

# ProSafe VPN Firewall 50 FVS338 Reference Manual



## NETGEAR®

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

202-10046-09  
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](mailto:support@netgear.com)

North American NETGEAR website: <http://www.netgear.com>

## Trademarks

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

## Statement of Conditions

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

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

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

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

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

## EU Regulatory Compliance Statement

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

## Bestätigung des Herstellers/Importeurs

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

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

## Certificate of the Manufacturer/Importer

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

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

## Voluntary Control Council for Interference (VCCI) Statement

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

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

Read instructions for correct handling.

## Additional Copyrights

AES	Copyright (c) 2001, Dr. Brian Gladman, brg@gladman.uk.net, Worcester, UK. All rights reserved. TERMS Redistribution and use in source and binary forms, with or without modification, are permitted subject to the following conditions: <ol style="list-style-type: none"><li>1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.</li><li>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.</li><li>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.</li></ol> <p>This software is provided "as is" with no express or implied warranties of correctness or fitness for purpose.</p>
-----	---

Open SSL	<p>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:</p> <ol style="list-style-type: none"> <li>1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.</li> <li>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.</li> <li>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 (<a href="http://www.openssl.org/">http://www.openssl.org/</a>).”</li> <li>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 <a href="mailto:openssl-core@openssl.org">openssl-core@openssl.org</a>.</li> <li>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.</li> <li>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 (<a href="http://www.openssl.org/">http://www.openssl.org/</a>).”</li> </ol> <p>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 (<a href="mailto:eay@cryptsoft.com">eay@cryptsoft.com</a>). This product includes software written by Tim Hudson (<a href="mailto:tjh@cryptsoft.com">tjh@cryptsoft.com</a>).</p>
MD5	<p>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.</p>

PPP	<p>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 MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.</p>
Zlib	<p>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:</p> <ol style="list-style-type: none"> <li>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.</li> <li>2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.</li> <li>3. This notice may not be removed or altered from any source distribution.</li> </ol> <p>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 <a href="ftp://ds.internic.net/rfc/rfc1950.txt">ftp://ds.internic.net/rfc/rfc1950.txt</a> (zlib format), rfc1951.txt (deflate format), and rfc1952.txt (gzip format).</p>

## Product and Publication Details

<b>Model Number:</b>	FVS338
<b>Publication Date:</b>	January 2010
<b>Product Family:</b>	VPN firewall
<b>Product Name:</b>	ProSafe VPN Firewall 50
<b>Home or Business Product:</b>	Business
<b>Language:</b>	English
<b>Publication Part Number:</b>	202-10046-09
<b>Publication Version Number</b>	1.0



# Contents

## ProSafe VPN Firewall 50 FVS338 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
Full Routing on Both the Broadband and Serial WAN Ports .....	1-2
A Powerful, True Firewall with Content Filtering .....	1-2
Security .....	1-3
Autosensing Ethernet Connections with Auto Uplink .....	1-3
Extensive Protocol Support .....	1-3
Easy Installation and Management .....	1-4
Maintenance and Support .....	1-5
Package Contents .....	1-5
VPN Firewall Hardware Components .....	1-5
Front Panel .....	1-6
Rear Panel .....	1-7
Factory Default Login .....	1-8

### Chapter 2

#### Connecting the VPN Firewall to the Internet

Understanding the Connection Steps .....	2-1
Logging in to the VPN Firewall .....	2-2
Navigating the Menus .....	2-3
Configuring your Internet Connection .....	2-3
Manually Configuring Your Broadband Internet Connection .....	2-9
Configuring the WAN Mode .....	2-11
Configuring Dynamic DNS (Optional) .....	2-14

Configuring Advanced WAN Options (Optional) .....2-16  
    Additional WAN Related Configuration .....2-18

**Chapter 3**  
**LAN Configuration**

Choosing the VPN Firewall DHCP Options .....3-1  
Configuring the LAN Setup Options .....3-2  
Managing Groups and Hosts .....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 IPs Addresses .....3-10  
Configuring Static Routes .....3-11  
    Static Route Example .....3-13  
Configuring Routing Information Protocol (RIP) .....3-14

**Chapter 4**  
**Firewall Protection and Content Filtering**

About Firewall Security and Content Filtering .....4-1  
Using Rules to Block or Allow Specific Kinds of Traffic .....4-2  
    Services-Based Rules .....4-2  
    Viewing the Firewall Rules .....4-7  
    Order of Precedence for Firewall Rules .....4-8  
    Setting the Default Outbound Policy .....4-8  
    Creating a LAN WAN Outbound Services Rule .....4-8  
    Creating a LAN WAN Inbound Services Rule .....4-9  
    Modifying Rules .....4-10  
    Inbound Rules Examples .....4-11  
    Outbound Rules Example: Blocking Instant Messenger .....4-14  
Configuring Other Firewall Features .....4-15  
    Attack Checks .....4-15  
    Configuring Session Limits .....4-17  
    Managing the Application Level Gateway for SIP Sessions .....4-19  
Creating Services, QoS Profiles, and Bandwidth Profiles .....4-20  
    Adding Customized Services .....4-20



Specifying Quality of Service (QoS) Priorities .....	4-22
Creating Bandwidth Profiles .....	4-23
Setting a Schedule to Block or Allow Specific Traffic .....	4-25
Blocking Internet Sites (Content Filtering) .....	4-26
Configuring Source MAC Filtering .....	4-29
Configuring IP/MAC Address Binding .....	4-31
Configuring Port Triggering .....	4-33
E-Mail Notifications of Event Logs and Alerts .....	4-36
Administrator Tips .....	4-36

## Chapter 5

### Virtual Private Networking

Considerations for Dual WAN Port Systems .....	5-1
Using the VPN Wizard for Client and Gateway Configurations .....	5-2
Creating Gateway to Gateway VPN Tunnels with the Wizard .....	5-2
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 .....	5-15
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
ModeConfig 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 .....6-7  
Configuring Users, Administrative Settings, and Remote Management .....6-7  
    Changing Passwords and Settings .....6-8  
    Adding External Users .....6-9  
    Configuring an External Server for Authentication .....6-10  
    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 Router Configuration and System Status .....6-30  
    Monitoring VPN Firewall Statistics .....6-32  
    Monitoring WAN Ports Status .....6-33  
    Monitoring Attached Devices .....6-34  
    Monitoring VPN Tunnel Connection Status .....6-35  
    Viewing the VPN Logs .....6-36  
    Viewing the DHCP Log .....6-37  
    Viewing Port Triggering Status .....6-37

**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
Performing Diagnostics .....	7-8

## Appendix A

### Default Settings and Technical Specifications

## Appendix B

### System Logs and Error Messages

System Log Messages .....	B-1
System Startup .....	B-1
Reboot .....	B-2
NTP .....	B-2
Login/Logout .....	B-3
VPN Firewall Restart .....	B-3
IPSec Restart .....	B-4
WAN Status .....	B-4
Web Filtering and Content Filtering Logs .....	B-7
Traffic Metering Logs .....	B-8
Unicast Logs .....	B-8
FTP Logging .....	B-9
Invalid Packet Logging .....	B-10
Routing Logs .....	B-12
LAN to WAN Logs .....	B-13
WAN to LAN Logs .....	B-13

## Appendix C

### Two Factor Authentication

Why do I need Two-Factor Authentication? .....	C-1
What are the benefits of Two-Factor Authentication? .....	C-1
What is Two-Factor Authentication .....	C-2

NETGEAR Two-Factor Authentication Solutions ..... C-2

- Appendix D**
- Related Documents**
- Index**

# About This Manual

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

## Conventions, Formats and Scope

---


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


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


<i>Italics</i>	Emphasis, books, CDs, file and server names, extensions
<b>Bold</b>	User input, IP addresses, GUI screen text
Fixed	Command prompt, CLI text, code
<i>italics</i>	URL links

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

	<b>Note:</b> This format is used to highlight information of importance or special interest.
---	--

	<b>Tip:</b> This format is used to highlight a procedure that will save time or resources.
---	--

	<b>Warning:</b> Ignoring this type of note may result in a malfunction or damage to the equipment.
---	--

	<b>Danger:</b> This is a safety warning. Failure to take heed of this notice may result in personal injury or death.
---	--

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

Product Version	ProSafe VPN Firewall 50
Manual Publication Date	January 2010

For more information about network, Internet, firewall, and VPN technologies, see the links to the NETGEAR website in [Appendix D, “Related Documents.”](#)



**Note:** Updates to this product 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
202-10046-02	1.0		Product update: New firmware and new user Interface
202-10046-03	1.0		Remove Trend Micro
202-10046-04	1.0		Updated features
202-10046-05	1.0		New features: IP/MAC Binding; Bandwidth Limits; Session Limits; IKE Keep Alive; Dead Peer Detection; Oray support
202-10046-05	1.1		Document corrections
202-10046-05	1.2		Document additions to Appendix B
202-10046-06	1.0		Maintenance release

202-10046-08	1.0		<p>Adds these corrections and topics for the March 2009 firmware maintenance release:</p> <ul style="list-style-type: none"> <li>• WIKID 2 factor authentication</li> <li>• SIP AGL support</li> <li>• DHCP Relay support</li> <li>• Update VPN configuration procedure topics</li> <li>• Update the Certificate management topic</li> <li>• Correct the firewall scheduling topic</li> </ul>
202-10046-09	1.0	January 2010	<p>Added the following new features for the January 2010 firmware maintenance release:</p> <ul style="list-style-type: none"> <li>• Connection reset and delay options on the Broadband ISP Settings screen (see <a href="#">“Manually Configuring Your Broadband Internet Connection”</a>).</li> <li>• Support for DNS 3322 in the Dynamic DNS submenu (see <a href="#">“Configuring Dynamic DNS (Optional)”</a>).</li> <li>• Support for an address range for inbound LAN rules on the Add LAN WAN Inbound Service screen (see <a href="#">“Inbound Rules (Port Forwarding)”</a> and <a href="#">“Creating a LAN WAN Inbound Services Rule”</a>).</li> <li>• Support for new log options such as Resolved DNS Names and VPN on the Firewall Logs &amp; E-mail screen (see <a href="#">“Activating Notification of Events and Alerts”</a>).</li> </ul> <p>In addition, made the following substantial changes to the book:</p> <ul style="list-style-type: none"> <li>• Provided new captures for almost all screens and resized the some existing screen captures for better viewing.</li> <li>• Made global stylistic changes for consistency and clarity.</li> <li>• Made minor revisions in <a href="#">Chapter 1, “Introduction.”</a></li> <li>• Reorganized <a href="#">Chapter 2, “Connecting the VPN Firewall to the Internet.”</a> In addition: <ul style="list-style-type: none"> <li>* Revised all sections in this chapter.</li> <li>* Added the <a href="#">“Understanding the Connection Steps”</a> section.</li> <li>* Added the <a href="#">“Navigating the Menus”</a> section.</li> <li>* Added the <a href="#">“Additional WAN Related Configuration”</a> section.</li> <li>* Moved the <a href="#">“Enabling the Traffic Meter”</a> section to <a href="#">Chapter 6, “VPN Firewall and Network Management.”</a></li> </ul> </li> <li>• Reorganized <a href="#">Chapter 3, “LAN Configuration,”</a> In addition: <ul style="list-style-type: none"> <li>* Made major revision in the <a href="#">“Configuring the LAN Setup Options”</a> section.</li> <li>* Revised all sections in this chapter.</li> </ul> </li> </ul>

202-10046-09 (continued)	1.0	January 2010	<p>(continued)</p> <ul style="list-style-type: none"> <li>• Reorganized <a href="#">Chapter 4, “Firewall Protection and Content Filtering.”</a> In addition: <ul style="list-style-type: none"> <li>* Revised all sections in this chapter.</li> <li>* Added the <a href="#">“Configuring Other Firewall Features”</a> section (which includes the new <a href="#">“Managing the Application Level Gateway for SIP Sessions”</a> subsection).</li> <li>* Added the <a href="#">“Creating Services, QoS Profiles, and Bandwidth Profiles”</a> section.</li> </ul> </li> <li>• Reorganized <a href="#">Chapter 5, “Virtual Private Networking.”</a> In addition: <ul style="list-style-type: none"> <li>* Made a major revision of the <a href="#">“Managing Certificates”</a> section in this chapter.</li> <li>* Added the <a href="#">“Configuring Keepalives and Dead Peer Detection”</a> section.</li> <li>* Added the <a href="#">“Configuring NetBIOS Bridging with VPN”</a> section.</li> <li>* Made revisions in all other sections of this chapter.</li> </ul> </li> <li>• Reorganized <a href="#">Chapter 6, “VPN Firewall and Network Management.”</a> In addition: <ul style="list-style-type: none"> <li>* Made major revisions in the <a href="#">“Configuring Users, Administrative Settings, and Remote Management”</a> section.</li> <li>* Made major revisions in the <a href="#">“Monitoring System Performance”</a> section.</li> <li>* Added the <a href="#">“Monitoring VPN Firewall Statistics”</a> section.</li> <li>* Added the <a href="#">“Monitoring Attached Devices”</a> section.</li> <li>* Included the <a href="#">“Enabling the Traffic Meter”</a> section (moved from <a href="#">Chapter 2, “Connecting the VPN Firewall to the Internet”</a>).</li> <li>* Moved the <a href="#">“Performing Diagnostics”</a> section to <a href="#">Chapter 7, “Troubleshooting.”</a></li> <li>* Made revisions in all other sections of this chapter.</li> </ul> </li> <li>• Revised all sections in <a href="#">Chapter 7, “Troubleshooting”</a> and included the <a href="#">“Performing Diagnostics”</a> section (moved from <a href="#">Chapter 6, “VPN Firewall and Network Management”</a>).</li> </ul>
-----------------------------	-----	-----------------	--



# Chapter 1

## Introduction

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

The FVS338 is a complete security solution that protects your network from attacks and intrusions. For example, the FVS338 provides support for Stateful Packet Inspection, Denial of Service (DoS) attack protection and multi-NAT support. The FVS338 supports multiple Web content filtering options, plus browsing activity reporting and instant alerts—both, via e-mail. Network administrators can establish restricted access policies based on time-of-day, Website addresses and address keywords, and share high-speed cable/DSL Internet access for a local network.

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

This chapter contains the following sections:

- [“Key Features”](#) on this page
- [“Package Contents”](#) on page 1-5
- [“VPN Firewall Hardware Components”](#) on page 1-5
- [“Factory Default Login”](#) on page 1-8

## Key Features

---

The FVS338 provides the following features:

- One 10/100 Mbps port for an Ethernet connection to a broadband WAN device, such as a cable modem or DSL modem, and one serial port for a dial-up modem connection to the Internet through the public switched telephone network (PSTN).
- Dual WAN ports (one broadband and one serial) provide for increased system reliability.
- Support for up to 50 VPN tunnels.
- Support for up to 400 internal LAN users (and 50K connections).
- Easy, web-based setup for installation and management.
- URL keyword content filtering and site blocking security.

- Quality of Service (QoS) support for traffic prioritization.
- Built in 8-port 10/100 Mbps switch.
- Extensive Protocol Support.
- Login capability.
- SNMP for manageability.
- Front panel LEDs for easy monitoring of status and activity.
- Flash memory for firmware upgrade.

## Full Routing on Both the Broadband and Serial WAN Ports

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

- Internet access via either the serial or broadband port.
- Auto rollover connectivity (fail-over) through an analog modem connected to the serial port. If the broadband Internet connection fails, after waiting for an pre-specified amount of time the FVS338 can automatically establish a backup dial-up Internet connection via its serial port.

## A Powerful, True Firewall with Content Filtering

Unlike simple Internet sharing NAT routers, the FVS338 is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- DoS protection. Automatically detects and thwarts DoS attacks such as Ping of Death, SYN Flood, LAND Attack, and IP Spoofing.
- Blocks unwanted traffic from the Internet to your LAN.
- Blocks access from your LAN to Internet locations or services that you specify as off-limits.
- Logs security incidents. The FVS338 will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the FVS338 to e-mail the log to you at specified intervals. You can also configure the FVS338 to send immediate alert messages to your e-mail address or e-mail pager whenever a significant event occurs.
- With its URL keyword filtering feature, the FVS338 prevents objectionable content from reaching your PCs. The FVS338's firewall allows you to control access to Internet content by screening for keywords within Web addresses. You can configure the firewall to log and report attempts to access objectionable Internet sites.

## Security

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

- **PCs Hidden by NAT.** NAT opens a temporary path to the Internet for requests originating from the local network. Requests originating from outside the LAN are discarded, preventing users outside the LAN from finding and directly accessing the PCs on the LAN.
- **Port Forwarding with NAT.** Although NAT prevents Internet locations from directly accessing the PCs on the LAN, the FVS338 allows you to direct incoming traffic to specific PCs based on the service port number of the incoming request. You can specify forwarding of single ports or ranges of ports.
- **Exposed Host (Software DMZ).** Incoming traffic from the Internet is normally discarded by the FVS338 unless the traffic is a response to one of your local computers or a service for which you have configured an inbound rule. Instead of discarding this traffic, you can have it forwarded to one computer on your network.

## Autosensing Ethernet Connections with Auto Uplink

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

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

## Extensive Protocol Support

The FVS338 supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP).

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

- **Automatic Configuration of Attached PCs by DHCP.** The FVS338 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 FVS338 provides its own address as a DNS server to the attached PCs. The FVS338 obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.
- **PPP over Ethernet (PPPoE).** PPPoE is a protocol for connecting remote hosts to the Internet over a DSL connection by simulating a dial-up connection. This feature eliminates the need to run a login program such as EnterNet or WinPOET on your PC.

## Easy Installation and Management

You can install, configure, and operate the FVS338 within minutes after connecting it to the network. The following features simplify installation and management tasks:

- **Browser-based management.** Browser-based configuration allows you to easily configure your firewall from almost any type of personal computer, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided and online help documentation is built into the browser-based Web Management Interface.
- **Smart Wizard.** The FVS338 automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- **VPN Wizard.** The FVS338 includes the NETGEAR VPN Wizard to easily configure VPN tunnels according to the recommendations of the Virtual Private Network Consortium (VPNC) to ensure the VPN tunnels are interoperable with other VPNC-compliant VPN routers and clients.
- **SNMP.** The FVS338 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 FVS338 incorporates built-in diagnostic functions such as Ping, Trace Route, DNS lookup, and remote reboot.
- **Remote management.** The FVS338 allows you to securely login to the Web Management Interface from a remote location on the Internet. For additional security, you can limit remote management access to a specified remote IP address or range of addresses, and you can choose a nonstandard port number.

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

## Maintenance and Support

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

- 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:

- FVS338 ProSafe VPN Firewall 50
- AC power adapter
- Category 5 Ethernet cable
- *Resource CD*, including:
  - Application Notes and other helpful information.
  - ProSafe VPN Client Software (one user license)
- Warranty and Support Information Card.

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

## VPN Firewall Hardware Components

---

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

## Front Panel

The FVS338 front panel shown below contains the port connections, status LEDs, and the factory defaults reset button.

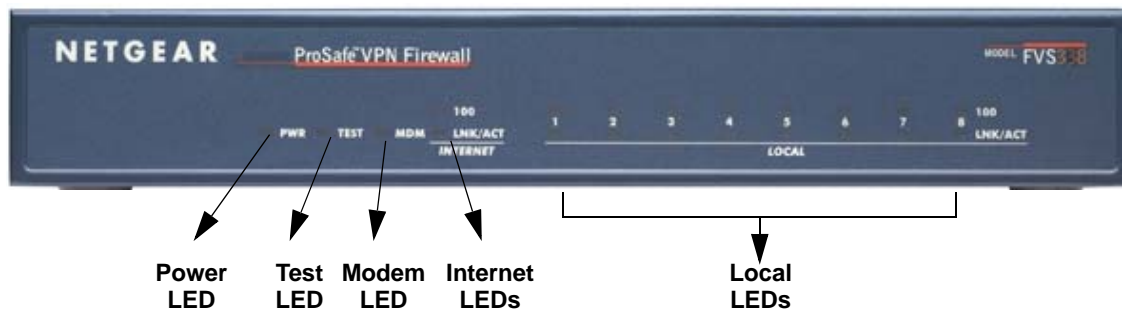


Figure 1-1

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

Table 1-1. Object Descriptions

Object	Activity	Description
Power LED	On (Green)	Power is supplied to the FVS338.
	Off	Power is not supplied to the FVS338.
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.
MDM LED	On (Green)	The serial port has successfully connected to an ISP and received an IP Address.
	Blinking (Green)	Server data is being transmitted or received by the serial port.
	Off	The serial port has no link.
Internet LEDs	<b>Link/Act LED</b>	
	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.

**Table 1-1. Object Descriptions (continued)**

Object	Activity	Description
<b>Internet LEDs</b> (continued)	<b>100 LED</b>	
	On (Green)	The WAN port is operating at 100 Mbps.
	Off	The WAN port is operating at 10 Mbps.
<b>Local LEDs</b>	<b>Link/Act LED</b>	
	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.
	<b>100 LED</b>	
	On (Green)	The LAN port is operating at 100 Mbps.
	Off	The LAN port is operating at 10 Mbps.

## Rear Panel

The rear panel of the FVS338 contains the On/Off switch and AC power connection.

**Figure 1-2**

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

- Modem port: serves as the WAN2 Internet (dial-up) port through the public switched telephone network (PSTN).
- Factory Defaults reset button.
- Local ports: 8-port RJ-45 10/100 Mbps Fast Ethernet Switch, N-way automatic speed negotiation, auto MDI/MDIX.
- Internet port: serves as the WAN1 Internet (broadband) port. One RJ-45 WAN port, N-way automatic speed negotiation, Auto MDI/MDIX.
- On/Off switch
- DC power in (12 VDC, 1.2A)

## Factory Default Login

---

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

- IP Address: **http://192.168.1.1** to reach the Web-based GUI from the LAN
- User name: **admin**
- Password: **password**

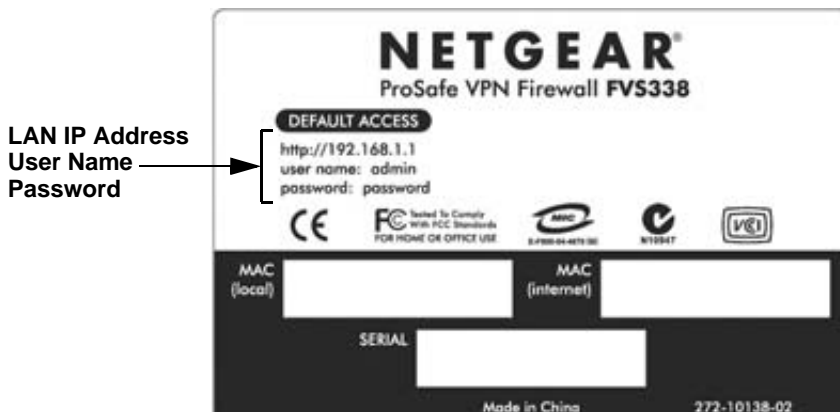


Figure 1-3

To log in to the FVS338 once it is connected:

1. Go to **http://192.168.1.1**.

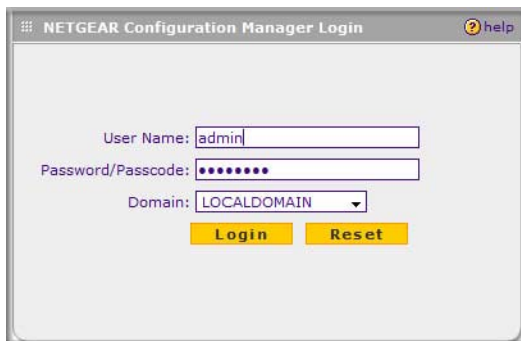


Figure 1-4

2. Enter **admin** for User Name and **password** for Password.



# Chapter 2

## Connecting the VPN Firewall to the Internet

This section provides instructions for connecting the ProSafe VPN Firewall 50 FVS338, including these topics:

- “Understanding the Connection Steps” on this page
- “Logging in to the VPN Firewall” on page 2-2
- “Navigating the Menus” on page 2-3
- “Configuring your Internet Connection” on page 2-3
- “Manually Configuring Your Broadband Internet Connection” on page 2-9
- “Configuring the WAN Mode” on page 2-11
- “Configuring Dynamic DNS (Optional)” on page 2-14
- “Configuring Advanced WAN Options (Optional)” on page 2-16

### Understanding the Connection Steps

---

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

1. **Connect the firewall physically to your network.** Connect the cables and restart your network according to the instructions in the installation guide. See the *ProSafe VPN Firewall 50 FVS338 Installation Guide* 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 in to 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 your Internet Connection” on page 2-3.
4. **Configure the WAN mode (required for dial-up backup WAN operation).** Select either NAT or classical routing, and select either single WAN mode or single WAN with dial-up backup WAN operation. See “Configuring the WAN Mode” on page 2-11.

5. **Configure dynamic DNS on the WAN ports (optional).** If required, configure your fully qualified domain names during this phase. See [“Configuring Dynamic DNS \(Optional\)”](#) on page 2-14.
6. **Configure the WAN options (optional).** Optionally, you can change the MAC address, the default MTU size, and the port speed. However, these are relatively advanced features and changing them is not usually required. See [“Configuring Advanced WAN Options \(Optional\)”](#) on page 2-16.

Each of these tasks is detailed separately in this chapter. Setting up VPN tunnels is covered in [Chapter 5, “Virtual Private Networking.”](#)

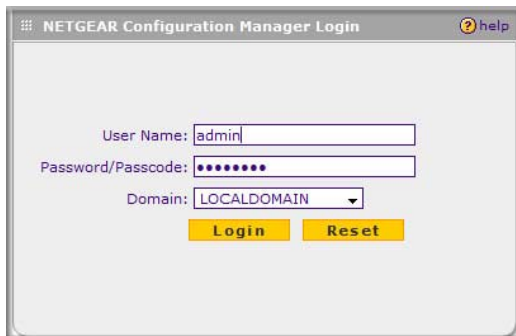
## Logging in to the VPN Firewall

---

To connect to the VPN firewall, your computer needs to be configured to obtain an IP address automatically from the VPN firewall by DHCP. For instructions on how to configure your computer for DHCP, see the [“Preparing Your Network”](#) document that you can access from [Appendix D, “Related Documents.”](#)

To log in to the VPN firewall:

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



**Figure 2-1**

2. Enter **admin** for the User Name and **password** for the 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**. The Web Configuration Manager appears, displaying the Router Status screen as the default screen.



**Note:** See “[Enabling Remote Management Access](#)” on page 6-14 for information on remote management. If you enable remote management, change your password to a more secure one than the standard factory default (see “[Changing Passwords and Settings](#)” on page 6-8).

## Navigating the Menus

The Web Configuration Manager menus are organized in a layered structure of main categories and submenus:

- **Main menu.** The horizontal orange bar near the top of the page is the main menu, containing the primary configuration categories. Clicking on a primary category changes the contents of the submenu bar.
- **Submenu.** The horizontal grey bar immediately below the main menu is the submenu, containing subcategories of the currently selected primary category.
- **Tab.** Immediately below the submenu bar, at the top of the menu active window, are one or more tabs, further subdividing the currently selected subcategory if necessary.
- **Option arrow.** To the right of the tabs on some menus are one or more blue dots with an arrow in the center. Clicking an option arrow brings up either a popup window or an advanced option menu.



**Tip:** In the instructions in this guide, we may refer to a menu using the notation primary | subcategory, such as Network Configuration | WAN Settings. In this example, Network is the selected primary category (in the main menu) and WAN Settings is the selected subcategory (in the submenu).

You can now proceed to the first configuration task, configuring the VPN firewall’s Internet connections.

## Configuring your Internet Connection

You can configure both broadband ISP settings and dial-up ISP settings from the WAN Settings submenu.

