DGFV338 ProSafe Wireless ADSL Modem VPN Firewall Router Reference Manual

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

April 2007
202-10161-01
v1.0

Technical Support

Please register to obtain technical support. Please retain your proof of purchase and warranty information.

To register your product, get product support or obtain product information and product documentation, go to *http://www.NETGEAR.com*. If you do not have access to the World Wide Web, you may register your product by filling out the registration card and mailing it to NETGEAR customer service.

You will find technical support information at: *http://www.NETGEAR.com/* through the customer service area. If you want to contact technical support by telephone, see the support information card for the correct telephone number for your country.
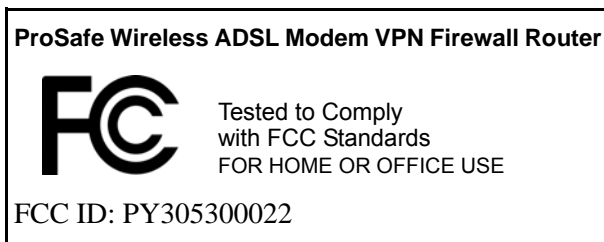
Trademarks

NETGEAR and the NETGEAR logo are registered trademarks and ProSafe is a trademark of NETEAR, 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

ProSafe Wireless ADSL Modem VPN Firewall Router

FC Tested to Comply
with FCC Standards
FOR HOME OR OFFICE USE

FCC ID: PY305300022

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

• This device may not cause harmful interference.

• This device must accept any interference received, including interference that may cause undesired operation.

Placement and Range Guidelines

Indoors, computers can connect over 802.11 wireless networks at a maximum range of 500 feet (152.4 m) for 802.11b devices. However, the operating distance or range of your wireless connection can vary significantly, based on the physical placement of the wireless access point.

For best results, identify a location for your wireless access point according to these guidelines:

- Away from potential sources of interference, such as PCs, large metal surfaces, microwaves, and 2.4 GHz cordless phones.
- In an elevated location such as a high shelf that is near the center of the wireless coverage area for all mobile devices.

Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the wireless access point.

To meet FCC and other national safety guidelines for RF exposure, the antennas for this device must be installed to ensure a minimum separation distance of 20cm (7.9 in.) from persons. Further, the antennas shall not be collocated with other transmitting structures.

FCC Statement

DECLARATION OF CONFORMITY

We Netgear,
4500 Great America Parkway
Santa Clara, CA 95054, USA
Tel: +1 408 907 8000
declare under our sole responsibility that the product(s)
DGFV338 *(Model Designation)*
ProSafe Wireless ADSL Modem VPN Firewall Router *(Product Name)*
complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices)

FCC Requirements for Operation in the United States

Radio Frequency Interference Warnings & Instructions

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 and correct the interference by one or more of the following measures:

- Reorient or locate 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.

Europe – EU Declaration of Conformity C ϵ $\textcircled{!}$

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN300 328, EN301 489-17, EN60950Europe – Declaration of Conformity in Languages of the European Community

Èesky [Czech]	*NETGEAR Inc.* tímto prohlašuje, _e tento Radiolan je ve shodě se základními po_adavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede *NETGEAR Inc.* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *NETGEAR Inc.*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *NETGEAR Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *NETGEAR Inc.*, declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente *NETGEAR Inc.* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Åëëçíéêþ [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *NETGEAR Inc.* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *NETGEAR Inc.* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente *NETGEAR Inc.* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *NETGEAR Inc.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuviø [Lithuanian]	Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, *NETGEAR Inc.*, jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.

Português [Portuguese]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*NETGEAR Inc.* týmto vyhlasuje, _e Radiolan spĺňa základné po_iadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *NETGEAR Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Icelandic]	Hér með lýsir *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	*NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

Countries of Operation & Conditions of Use in the European Community

This device is intended to be operated in all countries of the European Community. Requirements for indoor vs. outdoor operation, license requirements and allowed channels of operation apply in some countries as described below.

Note: The user must use the configuration utility provided with this product to ensure the channels of operation are in conformance with the spectrum usage rules for European Community countries as described below.

This device requires that the user or installer properly **enter the current country of operation** in the Radio Settings menu as described in the Reference Manual, **before operating this device**.

This device will automatically limit the allowable channels determined by the current country of operation. Incorrectly entering the country of operation may result in illegal operation and may cause harmful interference to other system. The user is obligated to ensure the device is operating according to the channel limitations, indoor/outdoor restrictions and license requirements for each European Community country as described in this document.

This device employs **a radar detection feature** required for European Community operation in the 5GHz band. This feature is automatically enabled when the country of operation is correctly configured for any European Community country. The presence of nearby radar operation may result in temporary interruption of operation of this device. The radar detection feature will automatically restart operation on a channel free of radar.

The **5GHz Turbo Mode** feature is not allowed for operation in any European Community country. The current setting for this feature is found in the 5GHz Radio Configuration Window as described in the user guide.

This device may be operated **indoors or outdoors** in all countries of the European Community using the 2.4GHz band: Channels 1 – 13, except where noted below:

• In **Italy** the end-user must apply for a license from the national spectrum authority to operate this device outdoors.

• In **France** outdoor operation is only permitted using the 2.4 – 2.454 GHz band: Channels 1 – 7.

• **Belgium** requires notifying spectrum agency if deploying >300meter wireless links in outdoor public areas using 2.4GHz band.

v

European Spectrum Usage Rules - Effective April 11, 2006				
Country	**5.15-5.25 (GHz) Channels: 36,40,44,48**	**5.25-5.35 (GHz) Channels: 52,56,60,64**	**5.47-5.725 (GHz) Channels: 100,104,108,112,116, 120,124,128,132,136,140**	**2.4-2.4835 (GHz) Channels: 1 to 13 (Except Where Noted)**
ALL EC Countries	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor
Belgium	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor or Outdoor!
France	Indoor Only	Indoor Only	Indoor or Outdoor	Indoor Ch. 1-13 Outdoor 1-7 Only
Greece	Indoor Only	Indoor Only	Indoor Only	Indoor Only
Italy	Indoor Only	Indoor Only	Indoor (Outdoor w/License)	Indoor (Outdoor w/ License)
Turbo Mode	Not Allowed in 5GHz			Same 2.4 GHz rules as above
AdHoc Mode	Not Allowed			Same 2.4 GHz rules as above

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das ProSafe Wireless ADSL Modem VPN Firewall Router 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 Wireless ADSL Modem VPN Firewall Router 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:	DGFV338
Publication Date:	April 2007
Product Family:	Wireless Firewall
Product Name:	ProSafe Wireless ADSL Modem VPN Firewall Router
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10161-01
Publication Version Number	1.0

Contents

xii

xvi

About This Manual

The *DGFV338 ProSafe™ Wireless ADSL Modem VPN Firewall Router Reference Manual* describes how to install, configure and troubleshoot the ProSafe Wireless ADSL Modem VPN Firewall Router. The information is this manual is intended for readers with intermediate computer and Internet skills.

Conventions, Format and Scope

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

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

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

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

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

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

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

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

• **Scope.** This manual is written for the Wireless ADSL Router according to these specifications:

Product Version	ProSafe Wireless ADSL Modem VPN Firewall Router
Manual Publication Date	April 2007

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. Web site at *http://kbserver.netgear.com/products/DGFV338.asp*.

How to Use This Manual

The HTML version of this manual includes the following:

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

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

• A 🔍 button to access the full NETGEAR, Inc. online knowledge base for the product model.

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

How to Print this Manual

To print this manual you can choose one of the following several options, according to your needs. Your computer must have the free Adobe Acrobat Reader installed in order to view and print PDF files. The Acrobat Reader is available on the Adobe website at *http://www.adobe.com*.

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

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

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

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

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

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

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

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

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

Chapter 1
Introduction

This chapter describes the features of the ProSafe™ Wireless ADSL Modem VPN Firewall Router. It also includes the minimum prerequisites for installation ("System Requirements" on page 1-5.), what's in the box ("Package Contents" on page 1-6) and a description of the front and back panels of the DGFV338 ("Hardware Description" on page 1-6). The location of the default settings to log in to the router is presented in "Router Login Factory Defaults" on page 1-9 and suggestions on placement of your router to achieve maximum wireless range are in "Placement of your NETGEAR ProSafe DGFV338" on page 1-10.

Key Features of the NETGEAR ProSafe DGFV338

The NETGEAR ProSafe DGFV338 with eight-port switch connects your local area network (LAN) to the Internet through an internal ADSL modem or through the Ethernet port via an external modem. It provides wireless LAN connectivity operating at 2.4GHz (802.11b/g).

The NETGEAR ProSafe DGFV338 has a built-in Stateful Packet Inspection Firewall (SPI) preventing Denial of Service attacks and provides Internet access for up to 253 users. The NETGEAR ProSafe DGFV338 provides you with multiple Web content filtering options, plus browsing activity reporting and instant alerts—both, via e-mail. Network administrators can establish restricted access policies based on time-of-day, Website addresses and address keywords, and share high-speed cable/DSL Internet access for a local network.

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

The NETGEAR ProSafe DGFV338 provides the following features:

- An internal ADSL modem supporting Annex A or Annex B (depending upon region).
- One 10/100 Mbps Ethernet WAN port.
- 802.11g, 802.11b, 802.11g/b, or Auto 108Mbps.
- Support for up to 50 IPSec VPN tunnels.
- Easy, web-based setup for installation and management.
- URL keyword Content Filtering and Site Blocking Security.
- Quality of Service (QoS) support for traffic prioritization.
- Built in 8-port 10/100 Mbps switch.

- Extensive Protocol Support.
- SNMP for manageability.
- Front panel LEDs for easy monitoring of status and activity.
- Flash memory for firmware upgrade.
- Auto Sensing and Auto Uplink™

Full Routing on Both the ADSL and 10/100 WAN Port

You can install, configure, and operate the DGFV338 to take full advantage of a variety of routing options on both the DSL and broadband WAN ports, including:

- Internet access via either the internal ADSL modem or through the Ethernet port connected to an external modem.

- Auto Rollover Mode between the internal ADSL modem and the external 10/100 ethernet WAN port. If the primary connection fails, the DGFV338 can automatically establish a backup connection via the secondary connection.

A Powerful, True Firewall with Content Filtering

DGFV338 is a true firewall, using stateful packet inspection to defend against attacks. Its firewall features include:

- DoS protection. Automatically detects and thwarts DoS attacks such as Ping of Death, SYN Flood, LAND Attack, and IP Spoofing.

- Blocks unwanted traffic from the Internet to your LAN.

- Blocks access from your LAN to Internet locations or services that you specify as off-limits.

- Logs security incidents. The DGFV338 will log security events such as blocked incoming traffic, attacks, and administrator logins. You can configure the firewall to email the log to you at specified intervals. You can also configure the firewall to send immediate alert messages to your email address or email pager whenever a significant event occurs.

- With its URL keyword filtering feature, the DGFV338 prevents objectionable content from reaching your PCs. The firewall allows you to control access to Internet content by screening for keywords within Web addresses. You can configure the firewall to log and report attempts to access objectionable Internet sites.

Security

The NETGEAR ProSafe DGFV338 is equipped with several features designed to maintain security, as described in this section.

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

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

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

Virtual Private Networking (VPN)

The NETGEAR ProSafe DGFV338 provides a secure encrypted connection between your local area network (LAN) and remote networks or clients. It includes the following VPN features:

- Supports 50 IPSec VPN tunnels.

- Supports industry-standard VPN protocols – The DGFV338 supports standard Manual or IKE keying methods, standard MD5 and SHA-1 authentication methods, and standard DES, 3DES and AES encryption methods.

- Supports 256-bit AES encryption for maximum security.

- The VPN Wizard configuration is based on the Virtual Private Network Consortium (VPNC) recommended settings.

Autosensing Ethernet Connections with Auto Uplink

With its internal 8-port 10/100 switch, the DGFV338 can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. Both the LAN and WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

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

Extensive Protocol Support

The NETGEAR ProSafe DGFV338 supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP).

- **IP Address Sharing by NAT**. The DGFV338 allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as NAT, allows the use of an inexpensive single-user ISP account.

