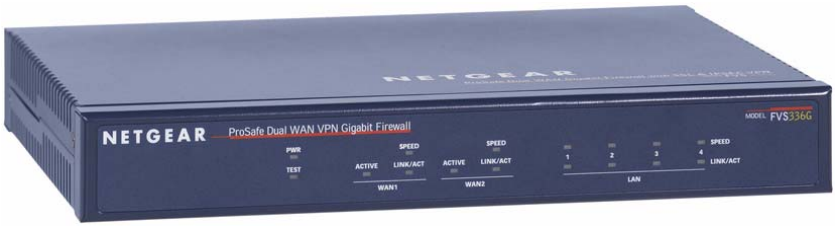
ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN FVS336G Reference Manual



NETGEAR®

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

March 2009
202-10257-04
v1.0

Trademarks

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

Statement of Conditions

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

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

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

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

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

EU Regulatory Compliance Statement

The ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN 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 Dual WAN Gigabit Firewall with SSL & IPsec VPN 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 Dual WAN Gigabit Firewall with SSL & IPsec VPN has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some

equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

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

Voluntary Control Council for Interference (VCCI) Statement

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

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

Read instructions for correct handling.

Additional Copyrights

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

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

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

Product and Publication Details

Model Number:	FVS336G
Publication Date:	March 2009
Product Family:	VPN Firewall
Product Name:	ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10257-04
Publication Version Number	1.0

Contents

About This Manual

The *NETGEAR® ProSafe™ Dual WAN Gigabit Firewall with SSL & IPsec VPN Reference Manual* describes how to install, configure and troubleshoot a ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN. The information in this manual is intended for readers with intermediate computer and networking 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:

Italic	Emphasis, books, CDs, file and server names, extensions
Bold	User input, IP addresses, GUI screen text
`Fixed`	Command prompt, CLI text, code
italic	URL links

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

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

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

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

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

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

Note: Product updates are available on the NETGEAR, Inc. website at *http://kbserver.netgear.com/products/FVS336G.asp*.

Revision History

Part Number	Version Number	Date	Description
202-10257-01	1.0	October 2007	First publication
202-10257-02	1.1	November 2007	Text corrections
202-10257-03	1.2	June 2008	Updated to align with router firmware update.
202-10257-04	1.0	March 2009	Adds these corrections and topics for the March 2009 firmware maintenance release: • WIKID 2 factor authentication • SIP AGL support • DHCP Relay support • Update VPN configuration procedure topics • Update the Certificate management topic • Correct the firewall scheduling topic

Chapter 1
Introduction

The ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN connects your local area network (LAN) to the Internet through one or two external broadband access devices such as cable modems or DSL modems. Dual wide area network (WAN) ports allow you to increase throughput to the Internet by using both ports together, or to maintain a backup connection in case of failure of your primary Internet connection.

As a complete security solution, the FVS336G incorporates a powerful and flexible firewall to safeguard your network, while providing advanced IPsec and SSL VPN technologies for secure and simple remote connections.

The use of Gigabit Ethernet LAN and WAN ports ensures extremely high data transfer speeds

The FVS336G is a plug-and-play device that can be installed and configured within minutes.

This chapter contains the following sections:

Key Features

The VPN firewall provides the following key features:

- Dual 10/100/1000 Mbps Gigabit Ethernet WAN ports for load balancing or failover protection of your Internet connection, providing increased system reliability or increased throughput.
- Built-in four-port 10/100/1000 Mbps Gigabit Ethernet LAN switch for extremely fast data transfer between local network resources.
- Advanced IPsec and SSL VPN support.
- Advanced stateful packet inspection (SPI) firewall with multi-NAT support.

- Easy, web-based setup for installation and management.
- Front panel LEDs for easy monitoring of status and activity.
- Flash memory for firmware upgrade.
- Internal universal switching power supply.

Dual WAN Ports for Increased Reliability or Outbound Load Balancing

The FVS336G has two broadband WAN ports. The second WAN port allows you to connect a second broadband Internet line that can be configured on a mutually-exclusive basis to:

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

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

- Single or multiple exposed hosts.
- Virtual private networks.

Advanced VPN Support for Both IPsec and SSL

The VPN firewall supports IPsec and SSL virtual private network (VPN) connections.

- IPsec VPN delivers full network access between a central office and branch offices, or between a central office and telecommuters. Remote access by telecommuters requires the installation of VPN client software on the remote computer.
  - IPsec VPN with broad protocol support for secure connection to other IPsec gateways and clients.
  - Bundled with the single-user license of the NETGEAR ProSafe VPN Client software (VPN01L)
  - Supports 25 concurrent IPsec VPN tunnels.
- SSL VPN provides remote access for mobile users to selected corporate resources without requiring a pre-installed VPN client on their computers.
  - Uses the familiar Secure Sockets Layer (SSL) protocol, commonly used for e-commerce transactions, to provide client-free access with customizable user portals and support for a wide variety of user repositories.

– Browser based, platform-independent, remote access through a number of popular browsers, such as Microsoft Internet Explorer or Apple Safari.

– Provides granular access to corporate resources based upon user type or group membership.

– Supports 10 concurrent SSL VPN sessions.

A Powerful, True Firewall with Content Filtering

Unlike simple Internet sharing NAT routers, the FVS336G is a true firewall, using stateful packet inspection (SPI) to defend against hacker attacks. Its firewall features include:

- Automatically detects and thwarts denial of service (DoS) attacks such as Ping of Death and SYN Flood.
- 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.
- Prevents objectionable content from reaching your PCs. You can control access to Internet content by screening for Web services, Web addresses, and keywords within Web addresses. You can configure the firewall to log and report attempts to access objectionable Internet sites.
- Permits scheduling of firewall policies by day and time.
- Logs security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the firewall to email the log to you at specified intervals. You can also configure the firewall to send immediate alert messages to your email address or email pager whenever a significant event occurs.

Autosensing Ethernet Connections with Auto Uplink

With its internal 4-port 10/100/1000 Mbps switch and dual 10/100/1000 WAN ports, the FVS336G can connect to either a 10 Mbps standard Ethernet network, a 100 Mbps Fast Ethernet network, or a 1000 Mbps Gigabit Ethernet network. The four LAN and two WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

The FVS336G 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 eliminates the need to worry about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

Extensive Protocol Support

The VPN firewall supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). For further information about TCP/IP, refer to "Internet Configuration Requirements" on page C-3.

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

Easy Installation and Management

You can install, configure, and operate the ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN 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.
- **Auto Detection of ISP**. The VPN firewall automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.

- **VPN Wizard.** The VPN firewall includes the NETGEAR VPN Wizard to easily configure IPsec VPN tunnels according to the recommendations of the Virtual Private Network Consortium (VPNC) to ensure the IPsec VPN tunnels are interoperable with other VPNC-compliant VPN routers and clients.
- **SNMP.** The VPN firewall supports the Simple Network Management Protocol (SNMP) to let you monitor and manage log resources from an SNMP-compliant system manager. The SNMP system configuration lets you change the system variables for MIB2.
- **Diagnostic Functions**. The firewall incorporates built-in diagnostic functions such as Ping, Trace Route, DNS lookup, and remote reboot.
- **Remote Management**. The firewall allows you to login to the Web Management Interface from a remote location on the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses.
- **Visual monitoring**. The VPN firewall's front panel LEDs provide an easy way to monitor its status and activity.

Maintenance and Support

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

- Flash memory for firmware upgrade.
- Free technical support seven days a week, 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:

- ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN.
- One AC power cable.
- Rubber feet.
- One Category 5 (Cat5) Ethernet cable.
- *Installation Guide, FVS336G ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN.*
- *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.

Front Panel Features

The ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN front panel shown below includes four groups of status indicator light-emitting diodes (LEDs), including Power and Test, WAN1, WAN2, and the LAN lights:

Figure 1-1

The function of each LED is described in the following table:

Table 1-1. LED Descriptions

Object	Activity	Description
PWR (Power)	On (Green) Off	Power is supplied to the VPN firewall. Power is not supplied to the VPN firewall.
TEST	On (Amber) Blinking (Amber) Off	Test mode: The system is initializing or the initialization has failed. Writing to Flash memory (during upgrading or resetting to defaults). The system has booted successfully.
WAN Ports		
ACTIVE	On (Green) On (Amber) Off	The WAN port has a valid Internet connection. The Internet connection is down or not being used because the port is in standby for failover. The WAN port is either not enabled or has no link.
SPEED	On (Green) On (Amber) Off	The LAN port is operating at 1,000 Mbps. The LAN port is operating at 100 Mbps. The LAN port is operating at 10 Mbps.
LINK/ACT (Link and Activity)	On (Green) Blinking (Green) Off	The WAN port has detected a link with a connected Ethernet device. Data is being transmitted or received by the WAN port. The WAN port has no link.

Table 1-1. LED Descriptions (continued)

Object	Activity	Description
LAN Ports		
SPEED	On (Green) On (Amber) Off	The LAN port is operating at 1,000 Mbps. The LAN port is operating at 100 Mbps. The LAN port is operating at 10 Mbps.
LINK/ACT (Link and Activity)	On (Green) Blinking (Green) Off	The WAN port has detected a link with a connected Ethernet device. Data is being transmitted or received by the WAN port. The WAN port has no link.

Rear Panel Features

The rear panel of the ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN includes Gigabit Ethernet LAN and WAN connections, a cable lock receptacle, power and reset switches, and an AC power connection.

Figure 1-2

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

1. Factory Defaults button: Using a sharp object, press and hold this button for about ten seconds until the front panel TEST light flashes to reset the VPN firewall to factory default settings. All configuration settings will be lost and the default password will be restored.
2. LAN Ethernet ports: Four switched N-way automatic speed negotiating, Auto MDI/MDIX, Gigabit Ethernet ports with RJ-45 connectors.
3. WAN Ethernet ports: Two independent N-way automatic speed negotiating, Auto MDI/MDIX, Gigabit Ethernet ports with RJ-45 connectors.
4. Cable security lock receptacle.
5. AC power receptacle: Universal AC input (100-240 VAC, 50-60 Hz).
6. On/off power switch.

Default IP Address, Login Name, and Password Location

Check the label on the bottom of the FVS336G's enclosure if you need a reminder of the following factory default information:

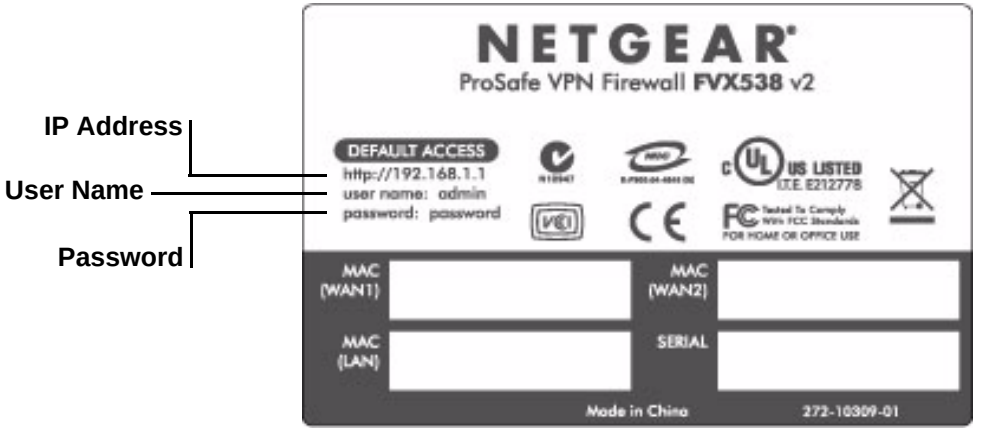


Figure 1-3

Qualified Web Browsers

To configure the ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN, an administrator must use Internet Explorer 5.1 or higher, Apple Safari 1.2 or higher, or Mozilla Firefox l.x Web browser with JavaScript, cookies, and SSL enabled.

Although these web browsers are qualified for use with the VPN firewall's Web Management Interface for configuring the VPN firewall, SSL VPN users should choose a browser that supports JavaScript, Java, cookies, SSL, and ActiveX to take advantage of the full suite of applications. Note that Java is only required for the SSL VPN portal, not the Web Management Interface.

Chapter 2
Connecting the FVS336G to the Internet

The initial Internet configuration of the ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN is described in this chapter.

This chapter contains the following sections:

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 *Installation Guide, FVS336G ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN* for complete steps. A PDF of the *Installation Guide* is on the NETGEAR website at: *http://kbserver.netgear.com*.
2. **Log in to the VPN Firewall**. After logging in, you are ready to set up and configure your VPN firewall. You can also change your password and enable remote management at this time. See "Logging into the VPN Firewall Router" on page 2-2.
3. **Configure the Internet connections to your ISP(s)**. During this phase, you will connect to your ISPs. You can also program the WAN traffic meters at this time if desired. See "Configuring the Internet Connections" on page 2-4.
4. **Configure the WAN mode (required for dual WAN operation)**. Select either dedicated (single WAN) mode, auto-rollover mode, or load balancing mode. For load balancing, you can also select any necessary protocol bindings. See "Configuring the WAN Mode (Required for Dual WAN)" on page 2-10.

5. **Configure dynamic DNS on the WAN ports (optional)**. Configure your fully qualified domain names during this phase (if required). See "Configuring Dynamic DNS (Optional)" on page 2-16.
6. **Configure the WAN options (optional)**. Optionally, you can enable each WAN port to respond to a ping, and you can change the factory default MTU size and port speed. However, these are advanced features and changing them is not usually required. See "Configuring the Advanced WAN Options (Optional)" on page 2-18.

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

Logging into the VPN Firewall Router

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, refer to the link in Appendix B, "Related Documents.

To connect and log in to the VPN firewall follow these steps:

1. Start any of the qualified browsers, as detailed in "Qualified Web Browsers" on page 1-8.
2. Enter **https://192.168.1.1** in the address field. The Manager login features appear in the browser.

Figure 2-1

3. In the User field, type **admin**
4. In the Password field, type **password**

   Note that both entries are in lower case letters.

5. Click **Login.** The Web Configuration Manager appears, displaying the Router Status menu:

Figure 2-2

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 the Internet Connections

To set up your VPN firewall for secure Internet connections, you configure WAN ports 1 and 2. The Web Configuration Manager offers two connection configuration options:

- Automatic detection and configuration of the network connection.
- Manual configuration of the network connection.

Each option is detailed in the sections following.

Automatically Detecting and Connecting

To automatically configure the WAN ports for connection to the Internet:

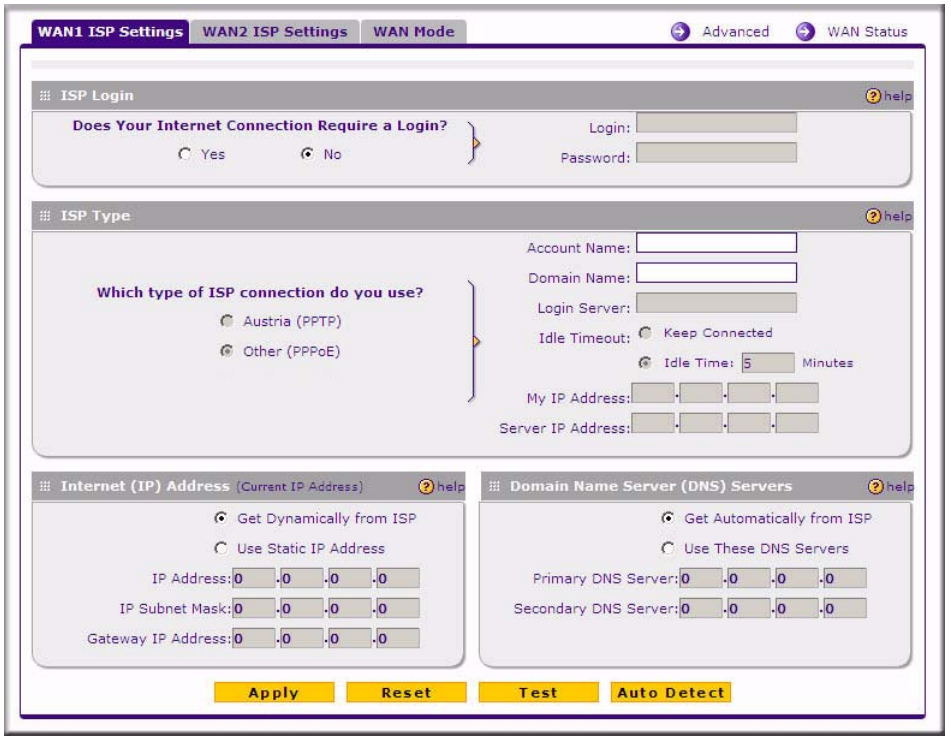


Figure 2-3

1. Select **Network Configuration** > **WAN Settings** from the menu. The WAN Settings tabs appear, with the WAN1 ISP Settings tab in view.
2. Click **Auto Detect** at the bottom of the menu. Auto Detect will probe the WAN port for a range of connection methods and suggest one that your ISP appears to support.

Figure 2-4

a. If Auto Detect is successful, a status bar at the top of the menu will display the results:.

b. If Auto Detect senses a connection method that requires input from you, it will prompt you for the information. All methods with their required settings are detailed in the following table.

Table 2-1. Internet connection methods

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

c. If Auto Detect does not find a connection, you will be prompted to (1) check the physical connection between your VPN firewall and the cable or DSL line, or to (2) check your VPN firewall's MAC address (For more information, see "Configuring the WAN Mode (Required for Dual WAN)" on page 2-10 and "Troubleshooting the ISP Connection" on page 10-4).

3. To verify the connection, click the **WAN Status** option arrow at the top right of the screen. A popup window appears, displaying the connection status of WAN port 1.

Figure 2-5

The WAN Status window should show a valid IP address and gateway. If the configuration was not successful, skip ahead to "Manually Configuring the Internet Connection" following this section, or see "Troubleshooting the ISP Connection" on page 10-4.

> **Note:** If the configuration process was successful, you are connected to the Internet through WAN port 1. If you intend to use the dual WAN capabilities of the VPN firewall, continue with the configuration process for WAN port 2.

4. Click the WAN2 ISP Settings tab.
5. Repeat the previous steps to automatically detect and configure the WAN2 Internet connection.
6. Open the WAN Status window and verify a successful connection

If your WAN ISP configuration was successful, you can skip ahead to "Configuring the WAN Mode (Required for Dual WAN)" on page 2-10.

If one or both automatic WAN ISP configurations failed, you can attempt a manual configuration as described in the following section, or see "Troubleshooting the ISP Connection" on page 10-4.

Manually Configuring the Internet Connection

Unless your ISP automatically assigns your configuration automatically via DHCP, you will need to obtain configuration parameters from your ISP in order to manually establish an Internet connection. The necessary parameters for various connection types are listed in Table 2-1.

To manually configure your **WAN1 ISP Settings:**

1. Select Network Configuration > WAN Settings > WAN1 ISP Settings and enter the following:
2. In the **ISP Login** options, choose one of these options:

Figure 2-6

- If your ISP requires an initial login to establish an Internet connection, click **Yes** (this is the default).
- If a login is not required, click **No** and ignore the Login and Password fields.

3. If you clicked **Yes**, enter the ISP-provided Login and Password information.
4. In the ISP Type options, select the type of ISP connection you use from the three listed options. (By default, “Other (PPPoE)” is selected, as shown below.

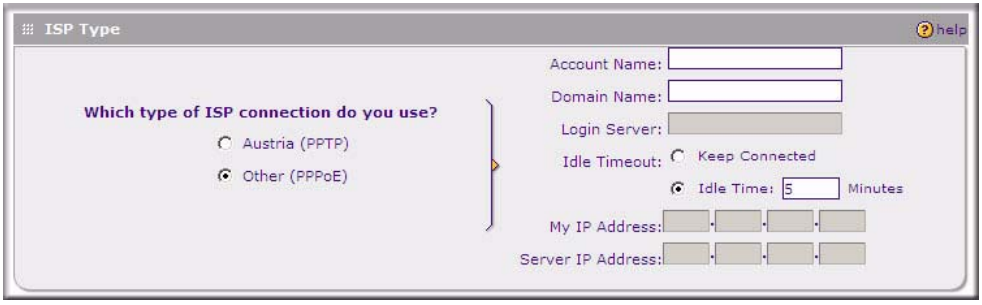


Figure 2-7

(If your connection is PPPoE or PPTP, your ISP will require an initial login.)

5. If you have installed login software such as WinPoET or Enternet, then your connection type is PPPoE. If your ISP uses PPPoE as a login protocol:

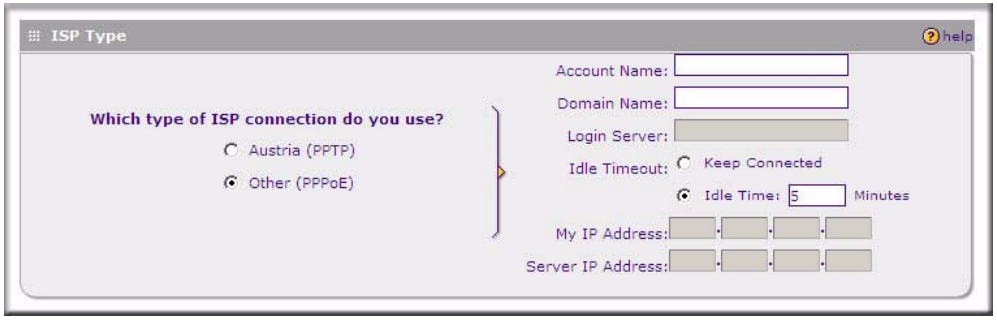


Figure 2-8

   a. Select **Other (PPPoE)**.
   b. Configure the following fields:
      - **Account Name**. Valid account name for the PPPoE connection
      - **Domain Name.** Name of your ISP’s domain or your domain name if your ISP has assigned one. In most cases, 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, click Idle Time and in the timeout field enter the number of minutes to wait before disconnecting.

6. If your ISP is Austria Telecom or any other ISP that uses PPTP as a login protocol:

   a. Select **Austria (PPTP)**.

   b. Configure the following fields:

      - **Account Name** (also known as Host Name or System Name)**.** Enter the valid account name for the PPTP connection (usually your email name as assigned by your ISP). Some ISPs require entering your full email address here.
      - **Domain Name.** Your domain name or workgroup name assigned by your ISP, or your ISPs domain name. You may leave this field blank.
      - **Idle Timeout.** Check the Keep Connected radio button to keep the connection always on. To logout after the connection is idle for a period of time, click 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.

7. Review the Internet (IP) Address options.

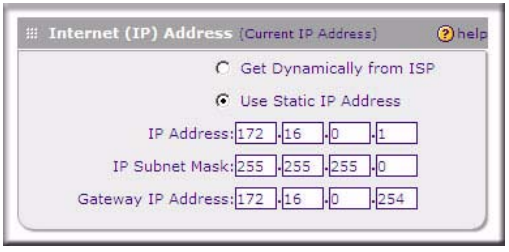


Figure 2-9

These options are inactive if BigPond Cable is selected.

8. If your ISP has assigned a fixed (static) IP address, select **Use Static IP Address**, and configure the following fields:

   - **IP Address.** Enter the Static IP address assigned to you, that identifies the VPN firewall to your ISP.
   - **Subnet Mask.** Enter the mask provided by the ISP or your network administrator.
   - **Gateway IP Address.** Enter the IP address of the ISP's gateway, provided by the ISP or your network administrator.

9. If your ISP has not assigned a static IP address, click **Get dynamically from ISP**. The text fields will be inactivated.

   The ISP will automatically assign an IP address to the VPN firewall using DHCP network protocol.

10. Review the Domain Name Server (DNS) Servers options.

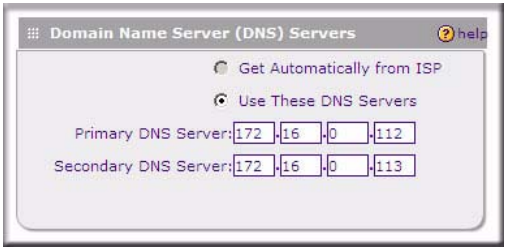


Figure 2-10

- If your ISP has not assigned any Domain Name Servers (DNS) addresses, click **Get dynamically from ISP**.
- If your ISP (or your IT department) has assigned DNS addresses, click **Use these DNS Servers** and enter the DNS server IP addresses provided to you in the fields.

11. Click **Apply** to save any changes to the WAN1 ISP Settings. (Or click **Reset** to discard any changes and revert to the previous settings.)

12. Click **Test** to evaluate your entries.

    The VPN firewall will attempt to connect to the NETGEAR Web site. If a successful connection is made, NETGEAR's Web site appears.

13. If you intend to use a dual WAN mode, click the **WAN2 ISP Settings** tab and configure the WAN2 ISP settings using the same steps as WAN1.

When you are finished, click Logout or proceed to additional setup and management tasks.

Configuring the WAN Mode (Required for Dual WAN)

The dual WAN ports of the ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN can be configured on a mutually exclusive basis for either auto-rollover (for increased system reliability) or load balancing (for maximum bandwidth efficiency), or one port can be disabled.

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

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

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

	**Note:** Scenarios could arise when load balancing needs to be bypassed for certain traffic or applications. If certain traffic needs to travel on a specific WAN interface, configure protocol binding rules for that WAN interface. The rule should match the desired traffic.

- **Single WAN Port Mode**. The selected WAN interface is made primary and the other is disabled.

For whichever WAN mode you choose, you must also choose either NAT or classical routing, as explained in the following sections.

Network Address Translation

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

- The VPN firewall uses NAT to select the correct PC (on your LAN) to receive any incoming data.
- If you only have a single public Internet IP address, you MUST use NAT. (the default setting).
- If your ISP has provided you with multiple public IP addresses, you can use one address as the primary shared address for Internet access by your PCs, and you can map incoming traffic on the other public IP addresses to specific PCs on your LAN. This one-to-one inbound mapping is configured using an inbound firewall rule.

Classical Routing

In classical routing mode, the VPN firewall performs routing, but without NAT. To gain Internet access, each PC on your LAN must have a valid static Internet IP address.

If your ISP has allocated a number of static 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.

To learn the status of the WAN ports, you can view the Router Status page (see "Monitoring VPN Tunnel Connection Status" on page 9-14) or look at the LEDs on the front panel (see "Front Panel Features" on page 1-6).

Configuring Auto-Rollover Mode

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

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

- By sending DNS queries to a DNS server, or
- By sending a Ping request to an IP address, or
- None (no failure detection is performed).

From each WAN interface, DNS queries or Ping requests are sent to the specified IP address. If replies are not received, after a specified number of retries, the corresponding WAN interface is considered down.

To configure the dual WAN ports for Auto-Rollover

1. Select Network Configuration > WAN Settings from the main menu and click the WAN Mode tab. The WAN Mode tab is displayed

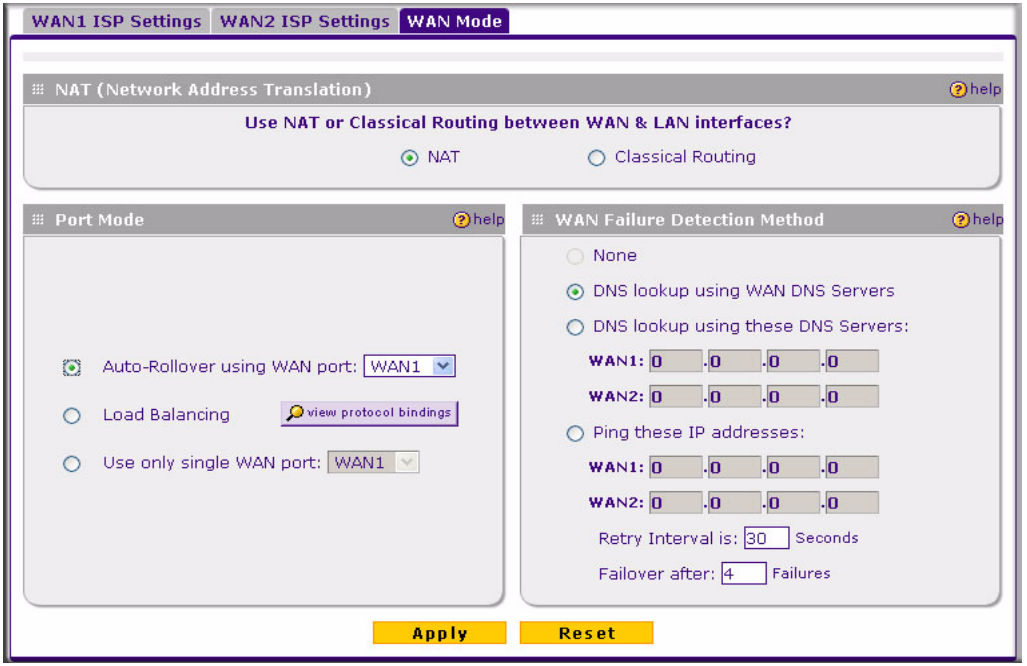


Figure 2-11

2. In the **Port Mode** section, select **Auto-Rollover Using WAN port**.
3. From the pull-down menu, choose which WAN port will act as the primary link for this mode.
4. In the **WAN Failure Detection Method** section, select one of the following detection failure methods:
   - **DNS lookup using ISP DNS Servers.** DNS queries are sent to the DNS server configured on the WAN ISP pages (see "Configuring the Internet Connections" on page 2-4).
   - **DNS lookup using this DNS Server.** Enter a public DNS server. DNS queries are sent to this server through the WAN interface being monitored.
   - **Ping to this IP addresses**. Enter a public IP address that will not reject the Ping request and will not consider Ping traffic to be abusive. Queries are sent to this server through the WAN interface being monitored.
5. Enter a **Retry Interval** in seconds. The DNS query or Ping is sent periodically after every test period. The default test period is 30 seconds.

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

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

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

Once a rollover occurs, an alert will be generated (see "E-Mail Notifications of Event Logs and Alerts" on page 4-29). When the VPN firewall detects that the failed primary WAN interface has been restored, it will automatically rollover again to the primary WAN interface. Alternatively, you can manually force traffic back on the original primary WAN interface by reapplying the Auto-Rollover settings in the WAN Mode menu.

Configuring Load Balancing

To use multiple ISP links simultaneously, select Load Balancing. In Load Balancing mode, either WAN port will carry any outbound protocol unless protocol binding is configured. When a protocol is bound to a particular WAN port, all outgoing traffic of that protocol will be directed to the bound WAN port. For example, if the HTTPS protocol is bound to WAN1 and the FTP protocol is bound to WAN2, then the VPN firewall will automatically route all outbound HTTPS traffic from the computers on the LAN through the WAN1 port. All outbound FTP traffic will be routed through the WAN2 port.

Protocol binding

Protocol binding addresses two issues:

- Segregation of traffic between links that are not of the same speed.
  High volume traffic can be routed through the WAN port connected to a high speed link and low volume traffic can be routed through the WAN port connected to the low speed link.
- Continuity of source IP address for secure connections.
  Some services, particularly HTTPS, will cease responding when a client's source IP address changes shortly after a session has been established.

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

1. Select Network >WAN Settings, and click the **WAN Mode** tab.
2. In the **Port Mode** section, select **Load Balancing**.

3. Click **view protocol bindings** (if required). The **WAN1 Protocol Bindings** screen is displayed.

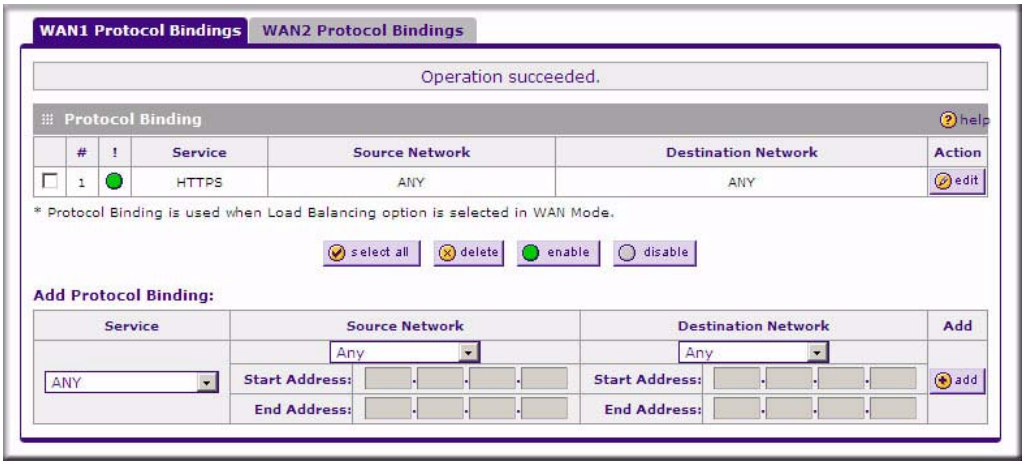


Figure 2-12

Enter the following data in the **Add Protocol Binding** options:

a. **Service**. From the pull-down menu, choose the desired Service or application to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see "About Services-Based Rules" on page 4-3).

b. **Source Network**. These settings determine which computers on your network are affected by this rule. Select the desired options:

- **Any**. All PCs and devices on your LAN.
- **Single address**. Enter the required address and the rule will be applied to that particular PC.
- **Address range**. If this option is selected, you must enter the start and finish fields.
- **Group 1-Group 8**. If this option is selected, the devices assigned to this group will be affected. (You may also assign a customized name to the group. See **Edit Group Names** on the **Groups and Hosts** menu in the **LAN Groups** sub-menu.)

c. **Destination Network**. These settings determine which Internet locations are covered by the rule, based on their IP address. Select the desired option:

- **Any**. All Internet IP address are covered by this rule.
- **Single address**. Enter the required address in the start field.