## Broadband ISP WAN Port Settings

To automatically configure the broadband ISP connection:

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

The screenshot shows the 'Broadband ISP Settings' configuration page. The top navigation bar includes 'Network Configuration', 'Security', 'VPN', 'Users', 'Administration', 'Monitoring', 'Web Support', and 'Logout'. The main menu shows 'WAN Settings', 'Dynamic DNS', 'LAN Settings', and 'Routing'. The sub-menu is 'Broadband ISP Settings', with 'Dial-up ISP Settings' and 'WAN Mode' also visible. The 'Advanced' and 'Broadband Status' buttons are in the top right. The 'ISP Login' section has a 'Does Your Internet Connection Require a Login?' question with 'Yes' and 'No' radio buttons, and fields for 'Login: admin' and 'Password'. The 'ISP Type' section asks 'Which type of Internet connection do you use?' with 'Austria (PPTP)' and 'Other (PPPoE)' radio buttons. It includes fields for 'Account Name', 'Domain Name', 'Idle Timeout' (radio buttons for 'Keep Connected' and 'Idle Time: 5 Minutes'), 'Connection Reset', 'Disconnect Time' (0 HH 0 MM), 'Delay: 0 Sec', 'My IP Address' (0.0.0.0), and 'Server IP Address'. The 'Internet (IP) Address' section has radio buttons for 'Get Dynamically from ISP' and 'Use Static IP Address', with fields for 'IP Address', 'IP Subnet Mask', and 'Gateway IP Address'. The 'Domain Name Server (DNS) Servers' section has radio buttons for 'Get Automatically from ISP' and 'Use These DNS Servers', with fields for 'Primary DNS Server' and 'Secondary DNS Server' (0.0.0.0). At the bottom, there are four buttons: 'Apply', 'Reset', 'Test', and 'Auto Detect'. An arrow points to the 'Auto Detect' button.

Figure 2-2

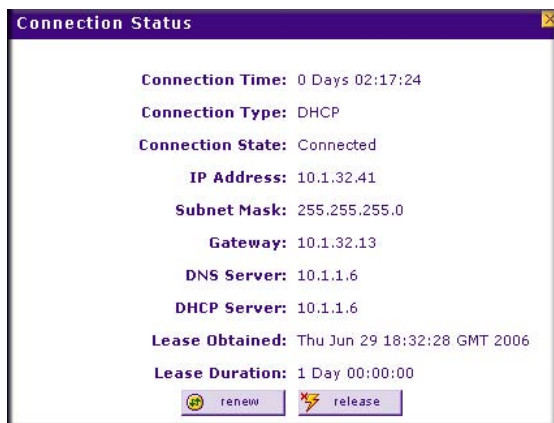
2. Click **Auto Detect** at the bottom of the screen to automatically detect the type of Internet connection provided by your ISP. Auto Detect will probe for different connection methods and suggest one that your ISP will most likely support.

When Auto Detect successfully detects an active Internet service, it reports which connection type it discovered. The options are described in the [Table 2-1](#).

**Table 2-1. Internet connection methods**

Connection Method	Data Required
PPPoE	Login (Requires username and password).
PPTP	Login (Requires username and password, local IP address, and PPTP server IP address).
DHCP (Dynamic IP)	No data is required.
Fixed IP	IP address and related data are supplied by your ISP.

3. Click **Broadband Status** at the top right of the screen to verify your broadband connection status. Click **connect** if a connection is not yet established.



**Figure 2-3**

If Auto Detect does not find a connection, you will be prompted to check the physical connection between your VPN firewall and the DSL line or to check your VPN firewall's MAC address (see [“Configuring Advanced WAN Options \(Optional\)”](#) on page 2-16).

4. As an optional step, set up the traffic meter for the broadband connection (see [“Configuring the WAN Mode”](#) on page 2-11).



**Note:** At this point in the configuration process, you are now connected to the Internet through the broadband Ethernet WAN. As an option, you can continue with the configuration of the dial-up ISP serial WAN interface.

## Dial-up ISP Serial WAN port Settings

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

To configure the dial-up ISP connection:

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

The screenshot shows the 'Dial-up ISP Settings' configuration page. The navigation bar at the top includes 'Network Configuration', 'Security', 'VPN', 'Users', 'Administration', 'Monitoring', 'Web Support', and 'Logout'. Below this, the 'WAN Settings' menu is expanded to show 'Dynamic DNS', 'LAN Settings', and 'Routing'. The 'Dial-up ISP Settings' tab is selected, with 'Broadband ISP Settings' and 'WAN Mode' also visible. The page is divided into several sections:

- Dial-up Account:** Fields for 'Account / User Name' (admin), 'Password' (masked), 'Telephone', and 'Alternative Telephone'.
- Dial-up Connection Status:** Options for 'Specify Connect and Disconnect Method'. 'Connect automatically, disconnect after idle for 0 min.' is unselected, while 'Connect and disconnect manually.' is selected. A 'Dialup Timeout Value' of 60 seconds is entered.
- Internet (IP) Address (Current IP Address):** Options for 'Get Dynamically from ISP' (selected) and 'Use Static IP Address'. 'Get Automatically From ISP' is also selected, while 'Use These DNS Servers' is unselected. Fields for IP Address, Primary DNS Server, and Secondary DNS Server are present.
- Modem Type:** 'Serial Line Speed' is set to 115200. 'Modem Type' is set to 'U.S. Robotics 56K FAX EXT PnP'. Under 'For User Defined Modem', 'Initial String' is 'AT&F', 'Dial-up Type' is 'Tone' (selected), and 'Other - use Dial String' is empty.

'Apply' and 'Reset' buttons are located at the bottom of the form.

Figure 2-4

3. In the **Dial-up Account** section of the screen, enter the following settings:
  - **Account/User name.** The account name or the user name provided by your ISP. This name will be used to log in to the ISP server.
  - **Password.** The account password for the dial-up ISP.
  - **Telephone.** The telephone number or access number to dial for connectivity. Enter the number using the format described in your modem's user manual.
  - **Alternative Telephone.** An alternative number that will be dialed if the first number is not available. (This is an option).
4. In the **Dial-up Connection Status** section of the screen, specify the method to use for your dial-up connection. The VPN firewall can automatically dial to the ISP when a connection is needed or can be configured to wait for manual intervention. Configure one of the following options:
  - Check the **Connect automatically disconnect after idle for \_\_\_ min.** radio box for the modem to connect automatically. Specify the idle minute time. The VPN firewall will connect whenever an outbound connection request is made from a computer on the LAN. The connection will be terminated if there is no data transfer during the specified time interval in the Dialup Timeout Value field (the default is 60 seconds).
  - Check the **Connect and disconnect manually** radio box to disable auto dialing and allow manual control over connecting via dial-up. To connect manually, click the **Dial-Up Status** link at the top and then click **Connect**. The connection will be terminated if there is no data transfer during the specified time interval in the Dialup Timeout Value field (the default is 60 seconds).
5. In the **Internet (IP Address)** section of the screen, select the IP address and DNS servers.





**Note:** Dial-up ISPs usually assign the IP address automatically when connecting.

- Select the IP address by selecting one of the following radio boxes:
  - **Get Dynamically from ISP.** Enables the VPN firewall to accept the IP address that is dynamically assigned by the ISP. This is the default setting.
  - **Use Static IP Address.** Requires the VPN firewall to function with the static IP address that was assigned by the ISP. Enter the IP address in the IP Address field.

- Select the DNS servers by selecting one of the following radio boxes:
    - **Get Automatically From ISP.** Enables the VPN firewall to accept the DNS servers that are dynamically assigned by the ISP. This is the default setting.
    - **Use These DNS Servers.** Requires the VPN firewall to function with the static DNS servers that were assigned by the ISP. Enter the IP addresses of the DNS servers in the Primary DNS Server and Secondary DNS Server fields. A secondary DNS server is optional.
6. Enter any modem-specific parameters to tune the VPN firewall for different modems:
- **Serial Line Speed.** Select the baud rate with which the serial port of the VPN firewall and the modem connect. Available speeds range from 4.8Kbps to 460.8Kbps.
  - **Modem Type.** If your modem type is listed in the pull-down menu, select it. For most 56Kbps modems, the U.S. Robotics 56K FAX EXT PnP selection should work. If this does not work, select **User Defined Modem** and enter the initial string for your modem. The initial string is usually defined in the modem’s user manual.
  - **Dial-up Type.** Select one of the following options:
    - Check the **Tone** radio box if your phone line supports touch tone dialing.
    - Select the **Pulse radio box** for pulse mode dialing.
    - Select the **Other – use Dial String** radio box to configure additional options such as auto-answer. Consult your modem manual for dial strings.
7. Click **Apply** to save your settings.

As an optional step, set up the traffic meter for the dial-up connection (see [“Configuring the WAN Mode” on page 2-11](#)).

	<b>Note:</b> The response time of your serial port Internet connection will be slower than a broadband Internet connection.
---	---

	<b>Tip:</b> If you experience connectivity problems with the dial-up ISP, try a different baud rate setting and ensure that the modem parameters you selected match the modem connected to the VPN firewall.
---	--



## Manually Configuring Your Broadband Internet Connection

If you know your broadband 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, and so on, before you begin. Unless your ISP automatically assigns your configuration automatically via DHCP, you will need the configuration parameters from your ISP.

To automatically configure the broadband ISP connection:

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

The screenshot shows the 'Broadband ISP Settings' page in a web browser. The page has a navigation bar at the top with links for Network Configuration, Security, VPN, Users, Administration, Monitoring, Web Support, and Logout. Below the navigation bar, there are sub-menus for WAN Settings, Dynamic DNS, LAN Settings, and Routing. The main content area is divided into several sections:

- ISP Login:** A section titled 'Does Your Internet Connection Require a Login?' with radio buttons for 'Yes' (selected) and 'No'. It includes fields for 'Login:' (containing 'admin') and 'Password:' (masked with dots).
- ISP Type:** A section titled 'Which type of ISP connection do you use?' with radio buttons for 'Austria (PPTP)' and 'Other (PPPoE)' (selected). It includes fields for 'Account Name:', 'Domain Name:', 'Idle Timeout:' (radio buttons for 'Keep Connected' and 'Idle Time: 5 Minutes'), 'Connection Reset:' (checked), 'Disconnect Time:' (0 HH 0 MM), 'Delay:' (0 Sec), 'My IP Address:' (0.0.0.0), and 'Server IP Address:'.
- Internet (IP) Address (Current IP Address):** A section with radio buttons for 'Get Dynamically from ISP' (unchecked) and 'Use Static IP Address' (selected). It includes checkboxes for 'Client Identifier' and 'Vendor Class Identifier'. It also has fields for 'IP Address:', 'IP Subnet Mask:', and 'Gateway IP Address:'.
- Domain Name Server (DNS) Servers:** A section with radio buttons for 'Get Automatically from ISP' (unchecked) and 'Use These DNS Servers' (selected). It includes fields for 'Primary DNS Server:' and 'Secondary DNS Server:'.

At the bottom of the page, there are four buttons: 'Apply', 'Reset', 'Test', and 'Auto Detect'.

Figure 2-5

2. **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**.
3. **What type of IPS connection do you use?** If your connection is PPTP or PPPoE, then you must log in (select the **Yes** radio box in the previous step). 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 in the previous step and skip this section. For example:
  - **Austria (PPTP)**. If your ISP uses PPTP for login, select this radio box. 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 Ethernet, 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.

4. 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.
  - **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.

5. If your ISP has not assigned any Domain Name Servers (DNS) addresses, select the **Get dynamically from ISP** radio box. If your ISP has assigned DNS addresses, select the **Use these DNS Servers** radio box. Ensure that you 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](http://www.google.com), [www.netgear.com](http://www.netgear.com), etc. to Internet addresses called IP addresses. Incorrect settings here will result in connectivity problems.

6. Click **Apply** to save the settings or click **Cancel** to revert to the previous settings.
7. 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 check on the connection status, click on the **Broadband Status** link.

## Configuring the WAN Mode

The WAN Mode screen allows you to configure how your VPN firewall uses your external Internet connections (for example, your WAN port or dial-up modem connections), and whether or not the connection rolls over to a secondary link when there is a failure on the primary link.

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

NAT is the default setting. Select NAT if your ISP has assigned only one IP address to you. The computers that connect through the VPN firewall must then be assigned IP addresses from a private subnet (for example: 192.168.1.0).

- **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 the VPN firewall.



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

To configure the WAN mode:

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

The screenshot shows the WAN Mode configuration page. At the top, there is a navigation bar with links: Network Configuration, Security, VPN, Users, Administration, Monitoring, Web Support, and Logout. Below this is a breadcrumb trail: WAN Settings :: Dynamic DNS :: LAN Settings :: Routing ::. The main content area has three tabs: Broadband ISP Settings, Dial-up ISP Settings, and WAN Mode (which is selected). The WAN Mode section is divided into three panels. The top panel, titled 'NAT (Network Address Translation)', contains the question 'Use NAT or Classical Routing between WAN & LAN interfaces?' with two radio buttons: 'NAT' (selected) and 'Classical Routing'. The bottom-left panel, titled 'Port Mode', has two radio buttons: 'Primary Broadband with Dialup as backup' and 'Use only single WAN port: Broadband' (selected). The bottom-right panel, titled 'WAN Failure Detection Method', has three radio buttons: 'DNS lookup using WAN DNS Servers' (selected), 'DNS lookup using this DNS Server:' (with IP address fields 0.0.0.0), and 'Ping this IP address:' (with IP address fields 0.0.0.0). Below these are fields for 'Test Period is: 30 Seconds' and 'Failover after: 4 Failures'. At the bottom of the page are 'Apply' and 'Reset' buttons.

Figure 2-6

2. Check either the **NAT** or **Classical Routing** radio box. NAT is the default.

3. In the **Port Mode** section of the screen, select the port mode settings to configure your VPN firewall to use only one WAN port (either the broadband port or the dial-up port) or to select the dial-up port as a backup.
  - If you are connected to only one ISP, then select the **Use only single WAN port** radio box and select the WAN port that is connected to your ISP from the pull-down menu.
  - If you have both ISP links connected for Internet connectivity, check the **Primary Broadband with Dialup as backup** for auto-rollover.
4. In the **WAN Failure Detection Method** section of the screen, configure the failure detection method to notify the VPN firewall of a link failure if you are using dial-up as a backup to engage auto-rollover. The VPN firewall checks the connection of the primary link at regular intervals to detect its status. Check the radio box of one of the following methods to detect link failure:
  - Select **DNS lookup using configured DNS Servers** to detect failure of the Broadband link, using the DNS servers configured on the Broadband ISP Settings screen.
  - Select **DNS lookup using this DNS Server** and enter the IP address of the DNS server to specify a DNS server for detecting WAN failure
  - Select **Ping this IP address** and enter an IP address to detect WAN failure by pinging to an IP address. Ensure that this destination host is reliable.

If a failure is detected on the primary broadband connection, the secondary dial-up connection connects to the Internet. When the primary connection is detected as back online, the secondary dial-up connection disconnects.

Specify the test period and failover number:

- **Test Period.** Enter the test period in seconds, which specifies how often the VPN firewall should run the configured detection method. The default is 30 seconds.
  - **Failover after.** Enter the number of failures that should occur before the VPN firewall rolls-over to the dial-up port. The default is 4.
5. Enter **Apply** to save your settings or **Cancel** to revert to the previous settings.

## Configuring Dynamic DNS (Optional)

---



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

Dynamic DNS (DDNS) is an Internet service that allows routers with varying public IP addresses to be located using Internet domain names. To use DDNS, you must setup an account with a DDNS provider such as DynDNS.org, TZO.com, Oray.net, or 3322.org. (Links to DynDNS, TZO, Oray, and 3322 are provided for your convenience on the Dynamic DNS Configuration screen.)

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 (fully qualified domain name) to your frequently-changing IP address.

For rollover mode, you will need an FQDN to implement features such as exposed hosts and virtual private networks, regardless of whether you have a fixed or dynamic IP address.

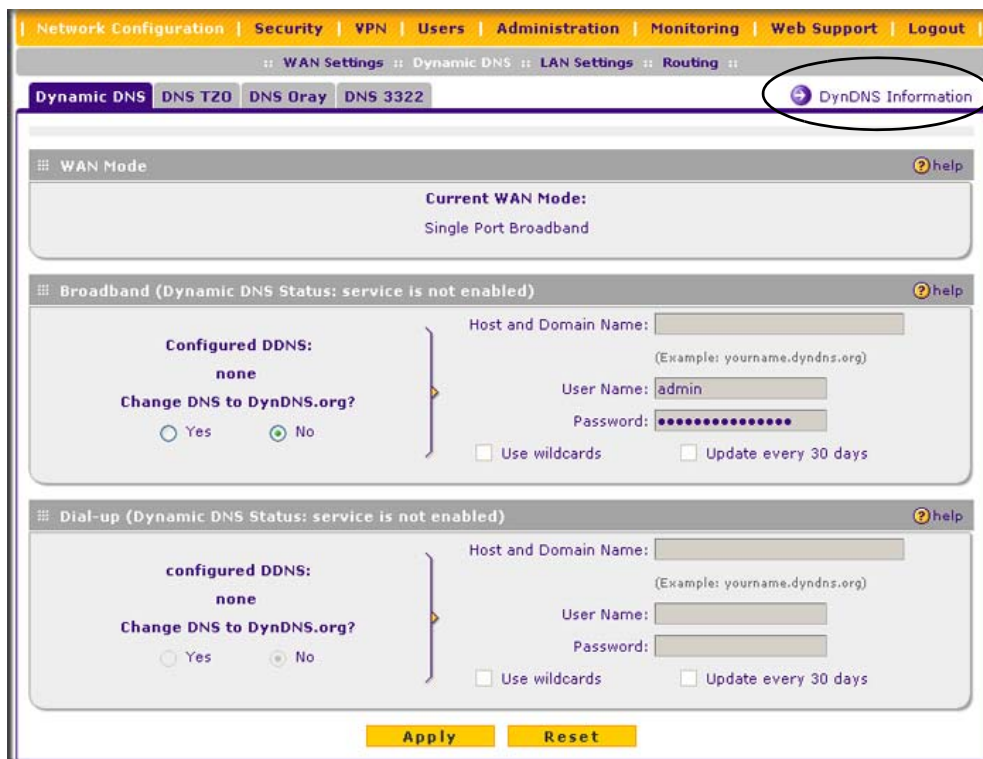
After you have configured your account information in the VPN firewall, whenever your ISP-assigned IP address changes, your VPN firewall will automatically contact your dynamic DNS service provider, log in to your account, and register your new IP address.



**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 a dynamic DNS address:

1. Select **Network Configuration** from the main menu and **Dynamic DNS** from the submenu. The Dynamic DNS screen displays (see [Figure 2-7 on page 2-15](#)).



**Figure 2-7**

A tab is provided for each supported DNS service provider.

The **WAN Mode** section on the screen displays the currently configured WAN Mode: Single Port Broadband, Single Port Dial-up, or Auto Rollover with Primary Broadband.

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

2. Select the Dynamic DNS Service radio box you want to enable. The fields corresponding to the selection you have selected will be highlighted. Each DNS service provider requires its own parameters.
3. Access the website of one of the DDNS service providers and set up an account. A link to each DDNS provider is near the top right of the window opposite to the DDNS service provider tabs. The link is encircled with a line in [Figure 2-7](#).

4. After setting up your account, return to the Dynamic DNS Configuration screen and fill in the required fields for the DDNS service that 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 or click **Cancel** to revert to the previous settings.

## Configuring Advanced WAN Options (Optional)

To configure the broadband advanced WAN options:

1. Select **Network Configuration** from the main menu and **Broadband ISP Settings** from the submenu.
2. Click the **Advanced** link. The Broadband Advanced Options screens displays.

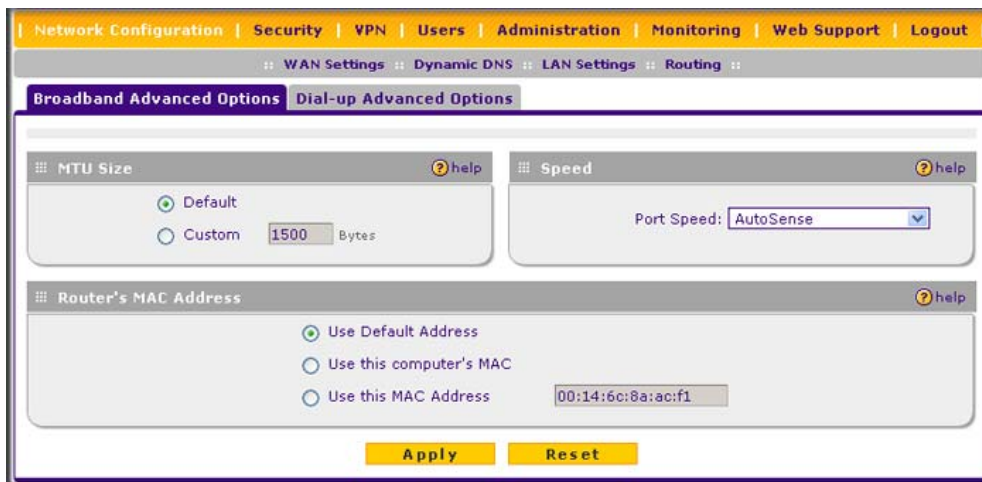


Figure 2-8



3. Edit the default information that you want to change in the following sections of the screen:
  - **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.
  - **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.

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

To configure the dial-up advanced WAN options:

1. Select **Network Configuration** from the main menu and **Dial-up ISP Settings** from the submenu.
2. Click the **Advanced** link. The Dial-up Advanced Options screens displays.
3. If required, change the standard MTU value for the dial-up modem. This is the only settings that you can change on this screen. The standard value for the MTU is 576 bytes, but some ISPs may require that you reduce the MTU. However, this is rarely required, and should not be done unless specifically required by the ISP.
4. Click **Apply** to save your settings.

## Additional WAN Related Configuration

- If you want the ability to manage the VPN firewall remotely, enable remote management at this time (see [“Enabling Remote Management Access” on page 6-14](#)). If you enable remote management, we strongly recommend 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 the WAN, if desired. See [“Enabling the Traffic Meter” on page 6-27](#).

# Chapter 3

## LAN Configuration

This chapter describes how to configure the LAN settings, LAN groups, and routing features of your ProSafe VPN Firewall 50 FVS338, including the following sections:

- [“Choosing the VPN Firewall DHCP Options”](#) on this page
- [“Configuring the LAN Setup Options”](#) on page 3-2
- [“Managing Groups and Hosts”](#) on page 3-6
- [“Configuring Multi-Home LAN IPs Addresses”](#) on page 3-10
- [“Configuring Static Routes”](#) on page 3-11
- [“Configuring Routing Information Protocol \(RIP\)”](#) on page 3-14

### 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 D, “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 firewall will act as a proxy for all DNS requests and communicate with the ISP's DNS servers (as configured on the Broadband ISP Settings screen and Dial-up ISP Settings screen). All DHCP clients will receive the primary/secondary DNS IP addresses along with the IP address where the DNS proxy is running, which is the the devices'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 FVS338 as a DHCP server but rather as a DHCP relay agent for a DHCP server somewhere else on your network.

To configure the LAN options:

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

The screenshot displays the LAN Setup configuration page. At the top, there is a navigation bar with tabs for Network Configuration, Security, VPN, Users, Administration, Monitoring, Web Support, and Logout. Below this, there are sub-tabs for LAN Setup, LAN Groups, and LAN Multi-homing. The main content area is divided into three sections:

- LAN TCP/IP Setup:** Contains fields for IP Address (192.168.4.1) and Subnet Mask (255.255.255.0).
- DHCP:** Includes radio buttons for 'Disable DHCP Server' and 'Enable DHCP Server' (selected). It also has a checkbox for 'Enable LDAP information'. Fields include Domain Name (netgear.com), Starting IP Address (192.168.4.2), Ending IP Address (192.168.4.100), Primary DNS Server, Secondary DNS Server, WINS Server, Lease Time (24 Hours), and Relay Gateway.
- Advanced Settings:** Contains checkboxes for 'Enable DNS Proxy' and 'Enable ARP Broadcast', both of which are checked.

At the bottom of the form, there are 'Apply' and 'Reset' buttons.

**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.
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 "network" as the LAN TCP/IP address of the VPN firewall (the IP address 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 radio 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 [“Inbound Rules Examples”](#) on page 4-11).

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.

- **Enable ARP Broadcast.** If ARP broadcast is enabled (which is the default setting), the Address Resolution Protocol (ARP) is broadcast on the LAN so that IP addresses can be mapped to physical addresses (that is, MAC addresses).

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



**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

---

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:

- **Using the DHCP Server.** 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

The Network Database offers a number of advantages:

- Generally, you do not need to enter either IP address or MAC addresses. Instead, you can just select the desired PC or device.
- No need to reserve an IP address for a PC in the DHCP Server. All IP address assignments made by the DHCP Server will be maintained until the PC or device is removed from the database, either by expiry (inactive for a long time) or by you.
- No need to use a fixed IP address on PCs. Because the address allocated by the DHCP Server will never change, you don't 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 4-26).



- If necessary, you can also create firewall rules to apply to a single PC (see “[Configuring Source MAC Filtering](#)” on page 4-29). 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.

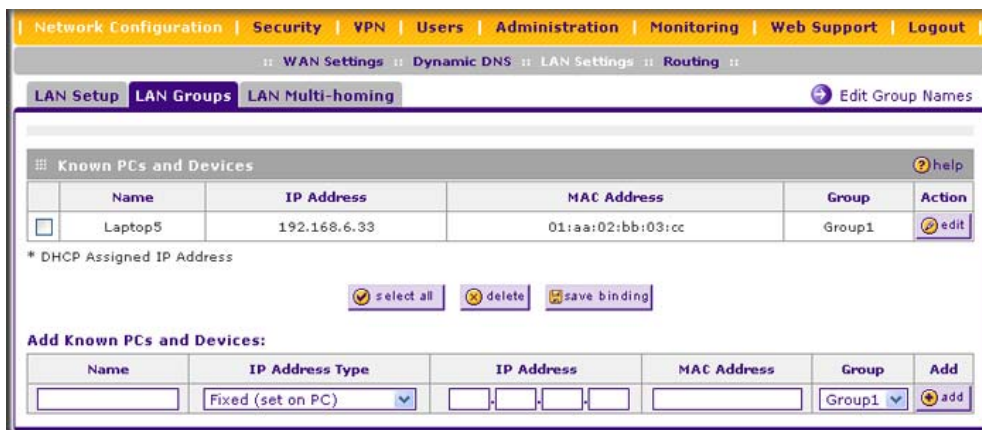


Figure 3-2

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 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, click **edit**.
- **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 itself.
    - 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](#)).

	<b>Note:</b> 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.
---	--

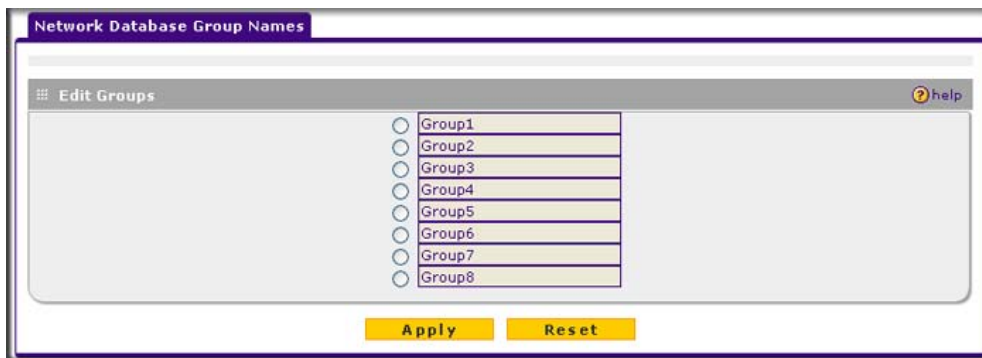
- **IP Address.** The IP address that this computer or device is assigned. If the IP Address Type is **Reserved (DHCP Client)**, the VPN firewall will reserve the IP address for the associated MAC address.
  - **MAC Address.** The MAC address of the computer’s network interface. The MAC address format 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](#).



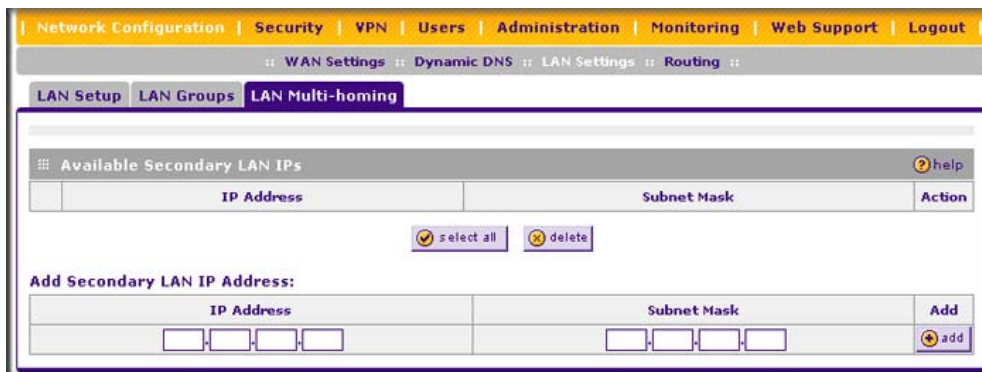
**Note:** The reserved address will not be assigned until the next time the PC contacts the VPN firewall's DHCP server. Reboot the PC or access its IP configuration and force a DHCP release and renew.