- **Automatic Configuration of Attached PCs by DHCP**. The DGFV338 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.

- **PPP over ATM (PPPoA)**. PPPoA is an asynchronous point-to-point protocol for connecting to the Internet over ADSL.

Easy Installation and Management

You can install, configure, and operate the ProSafe Wireless ADSL Modem VPN Firewall Router within minutes after connecting it to the network. The following features simplify installation and management tasks:

- **Browser-based management**. Browser-based configuration allows you to easily configure your firewall from almost any type of personal computer, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided and online help documentation is built into the browser-based Web Management Interface.

- **Smart Wizard.** The NETGEAR ProSafe DGFV338 automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.

- **VPN Wizard**. The NETGEAR ProSafe DGFV338 includes the NETGEAR VPN Wizard to easily configure VPN tunnels according to the recommendations of the Virtual Private Network Consortium (VPNC) to ensure the VPN tunnels are interoperable with other VPNC-compliant VPN routers and clients.

- **SNMP**. The NETGEAR ProSafe DGFV338 supports the Simple Network Management Protocol (SNMP) to let you monitor and manage 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, Packet Capture, DNS lookup, and remote reboot.

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

- **Visual monitoring**. The front panel LEDs of the NETGEAR ProSafe DGFV338 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 NETGEAR ProSafe DGFV338:

- Flash memory for firmware upgrade

- On-line technical support and telephone support for registered products.

System Requirements

Before installing the DGFV338, make sure your system meets these requirements:

- The Category 5 UTP straight through Ethernet cable with RJ-45 connector included in the package, or one like it
- A 100-240 V, 50-60 HZ AC power source.
- Cable, DSL, Satellite or Wireless Broadband modem (for Ethernet connection).
- Internet service.
- ADSL service (for ADSL connectivity).

- A Web browser for configuration such as Mozilla Firefox, Microsoft Internet Explorer 5.0 or above, or Netscape Navigator 7.2 or above.
- Network card for each connected PC.
- Network Software (for example, Windows).

Package Contents

The product package should contain the following items:

- ProSafe Wireless ADSL Modem VPN Firewall Router.
- AC power adapter.
- Two 2.4 GHz wireless antennas.
- ADSL Microfilter (UK only)
- Category 5 Ethernet cable.
- Telephone cable with RJ-11 connector
- *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.

Hardware Description

This section describes the front and rear hardware functions of the wireless ADSL firewall.

Router Front Panel

The ProSafe Wireless ADSL Modem VPN Firewall Router front panel shown below contains the power and test LEDs, Internet status LEDs, and the LAN status LEDs.
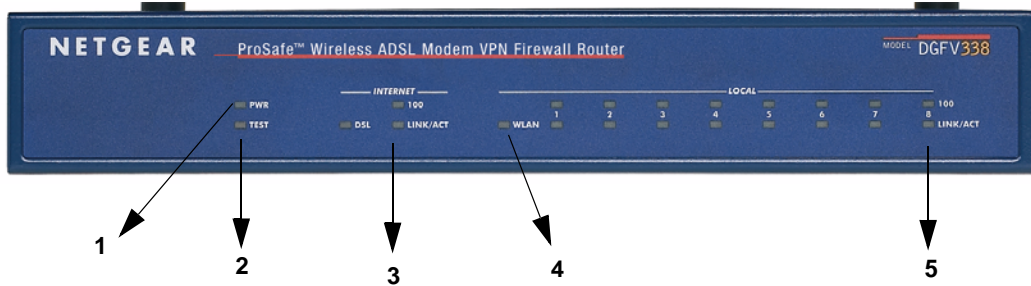
Figure 1-1

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

Table 0-1. Object Descriptions

Nos.	LEDs	Activity	Description
1	Power - 1	On (Green) Off	Power is supplied to the gateway Power is not supplied to the gateway.
2	Test - 2	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.
3	Internet LEDs	Link/Act LED On (Green) Blinking (Green) Off	The WAN port has detected a link with a connected Ethernet device. Data is being transmitted or received by the WAN port. The WAN port has no link.
		100 LED On (Green) Off	The WAN port is operating at 100 Mbps. The WAN port is operating at 10 Mbps.
		DSL LED On (Green) Blinking (Green) Off	The DSL modem has detected a link with the Internet. Data is being transmitted or received. The DSL modem has no connection.
4	WLAN	On (Green) Blinking (Green) Off	A wireless connection is detected. Data is being transmitted or received. No link is detected or the radio is disabled.

Table 0-1. Object Descriptions (continued)

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

Router Rear Panel

The rear panel of the ProSafe Wireless ADSL Modem VPN Firewall Router (Figure 1-2) contains the AC power connection; LAN, Ethernet and DSL port; and the reset button.
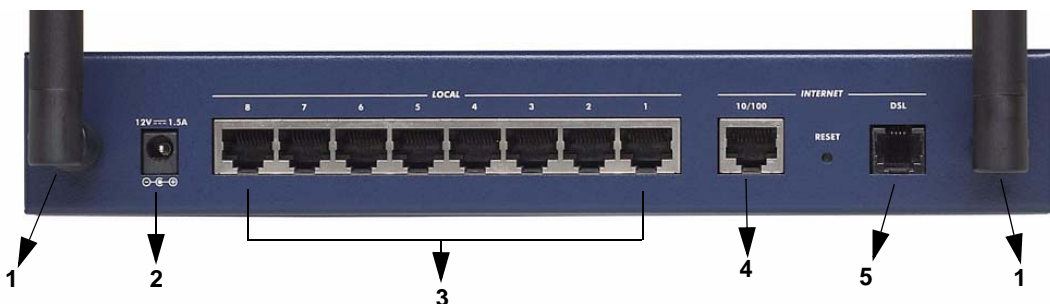
Figure 1-2

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

1. **Wireless antenna**. Two 2.4 GHz antennas attach to either end of the NETGEAR ProSafe DGFV338.

2. **DC Power connection (12VDC, 1.5A)**. Provides power to the gateway when the power supply is attached.

3. **Local LAN ports.** An 8-port RJ-45 10/100 Mbps Fast Ethernet Switch, N-way automatic speed negotiation, auto MDI/MDIX.

4. **Ethernet port**. serves as the 10/100 WAN port connection to an external modem. One RJ-45 WAN port, N-way automatic speed negotiation, Auto MDI/MDIX.

5. **ADSL port**. Serves as the direct WAN DSL connection to the Internet from the internal ADSL modem via a telephone cable.

Router Login Factory Defaults

Check the label on the bottom of the DGFV338's enclosure if you forget the following factory default information:

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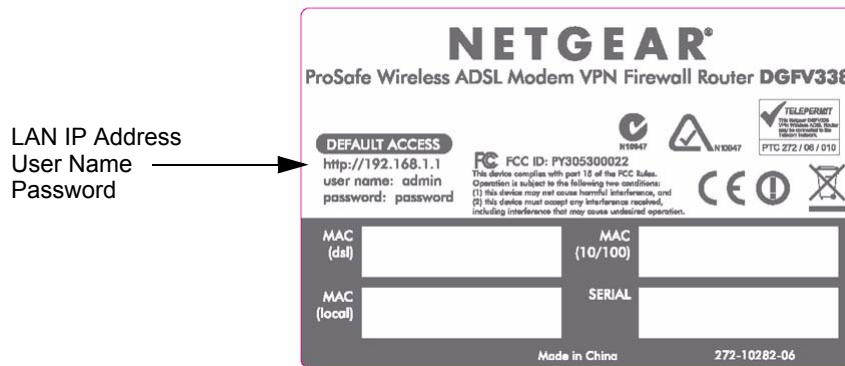- User name: **admin**
- Password: **password**

Figure 1-3

To log in to the DGFV338 once it is connected:

1. Open a Web browser.

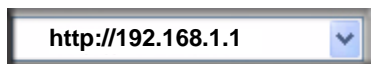2. Enter **http://192.168.1.1** as the URL.

Figure 1-4

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

Figure 1-5

For a complete list of the factory default settings of your NETGEAR ProSafe DGFV338, see Appendix A, "Default Settings and Technical Specifications"

Placement of your NETGEAR ProSafe DGFV338

> **Note:** Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the wireless ADSL firewall.

The operating distance or range of your wireless connection can vary significantly based on the physical placement of NETGEAR ProSafe DGFV338. The latency, data throughput performance, and notebook power consumption also vary depending on your configuration choices. For best results, place your wireless ADSL firewall:

- Near the center of the area in which your PCs will operate.

- In an elevated location, such as a high shelf where the wireless-connected PCs have line-of-sight access (even if through walls). The best location is elevated, such as wall mounted or on the top of a cubicle, and at the center of your wireless coverage area for all the mobile devices.

- Away from potential sources of interference, such as PCs, microwaves and cordless phones.

- With the antenna tight and in an upright position.

- Away from large metal surfaces.

Chapter 2
Basic Installation and Configuration

This section provides instructions for connecting the DGFV338. Typically, it takes approximately seven steps to complete connecting all facets of your gateway:

1. **Connect the gateway physically to your network.** If connecting through a modem, power off and disconnect the modem before starting. Connect the cables after turning off your modem, if you are connecting through your Ethernet port.

    If connecting through the built-in ADSL modem, connect the wireless firewall to a microfilter, and then connect the microfilter to your phone jack (see "Using ADSL Microfilters (optional)" on page 2-2 for instructions on using microfilters).

    For additional instructions on connecting your ProSafe DGFV338, refer to the *DGFV338 ProSafe Wireless ADSL Modem VPN Firewall Router Installation Guide* on your Resource CD or to the NETGEAR Website for an online electronic copy.

2. **Restart your network in the correct sequence.** It is important to pay attention to the order in which you restart your network. Then, check the LEDs and make sure the test lights are working appropriately.

3. **Log into the gateway.** After logging in, you are ready to set up and configure your gateway. You can also change your password and enable remote management at this time.

4. **Configure the WAN Setup options for your ISP Internet connection(s)**. During this phase, you will connect to your ISP(s). You can also program the WAN traffic meters at this time.

5. **Configure the WAN mode for your Internet connection(s)**. You can also configure the dynamic DNS on the WAN ports (if needed).

    You can configure either the ADSL ISP or the Ethernet ISP or you can enable both ADSL and Ethernet ISPs, and configure them to operate in Auto-rollover mode. You can also configure Advanced options such as the factory default MTU size, port speed, and uplink bandwidth.

6. **Set up your wireless LANs.** Select the appropriate Country/Region and Operating Mode for your antenna configuration.

    Because the wireless interface is disabled by default, the initial wireless configuration must be made from a wired connection (either via ADSL or Ethernet). During this step, you can also choose the wireless security method for your LAN gateway; for example, versions of either WEP or WPA.

7. **Set up your VPN connections using Auto Detect**. If you do not know your ISP connection, Auto Detect will attempt to automatically detect your connection type by probing for different connection methods. If you know your ISP type, you can set up your connections manually. (Ensure that you have the ISP information relevant to your connection type before you begin.

Using ADSL Microfilters (optional)

ADSL technology uses the same wires as your telephone service. However, ADSL adds signals to the telephone lines which create noise in the telephone service. You must use ADSL microfilters to filter out these signals before they reach your telephone. If you are planning on using the ADSL modem port, and an ADSL Microfilter is not included with your ProSafe DGFV338, you should acquire one.

There are two types of ADSL Microfilters: a one-line filter and a two-line filter with splitter.

- **One-Line Microfilter.** A simple microfilter provides an interface filter between your telephone and the phone jack as shown in Figure 2-1. Each device such as a telephone, fax machine, answering machine, or caller ID display requires an ADSL microfilter..
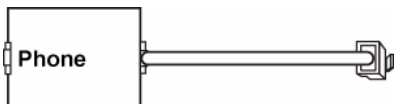

Figure 2-1

You can also connect the one-line filter to a phone-jack splitter to allow for connection of the wireless firewall. However, the phone-jack splitter must be a designated ADSL microfilter/ phone jack splitter.

