CA) such as via an in-house Windows server, or by an external organization such as Verisign or Thawte.

However, if the Digital Certificates contain the extKeyUsage extension then the certificate must be used for one of the purposes defined by the extension. For example, if the Digital Certificate contains the extKeyUsage extension defined to SNMPV2 then the same certificate cannot be used for secure web management.

The extKeyUsage would govern the certificate acceptance criteria in the VPN firewall when the same digital certificate is being used for secure web management.

In the VPN firewall, the uploaded digital certificate is checked for validity and also the purpose of the certificate is verified. Upon passing the validity test and the purpose matches its use (has to be SSL and VPN) the digital certificate is accepted. The additional check for the purpose of the uploaded digital certificate must correspond to use for VPN and secure web remote management via HTTPS. If the purpose defined is for VPN and HTTPS then the certificate is uploaded to the HTTPS certificate repository and as well in the VPN certificate repository. If the purpose defined is *only* for VPN then the certificate is only uploaded to the VPN certificate repository. Thus, certificates used by HTTPS and IPSec will be different if their purpose is not defined to be VPN and HTTPS.

The VPN firewall uses digital certificates to authenticate connecting VPN gateways or clients, and to be authenticated by remote entities. A certificate that authenticates a server, for example, is a file that contains:

- A public encryption key to be used by clients for encrypting messages to the server.
- Information identifying the operator of the server.
- A digital signature confirming the identity of the operator of the server. Ideally, the signature is from a trusted third party whose identity can be verified absolutely.

You can obtain a certificate from a well-known commercial Certificate Authority (CA) such as Verisign or Thawte, or you can generate and sign your own certificate. Because a commercial CA takes steps to verify the identity of an applicant, a certificate from a commercial CA provides a strong assurance of the server’s identity. A self-signed certificate will trigger a warning from most browsers as it provides no protection against identity theft of the server.

The VPN firewall contains a self-signed certificate from NETGEAR. We recommend that you replace this certificate prior to deploying the VPN firewall in your network.

From the Certificates screen, you can view the currently loaded certificates, upload a new certificate and generate a Certificate Signing Request (CSR). Your VPN firewall will typically hold two types of certificates:

- CA certificate. Each CA issues its own CA identity certificate in order to validate communication with the CA and to verify the validity of certificates signed by the CA.
- Self certificate. The certificate issued to you by a CA identifying your device.

Viewing and Loading CA Certificates

The Trusted Certificates (CA Certificates) table lists the certificates of CAs and contains the following data:

- **CA Identity (Subject Name)**. The organization or person to whom the certificate is issued.
- **Issuer Name**. The name of the CA that issued the certificate.
- **Expiry Time**. The date after which the certificate becomes invalid.

To view the VPN Certificates:

Select **VPN** from the main menu and **Certificates** from the submenu. The Certificates screen will display. The top section of the Certificates screen displays the **Trusted Certificates (CACertificates)** section.

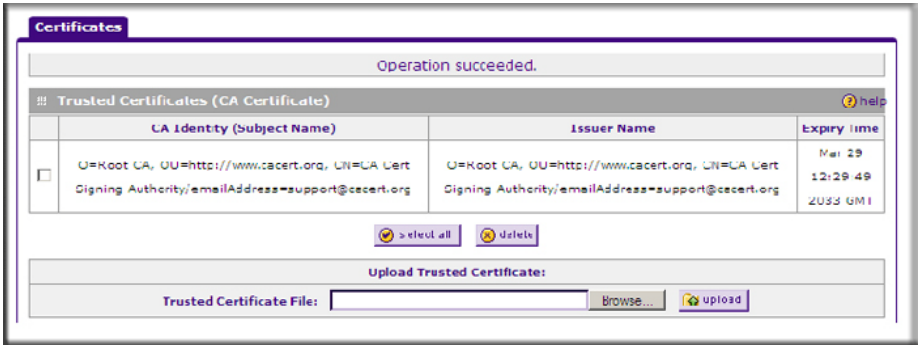


Figure 5-21

When you obtain a self certificate from a CA, you will also receive the CA certificate. In addition, many CAs make their certificates available on their Websites.

To load a CA certificate into your VPN firewall:

1. Store the CA certificate file on your computer.
2. Under **Upload Trusted Certificates** in the Certificates menu, click Browse and locate the CA certificate file.
3. Click **Upload**. The CA Certificate will appear in the **Trusted Certificates (CA Certificates)** table.

Viewing Active Self Certificates

The **Active Self Certificates** table on the Certificates screen shows the certificates issued to you by a CA and available for use.

Figure 5-22

For each self certificate, the following data is listed:

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

Obtaining a Self Certificate from a Certificate Authority

To use a self certificate, you must first request the certificate from the CA, then download and activate the certificate on your system. To request a self certificate from a CA, you must generate a Certificate Signing Request (CSR) for your VPN firewall. The CSR is a file containing information about your company and about the device that will hold the certificate. Refer to the CA for guidelines on the information you include in your CSR.

To generate a new Certificate Signing Request (CSR) file:

1. Locate the **Generate Self Certificate Request** section of the Certificates screen.

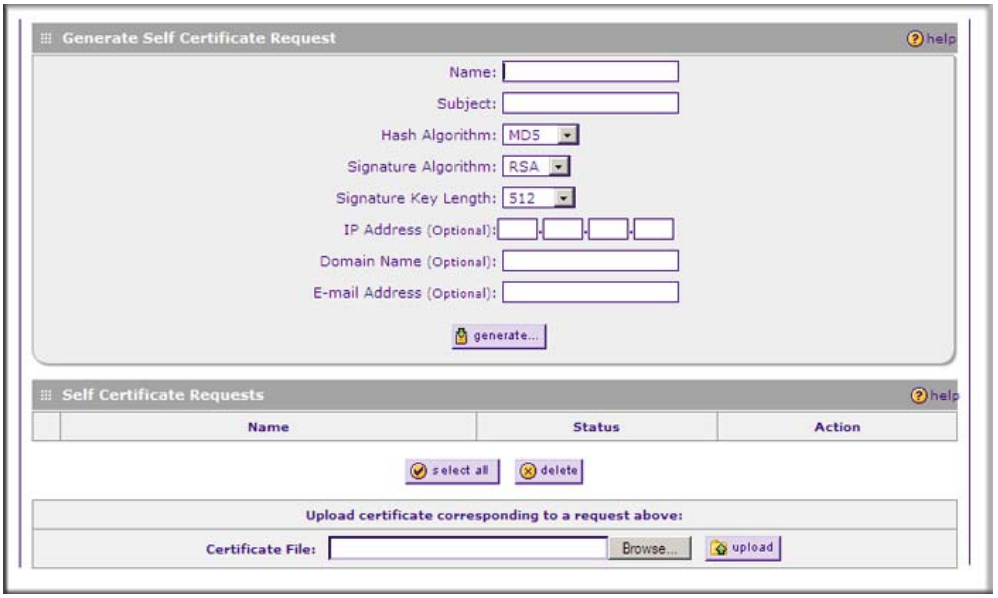


Figure 5-23

2. Configure the following fields:
   - **Name** – Enter a descriptive 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. (Using the same name, or a derivation of the name, in the Title field would be useful.)
   - From the pull-down menus, choose 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 decrease 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 an Internet domain name, you can enter it here. Otherwise, you should leave this field blank.
- **E-mail Address** – Enter the e-mail address of a technical contact in your organization.

4. Click **Generate**. A new certificate request is created and added to the **Self Certificate Requests** table.

Figure 5-24

5. In the **Self Certificate Requests** table, click **view** in the Action column to view the request.

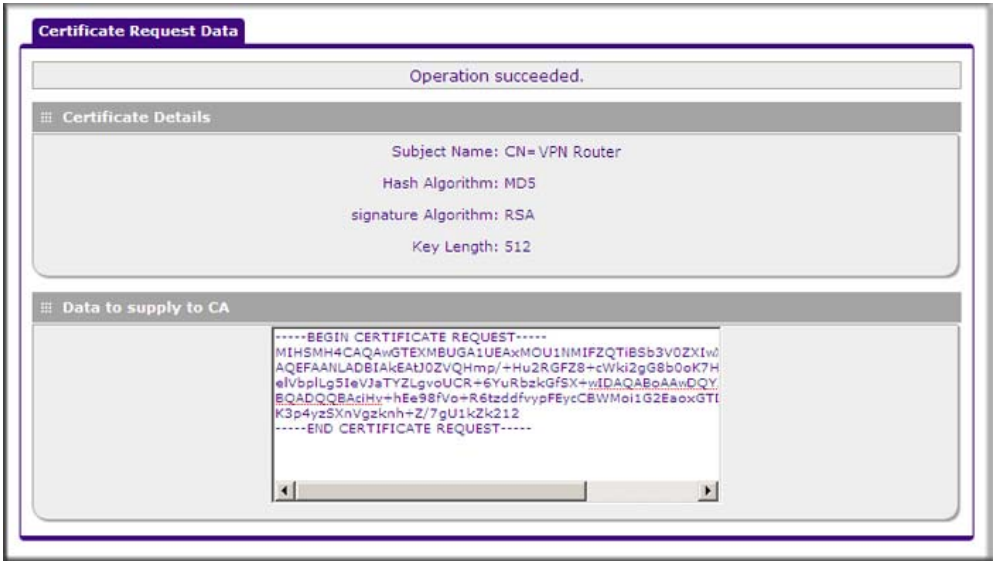


Figure 5-25

6. Copy the contents of the **Data to supply to CA** text box into a text file, including all of the data contained from "----BEGIN CERTIFICATE REQUEST---" to "---END CERTIFICATE REQUEST---".

7. Submit your certificate request to a CA:
   a. Connect to the website of the CA.
   b. Start the Self Certificate request procedure.
   c. When prompted for the requested data, copy the data from your saved text file (including "----BEGIN CERTIFICATE REQUEST---" and "---END CERTIFICATE REQUEST").
   d. Submit the CA form. If no problems ensue, the certificate will be issued.
8. Store the certificate file from the CA on your computer.
9. Return to the Certificates screen and locate the **Self Certificate Requests** section (see Figure 5-24 on page 5-24).
10. Select the checkbox next to the certificate request, then click **Browse** and locate the certificate file on your PC.
11. Click **Upload**. The certificate file will be uploaded to this device and will appear in the **Active Self Certificates** list.

If you have not already uploaded the CA certificate, do so now, as described in "Viewing and Loading CA Certificates" on page 5-21. You should also periodically check the **Certificate Revocation Lists (CRL)** table, as described in the following section.

Managing your Certificate Revocation List (CRL)

A CRL (Certificate Revocation List) file shows certificates that 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.

In the Certificates menu, you can view your currently-loaded CRLs and upload a new CRL.

To view your currently-loaded CRLs and upload a new CRL, follow these steps:

1. Locate the **Certificate Revocation Lists (CRL)** table at the bottom of the Certificates screen.

Figure 5-26

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

- **CA Identify –** 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.

2. Click **Browse** and locate the CRL file you previously downloaded from a CA.
3. Click **Upload.** The CRL file will be uploaded and the CA Identity will appear in the **Certificate Revocation Lists (CRL)** table. If you had a previous CA Identity from the same CA, it will be deleted.

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 VPN firewall 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 VPN firewall 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.

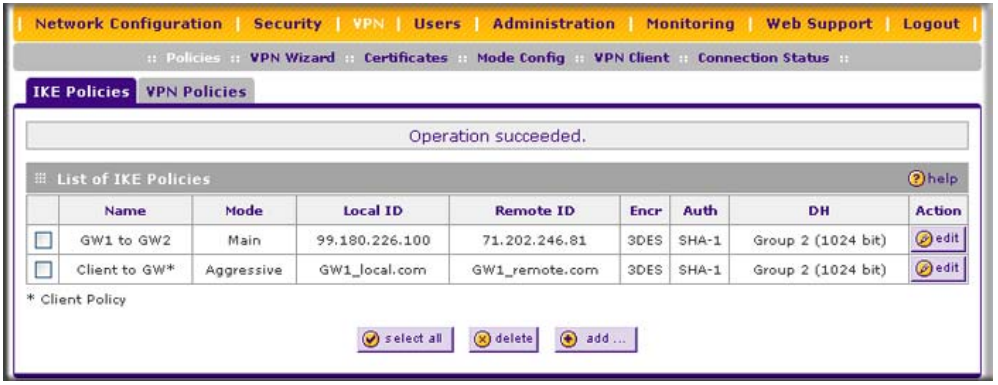


Figure 5-27

2. You can add XAUTH to an existing IKE policy by clicking **Edit** adjacent to the policy to be modified or you can create a new IKE policy incorporating XAUTH by clicking **Add**. (Figure 5-28 on page 5-28 shows the Add IKE Policy screen.)

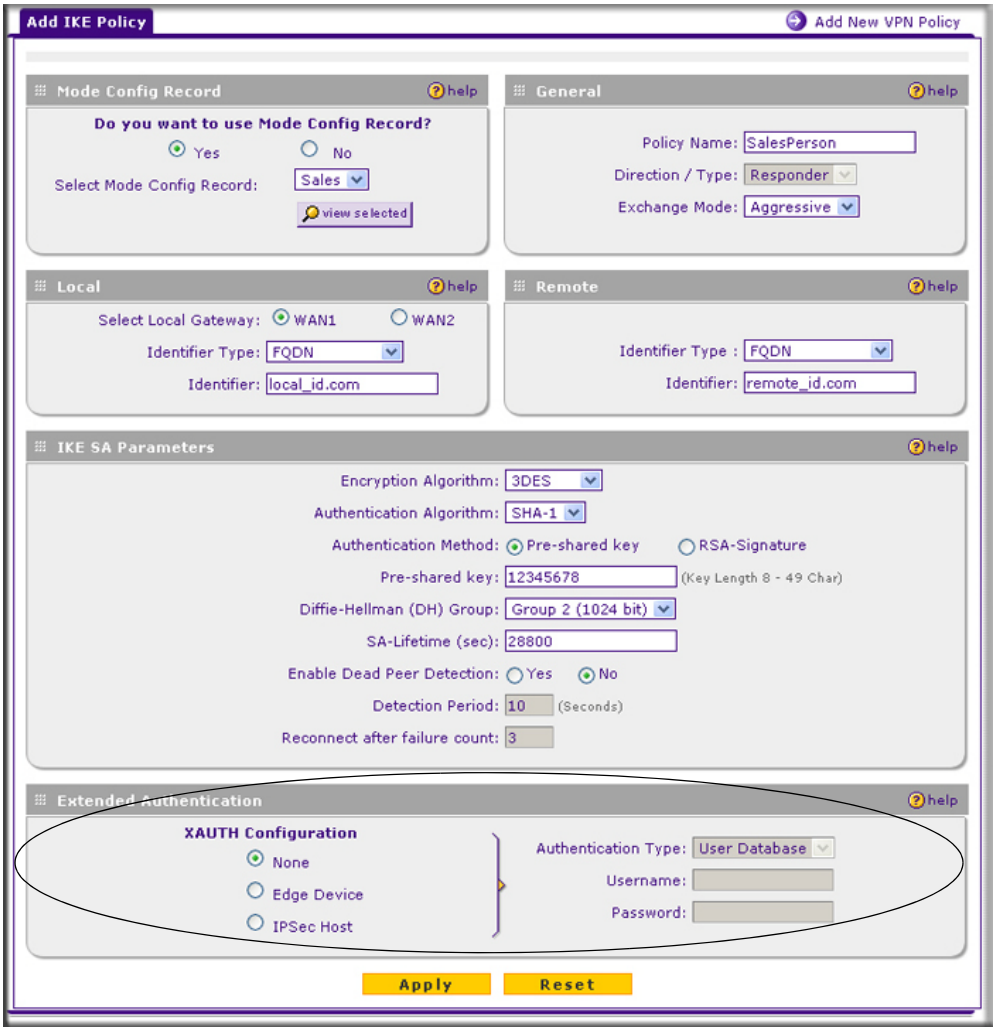


Figure 5-28

3. In the **Extended Authentication** section of the Add IKE Policy (or Edit IKE Policy) screen, select the **Authentication Type** from the pull-down menu which will be used to verify user account information. Select one of the following options:

   - **Edge Device**. Use the VPN firewall 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 VPN firewall's user database. Users must be added through the User Database screen (see "User Database Configuration" on page 5-29).
  - **RADIUS–CHAP** or **RADIUS–PAP** (depending on the authentication mode accepted by the RADIUS server) to add a RADIUS server. If RADIUS–PAP is selected, the VPN firewall will first check in the User Database to see if the user credentials are available. If the user account is not present, the VPN firewall will then connect to the RADIUS server (see "RADIUS Client Configuration" on page 5-30).

- **IPSec Host**. Enable authentication 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.

User Database Configuration

The User Database screen is used to configure and administer users when Extended Authentication is enabled as an Edge Device. Whether or not you use an external RADIUS server, you may want some users to be 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.

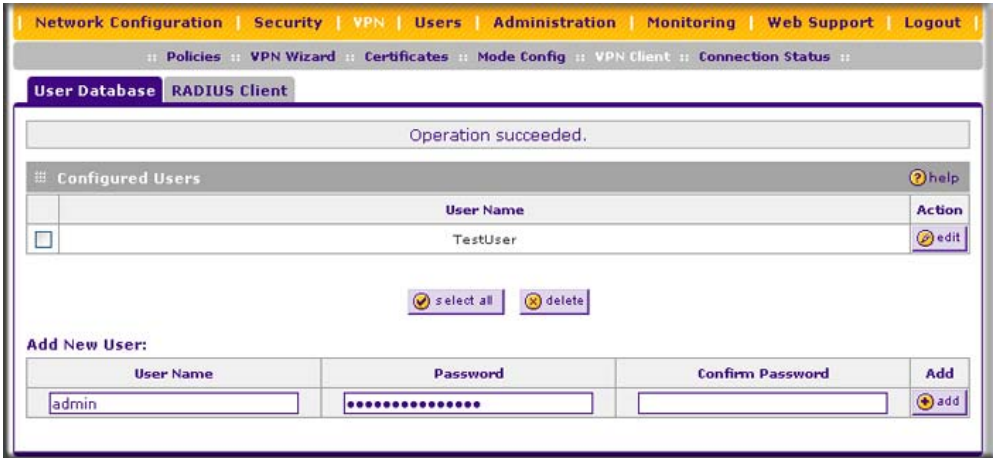


Figure 5-29

2. Enter a **User Name**. This is the unique ID of a user which will be added to the User Name database.
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 Users** table.

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.
3. Click **Reset** to cancel your changes or click **Apply** to save your settings 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 RADIUS servers:

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

2. Select the **RADIUS Client** tab. The RADIUS Client screen will display.

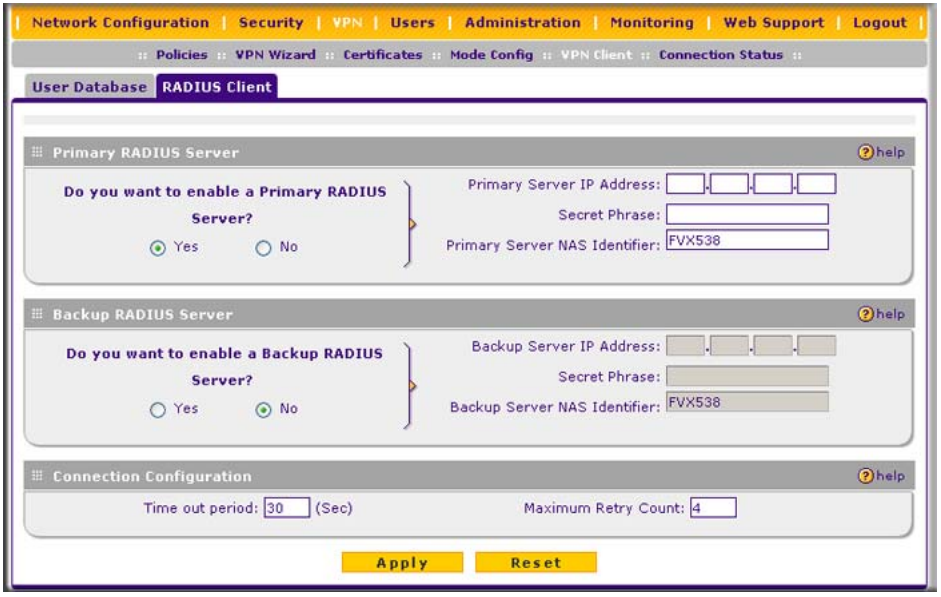


Figure 5-30

3. Enable the primary RADIUS server by checking the **Yes** radio box.
4. Enter the primary **RADIUS Server IP address**.
5. 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.
6. 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 VPN firewall 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 VPN firewall'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.
7. Enable a backup RADIUS server (if required) by following steps 3 through 6.

8. Set the **Time Out Period**, in seconds, that the VPN firewall should wait for a response from the RADIUS server.
9. Set the **Maximum Retry Count.** This is the number of attempts that the VPN firewall will make to contact the RADIUS server before giving up.
10. Click **Reset** to cancel any changes and revert to the previous settings or click **Apply** to save the settings.

Note: Selection of the Authentication Protocol, usually PAP or CHAP, is configured on the individual IKE policy screens.

Assigning IP Addresses to Remote Users (ModeConfig)

To simply the process of connecting remote VPN clients to the VPN firewall, you can use the ModeConfig screen to assign IP addresses to remote users, including a network access IP address, subnet mask, and name server addresses from the VPN firewall. 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 200
  - 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

Mode Config Operation

After the IKE Phase 1 negotiation is complete, the VPN connection initiator (which is the remote user with a VPN client) requests the IP configuration settings such as the IP address, subnet mask and name server addresses. The Mode Config feature 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 Mode Config record. The Mode Config feature allocates an

IP address from the configured IP address pool and activates a temporary IPsec policy, using the information that is specified in the Traffic Tunnel Security Level section of the Mode Config record (on the Add Mode Config Record screen that is shown in Figure 5-32 on page 5-34).

Note: After configuring a Mode Config record, you must manually configure an IKE policy and select the newly-created Mode Config record from the Select Mode Config Record pull-down menu (see "Configuring Mode Config Operation on the VPN Firewall." You do not need to make changes to any VPN policy.

Note: An IP address that is allocated to a VPN client is released only after the VPN client has gracefully disconnected or after the SA lifetime for the connection has timed out.

Configuring Mode Config Operation on the VPN Firewall

You need to configure two screens: the ModeConfig screen and the IKE Policies screen.

Configuring the Mode Config Screen

To configure the Mode Config screen:

1. From the main menu, select **VPN**, and then select **Mode Config** from the submenu. The Mode Config screen will display.

Figure 5-31

2. Click **Add**. The Add Mode Config Record screen will display.

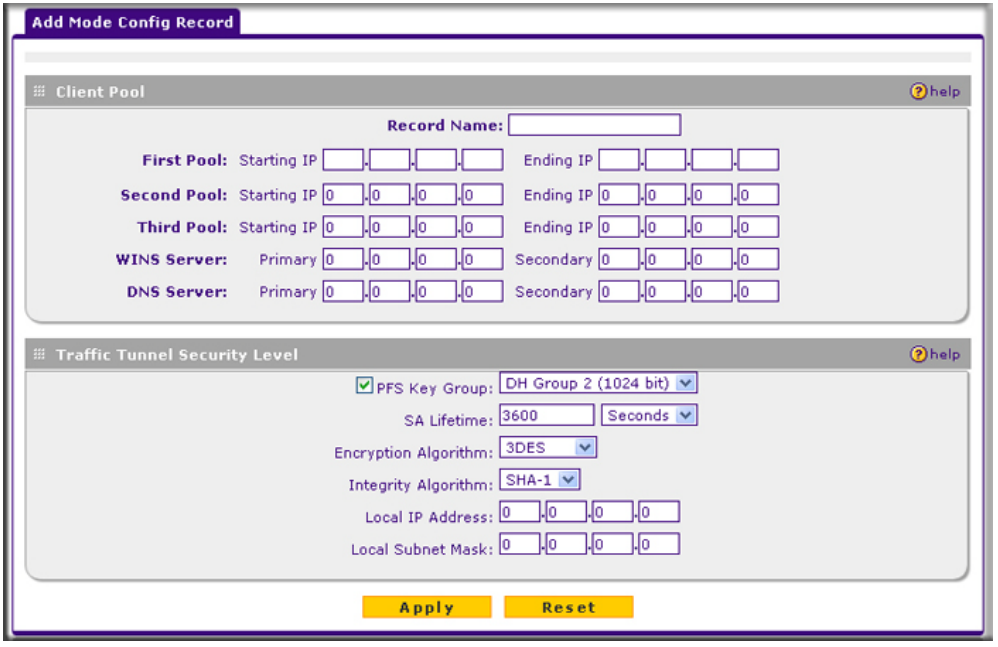


Figure 5-32

3. Enter a descriptive Record Name such as “Sales”.
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 VPN firewall’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 VPN firewall.)