- **Address range**. If this option is selected, you must enter the start and finish fields.

4. Click **Add** to save this rule**.**

   The new Protocol Binding Rule will be enabled and added to the Protocol Binding Table for the WAN1 port.

5. Open the **WAN2 Protocol Bindings** tab and repeat the previous steps to set protocol bindings for the WAN2 port.

Configuring Dynamic DNS (Optional)

Dynamic DNS (DDNS) is an Internet service that allows routers with varying public IP addresses to be located using Internet domain names. To use DDNS, you must setup an account with a DDNS provider such as DynDNS.org, TZO.com or Iego.net. (Links to DynDNS, TZO and Iego are provided for your convenience on the **Dynamic DNS Configuration** screen.) The VPN firewall firmware includes software that notifies dynamic DNS servers of changes in the WAN IP address, so that the services running on this network can be accessed by others on the Internet.

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

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

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

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

To configure Dynamic DNS:

1. Select Network Configuration > Dynamic DNS from the main menu and click the **Dynamic DNS Configuration** tab. The Dynamic DNS Configuration screen is displayed.

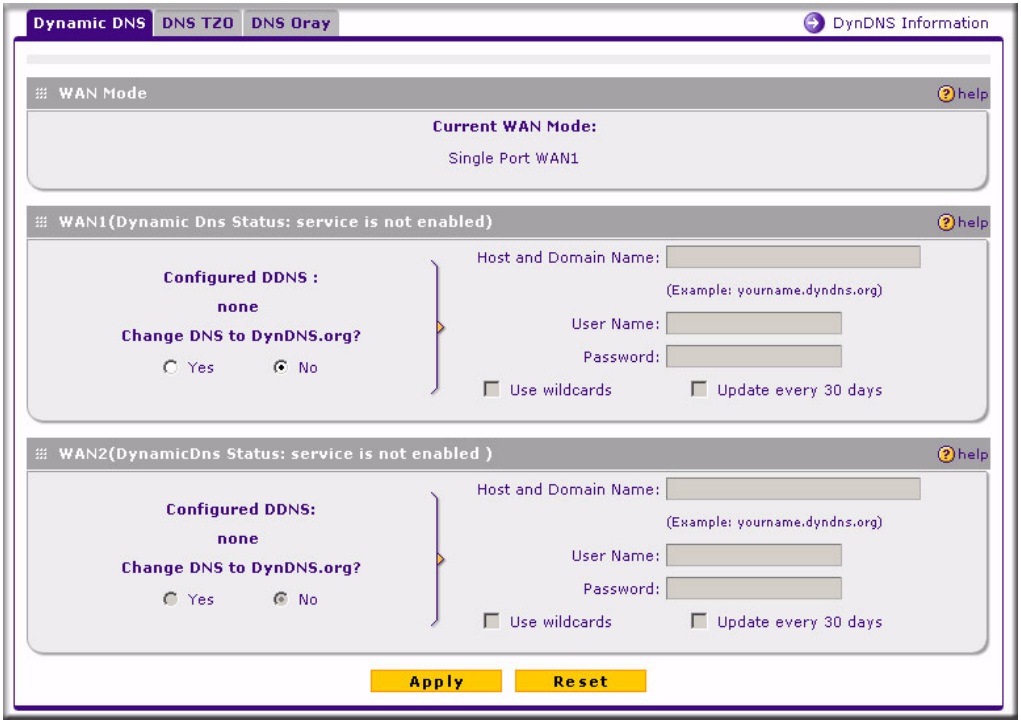


Figure 2-13

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

2. Select the tab for the DDNS service provider you will use.

3. Click the information or registration link in the upper right corner for registration information.

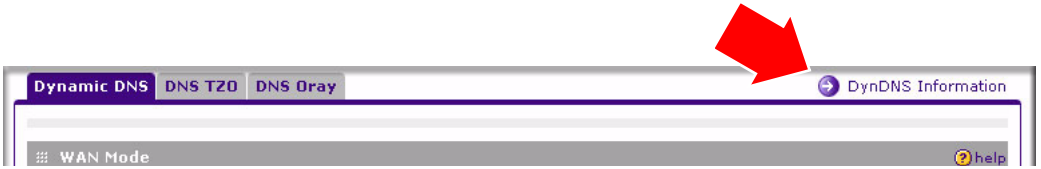


Figure 2-14:

4. Access the Web site of the DDNS service provider and register for an account (for example, for dyndns.org, go to *http://www.dyndns.org*).
5. For each WAN port, click the **Yes** radio button for **Change DNS to** <*your desired DDNS service*> and configure the active fields:
   a. Enter the account information for the service you have chosen (for example, user name, password, key, or domain).
   b. If your DDNS provider allows the use of wild cards in resolving your URL, you may select the **Use wildcards** check box to activate this feature. For example, the wildcard feature will cause `*.yourhost.dyndns.org` to be aliased to the same IP address as `yourhost.dyndns.org`
   c. If your WAN IP address does not change often, you may need to force a periodic update to the DDNS service to prevent your account from expiring. If it appears, you can select the **Update every 30 days** check box to enable a periodic update.
6. Click **Apply** to save your configuration.

Configuring the Advanced WAN Options (Optional)

To configure the Advanced WAN options:

1. Select **Network Configuration** > WAN Settings from the main menu. The WAN! ISP Settings screen will display.

2. Click the **Advanced** link to the right of the tabs. The **WAN1 Advanced Options** tab is displayed (along with the WAN2 Advanced Options tab).

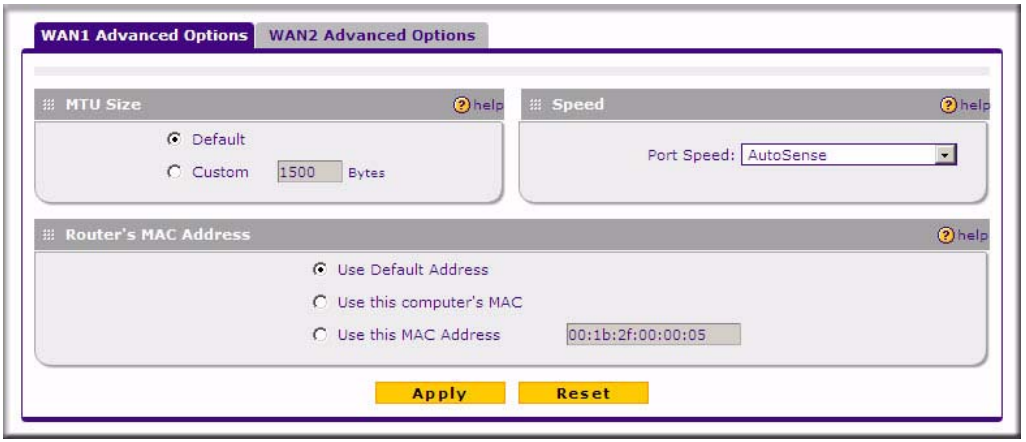


Figure 2-15

3. Edit the default information you want to change.

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

   b. **Port Speed**. In most cases, your VPN firewall can automatically determine the connection speed of the WAN port. If you cannot establish an Internet connection and the WAN Link or Speed LED blinks continuously, you may need to manually select the port speed. AutoSense is the default.

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

   c. **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 of these options:

      - Use this Computer's MAC address to have the VPN firewall 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 01:23:45:67:89:AB (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 changes.

Additional WAN Related Configuration

- If you want the ability to manage the firewall remotely, enable remote management at this time (see "Enabling Remote Management Access" on page 8-10). If you enable remote management, we strongly recommend that you change your password (see "Changing Passwords and Administrator Settings" on page 8-8).
- At this point, you can set up the traffic meter for each WAN, if desired. See "Enabling the Traffic Meter" on page 9-1.

Chapter 3
LAN Configuration

This chapter describes how to configure the advanced LAN features of your ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN.

This chapter contains the following sections

Choosing the Firewall DHCP Options

By default, the firewall will function as a DHCP (Dynamic Host Configuration Protocol) server, allowing it to assign IP, DNS server, WINS Server, and default gateway addresses to all computers connected to the firewall LAN. The assigned default gateway address is the LAN address of the firewall. IP addresses will be assigned to the attached PCs from a pool of addresses specified in this menu. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN. 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 "Preparing a Computer for Network Access" in Appendix B, "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 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 firewall will deliver the following parameters to any LAN device that requests DHCP:

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

DHCP Relay options allow you to make the 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 router will act as a proxy for all DNS requests and communicate with the ISP's DNS servers (as configured in the WAN settings page). All DHCP clients will receive the Primary/Secondary DNS IP along with the IP where the DNS Proxy is running, i.e. the box's LAN IP. 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 router and the router, in turn, sends those requests to the DNS servers of the active connection.

Configuring the LAN Setup Options

The **LAN IP Setup** menu 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 FVS336G as a DHCP server but rather as a DHCP relay agent for a DHCP server somewhere else on your network.

1. Go to **Network Configuration > LAN Setup** to display the **LAN Setup** tab page.

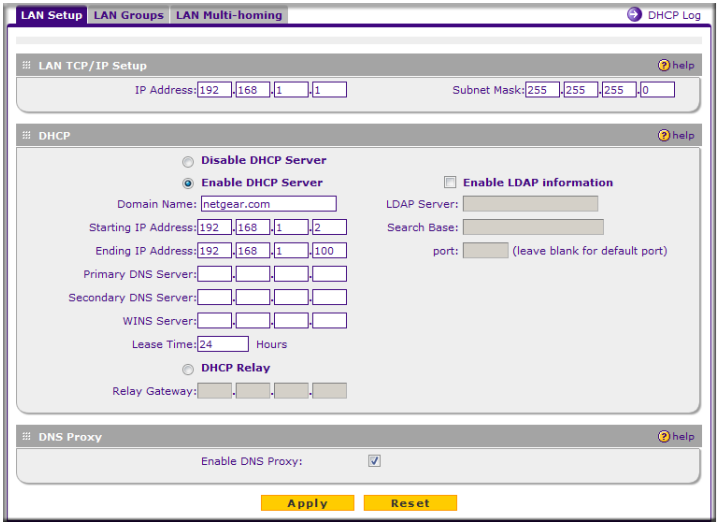


Figure 3-1

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 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 **Enable** or **Disable DHCP Server.**
   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 DHCP server is enabled, enter the following parameters:

   - **Domain Name.** (Optional) The DHCP will assign the entered domain to DHCP clients.

- **Starting IP Address**. Specifies the first of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN will be assigned an IP address between this address and the Ending IP Address. The IP address 192.168.1.2 is the default start address.
- **Ending IP Address**. Specifies the last of the contiguous addresses in the IP address pool. The IP address 192.168.1.100 is the default ending address.

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

- **Primary DNS Server**. (Optional) If an IP address is specified, the VPN firewall will provide this address as the primary DNS server IP address. If no address is specified, the VPN firewall will provide its own LAN IP address as the primary DNS server IP address.
- **Secondary DNS Server**. (Optional) If an IP address is specified, the VPN firewall will provide this address as the secondary DNS server IP address.
- **WINS Server**. (Optional) Specifies the IP address of a local Windows NetBios Server if one is present in your network.

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

b. **Enable LDAP Information**. This enables the DHCP server to provide LDAP server information.

- **Enable DNS Proxy**. When DNS proxy is enabled (the default), the DHCP server will provide the VPN firewall's LAN IP address as the DNS server for address name resolution. If this box is unchecked, the DHCP server will provide the ISP's DNS server IP addresses. The VPN firewall will still service DNS requests sent to its LAN IP address unless you disable DNS Proxy in the firewall settings (see "Attack Checks" on page 4-17).

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

> **Note:** Once you have completed the LAN setup, all outbound traffic is allowed and all inbound traffic is discarded. To change these default traffic rules, refer to Chapter 4, "Firewall Protection and Content Filtering.

Managing Groups and Hosts (LAN Groups)

The **Known PCs and Devices** table in the **LAN Groups** menu contains a list of all known PCs and network devices that are assigned dynamic IP addresses by the VPN firewall, or have been discovered by other means. Collectively, these entries make up the LAN Groups Database.

The LAN Groups Database is updated by these methods:

- **DHCP Client Requests**. By default, the DHCP server in this VPN firewall is enabled, and will accept and respond to DHCP client requests from PCs and other network devices. These requests also generate an entry in the LAN Groups 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 ARP requests. The ARP 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 appear in the database as Unknown.
- **Manual Entry**. You can manually enter information about a network device.

Some advantages of the LAN Groups Database are:

- Generally, you do not need to enter either IP address or MAC addresses. Instead, you can just select the desired PC or device.
- No need to reserve an IP address for a PC in the DHCP server. All IP address assignments made by the DHCP server will be maintained until the PC or device is removed from the database, either by expiry (inactive for a long time) or by you.
- No need to use a fixed IP on PCs. Because the address allocated by the DHCP server will never change, you don't need to assign a fixed IP to a PC to ensure it always has the same IP address.
- MAC level control over PCs. The LAN Groups 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 4-18).
  - If necessary, you can also create Firewall Rules to apply to a single PC (see "Configuring Source MAC Filtering" on page 4-21). 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 LAN Groups Database

To view the LAN Groups Database, follow these steps:

1. Select **Network Configuration > LAN Settings** from the main menu. The LAN Setup tab displays.
2. Click the **LAN Groups** tab. The LAN Groups tab is displayed.

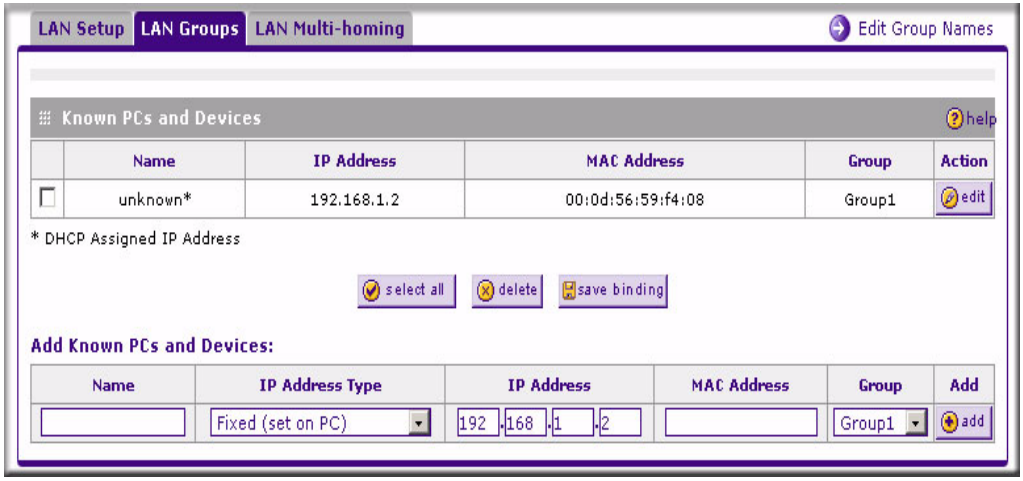


Figure 3-2

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

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

Adding Devices to the LAN Groups Database

To add devices manually to the LAN Groups Database, follow these steps:

1. In the **Add Known PCs and Devices** section, make the following entries:
   - **Name**. Enter the name of the PC or device.
   - **IP Address Type**. From the pull-down menu, choose how this device receives its IP address. The choices are:
     - **Fixed (Set on PC)**. The IP address is statically assigned on the computer.
     - **Reserved (DHCP Client)**. Directs the VPN firewall's DHCP server to always assign the specified IP address to this client during the DHCP negotiation (see "Configuring DHCP Address Reservation" on page 3-8).

   - **IP Address.** Enter the IP address that this computer or device is assigned in the IP Address field. If the IP Address Type is Reserved (DHCP Client), the VPN firewall will reserve the IP address for the associated MAC address.
   - **MAC Address.** Enter the MAC address of the computer's network interface in the MAC Address field. 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.** From the pull-down menu, select the LAN Group to which the computer will be assigned. (Group 1 is the default group.)
2. Click **Add.** The device will be added to the **Known PCs and Devices** table.
3. (Optional) To enable DHCP Address Reservation after the entry is in the table, select the check box for the new 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** tab, click the **Edit Group Names** link to the right of the tabs. The **Network Database Group Names** tab appears.

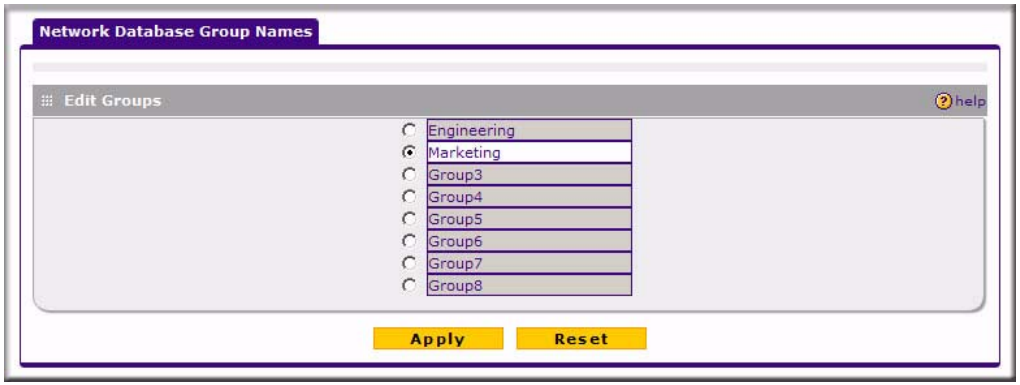


Figure 3-3

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.

Configuring 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 address 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 in the **LAN Groups** tab, specifying **Reserved (DHCP Client)**, as described in "Configuring DHCP Address Reservation" on page 3-8.

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

Configuring Multi Home LAN IP Addresses

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

To add a secondary LAN IP address, follow these steps:

1. Select Network Configuration > LAN Settings from the main menu, and click the LAN Multi-homing tab. The LAN Multi-homing screen displays.

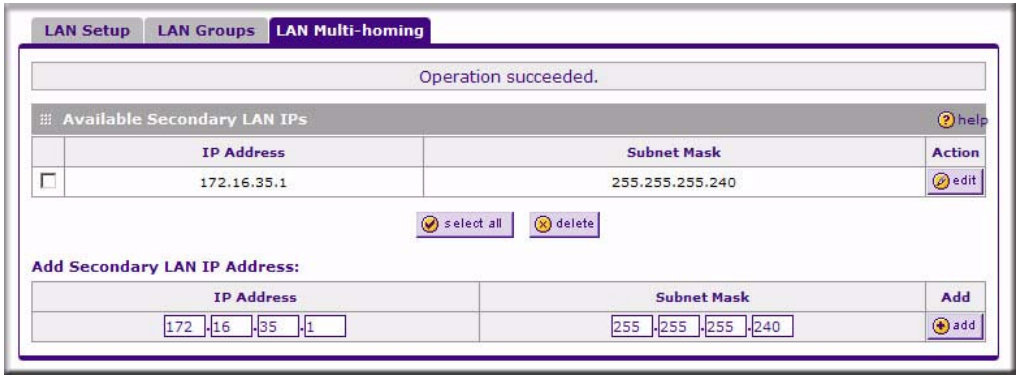


Figure 3-4

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

- **IP Address**. The “alias,” an additional IP address hosted by the LAN port of the VPN firewall. This address will be the gateway for computers on the secondary subnet.
- **Subnet Mask**. The IPv4 subnet mask that defines the range of the secondary subnet.

2. In the **Add Secondary LAN IP Address** section, enter the additional IP address and subnet mask to be assigned to the LAN port of the VPN firewall.
3. Click **Add.** The new Secondary LAN IP address will appear in the **Available Secondary LAN IPs** table.

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

Tip: The secondary LAN IP address will be assigned to the LAN interface of the VPN firewall and can be used as a gateway by computers on the secondary subnet.

Configuring Static Routes

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

Configuring Static Routes

To add or edit a static route:

1. Select Network Configuration > Routing from the main menu. The Routing screen displays.

Figure 3-5

2. Click **Add**. The **Add Static Route** tab is displayed.

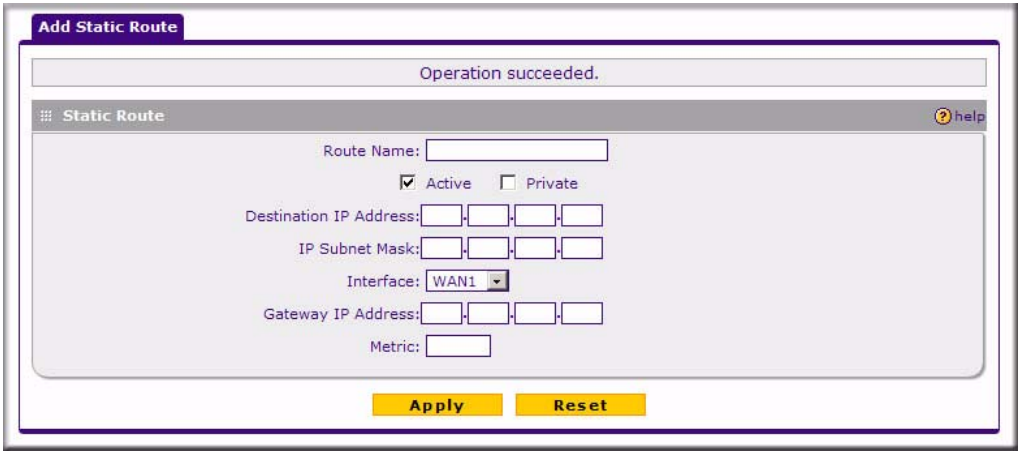


Figure 3-6

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

    The new static route will be added to the Static Route table.

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 parameters:

1. Select **Network Configuration** > **Routing** from the main menu.
2. Click the **RIP Configuration** link to the right of the tab. The **RIP Configuration** menu is displayed.

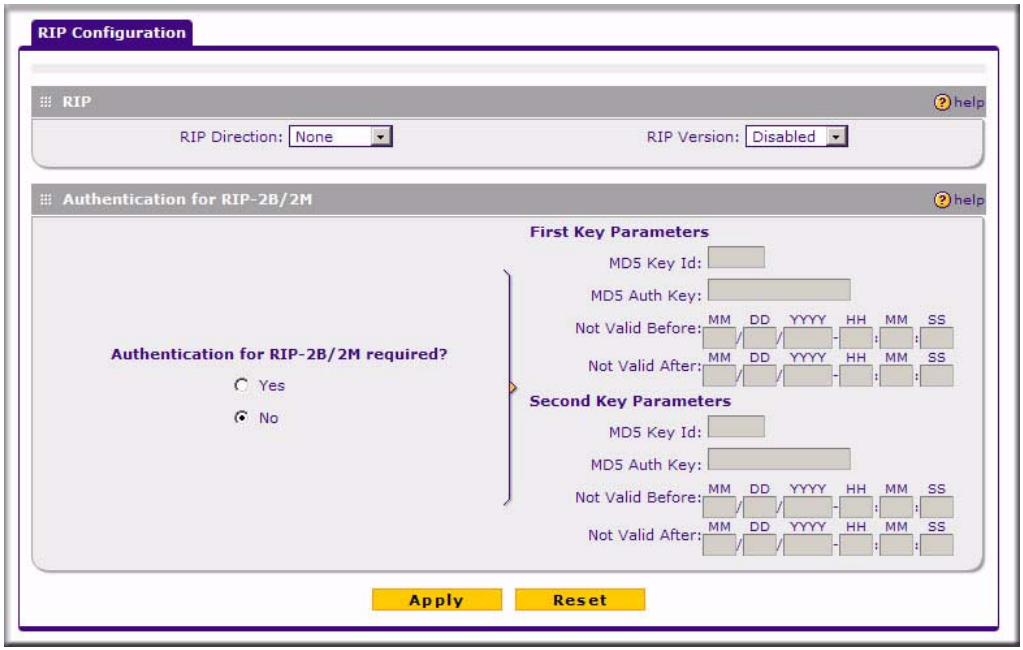


Figure 3-7

3. From the **RIP Direction** pull-down menu, choose the direction in which the VPN firewall will send and receive RIP packets. The choices are:
   - **None**. The VPN firewall neither broadcasts its route table nor does it accept any RIP packets from other routers. This effectively disables RIP.

- **Both**. The VPN firewall broadcasts its routing table and also processes RIP information received from other routers.
- **Out Only**. The VPN firewall broadcasts its routing table periodically but does not accept RIP information from other routers.
- **In Only**. The VPN firewall accepts RIP information from other routers, but does not broadcast its routing table.

4. From the **RIP Version** pull-down menu, choose the version from the following options:
   - **RIP-1**. A classful routing that does not include subnet information. This is the most commonly supported version.
   - **RIP-2**. Supports subnet information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format:
     - **RIP-2B**. 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 **YES** the feature, and input the **First Key Parameters** and **Second Key Parameters,** MD-5 keys to authenticate between routers.
6. Click **Add** to save your settings.

Chapter 4
Firewall Protection and Content Filtering

This chapter describes how to use the content filtering features of the ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN to protect your network.

This chapter contains the following sections:

About Firewall Protection and Content Filtering

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

A firewall is a special category of router that protects one network (the "trusted" network, such as your LAN) from another (the untrusted network, such as the Internet), while allowing communication between the two. You can further segment keyword blocking to certain known groups (see "Managing Groups and Hosts (LAN Groups)" on page 3-5 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:

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

A firewall has two default rules, one for inbound traffic and one for outbound traffic. The default rules of the FVS336G 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.

About Services-Based Rules

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

- **Outbound Rules (service blocking)**. Outbound traffic is normally allowed unless the firewall is configured to disallow it.
- **Inbound Rules (port forwarding)**. Inbound traffic is normally blocked by the firewall unless the traffic is in response to a request from the LAN side. The firewall can be configured to allow this otherwise blocked traffic.
- **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 4-14.
- **Quality of Service (QoS) priorities**. Each service at its own native priority that impacts its quality of performance and tolerance for jitter or delays. You can change this QoS priority if desired to change the traffic mix through the system (see "Setting Quality of Service (QoS) Priorities" on page 4-16).

Outbound Rules (Service Blocking)

The FVS336G allows you to block the use of certain Internet services by PCs on your network. This is called service blocking or port filtering.

The default policy can be changed to block all outbound traffic and enable only specific services to pass through the router. The following **Outbound Rules** table lists the configured rules for outgoing traffic. An outbound rule is defined by the following fields:

Table 4-1. Outbound Rules

Item	Description
Service Name	Select the desired Service or application to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see "Adding Customized Services" on page 4-14).
Action (Filter)	Select the desired action for outgoing connections covered by this rule: • BLOCK always • BLOCK by schedule, otherwise Allow • ALLOW always • ALLOW by schedule, otherwise Block **Note**: Any outbound traffic which is not blocked by rules you create will be allowed by the Default rule. ALLOW rules are only useful if the traffic is already covered by a BLOCK rule. That is, you wish to allow a subset of traffic that is currently blocked by another rule.

Table 4-1. Outbound Rules (continued)

Item	Description
Action (Select Schedule)	Select the desired time schedule (Schedule1, Schedule2, or Schedule3) that will be used by this rule. • This drop down menu gets activated only when “BLOCK by schedule, otherwise Allow” or “ALLOW by schedule, otherwise Block” is selected as Action. • Use schedule page to configure the time schedules (see “Setting a Schedule to Block or Allow Specific Traffic” on page 4-26).
LAN Users	Specifies which computers on your network are affected by this rule. Select the desired options: • Any – All PCs and devices on your LAN. • Single address – Enter the required address and the rule will be applied to that particular PC. • Address range – If this option is selected, you must enter the start and finish fields. • Groups – Select the Group to which this rule will apply. Use the LAN Groups screen (under Network Configuration) to assign PCs to Groups. See “Managing Groups and Hosts (LAN Groups)” on page 3-5.
WAN Users	Specifies which Internet locations are covered by the rule, based on their IP address. Select the desired option: • Any – All Internet IP address are covered by this rule. • Single address – Enter the required address in the start field. • Address range – If this option is selected, you must enter the start and end fields.
QoS Priority	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 “Setting Quality of Service (QoS) Priorities” on page 4-16.
Log	This determines whether packets covered by this rule are logged. Select the desired action: • Always – always log traffic considered by this rule, whether it matches or not. This is useful when debugging your rules. • Never – never log traffic considered by this rule, whether it matches or not.
Bandwidth Profile	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 “Configuring a Bandwidth Profile” on page 4-26.
NAT IP	Specifies whether the source IP address of the outgoing packets should be the WAN interface address or a specified address, which should belong to the WAN subnet.
NAT single IP is on:	Specifies to which WAN interface the NAT IP address belongs. All outgoing packets will be routed through the specified WAN interface only.

Note: See "Configuring Source MAC Filtering" on page 4-21 for yet another way to block outbound traffic from selected PCs that would otherwise be allowed by the firewall.

Inbound Rules (Port Forwarding)

When the FVS336G uses Network Address Translation (NAT), your network presents only one IP address to the Internet and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a Web server or game server) visible and available to the Internet. The rule tells the firewall to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as port forwarding.

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

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

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

Table 4-2. Inbound Rules

Item	Description
Service	Select the desired Service or application to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see "Adding Customized Services" on page 4-14).
Action (Filter)	Select the desired action for packets covered by this rule: • BLOCK always • BLOCK by schedule, otherwise Allow • ALLOW always • ALLOW by schedule, otherwise Block **Note**: Any inbound traffic which is not allowed by rules you create will be blocked by the Default rule.
Schedule	Select the desired time schedule (Schedule1, Schedule2, or Schedule3) that will be used by this rule (see "Setting a Schedule to Block or Allow Specific Traffic" on page 4-26). • This drop down menu gets activated only when "BLOCK by schedule, otherwise Allow" or "ALLOW by schedule, otherwise Block" is selected as Action. • Use schedule page to configure the time schedules.
Send to LAN Server	This field appears only with NAT Routing (not Classical). This LAN address determines which computer on your network is hosting this service rule. (You can also translate this address to a port number.)
Translate to Port Number	Check 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	Specifies the destination IP address applicable to incoming traffic. This is the public IP address that will map to the internal LAN server; it can either be the address of the WAN1 or WAN2 ports or another public IP address.
LAN users	This field appears only with Classical Routing (not NAT). Specifies which computers on your network are affected by this rule. Select the desired options: • Any – All PCs and devices on your LAN. • Single address – Enter the required address and the rule will be applied to that particular PC. • Address range – If this option is selected, you must enter the start and finish fields. • Groups – Select the Group to which this rule will apply. Use the LAN Groups screen (under Network Configuration) to assign PCs to Groups. See "Managing Groups and Hosts (LAN Groups)" on page 3-5.
WAN Users	Specifies which Internet locations are covered by the rule, based on their IP addresses. Select the desired option: • Any – All Internet IP address are covered by this rule. • Single address – Enter the required address in the start field. • Address range – If this option is selected, you must enter the start and end fields.

Table 4-2. Inbound Rules (continued)

Item	Description
Log	Specifies whether packets covered by this rule are logged. Select the desired action: • Always – Always log traffic considered by this rule, whether it matches or not. This is useful when debugging your rules. • Never – Never log traffic considered by this rule, whether it matches or not.
Bandwidth Profile	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 "Configuring a Bandwidth Profile" on page 4-26.

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. Enable only those ports that are necessary for your network. We also recommend enabling the server's application security and configuring user password or privilege levels, if provided.

Viewing the Rules

To view the firewall rules: Select **Security** > **Firewall** from the main menu. The LAN WAN Rules tab appears:

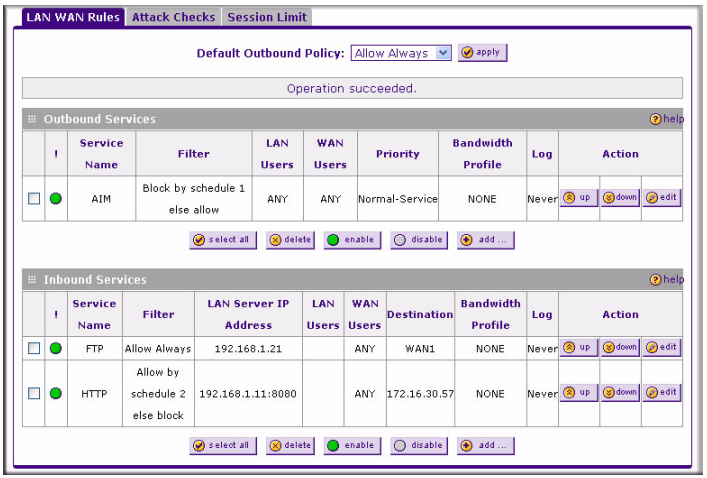


Figure 4-1

Order of Precedence for Rules

As you define new rules, they are added to the tables in the Rules menu as the last item in the list, as shown in Figure 4-1. For any traffic attempting to pass through the firewall, the packet information is subjected to the rules in the order shown in the Rules Table, beginning at the top and proceeding to the bottom, before applying the default rule. 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 to the Internet to pass through. Firewall rules can then be applied to block specific types of traffic from going out from the LAN to the Internet (Outbound). The default policy of Allow Always can be changed to block all outbound traffic which then allows you to enable only specific services to pass through the VPN firewall.

To change the Default Outbound Policy, follow these steps:

1. Click the LAN WAN Rules tab, shown in Figure 4-1.

2. Change the **Default Outbound Policy** by choosing Block Always from the drop-down menu.
3. Click **Apply**.

Creating a LAN WAN Outbound Services Rule

An outbound rule will block or allow the selected application from an internal IP LAN address to an external WAN IP address according to the schedule created in the Schedule menu.