## Configuring Multi-Home LAN IPs Addresses

If you have computers using different IP networks in the LAN, (for example., 172.16.2.0, 10.0.0.0), then you can add aliases to the LAN port and give 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/edit.** Click 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, and any other subnet attached to this VPN firewall.

Example:

Broadband port IP address: 10.0.0.1 with subnet 255.0.0.0

Dial-up port IP address: 20.0.0.1 with subnet 255.0.0.0

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 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 must configure static routes only for unusual cases such as multiple firewalls or multiple IP subnets located on your network.

To add or edit a static route:

1. Select **Network Configuration** from the main menu and **Routing** from the submenu. The Routing screen will display (see [Figure 3-5 on page 3-12](#)).

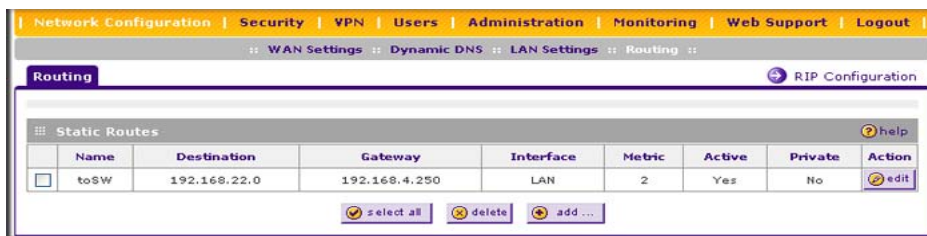


Figure 3-5

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

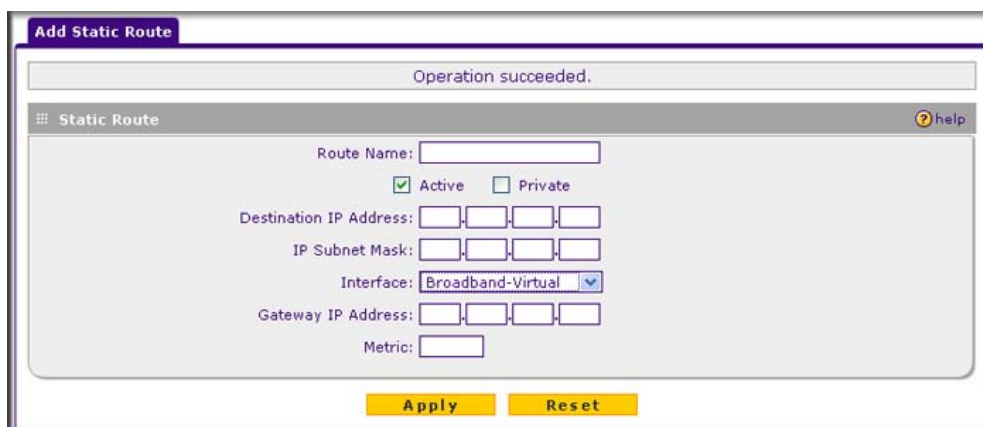


Figure 3-6

- Enter a name for the static route in the Route Name field (for identification purpose only).
- Determine whether the route is:
  - Active** or **Inactive**. A route can be added to the **Static Routes** table and made inactive, if not needed. This allows routes to be used as needed without deleting the entry and re-adding it. An inactive route is not broadcast if RIP is enabled. Select the **Active** radio box to make this route effective.
  - Private**: Determine whether the route can be shared with other routers when RIP is enabled. Select the **Private** radio box if you want to limit access to the LAN only. The route will not be shared in a RIP broadcast or multicast.
- Destination IP Address**. Enter the IP address of the route's final destination.
- IP Subnet Mask**. Enter the subnet mask of the route's final destination. If the destination is a single host, enter **255.255.255.255**.

7. **Interface.** From the pull-down menu, select the physical network interface (Broadband-Virtual, Broadband-Ethernet, Dialup, or LAN) through which this route is accessible.
8. **Gateway IP Address.** Enter the IP address of the gateway through which the destination host or network can be reached. (This must be a device on the same LAN segment as the VPN firewall.)
9. **Metric.** Enter the metric value that determines the priority of the route. If multiple routes to the same destination exist, the route with the lowest metric is chosen. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.
10. Click **Apply** to save the static route to the **Static Routes** table.

## Static Route Example

For example, a static route is needed if:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN firewall on your home network for connecting to the company where you are employed. This firewall's address on your LAN is 192.168.1.100.
- Your company's network is 134.177.0.0.

When you first configured your 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 3-5 on page 3-12](#)).
2. Click the **RIP Configuration** link. The RIP Configuration screen will display.

Figure 3-7

3. From the **RIP Direction** pull-down menu, select the direction for the VPN firewall to send and receive RIP packets:
  - **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.
  - **None.** The VPN firewall neither broadcasts its route table nor does it accept any RIP packets from other routers. This effectively disables RIP.
4. Select the **RIP Version** from the pull-down menu:
    - **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 **Apply** to save your settings.



# Chapter 4

## Firewall Protection and Content Filtering

The ProSafe VPN Firewall 50 FVS338 provides you with Web content filtering options such as block sites and keyword blocking. This chapter includes the following sections:

- [“About Firewall Security 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 4-15
- [“Creating Services, QoS Profiles, and Bandwidth Profiles”](#) on page 4-20
- [“Setting a Schedule to Block or Allow Specific Traffic”](#) on page 4-25
- [“Blocking Internet Sites \(Content Filtering\)”](#) on page 4-26
- [“Configuring Source MAC Filtering”](#) on page 4-29
- [“Configuring IP/MAC Address Binding”](#) on page 4-31
- [“Configuring Port Triggering”](#) on page 4-33
- [“E-Mail Notifications of Event Logs and Alerts”](#) on page 4-36
- [“Administrator Tips”](#) on page 4-36

### About Firewall Security 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”](#) 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 the Firewall Rules”](#) on page 4-7
- [“Order of Precedence for Firewall Rules”](#) on page 4-8
- [“Setting the Default Outbound Policy”](#) on page 4-8
- [“Setting the Default Outbound Policy”](#) on page 4-8
- [“Modifying Rules”](#) on page 4-10
- [“Inbound Rules Examples”](#) on page 4-11
- [“Outbound Rules Example: Blocking Instant Messenger”](#) on page 4-14

Firewall rules are used to block or allow specific traffic passing through from one side to the other. You can configure up to 600 rules on the FVS338. Inbound rules (WAN to LAN) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Outbound rules (LAN to WAN) determine what outside resources local users can have access to.

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

User-defined firewall rules for blocking or allowing traffic on the VPN firewall can be applied to inbound or outbound traffic.

### Services-Based Rules

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

- **Inbound Rules (port forwarding).** Inbound traffic is normally blocked by the c 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.

- **Outbound Rules (service blocking).** Outbound traffic is normally allowed unless the VPN firewall is configured to disallow it.
- **Customized Services.** Additional services can be added to the list of services in the factory default list. These added services can then have rules defined for them to either allow or block that traffic (see [“Adding Customized Services” on page 4-20](#)).
- **Quality of Service (QoS).** Each service at its own native priority that impacts its quality of performance and tolerance for jitter or delays. You can change this QoS priority if desired to change the traffic mix through the system (see [“Specifying Quality of Service \(QoS\) Priorities” on page 4-22](#)).

### 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 4-29](#) for yet another way to block outbound traffic from selected PCs that would otherwise be allowed by the VPN firewall.

**Table 4-1. Outbound 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 <a href="#">“Adding Customized Services” on page 4-20</a> ).
Action	Select the desired action for outgoing connections covered by this rule: <ul style="list-style-type: none"> <li>• BLOCK always</li> <li>• BLOCK by schedule, otherwise Allow</li> <li>• ALLOW always</li> <li>• ALLOW by schedule, otherwise Block</li> </ul> <p><b>Note:</b> Any outbound traffic that is not blocked by rules you create will be allowed by the default rule.</p> <p>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.</p>
Select Schedule	Select the desired time schedule (Schedule1, Schedule2, or Schedule3) that will be used by this rule. <ul style="list-style-type: none"> <li>• This pull-down menu gets activated only when “BLOCK by schedule, otherwise Allow” or “ALLOW by schedule, otherwise Block” is selected as Action.</li> <li>• Use the Schedule screen to configure the time schedules (see <a href="#">“Setting a Schedule to Block or Allow Specific Traffic” on page 4-25</a>).</li> </ul>

**Table 4-1. Outbound Rules (continued)**

Item	Description
LAN Users	<p>These settings determine which computers on your network are affected by this rule. Select the desired options:</p> <ul style="list-style-type: none"> <li>• Any – All PCs and devices on your LAN.</li> <li>• Single address - Enter the required address and the rule will be applied to that particular PC.</li> <li>• Address range – If this option is selected, you must enter the start and finish fields.</li> <li>• Groups – Select the Group you wish this rule to apply to. You can use the Network Database screen to assign PCs to Groups. See <a href="#">“Managing Groups and Hosts” on page 3-6</a>.</li> </ul>
WAN Users	<p>These settings determine which Internet locations are covered by the rule, based on their IP address. Select the desired option:</p> <ul style="list-style-type: none"> <li>• Any – All Internet IP address are covered by this rule.</li> <li>• Single address – Enter the required address in the start fields.</li> <li>• Address range – If this option is selected, you must enter the start and finish fields.</li> </ul>
QoS Priority	<p>Specifies the priority of a service which, in turn, determines the quality of that service for the traffic passing through the firewall. By default, the priority shown is that of the selected service. The user can change it accordingly. If the user does not make a selection (leaves it as Normal-Service), then the native priority of the service will be applied to the policy. See <a href="#">“Specifying Quality of Service (QoS) Priorities” on page 4-22</a>.</p>
Log	<p>This determines whether packets covered by this rule are logged. Select the desired action:</p> <ul style="list-style-type: none"> <li>• Always – always log traffic considered by this rule, whether it matches or not. This is useful when debugging your rules.</li> <li>• Never – never log traffic considered by this rule, whether it matches or not.</li> </ul>
Bandwidth Profile	<p>Specifies the name of a bandwidth limiting profile. Using a bandwidth profile, bandwidth consumed by different connections can be limited. If multiple connections correspond to the same firewall rule, they will share the same bandwidth limiting. See <a href="#">“Creating Bandwidth Profiles” on page 4-23</a>.</p>
NAT IP	<p>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.</p>
NAT Single IP Is On (interface)	<p>Specifies to which WAN interface the NAT IP address belongs. All outgoing packets will be routed through the specified WAN interface only.</p>

## 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 and how the PCs will access the server's LAN address impact the inbound rules. For example:

- If your external IP address is assigned dynamically by your ISP (DHCP enabled), the IP address may change periodically as the DHCP lease expires. Consider using 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 local LAN address of the PC. Attempts by local PCs to access the server using the external WAN IP address will fail.



**Note:** See [“Configuring Port Triggering” on page 4-33](#) for yet another way to allow certain types of inbound traffic that would otherwise be blocked by the VPN firewall.

**Table 4-2. Inbound Rules Fields**

Item	Description
Services	Select the desired service or application to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services screen (see <a href="#">“Adding Customized Services” on page 4-20</a> ).
Action	Select the desired action for packets covered by this rule: <ul style="list-style-type: none"> <li>• BLOCK always</li> <li>• BLOCK by schedule, otherwise Allow</li> <li>• ALLOW always</li> <li>• ALLOW by schedule, otherwise Block</li> </ul> <b>Note:</b> 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 (Schedule1, Schedule2, or Schedule3) that will be used by this rule. <ul style="list-style-type: none"> <li>• This pull-down menu gets activated only when “BLOCK by schedule, otherwise Allow” or “ALLOW by schedule, otherwise Block” is selected as Action.</li> <li>• Use the Schedule screen to configure the time schedules.</li> </ul>

**Table 4-2. Inbound Rules Fields**

Item	Description
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.)
Translate to Port Number	Check this box and enter a port number to assign the LAN server to a different service port number. Inbound traffic to the service port will have the destination port number modified to the port number configured here.
WAN Destination IP Address	These settings determine the destination IP address applicable to incoming traffic. This is the public IP address that will map to the internal server; it can either be the address of the broadband or dialup port, or of another public IP address.
LAN Users	<p>These settings determine which computers on your network are affected by this rule. Select the desired options:</p> <ul style="list-style-type: none"> <li>• Any – All PCs and devices on your LAN.</li> <li>• Single address - Enter the required address and the rule will be applied to that particular PC.</li> <li>• Address range – If this option is selected, you must enter the start and finish fields.</li> <li>• Groups – Select the group you wish this rule to apply to. You can use the Network Database screen to assign PCs to groups. See <a href="#">“Managing Groups and Hosts” on page 3-6.</a></li> </ul>
WAN Users	<p>These settings determine which Internet locations are covered by the rule, based on their IP address. Select the desired option:</p> <ul style="list-style-type: none"> <li>• Any – All Internet IP address are covered by this rule.</li> <li>• Single address – Enter the required address in the start fields.</li> <li>• Address range – If this option is selected, you must enter the start and finish fields.</li> </ul>
Log	<p>This determines whether packets covered by this rule are logged. Select the desired action:</p> <ul style="list-style-type: none"> <li>• Always – always log traffic considered by this rule, whether it matches or not. This is useful when debugging your rules.</li> <li>• Never – never log traffic considered by this rule, whether it matches or not.</li> </ul>
Bandwidth Profile	This setting determines 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 (that is, leaves it as None), then the native priority of the service will be applied to the policy. See <a href="#">“Creating Bandwidth Profiles” on page 4-23.</a>





**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 the Firewall Rules

To view the firewall rules, select **Security** from the main menu and **Firewall** from the submenu. The LAN WAN Rules screen will display (Figure 4-1 shows some examples).

Default Outbound Policy:

Operation succeeded.

### Outbound Services

	Service Name	Filter	LAN Users	WAN Users	Priority	Bandwidth Profile	Log	Action
<input type="checkbox"/>	AIM	Block by schedule 2 else allow	ANY	ANY	Normal-Service	NONE	Always	<input type="button" value="up"/> <input type="button" value="down"/> <input type="button" value="edit"/>

enable  disable

### Inbound Services

	Service Name	Filter	LAN Server IP Address	LAN Users	WAN Users	Destination	Bandwidth Profile	Log	Action
<input type="checkbox"/>	HTTP	Allow Always	192.168.0.99		ANY	WAN1	NONE	Never	<input type="button" value="up"/> <input type="button" value="down"/> <input type="button" value="edit"/>
<input type="checkbox"/>	CU-SEEME:UDP	Allow by schedule 1 else block	192.168.0.11		134.177.88.1-134.177.88.254	WAN1	NONE	Never	<input type="button" value="up"/> <input type="button" value="down"/> <input type="button" value="edit"/>
<input type="checkbox"/>	HTTP	Allow Always	192.168.1.75:8080		ANY	10.1.0.5	NONE	Never	<input type="button" value="up"/> <input type="button" value="down"/> <input type="button" value="edit"/>

enable  disable

Figure 4-1

## Order of Precedence for Firewall Rules

As you define new rules, they are added to the tables on the LAN WAN Rules screen, as shown in [Figure 4-1 on page 4-7](#)

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

## Setting the Default Outbound Policy

The default outbound policy is to allow all traffic from and to the Internet to pass through. Firewall rules can then be applied to block specific types of traffic from either going out from the LAN to the Internet (Outbound) or coming in from the Internet to the LAN (Inbound). The default policy can be changed to block all outbound traffic and enable only specific services to pass through the 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 (see [Figure 4-1 on page 4-7](#)).
2. Change the **Default Outbound Policy** by selecting **Block Always** from the pull-down menu.
3. Click **Apply**.

## Creating a LAN WAN Outbound Services Rule

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

You can also tailor these rules to your specific needs (see [“Administrator Tips” on page 4-36](#)).



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

To create a new 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.

The screenshot shows the 'Add LAN WAN Outbound Service' configuration window. At the top, a message box says 'Operation succeeded.' Below that, the window title is 'Outbound Service' with a help icon. The configuration fields are as follows:

- Service: ANY
- Action: BLOCK always
- Select Schedule: Schedule 1
- LAN Users: Any
- WAN Users: Any
- QoS Priority: Normal-Service
- Log: Never
- Bandwidth Profile: NONE
- NAT IP: WAN Interface Address
- NAT Single IP Is On: Broadband
- Start and Finish time fields for LAN and WAN users.

At the bottom, there are 'Apply' and 'Reset' buttons.

Figure 4-2

2. Configure the settings as explained in [Table 4-1](#) on page 4-3.
3. Click **Apply** to save your changes and reset the fields on this screen. The new rule will be listed on the **Outbound Services** table on the LAN WAN Rules screen.

## Creating a LAN WAN Inbound Services Rule

The **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 firewall. Only enable those ports that are necessary for your network.

To create a new inbound service rule in the LAN WAN Rules screen:

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

The screenshot shows the 'Add LAN WAN Inbound Service' configuration window. At the top, a message bar indicates 'Operation succeeded.' Below this is the 'Inbound Service' configuration form. The form includes the following fields and options:

- Service: ANY
- Action: BLOCK always
- Select Schedule: Schedule 1
- Send to LAN Server: Single Address
- Translate to Port Number:
- WAN Destination IP Address: Broadband
- LAN Users: Any
- WAN Users: Any
- Log: Never
- Bandwidth Profile: NONE

There are also Start and Finish time pickers for each of the LAN and WAN user groups. At the bottom of the form are 'Apply' and 'Reset' buttons.

Figure 4-3

2. Configure the settings as explained in [Table 4-2 on page 4-5](#).
3. Click **Apply** to save your settings. The new rule will be added to the **Inbound Services** table on the LAN WAN Rules screen.

## Modifying Rules

To make changes to an existing outbound or inbound service rule on the the LAN WAN 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 the Edit LAN WAN Outbound Service screen (identical to [Figure 4-2 on page 4-9](#)) or Edit LAN WAN Inbound Service screen (identical to [Figure 4-3 on page 4-10](#)) 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:

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.

## 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. In the example shown in [Figure 4-4](#), unrestricted access is provided from the Internet to the local Web server at LAN IP address 192.168.1.99.

The screenshot shows the 'Add LAN WAN Inbound Service' configuration window. The window title is 'Add LAN WAN Inbound Service' and it shows a message 'Operation succeeded.' at the top. The main area is titled 'Inbound Service' and contains the following settings:

- Service: HTTP
- Action: ALLOW always
- Select Schedule: Schedule 1
- Send to LAN Server: Single Address
- WAN Destination IP Address: Broadband
- LAN Users: Any
- WAN Users: Any
- Log: Never
- Bandwidth Profile: NONE

There are also fields for Start and Finish times for the rule, with the first Start field set to 192.168.0.99. At the bottom, there are 'Apply' and 'Reset' buttons.

Figure 4-4

## 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. In the example shown in [Figure 4-5](#), CU-SeeMe connections are allowed only from a specified range of external IP addresses. Connections are blocked during the period specified by Schedule 1.

The screenshot shows the configuration for an inbound service. The service is named 'CU-SEEME:UDP' and the action is 'ALLOW by schedule, otherwise block'. The schedule is set to 'Schedule 1'. The rule is configured to send traffic to a single LAN server. The WAN destination IP address is set to 'Broadband'. The LAN users are set to 'Any'. The WAN users are set to an 'Address Range'. The rule is configured to log 'Never' and has no bandwidth profile. Two IP address ranges are defined: the first starts at 192.168.0.11 and the second starts at 134.177.88.1 and finishes at 134.177.88.254.

Figure 4-5

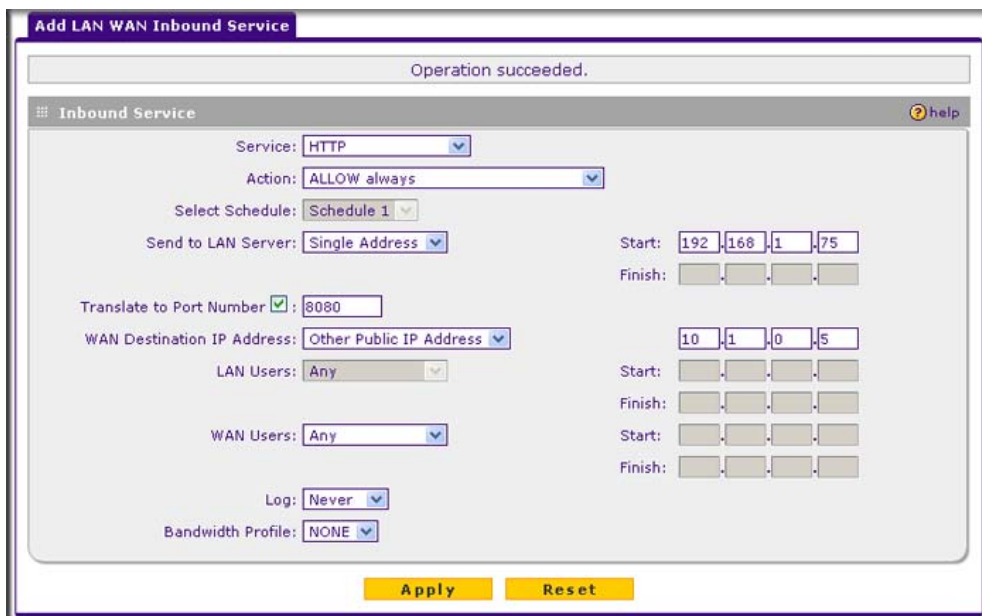
## LAN WAN Inbound Rule: Setting Up One-to-One NAT Mapping

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. 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 4-6 on page 4-13](#), 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 192.168.0.1). We also instruct the VPN firewall to translate the incoming HTTP port number (port 80) to a different port number (port 8080).

The following addressing scheme is used in this example:

- VPN firewall:
  - WAN primary public IP address: 10.1.0.1
  - WAN 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: 192.168.1.75
  - Port number for Web service: 8080



**Figure 4-6**

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 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 as this host:

1. Create an inbound rule that allows all protocols.

2. Place the rule below all other inbound rules.

Figure 4-7 shows the bottom part of the LAN WAN Rules screen with an example of the **Inbound Services** table.

➔

**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.

Inbound Services								help			
	!	Service Name	Filter	LAN Server IP Address	LAN Users	WAN Users	Destination	Log	Action		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	HTTP	Allow Always	192.168.1.2		ANY	19.1.9.52	Never	<input type="radio"/> up	<input type="radio"/> down	<input type="radio"/> edit
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ANY	Allow Always	192.168.0.15		ANY	WAN1	Never	<input type="radio"/> up	<input type="radio"/> down	<input type="radio"/> edit

select all  
  delete  
  enable  
  disable  
  add ...

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

Figure 4-7

## Outbound Rules Example: Blocking Instant Messenger

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

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 on the Schedule screen. You can also have the VPN firewall log any attempt to use Instant Messenger during that blocked period. See [Figure 4-8 on page 4-15](#).



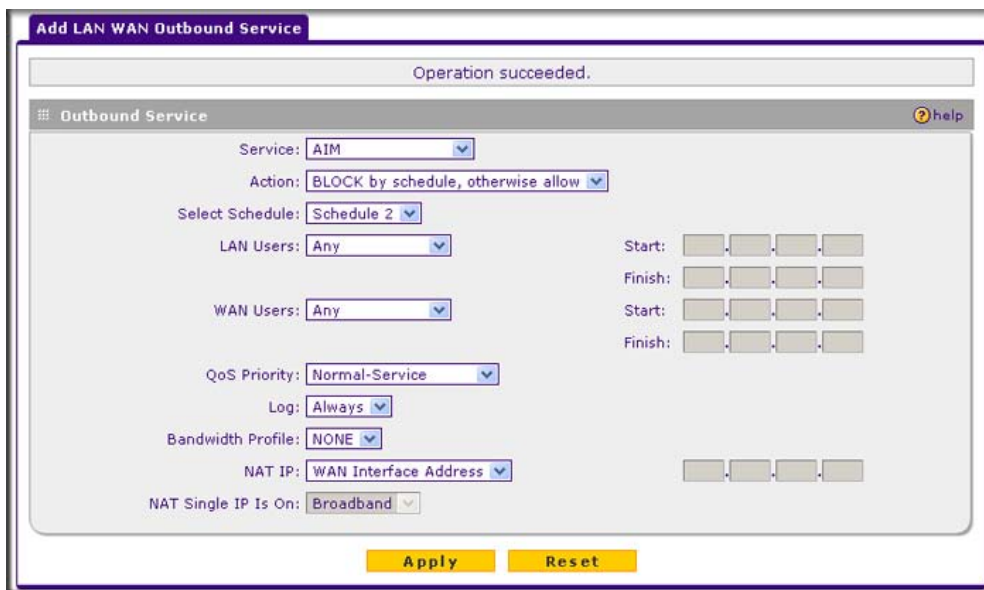


Figure 4-8

## 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 LAN and WAN networks.

To enable the appropriate Attack Checks for your environment:

1. Select **Security** from the main menu and **Firewall** from the submenu. The LAN WAN Rules screen displays.
2. Click the **Attack Checks** tab. The Attack Checks screen will display (see [Figure 4-9 on page 4-16](#)).

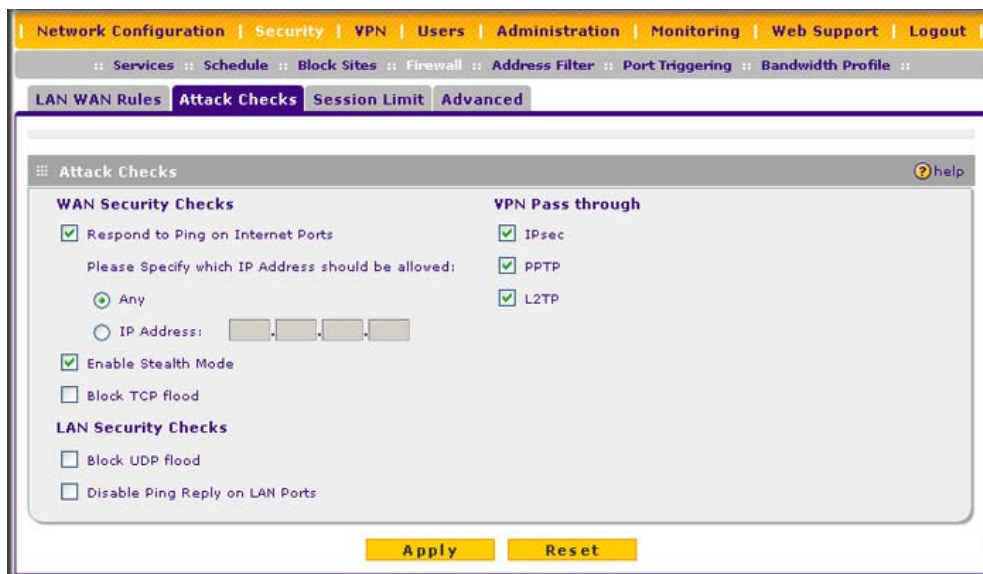


Figure 4-9

3. Check the boxes for the attack checks that 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.** If stealth mode, the VPN firewall will not respond to port scans from the WAN, thus making it less susceptible to discovery and attacks.
  - **Block TCP Flood.** A SYN flood is a form of denial of service attack in which an attacker sends a succession of SYN requests to a target system. When the system responds, the attacker does not complete the connections, thus leaving the connection half-open and flooding the server with SYN messages. No legitimate connections can then be made.

When blocking is enabled,, the VPN firewall will drop all invalid TCP packets and will be protected from a SYN flood attack.

- **LAN Security Checks.**

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

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

If enabled, the 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 is in NAT mode, all packets going to the remote VPN gateway are first filtered through NAT and then encrypted per the VPN policy.