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 **List of Mode Config Records** on the Mode Config screen.

Configuring an IKE Policy for Mode Config Operation

Next, you must configure an IKE policy:

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

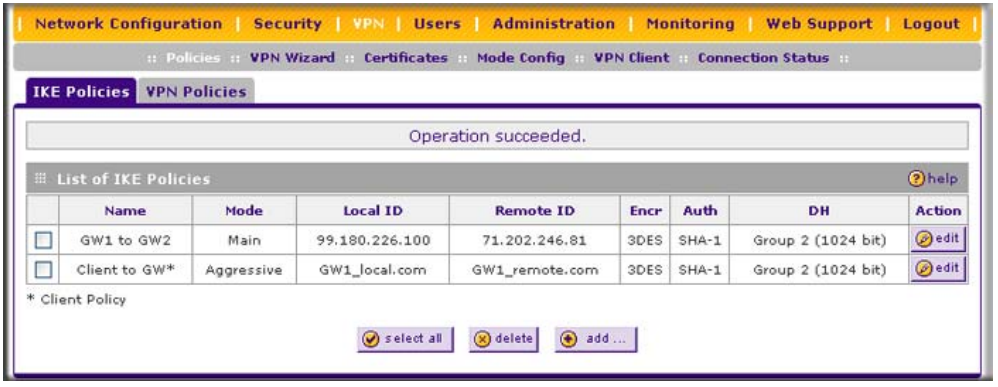


Figure 5-33

2. Click **Add** to configure a new IKE Policy. The Add IKE Policy screen will display.

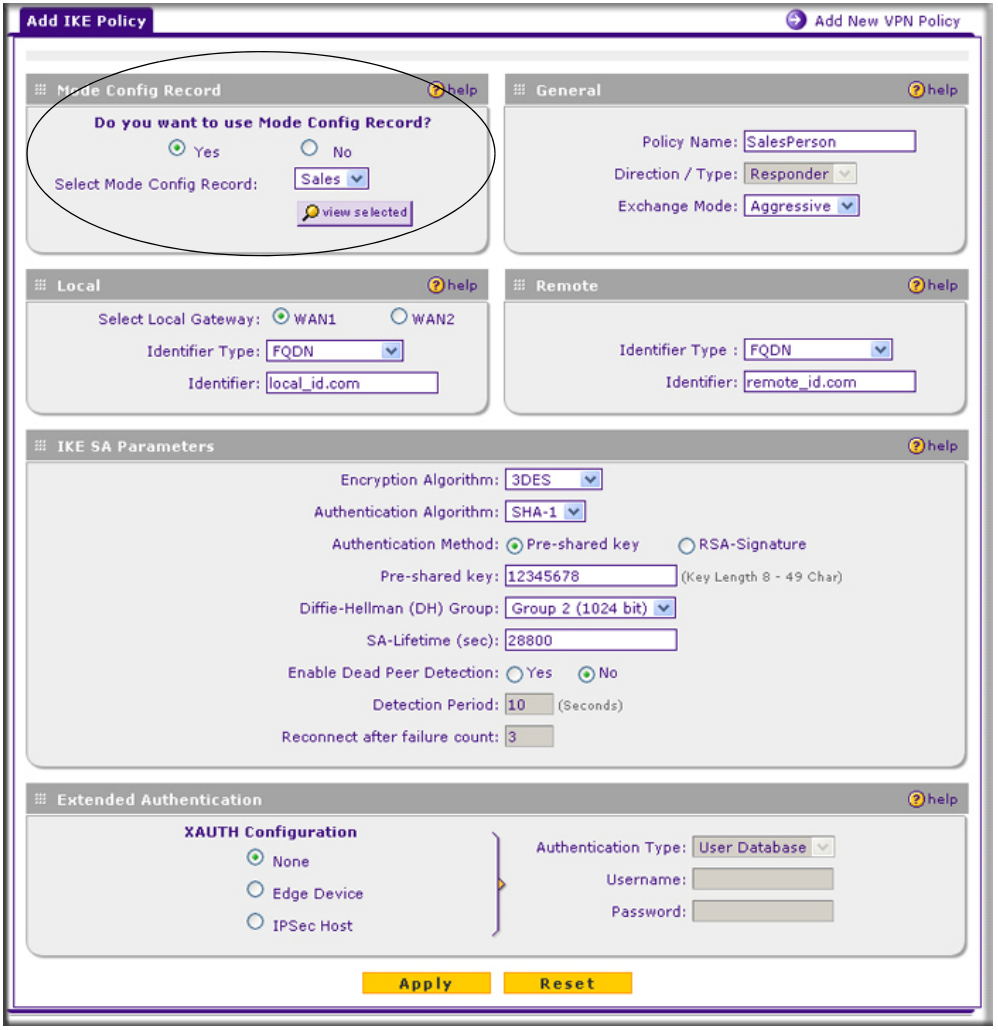


Figure 5-34

3. In the **Mode Config Record** section, 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** button.)

   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:
   - 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.
   - Set Direction/Type to Responder.
   - The Exchange Mode will automatically be set to Aggressive.
5. In the **Local** section, select **FQDN** for the Identity Type.
6. In the **Local** section, choose which WAN port to use as the VPN tunnel end point.
7. In the **Remote** section, enter an identifier in the Identity Type 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.
8. In the **IKE SA Parameters** section, 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
9. Enter a Pre-Shared Key that will also be configured in the VPN client.
10. XAUTH is disabled by default. To enable XAUTH, in the **Extended Authentication** section, select one of the following::
    - **Edge Device** to use the VPN firewall 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.)
    - **IPsec Host** if you want the VPN firewall 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).

    For more information on XAUTH, see “Configuring XAUTH for VPN Clients” on page 5-27.
11. 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 through the User Database screen (see “User Database Configuration” on page 5-29 or “RADIUS Client Configuration” on page 5-30).

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

12. Click **Apply.** The new policy will appear in the **List of IKE Policies** table.

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.

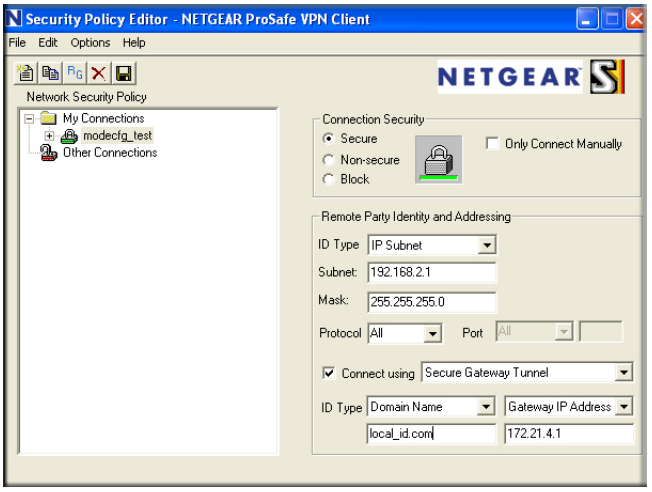


Figure 5-35

Enter the following information:

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”.

2. From the left side of the menu, click My Identity.

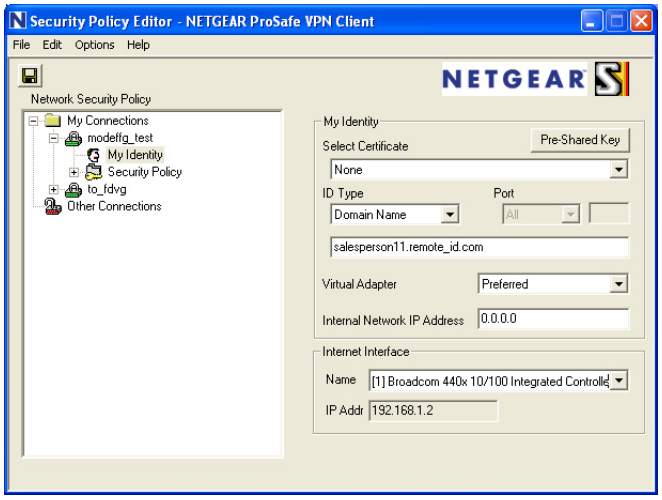


Figure 5-36

Enter the following information:

a. Click **Pre-Shared Key** and enter the key you configured in the VPN firewall’s Add IKE Policy screen

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 “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.

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

Enter the following information:

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.

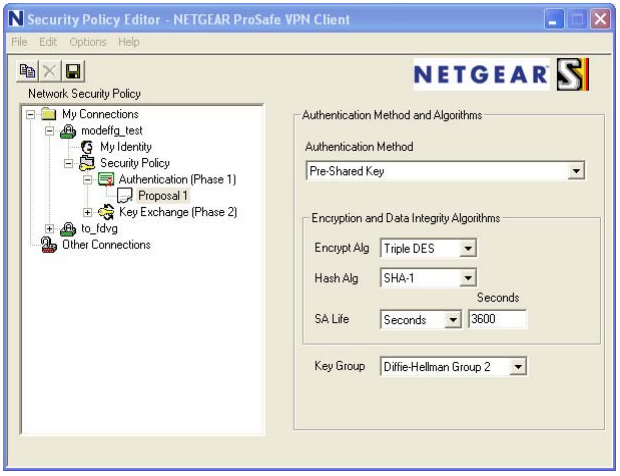


Figure 5-37

Enter the Authentication values to match those in the VPN firewall ModeConfig Record screen.

5. Click on Key Exchange (Phase 2) on the left-side of the menu and select Proposal 1.

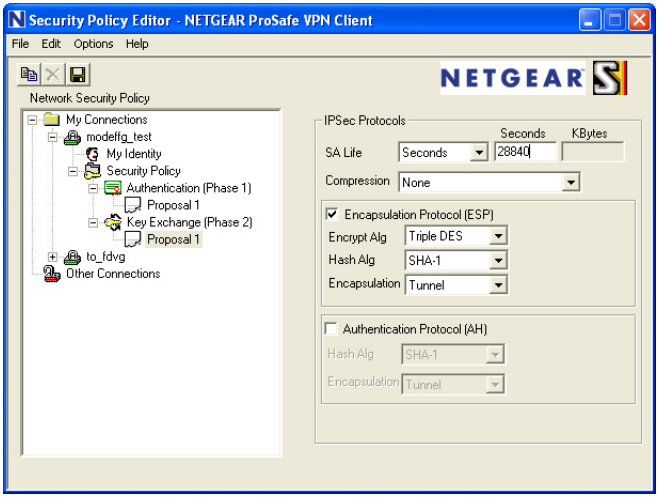


Figure 5-38

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).

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

Testing the Mode Config Connection

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.

Configuring Keepalives and Dead Peer Detection

In some cases, it may not be desirable to have a VPN tunnel drop when traffic is idle; for example, when client-server applications over the tunnel cannot tolerate the tunnel establishment time. If you require your VPN tunnel to remain connected, you can use the Keepalive and Dead Peer Detection features to prevent the tunnel from dropping and to force a reconnection if the tunnel drops for any reason.

For Dead Peer Detection to function, the peer VPN device on the other end of the tunnel must also support Dead Peer Detection. Keepalive, though less reliable than Dead Peer Detection, does not require any support from the peer device.

Configuring Keepalives

The keepalive feature maintains the IPSec SA by sending periodic ping requests to a host across the tunnel and monitoring the replies. To configure the keepalive on a configured VPN policy, follow these steps:

1. Select **VPN** from the main menu and **Policies** from the submenu.
2. Click the **VPN Policies** tab, then click the **edit** button next to the desired VPN policy.
3. In the **General** section of the Edit VPN Policy screen, locate the keepalive configuration settings.

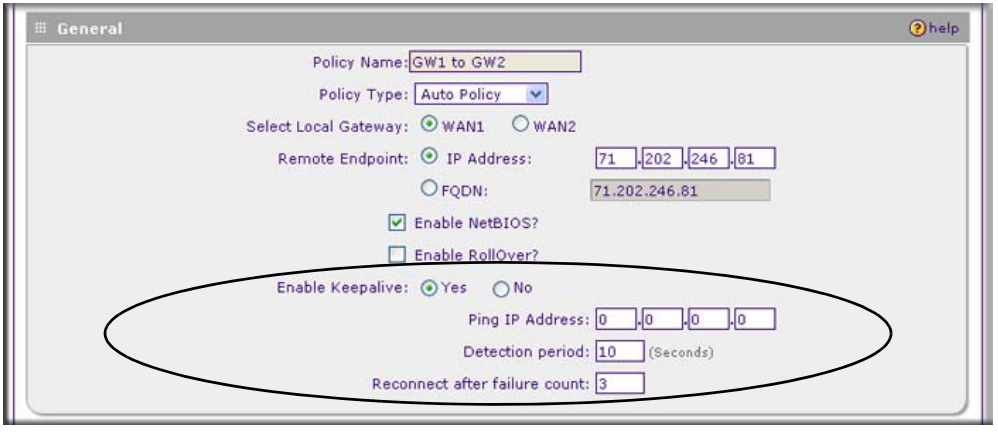


Figure 5-39

4. Click the **Yes** radio button to enable keepalive.

5. In the **Ping IP Address** boxes, enter an IP address on the remote LAN. This must be the address of a host that can respond to ICMP ping requests.
6. Enter the **Detection Period** to set the time between ICMP ping requests. The default is 10 seconds.
7. In **Reconnect after failure count**, set the number of consecutive missed responses that will be considered a tunnel connection failure. The default is 3 missed responses. When the VPN firewall senses a tunnel connection failure, it forces a reestablishment of the tunnel.
8. Click **Apply** at the bottom of the screen.

Configuring Dead Peer Detection

The Dead Peer Detection feature maintains the IKE SA by exchanging periodic messages with the remote VPN peer. To configure Dead Peer Detection on a configured IKE policy, follow these steps:

1. Select **VPN** from the main menu and **Policies** from the submenu.
2. Click the **IKE Policies** tab, then click the **edit** button next to the desired VPN policy.
3. In the **IKE SA Parameters** section of the Edit IKE Policy screen, locate the Dead Peer Detection configuration settings.

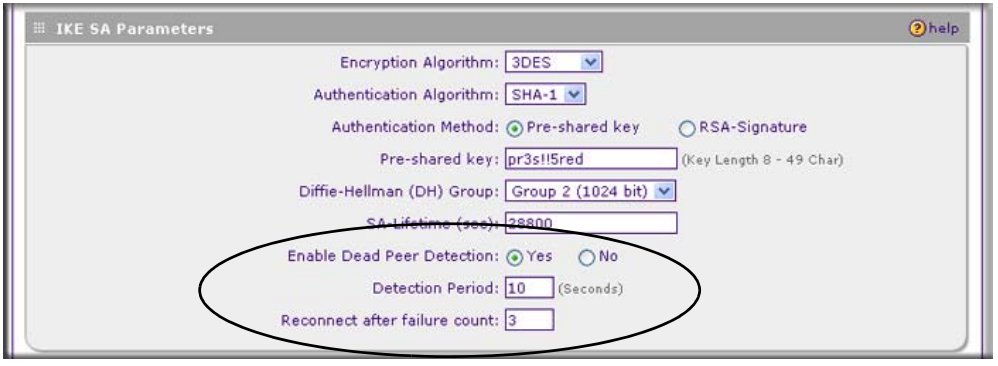


Figure 5-40

4. Click the **Yes** radio button to **Enable Dead Peer Detection**.
5. Enter the **Detection Period** to set the interval between consecutive DPD R-U-THERE messages. DPD R-U-THERE messages are sent only when the IPSec traffic is idle. The default is 10 seconds.

6. In **Reconnect after failure count**, set the number of DPD failures allowed before tearing down the connection. The default is 3 failures. When the VPN firewall senses an IKE connection failure, it deletes the IPSec and IKE Security Association and forces a reestablishment of the connection.
7. Click **Apply** at the bottom of the screen.

Configuring NetBIOS Bridging with VPN

Windows networks use the Network Basic Input/Output System (NetBIOS) for several basic network services such as naming and neighborhood device discovery. Because VPN routers do not normally pass NetBIOS traffic, these network services do not work for hosts on opposite ends of a VPN connection. To solve this problem, you can configure the VPN firewall to bridge NetBIOS traffic over the VPN tunnel. To enable NetBIOS bridging on a configured VPN tunnel, follow these steps:

1. Select **VPN** from the main menu and **Policies** from the submenu.
2. Click the **VPN Policies** tab, then click the **edit** button next to the desired VPN policy.
3. In the **General** section of the Edit VPN Policy screen, click the **Enable NetBIOS** checkbox.

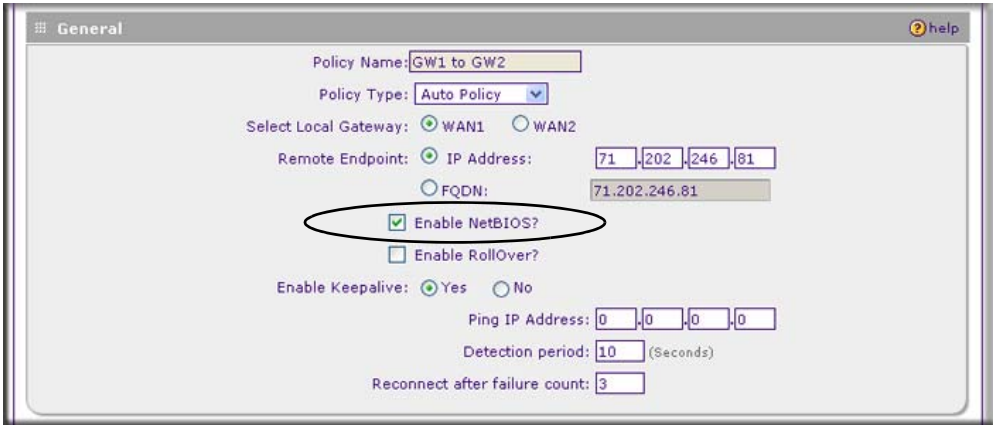


Figure 5-41

4. Click **Apply** at the bottom of the screen.

Chapter 6
VPN Firewall and Network Management

This chapter describes how to use the network management features of your ProSafe VPN Firewall 200 FVX538.

This chapter includes the following sections:

- "Performance Management" on this page
- "Configuring Users, Administrative Settings, and Remote Management" on page 6-8
- "Monitoring System Performance" on page 6-23

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.

Bandwidth Capacity

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

- LAN side: 1,800 Mbps (eight LAN ports at 100 Mbps each, plus one Gigabit LAN port)
- WAN side: 200 Mbps (load balancing mode, two WAN ports at 100 Mbps each) or 100 Mbps (rollover mode, one active WAN port at 100 Mbps)

In practice, the WAN side bandwidth capacity will be much lower when DSL or cable modems are used to connect to the Internet. At 1.5 Mbps, the WAN ports will support the following traffic rates:

- Load balancing mode: 3 Mbps (two WAN ports at 1.5 Mbps each)
- Rollover mode: 1.5 Mbps (one active WAN port at 1.5 Mbps)

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

Using the dual WAN ports in load balancing mode increases the bandwidth capacity of the WAN side of the VPN firewall. But there is no backup in case one of the WAN ports fail. In such an event and with one exception, the traffic that would have been sent on the failed WAN port gets diverted to the WAN port that is still working, thus increasing its loading. The exception is traffic that is bound by protocol to the WAN port that failed. This protocol-bound traffic is not diverted.

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
- Blocking sites
- Source MAC filtering

Service Blocking

You can control specific outbound traffic (for example, from LAN to WAN and from DMZ to WAN). The LAN WAN Rules screen and the DMZ WAN Rules screen list 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. (See “Using Rules to Block or Allow Specific Kinds of Traffic” on page 4-2 for the procedure on how to use this feature.)

	**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 (see “Managing Groups and Hosts (LAN Groups)” on page 3-6to assign PCs to a group using Network Database).

- **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 a rule. If the desired service or application does not appear in the list, you must define it using the Services screen (see “Adding Customized Services” on page 4-24).
- **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 the VPN firewall 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 Setup 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.
  - **Manual Entry**. You can manually enter information about a device.

  See “Managing Groups and Hosts (LAN Groups)” on page 3-6 for the procedure on how to use this feature.
- **Schedule**. If you have set firewall rules on one of the the LAN WAN Rules screen and the DMZ WAN Rules screen, you can configure three different schedules (that is, 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 Specific Traffic” on page 4-29 for the procedure on how to use this feature.)

Blocking 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 website is allowed.

- **Keyword (and Domain Name) Blocking**. You can specify up to 32 words that, should they appear in the website name (that is, 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 "Blocking Internet Sites (Content Filtering)" on page 4-30 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 "Configuring Source MAC Filtering" on page 4-33 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 VPN 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 (that is, the service is unavailable). You can also create additional firewall rules that are customized to block or allow specific traffic. (See "Using Rules to Block or Allow Specific Kinds of Traffic" on page 4-2 for the procedure on how to use this feature.)

Warning: This feature is for advanced administrators only! Incorrect configuration will cause serious problems.

You can control specific inbound traffic (that is, from WAN to LAN and from WAN to DMZ). The LAN WAN Rules screen and the DMZ WAN Rules screen list 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**. Passes the VPN traffic without any filtering, specially used when this firewall is between two VPN tunnel end points.
- **Drop fragmented IP packets**. Drops any fragmented IP packets.
- **UDP Flooding**. Limits the number of UDP sessions created from one LAN machine.
- **TCP Flooding**. Protects the VPN firewall from SYN flood attack.
- **Enable DNS Proxy**. Allows the VPN firewall to handle DNS queries from the LAN.
- **Enable Stealth Mode**. Prevents the VPN firewall from responding to incoming requests for unsupported services.

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 selected WAN interface Selecting ANY enables the rule for any LAN IP destination. WAN1 and WAN2 corresponds to the respective WAN interface governed by this rule.
- **Services**. You can specify the desired services or applications to be covered a rule. If the desired service or application does not appear in the list, you must define it using the Services screen (see "Adding Customized Services" on page 4-24).
- **Schedule**. If you have set firewall rules on one of the the LAN WAN Rules screen and the DMZ WAN Rules screen, you can configure three different schedules (that is, 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 Specific Traffic" on page 4-29 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 VPN firewall. Using this feature requires that you know the port numbers used by the Application.

Once configured, Port Triggering operates as follows:

- A PC makes an outgoing connection using a port number defined in the **Port Triggering** table.
- The VPN firewall 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.
- 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 the firewall cannot be sure when the application has terminated.

See "Configuring Port Triggering" on page 4-37 for the procedure on how to use this feature.

DMZ Port

The DMZ Setup screen allows you to set up the DMZ port. Specifying a Default DMZ server allows you to set up a computer or server that is available to anyone on the Internet for services that you haven't defined.

The default setting of the rules is that the DMZ port and both inbound and outbound traffic is disabled. Enabling the DMZ port increases the traffic through the WAN ports.

The VPN firewall makes LAN port 8 a dedicated hardware DMZ port when DMZ is enabled (see "VPN Firewall Front and Rear Panels" on page 1-6).

See "Configuring and Enabling the DMZ Port" on page 3-11 and "Configuring DMZ WAN Rules" on page 4-12 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 VPN 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 4-26 for the procedure on how to use this feature.

Tools for Traffic Management

The VPN firewall includes several tools that can be used to monitor the traffic conditions and control who has access to the Internet and the types of traffic they are allowed to have. See "Monitoring System Performance" on page 6-23 for a discussion of the tools.