You can also tailor these rules to your specific needs (see "Administrator Tips" on page 4-29).

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

To create a new outbound service rule in the LAN WAN Rules tab:

1. Click **Add** under the Outbound Services Table. The **Add LAN WAN Outbound Service** screen is displayed..

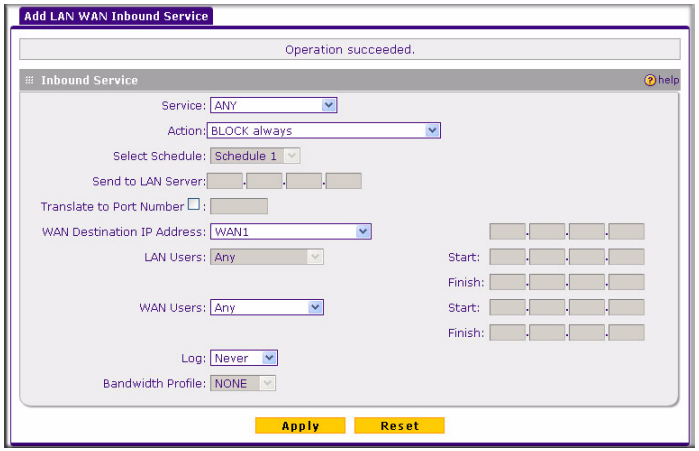


Figure 4-2

2. Configure the parameters based on the descriptions 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.

Creating a LAN WAN Inbound Services Rule

This Inbound Services Rules table lists all existing rules for inbound traffic. If you have not defined any rules, no rules will be listed. By default, all inbound traffic is blocked. 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 tab:

1. Click **Add** under the Inbound Services Table. The **Add LAN WAN Inbound Service** screen is displayed.

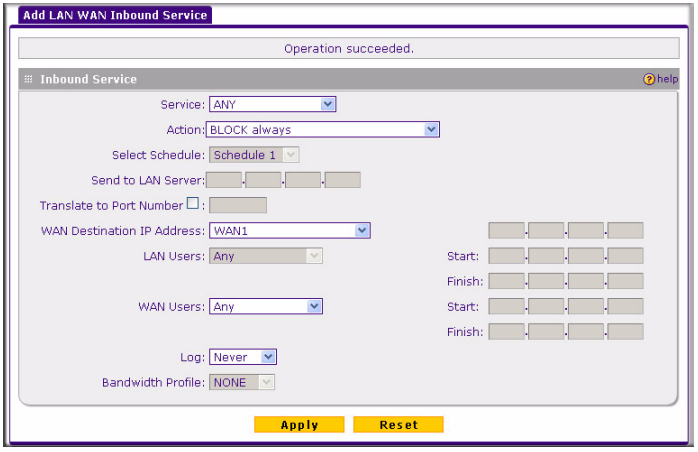


Figure 4-3

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

Modifying Rules

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

1. In the **Action** column adjacent to the rule, do the following:
   - Click **Edit** to make any changes to the rule definition of an existing rule. The Outbound Service or Inbound Service screen is displayed containing the data for the selected rule.
   - Click **Up** to move the rule up one position in the table rank.

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

	Note: Since rules are applied in the order listed (from top to bottom), the order of the rules may make a difference in how traffic is handled.

2. Check the box adjacent to the rule, then do any of the following:
   - Click **Enable** to enable the rule. The "!" Status icon will turn green.
   - Click **Disable** to disable the policy. A rule can be disabled if not in use and enabled as needed. Disabling a rule does not delete the configuration, but merely de-activates the rule. The status circle will change from green to grey, indicating that the rule is disabled. (By default, when a rule is added to the table it is automatically enabled.)
   - Click **Delete** to delete the rule.

Inbound Rules Examples

LAN WAN Inbound Rule: Hosting A Local Public Web Server

If you host a public Web server on your local network, you can define a rule to allow inbound Web (HTTP) requests from any outside IP address to the IP address of your Web server at any time of day.

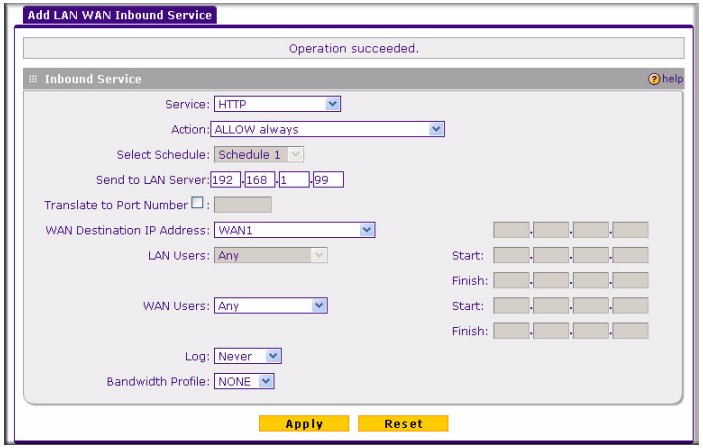


Figure 4-4

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.

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 to a local host only from a specified range of external IP addresses. Connections are blocked during the period specified by Schedule 1.

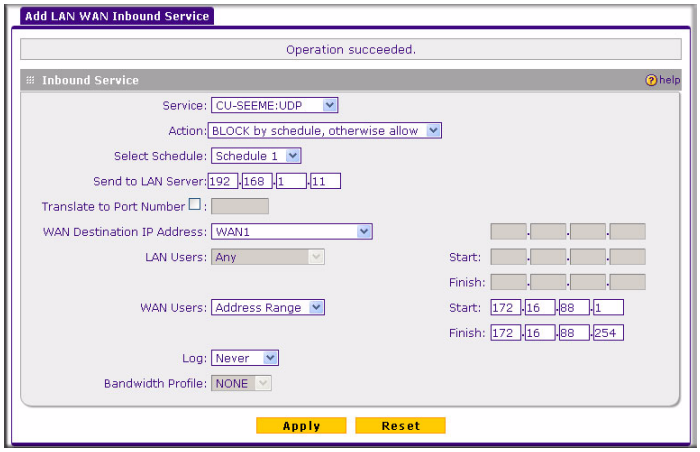


Figure 4-5

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, we have configured multi-NAT to support multiple public IP addresses on one WAN interface. The inbound rule instructs the VPN firewall to host an additional public IP address (10.1.0.5) and to associate this address with the Web server on the LAN (at 192.168.1.2). We also instruct the VPN firewall to translate the incoming HTTP port number (port 80) to a different port number (port 8080).

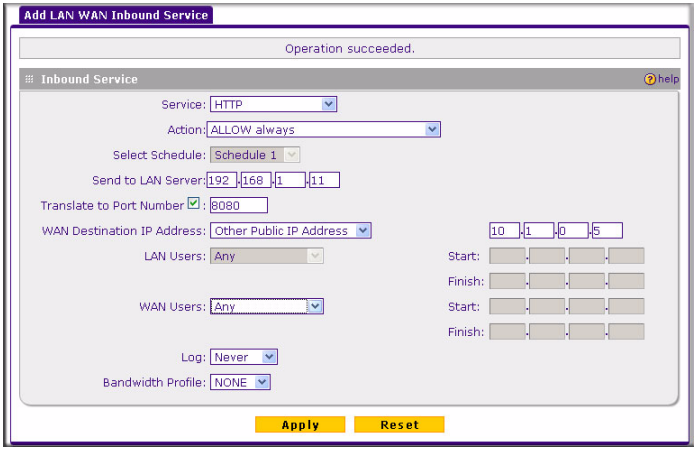


Figure 4-6

The following addressing scheme is used in this example:

- VPN firewall FVS336G
  - WAN1 primary public IP address: 10.1.0.1
  - WAN1 additional public IP address: 10.1.0.5
  - LAN IP address 192.168.1.1
- Web server PC on the VPN firewall's LAN
  - LAN IP address: 192.168.1.11
  - Port number for Web service: 8080

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

LAN WAN 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 new rule *below* all other inbound rules.

	**Note:** For security, NETGEAR strongly recommends that you avoid creating an exposed host. When a computer on your LAN 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.

Outbound Rules Example

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

LAN WAN Outbound Rule: Blocking Instant Messenger

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

Adding Customized Services

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

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

Although the FVS336G 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 menu shows a list of services that you have defined, as shown in Figure 4-7.

To define a new service, you must first 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 or newsgroups. When you have the port number information, you can enter it on the **Services** screen. You can configure up to 125 custom services.

To add a custom service:

1. Select **Security > Services** from the main menu. The **Services** screen is displayed.

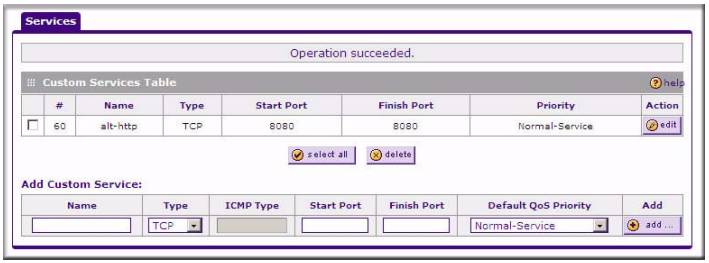


Figure 4-7

2. In the **Add Custom Services** section, enter a descriptive name for the service (this name is for your convenience).
3. Select the Layer 3 transport protocol of the service: TCP, UDP, or ICMP.
4. For TCP or UDP services, enter the first port of the range that the service uses. For ICMP services, enter the ICMP Type number.
5. For TCP or UDP services, 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 an existing service:

1. In the Custom Services Table, click the **Edit** button adjacent to the service you want to edit. The **Edit Service** screen is displayed.
2. Modify the parameters you wish to change.
3. Click **Apply** to confirm your changes. The modified service is displayed in the Custom Services Table.

Setting Quality of Service (QoS) Priorities

The QoS setting determines the priority of a service, which in turn determines the quality of that service for the traffic passing through the firewall. You can change the QoS Priority:

- On the **Services** screen in the Custom Services Table for customized services (see Figure 4-7).
- On the **Add LAN WAN Outbound Services** screen:

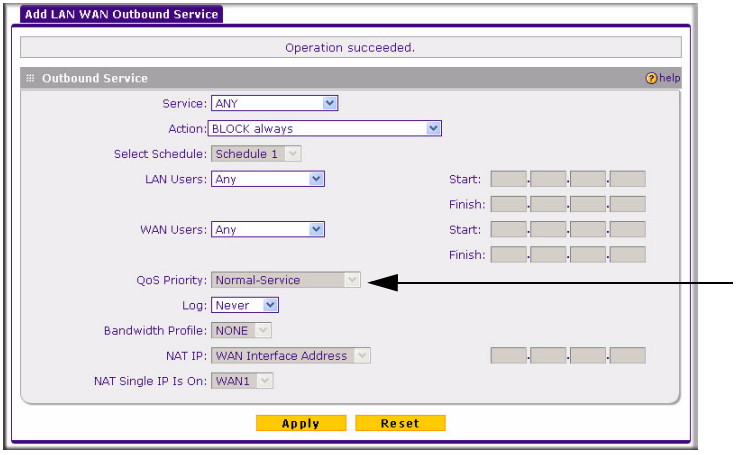


Figure 4-8

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 the data must be transferred over a link that has a low transmission cost. The IP packets for this service priority are marked with a ToS value of 1.
- **Maximize-Reliability.** Used when data needs to travel to the destination over a reliable link with little or no retransmission. The IP packets for this service 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 for the packet to reach the destination must be short (low link latency). The IP packets for this service priority are marked with a TOS value of 8.

Attack Checks

The Attack Checks menu 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 > Firewall** from the main menu and click **Attack Checks** to display the **Attack Checks** tab page.

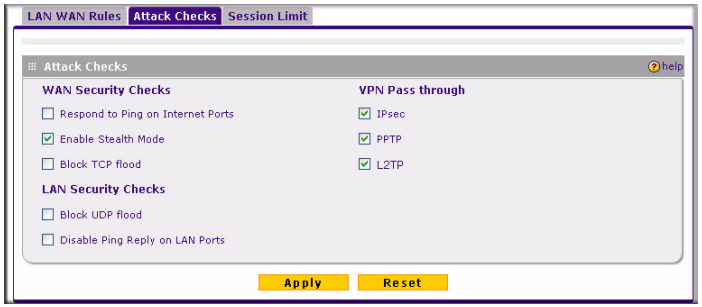


Figure 4-9

2. Check the boxes for the Attack Checks you wish to monitor. The various types of attack checks are listed and defined below.
3. 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 does not respond to an ICMP Echo (ping) packet coming from the Internet or WAN side. We recommend that you leave this option disabled to prevent hackers from easily discovering the VPN firewall via a ping, but it can be enabled as a diagnostic tool for connectivity problems.
  - **Enable Stealth Mode**—In stealth mode, the VPN firewall will not respond to port scans from the WAN or Internet, which makes it less susceptible to discovery and attacks.
  - **Block TCP Flood**. A SYN flood is a form of denial of service attack in which an attacker sends a succession of SYN requests to a target system. When the system responds, the attacker doesn't complete the connection, thus saturating the server with half-open connections. No legitimate connections can then be made.

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

- **LAN Security Checks**
  - **Block UDP flood—**A UDP flood is a form of denial of service attack in which the attacking machine sends a large number of UDP packets to random ports to the victim host. As a result, the victim host will check for the application listening at that port, see that no application is listening at that port, and reply with an ICMP Destination Unreachable packet.

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

    If flood checking is enabled, the VPN firewall will not accept more than 20 simultaneous, active UDP connections from a single computer on the LAN.
  - **Disable Ping Reply on LAN Ports**. To prevent the VPN firewall from responding to Ping requests from the LAN, click this checkbox.
  - **Disable DNS Proxy**. Whether DNS Proxy is enabled or disabled in the DHCP server configuration, the VPN firewall will service DNS requests sent to its own LAN IP address. To disable this service, check this checkbox.
- **VPN Pass through—**When the FVS336G is in NAT mode, all packets going to the Remote VPN Gateway are first filtered through NAT and then encrypted per the VPN policy.

  If a VPN client or gateway on the LAN side of the VPN firewall wants to connect to another VPN endpoint on the WAN, with the FVS336G between the two VPN end points, all encrypted packets will be sent to the FVS336G. Since the FVS336G filters the encrypted packets through NAT, the packets become invalid.

  IPSec, PPTP, and L2TP represent different types of VPN tunnels that can pass through the FVS336G. To allow the VPN traffic to pass through without filtering, enable those options for the type of tunnel(s) that will pass through the FVS336G.

Blocking Internet Sites (Content Filtering)

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

Several types of blocking are available:

- **Web Components blocking**. You can filter the following Web Component types: Proxy, Java, ActiveX, and Cookies. For example, by enabling Java filtering, “Java” files will be blocked. Certain commonly used web components can be blocked for increased security. Some of these components are can be used by malicious websites to infect computers that access them.
  - **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 Web site name (URL) or in a newsgroup name, will cause that site or newsgroup to be blocked by the VPN firewall.

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

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

Keyword application examples:

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

To enable Content Filtering:

1. Select **Security > Block Sites** to display he **Block Sites** screen.

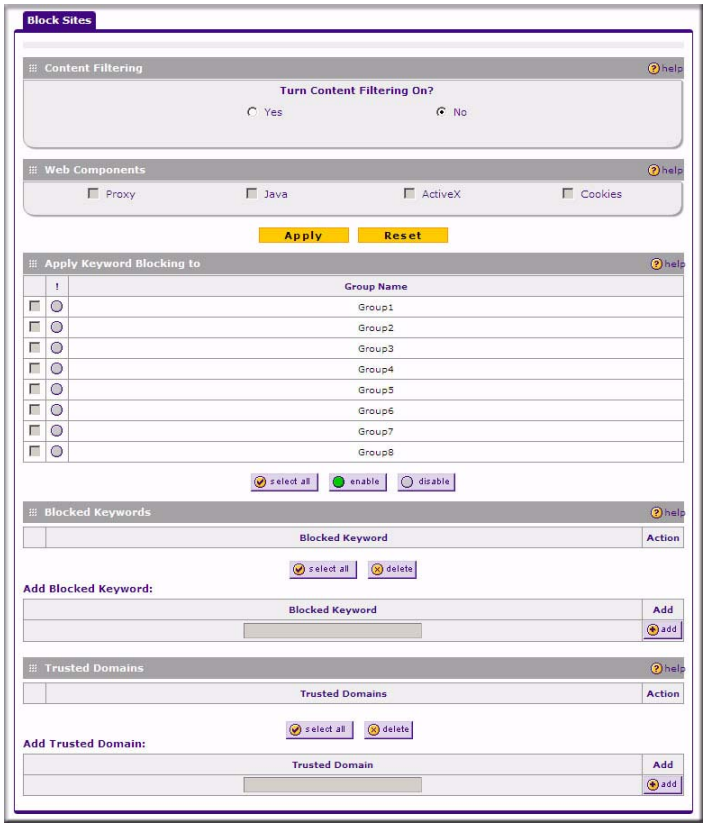


Figure 4-10

2. Select **Yes** to enable Content Filtering.
3. Click **Apply** to activate the menu controls.

4. Select any **Web Components** you wish to block and click **Apply.**
5. Select the groups to which Keyword Blocking will apply, then click **Enable** to activate Keyword blocking (or disable to deactivate Keyword Blocking).
6. Enter 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. In the **Add Trusted Domain** table, enter the name(s) of any domain for which the keyword filtering will be bypassed and click **Add**. The Trusted Domain will appear in the **Trusted Domains** table and will be exempt from filtering.

Configuring Source MAC Filtering

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

- By default, the source MAC address filter is disabled. Traffic received from any MAC address is allowed.
- When the source MAC address filter is enabled, outbound Internet traffic will be filtered using the **MAC Addresses** list in this menu. You can choose to block MAC addresses in the list or to allow only those addresses in the list.

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

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

1. Select **Security** > **Address Filter** > **Source MAC Filter** to display the **Source MAC Filter** tab page.

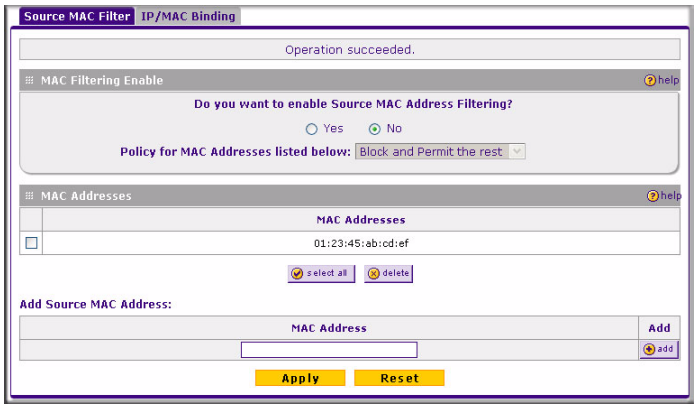


Figure 4-11

2. Click **Yes** to enable **Source MAC Filtering**.
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** box and click **Add**. The MAC address will appear in the **MAC Addresses** table. Repeat this process to add additional MAC addresses.

   A valid MAC address is six colon-separated pairs of hexadecimal digits (0 to 9 and a to f). For example: 01:23:45:ab:cd:ef.
5. Click **Add.** The MAC address will be added to the **MAC Addresses** table.
6. Click **Apply** to save your settings.

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

Configuring IP/MAC Address Binding Alerts

You can configure the FVS336G to drop packets and generate an alert when a device appears to have hijacked or spoofed another device's IP address. An IP address can be bound to a specific MAC address either by using a DHCP reserved address (see "Configuring DHCP Address Reservation" on page 3-8) or by manually binding in the IP/MAC Binding menu.

To enable IP/MAC address binding enforcement and alerts:

1. Select **Security > Address Filter** > **IP/MAC Binding** to display the **Source MAC Filter** tab page.

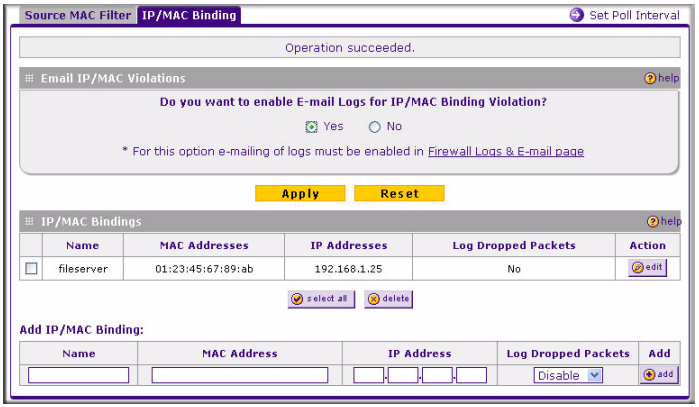


Figure 4-12

2. In the Email IP/MAC Violations frame, check the **Yes** radio button to enable IP/MAC address binding enforcement and alerts. Email alerts must be enabled (see "E-Mail Notifications of Event Logs and Alerts" on page 4-29).
3. Click **Apply.**
4. To add a manual binding entry, enter the following data in the **Add IP/MAC Bindings** section:
   a. Enter a **Name** for the bound host device.
   b. Enter the **MAC Address** and **IP Address** to be bound. 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.
   c. From the pull-down list, select whether dropped packets should be logged to a special counter. To view the counter, click the **Set Poll Interval** link at the top of the menu.
5. Click **Apply**. The specified binding will be added to the list.

Configuring Port Triggering

Port triggering allows some applications to function correctly that would otherwise be partially blocked by the firewall when the router is 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 router 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 router 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 inbound service rules.

Note these restrictions with Port Triggering:

- Only one PC can use a port triggering application at any time.
- After a PC has finished using a port triggering application, there is a time-out period before the application can be used by another PC. This is required because the VPN firewall cannot be sure when the application has terminated.

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

To add a port triggering rule:

1. Select **Security > Port Triggering** to display the **Port Triggering** tab page.

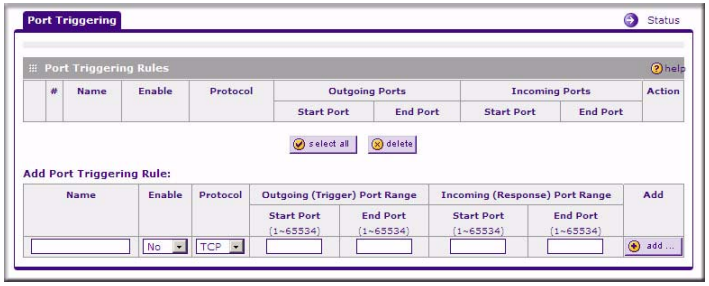


Figure 4-13

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, choose either TCP or UDP transport 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 check the status of the port triggering rules, click the **Status** option arrow to the right of the tab on the **Port Triggering** screen. The following data is displayed:

- Rule – The name of the port triggering rule.
- LAN IP Address – The IP address of the PC currently using this rule.
- Open Ports – The incoming ports associated with this rule. Incoming traffic using these ports will be sent to the LAN IP address above.
- Time Remaining – The time remaining before this rule is released, and thus available for other PCs. The timer is reset whenever incoming or outgoing traffic is received.

Setting a Schedule to Block or Allow Specific Traffic

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

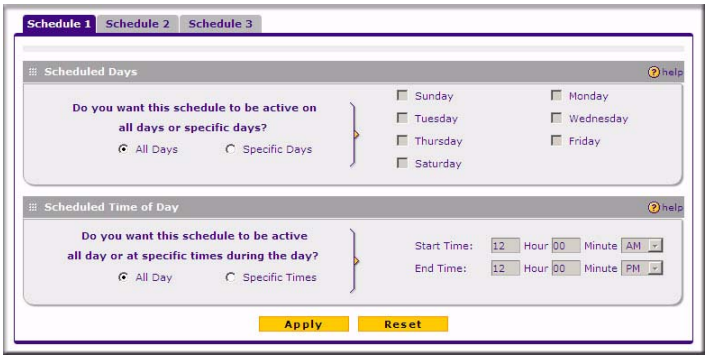


Figure 4-14

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

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

1. Select **Security** > **Schedule** to display the **Schedule 1** tab page.
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.**

Configuring a Bandwidth Profile

To prevent one user or group from using excessive inbound or outbound bandwidth, you can define a bandwidth profile to set a minimum and maximum bandwidth for an individual or group. You can apply a defined profile in a firewall rule to limit specific protocols or all traffic (see “Using Rules to Block or Allow Specific Kinds of Traffic” on page 4-2).

To create a bandwidth profile:

1. Select **Security** from the main menu and **Bandwidth Profile** from the submenu. The **Bandwidth Profile** menu will display.

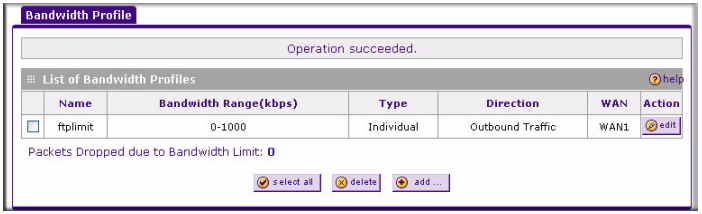


Figure 4-15

The **List of Bandwidth Profiles** displays existing profiles.

2. To create a new bandwidth profile, click **add**. The **Add Bandwidth Profile** menu will display.

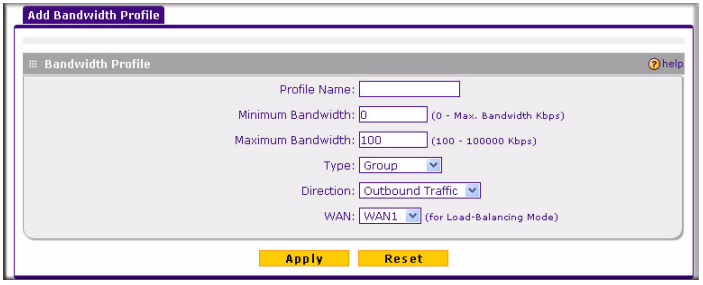


Figure 4-16

3. Enter the following data in the **Add IP/MAC Bindings** section:
   a. Enter a **Profile Name.** This name will become available in the firewall rules definition menus.
   b. Enter the **Minimum Bandwidth** and **Maximum Bandwidth** to be allowed.
   c. From the **Type** pull-down box, select whether the profile will apply to a group or individual.
   d. From the **Direction** pull-down box, select whether the profile will apply to outbound or inbound traffic.
4. Click **Apply**. The new bandwidth profile will be added to the list.

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 FVS336G 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 > Firewall > Session Limit** to display the Session Limit tab page.

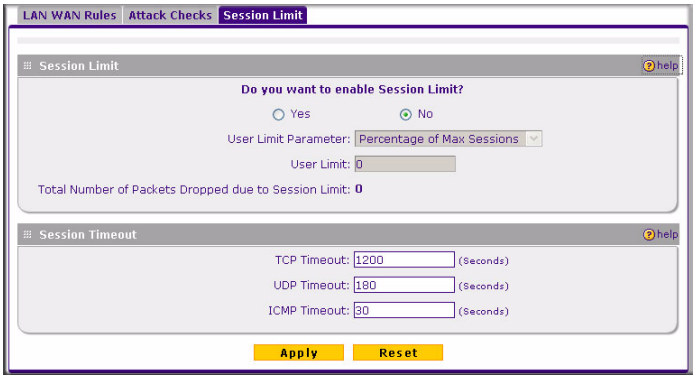


Figure 4-17

2. Click **Yes** to enable Session Limits.
3. In the pull-down menu, select whether you will limit sessions by percentage or by absolute number. The percentage is computed based on the total connection capacity of the device.When setting a limit based on absolute number, note that some protocols (for example, FTP and RSTP) create two sessions per connection.
4. Click **Apply**.

To monitor session limiting, return to this menu periodically and check the display of **Total Number of Packets Dropped due to Session Limit**, which indicates that session limits have been reached.

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 you input on the **Firewall Logs & E-mail** menu. In addition, if you have set up Content Filtering on the Block Sites screen (see "Blocking Internet Sites (Content Filtering)" on page 4-18), 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 9-4.

Administrator Tips

Consider the following operational items:

1. As an option, you can enable remote management if you have to manage distant sites from a central location (see "Enabling Remote Management Access" on page 8-10).
2. Although rules (see "Using Rules to Block or Allow Specific Kinds of Traffic" on page 4-2) are the basic way of managing the traffic through your system, you can further refine your control with the following optional features of the VPN firewall:
   - Groups and hosts (see "Managing Groups and Hosts (LAN Groups)" on page 3-5)
   - Services (see "About Services-Based Rules" on page 4-3)
   - Schedules (see "Setting a Schedule to Block or Allow Specific Traffic" on page 4-26)
   - Block sites (see "Blocking Internet Sites (Content Filtering)" on page 4-18)
   - Source MAC filtering (see "Configuring Source MAC Filtering" on page 4-21)
   - Port triggering (see "Configuring Port Triggering" on page 4-24)

Chapter 5
Virtual Private Networking Using IPsec

This chapter describes how to use the IPsec virtual private networking (VPN) features of the ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN to provide secure, encrypted communications between your local network and a remote network or computer.

This chapter contains the following sections:

Considerations for Dual WAN Port Systems

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

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

Refer to "Virtual Private Networks (VPNs)" on page C-10 for more on the IP addressing requirements for VPN in the dual WAN modes. For instructions on how to select and configure a dynamic DNS service for resolving FQDNs, see "Configuring Dynamic DNS (Optional)" on page 2-16. For instructions on WAN mode configuration, see "Configuring the WAN Mode (Required for Dual WAN)" on page 2-10.

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

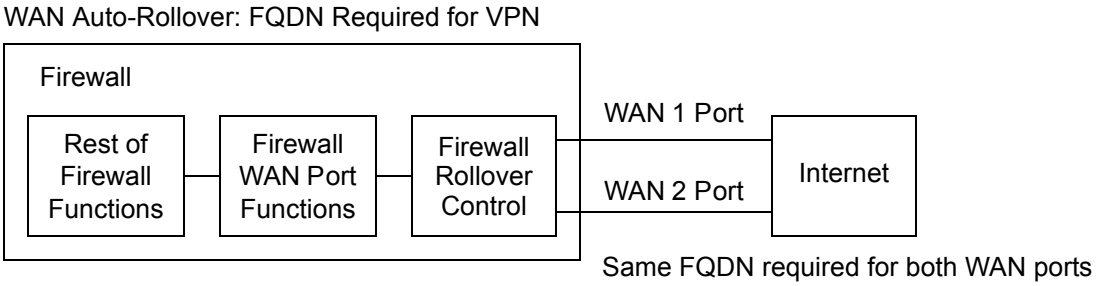


Figure 5-1

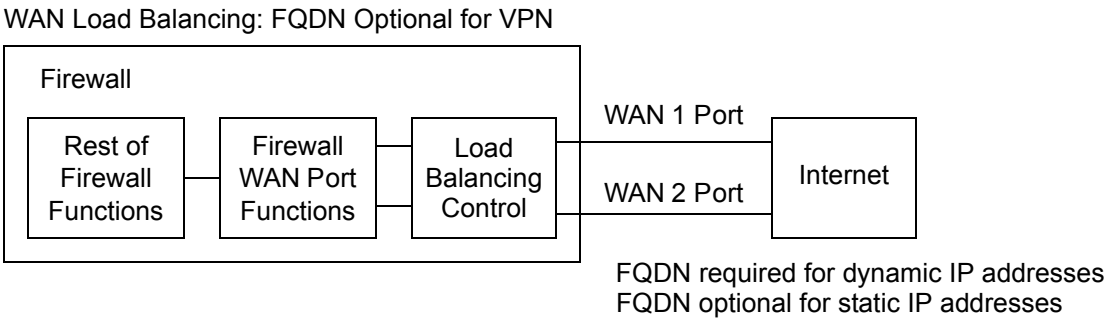


Figure 5-2

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

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

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

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

Using the VPN Wizard for Client and Gateway Configurations

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

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

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

Configuring a VPN tunnel connection requires that all settings and parameters on both sides of the VPN tunnel match or mirror each other precisely, which can be a daunting task. The VPN Wizard efficiently guides you through the setup procedure with a series of questions that will determine the IPsec keys and VPN policies it sets up. The VPN Wizard will also set the parameters for the network connection: Security Association, traffic selectors, authentication algorithm, and encryption. The parameters used by the VPN wizard are based on the recommendations of the VPN Consortium (VPNC), an organization that promotes multi-vendor VPN interoperability.

Creating Gateway to Gateway VPN Tunnels with the Wizard

Figure 5-3

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

1. Select **VPN > IPsec VPN > VPN Wizard** to display the VPN Wizard tab page.
   To view the wizard default settings, click the VPN Default values link. You can modify these settings after completing the wizard.