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

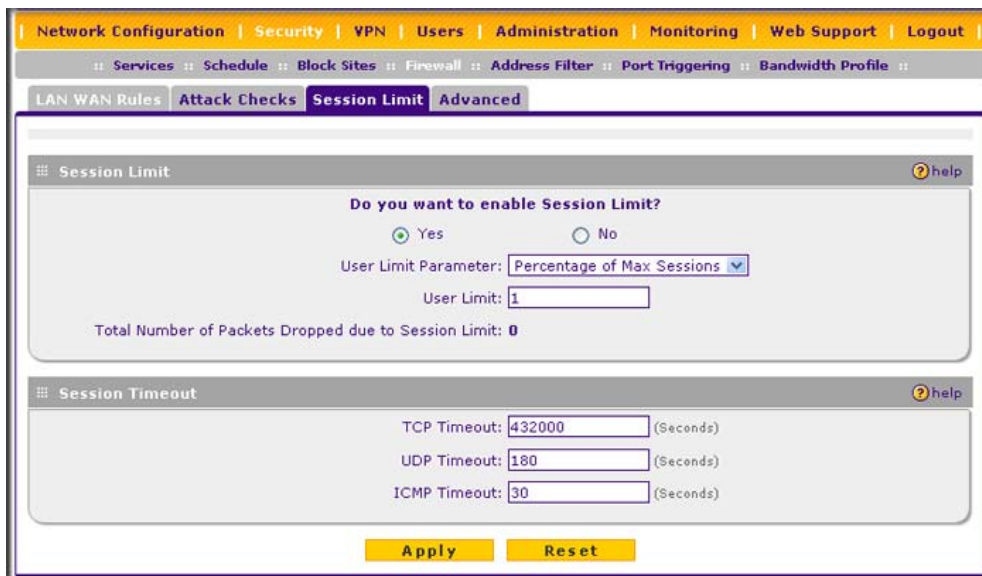
IPSec, PPTP, and L2TP represent different types of VPN tunnels that can pass through the VPN firewall. To allow the VPN traffic to pass through without filtering, enable those options for the type of tunnel(s) that will pass through the VPN firewall. By default, IPSec, PPTP, and L2TP are selected.

## Configuring Session Limits

To prevent one user or group from using excessive system resources, you can limit the total number of IP sessions allowed through the VPN firewall for an individual or group. You can specify the maximum number of sessions by either a percentage of maximum sessions or an absolute number of maximum sessions. Session limiting is disabled by default.

To configure session limits:

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




**Figure 4-10**

To enable session limits:

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

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**, the limit is the maximum number of sessions allowed from a single source machine as a percentage of the total connection capacity. (Session Limit is a machine-based value.) Otherwise, when the User Limit Parameter is set to **Number of Sessions**, the limit is an absolute value.

	<b>Note:</b> 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.

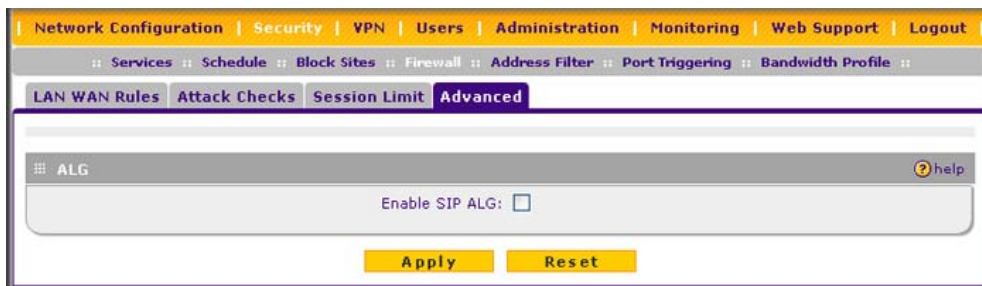


Figure 4-11

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 4-20](#).
- **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 4-22](#).
- **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 4-23](#).



**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 4-25](#).

### Adding Customized Services

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

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

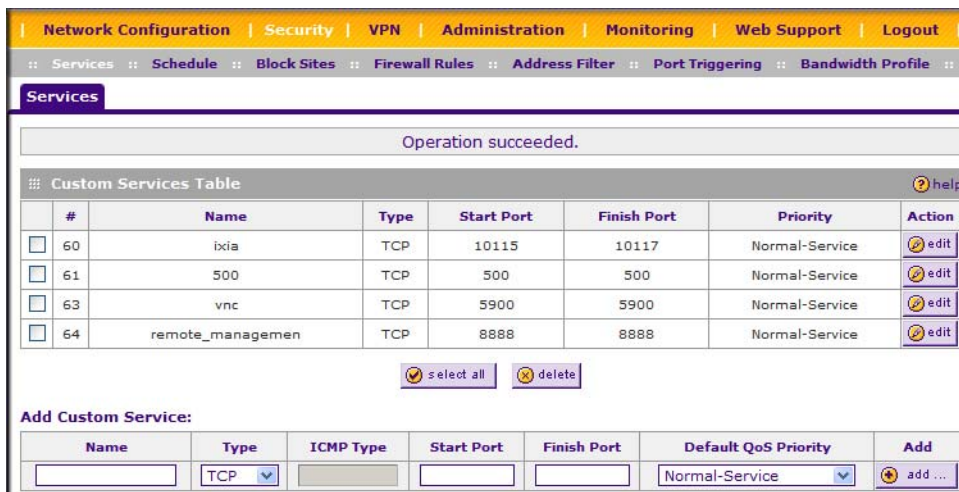
The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, “Assigned Internet Protocol Numbers.” Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application.

Although the 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 4-12 on page 4-21](#).

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 service:

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



**Figure 4-12**

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.
2. Modify the parameters you wish to change.
3. Click **Apply** to confirm your changes. The modified service will display in the **Custom Services Table**.

## Specifying Quality of Service (QoS) Priorities

The Quality of Service (QoS) Priorities setting determines the priority of a service, which in turn, determines the quality of that service for the traffic passing through the firewall. The user can change this priority:

- On the Services screen in the **Customer Services Table** for customized services (see [Figure 4-12 on page 4-21](#)).
- On the LAN WAN Outbound Services screen (see [Figure 4-8 on page 4-15](#)).

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

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

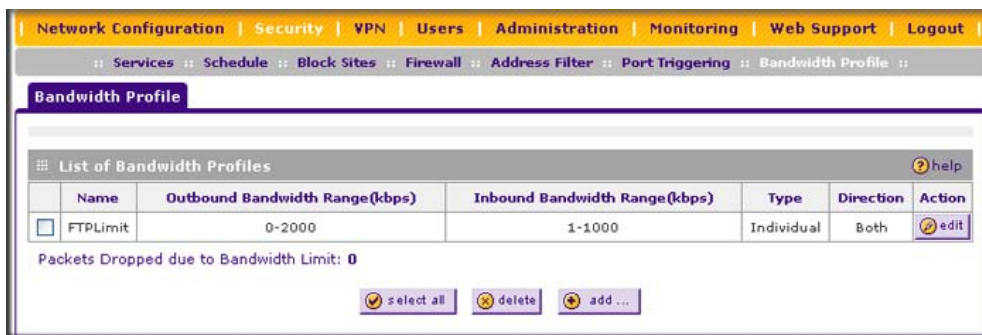
- If the rule has a bandwidth profile specification, then the device will create a bandwidth class in the kernel.
- If multiple connections correspond to the same firewall rule, they will share the same class.

An exception occurs in the case of an individual type 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.



**Figure 4-13**

2. Click **add** to add a new Bandwidth Profile. The Add New Bandwidth Profile screen will display (see [Figure 4-14](#) on page 4-24).

The screenshot shows a web-based configuration interface for adding a bandwidth profile. The window has a title bar 'Add Bandwidth Profile' and a main content area with a 'Bandwidth Profile' header and a 'help' icon. The configuration fields are as follows:

- Profile Name: [ ]
- Direction: [ Both ]
- Outbound Minimum Bandwidth: [ 0 ] (0 - Max. Outbound Bandwidth Kbps)
- Outbound Maximum Bandwidth: [ 100 ] (100 - 100000 Kbps)
- Inbound Minimum Bandwidth: [ 0 ] (0 - Max. Inbound Bandwidth Kbps)
- Inbound Maximum Bandwidth: [ 100 ] (100 - 100000 Kbps)
- Type: [ Group ]

At the bottom of the form are two buttons: 'Apply' and 'Reset'.

**Figure 4-14**

3. Enter the following data:
  - 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.
4. 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 time frames under which firewall rules may be applied.

Three schedules, Schedule 1, Schedule 2 and Schedule 3 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.

The screenshot displays the 'Schedule 1' configuration page. At the top, there is a navigation bar with links for Network Configuration, Security, VPN, Users, Administration, Monitoring, Web Support, and Logout. Below this is a breadcrumb trail: Services > Schedule > Block Sites > Firewall > Address Filter > Port Triggering > Bandwidth Profile. The main content area has three tabs: Schedule 1 (selected), Schedule 2, and Schedule 3. There are two main sections: 'Scheduled Days' and 'Scheduled Time of Day'. Each section has a question about whether the schedule should be active on all days or specific days/times, with radio buttons for selection. The 'Scheduled Days' section has checkboxes for Sunday through Friday. The 'Scheduled Time of Day' section has input fields for Start Time and End Time, each with hour, minute, and AM/PM dropdown menus. At the bottom, there are 'Apply' and 'Reset' buttons.

Figure 4-15

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 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 Blocking application examples:

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

To enable Content Filtering:

1. Select **Security** from the main menu and **Block Sites** from the submenu. The Block Sites screen will display (see [Figure 4-16 on page 4-28](#)).



Figure 4-16

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



**Note:** For additional ways of restricting outbound traffic, see [“Creating a LAN WAN Outbound Services Rule”](#) on page 4-8.

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

1. Select **Security** from the main menu and **Source MAC Filter** from the submenu. The Source MAC Filter screen will display (see [Figure 4-17](#) on page 4-30).

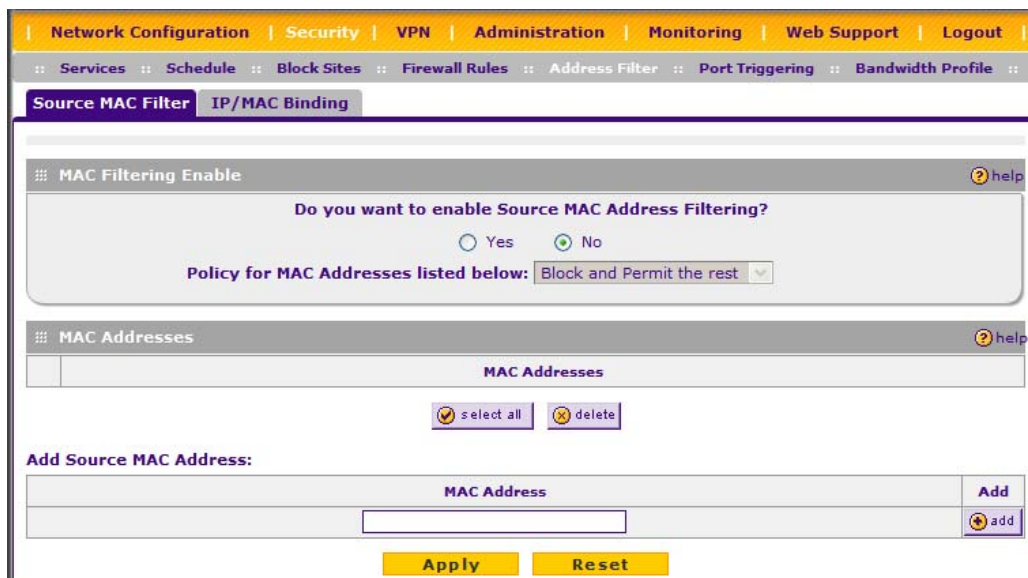


Figure 4-17

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. When you have completed adding MAC addresses, 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 firewall will 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 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 **IP/MAC Binding** from the submenu. The IP/MAC Binding screen will display.

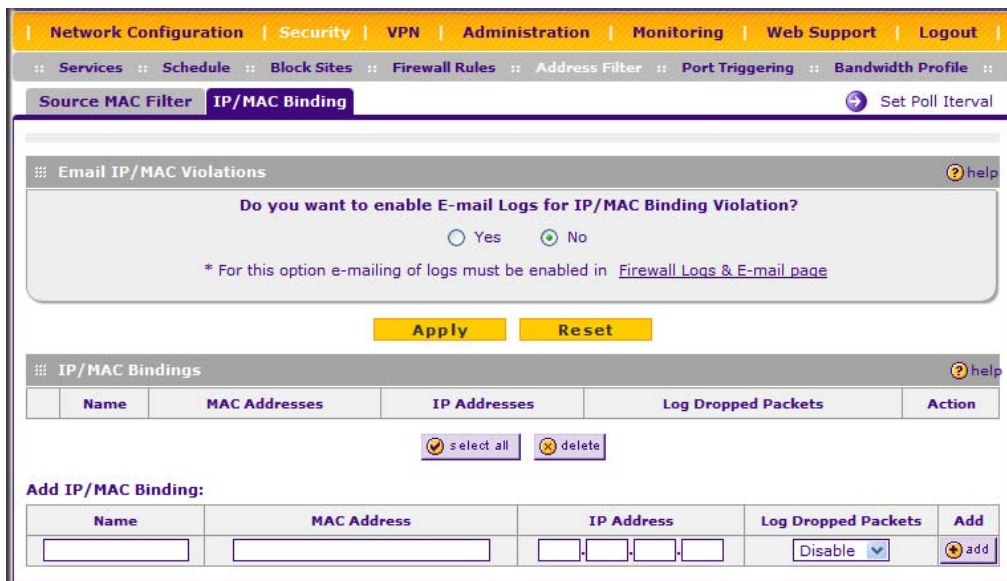


Figure 4-18

2. 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).
3. 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.
4. Click **add**. The new IP/MAC rule will be appear the **IP/MAC Bindings** 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 PC's 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 this VPN firewall cannot be sure when the application has terminated.



**Note:** For additional ways of allowing inbound traffic, see [“Creating a LAN WAN Inbound Services Rule”](#) on page 4-9.

To add a port triggering rule:

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

Operation succeeded.

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

select all delete

Add Port Triggering Rule:

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

**Figure 4-19**

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 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 4-20**

2. Modify any of the fields for this rule.
3. 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.

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

**Figure 4-21**

## 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 4-26](#)), 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 [“Enabling Remote Management Access” on page 6-14](#)).
- Although setting firewall 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 features of the VPN firewall:
  - Groups and hosts (see [“Managing Groups and Hosts” on page 3-6](#))
  - Services (see [“Services-Based Rules” on page 4-2](#))
  - Schedules (see [“Setting a Schedule to Block or Allow Specific Traffic” on page 4-25](#))
  - Block sites (see [“Blocking Internet Sites \(Content Filtering\)” on page 4-26](#))
  - Source MAC filtering (see [“Configuring Source MAC Filtering” on page 4-29](#))
  - Port triggering (see [“Configuring Port Triggering” on page 4-33](#))

# Chapter 5

## Virtual Private Networking

This chapter describes how to use the Virtual Private Networking (VPN) features of the ProSafe VPN Firewall 50 FVS338. 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 5-2
- [“Testing the Connections and Viewing Status Information”](#) on page 5-12
- [“Managing VPN Policies”](#) on page 5-15
- [“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

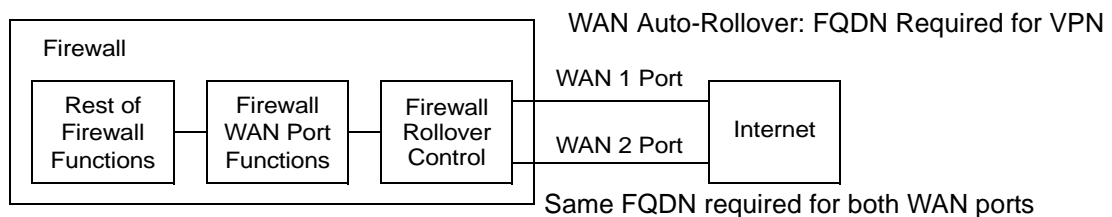
### Considerations for Dual WAN Port Systems

---

If both of the WAN ports of the VPN firewall are configured, you can enable Auto-Rollover mode for increased system reliability. Selecting Auto-Rollover mode 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 rollover mode.

The diagram and table below shows how the WAN mode selection relates to VPN configuration.



**Figure 5-1**

Table 5-1 summarizes the WAN addressing requirements for Auto-Rollover mode.

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

Configuration	WAN IP address	Rollover Mode <sup>a</sup>
VPN Road Warrior (client-to-gateway)	Fixed or DHCP	FQDN required
VPN Gateway-to-Gateway	Fixed or DHCP	FQDN required
VPN Telecommuter (client-to-gateway NAT router)	Fixed or DHCP	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

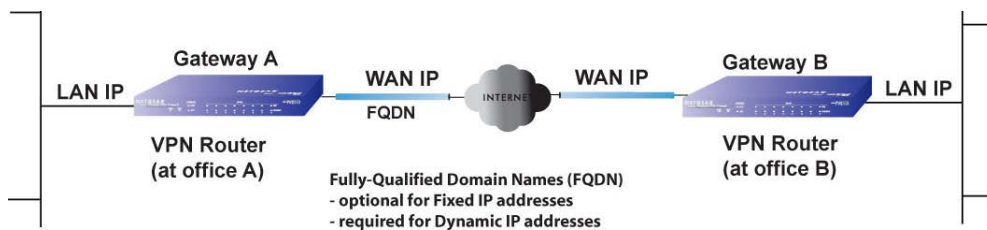
You use the VPN Wizard to configure multiple gateway or client VPN tunnel policies.

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.

### Creating Gateway to Gateway VPN Tunnels with the Wizard



**Figure 5-2**




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 5-3**


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 (broadband or dialup) to use as the VPN tunnel end point.


	<b>Note:</b> 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 Names** of the gateways which will connect.


- Both the remote WAN address and your local WAN address are required.

	<b>Tip:</b> 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.

	<b>Tip:</b> 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.

	<b>Note:</b> The Remote LAN IP address <i>must</i> 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 <i>could not</i> 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.

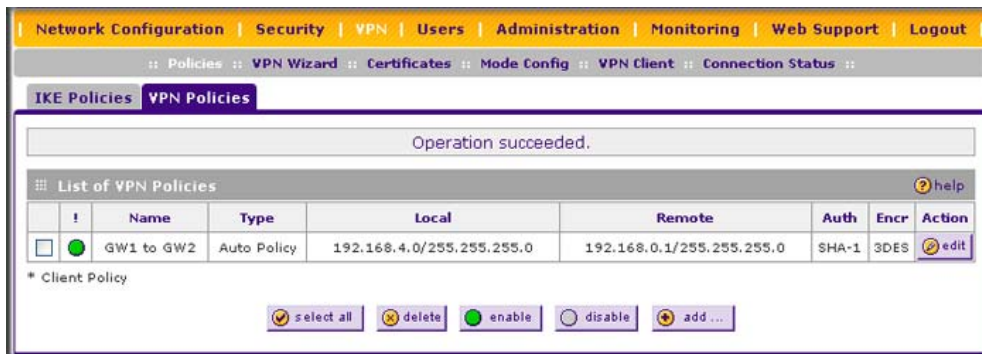


Figure 5-4

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.

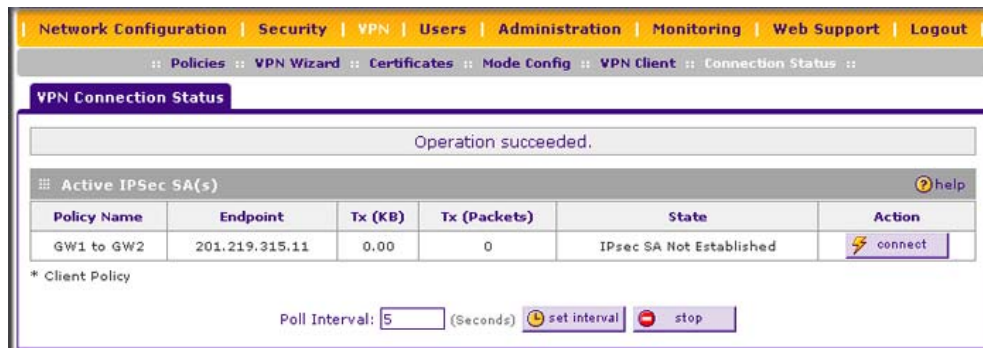


Figure 5-5

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

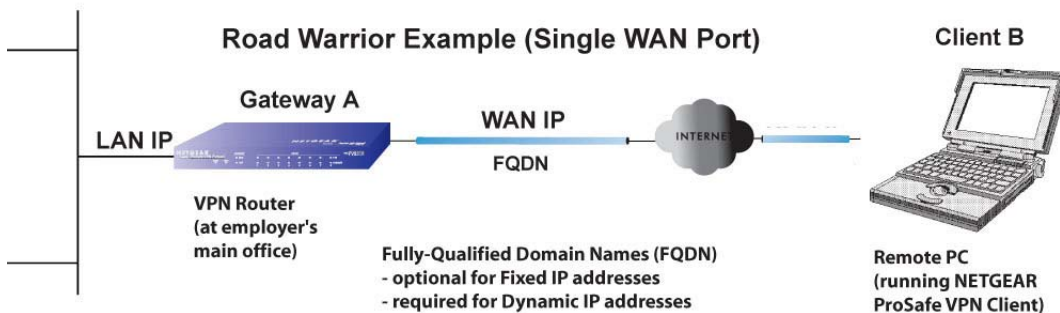


Figure 5-6

Follow these steps to configure the a VPN client tunnel:

- Configure the client policies on the gateway (see [“Use the VPN Wizard Configure the Gateway for a Client Tunnel”](#) on this page).
- Configure the VPN client to connect to the gateway (see [“Use the NETGEAR VPN Client Security Policy Editor to Create a Secure Connection”](#) on page 5-8).


### Use the VPN Wizard Configure the Gateway for a Client Tunnel

Follow these steps to set up a client 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 (see [Figure 5-7 on page 5-7](#)). To view the wizard default settings, click the **VPN Wizard Default Values** link.

Figure 5-7

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+eClient, 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.

	<p><b>Note:</b> 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.</p>
---	--

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

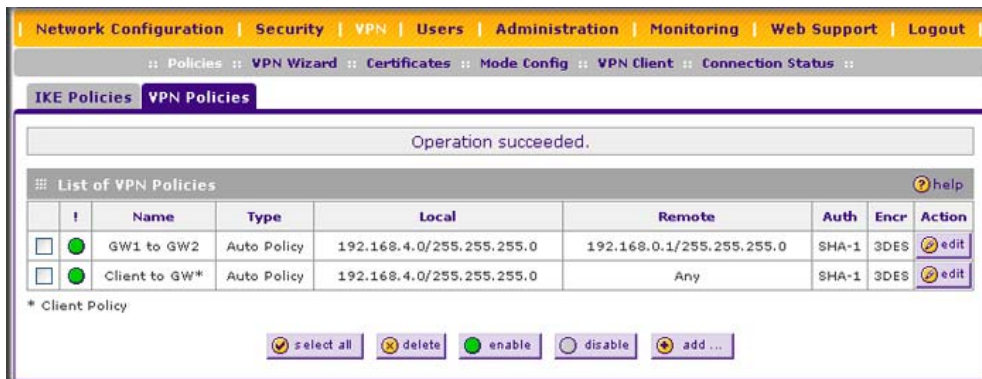


Figure 5-8

To view or modify the VPN policy, see [“Managing VPN Policies”](#) on page 5-15.

## 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 FVS338. Follow these steps to configure your VPN client.

- 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.

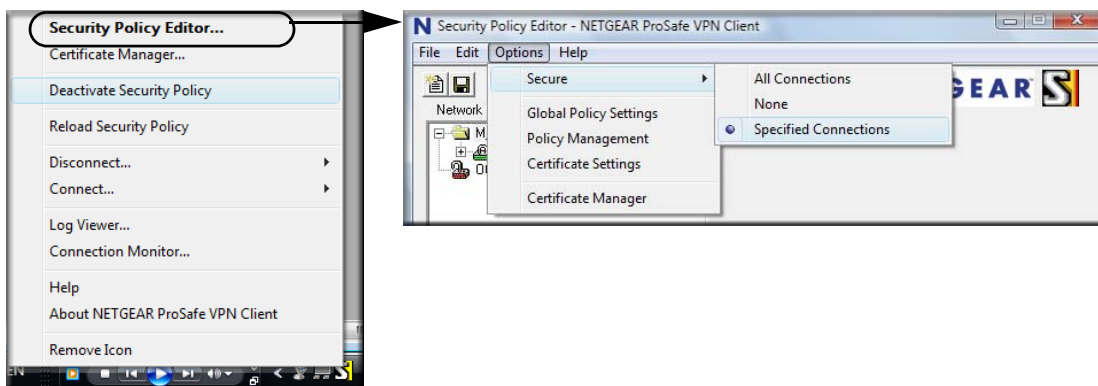
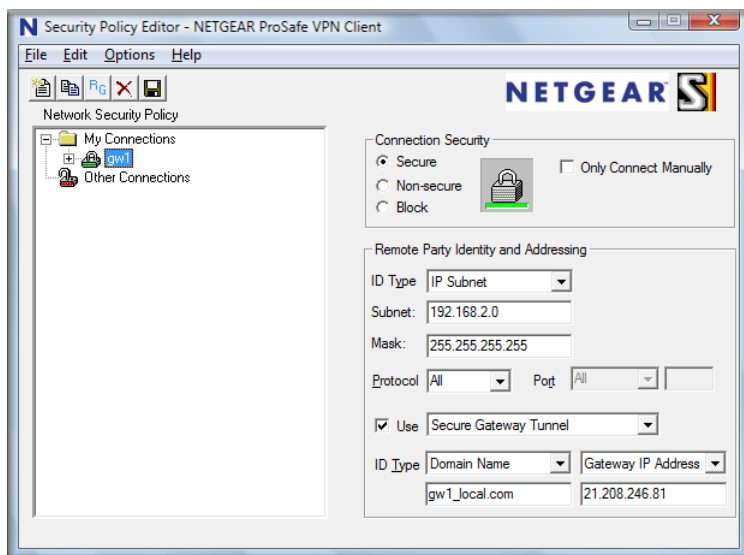


Figure 5-9

- 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**.

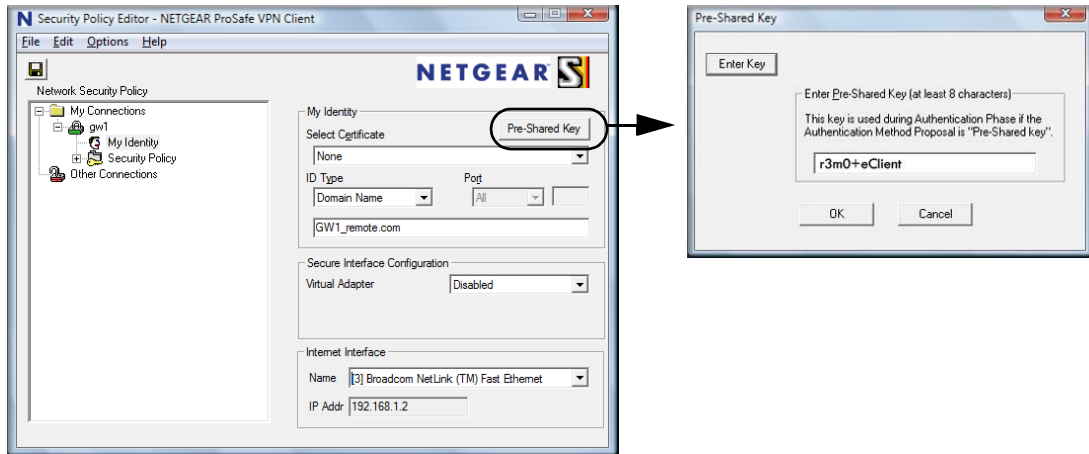


**Figure 5-10**

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 FVS338 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 FVS338 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 FVS338; 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 5-11**

- 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+eClient.”
  - 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 (see [Figure 5-12 on page 5-11](#)).
    - 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.