Configuring Users, Administrative Settings, and Remote Management

You can change the administrator and guest passwords and settings, configure authentication for external users, configure an SNMP manager, backup settings and upgrade firmware, and enable remote management. This section includes the following subsections:

- "Changing Passwords and Settings" on page 6-8
- "Adding External Users" on page 6-10
- "Configuring an External Server for Authentication" on page 6-11
- "Enabling Remote Management Access" on page 6-14
- "Using an SNMP Manager" on page 6-16
- "Managing the Configuration File" on page 6-18
- "Configuring Date and Time Service" on page 6-21

Changing Passwords and Settings

The default passwords for the VPN 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. Administrator access is read/write and guest access is read-only.

To modify the local authentication settings:

1. Select **Users** from the main menu and **Local Authentication** from the submenu. The Local Authentication screen will display (see Figure 6-1 on page 6-9).

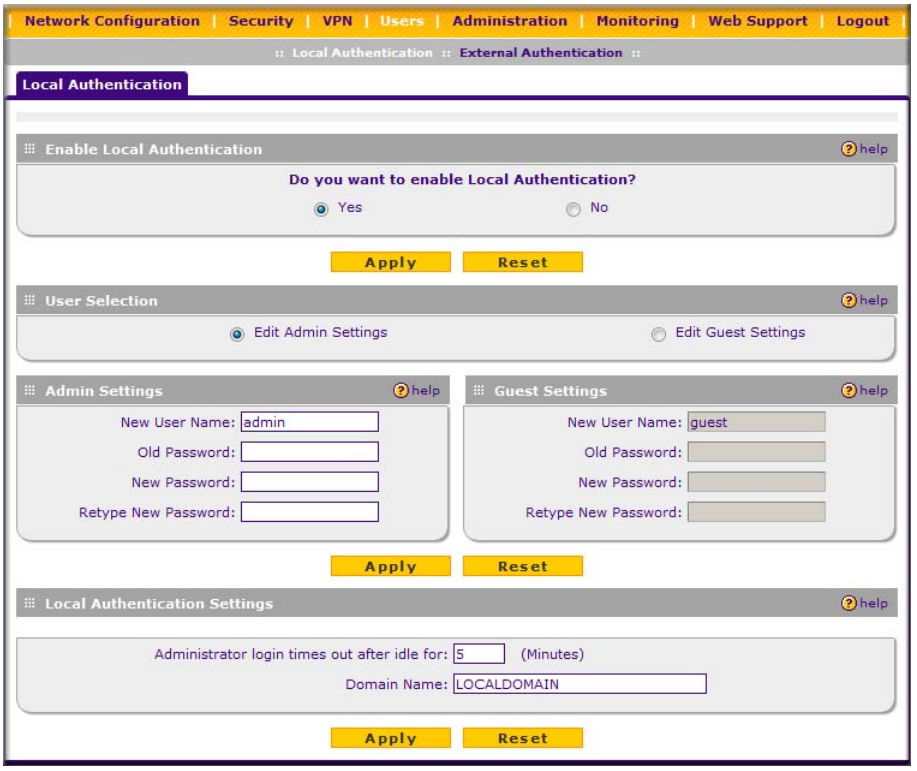


Figure 6-1

2. In the **Enable Local Authentication** section of the screen:
   a. Enable local authentication by selecting the **Yes** radio box.
   b. Click **Apply** to save your settings.
3. In the **User Selection** section of the screen, select either the **Edit Admin Settings** or **Edit Guest Settings** radio box.
4. In either the **Admin Settings** or the **Guest Settings** section of the screen:
   a. change the password by first entering the old password, and then entering the new password twice.
   b. Click **Apply** to save your settings.
5. In the **Local Authentication Settings** section of the screen:
   a. Change the **Idle Logout Time** field to the number of minutes you require. The default is 5 minutes.

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

	Note: The password and time-out value you enter will be changed back to **password** and 5 minutes, respectively, after a factory defaults reset.

Adding External Users

You can add external users for which you then can configure an authentication method (see "Configuring an External Server for Authentication" on page 6-11).

To add an external users:

1. Select **Users** from the main menu and **External Authentication** from the submenu. The External Users screen will display.

Figure 6-2

2. Click **Add**. The Add External User screen will display.

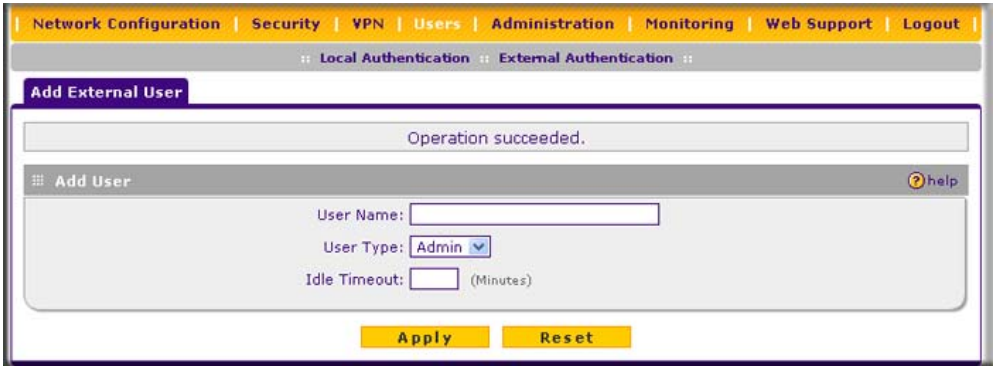


Figure 6-3

3. Configure the following fields:
   a. **User Name**. Enter a unique identifier, using any alphanumeric characters.
   b. **User Type**. Select either **Admin** or **Guest**.
   c. **Idle Timeout**. This is the period after which an idle user will be automatically logged out of the Web Configuration Manager.
4. Click **Apply** to save and apply your entries. The new user appears in the **Users** table on the External Users screen.

Configuring an External Server for Authentication

When an external user logs in, the VPN firewall will validate with the appropriate RADIUS, MIAS, or WIKID server that the external user is authorized to log in.

When specifying external authentication, you are presented with several authentication protocol choices, as summarized in the following table:

Table 6-1.Authentication Protocols

Authentication Protocol	Description
RADIUS	A network-validated PAP or CHAP password-based authentication method that functions with Remote Authentication Dial In User Service (RADIUS).
MIAS	A network-validated PAP or CHAP password-based authentication method that functions with Microsoft Internet Authentication Service (MIAS), which is a component of Microsoft Windows 2003 Server.
WiKID	WiKID Systems is a PAP or CHAP key-based two-factor authentication method that functions with public key cryptography. The client sends an encrypted PIN to the WiKID server and receives a one-time pass code with a short expiration period. The client logs in with the pass code. See Appendix D, “Two Factor Authentication” for more on WiKID authentication.
PAP	Password Authentication Protocol (PAP) is a simple protocol in which the client sends a password in clear text.
CHAP	Challenge Handshake Authentication Protocol (CHAP) executes a three-way handshake in which the client and server trade challenge messages, each responding with a hash of the other’s challenge message that is calculated using a shared secret value.

The chosen authentication protocol must be configured on the external server and on the authenticating client devices.

To configure external authentication:

1. Select **Users** from the main menu and **External Authentication** from the submenu. The External Users screen will display.
2. Select the **External Authentication** tab. The External Authentication screen will display.

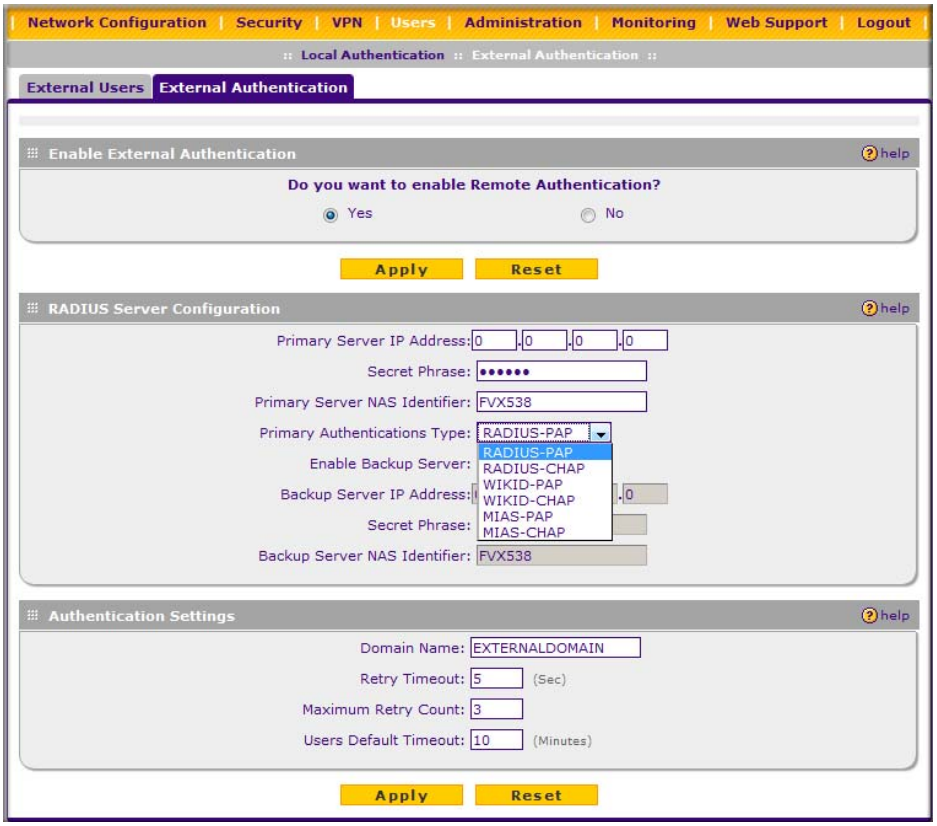


Figure 6-4

3. In the **Enable External Authentication** section of the screen, select the **Yes** radio button.
4. Click **Apply** to save the settings and enable external authentication.
5. In the **RADIUS Server Configuration** section of the screen, configure the following fields:
   - **Primary RADIUS Server IP address**. The IP address of the RADIUS server.
   - **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.

- **Primary Server NAS Identifier**. The identifier for the Network Access Server (NAS) must be present in a RADIUS request. Ensure that NAS identifier is configured identically on both client and server.

  The VPN firewall is acting as a NAS, 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 VPN firewall'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.

- **Primary Authentications Type**. From the pull-down menu, select the authentication type: RADIUS-PAP, RADIUS-CHAP, WIKID-PAP, WIKID-CHAP, MIAS-PAP, or MIAS-PAP. (For more information, see Table 6-1 on page 6-11.)

- As an option, you can enable a backup server by selecting the **Enable Backup Server** checkbox. If enabled, specify the following fields:

  – **Backup Server IP Address**. The IP address of the RADIUS backup server.

  – **Secret Phrase**. Transactions between the client and the RADIUS backup server are authenticated using a shared secret phrase, so the same secret phrase must be configured on both client and backup server.

  – **Backup Server NAS Identifier**. The identifier for the NAS must be present in a RADIUS request. Ensure that NAS identifier is configured identically on both client and backup server.

6. In the **Authentication Settings** section of the screen, configure the following fields:

   - **Domain Name**. The name of the external domain that will be displayed on the login screen.

   - **Retry Timeout**. The period in seconds that the VPN firewall should wait for a response from the RADIUS server.

   - **Maximum Retry Count**. The number of attempts that the VPN firewall will make to contact the RADIUS server. When this number is exceeded, the connection to the RADIUS server cannot be set up.

   - **Users Default Timeout**. The period in minutes that a user is automatically logged out when the connection is idle.

7. Click **Reset** to cancel the changes or click **Apply** to save the settings.

Enabling Remote Management Access

Using the Remote Management screen, 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 into the VPN Firewall" on page 2-2).

Note: Be sure to change the default configuration password of the VPN firewall 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 6-8 for the procedure on how to do this.

To configure the VPN firewall for remote management:

1. Select **Administration** from the main menu and **Remote Management** from the submenu. The Remote Management screen will display.

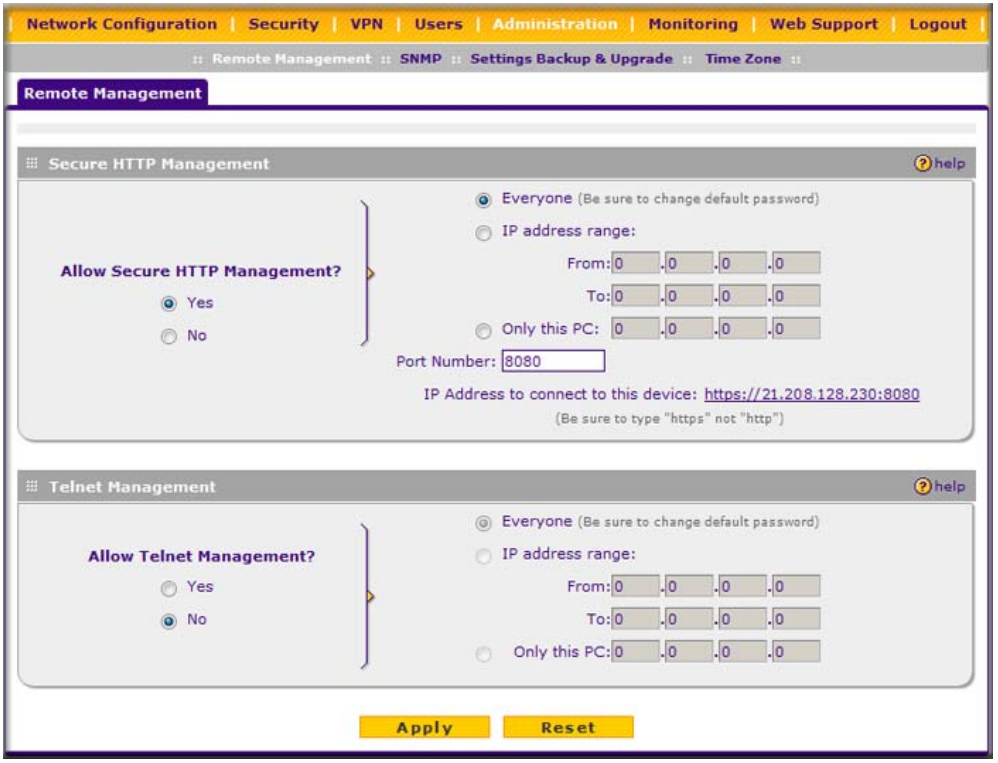


Figure 6-5

2. Check **Allow Remote Management** radio box.
3. Click the **Yes** radio button to enable secure HTTP management (enabled by default), and configure the external IP addresses that will be allowed to connect.
   a. To allow access from any IP address on the Internet, select **Everyone**.
   b. To allow access from a range of IP addresses on the Internet, select **IP address range**. Enter a beginning and ending IP address to define the allowed range.
   c. To allow access from a single IP address on the Internet, select **Only this PC**. Enter the IP address that will be allowed access.
4. Configure the port number that will be used for secure HTTP management. The default port number is 8080.

   Web browser access normally uses the standard HTTP service port 80. For greater security, you can change the remote management Web interface to a custom port by entering that number in the box provided. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.
5. To enable remote management by the command line interface (CLI) over Telnet, click **Yes** to Allow Telnet Management, and configure the external IP addresses that will be allowed to connect.
   a. To allow access from any IP address on the Internet, select **Everyone**.
   b. To allow access from a range of IP addresses on the Internet, select **IP address range**. Enter a beginning and ending IP address to define the allowed range.
   c. To allow access from a single IP address on the Internet, select **Only this P**C. Enter the IP address that will be allowed access.
6. Click **Apply** to have your changes take effect.

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

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

Note: To maintain security, the VPN firewall will reject a login that uses *http://address* rather than the SSL *https://address*.

Note: The first time you remotely connect to the VPN firewall with a browser via SSL, you may get a warning 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 unable to remotely connect to the VPN firewall after enabling HTTPS remote management, check whether other user policies, such as the default user policy, are preventing access.

Note: If you disable HTTPS remote management, all SSL VPN user connections will also be disabled.

Tip: If you are using a dynamic DNS service such as TZO, you can identify the WAN IP address of your VPN firewall by running `tracert` from the Windows Run menu option. Trace the route to your registered FQDN. For example, enter **`tracert FVX538.mynetgear.net`**, and the WAN IP address that your ISP assigned to the VPN firewall is displayed.

Using an SNMP Manager

Simple Network Management Protocol (SNMP) lets you monitor and manage your VPN firewall 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.

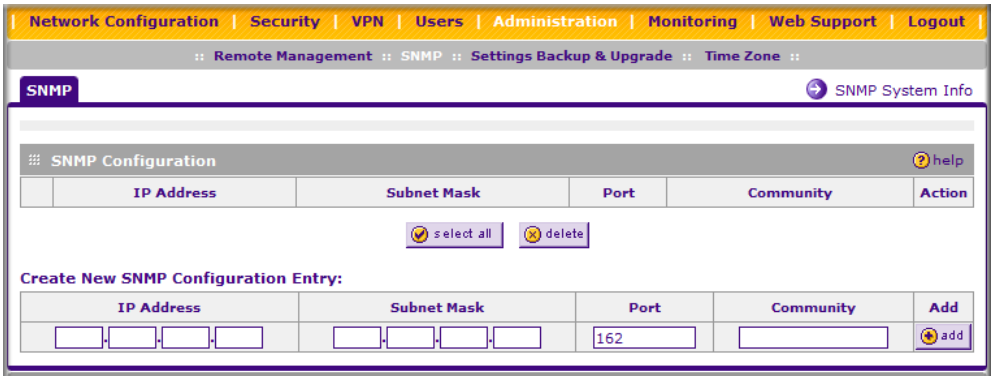


Figure 6-6

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. Note the following:
   - If you want to allow only the host address to access the VPN firewall and receive traps, 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.

To modify an SNMP configuration, click **Edit** in the **Action** column adjacent to the entry that you wish to modify.

When you click on the **SNMP System Info** link on the SNMP screen, the VPN firewall's identification information is displayed. This following identification information is available to the SNMP Manager: system contact, system location, and system name.

To modify the SNMP identification information:

1. Click the **SNMP System Info** link on the SNMP screen. The SNMP SysConfiguration screen will display.

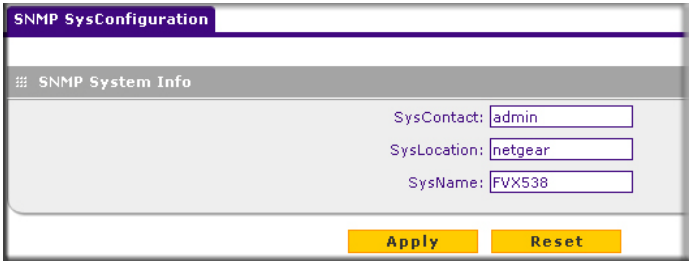


Figure 6-7

2. Modify any of the information that you want the SNMP Manager to use. You can edit the system contact, system location, and system name.
3. Click **Apply** to save your settings.

Managing the Configuration File

The configuration settings of the VPN firewall are stored within the VPN firewall in a configuration file. This file can be saved (backed up) to a user's PC, retrieved (restored) from the user's PC, or cleared to factory default settings.

Once you have installed the VPN firewall and have it working properly, you should back up a copy of your settings to a file on your computer. If necessary, you can later restore the VPN firewall settings from this file. The Settings Backup and Firmware 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.

Backing Up Settings

To back up settings:

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

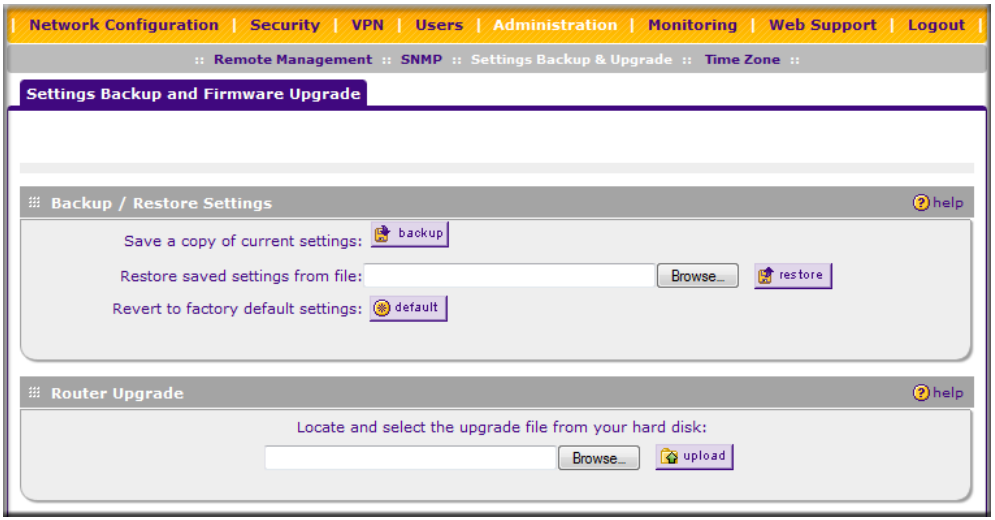


Figure 6-8

2. Click **backup** to save a copy of your current settings.

   If your browser is not 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 VPN firewall, do *not* interrupt the process. Do not try to go online, turn off the VPN firewall, shutdown the computer or do anything else to the VPN firewall until it finishes restarting!

Restoring Settings

To restore settings from a backup file:

1. On the Settings Backup and Firmware Upgrade screen, next to **Restore save settings from file**, click **Browse**.

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

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

Reverting to Factory Default Settings

To reset the VPN firewall to the original factory default settings:

1. On the Settings Backup and Firmware Upgrade screen, click **default**.
2. Manually restart the VPN firewall in order for the default settings to take effect. After rebooting, the VPN firewall'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,** the VPN firewall settings will be erased. All firewall rules, VPN policies, LAN/WAN settings and other settings will be lost. Back up your settings if you intend on using them again!

Upgrading the Firmware

You can install a different version of the VPN firewall firmware from the Settings Backup and Firmware Upgrade screen. To view the current version of the firmware that your VPN firewall is running, select **Monitoring** from the main menu. In the displayed Router Status screen, the System Info section shows the firmware version. When you upgrade your firmware, this section of the screen will change to reflect the new version.

To download a firmware version and upgrade the VPN firewall:

1. Go to the NETGEAR website at *http://www.netgear.com/support* and click **Downloads**.
2. From the **Product Selection** pull-down menu, choose the FVX538.
3. Click on the desired firmware version to reach the download page. Be sure to read the release notes on the download page before upgrading the VPN firewall's software.

   After downloading an upgrade file, you may need to unzip (uncompress) it before upgrading the VPN firewall. If Release Notes are included in the download, read them before continuing.
4. Select **Administration** from the main menu and **Settings Backup & Upgrade** from the submenu. The Settings Backup and Firmware Upgrade screen will display.
5. Click **Browse** in the **Router Upgrade** section.

6. Locate the downloaded file and click **Upload**. This will start the software upgrade to your VPN firewall. The software upgrade process might take some time. At the conclusion of the upgrade, your VPN firewall will reboot.

> **Warning:** After you have clicked **Upload**, do not try to go online, turn off the VPN firewall, shutdown the computer or do anything else to the VPN firewall until the VPN firewall finishes the upgrade! When the Test light turns off, wait a few more seconds before doing anything.

7. After the VPN firewall has rebooted, select **Monitoring** to display the Router Status screen, and confirm the new firmware version to verify that your VPN firewall 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 VPN firewall after upgrading it. Refer to the Release Notes included with the software to find out if this is required.

Configuring Date and Time Service

Date, time and NTP server designations can be configured 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 (see Figure 6-9 on page 6-22).

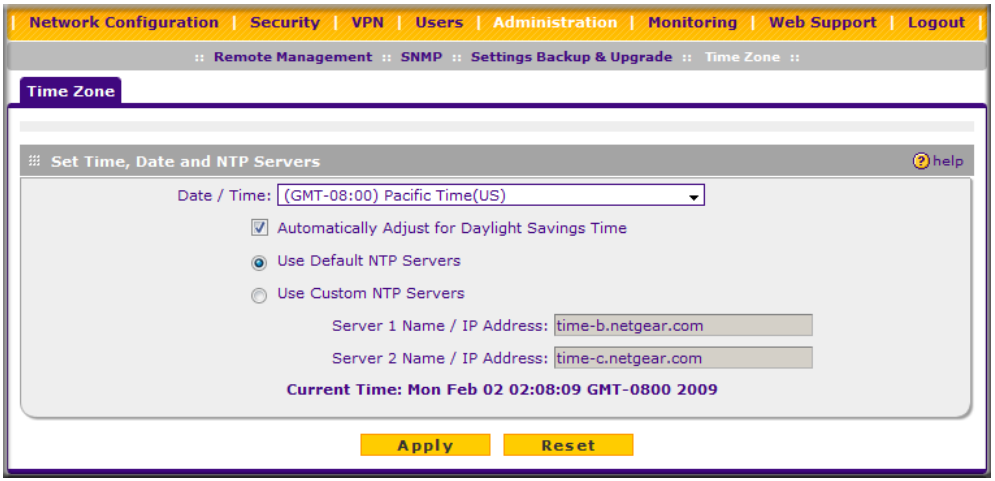


Figure 6-9

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**. The RTC is updated regularly by contacting a NETGEAR NTP server on the Internet. A primary and secondary (backup) server are preloaded.
   - **Use Custom NTP Servers**. To use a particular NTP server, enter the name or IP address of the NTP Server in the **Server 1 Name/IP Address** field. You can enter the address of a backup 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.