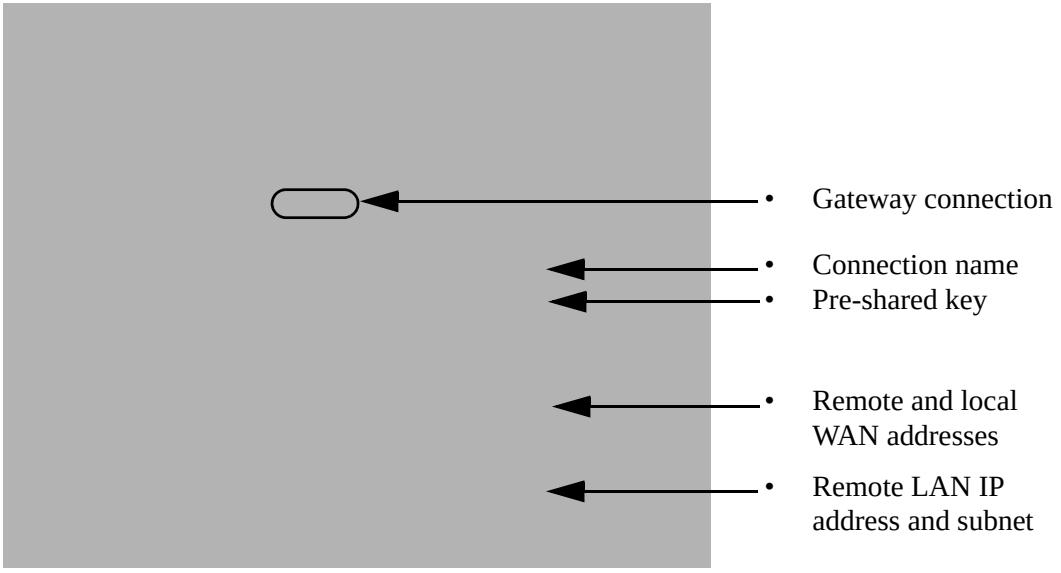


Figure 5-4

2. Select **Gateway** as your connection type.
3. Create a **Connection Name**. Enter a descriptive name for the connection. This name used to help you manage the VPN settings; is not supplied to the remote VPN endpoint.
4. Enter a **Pre-shared Key**. The key must be entered both here and on the remote VPN gateway, or the remote VPN client. This key must be a minimum of 8 characters and should not exceed 49 characters.
5. Choose which WAN port to use as the VPN tunnel end point.

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

6. Enter the **Remote and Local WAN IP Addresses or Internet Name**s of the gateways which will connect.

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

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

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

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

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

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

8. Click **Apply** to save your settings: the VPN Policies page shows the policy is now enabled.

Figure 5-5

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

After both firewalls are configured, go to **VPN > IPsec VPN > Connection Status** to display the status of your VPN connections.

Figure 5-6

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

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

Creating a Client to Gateway VPN Tunnel

Figure 5-7

Follow these steps to configure the a VPN client tunnel:

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

Use the VPN Wizard Configure the Gateway for a Client Tunnel

1. From the main menu, go to **VPN** > **IPSec VPN** > **VPN Wizard**. The VPN Wizard displays.

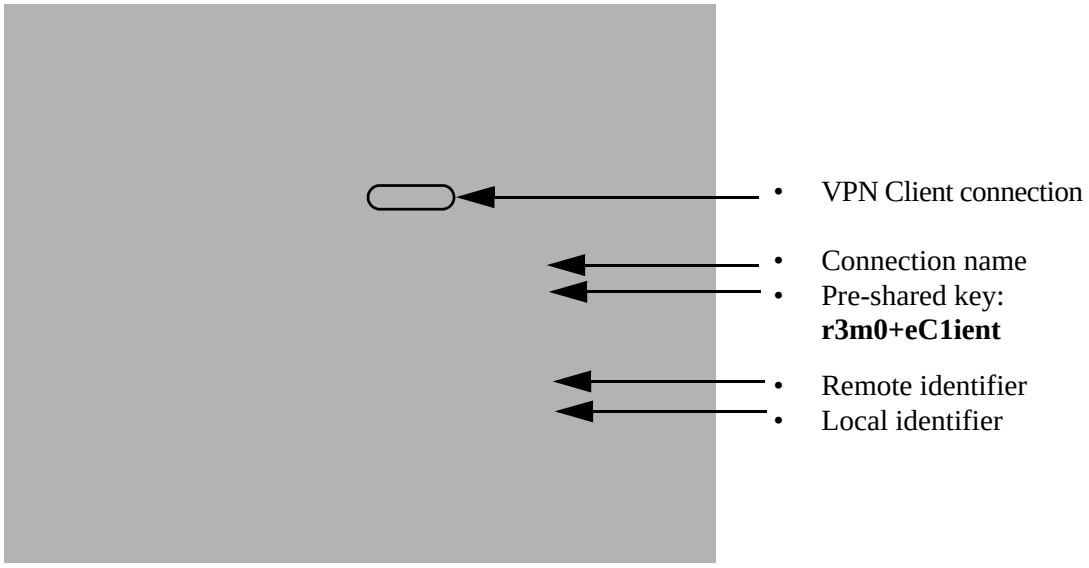


Figure 5-8

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

   This descriptive name is not supplied to the remote VPN client; it is only for your reference.
4. Enter a **Pre-shared Key**; in this example, we are using **r3m0+eC1ient,** which must also be entered in the VPN client software. The key length must be 8 characters minimum and cannot exceed 49 characters.
5. Choose which WAN port to use as the VPN tunnel end point.

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

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

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

7. Click **Apply** to save your settings: the VPN Policies page shows the policy is now enabled.

Figure 5-9

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

From a PC with the NETGEAR Prosafe VPN Client installed, configure a VPN client policy to connect to the FVS336G. Follow these steps to configure your VPN client.

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

Figure 5-10

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

Figure 5-11

Fill in the other options according to the instructions below.

- Under Connection Security, verify that the Secure radio button is selected.
- From the **ID Type** pull-down menu, choose **IP Subnet**.
- Enter the LAN IP **Subnet Address** and **Subnet Mask** of the FVS336G 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 FVS336G 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 FVS336G; in this example, we are using 21.208.216.81.

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

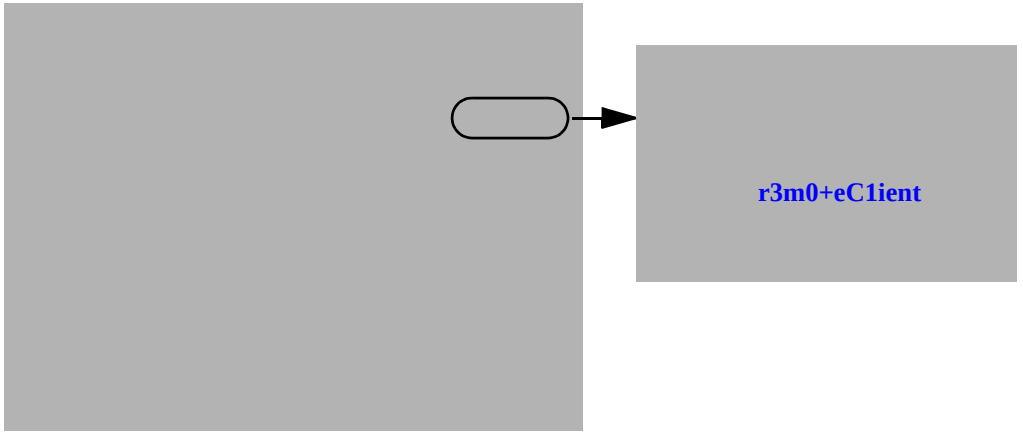


Figure 5-12

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

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

Figure 5-13

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

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

Testing the Connections and Viewing Status Information

Both the NETGEAR VPN Client and the FVS336G provide VPN connection and status information. This information is useful for verifying the status of a connection and troubleshooting problems with a connection.

NETGEAR VPN Client Status and Log Information

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

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

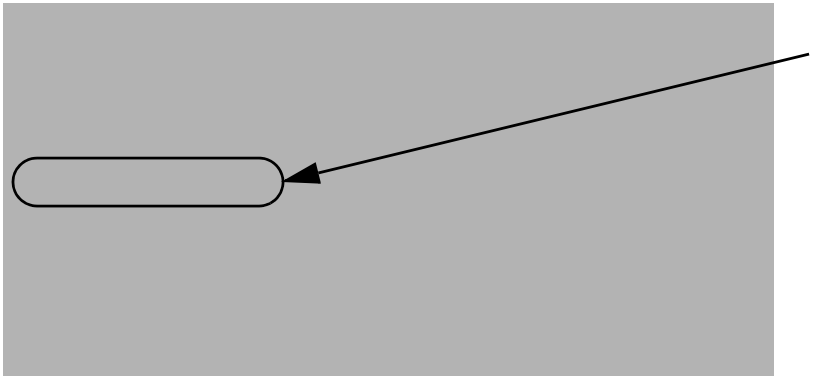


Figure 5-14

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

Figure 5-15

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

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

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

Figure 5-16

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

Figure 5-17

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

Table 5-2.

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

FVS336G VPN Connection Status and Logs

To view FVS336G VPN connection status, go to **VPN > Connection Status**.

Figure 5-18

To view FVS336G VPN logs, go to **Monitoring** > **VPNLogs**.

Figure 5-19

Managing VPN Policies

After you use the VPN Wizard to set up a VPN tunnel, a VPN policy and an IKE policy are stored in separate 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.

Managing 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 the following occur:

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 Tab Page

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 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 List of IKE Policies. Each policy contains the following data:

- **Name**. Uniquely identifies each IKE policy. The name is chosen by you and used for managing your policies; it is not supplied to the remote VPN endpoint.
- **Mode**. Two modes are available: either Main or Aggressive.
  - Main Mode is slower but more secure.
  - Aggressive mode is faster but less secure. (If specifying either a FQDN or a User FQDN name as the Local ID/Remote ID, aggressive mode is automatically selected.)
- **Local ID**. The IKE/ISAKMP identify of this device. (The remote VPN must have this value as their Remote ID.)
- **Remote ID**. The IKE/ISAKMP identify of the remote VPN gateway. (The remote VPN must have this value as its 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**. The Diffie-Hellman (DH) group used when exchanging keys. The DH group sets the number of bits. The VPN Wizard default setting is Group 2. (This setting must match the remote VPN.)

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

Managing VPN Policies

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

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

In addition, a Certificate Authority (CA) can also be used to perform authentication (see "Managing Certificates" on page 7-10). 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 Tab Page

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

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

Only one Client Policy may configured at a time (noted by an "*" next to the policy name). The Policy Table contains the following fields:

- **! (Status)**. Indicates whether the policy is enabled (green circle) or disabled (grey circle). To Enable or Disable a Policy, check the box adjacent to the circle and click **Enable** or **Disable**, as required.
- **Name**. Each policy is given a unique name (the Connection Name when using the VPN Wizard).
- **Type**. The Type is “Auto” or “Manual” as described previously (Auto is used during VPN Wizard configuration).
- **Local**. IP address (either a single address, range of address or subnet address) on your local LAN. Traffic must be from (or to) these addresses to be covered by this policy. (The Subnet address is supplied as the default IP address when using the VPN Wizard).
- **Remote**. IP address or address range of the remote network. Traffic must be to (or from) these addresses to be covered by this policy. (The VPN Wizard default requires the remote LAN IP address and subnet mask).
- **Auth**. Authentication Algorithm used for the VPN tunnel. The default setting using the VPN Wizard is SHA1. (This setting must match the Remote VPN.)
- **Encr**. Encryption algorithm used for the VPN tunnel. 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.

Configuring Extended Authentication (XAUTH)

When connecting many VPN clients to a VPN firewall, 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 firewall 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 can be 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 User Database to be authenticated against XAUTH, or you must enable a RADIUS-CHAP or RADIUS-PAP server.

	Note: You cannot modify an existing IKE policy to add **XAUTH** while the IKE policy 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 > IPsec VPN from the main menu.
2. Click the **IKE Policies** tab. The IKE Policies screen is displayed.

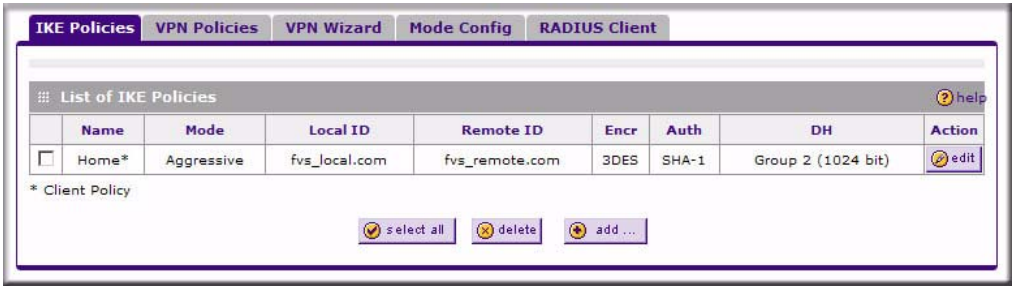


Figure 5-20

3. You can add **XAUTH** to an existing IKE Policy by clicking **Edit** adjacent to the policy to be modified or you can create a new IKE Policy incorporating **XAUTH** by clicking **Add.**
4. In the **Extended Authentication** section, choose the **Authentication Type** from the pull-down menu which will be used to verify user account information. Select

- **Edge Device** to use this VPN firewall as a VPN concentrator where one or more gateway tunnels terminate. When this option is chosen, you will need to specify the authentication type to be used in verifying credentials of the remote VPN gateways.
  - **User Database** to verify against the VPN firewall's user database. Users must be added through the User Database screen (see "User Database Configuration" on page 5-20).
  - **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 5-20).
- **IPsec Host** if you want to be authenticated by the remote gateway. In the adjacent **Username** and **Password** fields, type in the information user name and password associated with the IKE policy for authenticating this gateway (by the remote gateway).

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

User Database Configuration

When XAUTH is enabled as an Edge Device, users must be authenticated either by a local User Database account or by an external RADIUS server. Whether or not you use a RADIUS server, you may want some users to be authenticated locally. These users must be added to the List of Users table, as described in "Creating a New User Account" on page 7-4.

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 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 to verify this information first against a local User Database (if RADIUS-PAP is enabled) and then by relaying the information to a central authentication server such as a RADIUS server.

To configure the Primary RADIUS Server:

1. Select VPN > IPsec VPN from the main menu.

2. Click the **RADIUS Client** tab. The **RADIUS Client** screen is displayed.

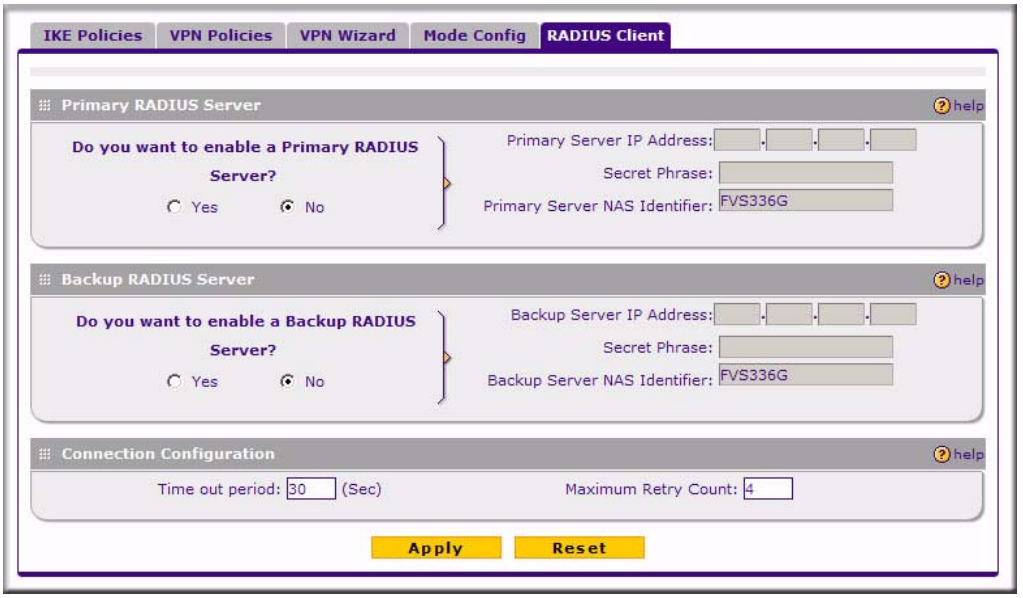


Figure 5-21

3. To activate (enable) the Primary RADIUS server, click the **Yes** radio button. The primary server options become active.
4. Configure the following entries:
   - **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** (Network Access Server). This Identifier MUST be present in a RADIUS request. Ensure that NAS Identifier is configured identically on both client and server.

The FVS336G 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 FVS336G'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.

5. Enable a Backup RADIUS Server (if required).
6. Set the **Time Out Period**, in seconds, that the VPN firewall should wait for a response from the RADIUS server.
7. Set the **Maximum Retry Count.** This is the number of tries the VPN firewall will make to the RADIUS server before giving up.
8. Click **Apply** to save the settings.

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

Assigning IP Addresses to Remote Users (ModeConfig)

To simply the process of connecting remote VPN clients to the FVS336G, the ModeConfig module can be used to assign IP addresses to remote users, including a network access IP address, subnet mask, and name server addresses from the 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 FVS336G ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN
  - WAN IP address: 172.21.4.1
  - LAN IP address/subnet: 192.168.2.1/255.255.255.0
- NETGEAR ProSafe VPN Client software IP address: 192.168.1.2

Mode Config Operation

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

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

Configuring the VPN Firewall

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

To configure the Mode Config menu:

1. Click **VPN** in the main menu.
2. Click **IPsec VPN** in the submenu.
3. Click the **Mode Config** tab. The Mode Config tab is displayed.

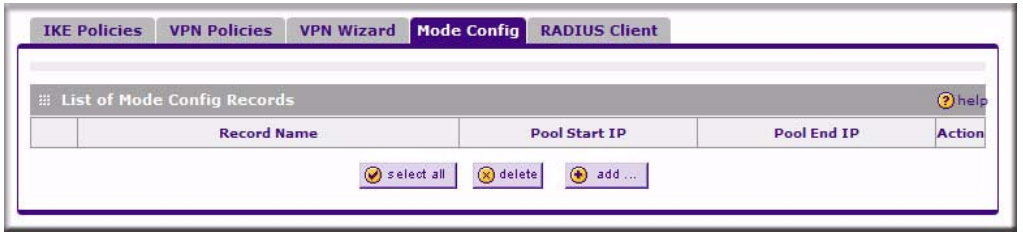


Figure 5-22

4. Click **Add.** The **Add Mode Config Record** screen is displayed

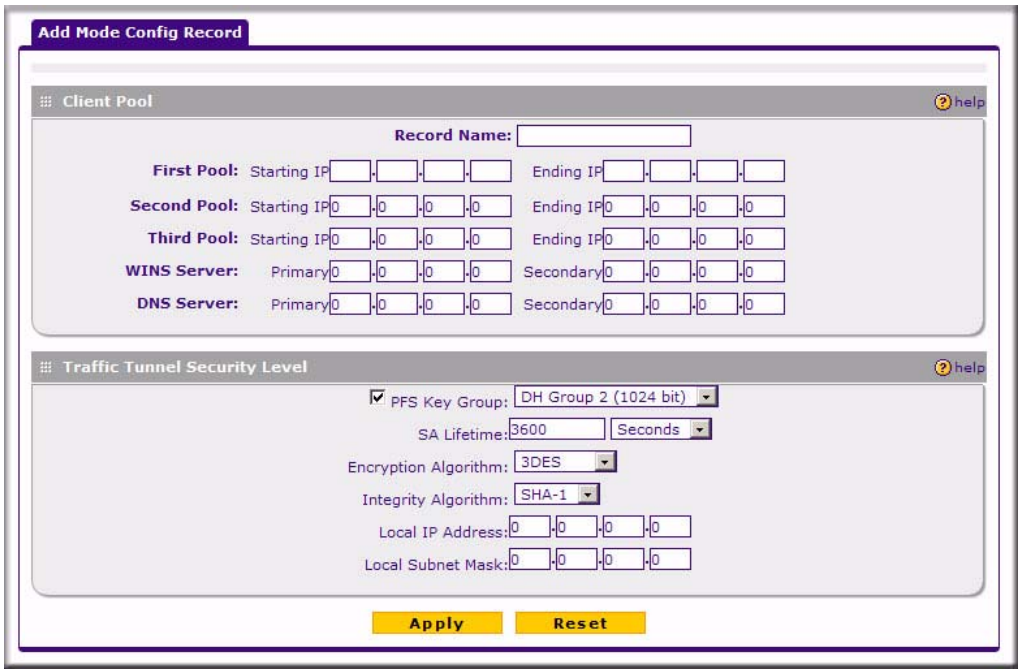


Figure 5-23

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

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

7. If you have a WINS Server on your local network, enter its IP address.
8. Enter one or two DNS Server IP addresses to be used by remote VPN clients.
9. If you enable Perfect Forward Secrecy (PFS), choose DH Group 1 or 2. This setting must match exactly the configuration of the remote VPN client,
10. 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.)

11. 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

12. Click **Apply**.

The new record should appear in the VPN Remote Host Mode Config Table.

Next, you must configure an IKE Policy:

1. Click VPN > IPsec VPN in the main menu. The **IKE Policies** screen is displayed showing the current policies in the **List of IKE Policies** Table.

2. Click **Add** to configure a new IKE Policy. The **Add IKE Policy** screen is displayed.

3. Enable **Mode Config** by checking the **Yes** radio button 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 button.)

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

4. In the **General** section:

a. Enter a descriptive name in the Policy Name Field such as “salesperson”. This name will be used as part of the remote identifier in the VPN client configuration.

b. Set Direction/Type to Responder.

c. The Exchange Mode will automatically be set to Aggressive.

5. For Local information:

a. Select Fully Qualified Domain Name for the Local Identity Type.

b. Enter an identifier in the Remote Identity Data field that is not used by any other IKE policies. This identifier will be used as part of the local identifier in the VPN client configuration.

6. Specify the IKE SA parameters. These settings must be matched in the configuration of the remote VPN client. Recommended settings are:

- Encryption Algorithm: 3DES
- Authentication Algorithm: SHA-1
- Diffie-Hellman: Group 2
- SA Lifetime: 3600 seconds

7. Enter a Pre-Shared Key that will also be configured in the VPN client.
8. XAUTH is disabled by default. To enable XAUTH, choose one of the following:
   - **Edge Device** to use this 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 this gateway to be authenticated by the remote gateway. Enter a Username and Password to be associated with the IKE policy. When this option is chosen, you will need to specify the user name and password to be used in authenticating this gateway (by the remote gateway).

   For more information on XAUTH, see "Configuring XAUTH for VPN Clients" on page 5-19.
9. If Edge Device was enabled, choose 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 "Creating a New User Account" on page 7-4 or "RADIUS Client Configuration" on page 5-20).

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.

10. Click **Apply.** The new policy will appear in the 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.
   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, choose 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 choose Secure Gateway Tunnel from the pull-down menu.

e. From the ID Type pull-down menu, choose Domain name and enter the FQDN of the VPN firewall; in this example it is “local_id.com”.

f. Choose Gateway IP Address from the second pull-down menu and enter the WAN IP address of the VPN firewall; in this example it is “172.21.4.1”.

2. From the left side of the menu, click My Identity and enter the following information:

a. Click **Pre-Shared Key** and enter the key you configured in the FVS336G IKE menu.

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

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

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

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

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

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

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

b. Check the Enable Perfect Forward Secrecy (PFS) box, and choose 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 choose Proposal 1. Enter the Authentication values to match those in the VPN firewall ModeConfig Record menu.

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

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

To test the connection:

1. Right-click on the VPN client icon in the Windows toolbar and click Connect. The connection policy you configured will appear; in this case “My Connections\modecfg_test”.

2. Click on the connection. Within 30 seconds the message “Successfully connected to MyConnections/modecfg_test is displayed and the VPN client icon in the toolbar will read “On”.
3. From the client PC, ping a computer on the VPN firewall LAN.

Configuring Keepalives and Dead Peer Detection

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

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

Configuring Keepalive

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 > Policies from the main menu.
2. Click the **VPN Policies** tab, then click the **edit** button next to the desired VPN policy.

3. In the **General** menu frame of the **Edit VPN Policy** menu, locate the keepalive configuration settings, as shown in Figure 5-24:

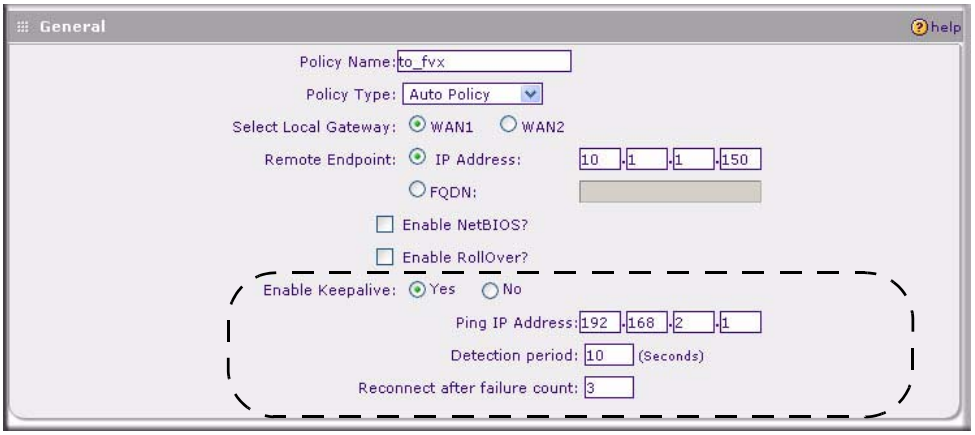


Figure 5-24

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 FVS336G senses a tunnel connection failure, it forces a reestablishment of the tunnel.
8. Click **Apply** at the bottom of the menu.

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** menu frame of the **Edit IKE Policy** menu, locate the Dead Peer Detection configuration settings, as shown in Figure 5-25.

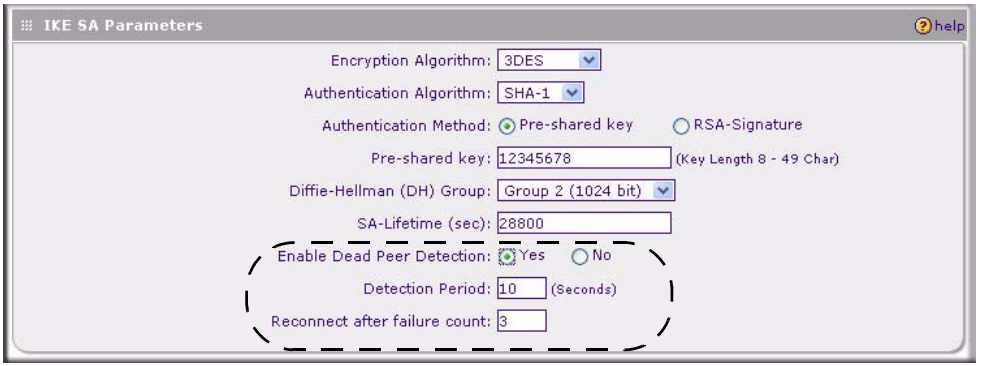


Figure 5-25

4. Click the **Yes** radio button to **Enable Dead Peer Detection**.
5. Enter the **Detection Period** to set the interval between consecutive DPD R-U-THERE messages. DPD R-U-THERE messages are sent only when the IPSec traffic is idle. The default is 10 seconds.
6. In **Reconnect after failure count**, set the number of DPD failures allowed before tearing down the connection. The default is 3 failures. When the FVS336G senses an IKE connection failure, it deletes the IPSec and IKE Security Association and forces a reestablishment of the connection.
7. Click **Apply** at the bottom of the menu.

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 FVS336G to bridge NetBIOS traffic over the VPN tunnel. To enable NetBIOS bridging on a configured VPN tunnel, follow these steps:

1. Select **VPN** > **Policies** from the main menu.
2. Click the **VPN Policies** tab, then click the **edit** button next to the desired VPN policy.

3. In the **General** menu frame of the **Edit VPN Policy** menu, click the **Enable NetBIOS** check box, as shown in Figure 5-26.

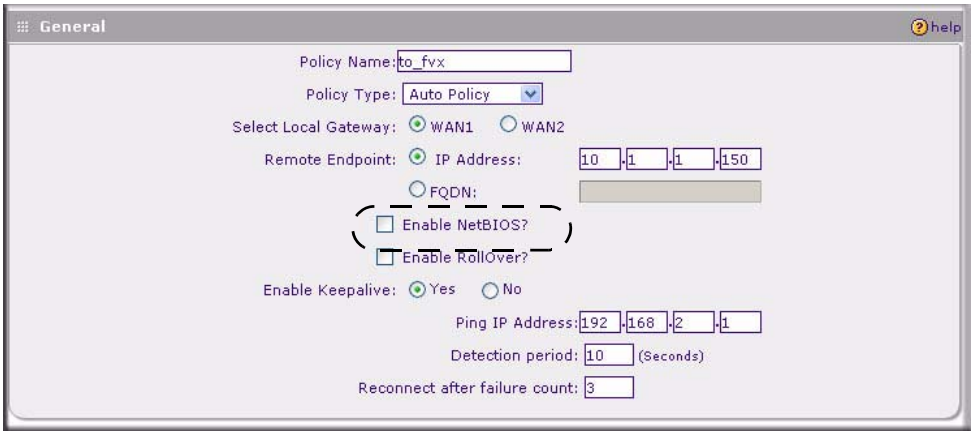


Figure 5-26

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

Chapter 6
Virtual Private Networking Using SSL Connections

The FVS336G ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN provides a hardware-based SSL VPN solution designed specifically to provide remote access for mobile users to their corporate resources, bypassing the need for a pre-installed VPN client on their computers. Using the familiar Secure Sockets Layer (SSL) protocol, commonly used for e-commerce transactions, the FVS336G can authenticate itself to an SSL-enabled client, such as a standard web browser. Once the authentication and negotiation of encryption information is completed, the server and client can establish an encrypted connection. With support for 10 concurrent sessions, users can easily access the remote network for a customizable, secure, user portal experience from virtually any available platform.

This chapter contains the following sections:

Understanding the Portal Options

The FVS336G's SSL VPN portal can provide two levels of SSL service to the remote user:

- VPN Tunnel

  The FVS336G can provide the full network connectivity of a VPN tunnel using the remote user's browser in the place of a traditional IPsec VPN client. The SSL capability of the user's browser provides authentication and encryption, establishing a secure connection to the VPN

firewall. Upon successful connection, an ActiveX-based SSL VPN client is downloaded to the remote PC that will allow the remote user to virtually join the corporate network. The SSL VPN Client provides a PPP (point-to-point) connection between the client and the VPN firewall, and a virtual network interface is created on the user's PC. The VPN firewall will assign the PC an IP address and DNS server IP addresses, allowing the remote PC to access network resources in the same manner as if it were connected directly to the corporate network, subject to any policy restrictions configured by the administrator.

- Port Forwarding

  Like VPN Tunnel, Port Forwarding is a web-based client that installs transparently and then creates a virtual, encrypted tunnel to the remote network. However, Port Forwarding differs from VPN Tunnel in several ways. For example, Port Forwarding:

  – Only supports TCP connections, not UDP or other IP protocols.

  – Detects and reroutes individual data streams on the user's PC to the Port Forwarding connection rather than opening up a full tunnel to the corporate network.

  – Offers more fine grained management than VPN Tunnel. The administrator defines individual applications and resources that will be available to remote users.

The SSL VPN portal can present the remote user with one or both of these SSL service levels, depending on the configuration by the administrator.

Planning for SSL VPN

To set up and activate SSL VPN connections, you will perform these basic steps in this order:

1. Edit the existing SSL Portal or create a new one.

When remote users log in to the SSL VPN firewall, they see a portal page that you can customize to present the resources and functions that you choose to make available.

2. Create one or more authentication domains for authentication of SSL VPN users.

When remote users log in to the SSL VPN firewall, they must specify a domain to which their login account belongs. The domain determines the authentication method to be used and the portal layout that will be presented, which in turn determines the network resources to which they will have access. Because you must assign a portal layout when creating a domain, the domain is created after you have created the portal layout.

3. Create one or more groups for your SSL VPN users.

When you define the SSL VPN policies that determine network resource access for your SSL VPN users, you can define global policies, group policies, or individual policies. Because you must assign an authentication domain when creating a group, the group is created after you have created the domain.

4. Create one or more SSL VPN user accounts.

   Because you must assign a group when creating a SSL VPN user account, the user account is created after you have created the group.

5. For port forwarding, declare the servers and services.

   Create a list of servers and services that can be made available through user, group, or global policies. You can also associate fully qualified domain names with these servers. The VPN firewall will resolve the names to the servers using the list you have created.

6. For VPN tunnel service, configure the virtual network adapter.

   In the VPN tunnel option, the VPN firewall creates a virtual network adapter on the remote PC that will function as if it were on the local network. Configure the portal's SSL VPN Client to define a pool of local IP addresses to be issued to remote clients, as well as DNS addresses. Declare static routes or grant full access to the local network, subject to additional policies.

7. For simplifying policies, define network resource objects.

   Network resource objects are groups of IP addresses, IP address ranges, and services. By defining resource objects, you can more quickly create and configure network policies.

8. Configure the policies.

   Policies determine access to network resources and addresses for individual users, groups, or everyone.

Creating the Portal Layout

The SSL VPN Portal Layouts menu allows you to create a custom page that remote users will see when they log into the portal. Because the page is completely customizable, it provides an ideal way to communicate remote access instructions, support information, technical contact info, or VPN-related news updates to remote users. The page is also well-suited as a starting page for restricted users; if mobile users or business partners are only permitted to access a few resources, the page you create will present only the resources relevant to these users.

Portal Layouts are applied by selecting from available portal layouts in the configuration of a Domain. When you have completed your Portal Layout, you can apply the Portal Layout to one or more authentication domains (see XREF to apply a Portal Layout to a Domain). You can also make the new portal the default portal for the SSL VPN gateway by selecting the default radio button adjacent to the portal layout name.