- **ADSL Microfilter with Built-In Splitter.** Use an ADSL microfilter with built-in splitter when there is a single wall outlet which must provide connectivity for both the wireless firewall and the telephone equipment.
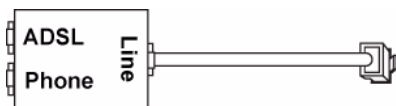

Figure 2-2

> ⚠️ **Warning:** Do not connect the wireless firewall to the ADSL line through a microfilter unless the microfilter is a combination ADSL microfilter/splitter specifically designed for this purpose. Doing so will block your connection to the Internet. If you have any doubts about this, connect the wireless firewall directly to your phone line.

Logging in and Configuring your Internet Connection

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

To log in to the wireless firewall:

1. Connect to the gateway by typing **http://192.168.1.1** in the address field of Internet Explorer, Netscape Navigator, or Mozilla Firefox. The login screen will display.

Figure 2-3

2. Enter **admin** for the gateway user name and **password** for the gateway password in lower case letters. Both fields are case-sensitive. (The gateway user name and password are not the same as any user name or password you may use to log in to your Internet connection.)

3. Click **Login**. The ProSafe Wireless ADSL Modem VPN Firewall Router user interface will display.

> **Note:** You might want to enable remote management at this time so that you can log in remotely in the future to manage the gateway. See "Enabling Remote Management Access" on page 6-8 for more information. Remote management enable is cleared with a factory default reset.

> **Note:** When you enable remote management, we strongly advise that you change your password. See "Changing the Passwords and Login Time-out" on page 6-7 for the procedure on how to do this.

Configuring Your Internet Connection using Auto Detect

Depending on how you connected your gateway to the Internet, you can configure your ISP settings by choosing the ADSL ISP settings (for DSL) or the Ethernet ISP settings (for 10/100). If you connected to both, you can configure both.

> **Note:** To enable Auto-Rollover, you must have both ADSL and Ethernet ports connected and configured. If you intend to configure both, configure your primary WAN port first.

To automatically configure your ADSL ISP settings and connect to the Internet:

1. Go to the **ADSL ISP Settings** screen shown in Figure 2-4 by selecting the primary menu option **Network Configuration** and the sub-menu option **WAN Settings**.

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

When Auto Detect successfully detects an active Internet service, it reports which connection type it discovered. The options are described in the Table 2-1., "Internet Service Connections".

To automatically configure your Ethernet ISP settings and connect to the Internet:

1. Select the **Ethernet ISP Settings** screen similar to the one shown in Figure 2-5 should display.

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

When Auto Detect successfully detects an active Internet service, it reports which connection type it discovered. The options are described in the Table 2-1., "Internet Service Connections".
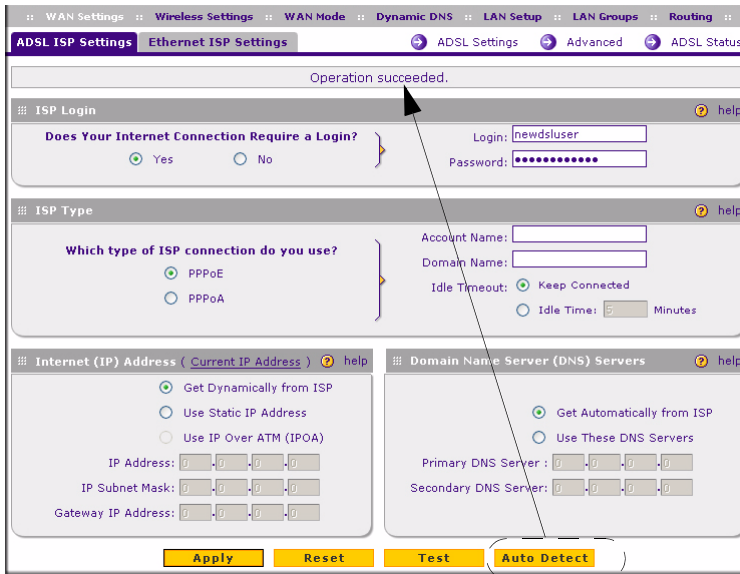

Figure 2-4
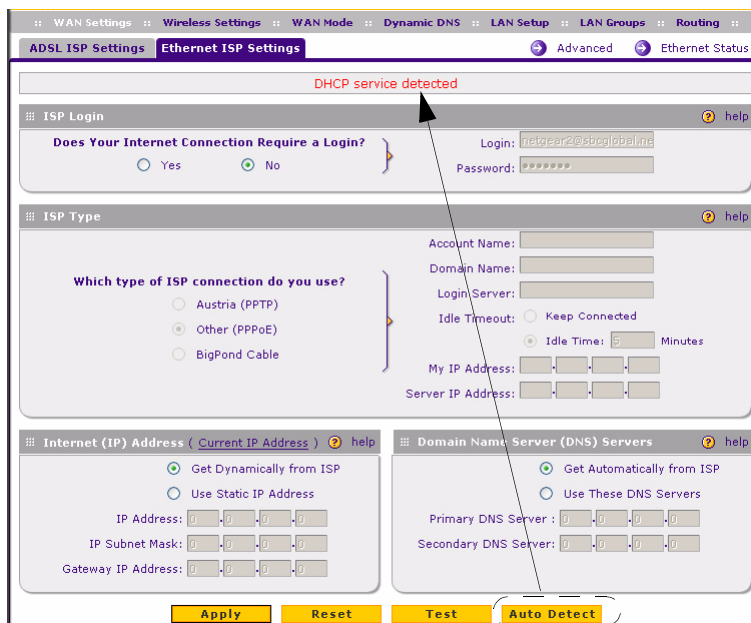
Figure 2-5

Table 2-1.   Internet Service Connections

Connection Method	Data Required
PPPoE	Login (Username, Password).
PPPoA	Login (Username, Password).
DHCP (Dynamic IP)	No data is required.
Static (Fixed) IP	Internet IP address, Subnet Mask and Gateway IP Address supplied by your ISP; and the Router's DNS Address (also supplied by your ISP).
IPoA	Internet IP Address and Subnet Mask; Gateway IP Address

Manually Configuring your ADSL Connection

Unless your ISP assigns your configuration automatically via DHCP, you will need the configuration parameters from your ISP. For example, if your router detected a PPPoE or PPPoA service, you must provide a Login sequence in order to obtain an Internet connection from your

ISP. If your ISP requires a Static IP address, then you must provide the fixed addresses for Static IP. The types of data you will need are highlighted in Table 2-1 by connection method, and explained in more detail below.

To configure your ADSL ISP connection:

1. Enter your ISP Login information. Select the **Does Your Internet Connection require a Login?** option based on the type of account your have with your ISP. If you need to enter login information every time you connect to the Internet, select **Yes**. Otherwise, select **No**.

   If your connection is PPTP, PPPoE or BigPond Cable, then you need to login. Choose Yes and enter:

   – **Login.** This is often the name that you use in your e-mail address (for example, if your main mail account is jdoe@aol.com, enter jdoe).

   > → **Note:** Some ISPs (for example, Earthlink) require that you use your full e-mail address when you log in.
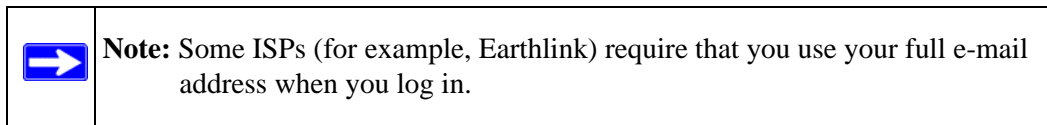
   – **Password**. Enter the password you use to log in to your ISP.

- Enter your **ISP Type** information:

   Select either the **PPPoE** or **PPPoA** radio box**.** (If you have installed log in software such as WinPoET or Enternet, then your connection type is PPPoE.) Select this option and configure the following fields:

   - **Account Name**: Valid account name for the PPPoE connection

   - **Domain Name**: Name of your ISPs domain or your domain name if your ISP has assigned one (optional).

   - **Idle Timeout**: Select Keep Connected, to keep the connection always on. To logout after the connection is idle for a period of time, select Idle Time and enter the number of minutes to wait before disconnecting, in the Timeout field.

2. Enter your **Internet (IP) Address**.

   – Select the **Get dynamically from ISP** radio box if you have not been assigned any static IP address. The ISP will automatically assign an IP address to the router using DHCP network protocol.

   – If your ISP has assigned a fixed (static) IP address, select **Use Static IP Address** and fill in the following fields:

- **IP Address**: Static IP address assigned to you. This will identify the router to your ISP.

- **IP Subnet Mask**: This is usually provided by the ISP or your network administrator.

- **Gateway IP Address**: IP address of your ISP's gateway. This is usually provided by the ISP or your network administrator.

3. Select your **Domain Name Servers** (DNS). Domain name servers (DNS) convert Internet names such as www.google.com, www.netgear.com, etc. to Internet addresses called IP addresses.

   – Select the **Get Automatically from ISP** radio box if you have not been assigned a static DNS IP address.

   – If the **Use these DNS Servers** radio box is selected, enter valid DNS server IP addresses in the Primary DNS Server and Secondary DNS Server fields.

4. Click **Apply** to save your settings. Click **Test** to verify that the connection is active.

> → **Note:** At this point in the configuration process, you should now be connected to the Internet through the internal ADSL modem and the DSL connection.

Repeat these steps to connect your secondary configuration, if required.

Manually Configuring your Ethernet Connection

Unless your ISP assigns your configuration automatically via DHCP, you will need the configuration parameters from your ISP. For example, if your router detected a PPPoE or PPPoA service, you must provide a Login sequence in order to obtain an Internet connection from your ISP. If your ISP requires a Static IP address, then you must provide the fixed addresses for Static IP. The types of data you will need are highlighted in Table 2-1 by connection method, and explained in more detail below.

To configure your Ethernet ISP connection:

1. Enter your ISP Login information. Select the **Does Your Internet Connection require a Login?** option based on the type of account your have with your ISP. If you need to enter login information every time you connect to the Internet, select **Yes**. Otherwise, select **No**.

   If your connection is PPTP, PPPoE or BigPond Cable, then you need to login. Choose Yes and enter:

– **Login.** This is often the name that you use in your e-mail address (for example, if your main mail account is jdoe@aol.com, enter jdoe).

> **Note:** Some ISPs (for example, Earthlink) require that you use your full e-mail address when you log in.

– **Password**. Enter the password you use to log in to your ISP.

- Enter your **ISP Type** information:

  – **Austria (PPTP)**: If your ISP is Austria Telecom or any other ISP that uses PPTP to log in, fill in the following fields:

    • **Account Name** (also known as Host Name or System Name): Valid account name for the PPTP connection. This is usually your email "ID" assigned by your ISP, the name before the "@" symbol in your email address. Some ISPs require that you enter your full email address here.

    • **Domain Name:** Domain name or workgroup name assigned by your ISP, or your ISPs domain name (optional).

    • **Idle Timeout:** Select Keep Connected, to Keep the Connection Always On. To logout after the connection is idle for a period of time, select Idle Time and enter the number of minutes to wait before disconnecting in the Timeout field. 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 a connection with the ISP server.

    • **Server IP Address**: IP address of the PPTP server.

  – **Other (PPPoE):** If you have installed log in software such as WinPoET or Enternet, then your connection type is PPPoE. Select this option and configure the following fields:

    • **Account Name**: Valid account name for the PPPoE connection

    • **Domain Name**: Name of your ISPs domain or your domain name if your ISP has assigned one (optional).

    • **Idle Timeout**: Select Keep Connected, to keep the connection always on. To logout after the connection is idle for a period of time, select Idle Time and enter the number of minutes to wait before disconnecting, in the Timeout field.

– **BigPond Cable**: If your ISP is Telstra BigPond Cable, select this option and fill in the Log In Server and Idle Timeout fields. The Log In Server is the IP address of the BigPond Log In Server local to your area. You can find log in server information at this URL: http://www.netgear.com.sg/support/bigpond.asp

2. Enter your **Internet (IP) Address**.

   – Select the **Get dynamically from ISP** radio box if you have not been assigned any static IP address. The ISP will automatically assign an IP address to the router using DHCP network protocol.

   – If your ISP has assigned a fixed (static) IP address, select **Use Static IP Address** and fill in the following fields:

     • **IP Address**: Static IP address assigned to you. This will identify the router to your ISP.