	Note: If you select the default NTP servers or if you enter a custom server FQDN, the VPN firewall must determine the IP address of the NTP server by a DNS lookup. You must configure a DNS server address on the WAN ISP Settings screen before the VPN firewall can perform this lookup.

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

Monitoring System Performance

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

- "Activating Notification of Events and Alerts" on page 6-23
- "Viewing the Logs" on page 6-26
- "Enabling the Traffic Meter" on page 6-27
- "Viewing the VPN Firewall Configuration and System Status" on page 6-30
- "Monitoring VPN Firewall Statistics" on page 6-31
- "Monitoring WAN Ports Status" on page 6-32
- "Monitoring Attached Devices" on page 6-33
- "Monitoring VPN Tunnel Connection Status" on page 6-34
- "Viewing the VPN Logs" on page 6-35
- "Viewing the DHCP Log" on page 6-36
- "Viewing Port Triggering Status" on page 6-36

Activating Notification of Events 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 e-mail address. For example, the VPN firewall will log security-related events such as: accepted and dropped packets on different segments of your LAN or DMZ; denied incoming and outgoing service requests; hacker probes and Login attempts; and other general information based on the settings that you enter on the Firewall Logs & E-mail screen. In addition, if you have set up content filtering on the Block Sites screen (see "Blocking Internet Sites (Content Filtering)" on page 4-30), 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 do not have e-mail notification enabled, you can view the logs on the Logs screen (see Figure 6-11 on page 6-26). Selecting all events will increase the size of the log, so it is good practice to select only those events which are required.

To configure logging and notifications:

1. Select **Monitoring** from the main menu and then **Firewall Logs & E-mail** from the submenu. The Firewall Logs & E-mail screen will display (see Figure 6-10 on page 6-24).

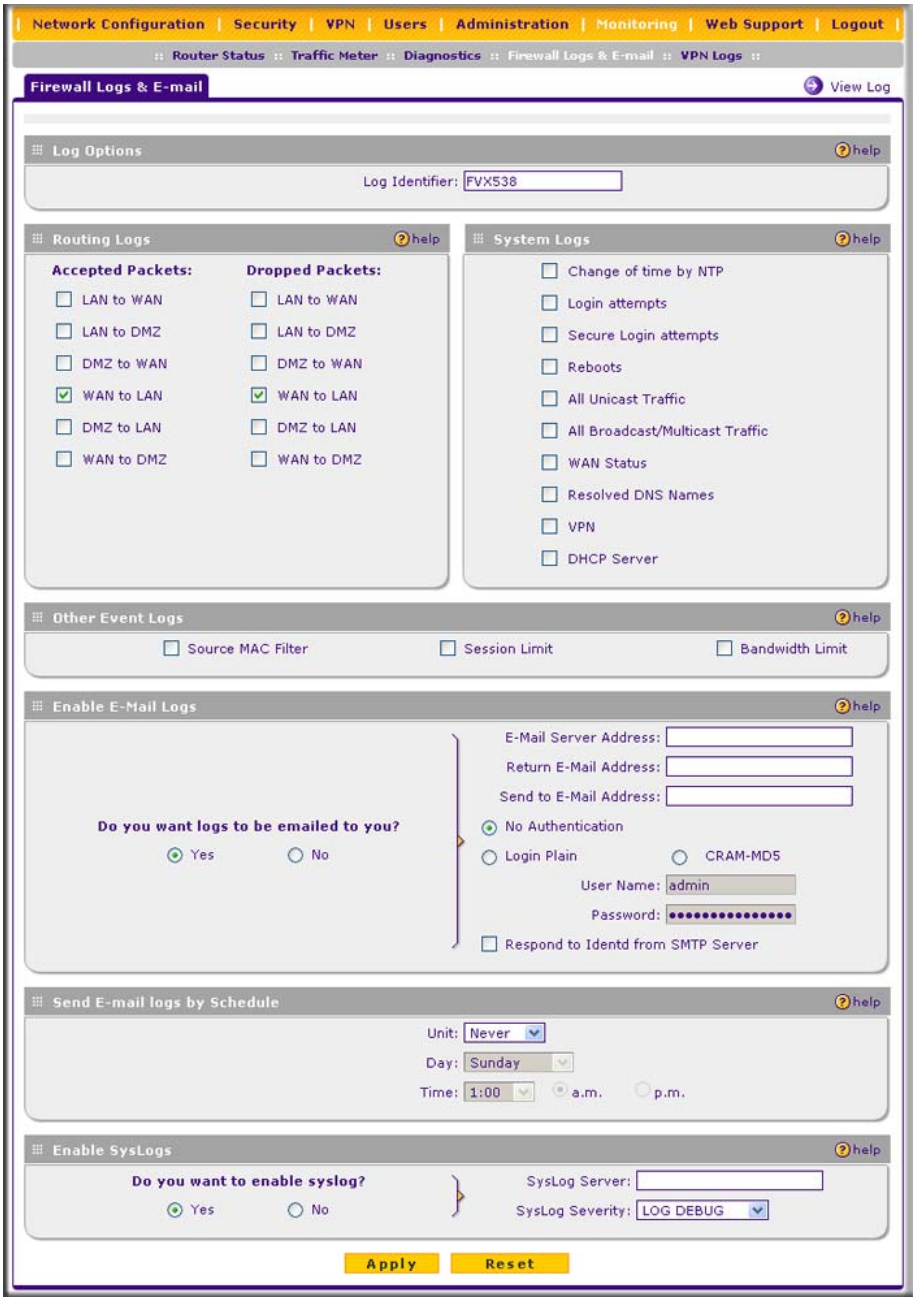

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout
Router Status :: Traffic Meter :: Diagnostics :: Firewall Logs & E-mail :: VPN Logs ::
Firewall Logs & E-mail
View Log
Log Options
help
Log Identifier: FVX538
Routing Logs
help
Accepted Packets:
LAN to WAN
LAN to DMZ
DMZ to WAN
WAN to LAN
DMZ to LAN
WAN to DMZ
Dropped Packets:
LAN to WAN
LAN to DMZ
DMZ to WAN
WAN to LAN
DMZ to LAN
WAN to DMZ
System Logs
help
Change of time by NTP
Login attempts
Secure Login attempts
Reboots
All Unicast Traffic
All Broadcast/Multicast Traffic
WAN Status
Resolved DNS Names
VPN
DHCP Server
Other Event Logs
help
Source MAC Filter
Session Limit
Bandwidth Limit
Enable E-Mail Logs
help
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: admin
Password:
Respond to Identd from SMTP Server
Send E-mail logs by Schedule
help
Unit: Never
Day: Sunday
Time: 1:00
a.m.
p.m.
Enable SysLogs
help
Do you want to enable syslog?
Yes
No
SysLog Server:
SysLog Severity: LOG DEBUG
Apply
Reset

Figure 6-10

2. In the **Log Options** section, enter the name of the log in the **Log Identifier** field. The Log Identifier is a mandatory field used to identify which device sent the log messages. The identifier is appended to log messages.
3. In the **Routing Logs** section, select the network segments for which you would like logs to be sent (for example, LAN to WAN under Dropped Packets).
4. In the **System Logs** section and the **Other Event Logs** section, select the type of events to be logged.
5. In the **Enable E-Mail Logs** section, select the **Yes** radio box to enable e-mail logs. Then enter:
   a. **E-mail Server address**. Enter either the IP address or Internet name of your ISP's outgoing e-mail SMTP server. If you leave this box blank, no logs will be sent to you.
   b. **Return E-mail Address**. Enter an e-mail address to appear as the sender.
   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, jsmith@example.com).
6. The **No Authentication** radio box is checked by default. If your SMTP server requires user authentication, select the required authentication type—either **Login Plain** or **CRAM-MD5**. Then enter the user name and password to be used for authentication.
7. To respond to IDENT protocol messages, check the **Respond to Identd from SMTP Server** box. The Ident Protocol is a weak scheme to verify the sender of e-mail (a common daemon program for providing the ident service is identd).
8. In the **Send E-mail logs by Schedule** section , enter a Schedule for sending the logs. From the **Unit** pull-down menu, choose: **Never**, **Hourly**, **Daily**, or **Weekly**. Then set the Day and Time fields that correspond to your selection.
9. In the **Enable SysLogs** section, you can configure the VPN 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 severity from the **SysLog Severity** pull-down menu. The SysLog levels of severity are as follows:
      - LOG_EMERG (System is unusable)
      - LOG_ALERT (Action must be taken immediately)
      - LOG_CRITICAL (Critical conditions)
      - LOG_ERROR (Error conditions)
      - LOG_WARNING (Warning conditions)

- LOG_NOTICE (Normal but significant conditions)
- LOG_INFO (Informational messages)
- LOG_DEBUG (Debug level messages)

10. Click **Reset** to cancel your changes and return to the previous settings or click **Apply** to save your settings.

Viewing the Logs

To view the logs:

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. Click the **View Log** link in the upper right-hand section of the screen. The Logs screen will display.

If the E-mail Logs option has been enabled on the Firewall Logs & E-mail screen, you can send a copy of the log by clicking **send log**.

Click **refresh log** to retrieve the latest update. Click **clear log** to delete all entries.

Log entries are described in Table 6-2. See Appendix C, “System Logs and Error Messages” for more information about log entry messages.

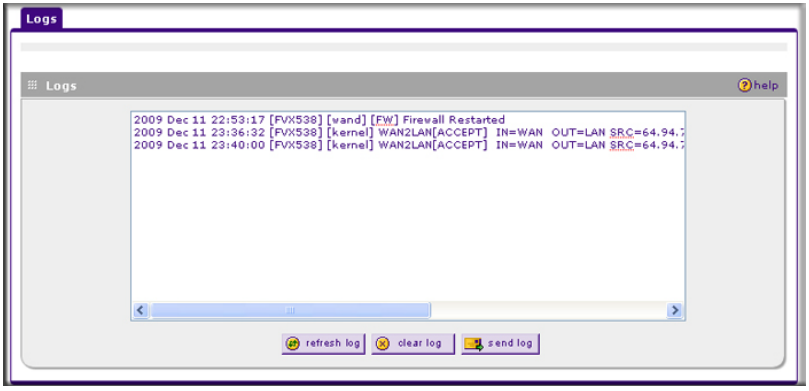


Figure 6-11

Table 6-2. Firewall Log Field 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.

Table 6-2. Firewall Log Field Descriptions (continued)

Field	Description
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 website.
Destination port and interface	The service port number of the destination device, and whether it's on the LAN, WAN or DMZ.

Enabling the Traffic Meter

If your ISP charges by traffic volume over a given period of time, or if you want to study traffic types over a period of time, you can activate the traffic meter for one or both WAN ports.

To monitor traffic limits on each of the WAN ports:

1. Select **Administration** from the main menu and **Traffic Meter** from the submenu. The WAN1 Traffic Meter screen will display. (The WAN1 and WAN2 ports are programmed separately.)

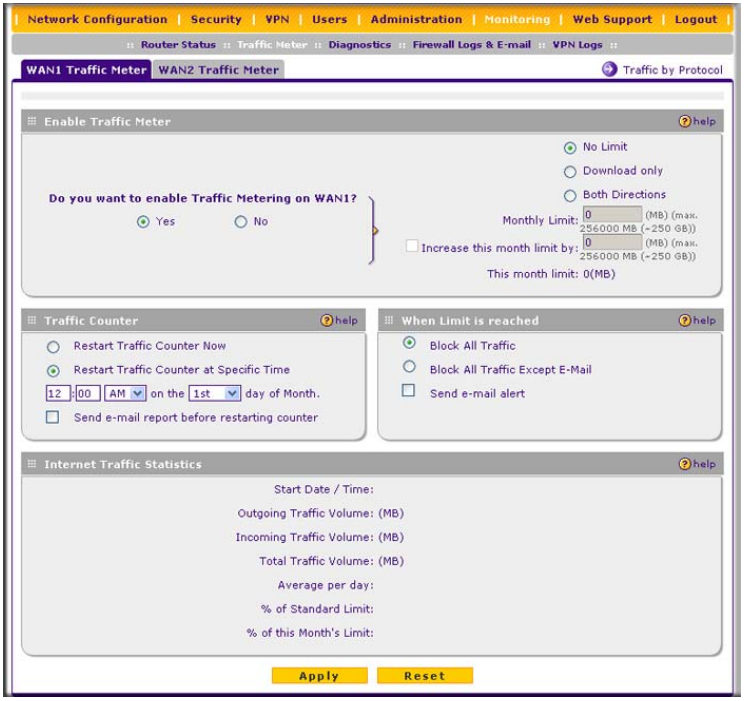


Figure 6-12

2. Enable the traffic meter by clicking the **Yes** radio button under **Do you want to enable Traffic Metering on WAN1?** The traffic meter will record the volume of Internet traffic passing through the WAN1. Select from the following options:

   - **No Limit**. Any specified restrictions will not be applied when traffic limit is reached.
   - **Download only**. The specified restrictions will be applied to the incoming traffic only
   - **Both Directions**. The specified restrictions will be applied to both incoming and outgoing traffic only
   - **Monthly Limit**. Use this option if your ISP charges for additional traffic. Enter the monthly volume limit and select the desired behavior when the limit is reached. 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 limit by**. Temporarily increase the traffic limit if you have reached the monthly limit, but need to continue accessing the Internet. Select the checkbox and enter the desired increase. (The checkbox will automatically be cleared when saved so that the increase is only applied once.)
   - **This month limit**. Displays the limit for the current month.

3. In the **Traffic Counter** section, make your traffic counter selections:

   - **Restart Traffic Counter Now**. Select this option and click **Apply** to restart the traffic counter immediately.
   - **Restart Traffic Counter at a Specific Time**. Restart the traffic counter at a specific time and day of the month. Fill in the time fields and choose **AM** or **PM** and the day of the month from the pull-down menus.
   - **Send e-mail report before restarting counter**. An e-mail report will be sent just before restarting the counter. You must configure the e-mail capability in order for this function to work (see “Activating Notification of Events and Alerts” on page 6-23).

4. In the **When limit is reached** section, make the following choice:

   - **Block All Traffic**. All access to and from the Internet will be blocked.

   > **Warning:** If the **Block All Traffic** radio button is selected, the WAN port shuts down once its traffic limit is reached

   - **Block all traffic except E-mail**. Only e-mail traffic will be allowed. All other traffic will be blocked.
   - **Send E-mail alert.** You must configure the e-mail capability in order for this function to work (see "Activating Notification of Events and Alerts" on page 6-23).

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

To configure the traffic meter for the WAN2 port, select the **WAN2 Traffic Meter** tab and repeat this process

The **Internet Traffic Statistics** section of the screen displays statistics on Internet traffic through the WAN port. If you have not enabled the traffic meter, these statistics are not available.

To display a report of Internet traffic by type, click the **Traffic by Protocol** link in the upper right-hand section of the Traffic Meter screen . The volume of traffic for each protocol will be displayed in a popup window. Traffic counters are updated in MBytes scale; the counter starts only when traffic passed is at least 1MB.

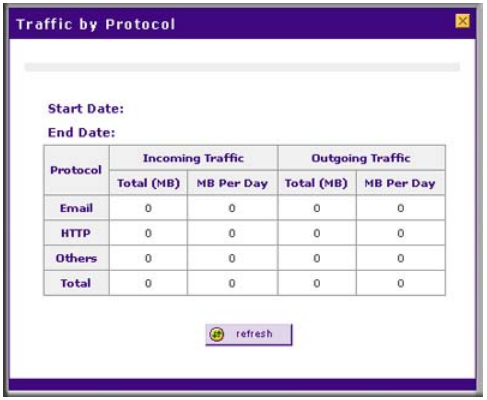


Figure 6-13

Viewing the VPN Firewall Configuration and System Status

The Router Status screen provides status and usage information. Select **Monitoring** from the main menu and **Router Status** from the submenu. The Router Status screen will display (see Figure 6-13 on page 6-29). The Router Status screen displays current settings and statistics for your VPN firewall. Because this information is read-only, any changes must be made on other screens.

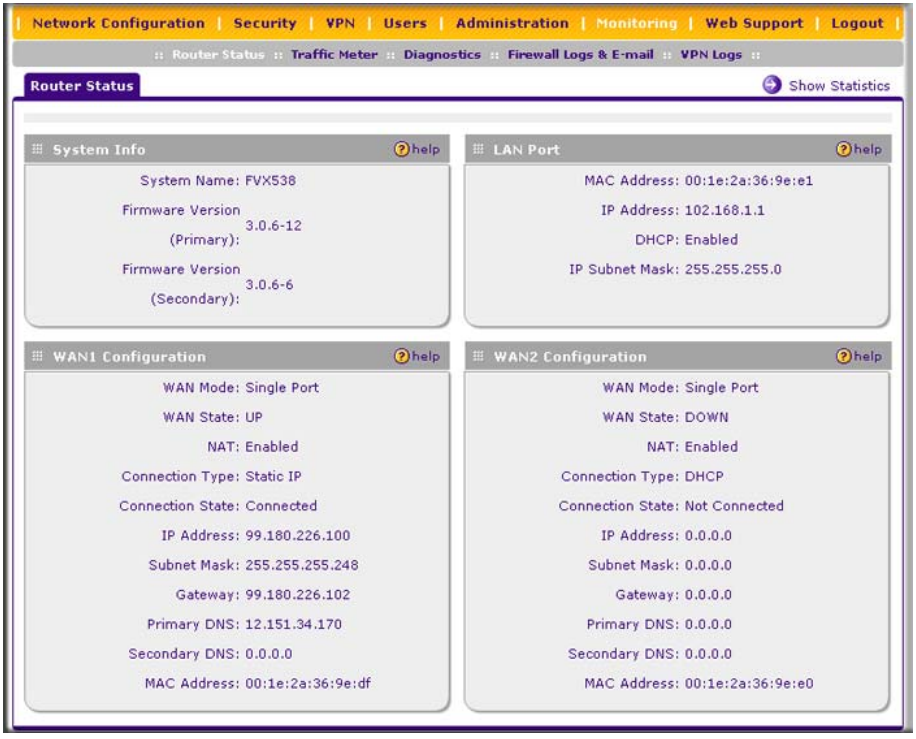


Figure 6-14

Table 6-3. Router Status Fields

Item	Description
System Name	This is the Account Name that you entered on the WAN ISP Settings screen.
Firmware Version	This is the current software the VPN firewall is using. This will change if you upgrade your VPN firewall.
LAN Port	Displays the current settings for MAC address, IP address, DHCP status and IP subnet mask that you set in the LAN IP Setup screen. DHCP can be either Enabled or Disabled.

Table 6-3. Router Status Fields (continued)

Item	Description
WAN1 Configuration	• WAN Mode: Single, Dual, or Rollover. • WAN State: UP or DOWN. • NAT: Enabled or Disabled. • Connection Type: Static IP, DHCP, PPPoE, or PPTP. • Connection State: Connected or Disconnected. • WAN IP Address.: The IP address of the WAN interface. • Subnet Mask: The IP subnet mask of the WAN interface. • Gateway: The gateway IP address for the WAN interface. • Primary DNS: The IP address of the primary DNS server for the WAN interface. • Secondary DNS: The IP address of the secondary DNS server for the WAN interface. • MAC Address: The MAC address of the WAN interface.
WAN2 Configuration	Displays the same details as for the WAN1 Configuration.

Monitoring VPN Firewall Statistics

To display the VPN firewall statistics:

1. Select **Monitoring** from the main menu and **Router Status** from the submenu. The Router Status screen will display (see Figure 6-14 on page 6-30).
2. Click the **Show Statistics** link in the upper right-hand section of the screen. The Router Statistics screen will display.

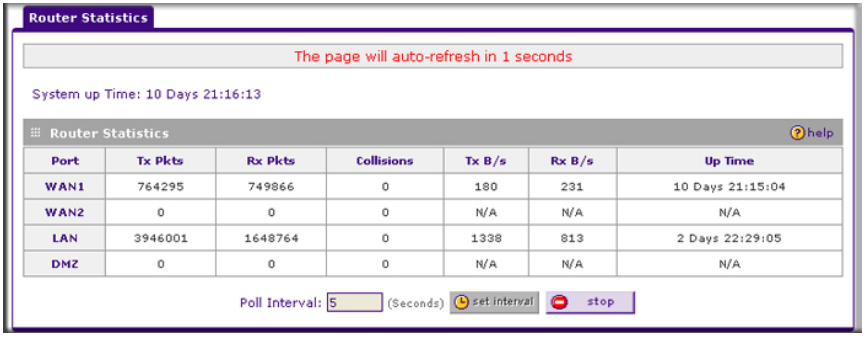


Figure 6-15

For each interface, the number of transmitted and received packets, the number of collided packets, the transmitted and received Bytes per second, and the interface up-time are shown.

To set the poll interval:

1. Click the **Stop** button.
2. From the Poll Interval pull-down menu, select a new interval (the minimum is 5 seconds, the maximum is 5 minutes).
3. Click the **Set Interval** button.

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. To monitor the status of the WAN ports:

1. Select **Network Configuration** from the main menu and **WAN Settings** from the submenu. The WAN1 ISP Settings screen will display.
2. Click the **WAN Status** link in the upper right-hand section of the screen. The Connection Status popup window displays a status report on the WAN1 port.

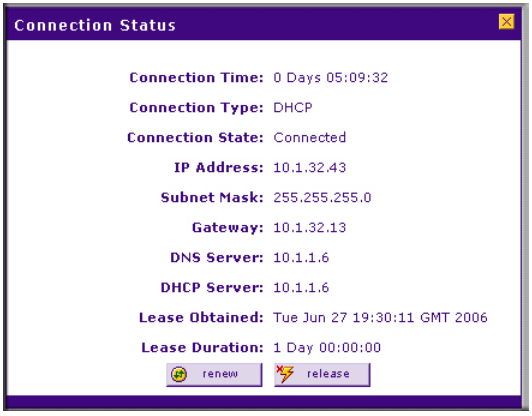


Figure 6-16

To get a status report on the WAN2 port, click the **WAN2 ISP Settings** tab, and then click the **WAN Status** link.

Monitoring Attached Devices

The LAN Groups screen contains a table of all IP devices that the VPN firewall has discovered on the local network.

To view the LAN Groups screen:

1. Select **Network Configuration** from the main menu and **LAN Settings** from the submenu.
2. Select the **LAN Groups** tab. The LAN Groups screen will display.

Figure 6-17

The **Known PCs and Devices** table lists the entries in the Network Database., which is an automatically-maintained list of LAN-attached devices. PCs and other LAN devices become known by the following methods:

- **DHCP Client Requests**. By default, the DHCP server in the VPN firewall 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 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. The scan will detect active devices that are not DHCP clients. However, sometimes the name of the PC or device cannot be accurately determined and will be shown as unknown.
- **Manually Adding Devices**. You can enter information in the **Add Known PCs and Devices** section and click **Add** to manually add a device to the database.

The **Known PCs and Devices** table lists all current entries in the LAN Groups database. For each PC or device, the following data is displayed

Table 6-4. Known PCs and Devices options

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.

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.