Note: The default portal address is **https://<*IP_Address*>/portal/SSL-VPN**. The domain **geardomain** is attached to the SSL-VPN portal.

The VPN firewall administrator may define individual layouts for the SSL VPN portal. The layout configuration includes the menu layout, theme, portal pages to display, and web cache control options. The default portal layout is the SSL-VPN portal. You can add additional portal layouts. You can also make any portal the default portal for the SSL VPN firewall by clicking the default button in the Action column of the List of Layouts, to the right of the desired portal layout.

To create a New Portal Layout:

1. Select VPN > SSL VPN from the main menu, and then select the Portal Layouts tab. The Portal Layouts screen will display.

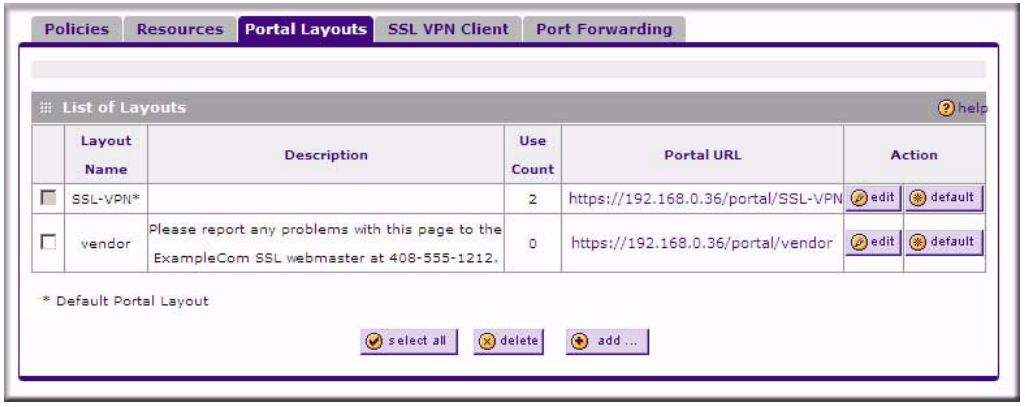


Figure 6-1

2. Click **Add**. The Add Portal Layout screen is displayed.

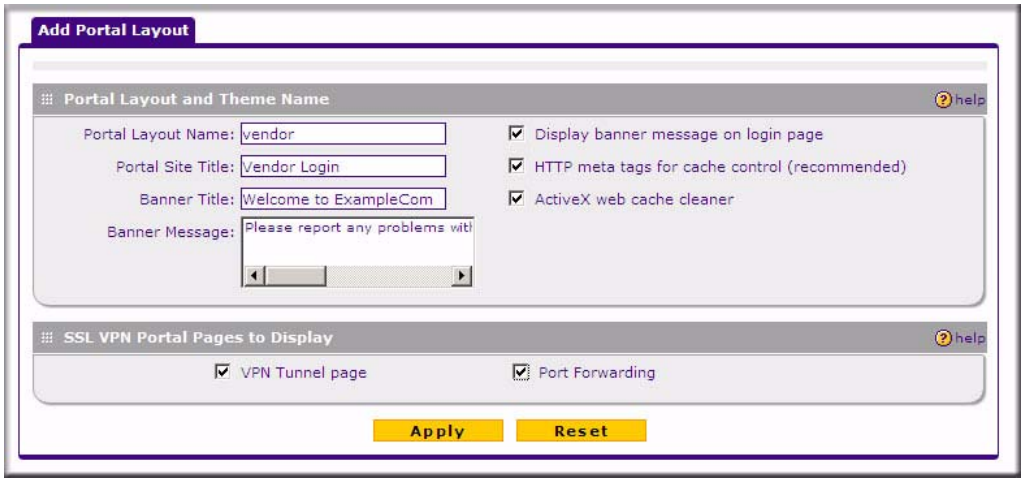


Figure 6-2

3. In the **Portal Layout and Theme Name** section of the menu, configure the following entries:

   a. Enter a descriptive name for the portal layout in the **Portal Layout Name** field. This name will be part of the path of the SSL VPN portal URL.

	Note: Custom portals are accessed at a different URL than the default portal. For example, if your SSL VPN portal is hosted at **https://vpn.company.com**, and you created a portal layout named “sales”, then users will be able to access the sub-site at **https://vpn.company.com/portal/sales**.

   Only alphanumeric characters, hyphen (-), and underscore (_) are accepted for the Portal Layout Name. If you enter other types of characters or spaces, the layout name will be truncated before the first non-alphanumeric character. Note that unlike most other URLs, this name is case sensitive.

   b. In the **Portal Site Title** field, enter a title that will appear at the top of the user’s web browser window.

   c. To display a banner message to users before they log in to the portal, enter the banner title text in the **Banner Title** field. Also enter the banner message text in the **Banner Message** text area. Enter a plain text message or include HTML and JavaScript tags. The maximum length of the login page message is 4096 characters. Select the **Display banner message**

on login page checkbox to show the banner title and banner message text on the Login screen as shown below

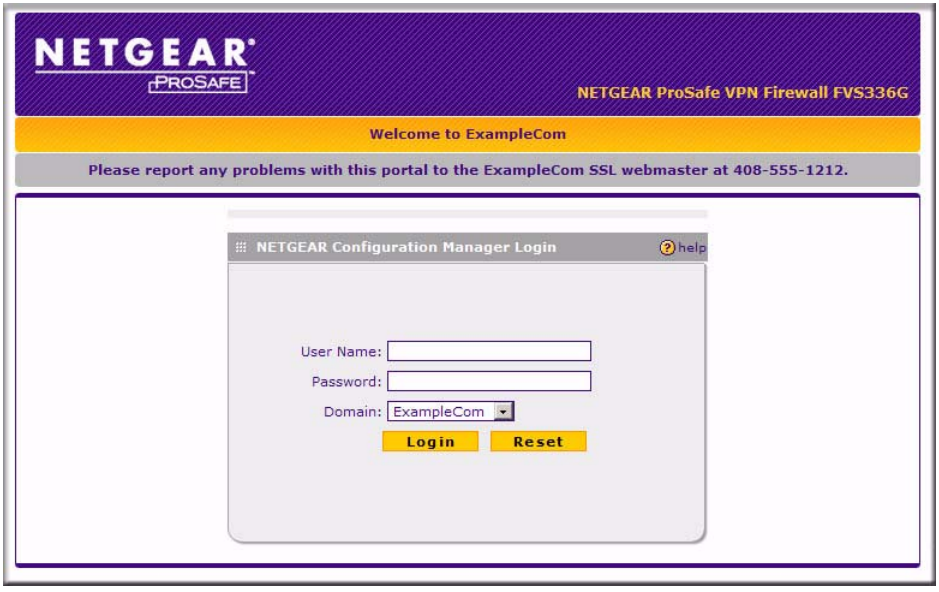


Figure 6-3

As shown in the figure, the banner title text is displayed in the orange header bar. The banner message text is displayed in the grey header bar.

d. Check the **Enable HTTP meta tags for cache control** checkbox to apply HTTP meta tag cache control directives to this Portal Layout. Cache control directives include:

```
<meta http-equiv=”pragma” content=”no-cache”>
<meta http-equiv=”cache-control” content=”no-cache”>
<meta http-equiv=”cache-control” content=”must-revalidate”>
```

These directives help prevent clients browsers from caching SSL VPN portal pages and other web content.

	Note: NETGEAR strongly recommends enabling HTTP meta tags for security reasons and to prevent out-of-date web pages, themes, and data being stored in a user’s web browser cache.

e. Check the “**ActiveX web cache cleaner** checkbox to load an ActiveX cache control when users log in to the SSL VPN portal.

The web cache cleaner will prompt the user to delete all temporary Internet files, cookies and browser history when the user logs out or closes the web browser window. The ActiveX web cache control will be ignored by web browsers that don't support ActiveX.

4. In the **SSL VPN Portal Pages to Display** section, check the checkboxes for the portal pages you wish users to access. Any pages that are not selected will not be visible from the portal navigation menu. Your choices are:
   - VPN Tunnel. Provides full network connectivity.
   - Port Forwarding. Provides access to specific defined network services.
5. Click **Apply** to confirm your settings.

   The "Operation Successful" message appears at the top of the tab. Your new layout appears in the List of Layouts table.

Configuring Domains, Groups, and Users

Remote users connecting to the SSL VPN firewall must be authenticated before being allowed to access the network. The login window presented to the user requires three items: a User Name, a Password, and a Domain selection. The Domain determines the authentication method to be used and the portal layout that will be presented.

You must create name and password accounts for your SSL VPN users. When you create a user account, you must specify a group. Groups are used to simplify the application of access policies. When you create a group, you must specify a domain. Therefore, you should create any needed domains first, then groups, then user accounts.

To configure Domains, Groups, and Users, see "Adding Authentication Domains, Groups, and Users" on page 7-1.

Configuring Applications for Port Forwarding

Port Forwarding provides access to specific defined network services. To define these services, you must specify the internal addresses and TCP applications (port numbers) that will be intercepted by the Port Forwarding client on the user's PC. The client will reroute this traffic to the VPN firewall.

Adding Servers

To configure Port Forwarding, you must define the internal host machines (servers) and TCP applications available to remote users. To add servers, follow these steps:

1. Select VPN > SSL VPN from the main menu, and then select the Port Forwarding tab. The Port Forwarding screen will display..

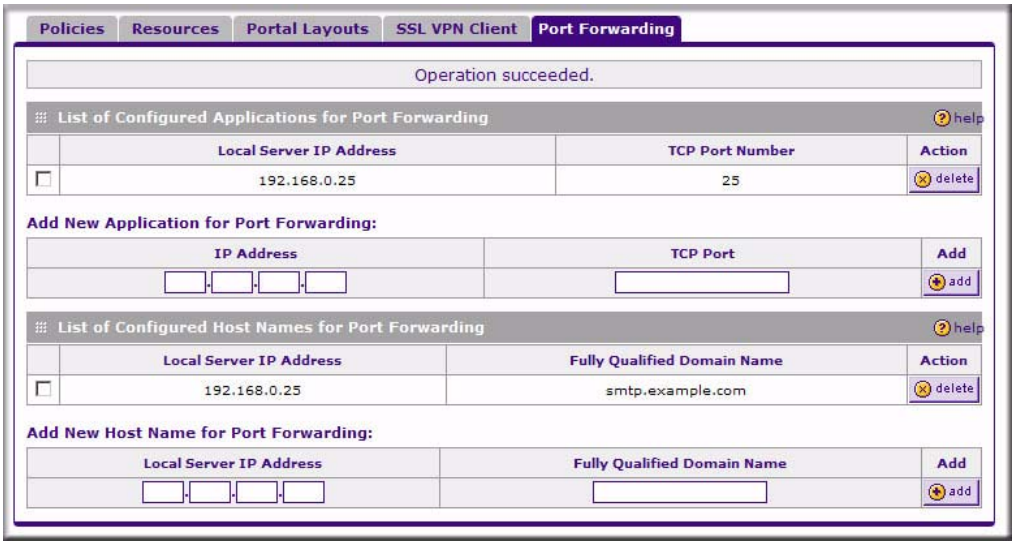


Figure 6-4

2. In the **Add New Application for Port Forwarding** section, enter the IP address of an internal server or host computer.
3. In the **TCP Port** field, enter the TCP port number of the application to be tunneled. The table below lists many commonly used TCP applications and port numbers.

Table 6-1. Port Forwarding Applications/TCP Port Numbers

TCP Application	Port Number
FTP Data (usually not needed)	20
FTP Control Protocol	21
SSH	22[a]
Telnet	23[a]
SMTP (send mail)	25
HTTP (web)	80

Table 6-1. Port Forwarding Applications/TCP Port Numbers (continued)

TCP Application	Port Number
POP3 (receive mail)	110
NTP (network time protocol)	123
Citrix	1494
Terminal Services	3389
VNC (virtual network computing)	5900 or 5800

a. Users can specify the port number together with the host name or IP address.

4. Click **Add**.

   The "Operation Succeeded" message appears at the top of the tab, and the new application entry is listed in the **List of Configured Applications**.

5. Repeat this process to add other applications for use in Port Forwarding.

Adding A New Host Name

Once the server IP address and port information has been configured, remote users will be able to access the private network servers using Port Forwarding. As a convenience for users, you can also specify host name to IP address resolution for the network servers. Host Name Resolution allows users to access TCP applications at familiar addresses such as **mail.example.com** or **ftp.example.com** rather than by IP addresses.

To add a host name for client name resolution, follow these steps:

1. Select the Port Forwarding tab, shown in Figure 6-4.
2. If the server you want to name does not appear in the **List of Configured Applications for Port Forwarding**, you must add it before you can rename it.
3. In the **Add New Host Name for Port Forwarding** section, enter the IP address of the server you want to name.
4. In the **Fully Qualified Domain Name** field, enter the full server name.
5. Click **Add**.

   The "Operation Succeeded" message appears at the top of the tab, and the new entry is listed in the **List of Configured Host Names**.

Remote users can now securely access network applications once they have logged into the SSL VPN portal and launched Port Forwarding.

Configuring the SSL VPN Client

The SSL VPN Client within the FVS336G will assign IP addresses to remote VPN tunnel clients. Because the VPN tunnel connection is a point-to-point connection, you can assign IP addresses from the corporate subnet to the remote VPN tunnel clients.

Some additional considerations are:

- So that the virtual (PPP) interface address of a VPN tunnel client does not conflict with addresses on the corporate network, configure an IP address range that does not directly overlap with addresses on your local network. For example, if 192.168.1.1 through 192.168.1.100 are currently assigned to devices on your local network, then start the client address range at 192.168.1.101 or choose an entirely different subnet altogether.
- The VPN tunnel client cannot contact a server on the corporate network if the VPN tunnel client's Ethernet interface shares the same IP address as the server or the VPN firewall (for example, if your laptop has a network interface IP address of 10.0.0.45, then you won't be able to contact a server on the remote network that also has the IP address 10.0.0.45).
- If you assign an entirely different subnet to the VPN tunnel clients than the subnet used by the corporate network, you must
  - Add a client route to configure the VPN tunnel client to connect to the corporate network using the VPN tunnel.
  - Create a static route on the corporate network's firewall to forward local traffic intended for the VPN tunnel clients to the VPN firewall.
- Select whether you want to enable full tunnel or split tunnel support based on your bandwidth:
  - Full tunnel. Sends all of the client's traffic across the VPN tunnel.
  - Split tunnel. Sends only traffic destined for the corporate network based on the specified client routes. All other traffic is sent to the Internet. Split tunnel allows you to manage your company bandwidth by reserving the VPN tunnel for corporate traffic only.

Configuring the Client IP Address Range

Determine the address range to be assigned to VPN tunnel clients, then define the address range.

To configure the client IP address range:

1. Select **VPN** > SSL VPN from the main menu, and then select the SSL VPN Client tab. The SSL VPN Client screen will display..

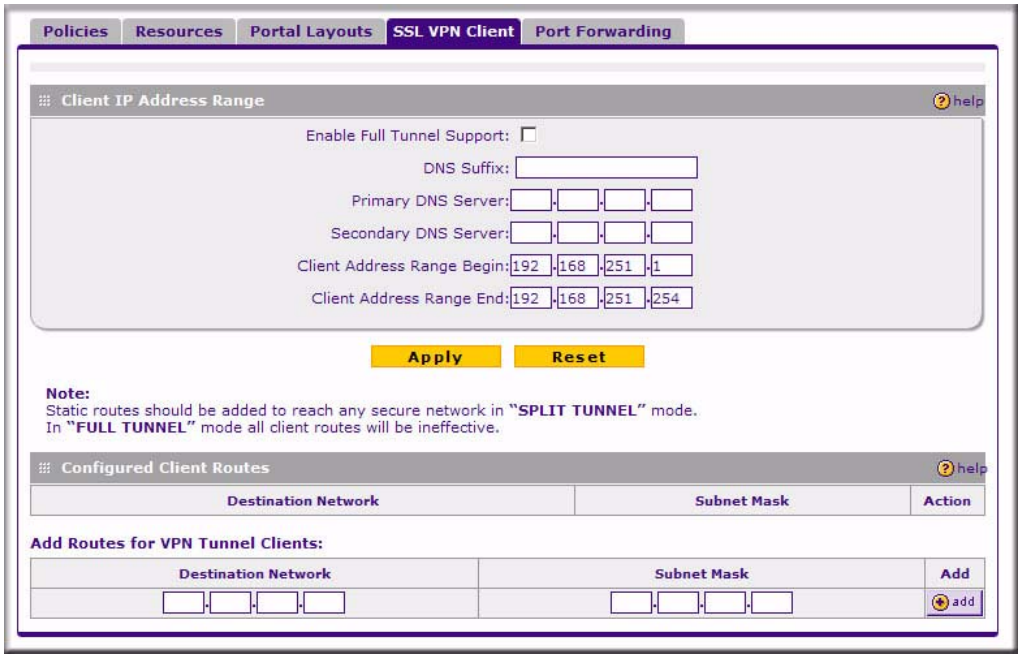


Figure 6-5

2. Select **Enable Full Tunnel Support** unless you want split tunneling.
3. (Optional) Enter a **DNS Suffix** to be appended to incomplete DNS search strings.
4. Enter Primary and Secondary DNS Server IP addresses to be assigned to the VPN tunnel clients.
5. In the **Client Address Range Begin** field, enter the first IP address of the IP address range.
6. In the **Client Address Range End** field, enter the last IP address of the IP address range.
7. Click **Apply**.

   The “Operation Successful” message appears at the top of the tab.

VPN tunnel clients are now able to connect to the VPN firewall and receive a virtual IP address in the client address range.

Adding Routes for VPN Tunnel Clients

The VPN Tunnel Clients assume that the following networks are located across the VPN over SSL tunnel:

- The subnet containing the client IP address (PPP interface), as determined by the class of the address (Class A, B, or C).
- Subnets specified in the Configured Client Routes table.

If the assigned client IP address range is in a different subnet than the corporate network or if the corporate network has multiple subnets, you must define Client Routes.

To add an SSL VPN Tunnel client route, follow these steps:

1. Access the SSL VPN Client tab shown in Figure 6-5.
2. In the **Add Routes** section, enter the Destination Network IP address of a local area network or subnet. For example, enter 192.168.0.0.
3. Enter the appropriate **Subnet Mask**.
4. Click **Add**.

   The “Operation Successful” message appears at the top of the tab and the new client route is listed in the Configured Client Routes table.

	**Note:** You must also add a static route on your corporate firewall that directs local traffic destined for the VPN tunnel client address range to the VPN firewall.

Restart the VPN firewall if VPN tunnel clients are currently connected. Restarting forces clients to reconnect and receive new addresses and routes.

Replacing and Deleting Client Routes

If the specifications of an existing route need to be changed, follow these steps:

1. Make a new entry with the correct specifications.
2. In the **Configured Client Routes** table, click the **Delete** button adjacent to the out-of-date route entry.

3. If an existing route is no longer needed for any reason, you can delete it.

Using Network Resource Objects to Simplify Policies

Network resources are groups of IP addresses, IP address ranges, and services. By defining resource objects, you can more quickly create and configure network policies. You will not need to redefine the same set of IP addresses or address ranges when configuring the same access policies for multiple users.

Defining network resources is optional; smaller organizations can choose to create access policies using individual IP addresses or IP networks rather than predefined network resources. But for most organizations, we recommend that you use network resources. If your server or network configuration changes, by using network resources you can perform an update quickly instead of individually updating all of the user and group policies.

Adding New Network Resources

To define a network resource:

1. Select **VPN > SSL VPN** from the main men, and then select the Resources tab. The Resources screen will display.

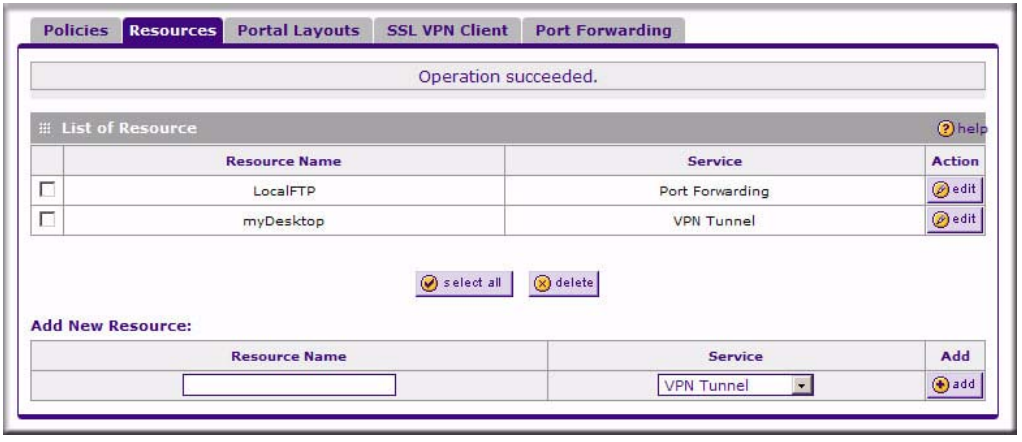


Figure 6-6

2. In the **Add New Resource** section, type the (qualified) resource name in the **Resource Name** field.

3. In the **Service** pull-down menu, select the type of service to which the resource will apply: either VPN Tunnel or Port Forwarding.
4. Click **Add**.

   The "Operation Successful" message appears at the top of the tab, and the newly-added resource name appears on the List of Resources table.
5. Adjacent to the new resource, click the **Edit** button. The **Add Resource Addresses** screen displays.

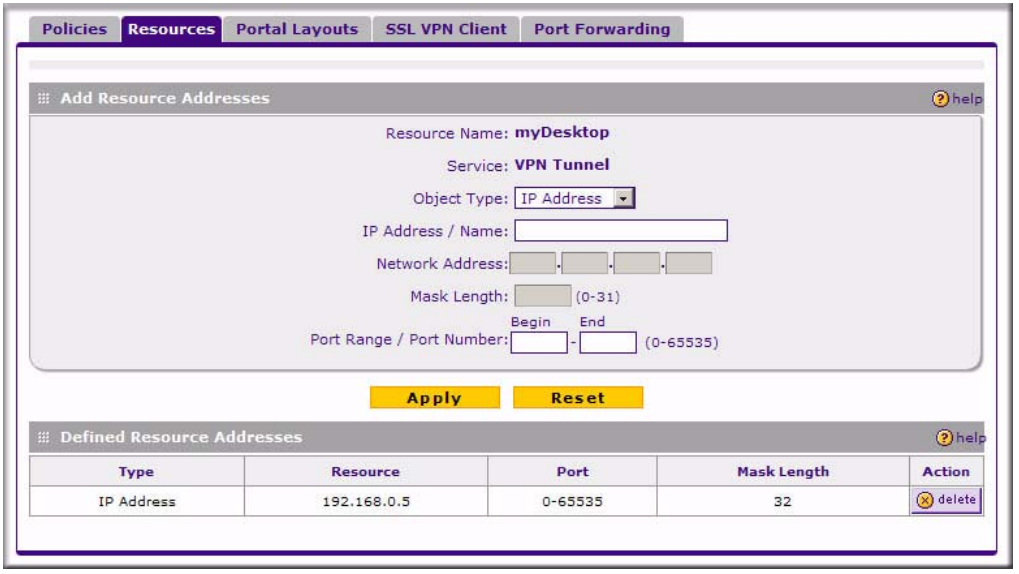


Figure 6-7

6. From the **Object Type** pull-down menu, select either IP Address or IP Network:
   - If you selected IP Address, enter an IP address or fully qualified domain name in the **IP Address/Name** field.
   - If you selected IP Network, enter the IP network address in the **Network Address** field. Enter the mask length in the **Mask Length** (0-31) field.
7. Enter the **Port Range or Port Number** for the IP Address or IP Network you selected.
8. Click **Apply** to add the IP address or IP network to the resource. The new configuration appears in the **Defined Resource Addresses** table, as shown in Figure 6-7.

Configuring User, Group, and Global Policies

An administrator can define and apply user, group and global policies to predefined network resource objects, IP addresses, address ranges, or all IP addresses and to different SSL VPN services. A specific hierarchy is invoked over which policies take precedence. The VPN firewall policy hierarchy is defined as:

1. User Policies take precedence over all Group Policies.
2. Group Policies take precedence over all Global Policies.
3. If two or more user, group or global policies are configured, *the most specific policy* takes precedence.

For example, a policy configured for a single IP address takes precedence over a policy configured for a range of addresses. And a policy that applies to a range of IP addresses takes precedence over a policy applied to all IP addresses. If two or more IP address ranges are configured, then the smallest address range takes precedence. Hostnames are treated the same as individual IP addresses.

Network resources are prioritized just like other address ranges. However, the prioritization is based on the individual address or address range, not the entire network resource.

For example, let's assume the following global policy configuration:

- Policy 1: A Deny rule has been configured to block all services to the IP address range 10.0.0.0 – 10.0.0.255.
- Policy 2: A Deny rule has been configured to block FTP access to 10.0.1.2 – 10.0.1.10.
- Policy 3: A Permit rule has been configured to allow FTP access to the predefined network resource, FTP Servers. The FTP Servers network resource includes the following addresses: 10.0.0.5 – 10.0.0.20 and ftp.company.com, which resolves to 10.0.1.3.

Assuming that no conflicting user or group policies have been configured, if a user attempted to access:

- An FTP server at 10.0.0.1, the user would be blocked by Policy 1.
- An FTP server at 10.0.1.5, the user would be blocked by Policy 2.
- An FTP server at 10.0.0.10, the user would be granted access by Policy 3. The IP address range 10.0.0.5 - 10.0.0.20 is more specific than the IP address range defined in Policy 1.

- An FTP server at ftp.company.com, the user would be granted access by Policy 3. A single host name is more specific than the IP address range configured in Policy 2.

	Note: The user would not be able to access ftp.company.com using its IP address 10.0.1.3. The VPN firewall policy engine does not perform reverse DNS lookups.

Viewing Policies

To view the existing policies, follow these steps:

1. Select **VPN** > SSL VPN from the main menu, and then select the Policies tab. The Policies screen will display.

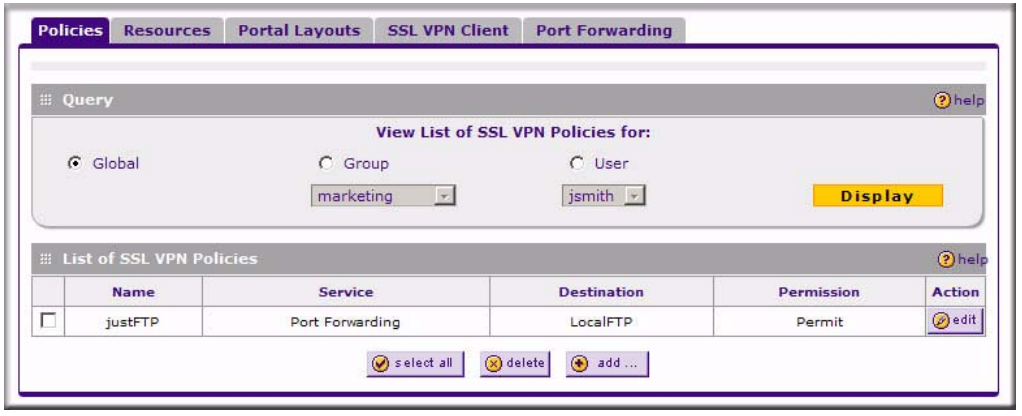


Figure 6-8

2. Make your selection from the following Query options:
   - Click **Global** to view all global policies.
   - Click **Group** to view group policies, and choose the relevant group's name from the pull-down menu.
   - Click **User** to view group policies, and choose the relevant user's name from the pull-down menu.
3. Click the **Display** button. The List of SSL VPN Policies will display the list for your selected Query option.

Adding a Policy

To add a policy, follow these steps:

1. Select **VPN** > SSL VPN from the main menu, and select the Policies tab. The Policies screen will display.

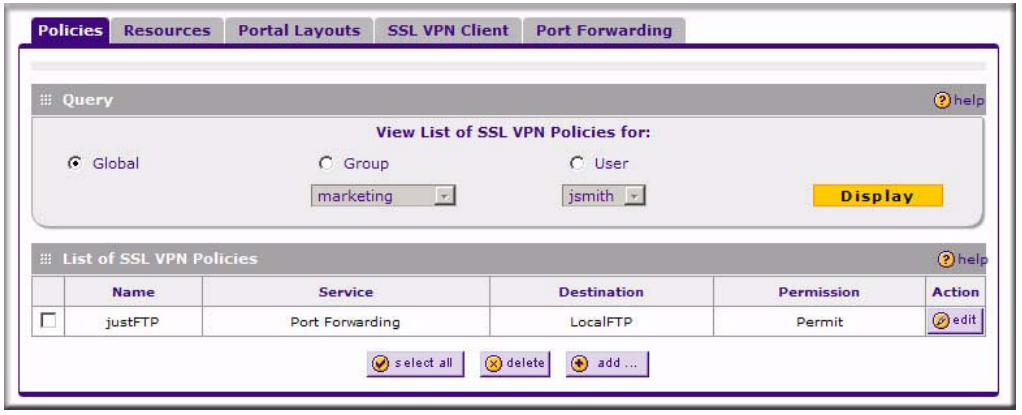


Figure 6-9

2. Make your selection from the following Query options:
   - Click **Global** if this new policy is to exclude all users and groups.
   - Click **Group** if this new policy is to be limited to a selected group. Open the pull-down menu and choose the relevant group's name.
   - Click **User** if this new policy is to be limited to a selected user. Open the pull-down menu and choose the individual user's name.

> **Note:** You should have already created the needed groups or users as described in "Adding Authentication Domains, Groups, and Users" on page 7-1.

3. Click **Add**. The **Add Policies** screen appears.
4. In the **Add SSL VPN Policies** section, review the **Apply Policy To** options and click one.

   Depending upon your selection, specific options to the right are activated or inactivated as noted in the following:

- If you choose **Network Resource**, you'll need to enter a descriptive Policy Name, then choose a **Defined Resource** and relevant **Permission** (PERMIT or DENY) from the pull-down menus.

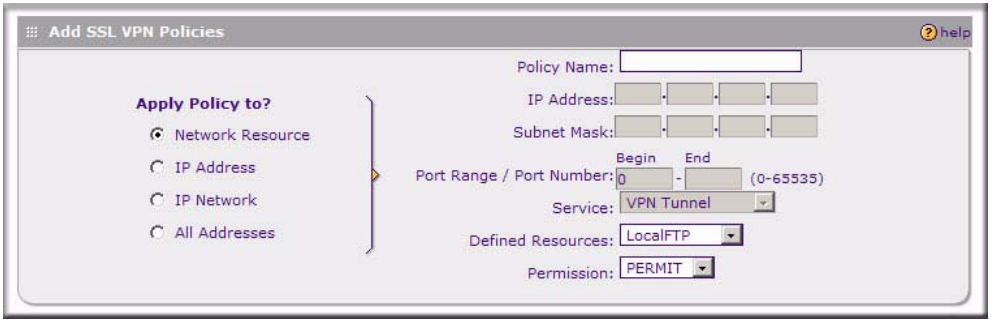


Figure 6-10

If a needed network resource has not been defined, you can add it before proceeding with this new policy. See "Adding New Network Resources " on page 6-13.

- If you choose **IP Address**, you'll need to enter a descriptive **Policy Name**, the specific **IP Address**, then choose the **Service** and relevant **Permission** from the pull-down menus.

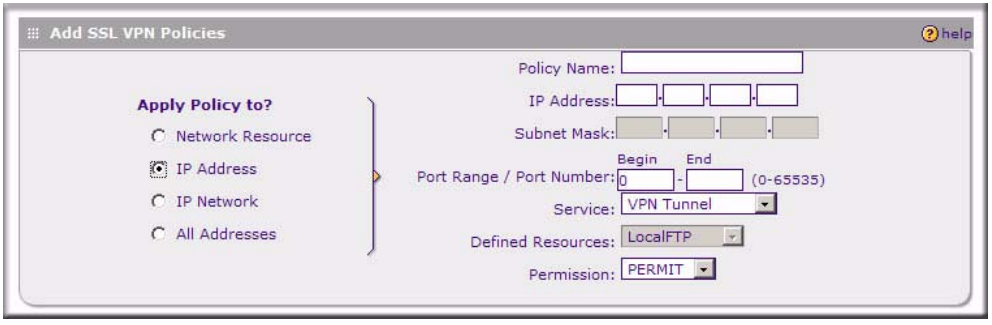


Figure 6-11

- If you choose **IP Network**, you'll need to enter a descriptive **Policy Name**, **IP Address**, **Subnet Mask**, then choose the **Service** and relevant **Permission** from the pull-down menus.

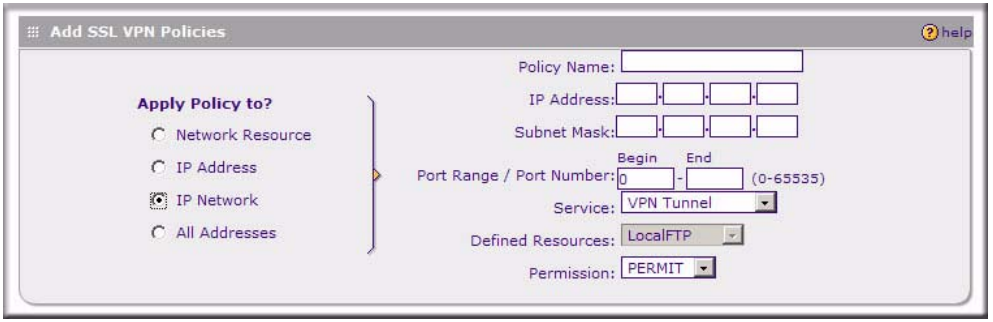


Figure 6-12

- If you choose **All Addresses**, you'll need to enter a descriptive **Policy Name**, then choose the **Service** and relevant **Permission** from the pull-down menus.