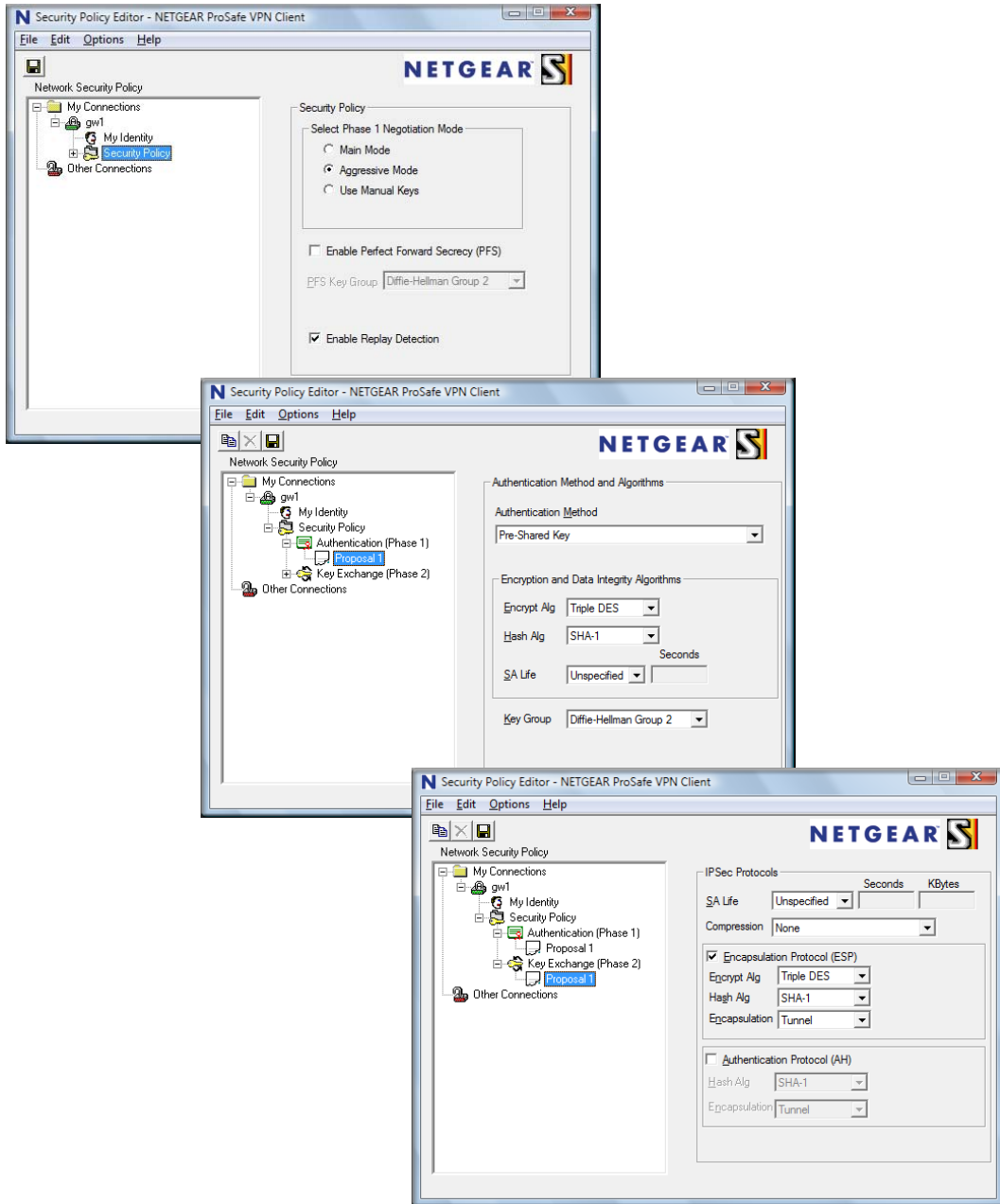


Figure 5-12

## 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**.

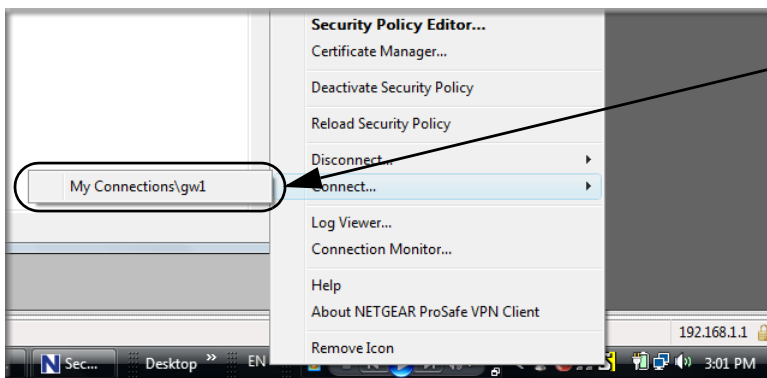


Figure 5-13

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



Figure 5-14

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.

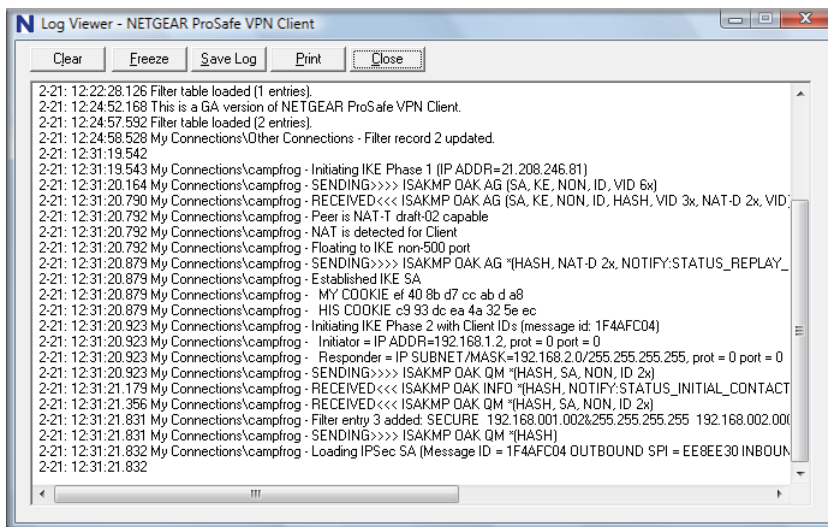


Figure 5-15

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

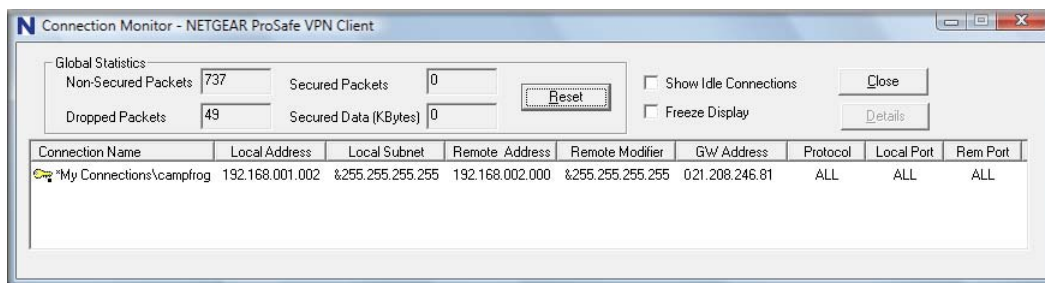





Figure 5-16

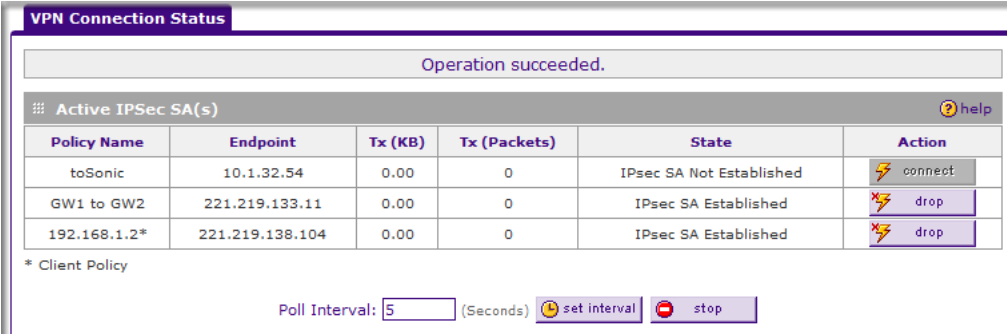
The VPN client system tray icon provides a variety of status indications, which are listed below.

**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.



VPN Connection Status

Operation succeeded.

Active IPsec SA(s) help

Policy Name	Endpoint	Tx (KB)	Tx (Packets)	State	Action
toSonic	10.1.32.54	0.00	0	IPsec SA Not Established	 connect
GW1 to GW2	221.219.133.11	0.00	0	IPsec SA Established	 drop
192.168.1.2*	221.219.138.104	0.00	0	IPsec SA Established	 drop

\* Client Policy

Poll Interval:  (Seconds) set interval stop

**Figure 5-17**

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.

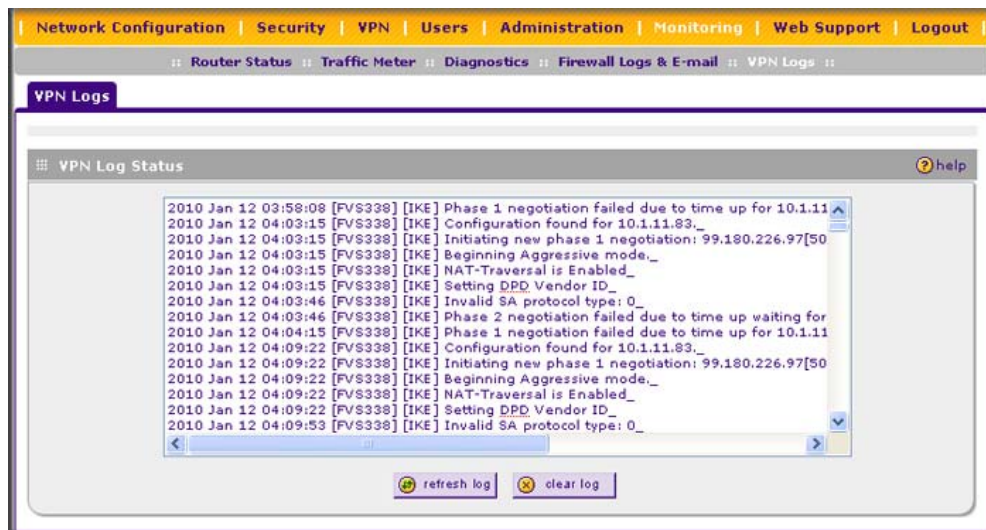


Figure 5-18

## 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:

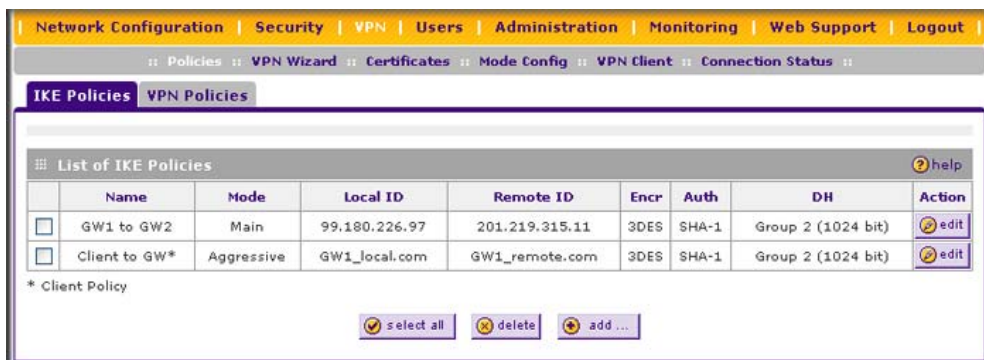
1. The VPN Policy Selector determines that some traffic matches an existing VPN policy. If the VPN policy is of type “Auto”, then the Auto Policy Parameters defined in the VPN policy are accessed which specify which IKE Policy to use.
2. If the VPN policy is a “Manual” policy, then the Manual Policy 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 (see [Figure 5-19 on page 5-17](#)).



**Figure 5-19**

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. If the policy is a client policy, it will be prepended by an “\*”.
- **Mode.** Two modes are available: either “Main” or “Aggressive”.
  - Main Mode is slower but more secure.
  - Aggressive mode is faster but less secure. (If specifying either a FQDN or a User FQDN name as the Local ID/Remote ID, aggressive mode is automatically selected.)
- **Local ID.** The IKE/ISAKMP 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 D, “Related Documents.”](#)

## 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 5-8 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 them, or delete them entirely. The rules for VPN policy use conform to:

1. Traffic covered by a policy will automatically be sent via a VPN tunnel.
2. 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). Client policies are annotated by an “\*”.
- **Type.** The type is “Auto” or “Manual” as described previously (Auto is used during VPN Wizard configuration).
- **Local.** IP address (either a single address, range of address or subnet address) on your local LAN. Traffic must be from (or to) these addresses to be covered by this policy. (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 Certificates (also known as X509 Certificates) are used to authenticate the identity of users and systems, and are issued by various CAs (Certification Authorities). Digital Certificates are used by the VPN firewall during the IKE (Internet Key Exchange) authentication phase as an alternative authentication method.

The VPN firewall uses Digital 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 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 FVS338 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.

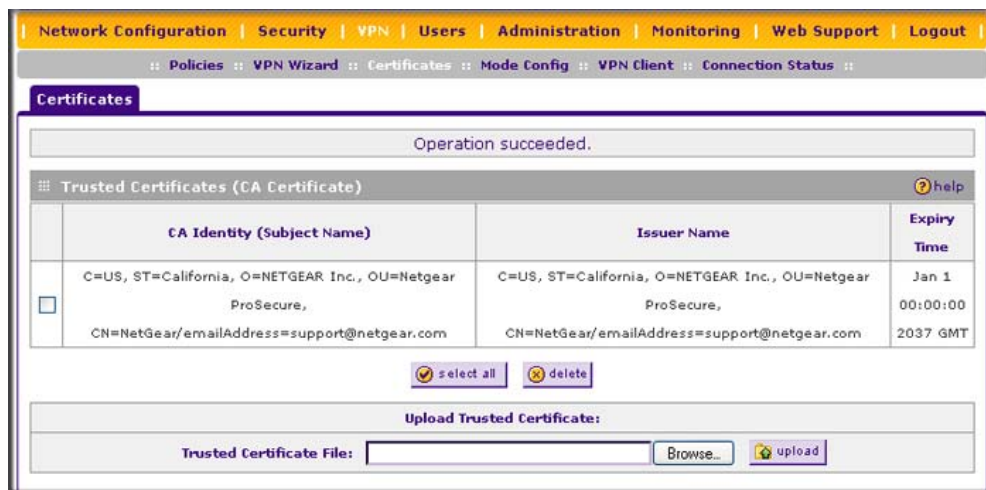
## Viewing and Loading CA Certificates

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 (CA Certificates)** section.



**Figure 5-20**

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** on the Certificates screen, 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.



Name	Subject Name	Serial Number	Issuer Name	Expiry Time
------	--------------	---------------	-------------	-------------

Figure 5-21

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 (see [Figure 5-22 on page 5-23](#)).

The screenshot shows a web interface for generating self-certificates. The top part is a form with fields for Name, Subject, Hash Algorithm (MD5), Signature Algorithm (RSA), Signature Key Length (512), IP Address (Optional), Domain Name (Optional), and E-mail Address (Optional). A 'generate...' button is below the form. The bottom part is a table titled 'Self Certificate Requests' with columns for Name, Status, and Action. Below the table are 'select all' and 'delete' buttons. At the bottom, there is a section for uploading a certificate, with a 'Certificate File:' input field, a 'Browse...' button, and an 'upload' button.

**Figure 5-22**

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 5-23

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

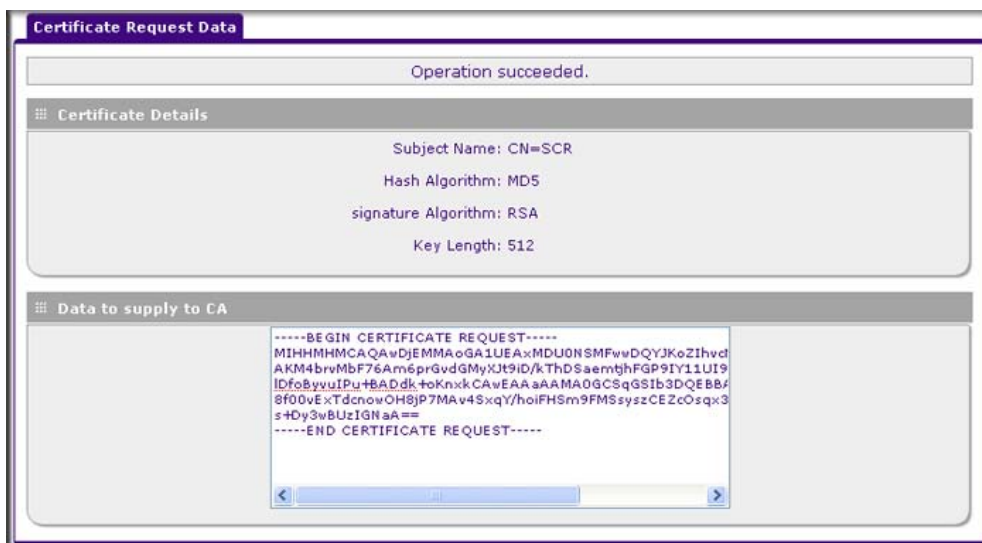


Figure 5-24

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 occur, the certificate will be issued.
8. Store the certificate file from the CA on your computer and backup the certificate file from the CA in another location.
9. Return to the Certificates screen and locate the **Self Certificate Requests** section.



Figure 5-25

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** table.

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.

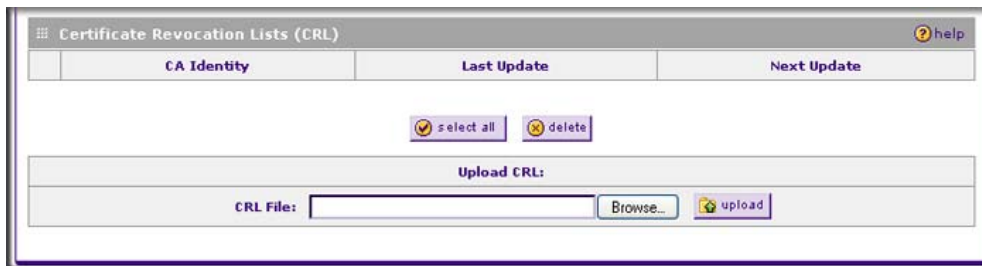
## Managing your Certificate Revocation List (CRL)

A CRL 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.

On the Certificates screen, 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 (see [Figure 5-26 on page 5-26](#)).



**Figure 5-26**

The **Certificate Revocation Lists (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

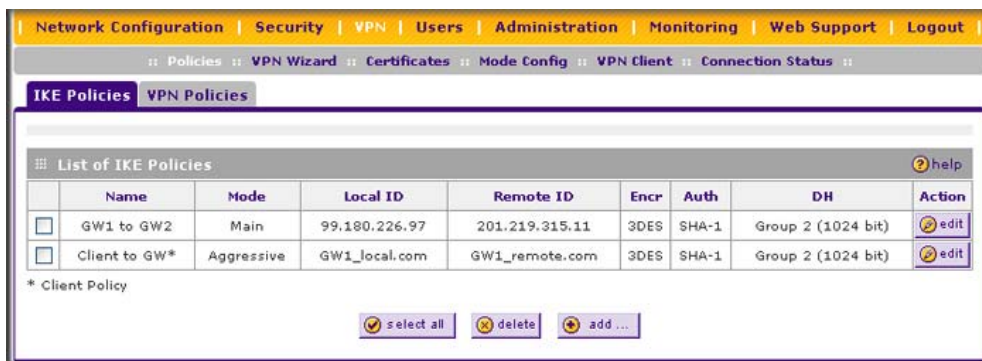
Once the XAUTH has been enabled, you must establish user accounts on the local database to be authenticated against XAUTH, or you must enable a RADIUS-CHAP or RADIUS-PAP server.



**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 either modify an existing IKE policy by clicking **edit** adjacent to the policy, or create a new IKE Policy by clicking **add**. (Figure 5-28 on page 5-28 shows the Add IKE Policy screen.)

The screenshot shows the 'Add IKE Policy' configuration interface. It is divided into several sections:

- Mode Config Record:** A question 'Do you want to use Mode Config Record?' with 'Yes' and 'No' radio buttons. 'No' is selected. Below is a 'Select Mode Config Record:' dropdown menu and a 'view selected' button.
- General:** 'Policy Name:' text box, 'Direction / Type:' dropdown set to 'Both', and 'Exchange Mode:' dropdown set to 'Main'.
- Local:** 'Select Local Gateway:' with 'Broadband' and 'Dialup' radio buttons. 'Broadband' is selected. Below is 'Identifier Type:' dropdown set to 'Local Wan IP' and an 'Identifier:' text box.
- Remote:** 'Identifier Type:' dropdown set to 'Remote Wan IP' and an 'Identifier:' text box.
- IKE SA Parameters:** 'Encryption Algorithm:' dropdown set to '3DES', 'Authentication Algorithm:' dropdown set to 'SHA-1', 'Authentication Method:' with 'Pre-shared key' selected and 'RSA-Signature' unselected, 'Pre-shared key:' text box, 'Diffie-Hellman (DH) Group:' dropdown set to 'Group 2 (1024 bit)', 'SA-Lifetime (sec):' text box set to '28800', 'Enable Dead Peer Detection:' with 'Yes' and 'No' radio buttons. 'No' is selected, 'Detection Period:' text box set to '10' (Seconds), and 'Reconnect after failure count:' text box set to '3'.
- Extended Authentication:** This section is circled in black. It contains 'XAUTH Configuration' with 'None', 'Edge Device', and 'IPSec Host' radio buttons. 'None' is selected. To the right is 'Authentication Type:' dropdown set to 'User Database', 'Username:' text box set to 'admin', and 'Password:' text box with masked characters.

At the bottom of the form are 'Apply' and 'Reset' buttons.

**Figure 5-28**

- 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 gateway.

Specify one of the following authentication types:

- **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 VPN client users for use by the XAUTH server. Whether or not you use an external RADIUS server, you may want to have some users authenticated locally. These users must be added to the User Database **Configured Users** table.

To add a new user:

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

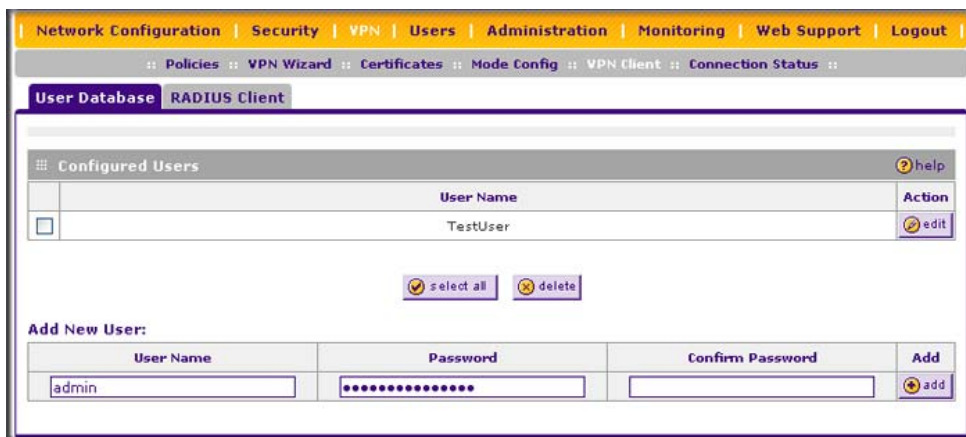


Figure 5-29

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 (see [Figure 5-30 on page 5-31](#)).

**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 **Apply** to save the settings.



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

## Assigning IP Addresses to Remote Users (ModeConfig)

---

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

### ModeConfig Operation

After 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 ModeConfig 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.

To configure the ModeConfig screen:

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

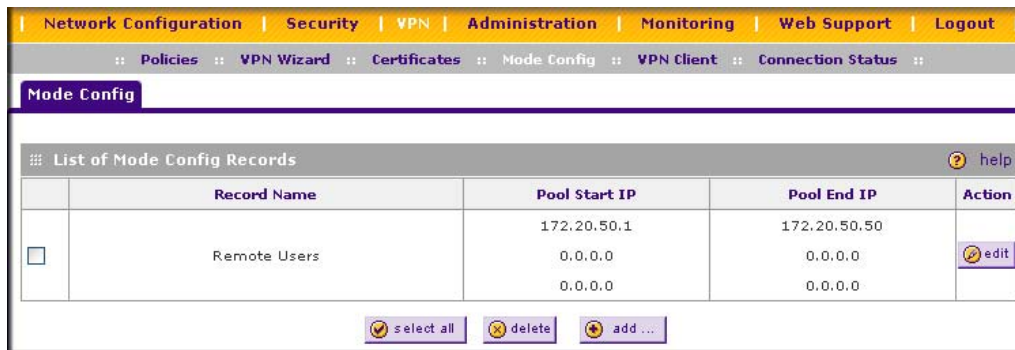


Figure 5-31

- Click **add**. The Add Mode Config Record screen will display.

**Figure 5-32**

- Enter a descriptive Record Name such as “Remote Users”.
- Assign at least one range of IP Pool addresses in the First IP Pool field to give to remote VPN clients.

	<b>Note:</b> 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.
--	--

- If you have a WINS server on your local network, enter its IP address.
- Enter one or two DNS server IP addresses to be used by remote VPN clients.
- 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,
- 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 showing the current policies in the **List of IKE Policies** table.

	Name	Mode	Local ID	Remote ID	Encr	Auth	DH	Action
<input type="checkbox"/>	GW1 to GW2	Main	99.180.226.97	201.219.315.11	3DES	SHA-1	Group 2 (1024 bit)	<a href="#">edit</a>
<input type="checkbox"/>	Client to GW*	Aggressive	GW1_local.com	GW1_remote.com	3DES	SHA-1	Group 2 (1024 bit)	<a href="#">edit</a>

\* Client Policy

[select all](#) [delete](#) [add...](#)

Figure 5-33

- Click **add** to configure a new IKE policy. The Add IKE Policy screen will display.

The screenshot shows the 'Add IKE Policy' configuration window. The 'Mode Config Record' section is circled in red. It contains the following elements:

- Do you want to use Mode Config Record?** with radio buttons for  Yes and  No.
- Select Mode Config Record:** a pull-down menu.
- view selected** button.

Other sections include:

- General:** Policy Name (text field), Direction / Type (Both), Exchange Mode (Main).
- Local:** Select Local Gateway (Broadband, Dialup), Identifier Type (Local Wan IP), Identifier (text field).
- Remote:** Identifier Type (Remote Wan IP), Identifier (text field).
- IKE SA Parameters:** Encryption Algorithm (3DES), Authentication Algorithm (SHA-1), Authentication Method (Pre-shared key, RSA-Signature), Pre-shared key (text field), Diffie-Hellman (DH) Group (Group 2 (1024 bit)), SA-Lifetime (sec) (28800), Enable Dead Peer Detection (No), Detection Period (10 seconds), Reconnect after failure count (3).
- Extended Authentication:** XAUTH Configuration (None, Edge Device, IPSec Host), Authentication Type (User Database), Username (admin), Password (masked).

Buttons for **Apply** and **Reset** are at the bottom.

**Figure 5-34**

- 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** radio box.)

Mode Config works only in Aggressive Mode, and Aggressive Mode requires that both ends of the tunnel be defined by a FQDN.

4. In the **General** section:
  - 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 **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
8. Enter a Pre-Shared Key that will also be configured in the VPN client.
9. 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](#).

10. 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.

11. 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.

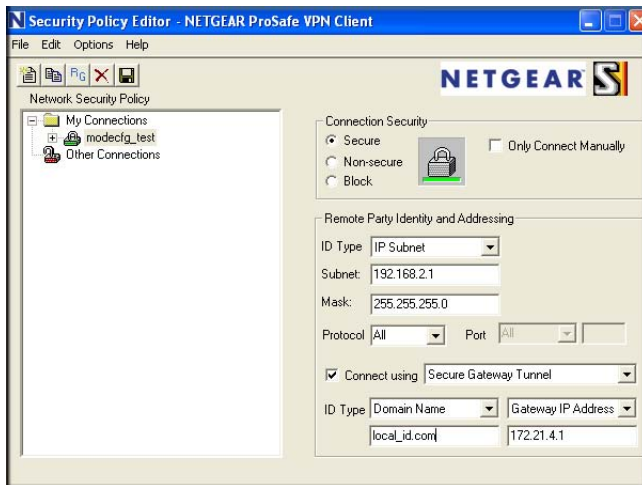
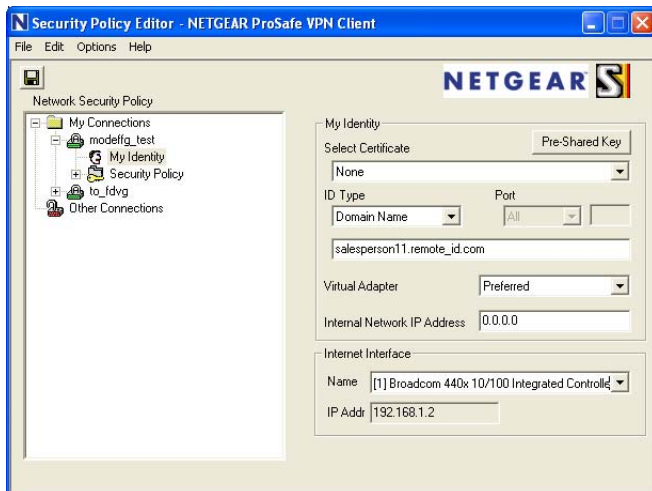


Figure 5-35

- 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”.