     • **IP Subnet Mask**: This is usually provided by the ISP or your network administrator.

     • **Gateway IP Address**: IP address of your ISP's gateway. This is usually provided by the ISP or your network administrator.

3. Select your **Domain Name Servers** (DNS). Domain name servers (DNS) convert Internet names such as www.google.com, www.netgear.com, etc. to Internet addresses called IP addresses.

   – Select the **Get Automatically from ISP** radio box if you have not been assigned a static DNS IP address.

   – If the **Use these DNS Servers** radio box is selected, enter valid DNS server IP addresses in the Primary DNS Server and Secondary DNS Server fields.

4. Click **Apply** to save your settings. Click **Test** to verify that the connection is active.

> **Note:** At this point in the configuration process, you should now be connected to the Internet through the internal ADSL modem and the DSL connection or the Ethernet or both.

Selecting Advanced Options for your Ethernet or ADSL Connection

Several other Advanced options that can be altered from their default values affect the MTU size, Ethernet port speed and the MAC (Media Access Control) address of your computer or router. These Advanced Options are available for both ADSL and Ethernet connections.

- **MTU Size.** The normal MTU value for most networks is 1500 Bytes, or 1492 for PPPoE connections. For some ISPs, you may need to reduce the MTU size. However, this is rarely required and should not be attempted unless you are sure it is necessary for your ISP connection.

- **Port Speed (Ethernet only)**. Usually, your router can automatically determine the connection speed of the 10/100 port. If you cannot establish an Internet connection and the Internet LED blinks continuously, manually select the port speed.

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

- **Router MAC Address**. Each computer or router on your network has a unique 32-bit local Ethernet address, known as the Media Access Control (MAC) address. In most cases the default Use Default Address will suffice. If your ISP requires MAC authentication, then select either:

  – Use This Computer's MAC address, where the router will use the MAC address of the computer you are now using, or

  – Use This MAC Address, where you manually enter the MAC address that your ISP expects. The format is XX:XX:XX:XX:XX:XX.

If you set up an ADSL connection, in addition to the Advanced ADSL settings, there are some additional specific ADSL settings that also should be configured. These include: Multiplexing Method, VPI and VCI.

To configure your ADSL settings:

1. Click he **ADSL Settings** link at the top of the **ADSL ISP Settings** screen. The **ADSL Settings** screen will display.
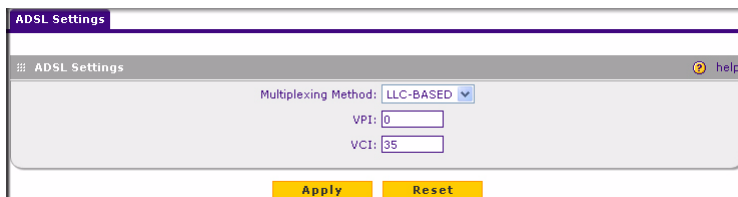

Figure 2-6

2. Configure your ADSL Settings. If you don't know your settings, contact your ISP. These parameters must be submitted to correctly establish a DSL connection on the WAN interface:

   a. Multiplexing Method: Both VC-BASED multiplexing and LLC-BASED multiplexing methods are supported.

Basic Installation and Configuration   2-11

b. VPI (Virtual Path Identifier) value: This is provided by your ISP to identify the ATM network (in conjunction with the VCI value).

c. VCI (Virtual Channel Identifier) value: This is provided by your ISP (in conjunction with the VPI value) to identify the ATM network.

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

To configure your Advanced ADSL ISP Settings:

1. Click the **Advanced** link at the tops of the **ADSL ISP Settings** screen. The **ADSL Advanced Options** screen will display.
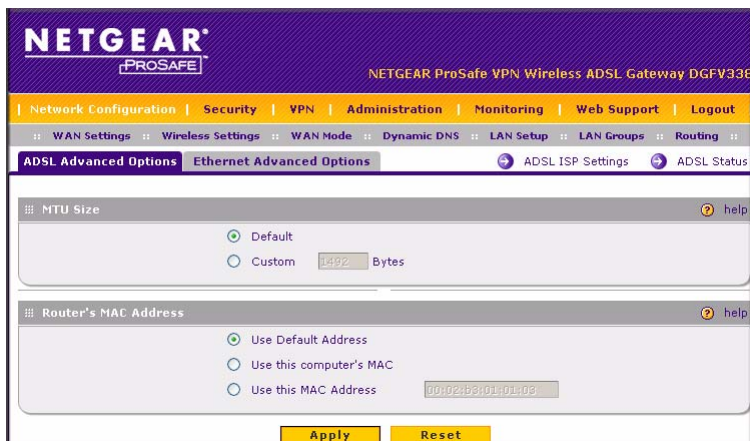

Figure 2-7

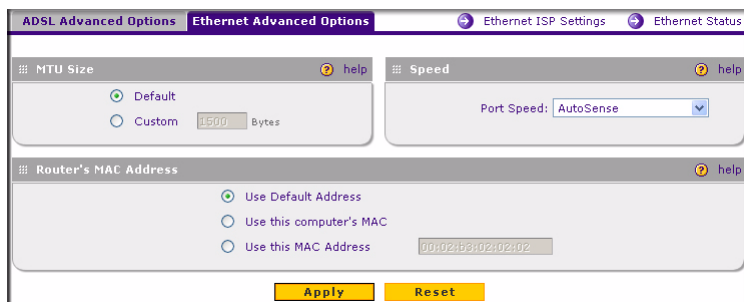**2.** Enter the **MTU Size**. The MTU (Maximum Transmit Unit) is the size of the largest packet that can be sent over the network. The standard MTU value for Ethernet networks is usually 1500 Bytes and for PPPoE connections, it is 1492 Bytes. Unless a change is required by your ISP, it is recommended that the MTU values be left as is.

3. Enter the **Router's MAC Address.** Similar to other Ethernet devices, the router has its own 48-bit local Ethernet address, also referred to as the MAC (Media Access Control) address. The default is set to Use default address.

– If your ISP requires MAC authentication and another MAC address has been previously registered with your ISP, then select either Use this Computer's MAC address to assign the MAC address of the computer through which you are accessing the router.

– Select Use This MAC Address and manually type in the MAC address expected by your ISP.

Basic Installation and Configuration

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

4. Click **Apply** to save the settings. Click **Reset** to revert to the previous settings.

To configure you Ethernet ISP Advanced options:

1. Select the **Advanced** link at the top of the **Ethernet ISP Settings** screen. The4 **Ethernet Advanced Options** screen will display.

Figure 2-8

2. Enter the **MTU Size.** The MTU (Maximum Transmit Unit) is the size of the largest packet that can be sent over the network. The standard MTU value for Ethernet networks is usually 1500 Bytes and for PPPoE connections, it is 1492 Bytes. Unless a change is required by your ISP, it is recommended that the MTU values be left as is.

3. Enter your **Port Speed.** Most new devices with Ethernet ports run at full-duplex, 100Mbps modes. The router can automatically negotiate the speed with the other end of the Ethernet connection. However, if the Internet LED blinks continuously, you may need to set the port speed manually. This could occur with some older broadband modems. If the Ethernet port of the broadband modem supports 100BaseT, select 100BaseT; otherwise, select 10BaseT. Use the half-duplex settings if full-duplex modes do not function properly.

4. Enter the **Router's MAC Address.** The router has its own 48-bit local Ethernet address, also referred to as the MAC (Media Access Control) address. The default is set to Use default address. If your ISP requires MAC authentication and another MAC address has been previously registered with your ISP, then select either Use this Computer's MAC address to assign the MAC address of the computer through which you are accessing the router, or select Use This MAC Address and manually type in the MAC address expected by your ISP. The format for the MAC address is XX:XX:XX:XX:XX:XX where X is a number from 0 to 9 (inclusive) or an alphabetical letter between A and F (inclusive).

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

> → **Note:** You can also set up the traffic meter for the Ethernet ISP, if desired, at this time. See "Programming the Traffic Meter" on page 2-20.

Configuring the WAN Mode

The WAN ports of the ProSafe Wireless ADSL Modem VPN Firewall Router can be configured for NAT or Classical Routing. You must select one of them—NAT being the most common:

- **NAT**. NAT is the technology which allows all PCs on your LAN to share a single Internet IP address. From the Internet, there is only a single device (the Router) 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 Router uses NAT to select the correct PC (on your LAN) to receive any incoming data.

> → **Note:** If you only have a single Internet IP address, you MUST use NAT.

- **Classical Routing**. In this mode, the Router performs Routing, but without NAT. To gain Internet access, each PC on your LAN must have a valid Internet IP address.

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

Depending on the WAN port configuration of the ProSafe DGFV338, you can select one of two options:

- **Auto-Rollover using WAN port**. If you have configured both the ADSL ISP and Ethernet ISP WAN ports of the ProSafe Wireless ADSL Modem VPN Firewall Router, you can select auto-rollover for increased system reliability. In this mode, the selected WAN interface is made primary and the other is the rollover link. As long as the primary link is up, all traffic is sent over the primary link. Once the primary WAN interface goes down, the rollover link is brought up to send the traffic.

- **Use Dedicated WAN port.**

  – **Dedicated ADSL**. If you have configured only the ADSL ISP, then select this interface. In this mode the ADSL interface will always be active and all traffic will be sent over this link; the other link will always be down. No link failure detection will occur.

  – **Dedicated Ethernet.** If this is your only ISP configuration, then select Dedicated Ethernet. In this mode the Ethernet interface will always be active and all traffic will be sent over this link; the other link will always be down. No link failure detection will occur.

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

- **DNS lookup using WAN DNS Servers (ISP DNS Servers).** In this case, DNS queries are sent to the DNS server configured on the ADSL and Ethernet ISP pages (see "Configuring Your Internet Connection using Auto Detect" on page 2-4).

- **DNS lookup using this DNS Server (for example, a public DNS Server)**, As an option, you can enter any public DNS server address. DNS queries are sent to this server through the WAN interface being monitored.

- **Ping to this IP address**. Enter a public IP address that will not reject the Ping request or will not consider the traffic abuse. Queries are sent to this server through the WAN interface being monitored.

- **Test Period**. DNS query is sent periodically after every test period. The default test period is 30 seconds.

- **Failover**. The WAN interface is considered down after the configured number of queries have failed to elicit a reply from the configured DNS server or from the Ping destination. The minimum number of failed queries is two. The rollover link is brought up after this, if Auto-Rollover has been selected.

To configure the WAN mode:

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

2. Select either the **NAT** or **Classical Routing** radio button. If you have a single Internet address, you must use NAT.
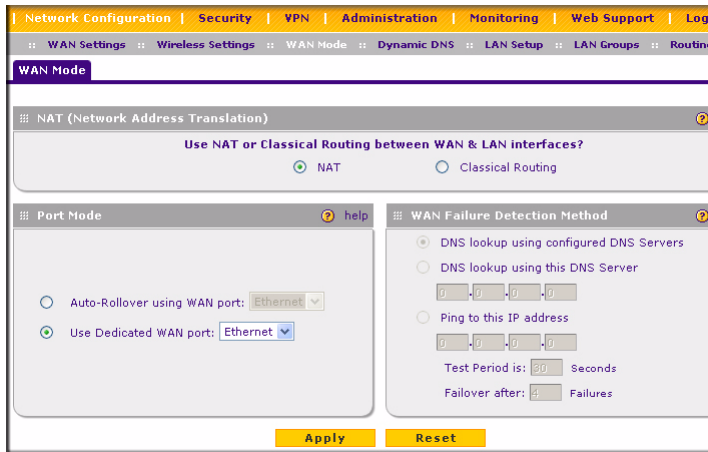
Figure 2-9

3. Select your WAN port configuration:

   • Select the Auto-Rollover radio button and designate the rollover port from the pull-down menu. Auto-Rollover is available only if you have connected and configured both an ADSL ISP and an Ethernet ISP connection.

   • Select the Use Dedicated WAN port radio button and select the dedicated port from the pull-down menu if you have configured and are connected to only one port.

4. Select the WAN Failure Detection Method, if Auto-Rollover is selected:

   • Select DNS lookup using this DNS Server and enter the server address (default), or

   • Select the Ping to this IP address and enter the ping address.