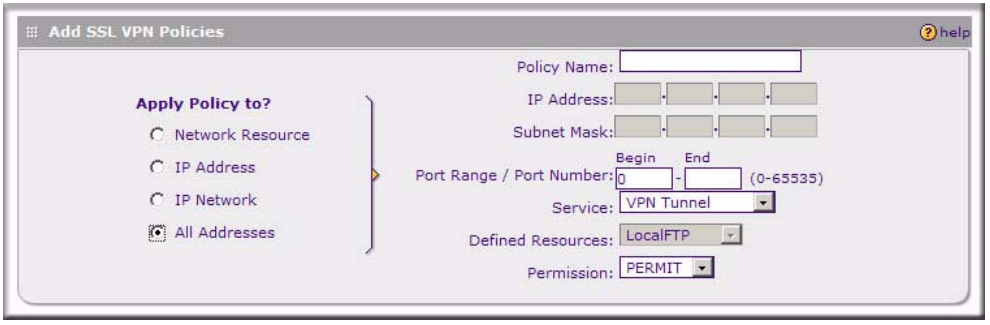


Figure 6-13

5. When you are finished making your selections, click **Apply**. The Policies screen reappears.

Your policy goes into effect immediately and is added to the policies in the **List of SSL VPN Policies** table on this screen.

Note: In addition to configuring SSL VPN user policies, be sure that HTTPS remote management is enabled. Otherwise, all SSL VPN user connections will be disabled. See "Enabling Remote Management Access" on page 8-10.

Chapter 7
Managing Users, Authentication, and Certificates

This chapter contains the following sections:

Adding Authentication Domains, Groups, and Users

You must create name and password accounts for all users who will connect to the VPN firewall. This includes administrators and SSL VPN clients. Accounts for IPsec VPN clients are only needed if you have enabled Extended Authentication (XAUTH) in your IPsec VPN configuration.

Users connecting to the VPN firewall must be authenticated before being allowed to access the VPN firewall or the VPN-protected network. The login window presented to the user requires three items: a User Name, a Password, and a Domain selection. The Domain determines the authentication method to be used and, for SSL VPN connections, the portal layout that will be presented.

	**Note:** IPsec VPN users will always belong to the default domain (geardomain) and are not assigned to groups.

Except in the case of IPsec VPN users, when you create a user account, you must specify a group. When you create a group, you must specify a domain. Therefore, you should create any needed domains first, then groups, then user accounts.

Creating a Domain

The domain determines the authentication method to be used for associated users. For SSL VPN connections, the domain also determines the portal layout that will be presented, which in turn determines the network resources to which the associated users will have access.

To create a domain:

1. Select Users > Domains from the main menu. The Domains screen displays.

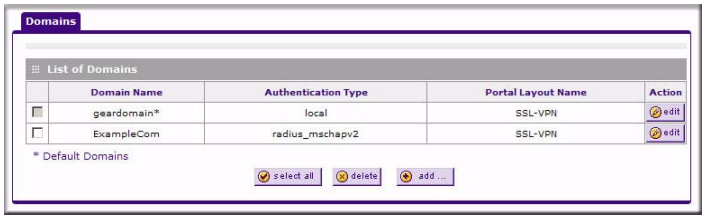


Figure 7-1

2. Click **Add**. The Add Domain screen displays.

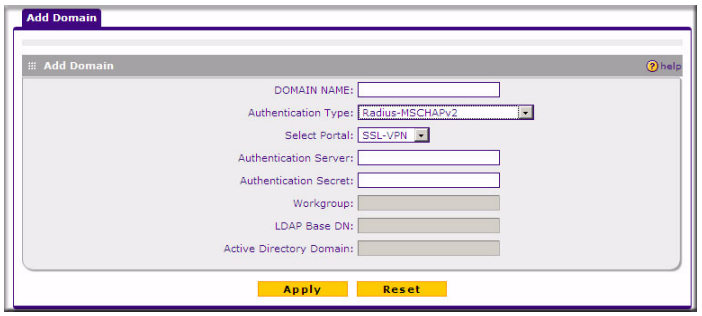


Figure 7-2

3. Configure the following fields:

   a. Enter a descriptive name for the domain in the **Domain Name** field.

   b. Select the **Authentication Type**.

   The required fields are activated in varying combinations according to your selection of Authentication Type:

Authentication Type	Required Authentication Information Fields
Local User Database	None
Radius-PAP	Authentication Server, Authentication Secret
Radius-CHAP	Authentication Server, Authentication Secret
Radius-MSCHAP	Authentication Server, Authentication Secret
Radius-MSCHAPv2	Authentication Server, Authentication Secret
NT Domain	Authentication Server, Workgroup

Authentication Type	Required Authentication Information Fields
Active Directory	Authentication Server, Active Directory Domain
LDAP	Authentication Server, LDAP Base DN

c. **Select a portal** to which this domain will be associated.

4. Click **Apply** to save and apply your entries. The Domain screen will display a new domain row.

Creating a Group

The use of groups simplifies the configuration of VPN policies when different sets of users will have different restrictions and access controls.

Note: Groups that are defined in the User menu are used for setting SSL VPN policies. These groups should not be confused with LAN Groups that are defined in the Network Configuration | LAN Settings | LAN Groups tab, which are used to simplify firewall policies.

To create a group:

1. Select Users > Groups from the main menu.The Groups screen displays.

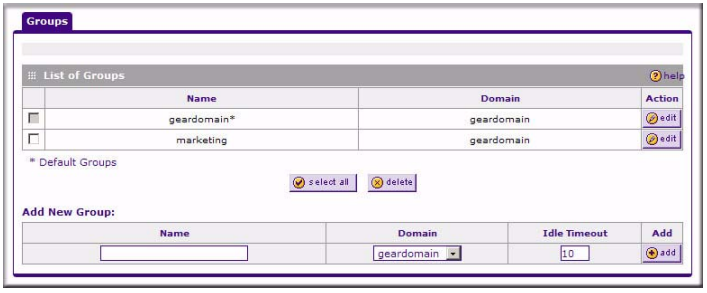


Figure 7-3

2. Configure the new group settings in the Add New Group section of the menu:

   a. **Name**. Enter a descriptive name for the group.

   b. **Domain**. Select the appropriate domain (only for Administrator or SSL VPN User).

c. **Timeout**. For an Administrator, this is the period at which an idle user will be automatically logged out of the Web Configuration Manager

3. Click **Add**.

   The new group appears in the **List of Groups**, ready for use in user account setup.

Creating a New User Account

To add individual user accounts:

1. Select Users > Users from the main menu. The Users screen will display.

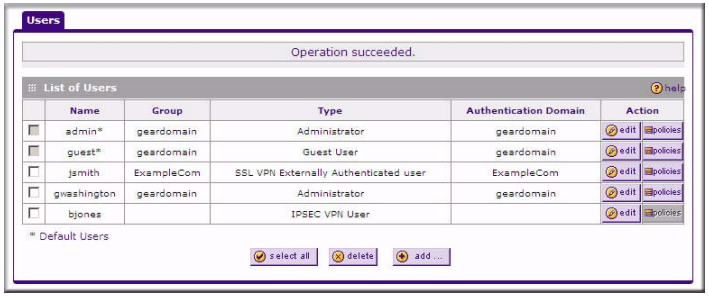


Figure 7-4

2. Click **Add**. The Add User tab screen is displayed.

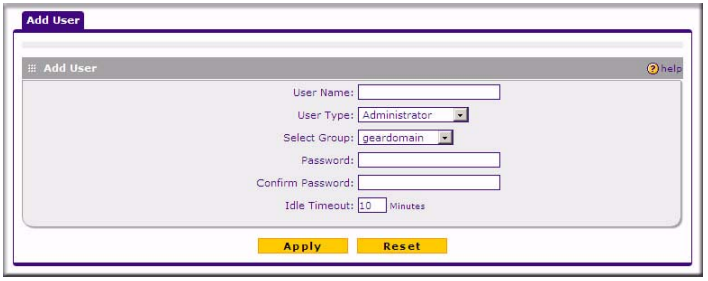


Figure 7-5

3. Configure the following fields:

   a. **User Name**. Enter a unique identifier, using any alphanumeric characters.

   b. **User Type**. Select either Administrator, SSL VPN User, or IPsec VPN User.

   c. **Select Group**. Select from a list of configured groups. The user will be associated with the domain that is associated with that group.

d. **Password/Confirm Password**. The password can contain alphanumeric characters, dash, and underscore.

e. **Idle Timeout**. For an Administrator, this is the period at 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 **List of Users**.

Setting User Login Policies

You can restrict the ability of defined users to log into the Web Configuration Manager. You can also require or prohibit logging in from certain IP addresses or using particular browsers.

To configure user login policies:

1. In the **Action** column in the **List of Users** table, click **Policies** adjacent to the user policy you want to configure. The **Login Policies** screen displays:.

Figure 7-6

2. To prohibit this user from logging in to the VPN firewall, select the **Disable Login** checkbox.
3. To prohibit this user from logging in from the WAN interface, select the **Deny Login from WAN Interface** checkbox. In this case, the user can log in only from the LAN interface.

	Note: For security reasons, **Deny Login from WAN Interface** is checked by default for admin and guest.

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

To restrict logging in based on IP address:

1. Select the **by Source IP Address** tab. The by Source IP Address screen will display.

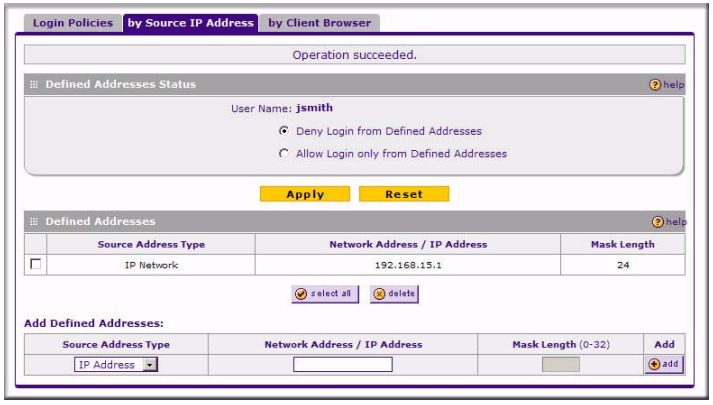


Figure 7-7

2. In the **Defined Addresses Status** section, select:
   - the **Deny Login from Defined Addresses** to deny logging in from the IP addresses that you will specify
   - the **Allow Login only from Defined Addresses** to allow logging in from the IP addresses that you will specify.
3. Click **Apply.**
4. To specify a single IP address, select **IP Address** from the **Source Address Type** pull-down menu and enter the IP address in the **Network Address/IP address** field.
5. To specify a subnet of IP addresses, select **IP Network** from the **Source Address Type** pull-down menu. Enter the network address and netmask length in the **Network Address/IP address** field.
6. Click **Add** to move the defined address to the **Defined Addresses** table.
7. Repeat these steps to add additional addresses or subnets.

To restrict logging in based on the user's browser:

1. Select the **by Client Browser** tab. The by Client Browser screen will display.

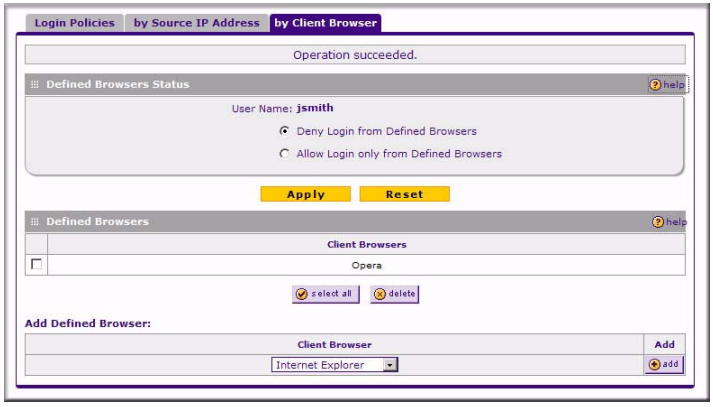


Figure 7-8

2. In the **Defined Browsers Status** section, select>
   - the **Deny Login from Defined Browsers** to deny logging in from browsers that you will specify
   - the **Allow Login only from Defined Browsers** to allow logging in from browsers that you will specify.
3. From the **Add Defined Browser** selection, select a browser from the **Client Browser** pull-down menu and click **Add** to move the defined browser to the **Defined Browsers** table.
4. Repeat these steps to add additional browsers, then click **Apply** to save your changes.

Changing Passwords and Settings

You can change the administrator and guest passwords and settings. Administrator access is read/write and guest access is read-only. The default passwords for the firewall's Web Configuration Manager is **password**.

To modify User or Admin settings:

1. Select **Users** from the main menu and **Local Authentication** from the submenu.

Figure 7-9

2. Select the Settings you wish to edit by checking either the **Edit Admin Settings** or **Edit Guest Settings** radio box.
3. Change the password by first entering the old password, and then entering the new password twice.
4. Click **Apply** to save your settings or **Cancel** to return to your previous settings.
5. Change the **Idle Logout Time** field to the number of minutes you require. The default is 5 minutes.

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

6. Click **Apply** to save this setting.

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

RADIUS Server External Authentication

For authentication to RADIUS or WIKID, you can define the authentication type.

Figure 7-10

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

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

Table 7-1.

Authentication Protocol	Description
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.
MIAS	Network validated PAP or CHAP password based authentication scheme.
WiKID	WiKID is a PAP or CHAP key-based two-factor authentication method using public key cryptography. The client sends an encrypted PIN to the WiKID server and receives a one-time passcode with a short expiration period. The client logs in with the passcode. See tAppendix D, "Two Factor Authentication" for more on WiKID authentication.

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

Managing Certificates

The FVS336G uses Digital Certificates (also known as X509 Certificates) during the Internet Key Exchange (IKE) authentication phase to authenticate connecting VPN gateways or clients, or to be authenticated by remote entities. The same Digital Certificates are extended for secure web access 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 FVS336G when the same digital certificate is being used for secure web management.

In the FVS336G, 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 & 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.

Your 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 VPN > Certificates menu, 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 > Certificates from the main menu. The Certificates screen displays. The top section of the Certificates screen displays the **Trusted Certificates (CA Certificates)**.

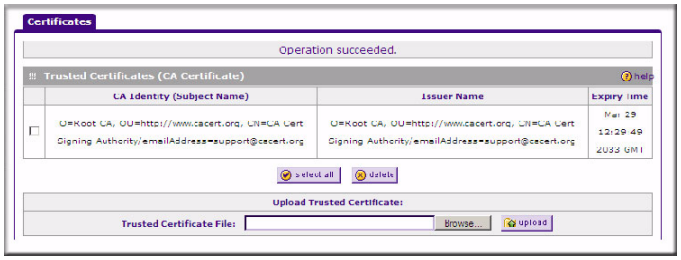


Figure 7-11

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

To load a CA certificate into your VPN firewall:

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

Viewing Active Self Certificates

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

Figure 7-12

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.
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.)

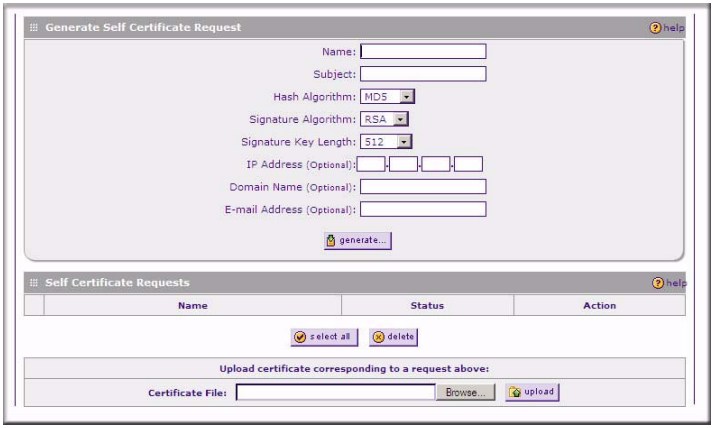


Figure 7-13

- 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.

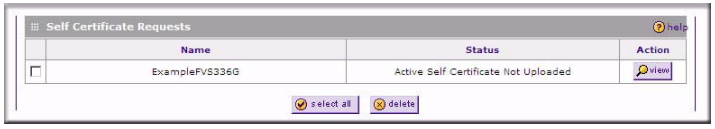


Figure 7-14

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

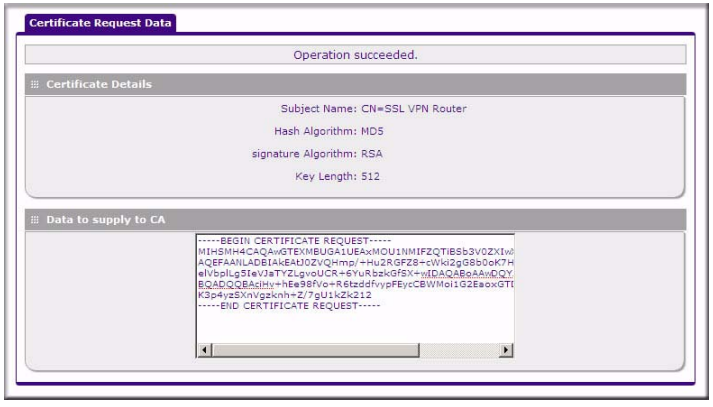


Figure 7-15

6. Copy the contents of the **Data to supply to CA** text box into a text file, including all of the data contained from "----BEGIN CERTIFICATE REQUEST---" to "---END CERTIFICATE REQUEST---".
7. Submit your certificate request to a CA:
   a. Connect to the website of the CA.
   b. Start the Self Certificate request procedure.
   c. When prompted for the requested data, copy the data from your saved text file (including "----BEGIN CERTIFICATE REQUEST---" and "---END CERTIFICATE REQUEST").
   d. Submit the CA form. If no problems ensue, the certificate will be issued.
8. Store the certificate file from the CA on your computer.
9. Return to the Certificates screen and locate the **Self Certificate Requests** section.

Figure 7-16

10. Select the checkbox next to the certificate request, then click **Browse** and locate the certificate file on your PC.
11. Click **Upload**. The certificate file will be uploaded to this device and will appear in the **Active Self Certificates** list.

If you have not already uploaded the CA certificate, do so now, as described in "Select VPN > Certificates from the main menu. The Certificates screen displays. The top section of the Certificates screen displays the Trusted Certificates (CA Certificates)." on page 7-12. You should also periodically check your CA's Certificate Revocation List, as described in "Managing your Certificate Revocation List (CRL)" on page 7-15.

Managing your Certificate Revocation List (CRL)

A CRL (Certificate Revocation List) file shows certificates that have been revoked and are no longer valid. Each CA issues their own CRLs. It is important that you keep your CRLs up-to-date. You should obtain the CRL for each CA regularly.

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

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

1. Select VPN > Certificates from the main menu.

   The Certificates menu will display showing the **Certificate Revocation Lists (CRL)** table at the bottom of the screen.

Figure 7-17

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

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

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

Chapter 8
Router and Network Management

This chapter describes how to use the network management features of your ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN. These features can be found by clicking on the appropriate heading in the Main Menu of the browser interface.

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

This chapter contains the following sections:

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: 4000 Mbps (four LAN ports at 1000 Mbps each)

- WAN side: 2000 Mbps (load balancing mode, two WAN ports at 1000 Mbps each) or 1000 Mbps (rollover mode, one active 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. At 1.5 Mbps, the WAN ports will support the following traffic rates:

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

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

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

Features That Reduce Traffic

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

- Service blocking
- Block sites
- Source MAC filtering

Service Blocking

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

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

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

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

- ALLOW by schedule, otherwise Block

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

- **LAN Users.** These settings determine which computers on your network are affected by this rule. Select the desired options:
  - Any**.** All PCs and devices on your LAN.
  - Single address**.** The rule will be applied to the address of a particular PC.
  - Address range**.** The rule is applied to a range of addresses.
  - Groups**.** The rule is applied to a Group (see "Managing Groups and Hosts (LAN Groups)" on page 3-5 to assign PCs to a Group using the LAN Groups Database).
- **WAN Users.** These settings determine which Internet locations are covered by the rule, based on their IP address.
  - Any**.** The rule applies to all Internet IP address.
  - Single address**.** The rule applies to a single Internet IP address.
  - Address range**.** The rule is applied to a range of Internet IP addresses.
- **Services.** You can specify the desired Services or applications to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see "About Services-Based Rules" on page 4-3 and "Adding Customized Services" on page 4-14).
- **Schedule.** You can specify whether the rule is to be applied on the Schedule 1, Schedule 2, or Schedule 3 time schedule (see "Setting a Schedule to Block or Allow Specific Traffic" on page 4-26).

See "Using Rules to Block or Allow Specific Kinds of Traffic" on page 4-2 for the procedure on how to use this feature.

Services

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

See "About Services-Based Rules" on page 4-3 for the procedure on how to use this feature.

Groups and Hosts

You can apply these rules selectively to groups of PCs to reduce the outbound or inbound traffic. The LAN Groups 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 LAN Groups 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 ARP. requests. The ARP 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 appear in the database as Unknown.
- **Manual Entry**. You can manually enter information about a device.

See "Managing Groups and Hosts (LAN Groups)" on page 3-5 for the procedure on how to use this feature.

Schedule

If you have set firewall rules on the Rules screen, you can configure three different schedules (for example, 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 4-26 for the procedure on how to use this feature.

Block Sites

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

- **Keyword (and Domain Name) Blocking.** You can specify up to 32 words that, should they appear in the Web site name (i.e., URL) or in a newsgroup name, will cause that site or newsgroup to be blocked by the VPN firewall.

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

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

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

See "Blocking Internet Sites (Content Filtering)" on page 4-18 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 4-21 for the procedure on how to use this feature.

Features That Increase Traffic

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

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

Port Forwarding

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

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

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

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

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

You can also enable a check on special rules:

- **VPN Passthrough.** Passes the VPN traffic without any filtering, specially used when this firewall is between two VPN tunnel end points.
- **Drop fragmented IP packets.** Drops any fragmented IP packets.
- **UDP Flooding.** Limits the number of UDP sessions created from one LAN machine.
- **TCP Flooding.** Protects the VPN firewall from SYN flood attack.
- **Enable DNS Proxy.** Allows the VPN firewall to handle DNS queries from the LAN.
- **Enable Stealth Mode.** Prevents the VPN firewall from responding to incoming requests for unsupported services.

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

- **LAN Users.** These settings determine which computers on your network are affected by this rule. Select the desired IP Address in this field.
- **WAN Users.** These settings determine which Internet locations are covered by the rule, based on their IP address.
  - Any: The rule applies to all Internet IP address.
  - Single address: The rule applies to a single Internet IP address.
  - Address range: The rule is applied to a range of Internet IP addresses.
- **Destination Address.** These settings determine the destination IP address for this rule which will be applicable to incoming traffic This rule will be applied only when the destination IP address of the incoming packet matches the IP address of the selected WAN interface Selecting ANY enables the rule for any LAN IP destination. WAN1 and WAN2 corresponds to the respective WAN interface governed by this rule.

- **Services.** You can specify the desired Services or applications to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see "Adding Customized Services" on page 4-14).
- **Schedule.** You can specify whether the rule is to be applied on the Schedule 1, Schedule 2, or Schedule 3 time schedule (see "Setting a Schedule to Block or Allow Specific Traffic" on page 4-26).

See "Using Rules to Block or Allow Specific Kinds of Traffic" on page 4-2 for the procedure on how to use this feature.

Port Triggering

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

Once configured, port triggering operates as follows:

- A PC makes an outgoing connection using a port number defined in the Port Triggering table.
- This VPN firewall records this connection, opens the additional INCOMING port or ports associated with this entry in the Port Triggering table, and associates them with the PC.
- The remote system receives the PCs request and responds using the different port numbers that you have now opened.
- This 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 4-24 for the procedure on how to use this feature.

VPN Tunnels

The VPN firewall permits up to 25 IPsec VPN tunnels and 10 SSL VPN tunnels at a time. Each tunnel requires extensive processing for encryption and authentication.

See Chapter 5, "Virtual Private Networking Using IPsec" for the procedure on how to use IPsec VPN, and Chapter 6, "Virtual Private Networking Using SSL Connections for the procedure on how to use SSL VPN.

Using QoS to Shift the Traffic Mix

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

- You can accept the default priority defined by the service itself by not changing its QoS setting.
- You can change the priority to a higher or lower value than its default setting to give the service higher or lower priority than it otherwise would have.

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

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

See "Setting Quality of Service (QoS) Priorities" on page 4-16 for the procedure on how to use this feature.

Tools for Traffic Management

The ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN includes several tools that can be used to monitor the traffic conditions of the firewall and control who has access to the Internet and the types of traffic they are allowed to have. See "Monitoring System Performance" on page 9-1 for a discussion of the tools.

Changing Passwords and Administrator 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 Admin user account settings, including password:

1. Select Users > Users from the main menu. The Users screen will display.

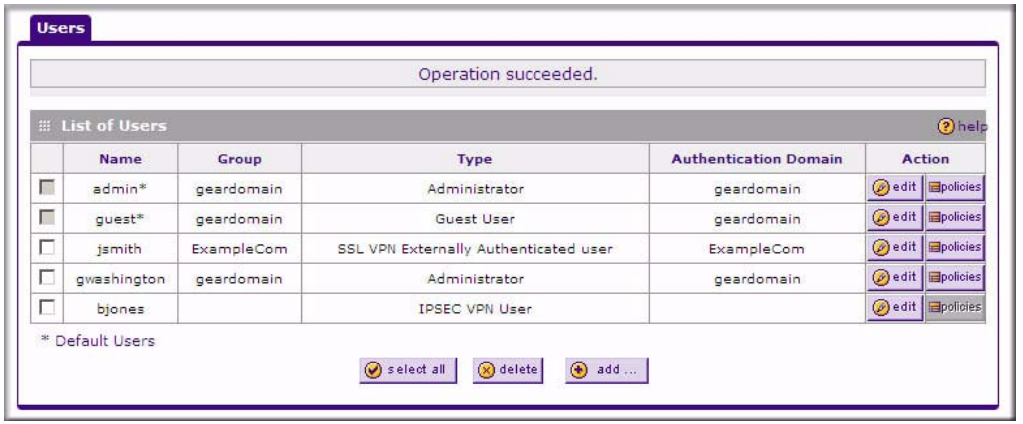


Figure 8-1

2. Select the checkbox adjacent to admin in the **Name** column, then click **Edit** in the **Action** column.

   The Edit User screen is displayed, with the current settings for Administrator displayed in the **Select User Type** pull-down menu.

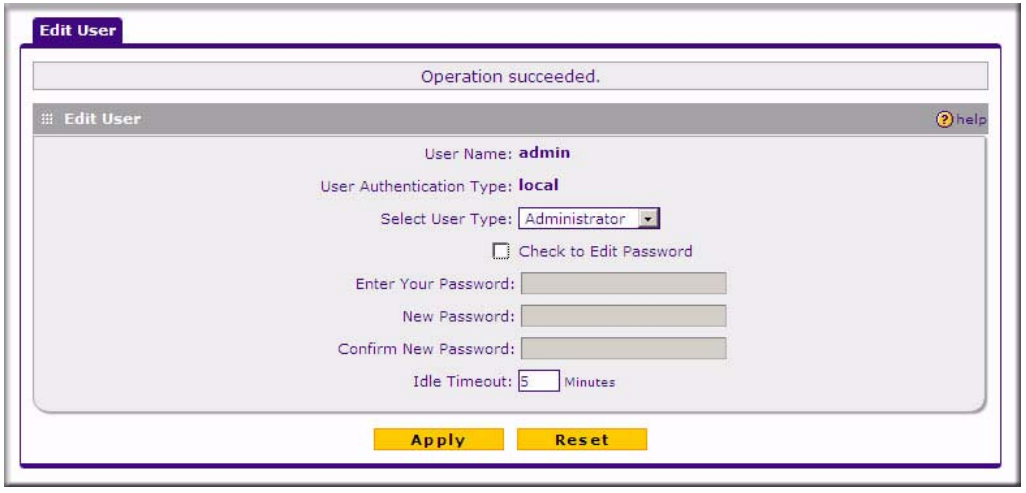


Figure 8-2

3. Select the **Check to Edit Password** checkbox. The password fields become active.
4. Enter the old password, then enter the new password twice.

5. (Optional) To change the idle timeout for an administrator login session, enter a new number of minutes in the **Idle Timeout** field.
6. Click **Apply** to save your settings or **Reset** to return to your previous settings.

	**Note:** If the administrator login timeout value is too large, you may have to wait a long time before you are able to log back into the VPN firewall if your previous login was disrupted (for example, if you did not click **Logout** on the Main Menu bar to log out).

	**Note:** After a factory default reset, the password and timeout value will be changed back to **password** and **5** minutes, respectively.

Enabling Remote Management Access

Using the Remote Management page, you can allow an administrator on the Internet to configure, upgrade, and check the status of your VPN firewall. You must be logged in locally to enable remote management (see "Logging into the VPN Firewall Router" on page 2-2).

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

To configure your firewall for Remote Management:

1. Select Administration > Remote Management from the main menu The **Remote Management** screen is displayed.

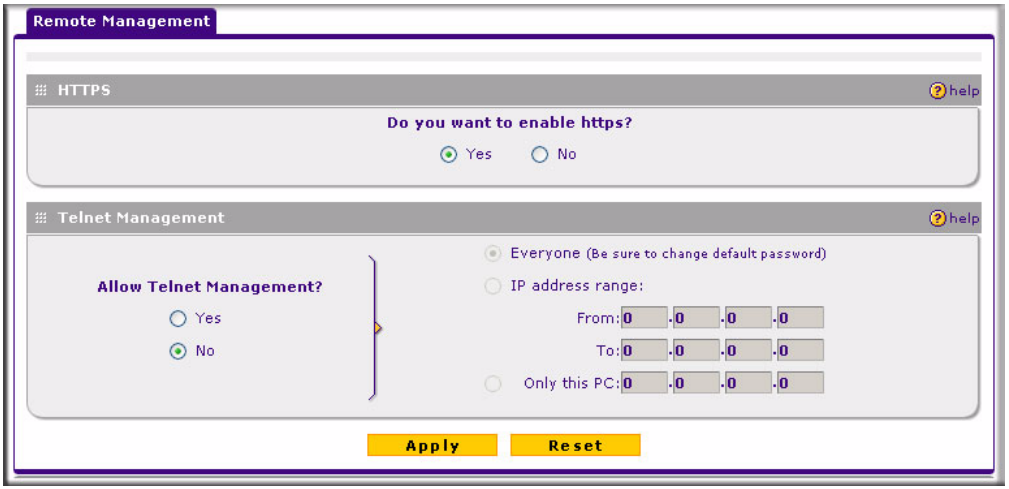


Figure 8-3

2. Click the **Yes** radio button to enable HTTPS remote management (enabled by default).
3. 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.

> **Note:** For enhanced security, restrict access to as few external IP addresses as practical. See "Setting User Login Policies" on page 7-5 for instructions on restricting administrator access. Be sure to use strong passwords.

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

For accessing your VPN firewall from the Internet, the Secure Sockets Layer (SSL) will be enabled. You will enter *https://* (not *http://*) and type your firewall's WAN IP address into your browser. For example, if your WAN IP address is 172.16.0.123, type the following in your browser:

https://172.16.0.123

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

	**Note:** To maintain security, the FVS336G will reject a login that uses *http://address* rather than the SSL *https://address*.

	**Note:** The first time you remotely connect to the FVS336G 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 FVS336G 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 FVS336G by running `tracert` from the Windows Run menu option. Trace the route to your registered FQDN. For example, enter **`tracert FVS336G.mynetgear.net`**, and the WAN IP address that your ISP assigned to the FVS336G is displayed.

Using the Command Line Interface

	**Note:** The command line interface is not supported at this time. Check the NETGEAR Web site for the latest status.

You can access the command line interface (CLI) using Telnet from the LAN or, if enabled in the Remote Management menu, from the WAN.

To access the CLI from a communications terminal when the VPN firewall is still set to its factory defaults (or use your own settings if you have changed them), do the following:

1. From your computer's command line prompt, enter the following command:

   ```
   telnet 192.168.1.1
   ```

2. Enter **admin** and **password** when prompted for the login and password information (or enter **guest** and **password** to log in as a read-only guest).
3. Enter **exit** to end the CLI session.

Any configuration changes made via the CLI are not preserved after a reboot or power cycle unless the user issues the CLI **save** command after making the changes.

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 > SNMP from the main menu. The **SNMP** screen is displayed.