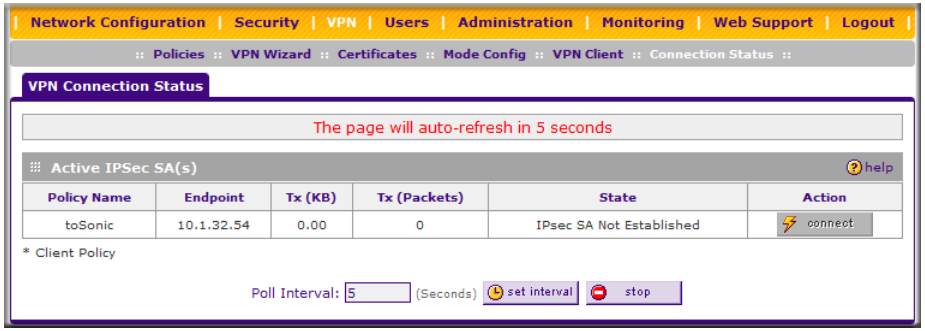


Figure 6-18

The Active IPsec (SA)s table lists each active connection with the following information

Table 6-5. 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.
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.

Viewing the 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..

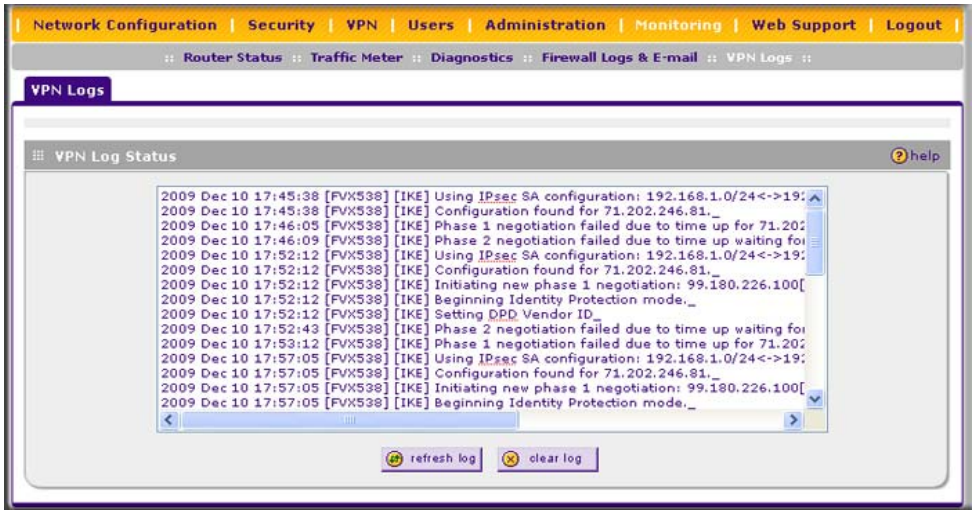


Figure 6-19

To view the most recent entries, click **refresh log**. To delete all the existing log entries, click **clear log**.

Viewing the DHCP Log

To display the DHCP log:

1. Select **Network Configuration** from the main menu and **LAN Settings** from the submenu. The LAN Setup screen will displays.
2. Click the **DHCP Log** link in the upper right-hand section of the screen. The DHCP Log popup screen will display.

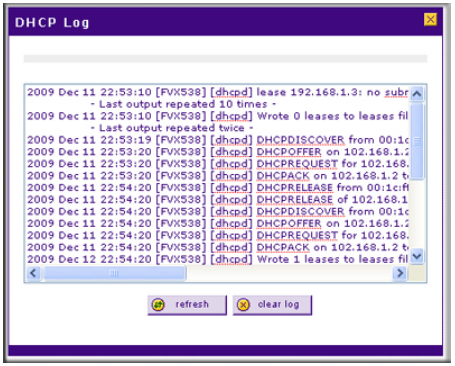


Figure 6-20

To view the most recent entries, click **refresh**. To delete all the existing log entries, click **clear log**.

Viewing Port Triggering Status

To display the port triggering status:

1. Select **Security** from the main menu and **Port Triggering** from the submenu. The Port Triggering screen will displays.
2. Click the **Status** link in the upper right-hand section of the screen. The Port Triggering Status popup screen will display.

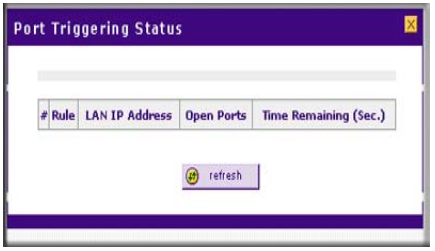


Figure 6-21

To view the most recent entries, click **refresh**.

Table 6-6. 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.

Chapter 7
Troubleshooting

This chapter provides troubleshooting tips and information for your ProSafe VPN Firewall 200 FVX538.

This chapter includes the following sections:

- "Basic Functions" on this page
- "Troubleshooting the Web Configuration Interface" on page 7-3
- "Troubleshooting the ISP Connection" on page 7-4
- "Troubleshooting a TCP/IP Network Using a Ping Utility" on page 7-5
- "Restoring the Default Configuration and Password" on page 7-7
- "Problems with Date and Time" on page 7-7
- "Using the Diagnostics Utilities" on page 7-8

Basic Functions

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

1. When power is first applied, verify that the PWR LED is on.
2. After approximately 2 minutes, 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 VPN firewall is turned on:

- Make sure that the power cord is properly connected to your VPN 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 VPN 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 VPN firewall.

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

- Cycle the power to see if the VPN firewall recovers.
- Clear the VPN firewall's configuration to factory defaults. This will set the VPN 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 VPN 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 VPN 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 VPN firewall's Web Configuration interface from a PC on your local network, check the following:

- Check the Ethernet connection between the PC and the VPN firewall as described in the previous section.
- Make sure your PC's IP address is on the same subnet as the VPN 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 VPN firewall and reboot your PC.

- If your VPN firewall's IP address has been changed and you do not know the current IP address, clear the VPN firewall's configuration to factory defaults. This will set the VPN 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 do not want to revert to the factory default settings and lose your configuration settings, you can reboot the VPN firewall and use sniffer to capture packets sent during the reboot. Look at the ARP packets to locate the VPN firewall'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 VPN 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 VPN firewall is unable to access the Internet, you should first determine whether the VPN firewall is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your VPN 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 VPN firewall's configuration at **http://192.168.1.1**.
3. Select **Monitoring** from the main menu and **Router Status** from the submenu.
4. Check that an IP address is shown for the WAN Port
   If 0.0.0.0 is shown, your VPN firewall has not obtained an IP address from your ISP.

If your VPN 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 VPN firewall by performing the following procedure:

1. Turn off power to the cable or DSL modem.
2. Turn off power to your VPN 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 VPN firewall.

If your VPN 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 on the WAN1 ISP Settings or WAN2 ISP Settings screen (see Figure 2-1 on page 2-3).
- 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 VPN firewall's MAC address; or
  - Configure your VPN firewall to spoof your PC's MAC address. You can do this on the WAN1 Advanced Options or WAN2 Advanced Options screen (see Figure 2-7 on page 2-16).

If your VPN 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 VPN firewall configured as its TCP/IP gateway.

Troubleshooting a TCP/IP Network Using a Ping Utility

Most TCP/IP terminal devices and VPN 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 VPN Firewall

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

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

1. From the Windows toolbar, click **Start** and select **Run**.
2. In the field provided, type "ping" followed by the IP address of the VPN firewall; for example:

   ```
   ping 192.168.1.1
   ```

3. Click **OK.** A message, similar to the following, should display:

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

   If the path is working, you will see this message:

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

   If the path is not working, you will 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 VPN 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 VPN 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 VPN 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 on the WAN1 ISP Settings or WAN2 ISP Settings screen (see Figure 2-1 on page 2-3).

– 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 VPN firewall to "clone" or "spoof" the MAC address from the authorized PC. You can do this on the WAN1 Advanced Options or WAN2 Advanced Options screen (see Figure 2-7 on page 2-16).

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the VPN 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:

- Restore the VPN firewall to factory default settings from the Settings Backup and Firmware Upgrade screen (see "Reverting to Factory Default Settings" on page 6-20).
- Use the reset button on the rear panel of the VPN 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 VPN firewall.

To restore the factory defaults:

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 VPN firewall to reboot.

Problems with Date and Time

The Time Zone screen (select **Administration** from the main and **Time Zone** from the submenu) 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 and time shown is Thu Jan 01 00:01:52 GMT 1970. Cause: The VPN 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 VPN firewall, wait at least five minutes and check the date and time again.
- Time is off by one hour. Cause: The VPN firewall does not automatically sense Daylight Savings Time. Go to the Time Zone screen (see "Configuring Date and Time Service" on page 6-21), and select or deselect the check box marked "Automatically Adjust for Daylight Savings Time".

Using the Diagnostics Utilities

You can perform diagnostics such as pinging an IP address, performing a DNS lookup, displaying the routing table, rebooting the VPN firewall, and capturing packets.

Note: For normal operation, diagnostics are not required.

Select **Monitoring** from the main menu and **Diagnostics** from the submenu. The Diagnostics screen will display.

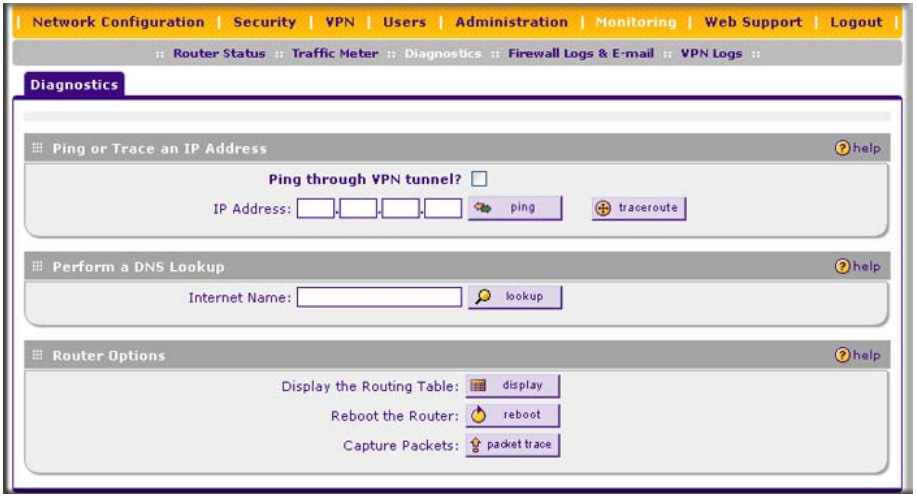
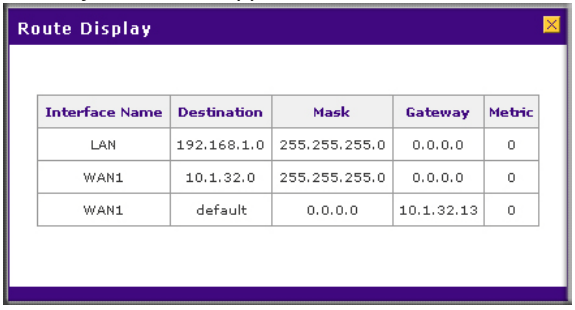


Figure 7-1

Table 7-1. Diagnostics

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. If the specified address is intended to be reached through a VPN tunnel, select **Ping through VPN tunnel**.
	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 such as 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. 
Reboot the Router	Used to perform a remote reboot (restart). You can use this if the VPN firewall seems to have become unstable or is not operating normally. **Note**: Rebooting will break any existing connections either to the VPN firewall (such as a management session) or through the VPN firewall (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.

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. VPN firewall Default Configuration 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. VPN firewall Default Configuration Settings (continued)

Feature		Default Behavior
Management		
	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 200 are listed in the following table.

Table A-2. VPN firewall Technical Specifications

Feature		Specifications
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:	1.7 x 13 x 8.2 in.
	Weight:	2 kg (4.5 lb)

Table A-2. VPN firewall Technical Specifications (continued)

Feature		Specifications
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; 1000BASE-T

Appendix B
Network Planning for Dual WAN Ports

This appendix describes the factors to consider when planning a network using a VPN firewall that has dual WAN ports.

This appendix contains the following sections:

- "What You Will Need to Do Before You Begin" on page B-1
- "Overview of the Planning Process" on page B-5
- "Inbound Traffic" on page B-7
- "Virtual Private Networks (VPNs)" on page B-9

What You Will Need to Do Before You Begin

The ProSafe VPN Firewall 200 is a powerful and versatile solution for your networking needs. But to make the configuration process easier and to understand all of the choices available to you, you need to think through the following items before you begin:

1. Plan your network

    a. Determine whether you are going to use one or both WAN ports. For one WAN port, you may need a fully qualified domain name either for convenience or if you have a dynamic IP address.

    b. If you are going to use both WAN ports, determine whether you are going to use them in rollover mode for increased system reliability or load balancing mode for maximum bandwidth efficiency. See the topics in this appendix for more information. Your decision has the following implications:

    Fully qualified domain name

    – For rollover mode, you are going to need a fully qualified domain name to implement features such as exposed hosts and virtual private networks.

    – For load balancing mode, you may still need a fully qualified domain name either for convenience or if you have a dynamic IP address.

    Protocol binding

– For rollover mode, protocol binding does not apply.

– For load balancing mode, you need to decide which protocols you want to bind to a specific WAN port if you are going to take advantage of this option.

– You can also add your own service protocols to the list.

3. Set up your accounts

a. Have active Internet services such as that provided by cable or DSL broadband accounts and locate the Internet Service Provider (ISP) configuration information.

- In this document, the WAN side of the network is presumed to be provisioned as shown in Figure B-1with two ISPs connected to the VPN firewall through separate physical facilities.
- Each VPN firewall WAN port must be configured separately, however, whether you are using a separate ISP for each WAN port or are having the traffic of both WAN ports routed through the same ISP.

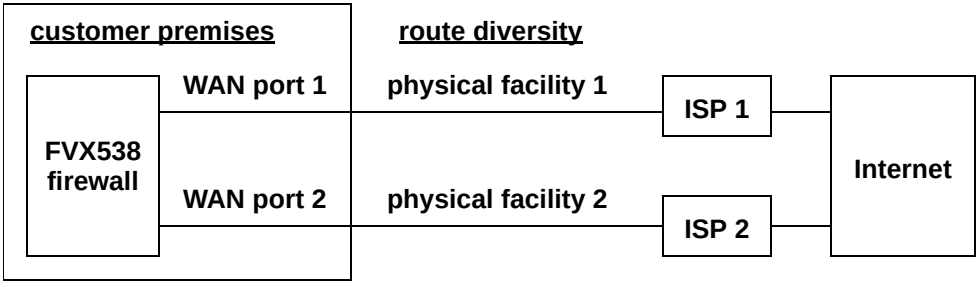


Figure B-1

- If your ISPs charge by the amount of bandwidth you use each month, you may want to consider setting up a traffic meter to keep track of your traffic.

b. Contact a Dynamic DNS Service and set up your fully qualified domain names if you need or want them.

3. Plan your network management approach

- The VPN firewall is capable of being managed remotely, but this feature must be enabled locally after each factory default reset.

  You are strongly advised to change the default **password** password to something that is more secure at the time you enable remote management.

- There are a variety of WAN options you can choose when the factory default settings are not applicable to your installation. These include enabling a WAN port to respond to a ping and setting MTU size, port speed, and upload bandwidth.

4. Prepare to physically connect the VPN firewall to cable or DSL modems and a computer. Instruction for connecting your VPN firewall are in *Installation Guide, FVX538 ProSafe VPN Firewall 200*.

Cabling and Computer Hardware Requirements

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

Computer Network Configuration Requirements

The VPN firewall includes a built-in Web Configuration Manager. To access the configuration menus on the VPN firewall, your must use a Java-enabled Web browser program that supports HTTP uploads such as Microsoft Internet Explorer 6 or higher, Mozilla Firefox 3 or higher, or Apple Safari 3 or higher with JavaScript, cookies, and you must have SSL enabled.

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

Note: For help with DHCP configuration, please refer to the link in Appendix E, "Related Documents."

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

Internet Configuration Requirements

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

- Host and Domain Names
- ISP Login Name and Password
- ISP Domain Name Server (DNS) Addresses

- Fixed IP Address which is also known as Static IP Address

Where Do I Get the Internet Configuration Parameters?

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

- Your ISPs provide all the information needed to connect to the Internet. If you cannot locate this information, you can ask your ISPs to provide it or you can try one of the options below.
- If you have a computer already connected using the active Internet access account, you can gather the configuration information from that computer.
  - For Windows 95/98/ME, open the Network control panel, select the TCP/IP entry for the Ethernet adapter, and click Properties. Record all the settings for each screen.
  - For Windows 2000/XP, open the Local Area Network Connection, select the TCP/IP entry for the Ethernet adapter, and click Properties. Record all the settings for each screen.
  - For Macintosh computers, open the TCP/IP or Network control panel. Record all the settings for each section.

Once you locate your Internet configuration parameters, you may want to record them on the pages below.

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

==========

Internet Connection Information Form

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

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

Login Name: _____ Password: _____

Service Name: _____

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

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

Gateway IP Address: _____._____._____._____

Subnet Mask: _____._____._____._____

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

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

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

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

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

ISP Host Name: _____ ISP Domain Name: _____

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

Dynamic DSN Service Provider: _____ FQDN: _____

==========

Overview of the Planning Process

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

- Inbound traffic (for example, port forwarding, port triggering, DMZ port)
- Virtual private networks (VPNs)

The two WAN ports can be configured on a mutually-exclusive basis to either:

- Rollover for increased reliability, or
- Balance the load for outgoing traffic.

These two categories of considerations interact to make the planning process more challenging.

Inbound Traffic

Unrequested incoming traffic can be directed to a PC on your LAN rather than being discarded. The mechanism for making the IP address public depends on whether the dual WAN ports are configured to either roll over or balance the loads.

Virtual Private Networks (VPNs)

A virtual private network (VPN) tunnel provides a secure communication channel between either two gateway VPN firewalls or between a remote PC client and gateway VPN firewall. As a result, the IP address of at least one of the tunnel end points must be known in advance in order for the other tunnel end point to establish (or re-establish) the VPN tunnel.

Note: Once the gateway firewall WAN port rolls over, the VPN tunnel collapses and must be re-established using the new WAN IP address.

The Roll-over Case for Firewalls With Dual WAN Ports

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

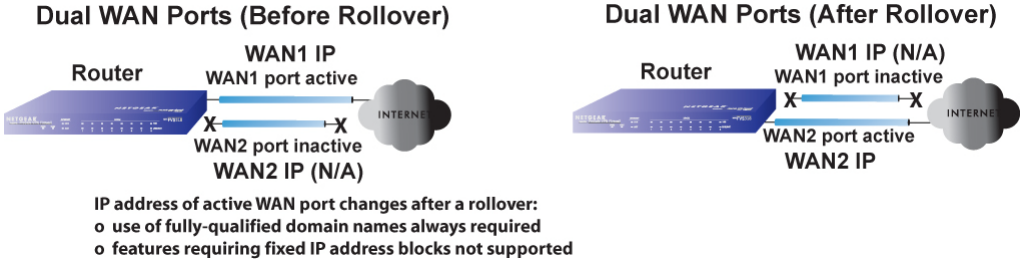


Figure B-2

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

The Load Balancing Case for Firewalls With Dual WAN Ports

Load balancing for the dual WAN port case is similar to the single WAN port case when specifying the IP address. Each IP address is either fixed or dynamic based on the ISP: fully-qualified domain names must be used when the IP address is dynamic and are optional when the IP address is static.

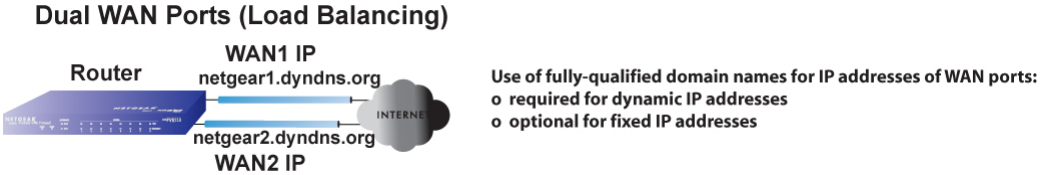


Figure B-3

Inbound Traffic

Incoming traffic from the Internet is normally discarded by the firewall unless the traffic is a response to one of your local computers or a service that you have configured in the Inbound Rules menu. Instead of discarding this traffic, you can have it forwarded to one or more LAN hosts on your network.

The addressing of the VPN firewall's dual WAN port depends on the configuration being implemented:

Table B-1. IP Addressing Requirements for Exposed Hosts in dual WAN Port Systems

Configuration and WAN IP address		Single WAN Port (reference case)	Dual WAN Port Cases	
			Rollover	Load Balancing
Inbound traffic • Port forwarding • Port triggering • DMZ port	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required

Inbound Traffic to Single WAN Port (Reference Case)

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

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

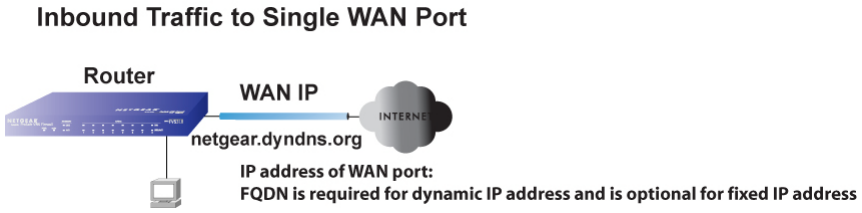


Figure B-4

Inbound Traffic to Dual WAN Port Systems

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

Inbound Traffic: Dual WAN Ports for Improved Reliability

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

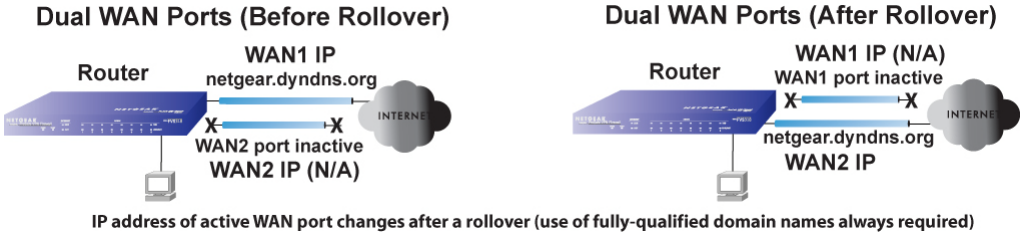


Figure B-5

Inbound Traffic: Dual WAN Ports for Load Balancing

In the dual WAN port case for load balancing, the Internet address of each WAN port is either fixed if the IP address is fixed or a fully-qualified domain name if the IP address is dynamic.

Note: Load balancing is implemented for outgoing traffic and not for incoming traffic. Consider making one of the WAN port Internet addresses public and keeping the other one private in order to maintain better control of WAN port traffic.

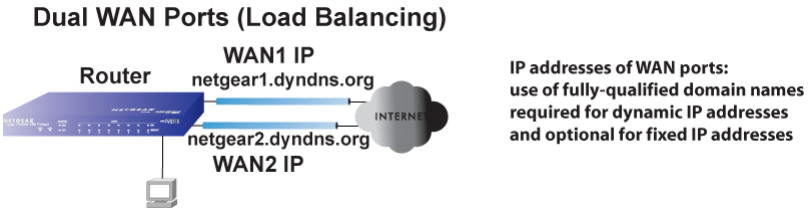


Figure B-6

Virtual Private Networks (VPNs)

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

Table B-2. IP Addressing Requirements for VPNs in Dual WAN Port Systems

Configuration and WAN IP address		Single WAN Port (reference case)	Dual WAN Port Cases	
			Rollover[a]	Load Balancing
VPN Road Warrior (client-to-gateway)	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required
VPN Gateway-to-Gateway	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required

Table B-2. IP Addressing Requirements for VPNs in Dual WAN Port Systems

Configuration and WAN IP address		Single WAN Port (reference case)	Dual WAN Port Cases	
			Rollover[a]	Load Balancing
VPN Telecommuter (client-to-gateway through a NAT router)	Fixed	Allowed (FQDN optional)	FQDN required	Allowed (FQDN optional)
	Dynamic	FQDN required	FQDN required	FQDN required

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

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

- Rollover Case for Dual Gateway WAN Ports

  Rollover for the dual gateway WAN port case is different from the single gateway WAN port case when specifying the IP address of the VPN tunnel end point. Only one WAN port is active at a time and when it rolls over, the IP address of the active WAN port always changes. Hence, the use of a fully-qualified domain name is always required, even when the IP address of each WAN port is fixed.