   Once a rollover occurs, when the primary port is restored, the router will automatically switch back to the designated primary port.

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

Configuring Dynamic DNS (If Needed)

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

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

For 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.

The gateway contains a client that can connect to a dynamic DNS service provider. To use this feature, you must select a service provider and obtain an account with them. After you have configured your account information in the gateway, whenever your ISP-assigned IP address changes, your gateway will automatically contact your dynamic DNS service provider, log in to your account, and register your new IP address.

To configure Dynamic DNS:

1. Select **Network Configuration** from the main menu and **Dynamic DNS** from the submenu. The **Dynamic DNS Configuration** screen will display with the default None selected.
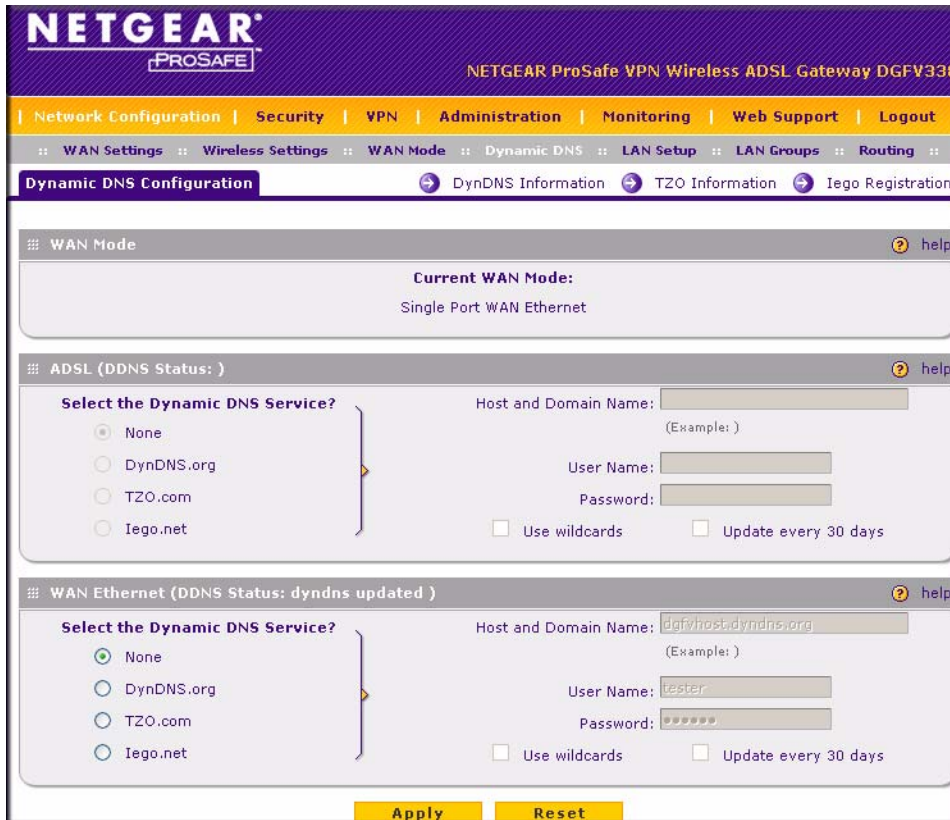

Figure 2-10

Each DNS service provider requires its own parameters (Figure 2-11).

DynDNS Service Screen

Figure 2-11

2. Access the Web site of the Dynamic DNS service provider you have chosen and register for an account (for example, for dyndns.org, go to *http://www.dyndns.org*).

3. Complete entering the Dynamic DNS screen for the service you have chosen:

    a. Select the Use a dynamic DNS service check box of the name of your dynamic DNS Service Provider.

    b. Enter the entire FQDN that your dynamic DNS service provider gave you, (for example, **myName.dyndns.org**).

    c. Enter the User Name and Password (or key) for logging into your dynamic DNS account.

    d. If your dynamic DNS provider allows the use of wild cards in resolving your URL, you may select the Use wild cards 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`

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

Programming the Traffic Meter

The traffic meter is useful when an ISP charges by traffic volume over a given period of time or if you want to look at traffic types over a period of time. The fields are described in Table 2-2 and are the same for both ADSL and Ethernet but are specific to each WAN interface and must be set individually. Figure 2-12 displays the traffic meter screen for the ADSL connection.

Traffic Meter ADSL

Figure 2-12

Table 2-2.   Traffic Meter Parameters

Parameter	Description
Enable Traffic Meter	Check this if you wish to record the volume of Internet traffic passing through the Router's WAN1 or WAN2 port.WAN1 or WAN2 can be selected through the drop down menu, the entire configuration is specific to each wan interface. • No Limit - If this is selected specified restriction will not be applied when traffic limit is reached. • Download only - If this is selected the specified restriction will be applied to the incoming traffic only • Both Directions - If this is selected the specified restriction will be applied to both incoming and outgoing traffic only
Enable Monthly Limit	Use this if your ISP charges for additional traffic. If enabled, enter the monthly volume limit and select the desired behavior when the limit is reached. **Note**: Both incoming and outgoing traffic are included in the limit.
Increase this month's limit	Use this to temporarily increase the Traffic Limit if you have reached the monthly limit, but need to continue accessing the Internet. Check the checkbox and enter the desired increase. (The checkbox will automatically be cleared when saved so the increase is only applied once.)
This month's limit	This displays the limit for the current month.
Restart traffic counter	This determines when the traffic counter restarts. Choose the desired time and day of the month.
Restart Counter Now	Click this button to restart the Traffic Counter immediately.
Send E-mail Report before restarting counter	If checked, an E-mail report will be sent immediately before restarting the counter. You must configure the E-mail screen in order for this function to work (see "Event Logs and Alerts" on page 4-32).
When limit is reached	Select the desired option: • Block all traffic - all access to and from the Internet will be blocked. • Block all traffic except E-mail - Only E-mail traffic will be allowed. All other traffic will be blocked. • If using this option, you may also select the Send E-mail alert option. You must configure the E-mail screen in order for this function to work.
Internet Traffic Statistics	This displays statistics on Internet Traffic via the WAN port. If you have not enabled the Traffic Meter, these statistics are not available.
Traffic by Protocol	Click this button if you want to know more details of the Internet Traffic. The volume of traffic for each protocol will be displayed in a sub-window.Traffic counters are updated in MBytes scale, counter starts only when traffic passed is at least 1MB.

To Program the Traffic Meter (if desired):

1. Select Monitoring from the main menu and Traffic Meter from the submenu. The default ADSL screen shown in Figure 2-12 will display.

2. Fill in the fields from the descriptions in Table 2-2.

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

4. Click **Traffic by Protocol** to view the traffic details for each interface.

   You can also choose to monitor both interfaces since the configuration is specific to each connected WAN interface.

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

6. Select the WAN Ethernet Traffic Meter tab and repeat the process to program the WAN Ethernet Traffic Meter (if applicable).

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

Chapter 3
Wireless Configuration

This chapter describes how to configure the wireless features of your ProSafe DGFV338.

In planning your wireless network, you should consider the level of security required. You should also select the physical placement of your DGFV338 in order to maximize the network speed (see Chapter 2, "Basic Installation and Configuration"). For further information on wireless networking, refer to Appendix B, "Related Documents for a link to resource material on the NETGEAR website.

→ **Note:** Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the wireless firewall. For complete range and performance specifications, please see Appendix A, "Default Settings and Technical Specifications."

Implementing Wireless Security

Be aware that the time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

→ **Note:** Indoors, computers can connect to wireless networks at ranges of 300 feet or more. Such distances allow others outside of your area to access your network.

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The wireless firewall provides highly effective security features which are covered in detail in this chapter.
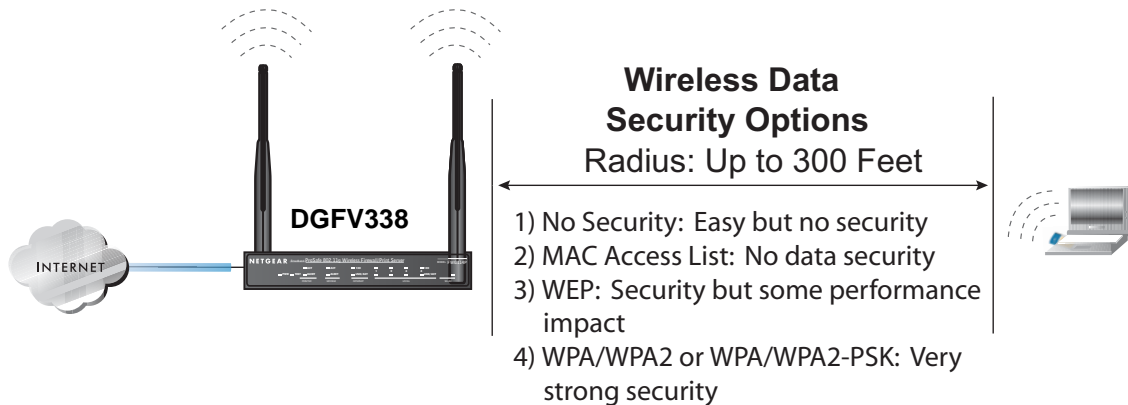

Figure 3-1

There are several ways you can enhance the security of your wireless network:

• **Restrict Access Based on MAC Address.** You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the DGFV338. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.

• **Turn Off the Broadcast of the Wireless Network Name SSID.** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies wireless network "discovery" feature of some products, such as Windows XP, but the data is still exposed.

• **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption will block all but the most determined eavesdropper.

• **WPA/WPA2 with RADIUS or WPA/WPA2-PSK.** Wi-Fi Protected Access (WPA and WPA2) data encryption provides data security. The very strong authentication along with dynamic per frame rekeying of WPA and WPA2 make it virtually impossible to compromise. Because this is a new standard, wireless device driver and software availability may be limited.

Understanding Wireless Settings

Before configuring your wireless settings, you may want to review the Wireless Settings choices to determine what type of security is required for your wireless LAN network and to gather any security information that may be required. A description of the various types of security available on the wireless firewall, as well as a description of the other wireless settings you will be prompted to make follows.

The Wireless Settings menu is divided into two basic sections: (1) Wireless Networks and Wireless Access Point which deals with setting up the proper stations, channels, and regions for your wireless device; as well as setting up the appropriate broadcast method, and (2) Wireless Security Type which deals with setting up the security on each of your LANs.

Figure 3-2

Wireless LANs

Configuring the Wireless settings for your LAN consists of the following categories:

- **Wireless Network.** Wireless Network Name (SSID). The SSID is also known as the wireless network name. Enter a value of up to 32 alphanumeric characters. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device you want to participate in the 802.11b/g wireless network will need to use this SSID for that network. The DGFV338 default SSID is: **NETGEAR**.

- **Country/Region.** Lists the various regions where the DGFV338 can be used. It may not be legal to operate the wireless features of the wireless firewall in a region other than the one specified for your area.

> → **Note:** If your country or region is not listed, please check with your local government agency or check the NETGEAR website for more information on which channels to use.

- **Operating Mode**. The various options are**:**

  - g & b – Both 802.11g and 802.11b wireless stations can be used.

    The default is "g & b" which allows both 802.11g and 802.11b wireless stations to access this device. The 802.11b and 802.11g wireless networking protocols are configured in exactly the same fashion. The DGFV338 will automatically adjust to the 802.11g or 802.11b protocol the device requires without compromising the speed of the other devices.

  - g only – Only 802.11g wireless stations can be used (data rate 54 Mbit/sec).

  - b only – All 802.11b wireless stations can be used (11 Mbit/sec). 802.11g wireless stations can still be used if they can operate in 802.11b mode.

- **Operating Channel.** The default is Auto. This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby access point.

- **Wireless Access Point.**

  - Enable **Wireless Access Point.** This checkbox should be enabled to turn on the wireless radio. (The default is disabled.)

  - Enable A**llow Broadcast of Name**. The default setting is to enable SSID broadcast. If you disable broadcast of the SSID, only devices that have the correct SSID can connect. Disabling SSID broadcast somewhat hampers the wireless network "discovery" feature of some products.