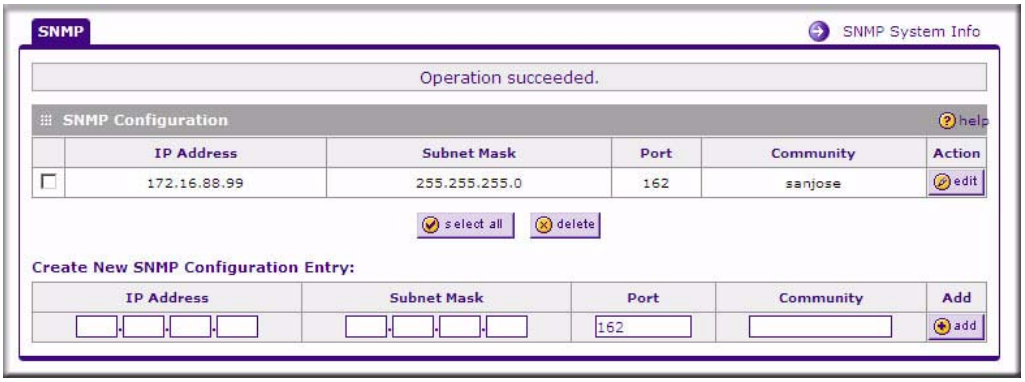


Figure 8-4

2. Configure the following fields in the **Create New SNMP Configuration Entry** section:

   a. Enter the IP Address of the SNMP manager in the **IP Address** field and the Subnet Mask in the **Subnet Mask** field.

   – To allow only the host address to access the VPN firewall and receive traps, enter an IP Address of, for example, 192.168.1.101 with a Subnet Mask of 255.255.255.**255**.

   – To allow a subnet access to the VPN firewall through SNMP, enter an IP address of, for example,192.168.1.101 with a Subnet Mask of 255.255.255.**0**. The traps will still be received on 192.168.1.101, but the entire subnet will have access through the community string.

   – 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.

   b. Enter the trap port number of the configuration in the **Port** field. The default is 162.

   c. Enter the trap community string of the configuration in the **Community** field.

3. Click **Add** to create the new configuration. The entry is displayed in the **SNMP Configuration** table.

The **SNMP System Info** option arrow at the top of the tab opens the **SNMP SysConfiguration** menu that displays the SNMP System contact information available to the SNMP manager:

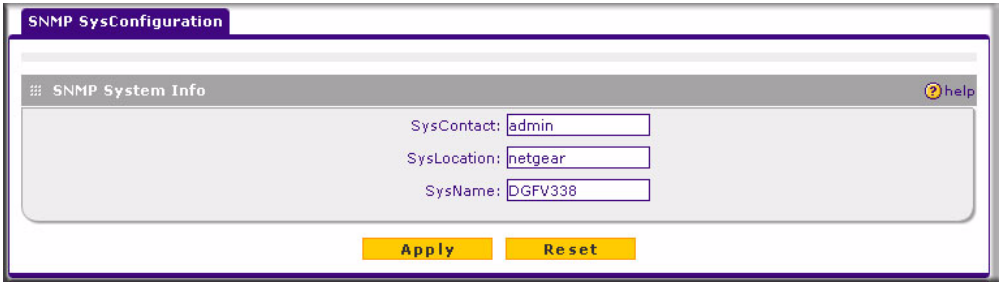


Figure 8-5

You can edit the System Contact, System Location, and System name.

Configuration File Management

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

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.

Backup and Restore Settings

To backup settings:

1. Select Administration > Settings Backup and Firmware Upgrade from the main menu. The **Settings Backup and Firmware Upgrade** screen is displayed.

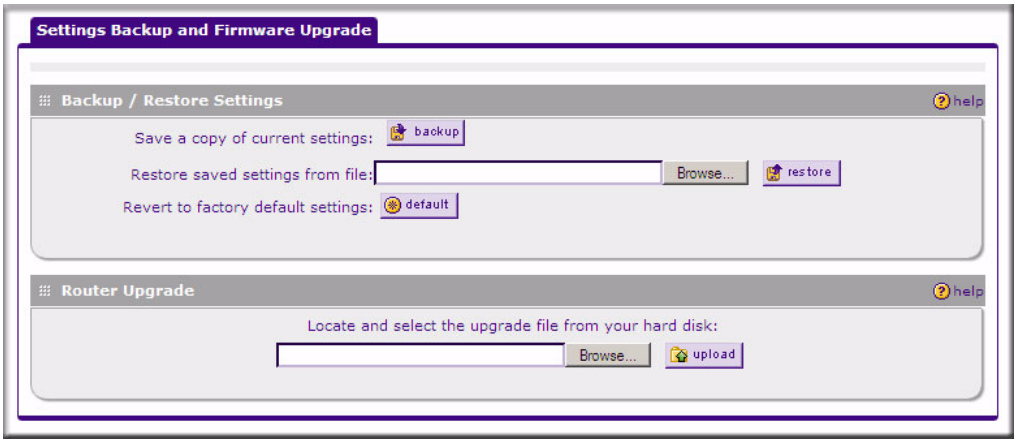


Figure 8-6

2. Click **Backup** to save a copy of your current settings.
   - If your browser isn't set up to save downloaded files automatically, locate where you want to save the file, specify file name, and click Save.
   - If you have your browser set up to save downloaded files automatically, the file will be saved to your browser's download location on the hard disk.

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

To restore settings from a backup file:

1. 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.

Revert to Factory Default Settings

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

1. Click **default**.
2. You must 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,** your VPN firewall settings will be erased. All firewall rules, VPN policies, LAN/WAN settings and other settings will be lost. Backup your settings if you intend on using them!

Upgrading the Firmware

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

To download a firmware version:

1. Go to the NETGEAR Web site at *http://www.netgear.com/support* and click **Downloads.**
2. From the **Product Selection** pull-down menu, choose the FVS336G.
3. Click on the desired firmware version to reach the download page. Be sure to read the release notes on the download page before continuing.
4. Follow the **To Upgrade** steps to download your firmware.

To upgrade the router software:

1. Select Administration > Settings Backup and Firmware Upgrade from the main menu.
2. Click **Browse** in the **Router Upgrade** section.

3. Locate the downloaded file and click **upload.** This will start the software upgrade to your VPN firewall. This may take some time. At the conclusion of the upgrade, your VPN firewall will reboot.

Warning: 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 continuing.

4. After the VPN firewall has rebooted, check the firmware version in the **Router Status** screen to verify that your router now has the new firmware 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 notes on the firmware download page to find out if this is required.

Configuring Date and Time Service

Date, time and NTP server designations can be reset 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 > Time Zone from the main menu. The **Time Zone** screen is displayed.

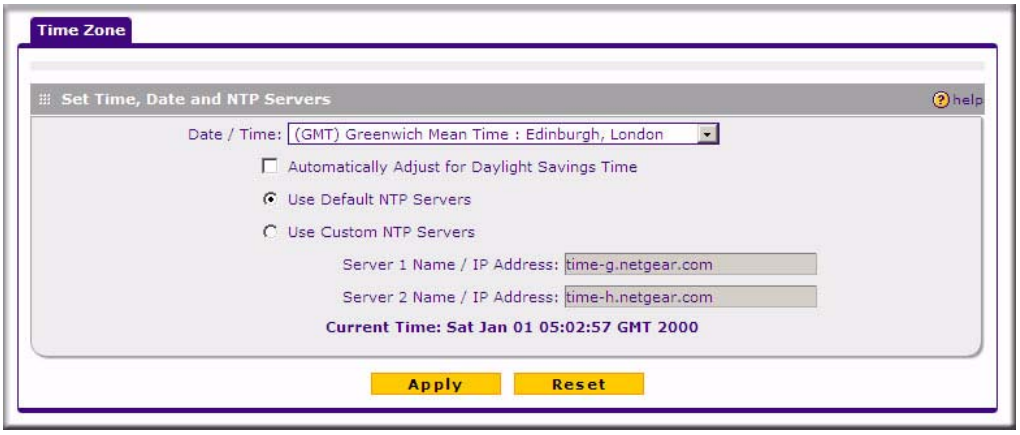


Figure 8-7

2. From the **Date/Time** pull-down menu, choose 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, select **Automatically Adjust for Daylight Savings Time**.
4. Select an NTP Server option:
   - **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 in the Network menu before the VPN firewall can perform this lookup.

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

Chapter 9
Monitoring System Performance

This chapter describes the full set of system monitoring features of your ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN. You can be alerted to important events such as WAN port rollover, WAN traffic limits reached, and login failures and attacks. You can also view status information about the firewall, WAN ports, LAN ports, and VPN tunnels.

This chapter contains the following sections:

Enabling the Traffic Meter

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

To monitor traffic limits on each of the WAN ports:

1. Select Monitoring > Traffic Meter from the main menu, and then the WAN1 Traffic Meter tab. The WAN1 Traffic Meter screen will display.

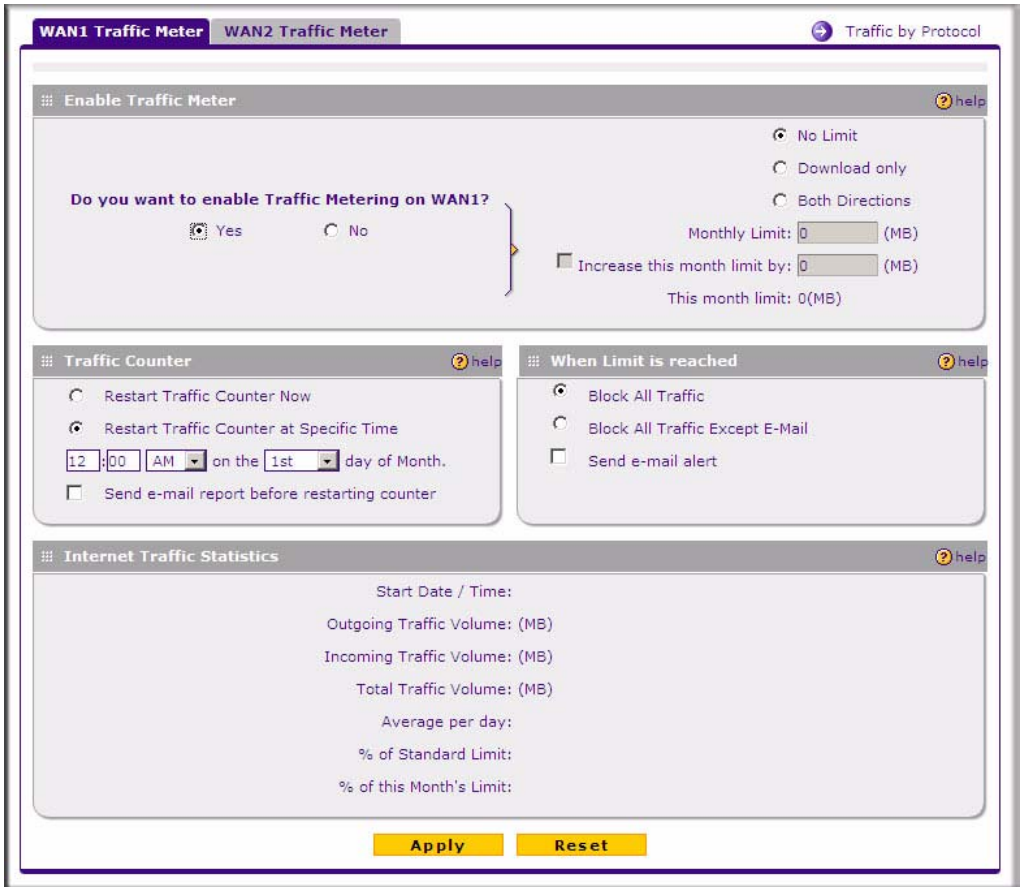


Figure 9-1

2. Enable the traffic meter by clicking the **Yes** radio button under **Do you want to enable Traffic Metering on WAN1?** The traffic meter will record the volume of Internet traffic passing through the WAN1. Select 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**. Enter the monthly volume limit and select the desired behavior when the limit is reached.

	Note: Both incoming and outgoing traffic are included in the limit

- **Increase this month limit by**. Temporarily increase the Traffic Limit if you have reached the monthly limit, but need to continue accessing the Internet. Select the checkbox and enter the desired increase. (The checkbox will automatically be cleared when saved so that the increase is only applied once.)
- **This month limit**. Displays the limit for the current month.

3. In the **Traffic Counter** section, make your traffic counter selections:
   - **Restart Traffic Counter Now**. Select this option and click Apply to restart the Traffic Counter immediately.
   - **Restart Traffic Counter at a Specific Time**. Restart the Traffic Counter at a specific time and day of the month. Fill in the time fields and choose AM or PM and the day of the month from the pull-down menus.
   - **Send e-mail report before restarting counter**. An E-mail report will be sent immediately before restarting the counter. You must configure the E-mail screen in order for this function to work (see "E-Mail Notifications of Event Logs and Alerts" on page 4-29).
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 screen in order for this function to work.
5. Click **Apply** to save your settings.

   The **Internet Traffic Statistics** section displays statistics on Internet Traffic via the WAN port. If you have not enabled the Traffic Meter, these statistics are not available.
6. Click the **Traffic by Protocol** link, in the upper right header, to see a report of the Internet traffic by type. 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.
7. Click the WAN2 Traffic Meter tab and repeat this process to configure the Traffic Meter for the WAN2 port.

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, your VPN firewall will log security-related events such as: accepted and dropped packets on different segments of your LAN; denied incoming and outgoing service requests; hacker probes and login attempts; and other general information based on the settings you input on the **Firewall Logs & E-mail** menu. In addition, if you have set up Content Filtering on the Block Sites screen (see "Blocking Internet Sites (Content Filtering)" on page 4-18), a log will be generated when someone on your network tries to access a blocked site.

You must have e-mail notification enabled to receive the logs in an e-mail message. If you don't have e-mail notification enabled, you can view the logs by clicking the **View Logs** option arrow to the right of the tab. 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 > Firewall Logs & E-mail from the main menu. The Firewall Logs & E-mail screen displays.
2. Enter the name of the log in the **Log Identifier** field. 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, select the type of system events to be logged.
5. Check **Yes** 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. **No Authentication** is selected 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.

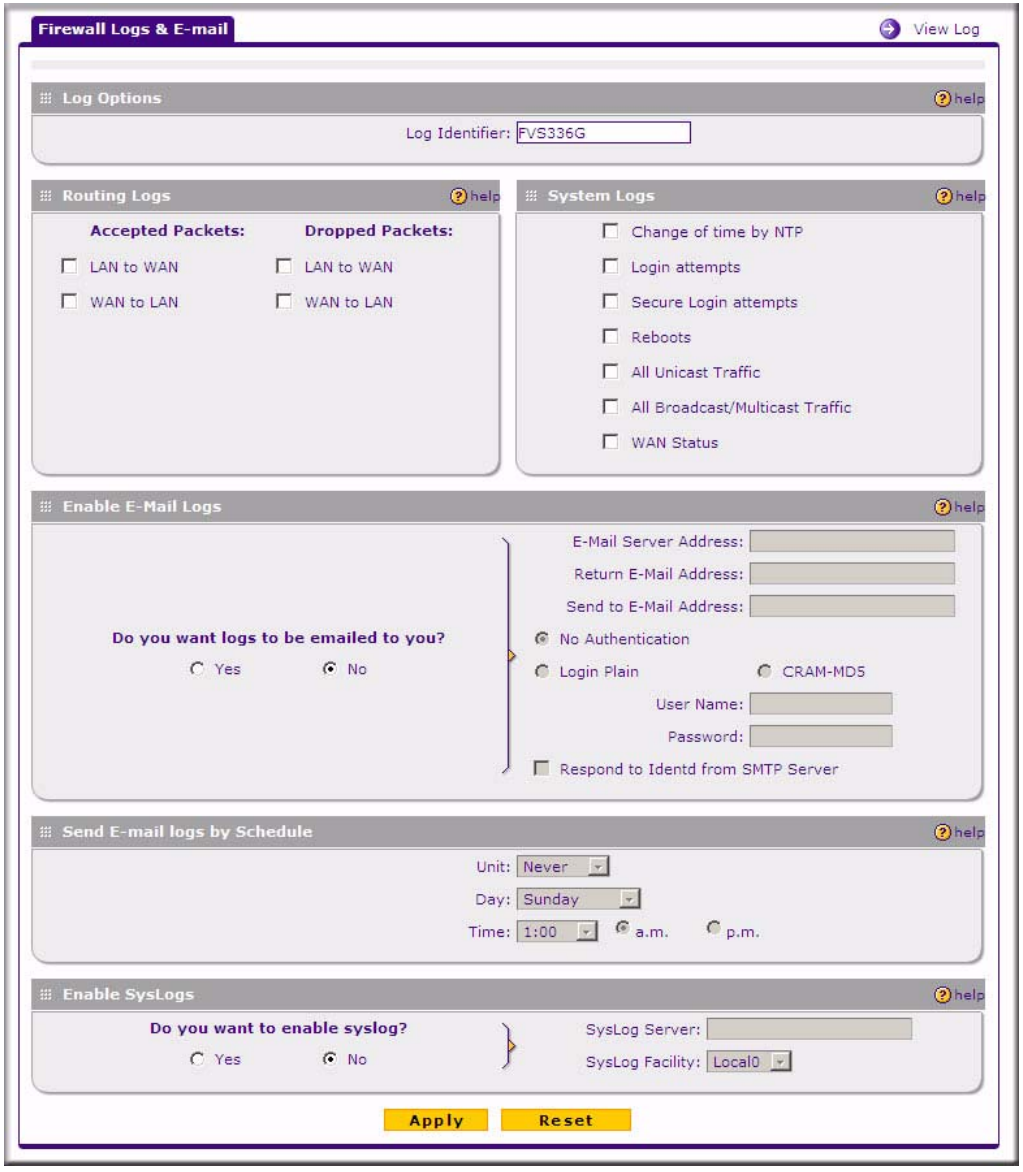


Figure 9-2

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. 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. You can configure the firewall to send system logs to an external PC that is running a syslog logging program. Click **Yes** to enable SysLogs and send messages to the syslog server, then:
   a. Enter your **SysLog Server** IP address
   b. Select the appropriate syslog facility from the **SysLog Facility** pull-down menu. The SysLog Facility levels of severity are described in the table below.
10. Click **Apply** to save your settings.

Numerical Code	Severity
0	Emergency: System is unusable
1	Alert: Action must be taken immediately
2	Critical: Critical conditions
3	Error: Error conditions
4	Warning: Warning conditions
5	Notice: Normal but significant conditions
6	Informational: Informational messages
7	Debug: Debug level messages

Viewing Firewall Logs

To view the Firewall logs:

1. Select Monitoring > Firewall Logs & E-mail from the main menu. The Firewall Logs & E-mail screen displays
2. Click the **View Log** link in the upper right-hand section of the screen. The **Logs** screen is displayed.
3. If the E-mail Logs options as been enabled, you can send a copy of the log by clicking **Send Log.**
4. Click **Refresh Log** to retrieve the latest update; click **Clear Log** to delete all entries.

Log entries are described in Table 9-1.

Table 9-1. Firewall Logs Field Descriptions

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

Viewing Router Configuration and System Status

The **Router Status** screen provides status and usage information. To view the router configuration and system status:

1. Select Monitoring > Router Status from the main menu. The Router Status screen is displayed.

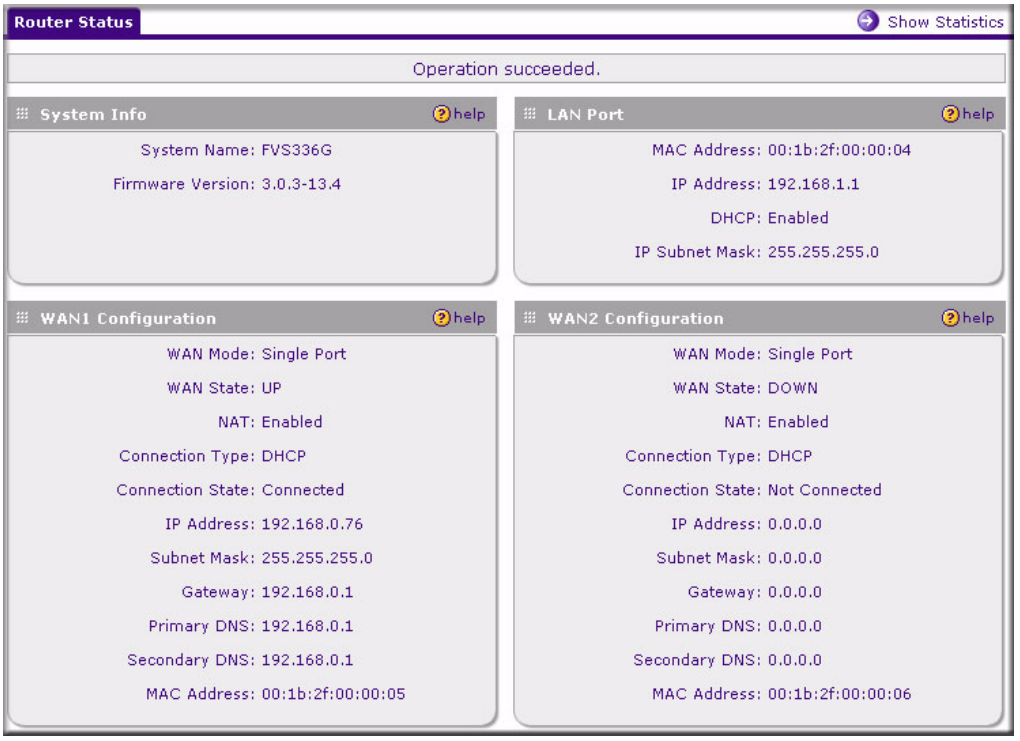


Figure 9-3

The following information is displayed:

Item	Description
System Name	This is the Account Name that you entered in the Basic Settings page.
Firmware Version	This is the current software the router is using. This will change if you upgrade your router.
LAN Port	Displays the current settings for MAC address, IP address, DHCP role and IP Subnet Mask that you set in the LAN IP Setup page. DHCP can be either Server or None.

Item	Description
WAN1 Configuration	Indicates whether the WAN Mode is Single, Dual, or Rollover, and whether the WAN State is UP or DOWN. It also is displayed if: • NAT is Enabled or Disabled. • Connection Type: DHCP enabled or disabled. • Connection State • WAN IP Address • Subnet Mask • Gateway Address • Primary and Secondary DNS Server Addresses • MAC Address.
WAN2 Configuration	Displays the same details as for WAN1 Configuration.

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

Monitoring the Status of WAN Ports

You can monitor the status of both of the WAN connections, the Dynamic DNS Server connections, and the DHCP Server connections. To monitor the status of the WAN ports:

1. Select Network Configuration > WAN Settings from the main menu. The **WAN1 ISP Settings** screen is displayed.
2. Click the **WAN Status** link in the upper right-hand section of the screen. The **Connection Status** popup window displays a status report on the WAN1 port.
3. To get a status report on the WAN2 port, click the **WAN2 ISP Settings** tab, and then click the **WAN Status** link.

Figure 9-4

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 > LAN Settings from the main menu, and then select the LAN Groups tab. The LAN Groups screen will display.
2. The **Known PCs and Devices** database 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 (in the LAN Setup menu) 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.

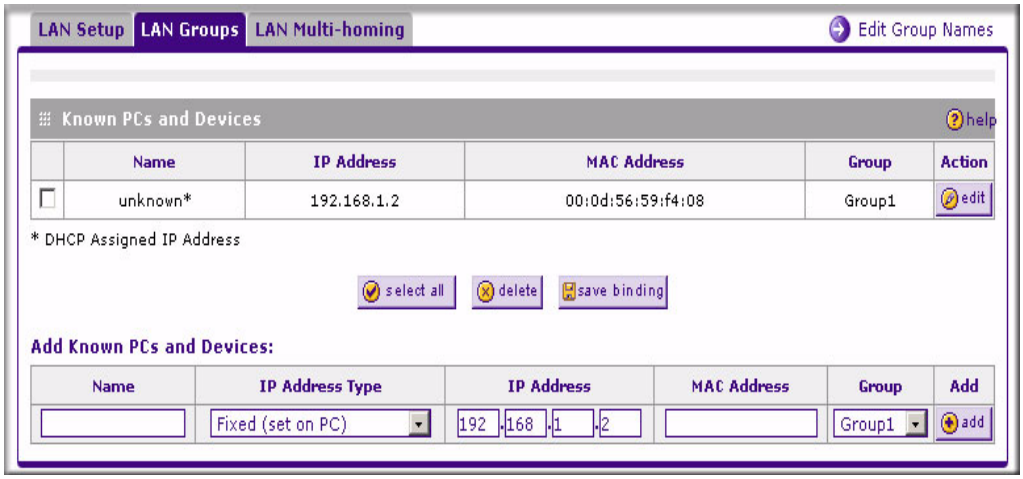


Figure 9-5

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 9-2. 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.

Reviewing the DHCP Log

To review the most recent entries in the DHCP log:

1. Select **Network Configuration > LAN Settings** from the main menu, and then click the LAN Setup tab. The LAN Setup screen will display.

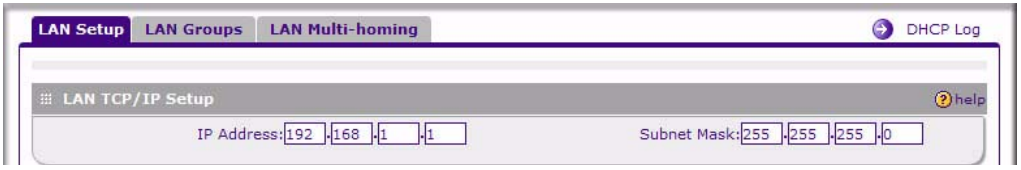


Figure 9-6

2. Click the **DHCP Log** link to the right of the tabs. The **DHCP Log** appears in a popup window.

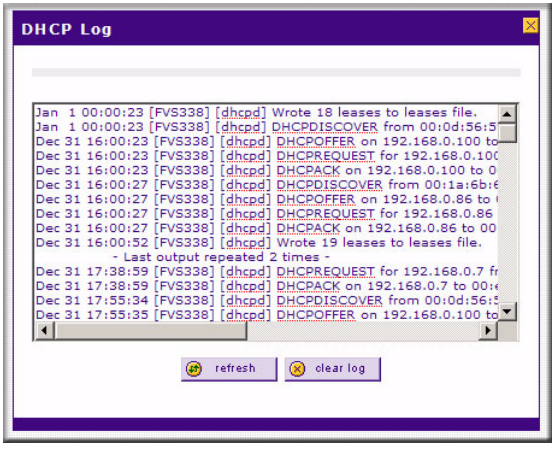


Figure 9-7

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

Monitoring Active Users

The Active Users menu screen displays a list of administrators and SSL VPN users currently logged into the device.

To display the list of active users:

1. Select **Monitoring** > **Active Users** from the main menu. The Active Users screen is displayed.

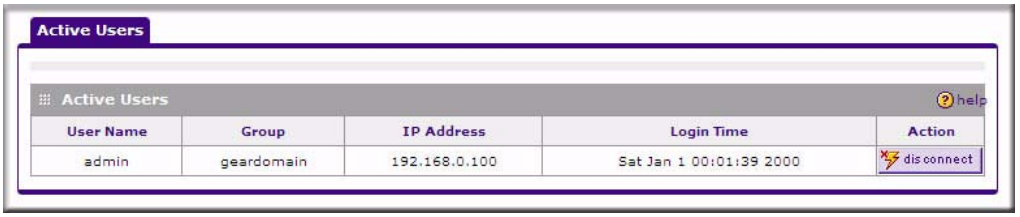


Figure 9-8

The active user's username, group, and IP address are listed in the table with a timestamp indicating the time and date that the user logged in.

2. You can disconnect an active user by clicking **Disconnect** to the right of the user's list entry.

Viewing Port Triggering Status

To view the status of Port Triggering:

1. Select Security > Port Triggering from the main menu.The Port Triggering screen will display.

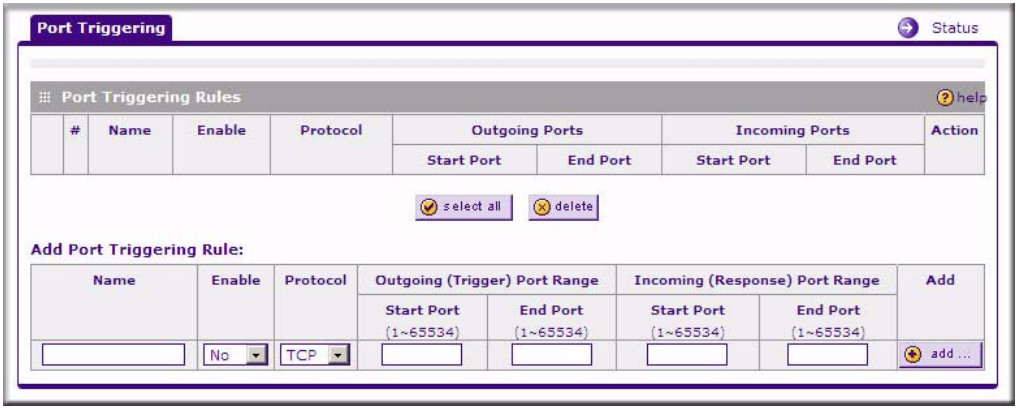


Figure 9-9

2. When the **Port Triggering** screen is displayed, click the **Status** link to the right of the tab to display the **Port Triggering Status**.

Figure 9-10

The status window displays the following information:

Item	Description
Rule	The name of the port triggering rule associated with this entry.
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 made available for other PCs. This timer is restarted whenever incoming or outgoing traffic is received.

Monitoring VPN Tunnel Connection Status

To review the status of current VPN tunnels:

1. Select VPN > Connection Status from the main menu, and then select the IPsec VPN Connection Status tab. The **IPsec Connection Status** screen is displayed.

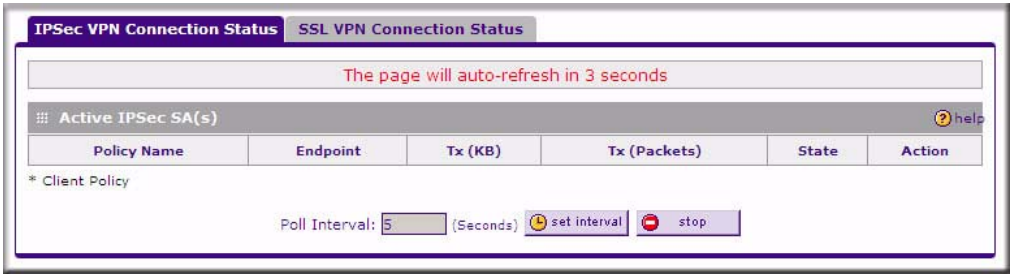


Figure 9-11

The Active IPsec SAs table lists each active connection with the following information.

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.

2. Select the SSL VPN Connection Status tab.The SLL VPN Connection Status screen will display

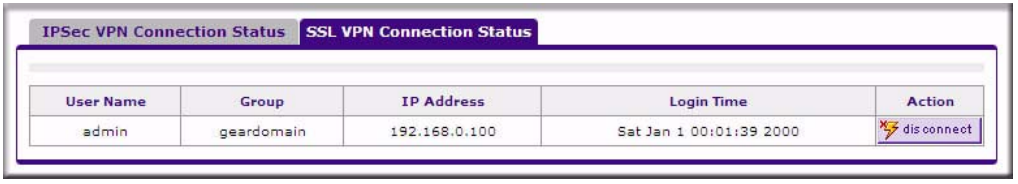


Figure 9-12

The active SSL VPN user's username, group, and IP address are listed in the table with a timestamp indicating the time and date that the user connected.

3. You can disconnect an active SSL VPN user by clicking **Disconnect** to the right of the user's list entry.

Reviewing the VPN Logs

The **VPN Logs** screen gives log details for recent VPN activity.

1. Select Monitoring > VPN Logs from the main menu, and select the IPsec VPN Logs tab. The IPsec VPN Logs screen will display.

Figure 9-13

2. To view the most recent entries, click **refresh log**. To delete all the existing log entries, click **clear log**.
3. Select the SSL VPN Logs tab to view SSL VPN log details.

Chapter 10
Troubleshooting

This chapter provides troubleshooting tips and information for your ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN. After each problem description, instructions are provided to help you diagnose and solve the problem.

This chapter contains the following sections:

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 two minutes, verify that:
   a. The TEST LED is not lit.
   b. The LAN port LINK/ACT LEDs are lit for any local ports that are connected.
   c. The WAN port LINK/ACT LEDs are lit for any WAN ports that are connected.

   If a port's LINK/ACT LED is lit, a link has been established to the connected device. If a LAN port is connected to a 1000 Mbps device, verify that the port's SPEED LED is green. If the port is 100 Mbps, the LED will be amber. If the port is 10 Mbps, the LED will be off.

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

Power LED Not On

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

- Make sure that the power cord is properly connected to your VPN firewall and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12 V DC power adapter supplied by NETGEAR for this product.

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

LEDs Never Turn Off

When the VPN firewall is turned on, the LEDs turns on for about 10 seconds and then turn off. If all the LEDs stay on, there is a fault within the 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 10-7.

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

LAN or WAN Port LEDs Not On

If either the LAN LEDs or WAN LEDs 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 192.168.1.2 to 192.168.1.254.

Note: If your PC's IP address is shown as 169.254.x.x: 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 don't 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 10-7.

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

- Make sure you are using the SSL *https://address* login rather than *http://address*.
- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

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

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

Troubleshooting the ISP Connection

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

To check the WAN IP address:

1. Launch your browser and navigate to an external site such as www.netgear.com
2. Access the Main Menu of the VPN firewall's configuration at https://192.168.1.1
3. Under the Monitoring menu, click Router Status.
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 in the Basic Settings menu.

- Your ISP only allows one Ethernet MAC address to connect to the Internet, and may check for your PC's MAC address. In this case:
  - Inform your ISP that you have bought a new network device, and ask them to use the VPN firewall's MAC address; or
  - Configure your VPN firewall to spoof your PC's MAC address. This can be done in the Basic Settings menu. Refer to "Manually Configuring the Internet Connection" on page 2-7.