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

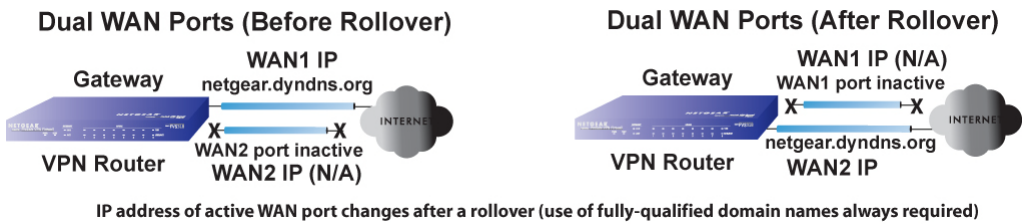


Figure B-7

- Load Balancing Case for Dual Gateway WAN Ports

Load balancing for the dual gateway WAN port case is the same as the single gateway WAN port case when specifying the IP address of the VPN tunnel end point. Each IP address is either fixed or dynamic based on the ISP: fully-qualified domain names must be used when the IP address is dynamic and are optional when the IP address is static.

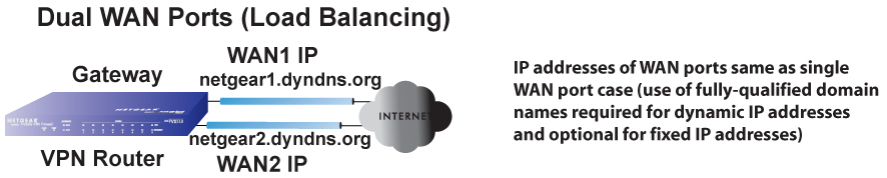


Figure B-8

VPN Road Warrior (Client-to-Gateway)

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

- Single gateway WAN port
- Redundant dual gateway WAN ports for increased reliability (before and after rollover)
- Dual gateway WAN ports used for load balancing

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

In the case of the single WAN port on the gateway VPN firewall, the remote PC client initiates the VPN tunnel because the IP address of the remote PC client is not known in advance. The gateway WAN port must act as the responder.

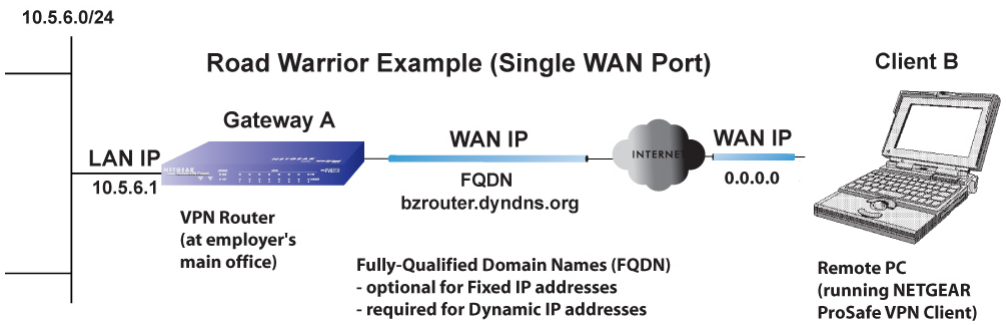


Figure B-9

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

VPN Road Warrior: Dual Gateway WAN Ports for Improved Reliability

In the case of the dual WAN ports on the gateway VPN firewall, the remote PC client initiates the VPN tunnel with the active gateway WAN port (port WAN1 in this example) because the IP address of the remote PC client is not known in advance. The gateway WAN port must act as a responder.

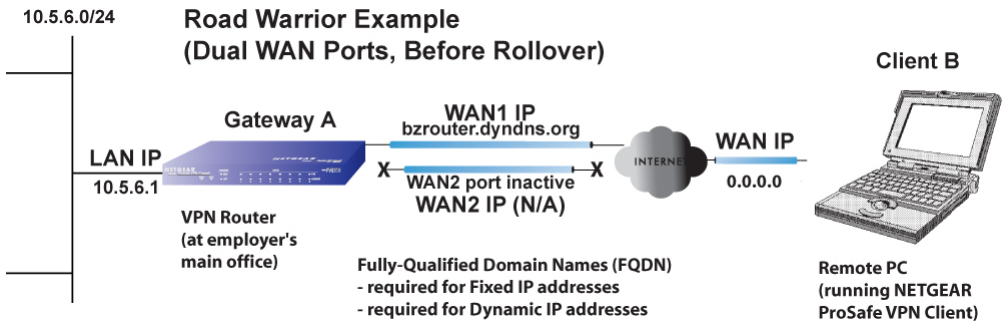


Figure B-10

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

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

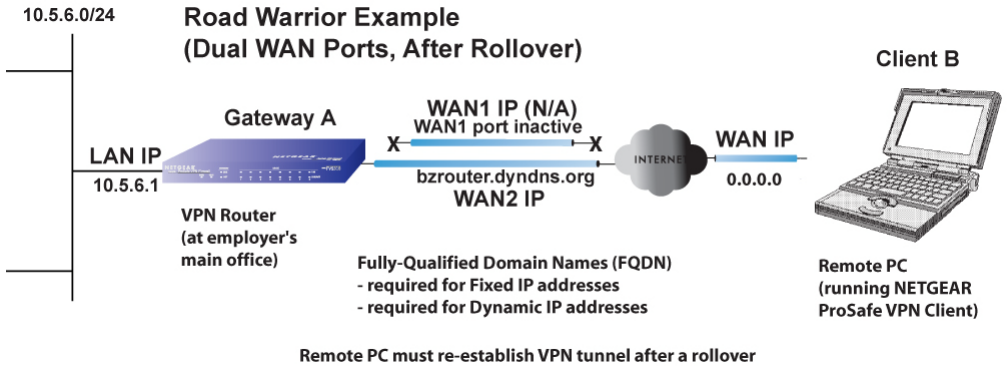


Figure B-11

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

VPN Road Warrior: Dual Gateway WAN Ports for Load Balancing

In the case of the dual WAN ports on the gateway VPN firewall, the remote PC initiates the VPN tunnel with the appropriate gateway WAN port (that is, port WAN1 or WAN2 as necessary to balance the loads of the two gateway WAN ports) because the IP address of the remote PC is not known in advance. The chosen gateway WAN port must act as the responder.

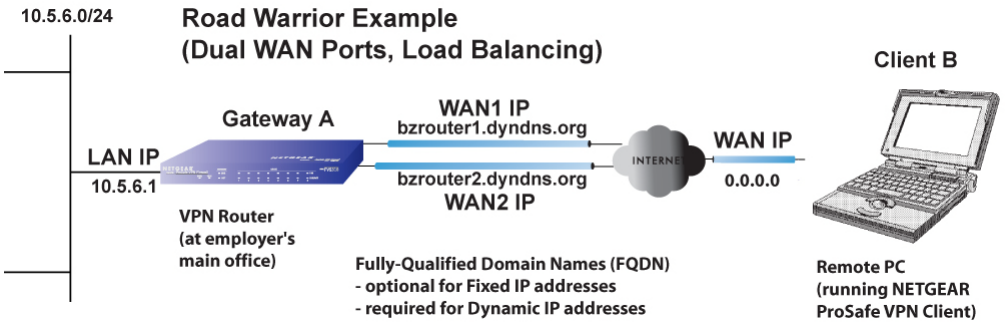


Figure B-12

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

VPN Gateway-to-Gateway

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

- Single gateway WAN ports
- Redundant dual gateway WAN ports for increased reliability (before and after rollover)
- Dual gateway WAN ports used for load balancing

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

In the case of single WAN ports on the gateway VPN firewalls, either gateway WAN port can initiate the VPN tunnel with the other gateway WAN port because the IP addresses are known in advance.

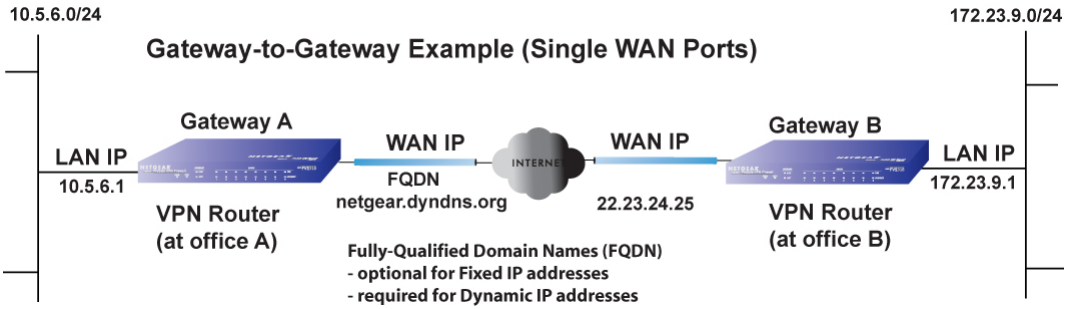


Figure B-13

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

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

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

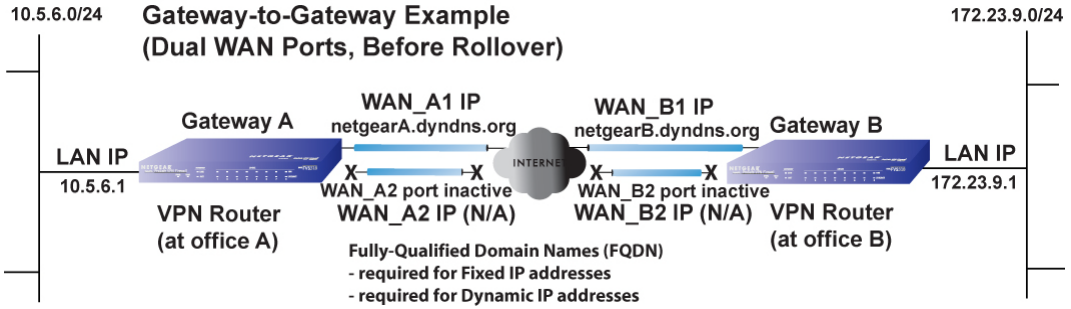


Figure B-14

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

After a rollover of a gateway WAN port, the previously inactive gateway WAN port becomes the active port (port WAN_A2 in this example) and one of the gateway VPN firewalls must re-establish the VPN tunnel.

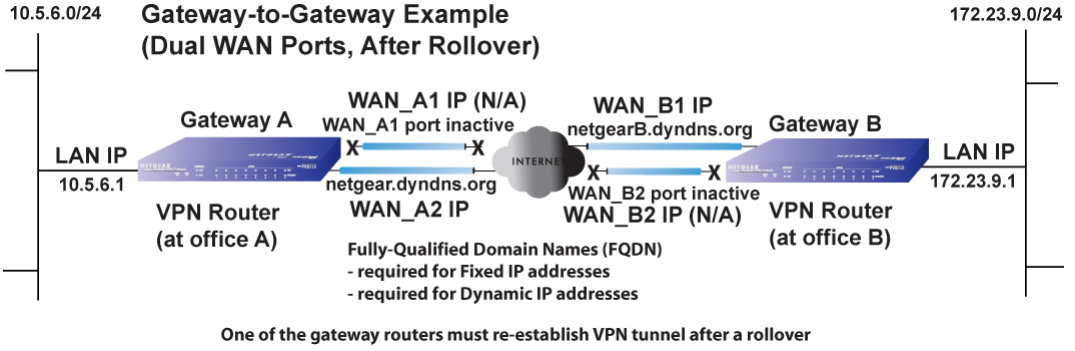


Figure B-15

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

VPN Gateway-to-Gateway: Dual Gateway WAN Ports for Load Balancing

In the case of the dual WAN ports on the gateway VPN firewall, either of the gateway WAN ports at one end can be programmed in advance to initiate the VPN tunnel with the appropriate gateway WAN port at the other end as necessary to manage the loads of the gateway WAN ports because the IP addresses of the WAN ports are known in advance.

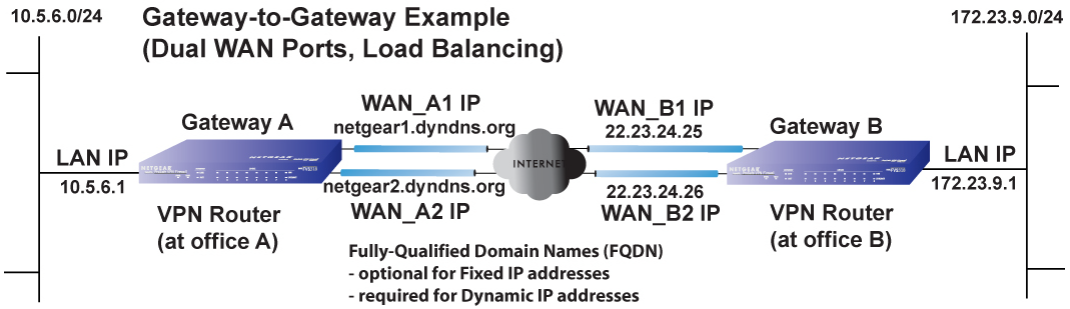


Figure B-16

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

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

Note: The telecommuter case presumes the home office has a dynamic IP address and NAT router.

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

- Single gateway WAN port
- Redundant dual gateway WAN ports for increased reliability (before and after rollover)

- Dual gateway WAN ports used for load balancing

VPN Telecommuter: Single Gateway WAN Port (Reference Case)

In the case of the single WAN port on the gateway VPN firewall, the remote PC client at the NAT router initiates the VPN tunnel because the IP address of the remote NAT router is not known in advance. The gateway WAN port must act as the responder.

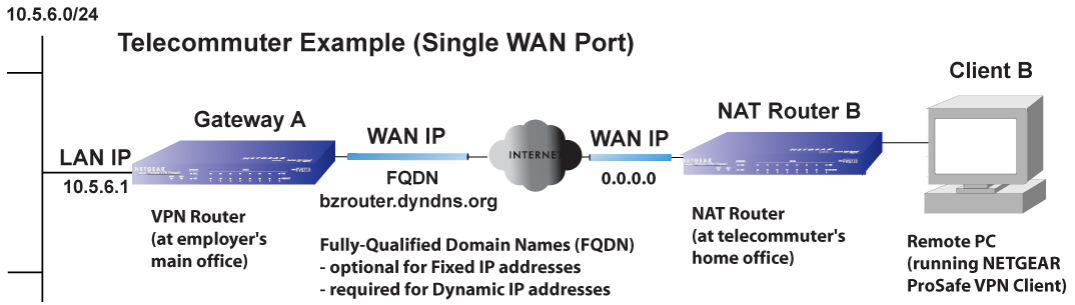


Figure B-17

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

VPN Telecommuter: Dual Gateway WAN Ports for Improved Reliability

In the case of the dual WAN ports on the gateway VPN firewall, the remote PC client initiates the VPN tunnel with the active gateway WAN port (port WAN1 in this example) because the IP address of the remote NAT router is not known in advance. The gateway WAN port must act as the responder.

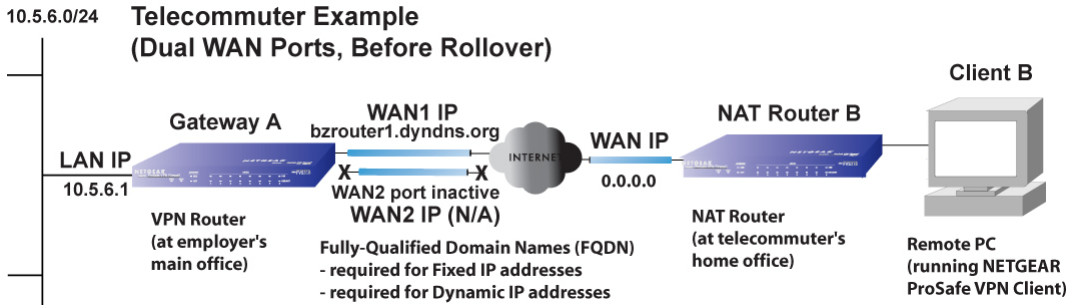


Figure B-18

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

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

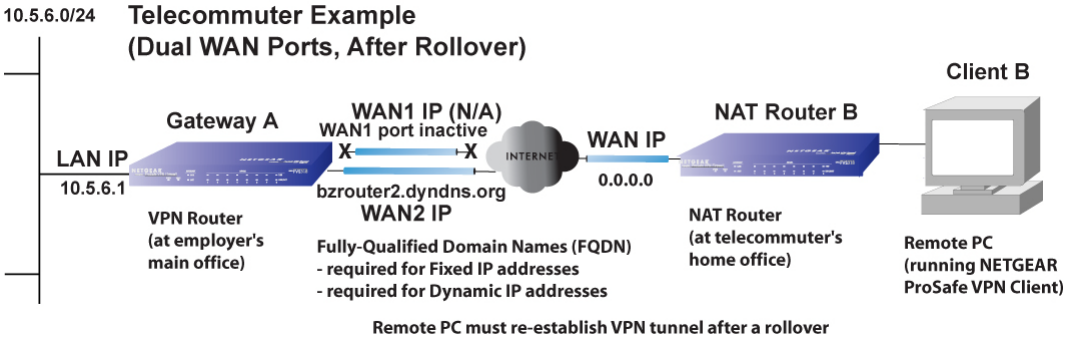


Figure B-19

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

VPN Telecommuter: Dual Gateway WAN Ports for Load Balancing

In the case of the dual WAN ports on the gateway VPN firewall, the remote PC client initiates the VPN tunnel with the appropriate gateway WAN port (that is, port WAN1 or WAN2 as necessary to balance the loads of the two gateway WAN ports) because the IP address of the remote NAT router is not known in advance. The chosen gateway WAN port must act as the responder.

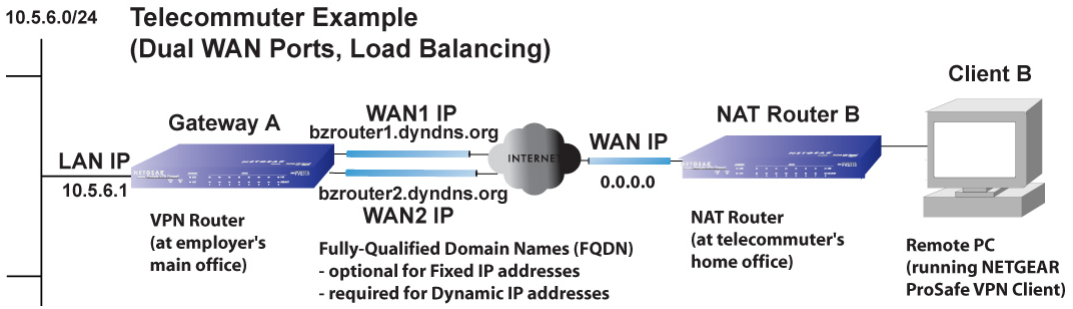


Figure B-20

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

Appendix C
System Logs and Error Messages

This appendix uses the following log parameter terms.

Table C-1. Log Parameter Terms

Term	Description
[FVX538]	System identifier
[kernel]	Message from the kernel.
CODE	Protocol code (e.g., protocol is ICMP, type 8) and CODE=0 means successful reply.
DEST	Destination IP Address of the machine to which the packet is destined.
DPT	Destination port.
IN	Incoming interface for packet.
OUT	Outgoing interface for packet.
PROTO	Protocol used.
SELF	Packet coming from the system only.
SPT	Source port
SRC	Source IP Address of machine from where the packet is coming.
TYPE	Protocol type

System Log Messages

This section describes log messages that belong to one of the following categories:

- Logs generated by traffic that is meant for the device.
- Logs generated by traffic that is routed or forwarded through the device.
- Logs generated by system daemons NTP, WAN daemon and others.

System Startup

This section describes log messages generated during system startup.

Table C-2. System Logs: System Startup

Message	Jan 1 15:22:28 [FVX538] [ledTog] [SYSTEM START-UP] System Started
Explanation	Log generated when the system is started.
Recommended Action	None

Reboot

This section describes log messages generated during system reboot.

Table C-3. System Logs: Reboot

Message	Nov 25 19:42:57 [FVX538] [reboot] Rebooting in 3 seconds
Explanation	Log generated when the system is rebooted from the web management.
Recommended Action	None

NTP

This section describes log messages generated by the NTP daemon during synchronization with the NTP server.

- The fixed time and date before NTP synchronizes with any of the servers is: Thu Jan 01 00:01:52 GMT 1970.
- The resynchronization interval is governed by the specification defined in: DOC-00045_Ntp_Spec.pdf.

Table C-4. System Logs: NTP

Message	Nov 28 12:31:13 [FVX538] [ntpdate] Looking Up time-f.netgear.com Nov 28 12:31:13 [FVX538] [ntpdate] Requesting time from time-f.netgear.com Nov 28 12:31:14 [FVX538] [ntpdate] adjust time server 69.25.106.19 offset 0.140254 sec Nov 28 12:31:14 [FVX538] [ntpdate] Synchronized time with time-f.netgear.com Nov 28 12:31:16 [FVX538] [ntpdate] Date and Time Before Synchronization: Tue Nov 28 12:31:13 GMT+0530 2006 Nov 28 12:31:16 [FVX538] [ntpdate] Date and Time After Synchronization: Tue Nov 28 12:31:16 GMT+0530 2006 Nov 28 12:31:16 [FVX538] [ntpdate] Next Synchronization after 2 Hours

Table C-4. System Logs: NTP (continued)

Explanation	Message1: DNS resolution for the NTP server (time-f.netgear.com) Message2: request for NTP update from the time server. Message3: Adjust time by re-setting system time. Message4: Display date and time before synchronization, that is when resynchronization started Message5: Display the new updated date and time. Message6: Next synchronization will be after the specified time mentioned. Example: In the above logs the next synchronization will be after two hours. The synchronization time interval is configurable via the CLI
Recommended Action	None

Login/Logout

This section describes logs generated by the administrative interfaces of the device.

Table C-5. System Logs: Login/Logout

Message	Nov 28 14:45:42 [FVX538] [login] Login succeeded: user admin from 192.168.10.10
Explanation	Login of user admin from host with IP address 192.168.10.10
Recommended Action	None
Message	Nov 28 14:55:09 [FVX538] [seclogin] Logout succeeded for user admin Nov 28 14:55:13 [FVX538] [seclogin] Login succeeded: user admin from 192.168.1.214
Explanation	Secure login/logout of user admin from host with IP address 192.168.1.214.
Recommended Action	None

Firewall Restart

This logging is always done.

Table C-6. System Logs: Firewall Restart

Message	Jan 23 16:20:44 [FVX538] [wand] [FW] Firewall Restarted
Explanation	Log generated when the firewall is restarted. This log is logged when firewall restarts after applying any changes in the configuration.
Recommended Action	None

IPSec Restart

This logging is always done.

Table C-7. System Logs: IPSec Restart

Message	Jan 23 16:20:44 [FVX538] [wand] [IPSEC] IPSEC Restarted
Explanation	Log generated when the IPSEC is restarted. This log is logged when IPSEC restarts after applying any changes in the configuration.
Recommended Action	None

WAN Status

This section describes the logs generated by the WAN component. If there are two ISP links for Internet connectivity, the VPN firewall can be configured either in Auto Rollover mode or Load Balancing mode.

Load Balancing

When the WAN mode is configured for Load Balancing, both the WAN ports are active simultaneously and the traffic is balanced between them. If one WAN link goes down, all the traffic is diverted to the WAN link that is active.

This section describes the logs generated when the WAN mode is set to Load Balancing.

Table C-8. System Logs: WAN Status, Load Balancing

Message	Dec 1 12:11:27 [FVX538] [wand] [LBFO] Restarting WAN1_ Dec 1 12:11:31 [FVX538] [wand] [LBFO] Restarting WAN2_ Dec 1 12:11:35 [FVX538] [wand] [LBFO] WAN1(UP), WAN2(UP)_ Dec 1 12:24:12 [FVX538] [wand] [LBFO] WAN1(UP), WAN2(DOWN)_ Dec 1 12:29:43 [FVX538] [wand] [LBFO] Restarting WAN2_ Dec 1 12:29:47 [FVX538] [wand] [LBFO] WAN1(UP), WAN2(DOWN)_
Explanation	Message 1 and Message 2 indicate that both the WANs are restarted. Message 3: This message shows that both the WANs are up and the traffic is balanced between the two WAN interfaces. Message 4: This message shows that one of the WAN links is down. At this point, all the traffic is directed through the WAN which is up
Recommended Action	None

Auto Rollover

When the WAN mode is configured for Auto Rollover, the primary link is active and secondary acts only as a backup. When the primary link goes down, the secondary link becomes active only until the primary link comes back up. The device monitors the status of the primary link using the configured WAN Failure Detection method.