- **Wireless Security Type.** A number of security options are available to use on your Wireless Network:

  – **None.** No data encryption is used.

  – **WEP**. Enables WEP (Wired Equivalent Privacy) data encryption (64-, or 128-, or 152-bit) and requires at least one shared key and a WEP passphrase. When selecting WEP, you can also select:

    • **Open System**. No data encryption is used.

    • **Shared Key**. Enables WEP data encryption (64-, 128-, or 152-bit) and requires at least one shared key and a WEP passphrase.

  – **WPA with PSK** (Wi-Fi Protected Access Pre-Shared Key). WPA-PSK can use TKIP or AES standard encryption.

  – **WPA2 with PSK**. WPA2 is a later version of WPA. Only select this if all clients support WPA2. If selected, you must use AES encryption, and enter the WPA passphrase (Network key).

  – **WPA-PSK and WPA2-PSK**. This selection allows clients to use either WPA (with AES encryption) or WPA2 (with TKIP encryption). If selected, encryption must be TKIP + AES.

  – **WPA with Radius**. This version of WPA requires the use of a Radius server for authentication. Each user (Wireless Client) must have a "user" login on the Radius Server— normally done via a digital certificate. Also, this device must have a "client" login on the Radius server. Data transmissions are encrypted using a key which is automatically generated.

  – **WPA2 with RADIUS**. WPA2 is a later version of WPA. Only select this if all clients support WPA2. If selected, you must use AES encryption, and configure the RADIUS Server Settings. Each user (Wireless Client) must have a "user" login on the Radius Server—normally done via a digital certificate. Also, this device must have a "client" login on the RADIUS server. Data transmissions are encrypted using a key which is automatically generated.

  – **WPA and WPA2 with RADIUS**. This selection allows clients to use either WPA (with AES encryption) or WPA2 (with TKIP encryption). If selected, encryption must be TKIP+AES. You must also configure the RADIUS Server Settings.

> **Note:** Not all wireless adapters support WPA and WPA2. Client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA and WPA2. However, the wireless adapter hardware *and* driver must also support WPA and WPA2. Consult the product document for your wireless adapter and WPA and WPA2 client software for instructions on configuring WPA and WPA2 settings.

Access Control List

The Access Control List enables the restriction of wireless PCs by their MAC addresses. Click the **Setup Access List** link at the top of the Wireless Settings screen to configure your trusted wireless stations.

- **Available Wireless Stations**. The Available Wireless Stations list displays any available wireless PCs and their MAC addresses.

  If the wireless PC appears in the **Available Wireless Cards** list, you can click on the radio button of that PC to capture its MAC address. If your wireless PC is not displayed, make sure that the PC is configured correctly.

- **Trusted Wireless Stations**. Lets you restrict wireless connections according to a list of Trusted Wireless Stations based on the PC MAC addresses. When the Trusted PCs Only radio button is selected, the DGFV338 checks the MAC address of the wireless station and only allows connections to PCs identified on the trusted PCs list.

- To restrict access based on MAC addresses, the Set up Access List radio button must be selected and the MAC Access Control List must be updated to include a listed of restricted PCs based on MAC address**.**

- **Add New Stations Manually**. If no wireless PCs appears in the Available Wireless Cards list, you can manually enter the Device Name and MAC address of the authorized wireless PC. The MAC address is a 12-character key that can usually be found on the bottom of the wireless device.

Wireless Advanced Options

⚠️ **Warning:** The ProSafe DGFV338 is already configured with the optimum settings. Do not alter these settings unless directed by NETGEAR support. Incorrect settings may disable the wireless firewall unexpectedly.

Advanced Wireless Router Settings

The **Wireless Advanced Options** settings are intended for administrator use—and should be used with caution and only as directed by NETGEAR. The Advanced Settings menu controls the following:

• **RTS Threshold** (Default: 2346). The Request to Send Threshold is the packet size that determines if the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) mechanism or the CSMA/CA mechanism should be used for packet transmission. With the CSMA/CD transmission mechanism, the transmitting station sends out the actual packet as soon as it has waited for the silence period. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data.

• **Fragmentation Length** (Default: 2346). This is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value.

• **Beacon Interval** (Default: 100). The Beacon Interval specifies the interval time (between 20ms and 1000ms) for each beacon transmission.

• **DTIM** (Default: 1). The DTIM (Delivery Traffic Indication Message) specifies the data beacon rate between 1 and 255.

• **Preamble Type** (Default: Auto). A long transmit preamble may provide a more reliable connection or a slightly longer range. A short transmit preamble gives better performance. Auto will automatically handle both long and short preambles.

• **SuperG Mode**. If enabled, the Wireless Router will enable data compression, packet bursting and large frame support. This feature is available only for SuperG compatible wireless devices.

– If you **Enable 108Mbps Features,** the throughput of the 802.11g connection will be doubled (typically 54 Mbps) to 108 Mbps and the wireless gateway will be SuperG enabled. SuperG can be used only on Channel 6.

–   If you **Enable eXtended Range (XR) Feature,** significantly longer range connections than basic 802.11 are maintained through dense barriers (walls, floors, etc.). Faint connections will maintain connectivity due to improved error correction and lowered noise vulnerability.

WEP and WPA/WPA2 Wireless Security Check List Form

For a new wireless network, print or copy this form and fill in the configuration parameters. For an existing wireless network, the person who set up or is responsible for the network will be able to provide this information. Be sure to set the Regulatory Domain correctly as the first step.

•   **SSID.** The Service Set Identification (SSID) identifies the wireless local area network. **NETGEAR** is the default DGFV338 SSID. However, you may customize it by using up to 32 alphanumeric characters. Write your customized SSID on the line below.

_____

Note: All wireless nodes in the same network must be configured with the same SSID:

•   **Authentication.** Choose "Shared Key" or above for more security. Circle one:

Open System, Shared Key, Legacy 802.1X, WPA with Radius, WPA2 with Radius, WPA and WPA2 with Radius, WPA-PSK, WPA2-PSK, or WPA-PSK and WPA2-PSK with Radius.

Note: If you selected any of the secure settings—Shared Key or above—the other devices in the network will not connect unless they are set to same Authentication type and have the other required mandatory fields correctly enabled as described previously.

•   **WEP Encryption Keys.** For all four 802.11b keys, choose the Key Size. Circle one: 64, 128, or 152 bits

Key 1: _____

Key 2: _____

Key 3: _____

Key 4: _____

•   **WPA-PSK or WPA2-PSK (Pre-Shared Key)**

Record the WPA-PSK or WPA2-PSK key. Key: _____

•   **WPA or WPA2 RADIUS Settings.** For WPA or WPA2, record the following RADIUS settings:

Server Name/IP Address: Primary _____ Secondary _____

Port: _____

Shared Key: _____

Configuring Your Wireless Settings

First configure your wireless network connection, then configure your Wireless Access Point settings. Lastly, configure your Wireless Security Type that matches your network configuration.

To configure your wireless network and enable your wireless access point:

1. Select Network Configuration from the main menu and Wireless Settings from the submenu. The Wireless Settings screen will display (as shown in Figure 3-3).

2. Enter your Wireless Network Name (SSID). The default SSID is NETGEAR, but NETGEAR strongly recommends that you change your Network Name to a different value. It can be up to 32 alphanumeric characters and is case sensitive.

3. Select the correct Country/Region setting to comply with local regulatory requirements ("Understanding Wireless Settings" on page 3-3 for an explanation of these settings).

4. Select the appropriate Operating Mode for your area and antenna configuration—802.11b/g, b only, or g only.

5. The **Enable Allow Broadcast Name (SSID)** radio box is checked (enabled) by default. When enabled, the SSID will broadcast its name to all Wireless Stations. Stations which have no SSID (or a "null" value) can then adopt the correct SSID for connections to this Access Point.

6. Check the **Enable Wireless Access Point** radio button to turn on the wireless radio.
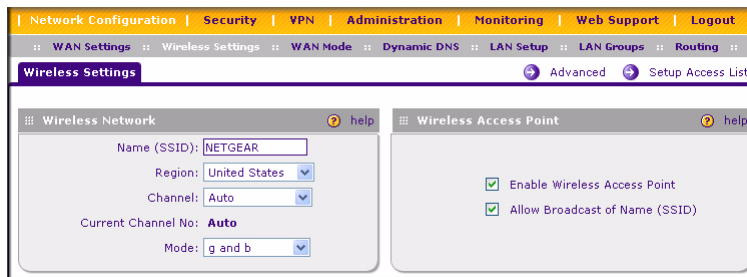
Figure 3-3

To configure the Wireless security settings on your ProSafe DGFV338:

1. Select the Wireless Security Type option you wish to use for your Wireless Network. The options are described in "Wireless LANs" on page 3-4.

   • **None**: No data encryption is used.

   • **WEP**. This enables WEP and requires at least one shared key (see "Configuring WEP" on page 3-10).

   • **WPA-PSK.** Uses standard WPA-PSK encryption (see "Configuring WPA-PSK" on page 3-12).

   • **WPA2-PSK**. WPA2 is a later version that uses only AES encryption (see "Configuring WPA2-PSK" on page 3-13.)

   • **WPA-PSK and WPA2-PSK**. Allows clients to use either WPA (with TKIP encryption) or WPA2 (with AES encryption) (see "Configuring WPA-PSK and WPA2-PSK" on page 3-14.)

   • **WPA with RADIUS**. This version of WPA requires the use of a RADIUS server for authentication.(see "Configuring WPA-PSK" on page 3-12.).

   • **WPA2 with RADIUS.** This is later version of WPA and requires the use of a RADIUS server (see "Configuring WPA2 with RADIUS" on page 3-16.)

   • **WPA and WPA2 with RADIUS**. This version of WPA and WPA2 allows the use of either AES or TKIP encryption with the RADIUS server (see "Configuring WPA and WPA2 with RADIUS" on page 3-17.).

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

Configuring WEP

To configure WEP data encryption:

1. Select Network Authentication from the main menu and Wireless Settings from the submenu.

2. In the Wireless Security Type section, select the WEP radio box.

3. From the WEP section, define the WEP security characteristics:

   • Select Authentication type from the drop-down menu:

     – Automatic (default). Allows either Open System or Shared Key

     – Open System

     – Shared Key

• Select which encryption strength you want to use from the Encryption drop-down menu (64 bits, 128 bits, or 152 bits).

> → **Note:** 64-bit and 128-bit are the standard encryption strength options. 152-bit key length is a proprietary mode that will only work with other wireless devices that support this mode.

• Enter a WEP Passphrase (a word or group of printable characters) in the Passphrase box and click Generate Keys to automatically configure the WEP Key(s).

  You can manually or automatically program the four data encryption keys. These values must be identical on all PCs and devices in your network. Choose either:

  – Automatic – Click **Generate**. The four key boxes will be automatically populated with key values.

  – Manual – Enter the number of hexadecimal digits appropriate to the encryption strength: 10 digits for 64-bit and 26 digits for 128-bit (any combination of 0-9, a-f, or A-F).

Figure 3-4

• Select the key to be used as the default key by checking the radio box. (Data transmissions are always encrypted using the default key.)

  See the document "Wireless Communications" for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard. A link to this document on the NETGEAR website is in Appendix B, "Related Documents."