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 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 firewall is set up correctly.

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

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

   ```
   ping 192.168.1.1
   ```
3. Click **OK.** A message, similar to the following, should display:

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

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

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

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

```
Request timed out
```

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

- Wrong physical connections
  - Make sure the LAN port LED is on. If the LED is off, follow the instructions in "LAN or WAN Port LEDs Not On" on page 10-2.
  - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and 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 in the Basic Settings menu.

- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your VPN firewall to "clone" or "spoof" the MAC address from the authorized PC. Refer to "Manually Configuring the Internet Connection" on page 2-7.

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 "Configuration File Management" on page 8-15).
- Use the reset button on the rear panel of the VPN firewall. Use this method for cases when the administration password or IP address is not known.

To restore the factory default configuration settings without knowing the administration password or IP address, you must use the reset button on the rear panel of the VPN firewall.

To restore the factory defaults:

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

Problems with Date and Time

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

- Date shown is January 1, 2000. Cause: The 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. Check the Time Zone menu, and check or uncheck the box marked “Adjust for Daylight Savings Time”.

Using the Diagnostics Utilities

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

Note: For normal operation, diagnostics are not required.

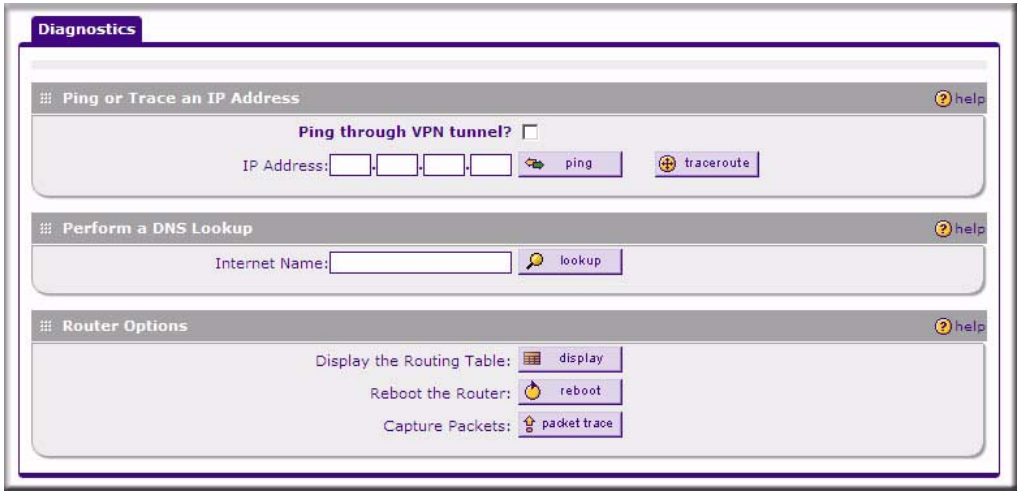


Figure 10-1

Table 10-1. Diagnostics

Item	Description
Ping or trace an IP address	Ping – Used to send a ping packet request to a specified IP address—most often, to test a connection. If the request times out (no reply is received), it usually means that the destination is unreachable. However, some network devices can be configured not to respond to a ping. The ping results will be displayed in a new screen; click "Back" on the Windows menu bar to return to the Diagnostics screen. If the specified address is intended to be reached through a VPN tunnel, check **Ping through VPN tunnel**.
	Traceroute – Lists all routers between the source (this device) and the destination IP address. The traceroute results will be displayed in a new screen; click "Back" on the Windows menu bar to return to the Diagnostics screen.
Perform a DNS lookup	A DNS (Domain Name Server) converts the Internet name (for example, 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 request a DNS lookup to find the IP address.
Display the routing table	This operation will display the internal routing table, which can be used by Technical Support to diagnose routing problems.
Reboot the VPN firewall	Used to perform a remote reboot (restart). You can use this if the VPN firewall seems to have become unstable or is not operating normally.
	Note: Rebooting will break any existing connections either to the VPN firewall (such as your management session) or through the VPN firewall (for example, LAN users accessing the Internet). However, connections to the Internet will automatically be re-established when possible.
Packet trace	Packet Trace selects the interface and starts the packet capture on that interface.

Appendix A
Default Settings and Technical Specifications

You can use the reset button located on the rear panel to reset all settings to their factory defaults. This is called a hard reset.

- To perform a hard reset, press and hold the reset button for approximately 10 seconds (until the TEST LED blinks rapidly). Your device will return to the factory configuration settings shown in Table A-1 below.
- Pressing the reset button for a shorter period of time will simply cause your device to reboot.

Table A-1. VPN firewall Default Configuration Settings

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

Table A-1. VPN firewall Default Configuration Settings (continued)

Feature		Default Behavior
	Time Zone	GMT
	Time Zone Adjusted for Daylight Saving Time	Disabled
	SNMP	Disabled
	Remote Management	Disabled
Firewall		
	Inbound (communications coming in from the Internet)	Denied
	Outbound (communications from the LAN to the Internet)	Allowed (all)
	Source MAC filtering	Disabled
	Stealth Mode	Enabled

Technical specifications for the ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN are listed in the following table.

Table A-2. VPN firewall Technical Specifications

Feature		Specifications
Network Protocol and Standards Compatibility		
	Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP PPP over Ethernet (PPPoE)
Power Adapter		
	North America:	120V, 60 Hz, input
	United Kingdom, Australia:	240V, 50 Hz, input
	Europe:	230V, 50 Hz, input
	Japan:	100V, 50/60 Hz, input
Physical Specifications		
	Dimensions:	1.7 x 13 x 8.2 in.
	Weight:	2 kg (4.5 lb)

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

Feature		Specifications
Environmental Specifications		
	Operating temperature:	0° to 40° C (32º to 104º F)
	Operating humidity:	90% maximum relative humidity, noncondensing
Electromagnetic Emissions		
	Meets requirements of:	FCC Part 15 Class B
		VCCI Class B
		EN 55 022 (CISPR 22), Class B
Interface Specifications		
	LAN:	10BASE-T or 100BASE-Tx 1000BASE-T, RJ-45
	WAN:	10BASE-T or 100BASE-Tx 1000BASE-T, RJ-45

Table A-3. SSL VPN Technical Specifications

Parameter	Specification
Network Management	Web-based configuration and status monitoring
Concurrent Users Supported	10 tunnels
Encryption	DES, 3DES, AES, MD5, SHA-1
Authentication Loca	l User database, RADIUS, LDAP, MS Active Directory
Certificates supported X.5	09, CRL
Electromagnetic Compliance	FCC Part 15 Class B, CE, and C-TICK
Environmental Specifications	Operating temperature: 0 to 50° C Operating humidity: 5-95%, non-condensing

Appendix B
Related Documents

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

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

Appendix C
Network Planning for Dual WAN Ports

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

This appendix contains the following sections:

What You Will Need to Do Before You Begin

The ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN is a powerful and versatile solution for your networking needs. To make the configuration process easier and to understand all of the choices available to you, you should consider the following items before you begin:

1. Plan your network
    a. Determine whether you will use one or both WAN ports. For one WAN port, you may need a fully qualified domain name either for convenience or to remotely access a dynamic WAN IP address.
    b. If you intend to use both WAN ports, determine whether you will use them in rollover mode for increased system reliability or load balancing mode for maximum bandwidth efficiency. See the topics in this appendix for more information. Your decision has the following implications:
        - Fully qualified domain name
            – For rollover mode, you will need a fully qualified domain name to implement features such as exposed hosts and virtual private networks.
            – For load balancing mode, you may still need a fully qualified domain name either for convenience or to remotely access a dynamic WAN IP address.
        - Protocol binding

– For rollover mode, protocol binding does not apply.

– For load balancing mode, decide which protocols should be bound to a specific WAN port.

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

3. Set up your accounts

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

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

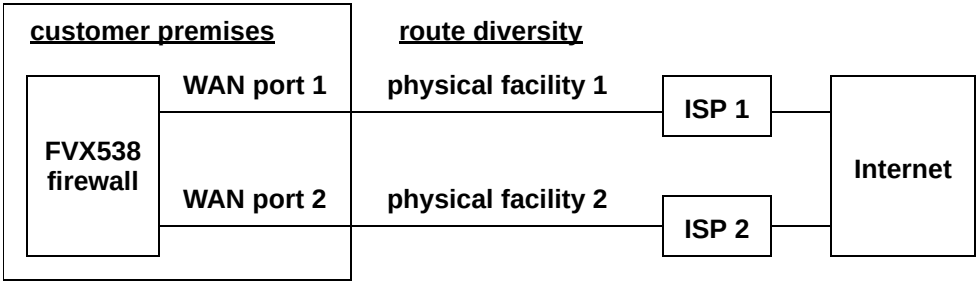


Figure C-1

- If your ISP charges by the volume of data traffic each month, consider enabling a traffic meter to monitor or limit your traffic.

b. Contact a Dynamic DNS Service and register fully qualified domain names for one or both WAN ports.

3. Plan your network management approach

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

  You are strongly advised to change the default management password to a strong password before enabling remote management.

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

4. Prepare to physically connect the firewall to your cable or DSL modems and a computer. Instruction for connecting your VPN firewall are in the *Installation Guide, FVS336G ProSafe Dual WAN Gigabit Firewall with SSL & IPsec VPN*.

Cabling and Computer Hardware Requirements

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

Computer Network Configuration Requirements

The FVS336G includes a built-in Web Configuration Manager. To access the configuration menus on the FVS336G, your must use a Java-enabled Web browser program that supports HTTP uploads such as Microsoft Internet Explorer or Netscape Navigator. NETGEAR recommends using Internet Explorer or Netscape Navigator 5.0 or above. Free browser programs are readily available for Windows, Macintosh, or UNIX/Linux.

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

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

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

Internet Configuration Requirements

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

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

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

Where Do I Get the Internet Configuration Parameters?

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

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

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

Internet Connection Information Form

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

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

Login Name: _____ Password: _____

Service Name: _____

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

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

Gateway IP Address: _____._____._____._____

Subnet Mask: _____._____._____._____

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

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

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

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

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

ISP Host Name: _____ ISP Domain Name: _____

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

Dynamic DSN Service Provider: _____ FQDN: _____

Overview of the Planning Process

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

- Inbound traffic (port forwarding, port triggering)
- Outbound traffic (protocol binding)
- Virtual private networks (VPNs)

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

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

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

Inbound Traffic

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

Virtual Private Networks (VPNs)

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

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

The Roll-over Case for Firewalls With Dual WAN Ports

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

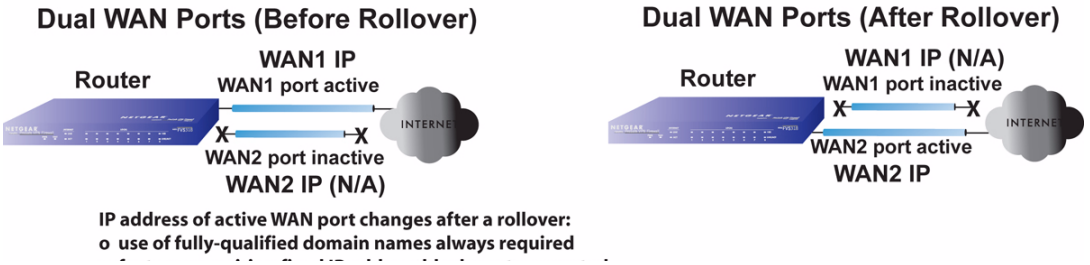


Figure C-2

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

The Load Balancing Case for Firewalls With Dual WAN Ports

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

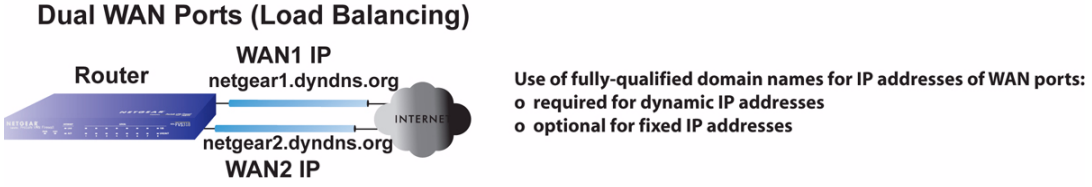


Figure C-3

Inbound Traffic

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

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

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

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

Inbound Traffic to Single WAN Port (Reference Case)

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

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

Figure C-4

Inbound Traffic to Dual WAN Port Systems

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

Inbound Traffic: Dual WAN Ports for Improved Reliability

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

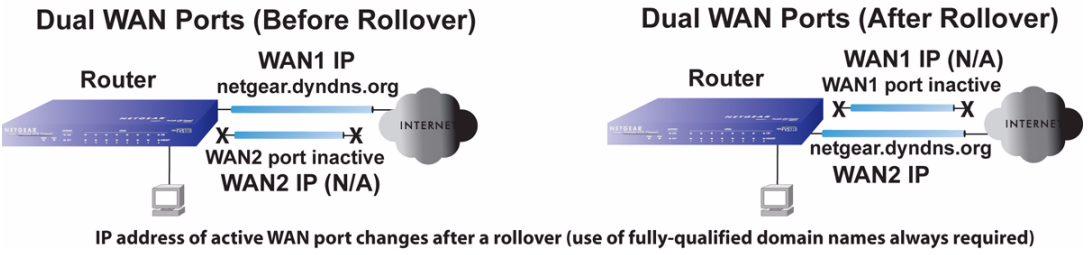


Figure C-5

Inbound Traffic: Dual WAN Ports for Load Balancing

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

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

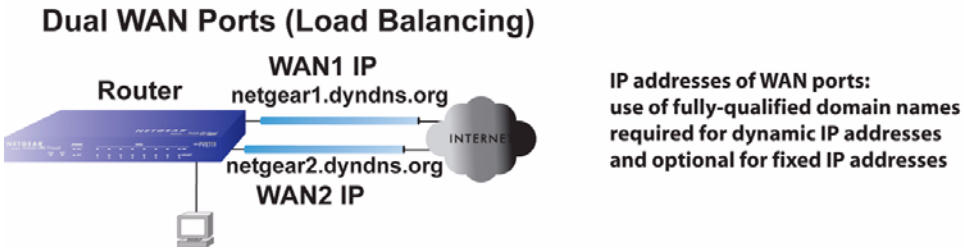


Figure C-6

Virtual Private Networks (VPNs)

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

Table C-2. IP addressing requirements for VPNs in dual WAN port systems

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

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

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

- Rollover Case for Dual Gateway WAN Ports

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

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

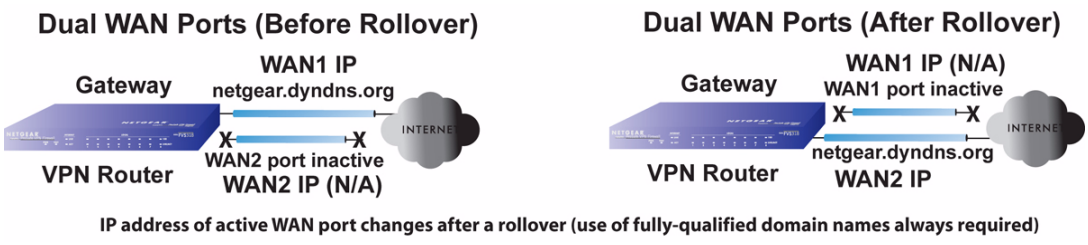


Figure C-7

- Load Balancing Case for Dual Gateway WAN Ports

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

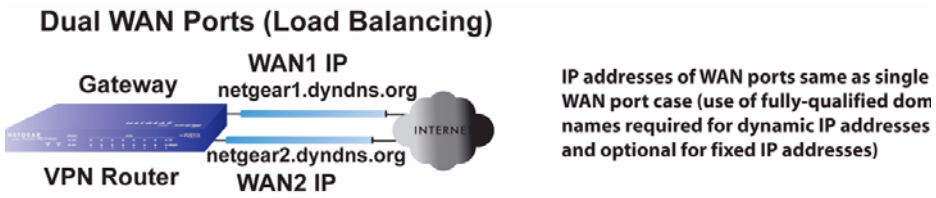


Figure C-8

VPN Road Warrior (Client-to-Gateway)

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

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

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

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

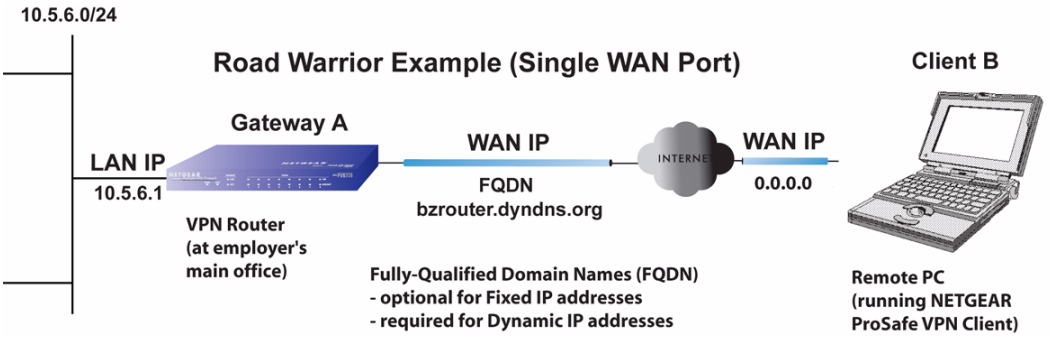


Figure C-9

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

VPN Road Warrior: Dual Gateway WAN Ports for Improved Reliability

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

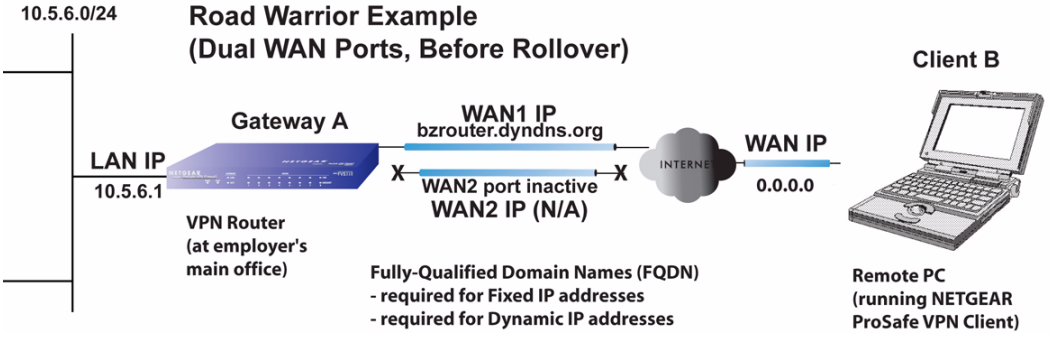


Figure C-10

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

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

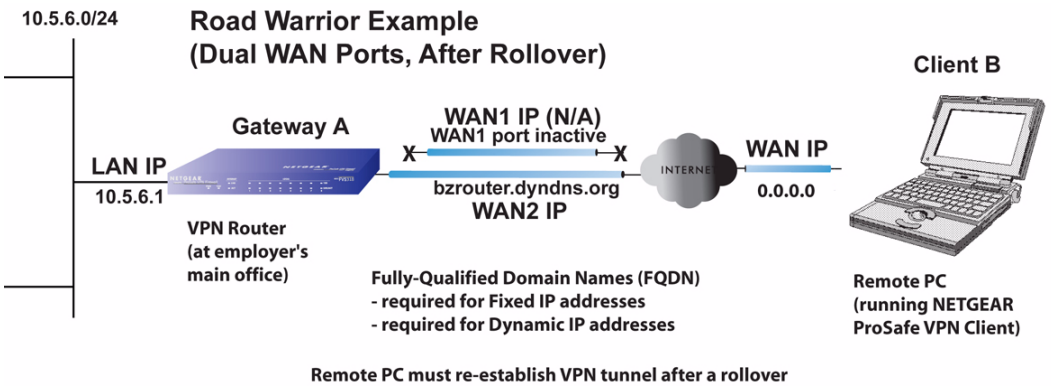


Figure C-11

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

VPN Road Warrior: Dual Gateway WAN Ports for Load Balancing

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

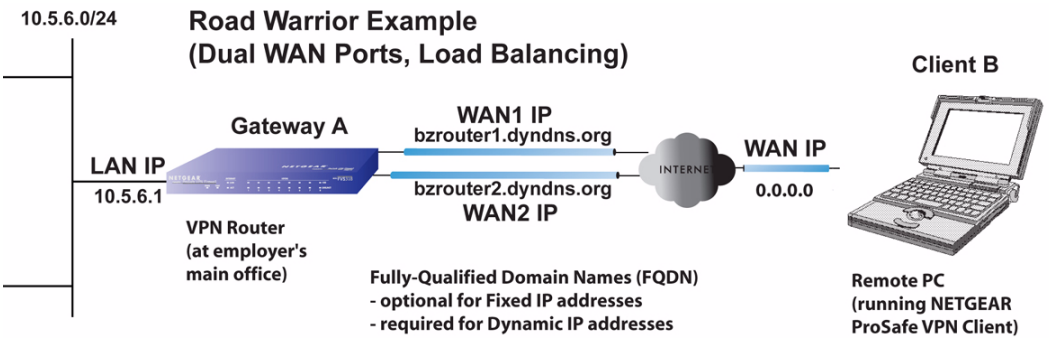


Figure C-12

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

VPN Gateway-to-Gateway

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

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

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

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

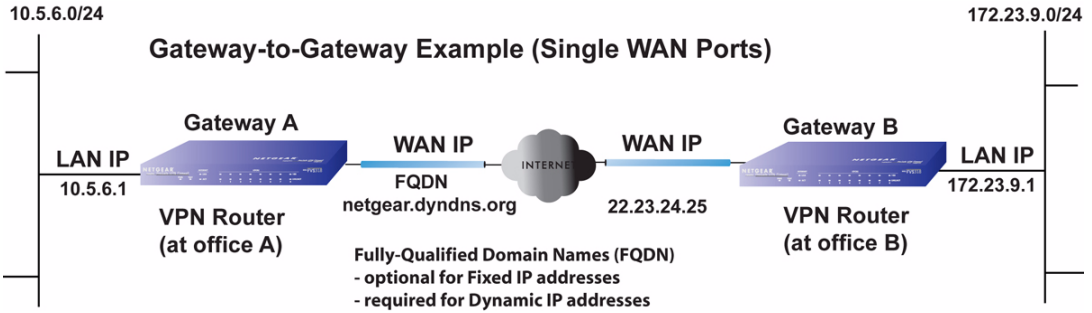


Figure C-13

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

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

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

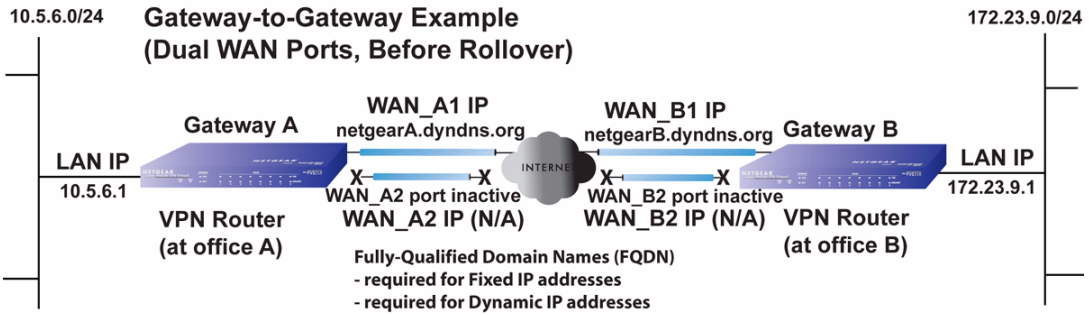


Figure C-14

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

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

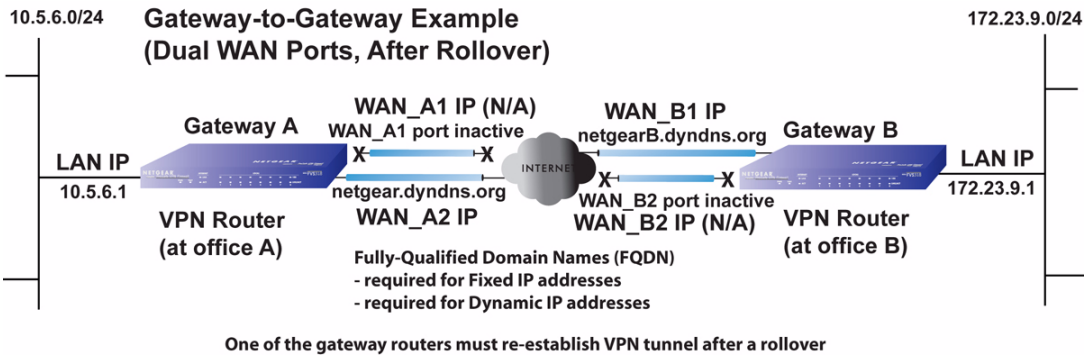


Figure C-15

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

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

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

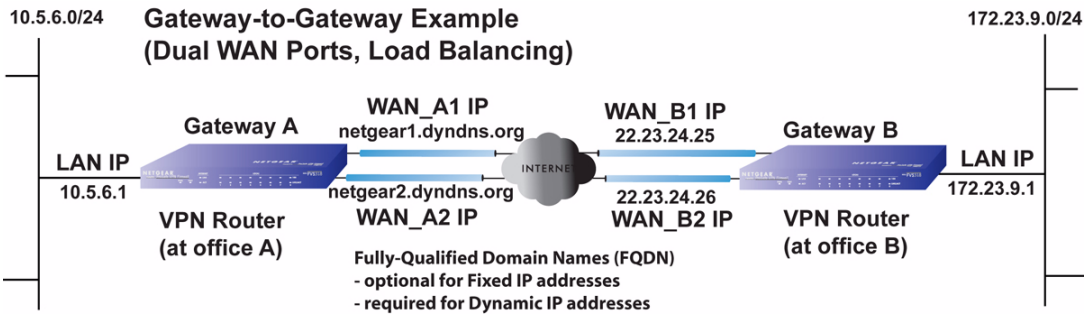


Figure C-16

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

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

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

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

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

VPN Telecommuter: Single Gateway WAN Port (Reference Case)

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

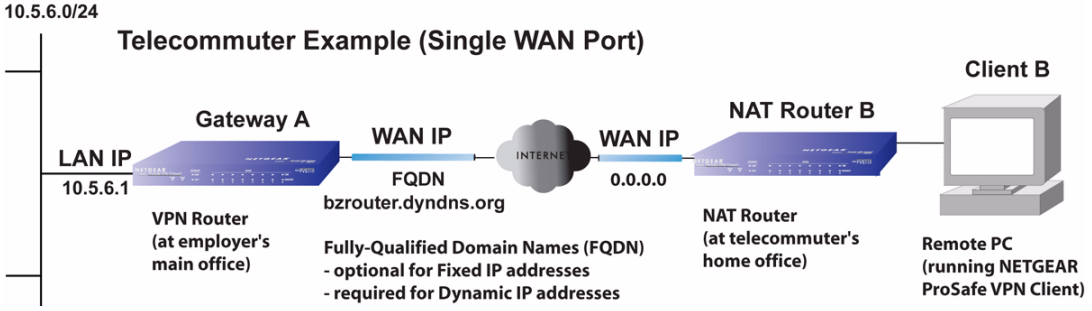


Figure C-17

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

VPN Telecommuter: Dual Gateway WAN Ports for Improved Reliability

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

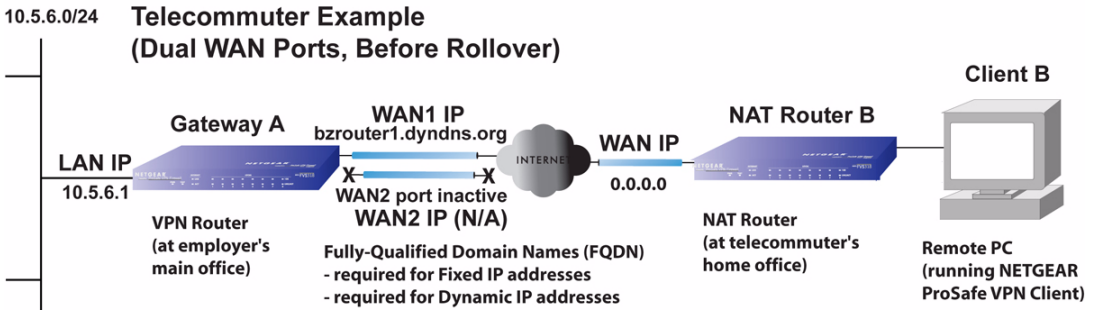


Figure C-18

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

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

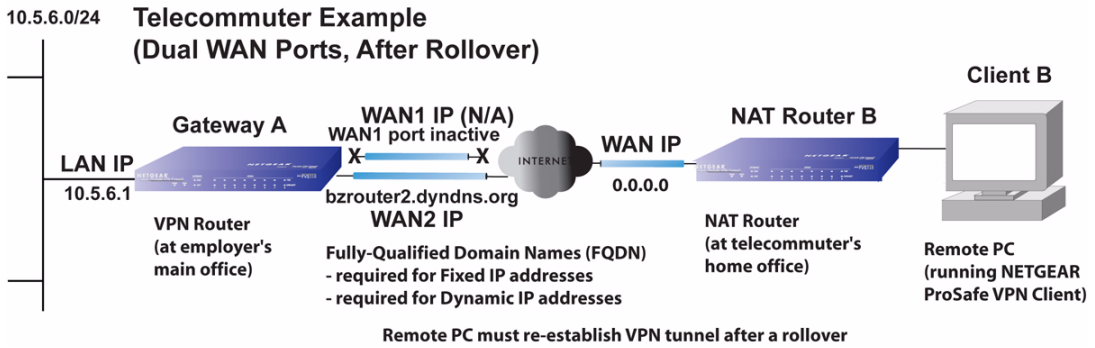


Figure C-19

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

VPN Telecommuter: Dual Gateway WAN Ports for Load Balancing

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

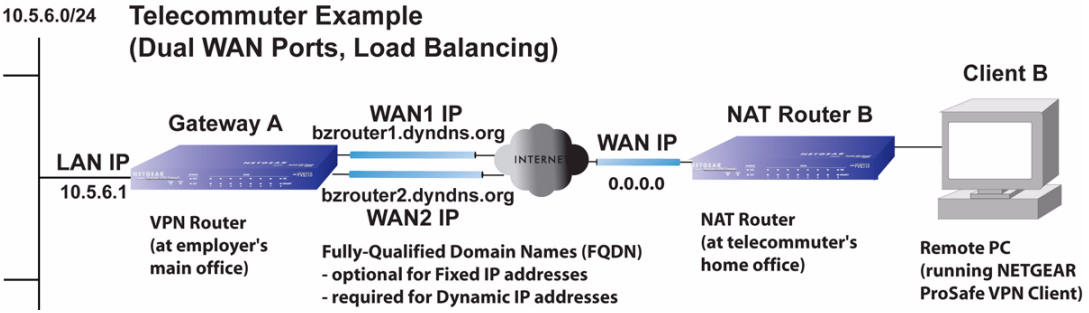


Figure C-20

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

Appendix D
Two Factor Authentication

This appendix provides an overview of two factor authentication, and an example of how to implement the WiKID solution.

This appendix contains the following sections:

Why do I need Two-Factor Authentication?

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 becoming more sophisticated where 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 – fox example, biometrics such as fingerprints or retinal.

We will only focus and discuss 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 Windows Active Directory or LDAP as the authentication server, administrators now have the option to use WiKID to do 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 once 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 a quick example of how WiKID work.

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 one-time passcode (OTP) from the WiKID authentication server:

Figure D-1

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

Figure D-2

	Note: The one-time passcode is time synchronized to the authentication server so that the OTP can only be used once and must be used before the expiration time. If a user does not use this passcode before it is expired, the user will need to go through the request process again to generate a new OTP.

3. The user then goes to the two factor login page and enters the generated one-time passcode as the login password.

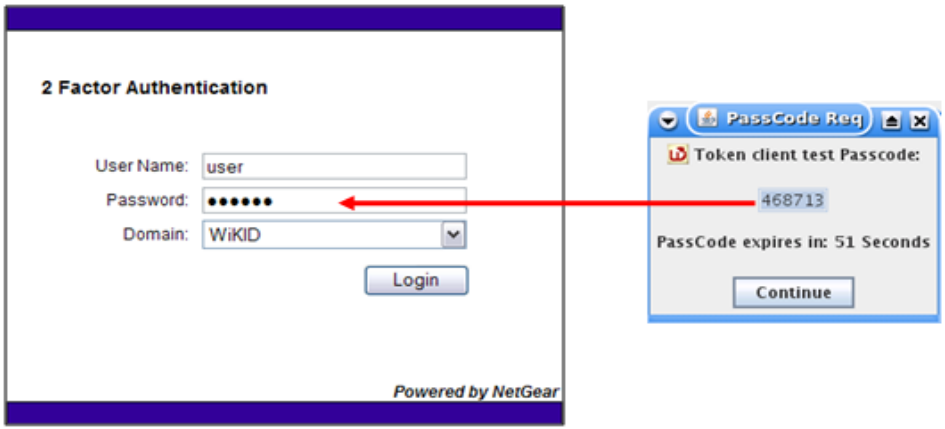


Figure D-3

Two-Factor Authentication is a new and easy way to enhance networking security products without having to replace the existing hardware. To obtain and try the new Two-Factor Authentication solution on your products, visit NETGEAR Support website at http://kbserver.netgear.com.

Index

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X