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



**Figure 5-36**

Enter the following information:

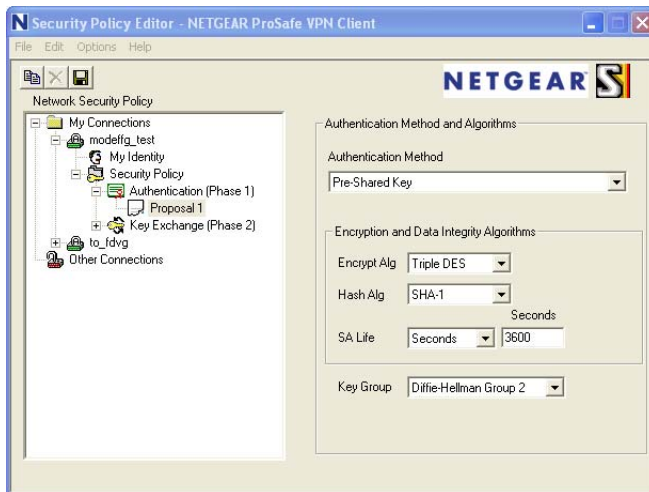
- Click **Pre-Shared Key** and enter the key you configured on the VPN firewall's Add IKE Policy screen.
- From the Select Certificate pull-down menu, select **None**.
- From the ID Type pull-down menu, select **Domain Name** and create an identifier based on the name of the IKE policy you created; for example "remote\_id.com".
- Under Virtual Adapter pull-down menu, select Preferred. The Internal Network IP Address should be 0.0.0.0.

	<b>Note:</b> 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."
---	--

- Select your Internet Interface adapter from the Name pull-down menu.
- On the left-side of the menu, select Security Policy.

Enter the following information:

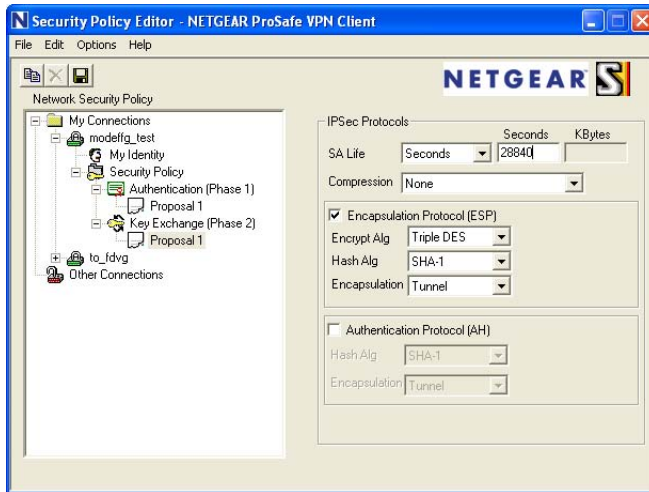
- a. Under Security Policy, Phase 1 Negotiation Mode, check the **Aggressive Mode** radio button.
  - b. Check the **Enable Perfect Forward Secrecy (PFS)** radio button, and select the **Diffie-Hellman Group 2** from the PFS Key Group pull-down menu.
  - c. **Enable Replay Detection** should be checked.
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.

- 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).

- 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:

- 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”.
- 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”.
- 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.

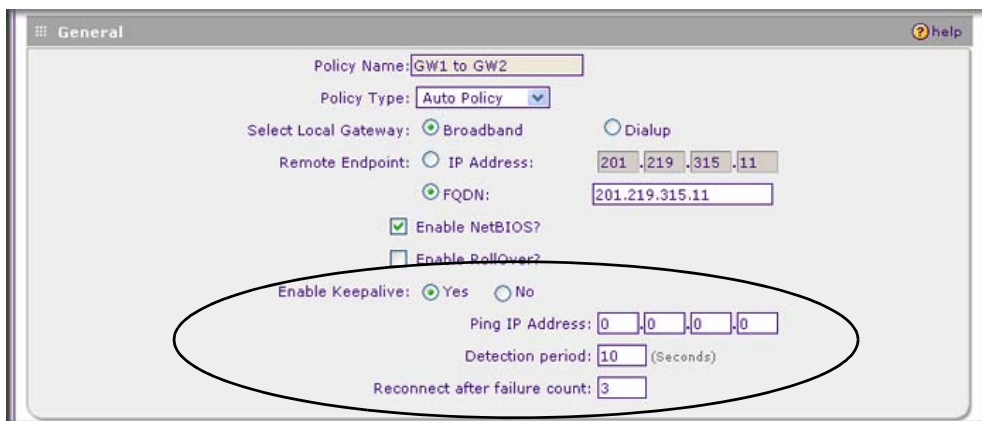


Figure 5-39

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.

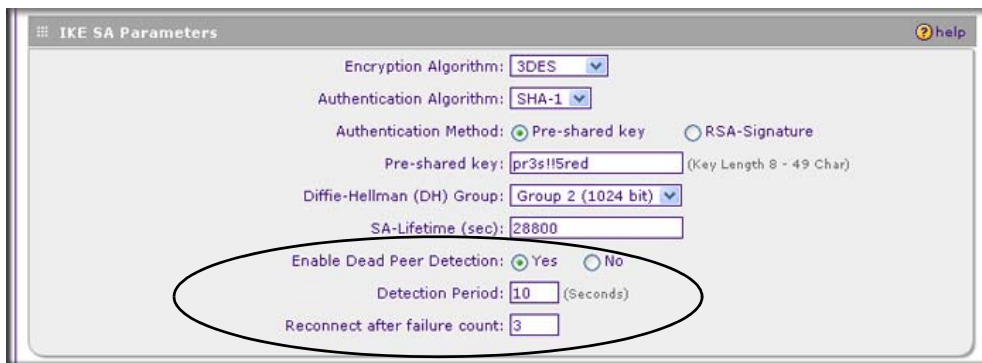


Figure 5-40

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.

- 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.
- 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:

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



Figure 5-41

- 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 50 FVS338.

This chapter includes the following sections:

- [“Performance Management”](#) on this page
- [“Configuring Users, Administrative Settings, and Remote Management”](#) on page 6-7
- [“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: 8000 Mbps (eight LAN ports at 1000 Mbps each)
- WAN side: 1000 Mbps (one WAN port at 1000 Mbps)

In practice, the WAN-side bandwidth capacity will be much lower when DSL or cable modems are used to connect to the Internet. As a result and depending on the traffic being carried, the WAN side of the firewall will be the limiting factor to throughput for most installations. If the dial-up port is used for the WAN connection, the WAN-side bandwidth capacity is severely limited.

## 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). The LAN WAN Rules screen lists all existing rules for outbound traffic. If you have not defined any rules, only the default rule will be listed. The default rule allows all outgoing traffic. (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 (you use the Network Database to assign PCs to groups—see [“Managing Groups and Hosts”](#) on page 3-6).
- **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 [“Services-Based Rules” on page 4-2](#) and [“Adding Customized Services” on page 4-20](#)).
- **Groups and Hosts.** You can apply these rules selectively to groups of PCs to reduce the outbound or inbound traffic. The Network Database is an automatically-maintained list of all known PCs and network devices. PCs and devices become known by the following methods:
  - **DHCP Client Request.** By default, the DHCP server in this 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” on page 3-6](#) for the procedure on how to use this feature.
- **Schedule.** If you have set firewall rules on the LAN 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 4-25](#) 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 (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 4-26 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 4-29 for the procedure on how to use this feature.

## VPN Firewall Features That Increase Traffic

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

- Port forwarding
- Port triggering
- Exposed hosts
- VPN tunnels

### Port Forwarding

The 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). The LAN WAN Rules screen lists all existing rules for inbound traffic. If you have not defined any rules, only the default rule will be listed. The default rule blocks all inbound traffic.

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

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

You can also enable a check on special rules:

- **VPN Passthrough.** 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 WAN interface selected or Specific IP address entered in this field. Selecting ANY enables the rule for any IP in the destination field.

- **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 4-20](#)).
- **Schedule.** If you have set firewall rules on the LAN 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 4-25](#) 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, operation is 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 PC's 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 4-33](#) 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 4-22 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 [“Viewing the Router Configuration and System Status”](#) on page 6-30 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 6-9
- [“Configuring an External Server for Authentication”](#) on page 6-10
- [“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 administrator and guest password for the 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 the guest account.

To modify the Administrator user account settings, including the password:

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

The screenshot shows the 'Local Authentication' configuration page. At the top, there is a navigation bar with links: Network Configuration, Security, VPN, Users, Administration, Monitoring, Web Support, and Logout. Below the navigation bar, there are two tabs: 'Local Authentication' (selected) and 'External Authentication'. The main content area is divided into several sections:

- Enable Local Authentication:** A section with a question 'Do you want to enable Local Authentication?' and two radio buttons: 'Yes' (selected) and 'No'. Below are 'Apply' and 'Reset' buttons.
- User Selection:** A section with two radio buttons: 'Edit Admin Settings' (selected) and 'Edit Guest Settings'. Below are 'Apply' and 'Reset' buttons.
- Admin Settings:** A section with four input fields: 'New User Name' (containing 'admin'), 'Old Password', 'New Password', and 'Retype New Password'. Below are 'Apply' and 'Reset' buttons.
- Guest Settings:** A section with four input fields: 'New User Name' (containing 'guest'), 'Old Password', 'New Password', and 'Retype New Password'. Below are 'Apply' and 'Reset' buttons.
- Local Authentication Settings:** A section with two input fields: 'Administrator login times out after idle for' (containing '5') and 'Domain Name' (containing 'LOCALDOMAIN'). Below are 'Apply' and 'Reset' buttons.

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 6-10).

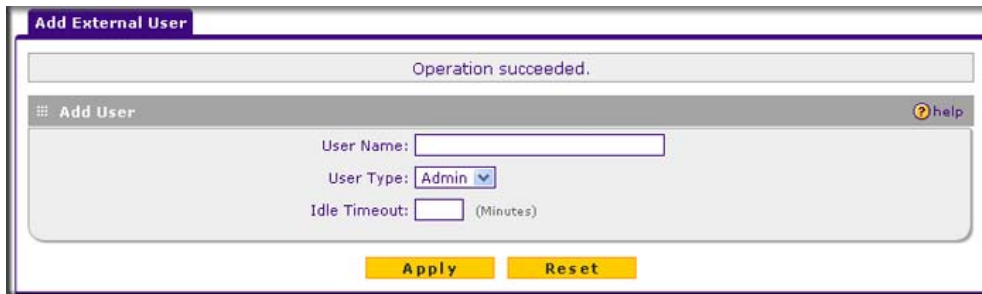
To add an external users:

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.



The screenshot shows a web interface for adding an external user. At the top, a purple header bar contains the text "Add External User". Below this is a light gray box with the message "Operation succeeded.". Underneath is a darker gray bar with a hamburger menu icon, the text "Add User", and a "help" icon. The main form area has three input fields: "User Name:" followed by a text box, "User Type:" followed by a dropdown menu showing "Admin", and "Idle Timeout:" followed by a text box and the label "(Minutes)". At the bottom of the form are two yellow buttons labeled "Apply" and "Reset".

**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 [Table 6-1 on page 6-11](#).

**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 <a href="#">Appendix C, "Two Factor Authentication"</a> 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 (see [Figure 6-4 on page 6-12](#)).

The screenshot displays the configuration interface for External Authentication. The top navigation bar includes: Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout. The current page is titled "External Authentication" and contains three main sections:

- Enable External Authentication:** A dialog box asking "Do you want to enable Remote Authentication?" with radio buttons for "Yes" (selected) and "No". Below are "Apply" and "Reset" buttons.
- RADIUS Server Configuration:** Fields for:
  - Primary Server IP Address: 0 . 0 . 0 . 0
  - Secret Phrase: [masked]
  - Primary Server NAS Identifier: FVS338
  - Primary Authentications Type: RADIUS-PAP (dropdown)
  - Enable Backup Server: [checkbox]
  - Backup Server IP Address: 0 . 0 . 0 . 0
  - Secret Phrase: [masked]
  - Backup Server NAS Identifier: FVS338Below are "Apply" and "Reset" buttons.
- Authentication Settings:** Fields for:
  - Domain Name: EXTERNALDOMAIN
  - Retry Timeout: 5 (Sec)
  - Maximum Retry Count: 3
  - Users Default Timeout: 10 (Minutes)Below are "Apply" and "Reset" buttons.

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.

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 in to the VPN Firewall](#)” on page 2-2).



**Note:** Be sure to change the VPN firewall default configuration password to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both upper and lower case), numbers, and symbols. Your password can be up to 30 characters. See “[Changing Passwords and Settings](#)” on page 6-8 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.

Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout

Remote Management :: SNMP :: Settings Backup & Upgrade :: Time Zone

### Remote Management

Secure HTTP Management (Status: Accessible on primary WAN1, WAN2) help

Allow Secure HTTP Management?

Yes  
 No

Everyone (Be sure to change default password)  
 IP address range:  
From: 0 . 0 . 0 . 0  
To: 0 . 0 . 0 . 0  
 Only this PC: 0 . 0 . 0 . 0

Port Number: 8080

IP Address to connect to this device: <https://99.180.226.97:8080>  
(Be sure to type "https" not "http")

Telnet Management (Status: Service is Disabled) help

Allow Telnet Management?

Yes  
 No

Everyone (Be sure to change default password)  
 IP address range:  
From: 0 . 0 . 0 . 0  
To: 0 . 0 . 0 . 0  
 Only this PC: 0 . 0 . 0 . 0

Apply Reset

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 PC**. 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 FVS338.mynetgear.net`, and the WAN IP address that your ISP assigned to the VPN firewall is displayed.

## Using an SNMP Manager

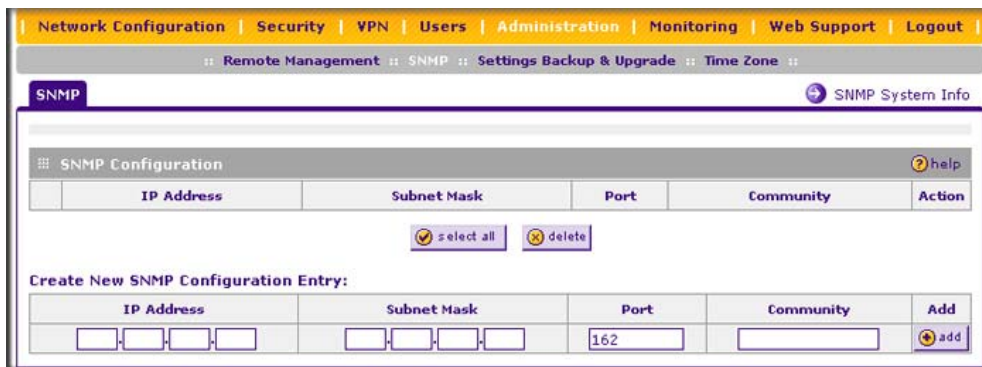
Simple Network Management Protocol (SNMP) lets you monitor and manage your VPN firewall from an SNMP Manager. It provides a remote means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

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**

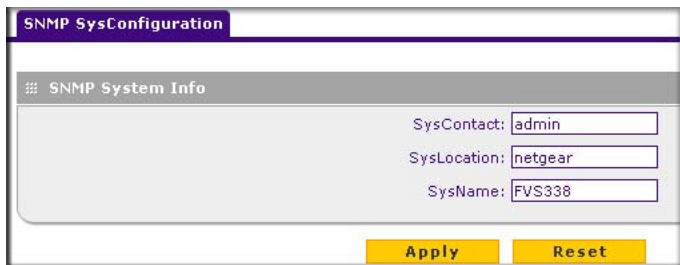
2. Under **Create New SNMP Configuration Entry**, enter the IP Address of the SNMP manager in the **IP Address** field and the subnet mask in the **Subnet Mask** field. Note the following:
  - If you want to allow only the host address to access the VPN firewall and receive traps, enter an IP Address 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.



The screenshot shows a web interface titled "SNMP SysConfiguration". Below the title bar is a sub-header "SNMP System Info". The main content area contains three text input fields: "SysContact:" with the value "admin", "SysLocation:" with the value "netgear", and "SysName:" with the value "FVS338". At the bottom of the form are two yellow buttons labeled "Apply" and "Reset".

**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.

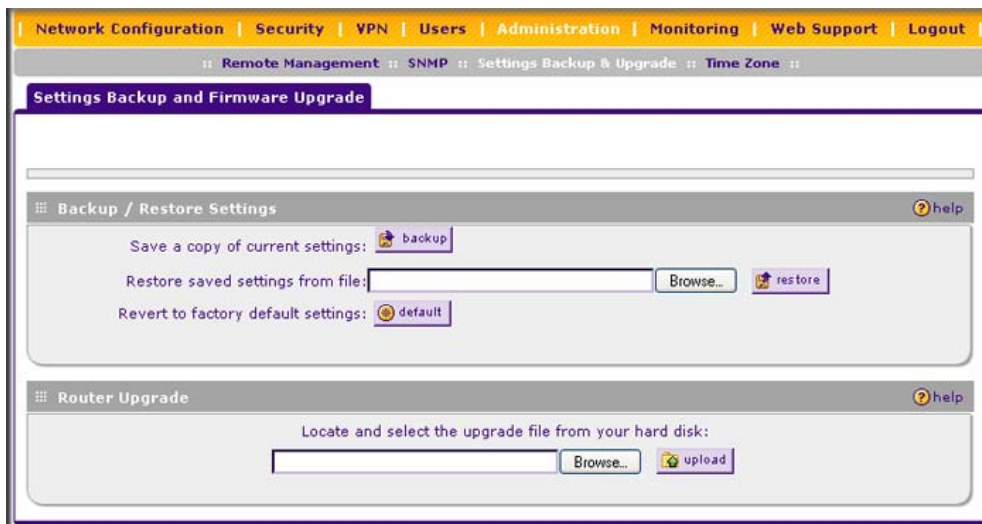



Figure 6-8

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.

	<p><b>Warning:</b> Once you start restoring settings or erasing the VPN firewall, do <i>not</i> 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!</p>
---	--

## 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 page 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 & Upgrade screen. To view the current version of the firmware that the 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 FVS338.
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](#)).

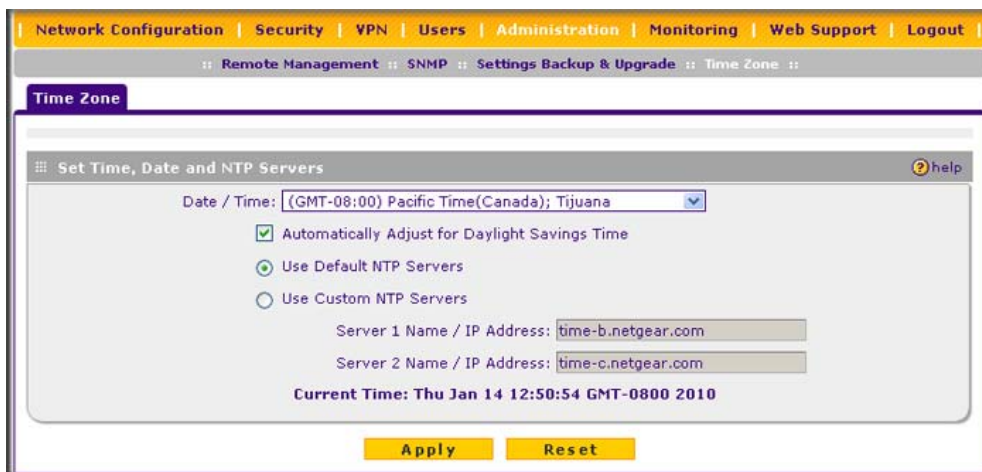


Figure 6-9

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 an 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 Broadband ISP Settings screen or Dial-up ISP Settings screen before the VPN firewall can perform this lookup.

5. Click **Apply** to save your 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 this page.
- [“Viewing the Logs”](#) on page 6-26
- [“Enabling the Traffic Meter”](#) on page 6-27
- [“Viewing the Router Configuration and System Status”](#) on page 6-30
- [“Monitoring VPN Firewall Statistics”](#) on page 6-32
- [“Monitoring WAN Ports Status”](#) on page 6-33
- [“Monitoring Attached Devices”](#) on page 6-34
- [“Monitoring VPN Tunnel Connection Status”](#) on page 6-35
- [“Viewing the VPN Logs”](#) on page 6-36
- [“Viewing the DHCP Log”](#) on page 6-37
- [“Viewing Port Triggering Status”](#) on page 6-37

### 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; 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 4-26), 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 6-10 on page 6-24](#)). 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](#)).

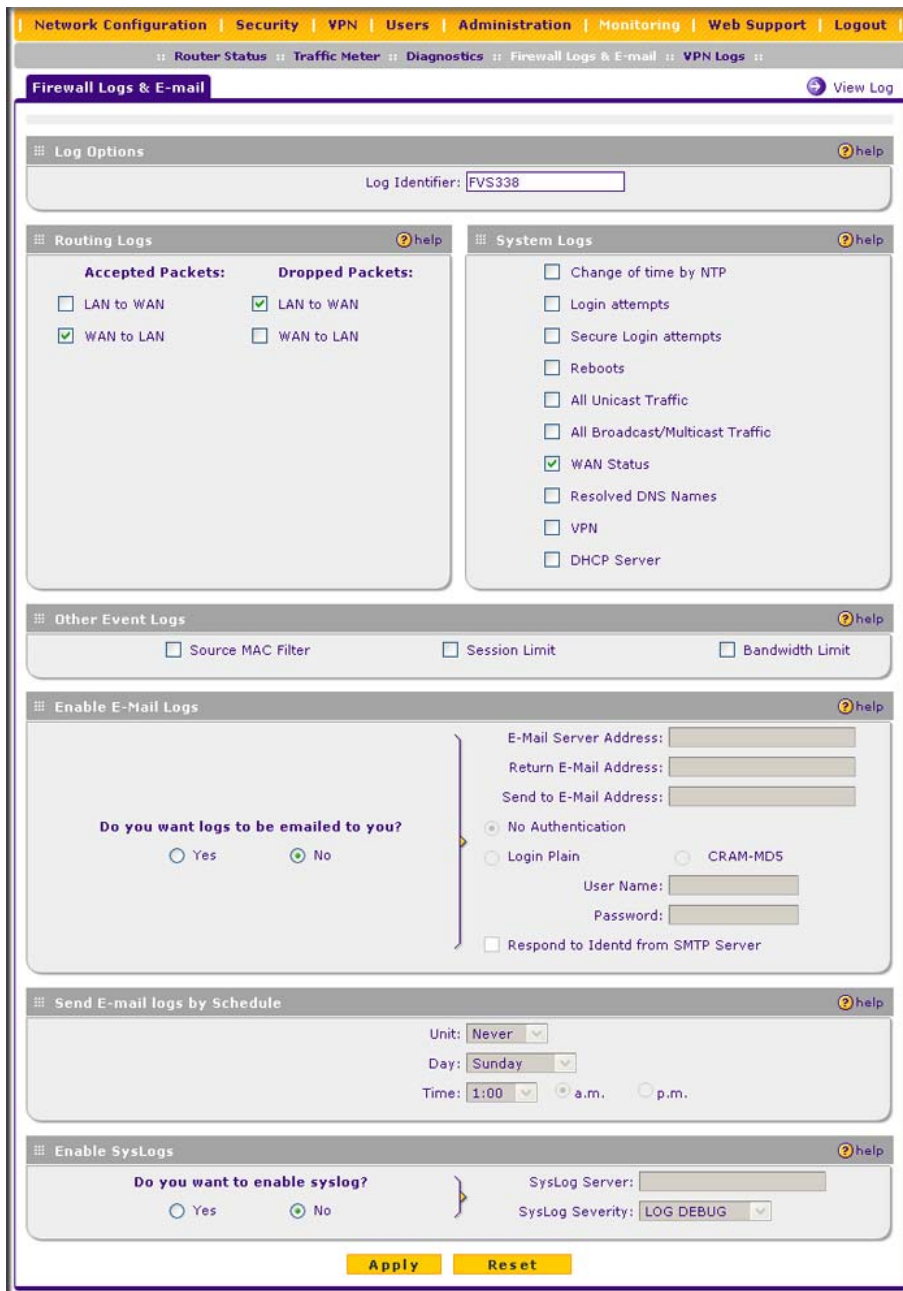


Figure 6-10

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 **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.

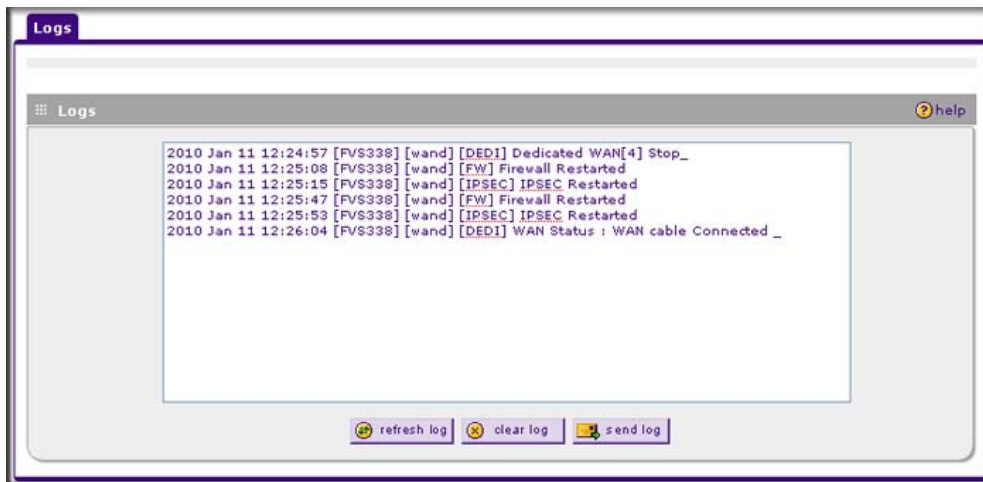


Figure 6-11

If the E-mail Logs option as been enabled, 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 on page 6-27](#). Refer to [Appendix B, “System Logs and Error Messages”](#) for more information about log entry messages.

**Table 6-2. Log Entry Descriptions**

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

To monitor traffic limits on each of the WAN ports:

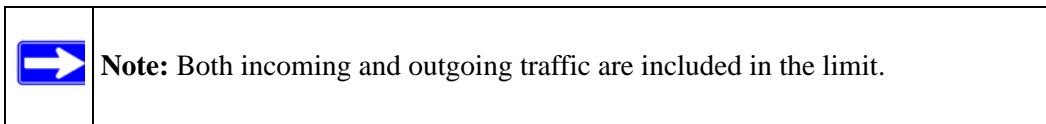
1. From the main menu, select **Monitoring**, and then select **Traffic Meter** from the submenu. The Broadband Traffic Meter screen will display (see [Figure 6-12 on page 6-28](#)).

The screenshot displays the 'Broadband Traffic Meter' configuration page. At the top, there is a navigation bar with tabs for Network Configuration, Security, VPN, Users, Administration, Monitoring, Web Support, and Logout. Below this is a secondary navigation bar with links for Router Status, Traffic Meter, Diagnostics, Firewall Logs & E-mail, and VPN Logs. The main content area is titled 'Broadband Traffic Meter' and includes a 'Traffic by Protocol' link. The 'Enable Traffic Meter' section contains a question 'Do you want to enable Traffic Metering on Broadband?' with 'Yes' selected. To the right, there are radio buttons for 'No Limit', 'Download only', and 'Both Directions' (selected). Below these are input fields for 'Monthly Limit' (250000 MB) and 'Increase this month limit by' (0 MB). The 'Traffic Counter' section has three options: 'Restart Traffic Counter Now', 'Restart Traffic Counter at Specific Time' (selected), and 'Send e-mail report before restarting counter'. The 'When Limit is Reached' section has three options: 'Block All Traffic' (selected), 'Block All Traffic Except E-Mail', and 'Send e-mail alert'. The 'Internet Traffic Statistics' section shows the following data: Start Date / Time: Wed Jan 1 12:00:00 2010; Outgoing Traffic Volume: 57 (MB); Incoming Traffic Volume: 174 (MB); Total Traffic Volume: 232 (MB); Average per day: 17; % of Standard Limit: 0; % of this Month's Limit: 0. At the bottom, there are 'Apply' and 'Reset' buttons.