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

> **Note:** If you use a wireless computer to configure WEP settings, you will be disconnected when you click Apply. Reconfigure your wireless adapter to match the new settings or access the wireless firewall from a wired computer to make any further changes.
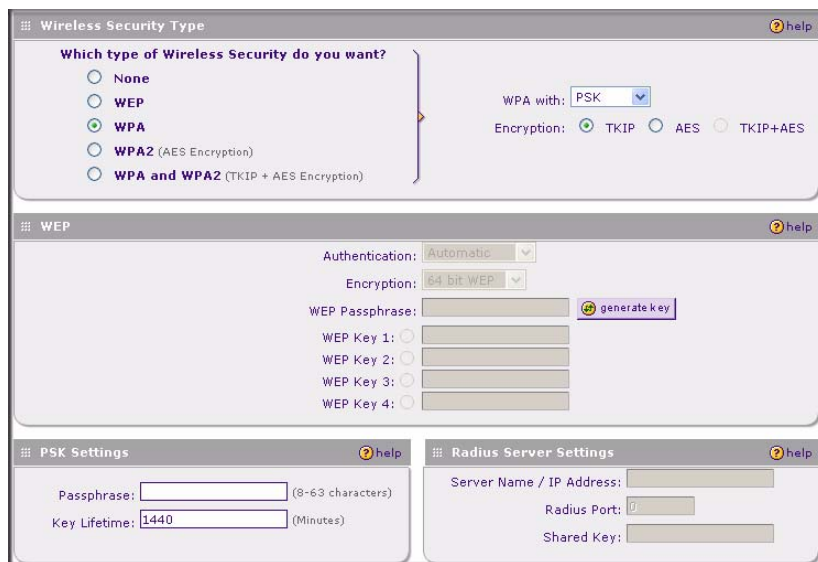
Configuring WPA-PSK

Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 or above include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

To configure WPA-PSK:

1. From the **Wireless Security Type** section, select **WPA**. **WPA with PSK** will be selected by default.

2. Select the Data Encryption mode: AES or TKIP (TKIP is the default).

3. Enter the Passphrase (Network Key). The 256-bit key used for encryption is generated from the Passphrase.

4. Enter the Key Lifetime (in minutes). This determines how often the encryption key is changed. (Shorter periods give better security, but adversely affect performance.)
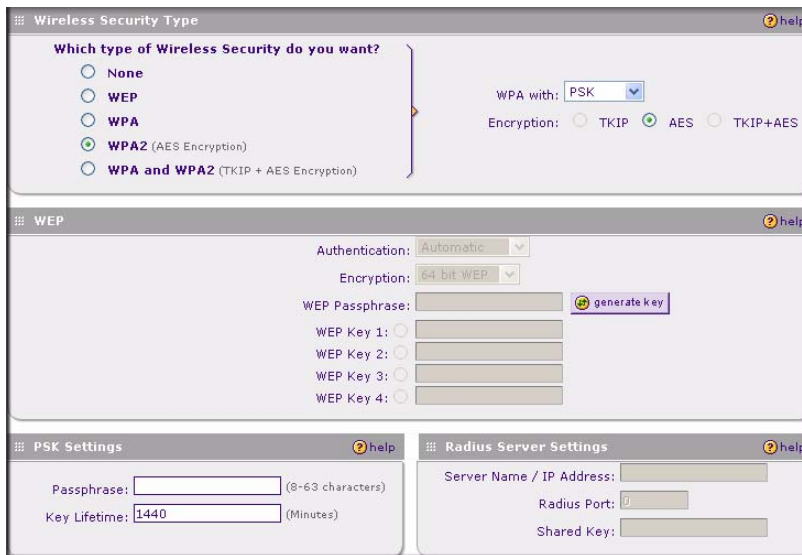
5. Click **Apply** to save your settings.

Figure 3-5

Configuring WPA2-PSK

Not all wireless adapters support WPA2. Furthermore, client software is required on the client. Make sure your client card supports WPA2. Consult the product document for your wireless adapter and WPA2 client software for instructions on configuring WPA2 settings.

To configure WPA2-PSK:

1. From the **Wireless Security Type** section, select the **WPA2** radio button. By default **WPN with PSK** will be selected and **Encryption** will be set to **AES**.

2. Enter the preshared Passphrase (Network Key).The 256-bit key used for encryption is generated from the Passphrase.

3. Enter the Key Lifetime (in minutes). This determines how often the encryption key is changed. (Shorter periods give better security, but adversely affect performance.)

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

Figure 3-6

Configuring WPA-PSK and WPA2-PSK

Not all wireless adapters support WPA and WPA2. Client software is required on the client:

- Windows XP and Windows 2000 with Service Pack 3 or above do include the client software that supports WPA. The wireless adapter hardware and driver must also support WPA.

- Service Pack 3 does not include the client software that supports WPA2. Make sure your client card supports WPA2. The wireless adapter hardware and driver must also support WPA2.

Consult the product documentation for your wireless adapter; WPA client software for instructions on configuring WPA settings; and WPA2 client software for instructions on configuring WPA2 settings.

To configure **WPA-PSK** and **WPA2-PSK**:

1. From the **Wireless Security Type** section, select **WPA and WPA2**. By default, **WPA with PSK** is selected and **Encryption** will be set to **TKIP+AES**.

2. Enter the Passphrase (Network Key).The 256-bit key used for encryption is generated from the Passphrase.

3. Enter the Key Lifetime (in minutes). This determines how often the encryption key is changed. (Shorter periods give better security, but adversely affect performance.)

Figure 3-7

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

Configuring WPA with RADIUS

Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 or above do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

To configure WPA with RADIUS:

1. Choose the **WPA** radio box.

2. Then select **RADIUS** from the **WPA with** pull down menu. Data Encryption will be set to **TKIP** by default.

3. Enter the following in the **RADIUS Server Settings** section:

   a. Enter the RADIUS Server Name or IP Address. This is the name or IP address of the primary RADIUS Server on your LAN (required field).

   b. Enter the RADIUS port number for connecting to the RADIUS Server.

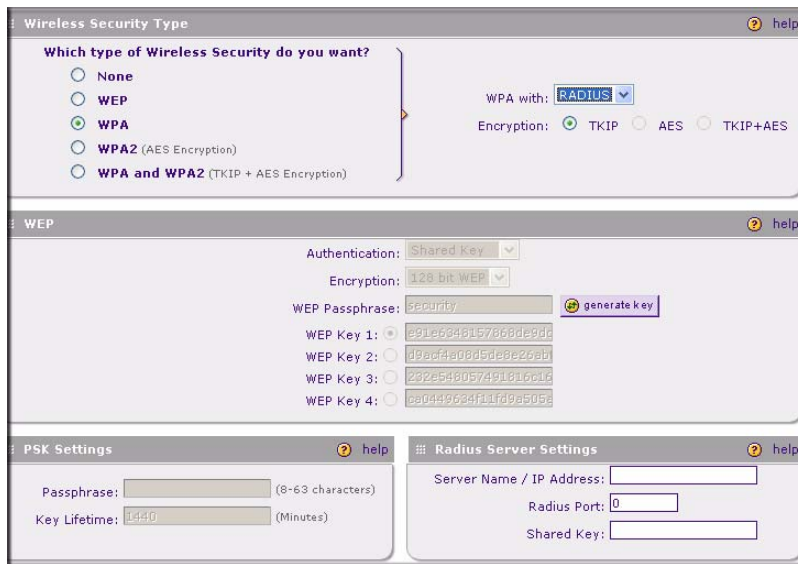   **c.** Enter the Shared Key. The value must match the value used on the RADIUS Server.

Figure 3-8

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

Configuring WPA2 with RADIUS

Not all wireless adapters support WPA2. Furthermore, client software is required on the client. Make sure your client card supports WPA2. Consult the product document for your wireless adapter and WPA2 client software for instructions on configuring WPA2 settings.

To configure WPA2 with RADIUS:

1. In the **Wireless Security Type** section, select the WPA2 radio box.

2. Then select **RADIUS** from the **WPA with** pull down menu. By default, Data Encryption will be set to **AES.**

3. Enter the following RADIUS Server Settings:

    a. Enter the RADIUS Server Name or IP Address. This is the name or IP address of the primary RADIUS Server on your LAN (required field).

    b. Enter the RADIUS port number for connecting to the RADIUS Server.

    c. Enter the Shared Key. The value must match the value used on the RADIUS Server.

4. Click **Apply** to save your settings.
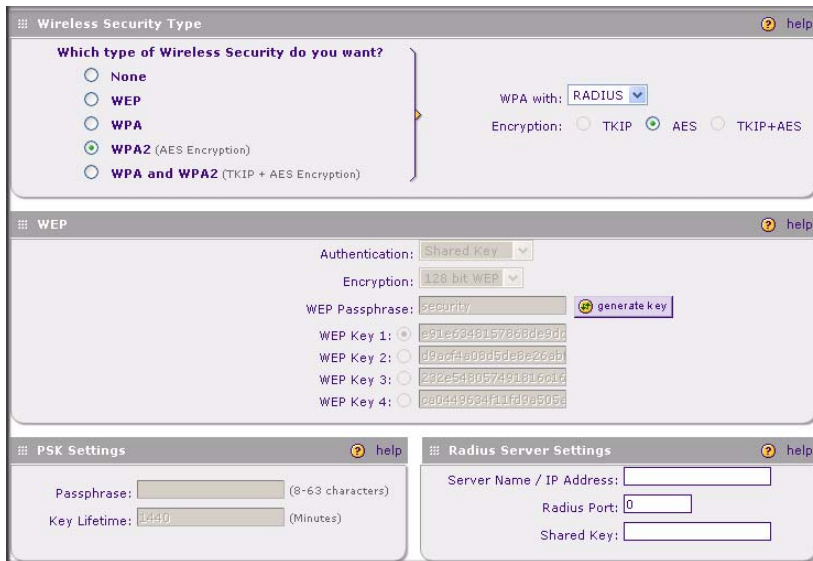
Figure 3-9

Configuring WPA and WPA2 with RADIUS

Not all wireless adapters support WPA and WPA2. Client software is required on the client:

- Windows XP and Windows 2000 with Service Pack 3, or above, do include the client software that supports WPA. The wireless adapter hardware and driver must also support WPA.

- Service Pack 3 does not include the client software that supports WPA2. Make sure your client card supports WPA2. The wireless adapter hardware and driver must also support WPA2.

Consult the product documentation for your wireless adapter; WPA client software for instructions on configuring WPA settings; and WPA2 client software for instructions on configuring WPA2 settings.

To configure WPA and WPA2 with RADIUS:

1. In the **Wireless Security Type** section, select the WPA and WPA2 radio box.

2. Then select **RADIUS** from the **WPA with** pull down menu. By default, Data Encryption will be set to **TKIP+AES.**

3. Enter the following RADIUS Server Settings:

   a. Enter the RADIUS Server Name or IP Address. This is the name or IP address of the primary RADIUS Server on your LAN (required field).

  b. Enter the RADIUS port number for connecting to the RADIUS Server.

  c. Enter the Shared Key. The value must match the value used on the RADIUS Server.

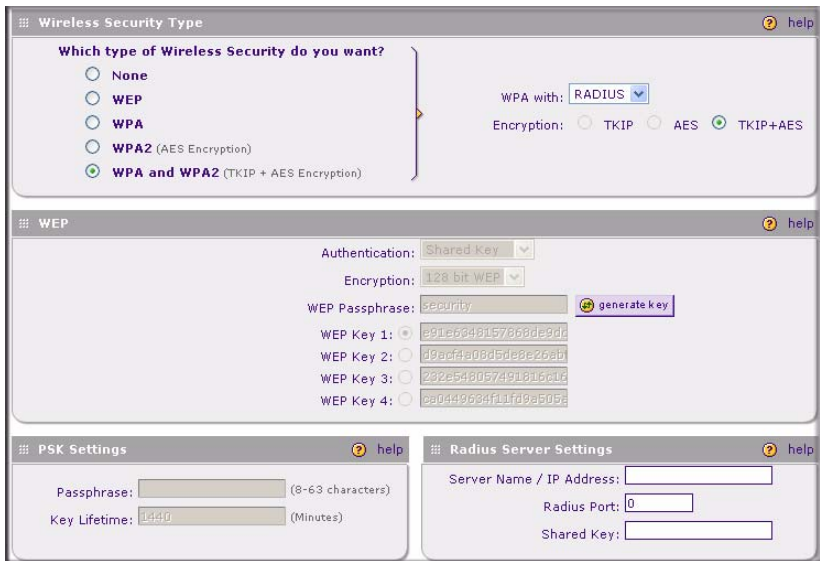**4.** Click **Apply** to save your settings.

Figure 3-10

Restricting Wireless Access by MAC Address

The **Setup Access List** link at the top of the **Wireless Settings** screen lets you set up an Access Control List that can block the network access privilege of any specified stations through the ProSafe DGFV338. When you enable access control, the ProSafe DGFV338 only accepts connections from wireless PCs on the selected access control list. This provides an additional layer of security. (The default is disabled.)