This section describes the logs generated when the WAN mode is set to Auto Rollover.

System Logs: WAN Status, Auto Rollover

Message	Nov 17 09:59:09 [FVX538] [wand] [LBFO] WAN1 Test Failed 1 of 3 times_ Nov 17 09:59:39 [FVX538] [wand] [LBFO] WAN1 Test Failed 2 of 3 times_ Nov 17 10:00:09 [FVX538] [wand] [LBFO] WAN1 Test Failed 3 of 3 times_ Nov 17 10:01:01 [FVX538] [wand] [LBFO] WAN1 Test Failed 4 of 3 times_ Nov 17 10:01:35 [FVX538] [wand] [LBFO] WAN1 Test Failed 5 of 3 times_ Nov 17 10:01:35 [FVX538] [wand] [LBFO] WAN1(DOWN), WAN2(UP), ACTIVE(WAN2)_ Nov 17 10:02:25 [FVX538] [wand] [LBFO] WAN1 Test Failed 6 of 3 times_ Nov 17 10:02:25 [FVX538] [wand] [LBFO] Restarting WAN1_ Nov 17 10:02:57 [FVX538] [wand] [LBFO] WAN1 Test Failed 7 of 3 times_ Nov 17 10:03:27 [FVX538] [wand] [LBFO] WAN1 Test Failed 8 of 3 times_ Nov 17 10:03:57 [FVX538] [wand] [LBFO] WAN1 Test Failed 9 of 3 times_ Nov 17 10:03:57 [FVX538] [wand] [LBFO] Restarting WAN1_
Explanation	The Logs suggest that the fail-over was detected after 5 attempts instead of 3. However, the reason the messages appear as above is because of the WAN state transition logic which is part of the failover algorithm. The above logs can be interpreted as below. The primary link failure is properly detected after the 3rd attempt. Thereafter the algorithm attempts to restart WAN and checks once again to see if WAN1 is still down. This results in the 4th failure detection message. If it is then it starts secondary link and once secondary link is up, secondary link is marked as active. Meanwhile secondary link has failed once more and that results 5th failure detection message. Please note that the 5th failure detection and the message suggesting secondary link is active have the same timestamp and so they happen in the same algorithm state-machine cycle. So although it appears that the failover did not happen immediately after 3 failures, internally, the failover process is triggered after the 3rd failure and transition to secondary link is completed by the 5th failure. The primary link is also restarted every 3 failures till it is functional again. In the above log, primary link was restarted after the 6th failure, that is, 3 failures after the failover process was triggered.
Recommended Action	Check the WAN settings and WAN failure detection method configured for the primary link.

PPP Logs

This section describes the WAN PPP connection logs. The PPP type can be configured from the web management.

PPPoE Idle-Timeout Logs.

Table C-9. System Logs: WAN Status, PPPoE Idle-Timeout

Message	Nov 29 13:12:46 [FVX538] [pppd] Starting connection Nov 29 13:12:49 [FVX538] [pppd] Remote message: Success Nov 29 13:12:49 [FVX538] [pppd] PAP authentication succeeded Nov 29 13:12:49 [FVX538] [pppd] local IP address 50.0.0.62 Nov 29 13:12:49 [FVX538] [pppd] remote IP address 50.0.0.1 Nov 29 13:12:49 [FVX538] [pppd] primary DNS address 202.153.32.3 Nov 29 13:12:49 [FVX538] [pppd] secondary DNS address 202.153.32.3 Nov 29 11:29:26 [FVX538] [pppd] Terminating connection due to lack of activity. Nov 29 11:29:28 [FVX538] [pppd] Connect time 8.2 minutes. Nov 29 11:29:28 [FVX538] [pppd] Sent 1408 bytes, received 0 bytes. Nov 29 11:29:29 [FVX538] [pppd] Connection terminated.
Explanation	Message 1: PPPoE connection establishment started. Message 2: Message from PPPoE server for correct login Message 3: Authentication for PPP succeeded. Message 4: Local IP address assigned by the server. Message 5: Server side IP address. Message 6: primary DNS configured in WAN status page. Message 7: secondary DNS configured in WAN status page. Message 8: The PPP link has transitioned to idle mode. This event occurs if there is no traffic from the LAN network. Message 9: The time in minutes for which the link has been up. Message 10: Data sent and received at the LAN side during the link was up. Message 11: PPP connection terminated after idle timeout
Recommended Action	To reconnect during idle mode, initiate traffic from the LAN side.

PPTP Idle-Timeout Logs.

Table C-10. System Logs: WAN Status, PPTP Idle-Timeout

Message	Nov 29 11:19:02 [FVX538] [pppd] Starting connection Nov 29 11:19:05 [FVX538] [pppd] CHAP authentication succeeded Nov 29 11:19:05 [FVX538] [pppd] local IP address 192.168.200.214 Nov 29 11:19:05 [FVX538] [pppd] remote IP address 192.168.200.1 Nov 29 11:19:05 [FVX538] [pppd] primary DNS address 202.153.32.2 Nov 29 11:19:05 [FVX538] [pppd] secondary DNS address 202.153.32.2 Nov 29 11:20:45 [FVX538] [pppd] No response to 10 echo-requests Nov 29 11:20:45 [FVX538] [pppd] Serial link appears to be disconnected. Nov 29 11:20:45 [FVX538] [pppd] Connect time 1.7 minutes. Nov 29 11:20:45 [FVX538] [pppd] Sent 520 bytes, received 80 bytes. Nov 29 11:20:51 [FVX538] [pppd] Connection terminated.
Explanation	Message 1: Starting PPP connection process Message 2: Message from server for authentication success Message 3: Local IP address assigned by the server. Message 4: Server side IP address. Message 5: primary DNS configured in WAN status page. Message 6: secondary DNS configured in WAN status page. Message 7: Sensing idle link Message 8: Idle link sensed Message 9: Data sent and received at the LAN side during the link was up. Message 10: PPP connection terminated after idle timeout
Recommended Action	To reconnect during idle mode, initiate traffic from the LAN side.

PPP Authentication Logs.

Table C-11. System Logs: WAN Status, PPP Authentication

Message	Nov 29 11:29:26 [FVX538] [pppd] Starting link Nov 29 11:29:29 [FVX538] [pppd] Remote message: Login incorrect Nov 29 11:29:29 [FVX538] [pppd] PAP authentication failed Nov 29 11:29:29 [FVX538] [pppd] Connection terminated.WAN2(DOWN)_
Explanation	Starting link: Starting PPPoE connection process Remote message: Login incorrect: Message from PPPoE server for incorrect login PAP authentication failed: PPP authentication failed due to incorrect login Connection terminated: PPP connection terminated
Recommended Action	If authentication fails, then check the login/password and enter the correct one.

Web Filtering and Content Filtering Logs

To enable web keyword filtering logs from the CLI, set the value of keywordLog to 1.

The CLI command is: monitor/firewallLogs/logger/loggerConfig keywordLog 1.

Table C-12. System Logs: Web Filtering and Content Filtering

Message	Jan 23 16:36:35 [FVX538] [kernel] [KEYWORD_BLOCKED] [URL]==>[www.redhat.com/] IN=SELF OUT=SELF SRC=192.168.10.210 DST=209.132.177.50 PROTO=TCP SPT=4282 DPT=80
Explanation	• This packet is blocked by keyword blocking • The URL blocked due to keyword blocking is shown by [URL] along with source and destination IP addressed, protocol, source port and destination port. • For other parameters, refer to Table C-1.
Recommended Action	None
Message	Jan 23 16:53:32 [FVX538] [kernel] [JAVA_BLOCKED] [URL]==>[www.java.com/js/css.js] IN=SELF OUT=SELF SRC=192.168.10.210 DST=72.5.124.95 PROTO=TCP SPT=4294 DPT=80
Explanation	• This packet is blocked by content filtering with java components • The URL blocked due to java content filtering is [URL] along with source and destination IP addressed, protocol, source port and destination port. • For other parameters, refer to Table C-1.
Recommended Action	None
Message	Jan 23 16:56:08 [FVX538] [kernel] [COOKIE_BLOCKED] [URL]==>[www.java.com/en/img/headline/340x155_sportsforeveryone.jpg] IN=SELF OUT=SELF SRC=192.168.10.210 DST=72.5.124.95 PROTO=TCP SPT=4321 DPT=80
Explanation	• This packet is blocked by content filtering for cookies • The URL blocked due to cookie filtering shown by [URL] along with source and destination IP addressed, protocol, source port and destination port. • For other parameters, refer to Table C-1.
Recommended Action	None
Message	Jan 23 16:53:32 [FVX538] [kernel] [JAVA_BLOCKED] [URL]==>[www.java.com/js/css.js] IN=SELF OUT=SELF SRC=192.168.10.210 DST=72.5.124.95 PROTO=TCP SPT=4294 DPT=80
Explanation	• This packet is blocked by content filtering with java components • The URL blocked due to java content filtering is [URL] along with source and destination IP addressed, protocol, source port and destination port. • For other parameters, refer to Table C-1.
Recommended Action	None

Traffic Metering Logs

Table C-13. System Logs: Traffic Metering

Message	Jan 23 19:03:44 [TRAFFIC_METER] TRAFFIC_METER: Monthly Limit of 10 MB has reached for WAN1._
Explanation	Traffic limit to WAN1 that was set as 10Mb has been reached. This stops all the incoming and outgoing traffic if configured like that in “When Limit is reached” on Traffic Meter web page.
Recommended Action	To start the traffic, restart the Traffic Limit Counter.

Unicast Logs

Table C-14. System Logs: Unicast

Message	Nov 24 11:52:55 [FVX538] [kernel] UCAST IN=SELF OUT=WAN SRC=192.168.10.1 DST=192.168.10.10 PROTO=UDP SPT=800 DPT=2049
Explanation	• This packet (Unicast) is destined to the device from the WAN network. • For other parameters, refer to Table C-1.
Recommended Action	None

ICMP Redirect Logs

Table C-15. System Logs: Unicast, Redirect

Message	Feb 2007 22 14:36:07 [FVX538] [kernel] [LOG_PACKET] SRC=192.168.1.49 DST=192.168.1.124 PROTO=ICMP TYPE=5 CODE=1
Explanation	• This packet is ICMP Redirect message sent to the router bye another router. • For other parameters, refer to Table C-1.
Recommended Action	To enable these logs, from CLI command prompt of the router, enter this command: monitor/firewallLogs/logger/loggerConfig logIcmpRedirect 1 And to disable it, monitor/firewallLogs/logger/loggerConfig logIcmpRedirect 0

Multicast/Broadcast Logs

Table C-16. System Logs: Multicast/Broadcast

Message	Jan 1 07:24:13 [FVX538] [kernel] MCAST-BCAST IN=WAN OUT=SELF SRC=192.168.1.73 DST=192.168.1.255 PROTO=UDP SPT=138 DPT=138
Explanation	• This packet (Broadcast) is destined to the device from the WAN network. • For other parameters, refer to Table C-1.
Recommended Action	None

FTP Logging

Table C-17. System Logs: FTP

Message	Feb 2007 22 14:46:56 [FVX538] [kernel] [FTP-ACTIVE] SRC=192.168.10.211 DST=192.168.1.97 PROTO=TCP SPT=1983 DPT=21 Feb 2007 22 14:46:56 [FVX538] [kernel] [FTP-PASSIVE] SRC=192.168.10.211 DST=192.168.1.97 PROTO=TCP SPT=1984 DPT=21 Feb 2007 22 19:48:17 [FVX538] [kernel] [FTP-DATA][ACCEPT] SRC=192.168.10.10 DST=192.168.20.10 PROTO=TCP SPT=54879 DPT=6459
Explanation	• These packets are active and passive FTP session data transfers respectively. • For other parameters, refer to Table C-1.
Recommended Action	To enable these logs, from CLI command prompt of the router, enter this command: monitor/firewallLogs/logger/loggerConfig logFtp 1 And to disable it, monitor/firewallLogs/logger/loggerConfig logFtp 0

Invalid Packet Logging

Table C-18. System Logs: Invalid Packets

Message	2007 Oct 1 00:44:17 [FVX538] [kernel] [INVALID] [NO_CONNTRACK_ENTRY] [DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=TCP SPT=23 DPT=54899
Explanation	No Connecrtion Tracking entry exists
Recommended Action	1. Invalid packets are dropped. 2. Use this command to enable dropping and logging of the invalid packets: fw/rules/attackChecks/configure dropInvalid 1 To allow invalid packet and disable logging: fw/rules/attackChecks/configure dropInvalid 0

Table C-18. System Logs: Invalid Packets (continued)

Message	2007 Oct 1 00:44:17 [FVX538] [kernel] [INVALID][RST_PACKET][DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=TCP SPT=23 DPT=54899
Explanation	Invalid RST packet
Recommended Action	1. Invalid packets are dropped. 2. Use this command to enable dropping and logging of the invalid packets: fw/rules/attackChecks/configure dropInvalid 1 To allow invalid packet and disable logging: fw/rules/attackChecks/configure dropInvalid 0
Message	2007 Oct 1 00:44:17 [FVX538] [kernel] [INVALID][ICMP_TYPE][DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=ICMP TYPE=19 CODE=0
Explanation	Invalid ICMP Type
Recommended Action	1. Invalid packets are dropped. 2. Use this command to enable dropping and logging of the invalid packets: fw/rules/attackChecks/configure dropInvalid 1 To allow invalid packet and disable logging: fw/rules/attackChecks/configure dropInvalid 0
Message	2007 Oct 1 00:44:17 [FVX538] [kernel] [INVALID][TCP_FLAG_COMBINATION][DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=TCP SPT=23 DPT=54899
Explanation	Invalid TCP flag combination
Recommended Action	1. Invalid packets are dropped. 2. Use this command to enable dropping and logging of the invalid packets: fw/rules/attackChecks/configure dropInvalid 1 To allow invalid packet and disable logging: fw/rules/attackChecks/configure dropInvalid 0
Message	2007 Oct 1 00:44:17 [FVX538] [kernel] [INVALID][BAD_CHECKSUM]DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=TCP SPT=23 DPT=54899
Explanation	Bad Checksum
Recommended Action	1. Invalid packets are dropped. 2. Use this command to enable dropping and logging of the invalid packets: fw/rules/attackChecks/configure dropInvalid 1 To allow invalid packet and disable logging: fw/rules/attackChecks/configure dropInvalid 0
Message	2007 Oct 1 00:44:17 [FVX538] [kernel] [INVALID][BAD_HW_CHECKSUM][DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=ICMP TYPE=3 CODE=0

Table C-18. System Logs: Invalid Packets (continued)

Explanation	Bad Hardware Checksum for ICMP packets
Recommended Action	1. Invalid packets are dropped. 2. Use this command to enable dropping and logging of the invalid packets: fw/rules/attackChecks/configure dropInvalid 1 To allow invalid packet and disable logging: fw/rules/attackChecks/configure dropInvalid 0
Message	[INVALID][MALFORMED_PACKET][DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=TCP SPT=23 DPT=54899
Explanation	Malformed packet
Recommended Action	1. Invalid packets are dropped. 2. Use this command to enable dropping and logging of the invalid packets: fw/rules/attackChecks/configure dropInvalid 1 To allow invalid packet and disable logging: fw/rules/attackChecks/configure dropInvalid 0
Message	2007 Oct 1 00:44:17 [FVX538] [kernel] [INVALID][SHORT_PACKET][DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=TCP SPT=23 DPT=54899
Explanation	Short packet
Recommended Action	1. Invalid packets are dropped. 2. Use this command to enable dropping and logging of the invalid packets: fw/rules/attackChecks/configure dropInvalid 1 To allow invalid packet and disable logging: fw/rules/attackChecks/configure dropInvalid 0
Message	[INVALID][INVALID_STATE][DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=TCP SPT=23 DPT=54899
Explanation	Packet with Invalid State
Recommended Action	1. Invalid packets are dropped. 2. Use this command to enable dropping and logging of the invalid packets: fw/rules/attackChecks/configure dropInvalid 1 To allow invalid packet and disable logging: fw/rules/attackChecks/configure dropInvalid 0
Message	2007 Oct 1 00:44:17 [FVX538] [kernel] [INVALID][REOPEN_CLOSE_CONN][DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=TCP SPT=23 DPT=54899
Explanation	Attempt to re-open/close session

Table C-18. System Logs: Invalid Packets (continued)

Recommended Action	1. Invalid packets are dropped. 2. Use this command to enable dropping and logging of the invalid packets: fw/rules/attackChecks/configure dropInvalid 1 To allow invalid packet and disable logging: fw/rules/attackChecks/configure dropInvalid 0
Message	2007 Oct 1 00:44:17 [FVX538] [kernel] [INVALID][OUT_OF_WINDOW][DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=TCP SPT=23 DPT=54899
Explanation	Packet not in TCP window
Recommended Action	1. Invalid packets are dropped. 2. Use this command to enable dropping and logging of the invalid packets: fw/rules/attackChecks/configure dropInvalid 1 To allow invalid packet and disable logging: fw/rules/attackChecks/configure dropInvalid 0
Message	2007 Oct 1 00:44:17 [FVX538] [kernel] [INVALID][ERR_HELPER_ROUTINE][DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=TCP SPT=23 DPT=54899
Explanation	Error returned from helper routine
Recommended Action	1. Invalid packets are dropped. 2. Use this command to enable dropping and logging of the invalid packets: fw/rules/attackChecks/configure dropInvalid 1 To allow invalid packet and disable logging: fw/rules/attackChecks/configure dropInvalid 0

Routing Logs

This section is used to configure the logging options for each network segment like LAN-WAN for debugging purposes. This may generate a significant volume of log messages.

LAN to WAN Logs

Table C-19. Routing Logs: LAN to WAN

Message	Nov 29 09:19:43 [FVX538] [kernel] LAN2WAN[ACCEPT] IN=LAN OUT=WAN SRC=192.168.10.10 DST=72.14.207.99 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from LAN to WAN has been allowed by the firewall. • For other parameters, refer to Table C-1.
Recommended Action	None

LAN to DMZ Logs

Table C-20. Routing Logs: LAN to DMZ

Message	Nov 29 09:44:06 [FVX538] [kernel] LAN2DMZ[ACCEPT] IN=LAN OUT=DMZ SRC=192.168.10.10 DST=192.168.20.10 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from LAN to DMZ has been allowed by the firewall. • For other parameters, refer to Table C-1.
Recommended Action	None

DMZ to WAN Logs

Table C-21. Routing Logs: DMZ to WAN

Message	Nov 29 09:19:43 [FVX538] [kernel] DMZ2WAN[DROP] IN=DMZ OUT=WAN SRC=192.168.20.10 DST=72.14.207.99 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from DMZ to WAN has been dropped by the firewall. • For other parameters, refer to Table C-1.
Recommended Action	None

WAN to LAN Logs

Table C-22. Routing Logs: WAN to LAN

Message	Nov 29 10:05:15 [FVX538] [kernel] WAN2LAN[ACCEPT] IN=WAN OUT=LAN SRC=192.168.1.214 DST=192.168.10.10 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from LAN to WAN has been allowed by the firewall • For other parameters, refer to Table C-1.
Recommended Action	None

DMZ to LAN Logs

Table C-23. Routing Logs: DMZ to WAN

Message	Nov 29 09:44:06 [FVX538] [kernel] DMZ2LAN[DROP] IN=DMZ OUT=LAN SRC=192.168.20.10 DST=192.168.10.10 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from DMZ to LAN has been dropped by the firewall. • For other parameters, refer to Table C-1.
Recommended Action	None

WAN to DMZ Logs

Table C-24. Routing Logs: WAN to DMZ

Message	Nov 29 09:19:43 [FVX538] [kernel] WAN2DMZ[ACCEPT] IN=WAN OUT=DMZ SRC=192.168.1.214 DST=192.168.20.10 PROTO=ICMP TYPE=8 CODE=0
Explanation	• This packet from WAN to DMZ has been allowed by the firewall. • For other parameters, refer to Table C-1.
Recommended Action	None

Appendix D
Two Factor Authentication

This appendix provides an overview of Two-Factor Authentication, and an example of how to implement the WiKID solution.

This appendix contains the following sections:

- "Why do I need Two-Factor Authentication?" on this page.
- "NETGEAR Two-Factor Authentication Solutions" on page D-2

Why do I need Two-Factor Authentication?

In today's market, online identity theft and online fraud continue to be one of the fast-growing cyber crime activities used by many unethical hackers and cyber criminals to steal digital assets for financial gains. Many companies and corporations are losing millions of dollars and running into risks of revealing their trade secrets and other proprietary information as the results of these cyber crime activities. Security threats and hackers have become more sophisticated, and user names, encrypted passwords, and the presence of firewalls are no longer enough to protect the networks from being compromised. IT professionals and security experts have recognized the need to go beyond the traditional authentication process by introducing and requiring additional factors to the authentication process. NETGEAR has also recognized the need to provide more than just a firewall to protect the networks. As part the new maintenance firmware release, NETGEAR has implemented a more robust authentication system known as Two-Factor Authentication (2FA or T-FA) on its SSL and IPSec VPN firewall product line to help address the fast-growing network security issues.

What are the benefits of Two-Factor Authentication?

- **Stronger security**. Passwords cannot efficiently protect the corporate networks because attackers can easily guess simple passwords or users cannot remember complex and unique passwords. One-time passcode (OTP) strengthens and replaces the need to remember complex password.
- **No need to replace existing hardware**. Two-Factor Authentication can be added to existing NETGEAR products through via firmware upgrade.

- **Quick to deploy and manage**. The WiKID solution integrates seamlessly with the NETGEAR SSL and VPN firewall products.
- **Proven regulatory compliance**. Two-Factor Authentication has been used as a mandatory authentication process for many corporations and enterprises worldwide.

What is Two-Factor Authentication

Two-factor authentication is a new security solution that enhances and strengthens security by implementing multiple factors to the authentication process that challenge and confirm the users identities before they can gain access to the network. There are several factors that are used to validate the users to make that you are who you said you are. These factors are:

- Something you know—for example, your password or your PIN.
- Something you have—for example, a token with generated passcode that is either 6 to 8 digits in length.
- Something you are—for example, biometrics such as fingerprints or retinal.

This appendix focuses and discusses only the first two factors, something you know and something you have. This new security method can be viewed as a two-tiered authentication approach because it typically relies on what you know and what you have. A common example of two-factor authentication is a bank (ATM) card that has been issued by a bank institute:

- The PIN to access your account is "*something you know*"
- The ATM card is "*something you have*"

You must have both of these factors to gain access to your bank account. Similar to the ATM card, access to the corporate networks and data can also be strengthen using combination of the multiple factors such as a PIN and a token (hardware or software) to validate the users and reduce the incidence of online identity theft.

NETGEAR Two-Factor Authentication Solutions

NETGEAR has implemented 2 Two-Factor Authentication solutions from WiKID. WiKID is the software-based token solution. So instead of using only Windows Active Directory or LDAP as the authentication server, administrators now have the option to use WiKID to perform Two-Factor Authentication on NETGEAR SSL and VPN firewall products.

The WiKID solution is based on a request-response architecture where a one-time passcode (OTP), that is time-synchronized with the authentication server, is generated and sent to the user after the validity of a user credential has been confirmed by the server.

The request-response architecture is capable of self-service initialization by end-users, dramatically reducing implementation and maintenance costs. Here is an example of how WiKID works.