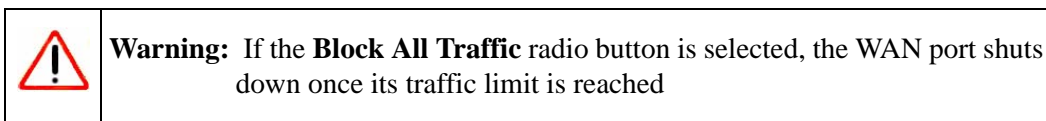
Figure 6-12

2. Enable the traffic meter by clicking the **Yes** radio button under **Do you want to enable Traffic Metering on Broadband?** The traffic meter will record the volume of Internet traffic passing through the broadband port. 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.



- **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.

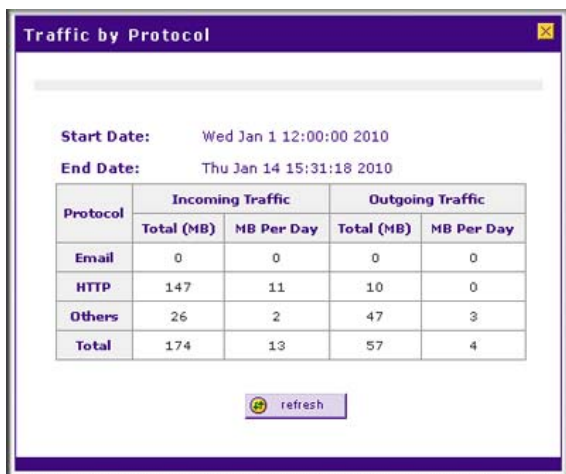


- **Block all traffic except E-mail.** Only e-mail traffic will be allowed. All other traffic will be blocked.
  - **Send E-mail alert.** You must configure the e-mail capability in order for this function to work (see [“Activating Notification of Events and Alerts”](#) on page 6-23).
5. Click **Apply** to save your settings.

To configure the traffic meter for the dial-up port, select the **Dial-up 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.



Protocol	Incoming Traffic		Outgoing Traffic	
	Total (MB)	MB Per Day	Total (MB)	MB Per Day
Email	0	0	0	0
HTTP	147	11	10	0
Others	26	2	47	3
Total	174	13	57	4

Figure 6-13

## Viewing the Router 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 6-14 on page 6-31](#)). 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.



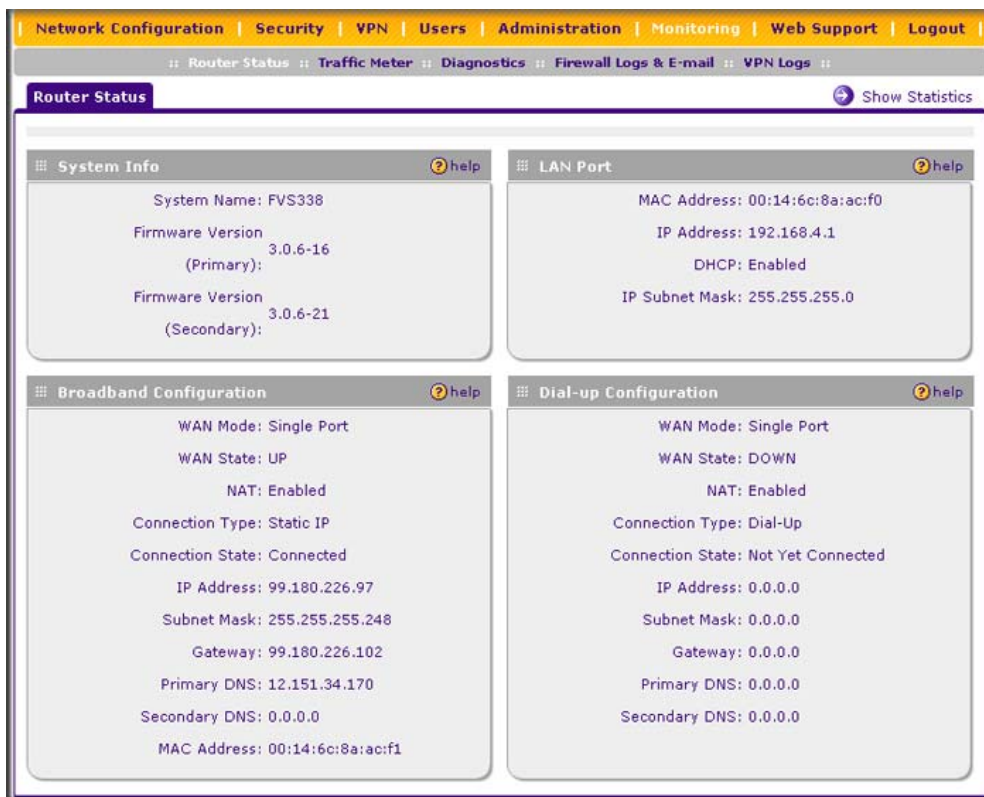


Figure 6-14

Table 6-3. Router Configuration Status Fields

Item	Description
System Name	This is the Account Name that you entered on the Broadband 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 on the LAN Setup screen. DHCP can be either Enabled or Disabled.

**Table 6-3. Router Configuration Status Fields (continued)**

Item	Description
Broadband Configuration	<ul style="list-style-type: none"> <li>• WAN Mode: Single, or Rollover.</li> <li>• WAN State: UP or DOWN.</li> <li>• NAT: Enabled or Disabled.</li> <li>• Connection Type: Static IP, DHCP, PPPoE, or PPTP.</li> <li>• Connection State: Connected or Disconnected.</li> <li>• WAN IP Address: The IP address of the WAN interface.</li> <li>• Subnet Mask: The IP subnet mask of the WAN interface.</li> <li>• Gateway: The gateway IP address for the WAN interface.</li> <li>• Primary DNS: The IP address of the primary DNS server for the WAN interface.</li> <li>• Secondary DNS: The IP address of the secondary DNS server for the WAN interface.</li> <li>• MAC Address: The MAC address of the WAN interface.</li> </ul>
Dialup Configuration	Displays the same details as for the broadband configuration with the exception that the Connection Type is always Dialup.

## 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 6-31](#)).
2. Click the **Show Statistics** link in the upper right-hand section of the screen. The Router Statistics screen will display.

The screenshot shows the 'Router Statistics' page. At the top, it says 'Operation succeeded.' Below that, 'System up Time: 3 Days 04:03:42'. The main part of the screen is a table titled 'Router Statistics' with a 'help' icon. The table has columns for Port, Tx Pkts, Rx Pkts, Collisions, Tx B/s, Rx B/s, and Up Time. The data is as follows:

Port	Tx Pkts	Rx Pkts	Collisions	Tx B/s	Rx B/s	Up Time
Broadband	139466	142809	0	125	330	3 Days 04:02:05
Dial-up						N/A
LAN	966493	54005	0	426	31	3 Days 04:04:08

At the bottom of the table, there is a 'Poll Interval' set to 5 seconds, with 'set interval' and 'stop' buttons.

**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 (broadband and dialup), 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 **Broadband Status** from the submenu. The Broadband 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 broadband port.



Figure 6-16

To get a status report on the dial-up port, click the **Dialup ISP Settings** tab, and then click the **Dialup 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**

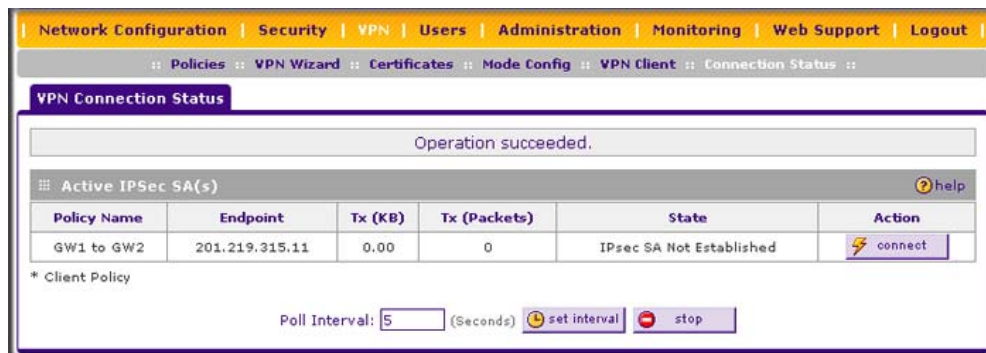
Item	Description
Name	The name of the PC or device. Sometimes, this can not be determined, and will be listed as Unknown. In this case, you can edit the entry to add a meaningful name.
IP Address	The current IP address. For DHCP clients, where the IP address is allocated by the DHCP Server in this device, 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**

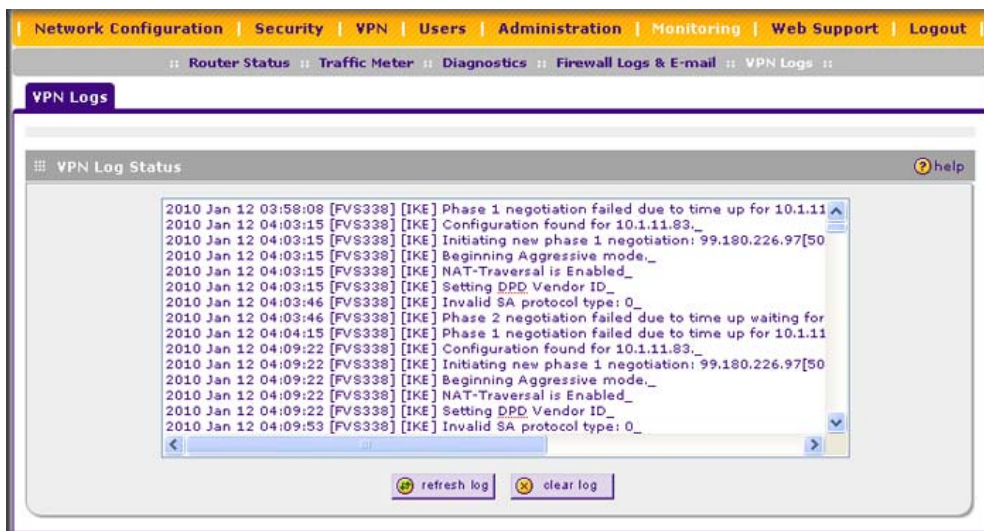
The Active IPsec (SA)s table lists each active connection with the following information

**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 display.
2. Click the **DHCP Log** link in the upper right-hand section of the screen. The DHCP Log popup screen will display.

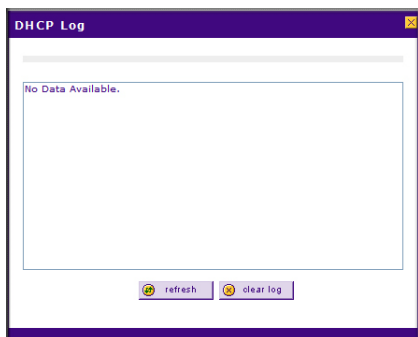


Figure 6-20

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 display.
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 50 FVS338. 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
- [“Performing Diagnostics”](#) 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 10 seconds, verify that:
  - a. The TEST LED is not lit.
  - b. The LAN port LEDs are lit for any local ports that are connected.
  - c. The Internet port LED is lit.

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

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

## Power LED Not On

If the Power and other LEDs are off when your 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 turn 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 screen 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](http://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 Broadband ISP Settings screen (see [Figure 2-5 on page 2-9](#)) or Dialup ISP Settings screen (see [Figure 2-4 on page 2-6](#)).
- 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 Broadband Advanced Options screen (see [Figure 2-8 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 on the Start button and select Run.
2. In the field provided, type Ping followed by the IP address of the VPN firewall, as in this example:

```
ping 192.168.1.1
```

3. Click on OK.

You should see a message like this one:

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

If the path is working, you see this message:

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

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

```
Request timed out
```

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

- Wrong physical connections
  - Make sure the LAN port LED is on. If the LED is off, follow the instructions in [“LAN or Internet Port LEDs Not On”](#) on page 7-2.
  - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and 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 Broadband ISP Settings screen (see [Figure 2-5 on page 2-9](#)) or Dialup ISP Settings screen (see [Figure 2-4 on page 2-6](#)).
- 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 Broadband Advanced Options screen (see [Figure 2-8 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:

- Use the Erase function of the VPN firewall (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.

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.”

## Performing Diagnostics

---

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.

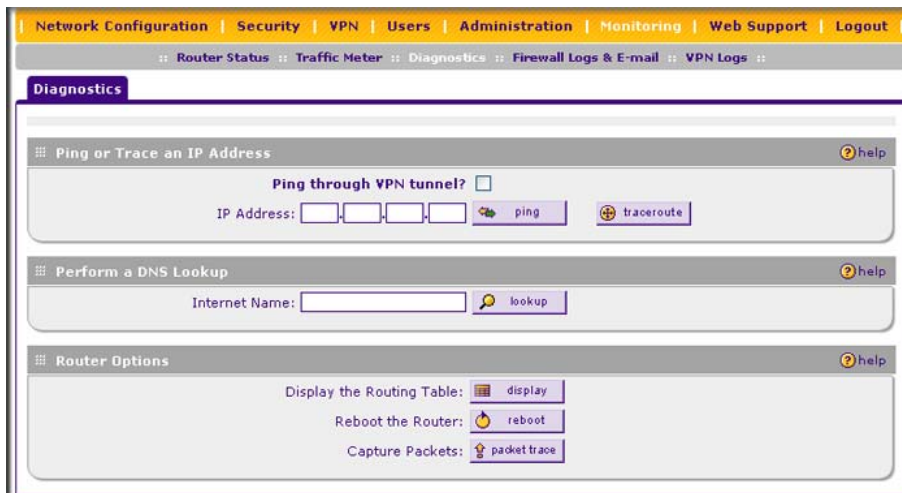
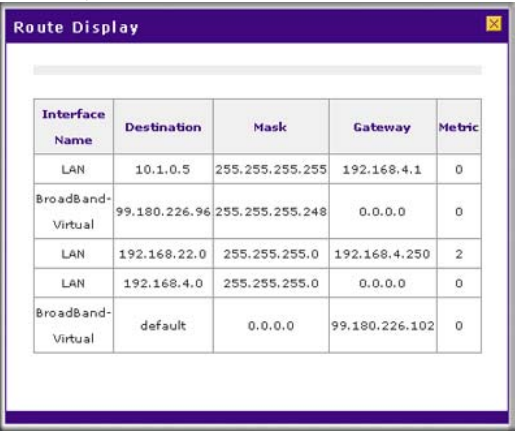


Figure 7-1



Table 7-1. Diagnostics Fields

Item	Description																														
Ping or Trace an IP address	<p>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 <b>Ping through VPN tunnel</b>.</p> <p>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.</p>																														
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	<p>This operation will display the internal routing table. This information is used, most often, by Technical Support.</p>  <table border="1" data-bbox="439 916 886 1170"> <thead> <tr> <th>Interface Name</th> <th>Destination</th> <th>Mask</th> <th>Gateway</th> <th>Metric</th> </tr> </thead> <tbody> <tr> <td>LAN</td> <td>10.1.0.5</td> <td>255.255.255.255</td> <td>192.168.4.1</td> <td>0</td> </tr> <tr> <td>BroadBand-Virtual</td> <td>99.180.226.96</td> <td>255.255.255.248</td> <td>0.0.0.0</td> <td>0</td> </tr> <tr> <td>LAN</td> <td>192.168.22.0</td> <td>255.255.255.0</td> <td>192.168.4.250</td> <td>2</td> </tr> <tr> <td>LAN</td> <td>192.168.4.0</td> <td>255.255.255.0</td> <td>0.0.0.0</td> <td>0</td> </tr> <tr> <td>BroadBand-Virtual</td> <td>default</td> <td>0.0.0.0</td> <td>99.180.226.102</td> <td>0</td> </tr> </tbody> </table>	Interface Name	Destination	Mask	Gateway	Metric	LAN	10.1.0.5	255.255.255.255	192.168.4.1	0	BroadBand-Virtual	99.180.226.96	255.255.255.248	0.0.0.0	0	LAN	192.168.22.0	255.255.255.0	192.168.4.250	2	LAN	192.168.4.0	255.255.255.0	0.0.0.0	0	BroadBand-Virtual	default	0.0.0.0	99.180.226.102	0
Interface Name	Destination	Mask	Gateway	Metric																											
LAN	10.1.0.5	255.255.255.255	192.168.4.1	0																											
BroadBand-Virtual	99.180.226.96	255.255.255.248	0.0.0.0	0																											
LAN	192.168.22.0	255.255.255.0	192.168.4.250	2																											
LAN	192.168.4.0	255.255.255.0	0.0.0.0	0																											
BroadBand-Virtual	default	0.0.0.0	99.180.226.102	0																											
Reboot the Router	<p>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.</p> <p><b>Note:</b> 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.</p>																														
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 Settings**

Feature	Default Behavior
<b>Router Login</b>	
User Login URL	http://192.168.1.1
User Name (case sensitive)	admin
Login Password (case sensitive)	password
<b>Internet Connection</b>	
WAN MAC Address	Use Default address
WAN MTU Size	1500
Port Speed	AutoSense
<b>Local Network (LAN)</b>	
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

**Table A-1. VPN Firewall Default Settings (continued)**

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

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

**Table A-2. VPN firewall Default Technical Specifications**

Feature		Specification
<b>Network Protocol and Standards Compatibility</b>		
	Data and Routing Protocols	TCP/IP, RIP-1, RIP-2, DHCP PPP over Ethernet (PPPoE)
<b>Power Adapter</b>		
	North America:	120V, 60 Hz, input
	United Kingdom, Australia:	240V, 50 Hz, input
	Europe:	230V, 50 Hz, input
	Japan:	100V, 50/60 Hz, input
<b>Physical Specifications</b>		
	Dimensions:	1.1 x 6.89 x 4.65 in.
	Weight:	0.3 kg (0.66 lb)

**Table A-2. VPN firewall Default Technical Specifications**

Feature	Specification
<b>Environmental Specifications</b>	
Operating temperature:	0° to 40° C (32° to 104° F)
Operating humidity:	90% maximum relative humidity, noncondensing
<b>Electromagnetic Emissions</b>	
Meets requirements of:	FCC Part 15 Class B VCCI Class B EN 55 022 (CISPR 22), Class B
<b>Interface Specifications</b>	
LAN:	10BASE-T or 100BASE-Tx, RJ-45
WAN:	10BASE-T or 100BASE-Tx, and 9-pin DIN Serial



# Appendix B

## System Logs and Error Messages

This appendix uses the following log parameter terms.

**Table B-1. Log Parameter Terms**

Term	Description
[FVS338]	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 B-2. System Logs: System Startup**

Message	Jan 1 15:22:28 [FVS338] [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 B-3. System Logs: Reboot**

Message	Nov 25 19:42:57 [FVS338] [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 B-4. System Logs: NTP**

Message	Nov 28 12:31:13 [FVS338] [ntpdate] Looking Up time-f.netgear.com Nov 28 12:31:13 [FVS338] [ntpdate] Requesting time from time-f.netgear.com Nov 28 12:31:14 [FVS338] [ntpdate] adjust time server 69.25.106.19 offset 0.140254 sec Nov 28 12:31:14 [FVS338] [ntpdate] Synchronized time with time-f.netgear.com Nov 28 12:31:16 [FVS338] [ntpdate] Date and Time Before Synchronization: Tue Nov 28 12:31:13 GMT+0530 2006 Nov 28 12:31:16 [FVS338] [ntpdate] Date and Time After Synchronization: Tue Nov 28 12:31:16 GMT+0530 2006 Nov 28 12:31:16 [FVS338] [ntpdate] Next Synchronization after 2 Hours
---------	---



**Table B-4. System Logs: NTP (continued)**

Explanation	<p>Message1: DNS resolution for the NTP server (time-f.netgear.com)</p> <p>Message2: request for NTP update from the time server.</p> <p>Message3: Adjust time by re-setting system time.</p> <p>Message4: Display date and time before synchronization, that is when resynchronization started</p> <p>Message5: Display the new updated date and time.</p> <p>Message6: Next synchronization will be after the specified time mentioned.</p> <p>Example: In the above logs the next synchronization will be after two hours.</p> <p>The synchronization time interval is configurable via the CLI</p>
Recommended Action	None

## Login/Logout

This section describes logs generated by the administrative interfaces of the device.

**Table B-5. System Logs: Login/Logout**

Message	Nov 28 14:45:42 [FVS338] [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	<p>Nov 28 14:55:09 [FVS338] [seclogin] Logout succeeded for user admin</p> <p>Nov 28 14:55:13 [FVS338] [seclogin] Login succeeded: user admin from 192.168.1.214</p>
Explanation	Secure login/logout of user admin from host with IP address 192.168.1.214.
Recommended Action	None

## VPN Firewall Restart

This logging is always done.

**Table B-6. System Logs: Firewall Restart**

Message	Jan 23 16:20:44 [FVS338] [wand] [FW] Firewall Restarted
Explanation	<p>Log generated when the firewall is restarted.</p> <p>This log is logged when firewall restarts after applying any changes in the configuration.</p>
Recommended Action	None

## IPSec Restart

This logging is always done.

**Table B-7. System Logs: IPSec Restart**

Message	Jan 23 16:20:44 [FVS338] [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 in Auto Rollover Mode.

### Auto Rollover

When WAN mode is configured to Auto Rollover, primary link is active and secondary acts as a backup. When primary link goes down, secondary becomes active until primary comes up. The device monitors the status of the primary link by 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 [FVS338] [wand] [LBFO] WAN1 Test Failed 1 of 3 times_ Nov 17 09:59:39 [FVS338] [wand] [LBFO] WAN1 Test Failed 2 of 3 times_ Nov 17 10:00:09 [FVS338] [wand] [LBFO] WAN1 Test Failed 3 of 3 times_ Nov 17 10:01:01 [FVS338] [wand] [LBFO] WAN1 Test Failed 4 of 3 times_ Nov 17 10:01:35 [FVS338] [wand] [LBFO] WAN1 Test Failed 5 of 3 times_ Nov 17 10:01:35 [FVS338] [wand] [LBFO] WAN1(DOWN), WAN2(UP), ACTIVE(WAN2)_ Nov 17 10:02:25 [FVS338] [wand] [LBFO] WAN1 Test Failed 6 of 3 times_ Nov 17 10:02:25 [FVS338] [wand] [LBFO] Restarting WAN1_ Nov 17 10:02:57 [FVS338] [wand] [LBFO] WAN1 Test Failed 7 of 3 times_ Nov 17 10:03:27 [FVS338] [wand] [LBFO] WAN1 Test Failed 8 of 3 times_ Nov 17 10:03:57 [FVS338] [wand] [LBFO] WAN1 Test Failed 9 of 3 times_ Nov 17 10:03:57 [FVS338] [wand] [LBFO] Restarting WAN1_
---------	--

**System Logs: WAN Status, Auto Rollover (continued)**

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 i.e. 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 B-8. System Logs: WAN Status, PPPoE Idle-Timeout**

Message	Nov 29 13:12:46 [FVS338] [pppd] Starting connection Nov 29 13:12:49 [FVS338] [pppd] Remote message: Success Nov 29 13:12:49 [FVS338] [pppd] PAP authentication succeeded Nov 29 13:12:49 [FVS338] [pppd] local IP address 50.0.0.62 Nov 29 13:12:49 [FVS338] [pppd] remote IP address 50.0.0.1 Nov 29 13:12:49 [FVS338] [pppd] primary DNS address 202.153.32.3 Nov 29 13:12:49 [FVS338] [pppd] secondary DNS address 202.153.32.3 Nov 29 11:29:26 [FVS338] [pppd] Terminating connection due to lack of activity. Nov 29 11:29:28 [FVS338] [pppd] Connect time 8.2 minutes. Nov 29 11:29:28 [FVS338] [pppd] Sent 1408 bytes, received 0 bytes. Nov 29 11:29:29 [FVS338] [pppd] Connection terminated.
---------	--

**Table B-8. System Logs: WAN Status, PPPoE Idle-Timeout (continued)**

Explanation	<p>Message 1: PPPoE connection establishment started.</p> <p>Message 2: Message from PPPoE server for correct login</p> <p>Message 3: Authentication for PPP succeeded.</p> <p>Message 4: Local IP address assigned by the server.</p> <p>Message 5: Server side IP address.</p> <p>Message 6: primary DNS configured in WAN status page.</p> <p>Message 7: secondary DNS configured in WAN status page.</p> <p>Message 8: The PPP link has transitioned to idle mode. This event occurs if there is no traffic from the LAN network.</p> <p>Message 9: The time in minutes for which the link has been up.</p> <p>Message 10: Data sent and received at the LAN side during the link was up.</p> <p>Message 11: PPP connection terminated after idle timeout</p>
Recommended Action	To reconnect during idle mode, initiate traffic from the LAN side.

**PPTP Idle-Timeout Logs.****Table B-9. System Logs: WAN Status, PPTP Idle-Timeout**

Message	<p>Nov 29 11:19:02 [FVS338] [pppd] Starting connection</p> <p>Nov 29 11:19:05 [FVS338] [pppd] CHAP authentication succeeded</p> <p>Nov 29 11:19:05 [FVS338] [pppd] local IP address 192.168.200.214</p> <p>Nov 29 11:19:05 [FVS338] [pppd] remote IP address 192.168.200.1</p> <p>Nov 29 11:19:05 [FVS338] [pppd] primary DNS address 202.153.32.2</p> <p>Nov 29 11:19:05 [FVS338] [pppd] secondary DNS address 202.153.32.2</p> <p>Nov 29 11:20:45 [FVS338] [pppd] No response to 10 echo-requests</p> <p>Nov 29 11:20:45 [FVS338] [pppd] Serial link appears to be disconnected.</p> <p>Nov 29 11:20:45 [FVS338] [pppd] Connect time 1.7 minutes.</p> <p>Nov 29 11:20:45 [FVS338] [pppd] Sent 520 bytes, received 80 bytes.</p> <p>Nov 29 11:20:51 [FVS338] [pppd] Connection terminated.</p>
Explanation	<p>Message 1: Starting PPP connection process</p> <p>Message 2: Message from server for authentication success</p> <p>Message 3: Local IP address assigned by the server.</p> <p>Message 4: Server side IP address.</p> <p>Message 5: primary DNS configured in WAN status page.</p> <p>Message 6: secondary DNS configured in WAN status page.</p> <p>Message 7: Sensing idle link</p> <p>Message 8: Idle link sensed</p> <p>Message 9: Data sent and received at the LAN side during the link was up.</p> <p>Message 10: PPP connection terminated after idle timeout</p>
Recommended Action	To reconnect during idle mode, initiate traffic from the LAN side.

**PPP Authentication Logs.****Table B-10. System Logs: WAN Status, PPP Authentication**

Message	Nov 29 11:29:26 [FVS338] [pppd] Starting link Nov 29 11:29:29 [FVS338] [pppd] Remote message: Login incorrect Nov 29 11:29:29 [FVS338] [pppd] PAP authentication failed Nov 29 11:29:29 [FVS338] [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, set value of keywordLog to 1 from CLI.

Command to set this value from CLI: monitor/firewallLogs/logger/loggerConfig keywordLog 1.

**Table B-11. System Logs: Web Filtering and Content Filtering**

Message	Jan 23 16:36:35 [FVS338] [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	<ul style="list-style-type: none"> <li>• This packet is blocked by keyword blocking</li> <li>• The URL blocked due to keyword blocking is shown by [URL] along with source and destination IP addressed, protocol, source port and destination port.</li> <li>• For other parameters, refer to <a href="#">Table B-1</a>.</li> </ul>
Recommended Action	None
Message	Jan 23 16:53:32 [FVS338] [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	<ul style="list-style-type: none"> <li>• This packet is blocked by content filtering with java components</li> <li>• The URL blocked due to java content filtering is [URL] along with source and destination IP addressed, protocol, source port and destination port.</li> <li>• For other parameters, refer to <a href="#">Table B-1</a>.</li> </ul>
Recommended Action	None
Message	Jan 23 16:56:08 [FVS338] [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

**Table B-11. System Logs: Web Filtering and Content Filtering (continued)**

Explanation	<ul style="list-style-type: none"> <li>This packet is blocked by content filtering for cookies</li> <li>The URL blocked due to cookie filtering shown by [URL] along with source and destination IP addressed, protocol, source port and destination port.</li> <li>For other parameters, refer to <a href="#">Table B-1</a>.</li> </ul>
Recommended Action	None
Message	Jan 23 16:53:32 [FVS338] [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	<ul style="list-style-type: none"> <li>This packet is blocked by content filtering with java components</li> <li>The URL blocked due to java content filtering is [URL] along with source and destination IP addressed, protocol, source port and destination port.</li> <li>For other parameters, refer to <a href="#">Table B-1</a>.</li> </ul>
Recommended Action	None

## Traffic Metering Logs

**Table B-12. 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 B-13. System Logs: Unicast**

Message	Nov 24 11:52:55 [FVS338] [kernel] UCAST IN=SELF OUT=WAN SRC=192.168.10.1 DST=192.168.10.10 PROTO=UDP SPT=800 DPT=2049
Explanation	<ul style="list-style-type: none"> <li>This packet (Unicast) is destined to the device from the WAN network.</li> <li>For other parameters, refer to <a href="#">Table B-1</a>.</li> </ul>
Recommended Action	None

## ICMP Redirect Logs

**Table B-14. System Logs: Unicast, Redirect**

Message	Feb 2007 22 14:36:07 [FVS338] [kernel] [LOG_PACKET] SRC=192.168.1.49 DST=192.168.1.124 PROTO=ICMP TYPE=5 CODE=1
Explanation	<ul style="list-style-type: none"> <li>This packet is ICMP Redirect message sent to the router by another router.</li> <li>For other parameters, refer to <a href="#">Table B-1</a>.</li> </ul>
Recommended Action	<p>To enable these logs, from CLI command prompt of the router, enter this command:</p> <pre>monitor/firewallLogs/logger/loggerConfig logIcmpRedirect 1</pre> <p>And to disable it,</p> <pre>monitor/firewallLogs/logger/loggerConfig logIcmpRedirect 0</pre>

## Multicast/Broadcast Logs

**Table B-15. System Logs: Multicast/Broadcast**

Message	Jan 1 07:24:13 [FVS338] [kernel] MCAST-BCAST IN=WAN OUT=SELF SRC=192.168.1.73 DST=192.168.1.255 PROTO=UDP SPT=138 DPT=138
Explanation	<ul style="list-style-type: none"> <li>This packet (Broadcast) is destined to the device from the WAN network.</li> <li>For other parameters, refer to <a href="#">Table B-1</a>.</li> </ul>
Recommended Action	None

## FTP Logging

**Table B-16. System Logs: FTP**

Message	<p>Feb 2007 22 14:46:56 [FVS338] [kernel] [FTP-ACTIVE] SRC=192.168.10.211 DST=192.168.1.97 PROTO=TCP SPT=1983 DPT=21</p> <p>Feb 2007 22 14:46:56 [FVS338] [kernel] [FTP-PASSIVE] SRC=192.168.10.211 DST=192.168.1.97 PROTO=TCP SPT=1984 DPT=21</p> <p>Feb 2007 22 19:48:17 [FVS338] [kernel] [FTP-DATA][ACCEPT] SRC=192.168.10.10 DST=192.168.20.10 PROTO=TCP SPT=54879 DPT=6459</p>
Explanation	<ul style="list-style-type: none"> <li>These packets are active and passive FTP session data transfers respectively.</li> <li>For other parameters, refer to <a href="#">Table B-1</a>.</li> </ul>
Recommended Action	<p>To enable these logs, from CLI command prompt of the router, enter this command:</p> <pre>monitor/firewallLogs/logger/loggerConfig logFtp 1</pre> <p>And to disable it,</p> <pre>monitor/firewallLogs/logger/loggerConfig logFtp 0</pre>

## Invalid Packet Logging

**Table B-17. System Logs: Invalid Packets**

Message	2007 Oct 1 00:44:17 [FVS338] [kernel] [INVALID] [NO_CONNTRACK_ENTRY] [DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=TCP SPT=23 DPT=54899
Explanation	No Connection Tracking entry exists
Recommended Action	<ol style="list-style-type: none"> <li>Invalid packets are dropped.</li> <li>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</li> </ol>
Message	2007 Oct 1 00:44:17 [FVS338] [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	<ol style="list-style-type: none"> <li>Invalid packets are dropped.</li> <li>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</li> </ol>
Message	2007 Oct 1 00:44:17 [FVS338] [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	<ol style="list-style-type: none"> <li>Invalid packets are dropped.</li> <li>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</li> </ol>
Message	2007 Oct 1 00:44:17 [FVS338] [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	<ol style="list-style-type: none"> <li>Invalid packets are dropped.</li> <li>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</li> </ol>



**Table B-17. System Logs: Invalid Packets (continued)**

Message	2007 Oct 1 00:44:17 [FVS338] [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	<ol style="list-style-type: none"> <li>Invalid packets are dropped.</li> <li>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</li> </ol>
Message	2007 Oct 1 00:44:17 [FVS338] [kernel] [INVALID][BAD_HW_CHECKSUM][DROP] SRC=192.168.20.10 DST=192.168.20.2 PROTO=ICMP TYPE=3 CODE=0
Explanation	Bad Hardware Checksum for ICMP packets
Recommended Action	<ol style="list-style-type: none"> <li>Invalid packets are dropped.</li> <li>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</li> </ol>
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	<ol style="list-style-type: none"> <li>Invalid packets are dropped.</li> <li>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</li> </ol>
Message	2007 Oct 1 00:44:17 [FVS338] [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	<ol style="list-style-type: none"> <li>Invalid packets are dropped.</li> <li>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</li> </ol>
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

**Table B-17. System Logs: Invalid Packets (continued)**

Recommended Action	<ol style="list-style-type: none"> <li>Invalid packets are dropped.</li> <li>Use this command to enable dropping and logging of the invalid packets:  <code>fw/rules/attackChecks/configure dropInvalid 1</code>  To allow invalid packet and disable logging:  <code>fw/rules/attackChecks/configure dropInvalid 0</code> </li> </ol>
Message	2007 Oct 1 00:44:17 [FVS338] [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
Recommended Action	<ol style="list-style-type: none"> <li>Invalid packets are dropped.</li> <li>Use this command to enable dropping and logging of the invalid packets:  <code>fw/rules/attackChecks/configure dropInvalid 1</code>  To allow invalid packet and disable logging:  <code>fw/rules/attackChecks/configure dropInvalid 0</code> </li> </ol>
Message	2007 Oct 1 00:44:17 [FVS338] [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	<ol style="list-style-type: none"> <li>Invalid packets are dropped.</li> <li>Use this command to enable dropping and logging of the invalid packets:  <code>fw/rules/attackChecks/configure dropInvalid 1</code>  To allow invalid packet and disable logging:  <code>fw/rules/attackChecks/configure dropInvalid 0</code> </li> </ol>
Message	2007 Oct 1 00:44:17 [FVS338] [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	<ol style="list-style-type: none"> <li>Invalid packets are dropped.</li> <li>Use this command to enable dropping and logging of the invalid packets:  <code>fw/rules/attackChecks/configure dropInvalid 1</code>  To allow invalid packet and disable logging:  <code>fw/rules/attackChecks/configure dropInvalid 0</code> </li> </ol>

## 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 B-18. Routing Logs: LAN to WAN**

Message	Nov 29 09:19:43 [FVS338] [kernel] LAN2WAN[ACCEPT] IN=LAN OUT=WAN SRC=192.168.10.10 DST=72.14.207.99 PROTO=ICMP TYPE=8 CODE=0
Explanation	<ul style="list-style-type: none"><li>• This packet from LAN to WAN has been allowed by the firewall.</li><li>• For other parameters, refer to <a href="#">Table B-1</a>.</li></ul>
Recommended Action	None

## WAN to LAN Logs

**Table B-19. Routing Logs: WAN to LAN**

Message	Nov 29 10:05:15 [FVS338] [kernel] WAN2LAN[ACCEPT] IN=WAN OUT=LAN SRC=192.168.1.214 DST=192.168.10.10 PROTO=ICMP TYPE=8 CODE=0
Explanation	<ul style="list-style-type: none"><li>• This packet from LAN to WAN has been allowed by the firewall</li><li>• For other parameters, refer to <a href="#">Table B-1</a>.</li></ul>
Recommended Action	None



# Appendix C

## 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 C-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 C-1

2. A one-time passcode (*something they have*) is generated for this user.



Figure C-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 screen and enters the generated one-time passcode as the login password.

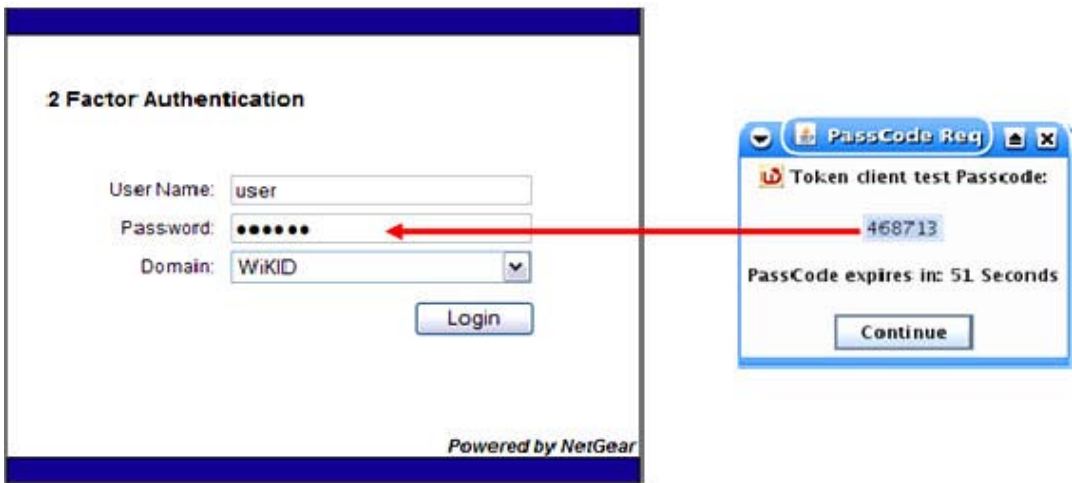


Figure C-3



# Appendix D

## 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	<a href="http://documentation.netgear.com/reference/enu/tcpip/index.htm">http://documentation.netgear.com/reference/enu/tcpip/index.htm</a>
Wireless Networking Basics	<a href="http://documentation.netgear.com/reference/enu/wireless/index.htm">http://documentation.netgear.com/reference/enu/wireless/index.htm</a>
Preparing Your Network	<a href="http://documentation.netgear.com/reference/enu/wsdhcp/index.htm">http://documentation.netgear.com/reference/enu/wsdhcp/index.htm</a>
Virtual Private Networking Basics	<a href="http://documentation.netgear.com/reference/enu/vpn/index.htm">http://documentation.netgear.com/reference/enu/vpn/index.htm</a>
Glossary	<a href="http://documentation.netgear.com/reference/enu/glossary/index.htm">http://documentation.netgear.com/reference/enu/glossary/index.htm</a>



## Numerics

3322.org [2-14](#)

## A

Add LAN WAN Inbound Service screen [4-9](#)

Add LAN WAN Outbound Service screen [4-9](#)

address reservation [3-9](#)

Advanced Options

MTU Size [2-17](#)

Port Speed [2-17](#)

Router's MAC Address [2-17](#)

AH

VPN Policies, use with [5-19](#)

ALG [4-19](#)

Application Level Gateway. *See* ALG.

ARP broadcast

enable [3-5](#)

Attack Checks

Block TCP Flood [4-16](#)

Respond To Ping On Internet [4-16](#)

Stealth Mode [4-16](#)

Attack Checks screen [4-15](#), [4-16](#)

authentication

WiKID [6-11](#)

Authentication Header. *See* AH.

Auto Uplink [1-3](#)

Auto VPN Policies [5-18](#)

Auto-Rollover

Dual WAN ports [5-1](#)

## B

Back up settings [6-18](#)

backup and restore settings

configuration of [6-19](#)

bandwidth capacity [6-1](#)

LAN side [6-1](#)

WAN side [6-1](#)

Bandwidth Profile screen [4-23](#)

Block Sites [6-3](#)

Content Filtering [4-26](#)

reducing traffic [6-3](#)

Block Sites screen

Content Filtering [4-27](#)

Block TCP Flood

Attack Checks [4-16](#)

block traffic

with schedule [4-25](#)

Broadband Status

monitoring [6-33](#)

## C

CA [5-18](#)

about [5-20](#)

certificate

generate new CSR [5-22](#)

Certificate Authority. *See* CA

Certificate Signing Request, *see* CSR

certificates

management of [5-22](#)

Certificates screen [5-21](#)

CLI management

by Telnet [6-15](#)

common protocols

definitions [4-20](#)

configuration

automatic by DHCP [1-4](#)

connecting the VPN firewall [2-1](#)

Content Filtering [1-2, 4-1](#)  
  Block Sites [4-26](#)  
  enabling [4-27](#)  
  Keyword Blocking [4-27](#)  
  Web Components [4-26](#)  
content filtering  
  Blocked Sites [4-1](#)  
  Keyword Blocking [4-1](#)  
crossover cable [1-3, 7-2](#)  
CSR [5-22](#)  
Customized Services [4-3](#)  
  service port numbers [4-20](#)

## D

date  
  troubleshooting [7-7](#)  
Daylight Savings Time  
  setting [6-22](#)  
DDNS  
  about [2-14](#)  
  providers of [2-14](#)  
Dead Peer Detection [5-17, 5-43](#)  
default configuration  
  restoring [7-7](#)  
default firewall rules [4-2](#)  
  Inbound [4-2](#)  
  Outbound [4-2](#)  
Default Outbound Policy  
  LAN WAN [4-8](#)  
denial of service attack [4-16](#)  
  UDP flood [4-17](#)  
Denial of Service. See DoS.  
DH  
  use with ModeConfig [5-34](#)  
DHCP  
  DNS server address [3-4](#)  
DHCP Address Pool [3-4](#)  
DHCP IP Address pool [3-1](#)  
DHCP log [6-37](#)  
  monitoring [6-37](#)  
DHCP server  
  about [3-1](#)

  address pool [3-4](#)  
  enable [3-4](#)  
  lease time [3-5](#)  
Diagnostics  
  DNS lookup [7-8](#)  
  Packet Trace [7-9](#)  
  pinging an IP address [7-8](#)  
  Reboot the Router [7-9](#)  
Diagnostics Fields  
  descriptions of [7-9](#)  
Diagnostics screen [7-8](#)  
Dialup ISP Status  
  monitoring [6-33](#)  
Dial-up Traffic Meter [6-30](#)  
Diffie-Hellman Group  
  use in IKE Policy [5-17](#)  
Digital [5-19](#)  
Digital Certificates [5-19](#)  
Disable DHCP Server [3-1](#)  
DNS  
  server IP address [3-4](#)  
DNS lookup [7-8](#)  
DNS Proxy [1-4](#)  
DNS proxy [6-5](#)  
Domain Name Blocking [4-27, 6-3](#)  
Domain Name Servers. See DNS.  
DOS protection  
download firmware  
  steps to [6-20](#)  
Dual WAN Port systems  
  VPN Tunnel addresses [5-2](#)  
Dynamic DNS  
  configuration of [2-14](#)  
Dynamic DNS Configuration screen [2-14](#)  
Dynamic DNS. See DDNS  
DynDNS.org [2-14](#)

## E

Edge Device  
  XAUTH, use with [5-26](#)

Edit Group Names [3-9](#)  
 Edit Service screen [4-22](#)  
 E-mail alerts [6-23](#)  
 E-mail logs, enabling notification [4-36](#)  
 E-mail Server address [6-25](#)  
 Enable ARP Broadcast [3-5](#)  
 Enable DHCP server [3-1](#)  
 Enable LDAP Information [3-5](#)  
 Encapsulating Security Payload. See ESP.  
 Ending IP Address  
   DHCP Address Pool [3-4](#)  
 ESP  
   VPN Policies, use with [5-19](#)  
 Ethernet [1-3](#)  
 Event Logs  
   emailing of [6-23](#)  
 Exposed Host [4-13](#)  
 Extended Authentication. See XAUTH.

## F

factory default settings  
   revert to [6-18](#)  
 filtering traffic  
   by MAC address  
     Source MAC filtering [4-29](#)  
 firewall  
   alerts, emailing of [6-23](#)  
   connecting [2-2](#), [2-3](#)  
   logging in to [2-2](#)  
   rear panel [1-7](#)  
   security, about [4-1](#)  
   status [6-30](#)  
   technical specifications [A-1](#)  
 firewall access  
   remote management [6-14](#)  
 Firewall Logs  
   emailing of [4-36](#), [6-23](#)  
   setting up [6-23](#)  
 Firewall Logs & E-mail screen [4-36](#), [6-23](#)  
 firewall protection [4-1](#)  
 firewall rules

  about [4-2](#)  
   ordering [4-8](#)  
 fragmented IP packets [6-5](#)

## G

Group Names  
   editing [3-9](#)  
 Groups  
   managing [3-6](#)  
   rules, covered by [6-3](#)  
 Groups and Hosts  
   About [3-6](#)

## I

ICMP Destination Unreachable [4-17](#)  
 IKE Policies  
   auto, rules of [5-16](#)  
   field definitions [5-16](#)  
   manual, rules of [5-16](#)  
   use with ModeConfig [5-35](#)  
 IKE/ISAKMP  
   use in IKE Policy [5-17](#)  
 Inbound Rules [4-2](#)  
   about [4-4](#)  
   configuring DHCP [4-5](#)  
   examples of [4-11](#)  
   Fields, definition of [4-5](#)  
   firewall [4-2](#)  
   Port Forwarding [4-4](#)  
 Inbound Service Rule  
   modifying [4-10](#)  
 Increased Traffic  
   Port Triggering [6-6](#)  
 Increased traffic  
   Port Forwarding [6-4](#)  
   VPN tunnels [6-6](#)  
 installation [1-4](#)  
 Installation, instructions for [2-1](#)  
 Internet  
   configuring the connection manually [2-9](#)  
   connection configuration [2-3](#)  
   traffic information [6-37](#)

Internet Protocol Numbers [4-20](#)

IP Address Pool

use with ModeConfig [5-34](#)

IP addresses

auto-generated [7-3](#)

DHCP address pool [3-1](#)

how to assign [3-1](#)

reserved [3-9](#)

IP/MAC Binding screen [4-32](#)

IPSec [4-17](#)

Connection Status Fields, description of [6-36](#)

IPSec Connection Status screen [6-35](#)

IPSec Host

authentication [5-29](#)

XAUTH, use with [5-27](#), [5-29](#)

IPsec Host

XAUTH, with ModeConfig [5-37](#)

ISP connection

troubleshooting [7-4](#)

## K

Keep alive [5-19](#)

Keep Connected

Idle Timeout [2-10](#)

Idle Timeout [2-10](#)

keepalive, VPN [5-42](#)

Keyword Blocking [6-3](#)

applying [4-29](#)

Content Filtering [4-27](#)

examples of [4-27](#)

## L

L2TP [4-17](#)

LAN

configuration [3-1](#)

ports and attached devices [6-37](#)

using LAN IP setup options [3-2](#)

LAN Groups menu [3-7](#)

LAN Security Checks

UDP flood [4-17](#)

LAN Setup screen [3-3](#), [6-37](#)

LAN side

bandwidth capacity [6-1](#)

LAN Users

Service Blocking [6-2](#)

LAN WAN Inbound Rules

configuring [4-9](#)

LAN WAN Inbound Services Rules

about [4-9](#)

add [4-9](#)

LAN WAN Rules

about [4-8](#)

LAN WAN Rules screen [4-8](#)

LDAP

overview [3-5](#)

lease time [3-5](#)

LEDs

explanation of [1-6](#)

troubleshooting [7-2](#)

LEDs Never Turn Off [7-2](#)

Lightweight Directory Access Protocol. *See* LDAP.

Local Public Web Server [4-11](#)

Log Entry Descriptions [6-27](#), [B-1](#)

Logs screen [6-26](#)

## M

MAC address [7-7](#)

format of [2-17](#)

spoofing [7-5](#)

main menu [2-3](#)

Manual VPN Policies

creating [5-18](#)

Mode Config screen [5-33](#)

ModeConfig

about [5-32](#)

configuration example [5-32](#)

guidelines [5-32](#)

VPN Client configuration, example [5-38](#)

modem [1-2](#)

monitoring devices [6-34](#)

by DHCP Client Requests [6-34](#)

by Scanning the Network [3-6](#), [6-34](#)

MTU Size [2-17](#)

multi-NAT [4-12](#)

## N

NAS

Identifier [5-31, 6-12](#)

NAT [4-1, 4-4](#)

multi-NAT [4-12](#)

NetBIOS bridging over VPN [5-44](#)

Network [4-1](#)

Network Access Server. See NAS.

Network Address Translation [1-3](#)

Network Address Translation. See NAT.

Network Database

creating [3-6](#)

Network Database Group Names screen [3-9](#)

Network Time Protocol. See NTP.

newsgroup [4-27](#)

NTP

servers, configuring [6-21](#)

troubleshooting [7-7](#)

NTP Servers

custom [6-22](#)

default [6-22](#)

## O

one-time passcode. See OTP.

One-to-One NAT Mapping [4-12](#)

option arrow [2-3](#)

Oray.net [2-14](#)

OTP [C-1, C-2](#)

Outbound Rules [4-3](#)

examples of [4-14](#)

Fields, description of [4-3](#)

firewall [4-2](#)

port filtering [4-3](#)

service blocking [4-3](#)

Outbound Service Rule

modifying [4-10](#)

## P

package contents [1-5](#)

Packet Trace [7-9](#)

Passwords

restoring [7-7](#)

passwords and login timeout

changing [6-8](#)

performance management [6-1](#)

Ping

Troubleshooting TCP/IP [7-5](#)

ping [7-9](#)

pinging an IP address [7-8](#)

port filtering [4-3](#)

Outbound Rules [4-3](#)

Port Forwarding [4-2, 4-4, 6-4](#)

Inbound Rules [4-4](#)

port forwarding [6-4](#)

port numbers [4-20](#)

port service numbers

common protocols [4-20](#)

Port Speed [2-17](#)

Port Triggering [6-6](#)

about [4-33](#)

guidelines [4-33](#)

Status [4-35](#)

status [6-37](#)

Port Triggering screen [4-34, 6-37](#)

Power LED Not On [7-2](#)

PPP over Ethernet [1-4](#)

PPPoE [1-4](#)

PPTP [4-17](#)

protocols

Routing Information [1-3](#)

## Q

QoS [4-3](#)

about [4-22](#)

managing, shifting traffic mix [6-7](#)

service levels [4-22](#)

Quality of Service. See QoS

## R

### RADIUS

description [6-11](#)

WiKID [6-11](#)

RADIUS Client screen [5-30](#)

### RADIUS server

configuring [5-30](#)

### RADIUS-CHAP

XAUTH, use with [5-27](#), [5-29](#)

### RADIUS-PAP

XAUTH, use with [5-27](#), [5-29](#)

Reboot the Router [7-9](#)

### reducing traffic

Block Sites [6-2](#)

Service Blocking [6-2](#)

Source MAC filtering [6-2](#)

remote management [6-14](#)

access [6-14](#)

### Reserved IP address

about [3-9](#)

### reserved IP address

restrictions [3-8](#)

Reserved IP addresses [3-9](#)

### Respond To Ping On Internet Ports

Attack Checks [4-16](#)

Restore saved settings [6-18](#)

Return E-mail Address [6-25](#)

### RFC 1349

ToS [4-22](#)

### RFC 2453

RIP [3-14](#)

### RIP [1-3](#)

about [3-14](#)

enabling [3-14](#)

RIP Configuration screen [3-14](#)

### router

upgrade software [6-20](#)

Router Status [6-30](#)

Router Status screen [6-30](#)

Router's MAC Address [2-17](#)

Routing Information Protocol. See RIP

Routing log messages [B-12](#)

Routing screen [3-11](#)

### rules

allowing traffic [4-2](#)

blocking traffic [4-2](#)

service blocking [4-3](#)

services-based [4-2](#)

running tracert [6-16](#)

## S

### Schedule

rules, covered by [6-3](#)

### schedule

blocking traffic [4-25](#)

Schedule 1 screen [4-25](#)

Security [1-3](#)

self certificate request [5-22](#)

Send To E-mail Address [6-25](#)

Service Blocking [4-3](#), [6-2](#)

LAN Users [6-2](#)

rules [6-2](#)

WAN Users [6-2](#)

service blocking [4-3](#)

### Services

common protocol numbers [4-20](#)

rules, covered by [6-3](#)

Services screen [4-21](#)

Session Initiation Protocol. See SIP.

Session Limits screen [4-18](#)

Settings Backup & Upgrade screen [6-18](#)

Simple Network Management Protocol. See SNMP.

SIP [4-19](#)

### 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 [4-29](#)

Source MAC Filtering [4-29](#), [6-4](#)



- enabling [4-29](#)
- reducing traffic [6-4](#)
- spoof MAC address [7-5](#)
- spoofing
  - UDP flood [4-17](#)
- Starting IP Address
  - DHCP Address Pool [3-4](#)
- stateful packet inspection [1-2, 4-1](#)
- Static Route
  - example of [3-13](#)
- static routes
  - configuring [3-11](#)
  - example [3-13](#)
- Stealth Mode
  - Attack Checks [4-16](#)
- stealth mode [6-5](#)
- submenu [2-3](#)
- SYN flood [6-5](#)
  - denial of service attack [4-16](#)
- Syslog Server [6-25](#)
- System log messages [B-1](#)

## T

- tab, menu [2-3](#)
- TCP flood
  - special rule [6-5](#)
- TCP/IP
  - network, Troubleshooting [7-5](#)
- time
  - daylight savings [7-8](#)
  - troubleshooting [7-7](#)
- Time Zone
  - setting of [6-21](#)
- Time Zone screen [6-21](#)
- ToS
  - service levels [4-22](#)
  - used with QoS [4-22](#)
- tracert
  - use with DDNS [6-16](#)
- Traffic
  - features that increase [6-4](#)

- management of [6-7](#)
  - reducing [6-2](#)
- traffic meter [2-18](#)
- Troubleshooting [7-1](#)
  - Date and Time [7-8](#)
  - ISP connection [7-4](#)
  - LEDs [7-2](#)
  - LEDs Never Turn Off [7-2](#)
  - NTP [7-7](#)
  - Power LED Not On [7-2](#)
  - Web configuration [7-3](#)
- Trusted Certificates [5-21](#)
  - about [5-21](#)
- Trusted Domains
  - building list of [4-29](#)
- two-factor authentication
  - WiKID [6-11](#)
- Two-Factor Authentication. *See* WiKID.
- TZO.com [2-14](#)

## U

- UDP flood
  - denial of service attack [4-17](#)
  - special rule [6-5](#)
- User Database
  - configuring [5-29](#)
  - editing user [5-30](#)
  - XAUTH, use with [5-29](#)
- User Database screen [5-29](#)

## V

- Videoconferencing
  - from restricted addresses [4-12](#)
- Virtual Private Networking. *See* VPN
- VoIP (voice over IP) sessions [4-19](#)
- VPN
  - activity, monitoring [6-36](#)
- VPN Client
  - configuring [5-6](#)
- VPN firewall
  - connecting [2-1](#)

VPN Logs screen [6-36](#)  
VPN Pass through [4-17](#)  
VPN Policies  
    about [5-18](#)  
    Auto [5-18](#)  
    Manual method [5-18](#)  
VPN Policies screen [5-5, 5-8](#)  
VPN policy  
    rules of use [5-18](#)  
VPN Tunnel  
    connection status, monitoring [6-35](#)  
VPN Tunnel addresses  
    Dual WAN Port systems [5-2](#)  
VPN Tunnels [6-6](#)  
VPN tunnels  
    IPSec [4-17](#)  
    L2TP [4-17](#)  
    PPTP [4-17](#)  
VPN Wizard  
    Gateway tunnel [5-2](#)  
    VPN Client, configuring [5-6](#)  
VPNC [5-2](#)

## W

WAN  
    configuring Advanced options [2-16](#)  
    port connection status [6-37](#)  
WAN Ports Status  
    monitoring [6-33](#)  
WAN side  
    bandwidth capacity [6-1](#)  
WAN Users  
    Service Blocking [6-2](#)  
Web Component Blocking [6-4](#)  
Web Components  
    blocking [4-29](#)  
    content filtering [4-26](#)  
Web configuration  
    troubleshooting [7-3](#)  
WiKID [6-11](#)  
    authentication, overview [C-1](#)

## X

XAUTH  
    about [5-26](#)  
    configuring [5-27](#)  
    Edge Device [5-26](#)  
    IPSec Host [5-27](#)  
    RADIUS-CHAP [5-27](#)  
    RADIUS-PAP [5-27](#)  
    User Database [5-29](#)