1. The user launches the WiKID token software, enter the PIN that has been given to them (*something they know*) and then press “continue” to receive the OTP from the WiKID authentication server:

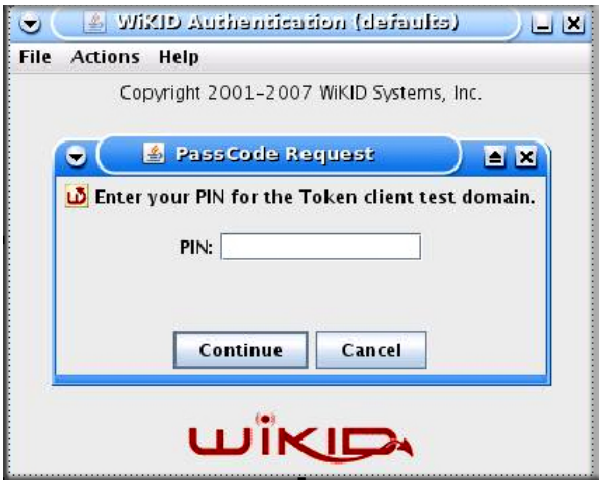


Figure D-1

2. A one-time passcode (*something they have*) is generated for this user.

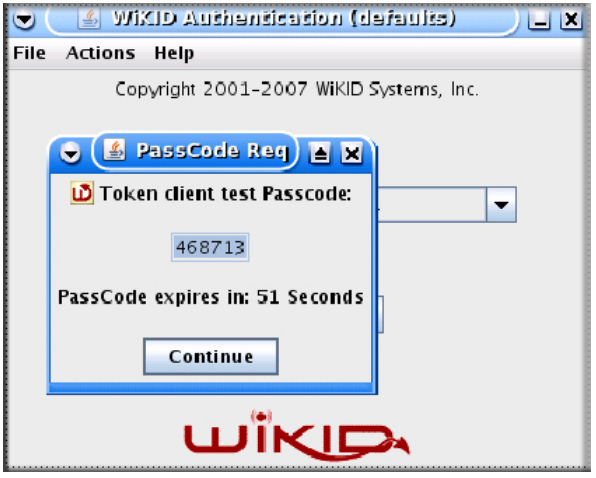


Figure D-2

Note: The one-time passcode is time synchronized to the authentication server so that the OTP can only be used once and must be used before the expiration time. If a user does not use this passcode before it is expired, the user must go through the request process again to generate a new OTP.

3. The user then proceeds to the Two-Factor Authentication login page and enters the generated one-time passcode as the login password.

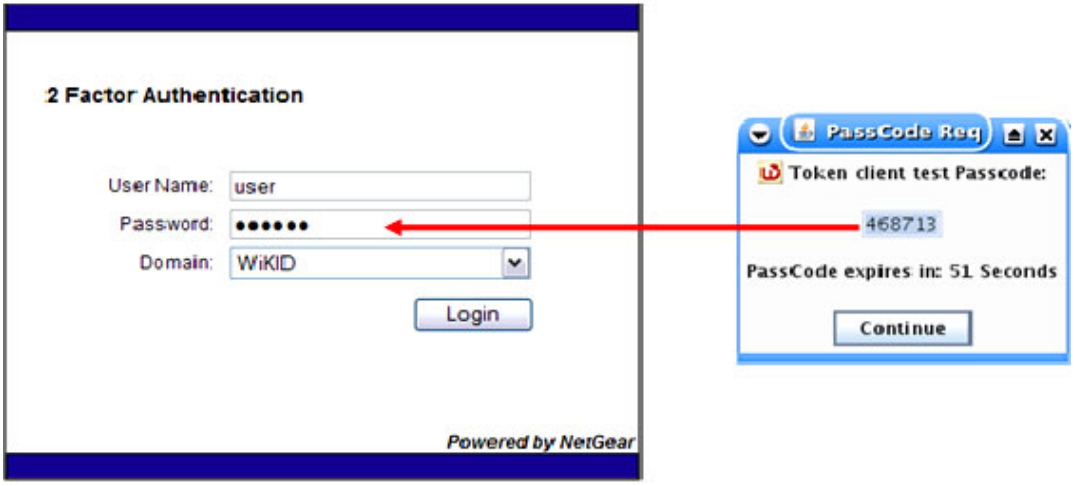


Figure D-3

Appendix E
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
TCP/IP Networking Basics	*http://documentation.netgear.com/reference/enu/tcpip/index.htm*
Wireless Networking Basics	*http://documentation.netgear.com/reference/enu/wireless/index.htm*
Preparing Your Network	*http://documentation.netgear.com/reference/enu/wsdhcp/index.htm*
Virtual Private Networking Basics	*http://documentation.netgear.com/reference/enu/vpn/index.htm*
Glossary	*http://documentation.netgear.com/reference/enu/glossary/index.htm*

Index

Numerics

3322.org *2-14*

A

access
  remote management *6-14*
Add DMZ WAN Outbound Services screen *4-12*
Add LAN DMZ Outbound Service screen *4-14*
Add LAN WAN Inbound Service *4-11*
Add LAN WAN Outbound Service screen *4-10*
Add Mode Config Record screen *5-34*
Add Protocol Binding
  Destination Network *2-12*
  Service *2-12*
address reservation *3-9*
Advanced Options
  MTU Size *2-17*
  Port Speed *2-17*
  Router's MAC Address *2-17*
ALG *4-23*
Allowing Videoconference from Restricted Addresses
  example of *4-16*
Application Level Gateway. *See* ALG.
ARP broadcast
  enable *3-5*, *3-14*
Attack Checks
  about *4-20*
Attack Checks screen *4-20*
authentication
  WiKID *6-11*
Authentication Algorithm
  IKE Policy *5-18*
Authentication Header
  VPN Policy *5-19*
Auto Detect *2-3*
Auto Uplink *1-3*
Auto-Rollover
  configuration of *2-9*
  definition of *2-8*
  Dual WAN ports *5-1*
  restoring WAN interface *2-10*
  use with DDNS *2-14*
  Using WAN port *2-9*

B

Back up settings *6-18*
backup and restore settings *6-19*
bandwidth capacity *6-1*
  LAN side *6-1*
  Load balancing mode *6-1*
  Rollover mode *6-1*
  WAN side *6-1*
Bandwidth Profile screen *4-27*
BigPond Cable *2-6*
Block Sites *1-2*
  Content Filtering *4-30*
  reducing traffic *6-4*
Block Sites screen *4-32*
Block TCP Flood *4-21*
block traffic
  with schedule *4-29*
Blocking Instant Messenger
  example of *4-19*

C

CA *5-18*
  about *5-19*, *5-20*

Cat5 cable *B-3*

certificate
generate new CSR *5-22*

Certificate Authority. See CA.

Certificate Revocation List. See CRL.

Certificate Signing Request, see CSR

certificates
management of *5-22*

Classical Routing
definition of *2-8*

CLI management
by Telnet *6-15*

command line interface *6-16*

configuration
automatic by DHCP *1-4*

Connecting the VPN firewall *2-1*

Content *4-30*

Content Filtering *4-1*
about *4-30*
Block Sites *4-30*
enabling *4-32*
firewall protection, about *4-1*

content filtering *1-2, 4-1*

CRL
managing *5-25*

crossover cable *1-3, 7-2*

CSR *5-22*

Customized Service
editing *4-26*

customized service
adding *4-25*

Customized Services
adding *4-3, 4-25*

D

Date
setting *6-21*

date
troubleshooting *7-7*

Daylight Savings Time
adjusting for *6-22*

DDNS
about *2-14*
configuration of *2-14*
links to *2-15*
providers of *2-14*
services, examples *2-15*

DDNS providers
links to *2-15*

Dead Peer Detection *5-18, 5-43*

default configuration
restoring *7-7*

default IP Address *1-9*

default password *1-9, 2-2*

default user name *1-9, 2-2*

denial of service attack *4-21*

Denial of Service. See DoS.

Destination Network
Add Protocol Binding *2-12*

DHCP *2-4*
DNS server address *3-4, 3-13*

DHCP Address Pool *3-4, 3-13*

DHCP IP Address pool *3-1*

DHCP log
monitoring *6-36*

DHCP server
about *3-1*
address pool *3-4, 3-13*
enable *3-4*
lease time *3-5, 3-13*

diagnostics
DNS lookup *7-8*
packet capture *7-8*
ping *7-8*
rebooting *7-8*
routing table *7-8*

Diagnostics screen *7-8*

Diffie-Hellman Group
IKE Policy *5-18*

Disable DHCP Server *3-1*

Disable DNS Proxy *4-21*

DMZ
about *3-11*

firewall security *3-12*

DMZ Port
increasing traffic *6-7*

DMZ port *1-3*
setting up *3-12*

DMZ Setup screen *3-12*

DMZ WAN Inbound Rule
example of *4-17*

DMZ WAN Rule
example of *4-16*

DMZ WAN Rules
about *4-12*
modifying *4-12*, *4-13*

DMZ WAN Rules screen *4-12*

DNS
definition of *2-7*
server IP address *3-4*, *3-13*

DNS addresses *2-7*

DNS lookup *2-9*

DNS Proxy *1-4*

DNS proxy *6-5*
enable *3-5*, *3-14*

DNS queries
Auto-Rollover *2-9*

Domain Name
router *3-4*, *3-13*

Domain Name Blocking *4-31*

Domain Name Servers. See DNS.

DoS
about protection *1-2*

Dual WAN
configuration of *2-7*

Dual WAN Port
inbound traffic *B-8*
load balancing, inbound traffic *B-9*

Dual WAN Port systems
VPN Tunnel addresses *5-2*

Dual WAN Ports
features of *1-2*
network planning *B-1*

Dual WAN ports
Auto-Rollover, configuration of *2-9*
Load Balancing, configuration of *2-11*

Dynamic DNS
configuration of *2-14*

Dynamic DNS Configuration screen *2-14*

Dynamic DNS. See DDNS

DynDNS.org *2-14*

E

Easy *1-4*

Edge Device *5-28*
RADIUS Server *5-26*
User Database *5-26*
XAUTH, with ModeConfig *5-37*

Edit Group Names *2-12*, *3-9*

Edit Protocol Binding *2-12*

E-mail alerts *6-23*

e-mail logs
enabling notification *4-40*, *6-23*

E-mail Server address *6-25*

Enable ARP Broadcast *3-5*, *3-14*

Enable DHCP server *3-1*

Enable DNS Proxy *3-5*, *3-14*

Enable LDAP Information *3-5*, *3-13*

Enable the DHCP Server
DMZ port *3-13*

Encapsulating Security Payload
VPN Policy *5-19*

Ending IP Address
DHCP Address Pool *3-4*, *3-13*

Ethernet, Auto Uplink *1-3*

Event Logs
emailing of *4-40*, *6-23*

Extended Authentication. See XAUTH.

F

factory default login *1-9*

factory default settings
revert to *6-18*

firewall

connecting to the Internet *2-1, B-3*
features *1-1, 1-2, 1-4*
front panel *1-6*
rear panel *1-6*
technical specifications *A-1*
viewing activity *6-34*

Firewall Log
Field Description *6-26*

Firewall Logs
emailing of *4-40, 6-23*
setting up *6-23*
viewing *6-26*

Firewall Logs & E-mail screen *4-40, 6-23*

Firewall Protection
Content Filtering, about *4-1*

firewall protection *4-1*

firmware
downloading *6-20*
upgrade *6-20*

Fixed IP *2-4*

FQDN *2-14, 5-2*

fragmented IP packets *6-5*

fully qualified domain name. See FQDN.

FVX538
features of *1-1*

G

Gateway IP Address *2-7*

Gigabit Switch port *1-1*

Group Names
editing *3-9*

groups, managing *3-6*

H

hardware requirements *B-3*

Hosting A Local Public Web Server
example of *4-15*

hosts, managing *3-6*

I

IGP *3-16*

IKE Policies
management of *5-16*

IKE Policies screen *5-27*

IKE Policy
about *5-16*
ModeConfig, configuring with *5-35*
XAUTH, adding to *5-27*

Inbound Rules
default definition *4-2*
field descriptions *4-6*
order of precedence *4-8*
Port Forwarding *4-3, 4-5*
rules for use *4-5*

inbound rules *4-5*
example *4-16*

Inbound Services
field descriptions *4-6*

inbound traffic *B-5, B-7*
dual WAN ports *B-8, B-9*
single WAN port reference case *B-7*

increasing traffic *6-4*
DMZ Port *6-7*
Port Forwarding *6-5*
Port Triggering *6-6*
VPN Tunnels *6-7*

installation *1-4*

Installation, instructions for *2-1*

Interior Gateway Protocol. See IGP.

Internet
configuration requirements *B-3, B-4*
configuring the connection manually *2-5*
connecting to *2-1*

Internet connection
configuring *2-2*
manual configuration *2-5*

Internet service
connection types *2-4*

Internet Service Provider. See ISP.

IP addresses
auto-generated *7-3*

DHCP address pool *3-1*
how to assign *3-1*
multi home LAN *3-6*
reserved *3-9*
router default *3-3*
IP Subnet Mask
router default *3-4*
IP/MAC Binding screen *4-35*
IPSec Connection Status screen *6-34*
IPSec Host *5-26, 5-29*
IPsec Host
XAUTH, with ModeConfig *5-37*
ISP connection
troubleshooting *7-4*

K

Keep alive *5-19*
Keep Connected
Idle TImeout *2-6*
Idle Timeout *2-6*
keepalive, VPN *5-42*
Keyword Blocking *4-31*
applying *4-33*
Keyword Filtering *1-3*

L

LAN
configuration *3-1*
using LAN IP setup options *3-2*
LAN DMZ Rules *4-13*
LAN DMZ Rules screen *4-14*
LAN Groups menu *3-7*
LAN Security Checks *4-21*
LAN Setup screen *3-3, 6-36*
LAN side
bandwidth capacity *6-1*
LAN WAN Inbound Rule
example of *4-15, 4-16, 4-17*
LAN WAN Inbound Services Rules
about *4-11*
add *4-11*
LAN WAN Outbound Rule
example of *4-19*
LAN WAN Outbound Rules
about *4-10*
LAN WAN Rule
example of *4-16*
LAN WAN Rules
default outbound *4-9*
LAN WAN Rules screen *4-9*
LDAP
overview *3-5, 3-13*
lease time *3-5, 3-13*
LEDs
explanation of *1-6*
troubleshooting *7-2*
Lightweight Directory Access Protocol. *See* LDAP.
Load Balancing
configuration of *2-11*
definition of *2-8*
use with DDNS *2-14*
view protocol bindings *2-11*
Load balancing mode
bandwidth capacity *6-1*
Log Entry Descriptions *C-1*
logging in
default login *2-2*

M

MAC address *7-7*
configuring *2-4, 2-5*
format of *2-17*
spoofing *7-5*
MAC addresses
blocked, adding *4-33*
Maximum Failover *2-10*
ModeConfig *5-32*
about *5-32*
assigning remote addresses, example *5-32*
Client Configuration *5-38*
IKE Policies menu, configuring *5-33*
menu, configuring *5-33*

testing Client *5-41*

monitoring devices *6-33*
by DHCP Client Requests *3-6, 6-33*
by Scanning the Network *3-6, 6-33*

MTU Size *2-17*

Multi Home LAN IPs
about *3-10*

multi home LAN IPs *3-6*

multi-NAT *4-16*

N

NAS
Identifier *5-31, 6-13*

NAT
definition of *2-8*
features of *1-3*
firewall, use with *4-1*
multi-NAT *4-16*

NetBIOS bridging over VPN *5-44*

Network Access Server. See NAS.

Network Address Translation. See NAT

Network Address Translation. See NAT.

Network Configuration *2-9*

network configuration requirements *B-3*

Network Database
about *3-6*
advantages of *3-6*

Network Database Group Names screen *3-9*

network planning
Dual WAN Ports *B-1*

Network Time Protocol. See NTP.

newsgroup *4-32*

NTP *6-21*
troubleshooting *7-7*

NTP Servers
custom *6-22*
default *6-22*

NTP servers
setting *6-21*

O

one-time passcode. *See* OTP.

Oray.net *2-14*

OTP *D-1, D-2*

Outbound Rules
default definition *4-2*
field descriptions *4-3*
order of precedence *4-8*
service blocking *4-3*

outbound rules *4-3*

Outbound Services
field descriptions *4-3*

Outbound Services Rules
adding *4-10*

P

package contents *1-5*

passwords and login timeout
changing *6-8*

passwords,restoring *7-7*

performance management *6-1*

Ping
responding to *2-5*
troubleshooting TCP/IP *7-5*

ping *7-9*

Ping On Internet Ports *4-20*

Ping to an IP address
Auto-Rollover *2-9*

Ping to this IP address *2-9*

planning
inbound traffic *B-5, B-7*
VPNs *B-6*

port filtering
service blocking *4-3*

Port Forwarding
Inbound Rules *4-3, 4-5*
increasing traffic *6-5*
rules, about *4-5*

port forwarding *6-5*

Port Mode *2-9*

port numbers *4-24*
Port Speed *2-17*
Port Triggering
about *4-37*
adding a rule *4-38*
increasing traffic *6-6*
modifying a rule *4-39*
rules of use *4-37*
port triggering *6-6*
status *6-36*
Port Triggering screen *4-38, 6-36*
ports
explanation of WAN and LAN *1-6*
PPP over Ethernet. See PPPoE.
PPPoE *1-4, 2-4, 2-6*
Account Name *2-6*
Domain Name *2-6*
Internet connection *2-6*
PPPoP
Idle Timeout *2-6*
PPTP *2-4, 2-6*
Account Name *2-6*
Domain Name *2-6*
Idle Timeout *2-6*
My IP Address *2-6*
Server IP Address *2-6*
precedence, order of for rules *4-24*
protocol numbers
assigned *4-24*
protocols
Routing Information Protocol *1-4*

Q

QoS *4-3*
about *4-26*
priority definitions *4-26*
shifting traffic mix *6-7*
SIP 2.0 support *1-1*
Quality of Service. See QoS

R

rack mounting *1-8*
rack mounting hardware *1-8*
RADIUS
description *6-11*
WiKID *6-11*
RADIUS Server
about *5-30*
configuring *5-30*
Edge Device *5-26*
RADIUS-CHAP *5-26, 5-29*
AUTH, using with *5-27*
RADIUS-PAP *5-26, 5-29*
XAUTH, using with *5-27*
reducing traffic *6-2*
Block Sites *6-4*
Service Blocking *6-2*
Source MAC Filtering *6-4*
remote management *6-11*
access *6-14*
configuration *6-14*
remote users
assigning addresses *5-32*
ModeConfig *5-32*
requirements
hardware *B-3*
reserved IP address
restrictions *3-8*
Reserved IP Addresses *3-9*
Restore saved settings *6-18*
Return E-mail Address *6-25*
RFC 1349 *4-26*
RFC1700
protocol numbers *4-24*
RIP *3-16*
about *3-16*
configuring parameters *3-16*
static routes, use with *3-15*
versions of *3-17*
RIP Configuration screen *3-17*
Rollover mode
bandwidth capacity *6-1*
router
upgrade software *6-20*

router administration
tips on 4-40
router broadcast
RIP, use with 3-17
Router Status 2-8
Router Status screen 6-30
Router Upgrade
about 6-20
Router's MAC Address 2-17
Routing Information Protocol 1-4
Routing Information Protocol. See RIP.
Routing log messages C-13
Routing screen 3-14
rules
blocking traffic 4-2
inbound 4-5
inbound example 4-16
order of precedence 4-24
outbound 4-3
service blocking 4-3
services-based 4-3
running tracert 6-16

S

schedule
blocking traffic 4-29
Schedule 1 screen 4-29
Security
features of 1-3
self certificate request 5-22
Send To E-mail Address 6-25
Service
Add Protocol Binding 2-12
Service Based Rules 4-3
Service Blocking
reducing traffic 6-2
service blocking 4-3
Outbound Rules 4-3
port filtering 4-3
service numbers
common protocols 4-24
Services screen 4-25
Session Initiation Protocol. *See* SIP.
Session Limit screen 4-22
Setting Up One-to-One NAT Mapping
example of 4-16
Settings Backup & Upgrade screen 6-18
Settings Backup and Firmware Upgrade 6-19
Simple Network Management Protocol. See SNMP.
Single WAN Port
inbound traffic B-7
SIP 4-23
sniffer 7-3
SNMP
about 6-16
configuring 6-17
global access 6-17
host only access 6-17
subnet access 6-17
SNMP screen 6-17
Source MAC Filter screen 4-33
Source MAC Filtering
enabling 4-33
reducing traffic 6-4
Source Network
Add Protocol Binding 2-12
Specifying an Exposed Host
example of 4-17
spoof MAC address 7-5
Starting IP Address
DHCP Address Pool 3-4, 3-13
stateful packet inspection 1-2
firewall, use with 4-1
Static IP 2-4
static IP 2-7
Static Route
example of 3-16
static routes
about 3-14
add or edit 3-14
configuring 3-14
example 3-16

stealth mode *4-21, 6-5*

SYN flood *4-21, 6-5*

SysLog Server
  IP Address *6-25*

System log messages *C-1*

T

TCP flood
  special rule *6-5*

TCP/IP
  network, troubleshooting *7-5*

Test Period *2-10*

Time
  setting *6-21*

time
  daylight savings, troubleshooting *7-8*
  troubleshooting *7-7*

Time Zone
  setting of *6-21*

Time Zone screen *6-21*

ToS. See QoS.

tracert
  use with DDNS *6-16*

traffic
  increasing *6-4*
  reducing *6-2*

traffic management *6-8*

traffic meter *2-5, 2-17*
  WAN2 ISP settings *2-5*

Troubleshooting
  NTP *7-7*

troubleshooting *7-1*
  browsers *7-3*
  configuration settings, using sniffer *7-3*
  defaults *7-3*
  ISP connection *7-4*
  testing your setup *7-6*
  Web configuration *7-3*

Trusted Certificates *5-21*

Trusted Domains
  building list of *4-33*

two-factor authentication
  WiKID *6-11*

Two-Factor Authentication. *See* WiKID.

TZO.com *2-14*

U

UDP flood *4-21*
  special rule *6-5*

Use Default Address *2-5*

Use Static IP Address *2-7*

User Database *5-26, 5-29*
  adding user *5-29*
  editing user *5-30*

User Database screen *5-29*

V

view protocol bindings
  Load Balancing *2-11*

VoIP (voice over IP) sessions *4-23*

VPN
  gateway to gateway, about *B-14*
  gateway-to-gateway, Dual gateway *B-15*
  gateway-to-gateway, single gateway *B-14*
  Load Balancing, examples of *B-10*
  load balancing, with dual WAN ports *B-7*
  Road Warrior, dual gateway *B-12*
  Road Warrior, examples of *B-11*
  Road Warrior, single gateway *B-11*
  Rollover, examples of *B-10*
  rollover, with dual WAN ports *B-6*
  telecommuter, about *B-16*
  telecommuter, Dual gateway *B-17*
  telecommuter, single gateway *B-17*

VPN Client
  configuring *5-7*

VPN firewall
  Connecting *2-1*

VPN Logs
  monitoring *6-35*

VPN Logs screen *6-35*

VPN passthrough *4-21*

VPN Policies screen *5-5, 5-8*

VPN Policy
Auto 5-18
Auto generated 5-16
Manual 5-18
VPN Tunnel addresses
Dual WAN Port systems 5-2
VPN Tunnel Connection
monitoring status 6-34
VPN Tunnels
increasing traffic 6-7
VPN tunnels
load balancing mode 5-2
rollover mode 5-2
VPN Wizard
Gateway tunnel 5-3
VPN Client, configuring 5-7
VPNC 5-3
VPNs B-6, B-9
about B-9
gateway-to-gateway B-14, B-15, B-16
road warrior B-11, B-13
telecommuter B-17, B-19
viewing VPN tunnel status 6-34

W

WAN
configuring Advanced options 2-16
configuring WAN Mode 2-7
WAN Failure Detection Method 2-8, 2-9
WAN Mode 2-9
WAN Port 1 status 2-4
WAN Ports
monitoring status 6-32
WAN ports
status of 2-8
WAN Security Check
about 4-20
WAN Settings screen 2-16
WAN side
bandwidth capacity 6-1
WAN Status 2-4
WAN1 Advanced Options 2-16
WAN1 ISP Settings
manual setup 2-5
WAN1 ISP Settings screen 2-3
WAN1 Protocol Bindings 2-11
WAN1 Protocol Bindings screen 2-12
WAN2 ISP
settings 2-5
WAN2 ISP Settings
manual setup 2-7
WAN2 Protocol Bindings 2-12
WAN2 Protocol Bindings screen. 2-12
WAN2 Traffic Meter 6-29
Web Components 4-31
blocking 4-33
filtering, about 4-30
Web configuration
troubleshooting 7-3
WiKID 6-11
authentication, overview D-1
WinPoET 2-6
WINS server 3-5, 3-13

X

XAUTH
IPSec Host 5-26
types of 5-26