→ | **Note:** If configuring the DGFV338 from a wireless computer whose MAC address is not in the Trusted Wireless Stations list, if you enable Turn Access Control, you will lose your wireless connection when you click Apply. You must then access the wireless firewall from a wired computer or from a wireless computer which is on the Trusted Wireless Stations list to make any further changes.

To restrict access based on MAC addresses:

1. Log in to the DGFV338 using the default address of **http://192.168.1.1,** user name **admin** and default password **password**, or whatever LAN address and password you have set up.

2. Select **Network Configuration** from the main menu and **Wireless Settings** from the submenu. Then click the **Setup Access List** link at the top right of the screen. The **Access Control List** screen will display.
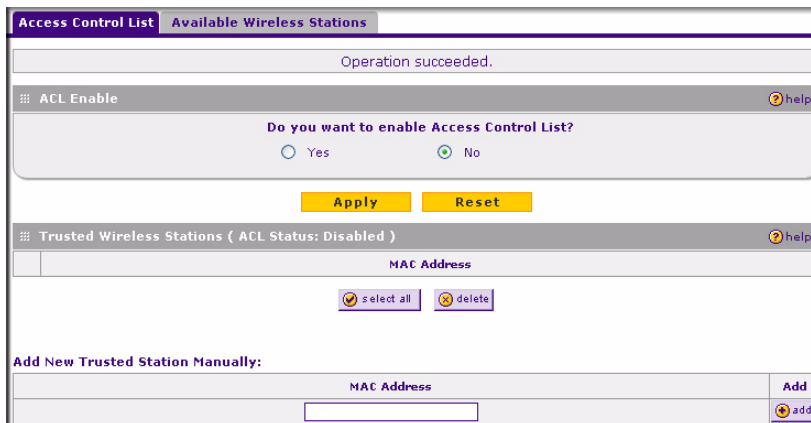
Figure 3-11

3. For **Do you want to enable Access Control List?,** check the **Yes** radio button and then click **Apply.**

4. The **Trusted Wireless Stations** table displays currently configured MAC addresses of wireless devices given permission to connect to this access point. If you have not entered any wireless stations this list will be empty. Delete an existing entry by selecting it and then click **Delete**.

5. You can add a **New Trusted Station Manually** by entering the MAC address of the client. Click **Add** and the new address will be entered in the Trusted Wireless Stations list.

---

6. Select the **Available Wireless Stations** tab to populate the **Available Wireless Stations** list with the MAC addresses of wireless stations found within range of this wireless gateway.

7. Click the **Add to Trusted List** icon adjacent to the MAC address for each wireless device you want to add to the **Trusted Wireless Stations** list. Once added, the wireless device can establish a connection with this wireless gateway. Now, only devices on this list will be allowed to wirelessly connect to the DGFV338.

> **Note:** The ACL "Yes" radio button must be enabled to activate the Trusted Wireless Stations feature.

Chapter 4
Security and Firewall Protection

This chapter describes how to use the Security features of the ProSafe Wireless ADSL Modem VPN Firewall Router to protect your network. These features can be found by selecting **Security** from the main menu of the browser interface.

Firewall Protection and Content Filtering Overview

The ProSafe Wireless ADSL Modem VPN Firewall Router provides Web Content filtering—by Domain name (Web sites) and by Keyword Blocking. Browsing activity reporting and instant alerts via e-mail provide reports on Content Filtering activities. Parents and network administrators can establish restricted access policies based on time-of-day, specific Web Components, Web sites and Web address keywords. You can also block Internet access by applications and services, such as chat or games.

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

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

Using Rules to Block or Allow Specific Kinds of Traffic

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

About Service Based Rules

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

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

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

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

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

A firewall has two default rules, one for inbound traffic and one for outbound traffic. The default rules of the DGFV338 are:

* **Default Inbound Policy**. Block all inbound traffic to the LAN from the Internet (WAN), except responses to requests from the LAN. To allow computers from the WAN to access services on the LAN, a firewall rule for each service must be added.

* **Default Outbound Policy**.Allow all traffic from the LAN to pass through to the Internet. Firewall rules can then be applied to block specific types of traffic from going out from the LAN to the WAN.

The Default Outbound Policy is shown in the LAN-WAN Rules table of the Firewall Rules sub-menu (under Security on the main menu) in Figure 4-1:
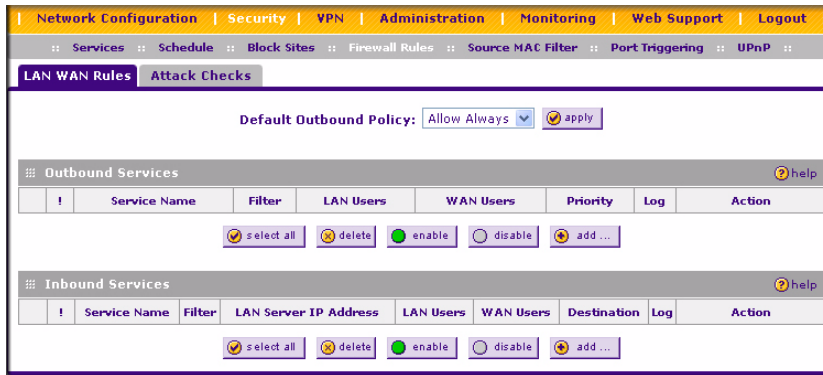
Figure 4-1

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

You can also tailor these rules to your specific needs (see "Security and Administrator Management" on page 4-35).

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

Outbound Rules (Service Blocking)

The DGFV338 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 Services** lists all the existing rules for outgoing traffic. A rule is defined by the following fields:

• **! (Status)**: A rule can be disabled if not in use and enabled as needed. A rule is disabled if the status light is grey and it is enabled if the status light is green. Disabling a rule does not delete the configuration, but merely de-activates the rule.

• **Service Name**: This is a unique name assigned to the service. The name usually indicates the type of traffic the rule covers such as ftp, ssh, telnet, ping, etc. Services not already in the list can be added on the **Add LAN WAN Outbound Services** screen.

- **Filter**: Defines an action to be taken on the enabled rule. It can be:

  – **Block Always:** Block selected service at all times.

  – **Enable Always**: Allow selected service to pass through at all times.

  – **Block by schedule, otherwise allow**: Works in conjunction with a schedule defined on the **Schedule** screen. The selected service will be blocked during the schedule interval (Schedule 1, Schedule 2 or Schedule 3) and will be allowed to pass through at other times.

  – **Allow by schedule, otherwise block**: Works in conjunction with a schedule defined on the **Schedule** screen. The selected service will be allowed to pass through during the schedule interval (Schedule 1, Schedule 2, or Schedule 3) and will be blocked at other times.

- **LAN Users**: Specifies whether one or more LAN IP addresses will be affected by the rule. This rule will affect packets for the selected service coming from the defined IP address or range of IP addresses on the LAN side.

  – **Any**: All computers on the LAN are included in the rule.

  – **Single Address**: A single LAN IP address that is affected by the rule.

  – **Address Range**: A range of LAN IP addresses that are affected by the rule.

  – **Group**: Computers that are part of the Group defined in the Network Database will be affected by the rule. (Groups are defined by selecting **Network Configuration** from the main menu, **LAN Groups** from the sub-menu and then clicking the **Edit Group Names** tab.)

- **WAN Users**: Specifies whether one or more WAN IP address will be affected by the rule. This rule will affect packets for the selected service to the defined IP address or range of IP addresses on the WAN side.

  – **Any**: All IP addresses on the WAN will be affected by the rule.

  – **Single Address:** A single WAN IP address will be affected by the rule.

  – **Address Range**: A range of IP addresses on the WAN will be affected by the rule.

- **Priority:** The priority assigned to IP packets of this service. The priorities are defined by "Type of Service (ToS) in the Internet Protocol Suite" standards, RFC 1349. The router marks the Type Of Service (ToS) field as defined below:

  – **Normal-Service**: No special priority given to the traffic. The IP packets for services with this priority are marked with a TOS value of 0.

  – **Minimize-Cost**: Used when data must be transferred over a link that has a lower "cost". The IP packets for services with this priority are marked with a TOS value of 1.

Security and Firewall Protection

- **Maximize-Reliability**: Used when data needs to travel to the destination over a reliable link and with little or no retransmission. The IP packets for services with this priority are marked with a ToS value of 2.

- **Maximize-Throughput**: Used when the volume of data transferred during an interval is important even if the latency over the link is high. The IP packets for services with this priority are marked with a ToS value of 4.

- **Minimize-Delay**: Used when the time required (latency) for the packet to reach the destination must be low. The IP packets for services with this priority are marked with a ToS value of 8.

• **Log**: Specifies whether the packets for this rule should be logged or not. If you select Always, the details for all packets that match this rule will be logged. If you select Never, logging will be disabled and no details logged.

For example, if an outbound rule for a schedule is selected as Block Always, then for every packet that tries to make an outbound connection for that service, a message with the packet's source address and destination address, along with other information will be recorded in the log.

> **Note:** Enabling the **Log** function may generate a significant number of log messages and is recommended that this be used for debugging purposes only.

• **Action**: You can move a rule **up** or **down** in priority or you can edit the rule by selecting the appropriate button.

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

Additional actions that can be taken on the rules listed in the Outbound Services table are:

• **Edit**: Modify the configuration of the selected rule.

• **Select All**: Selects all the rules in the table.

• **Delete**: Deletes the selected policy or policies.

• **Enable**: Enables the selected rule or rules.

• **Disable**: Disables the selected rule or rules.

• **Add**: Add a new rule.

To add a new Outbound Service:

1. Click the **Add** icon under the Outbound Services table. The **Add LAN-WAN Outbound Service** screen will display.
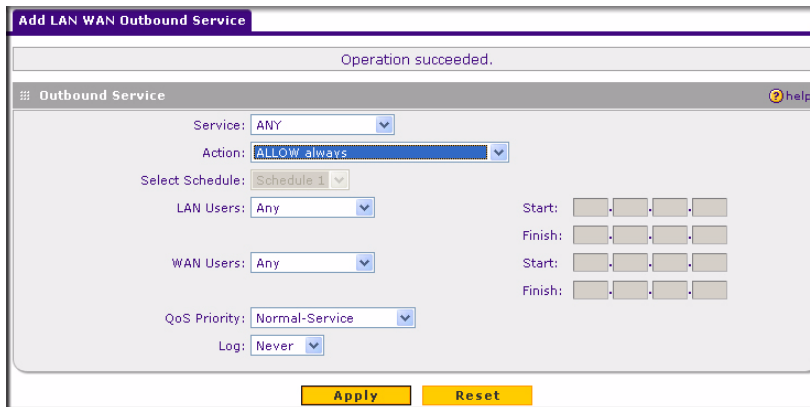

Figure 4-2

2. Fill out the Outbound Service fields for this policy (based on the field explanations above).

3. Click **Apply** to create your policy. The new service policy will display in the **Outbound Services** table.

> **Note:** See "To block keywords or Internet domains:" on page 4-27 for yet another way to block outbound traffic from selected PCs that would otherwise be allowed by the firewall.
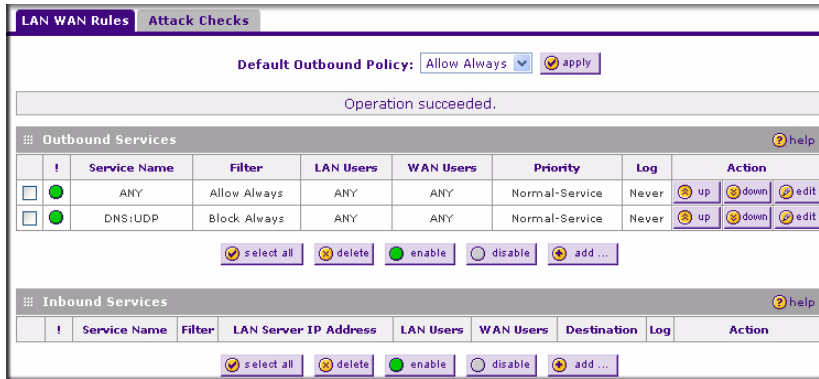
Figure 4-3

Outbound Rule Example: Blocking Instant Messenger

Outbound rules let you prevent users from using applications such as Instant Messenger. If you want to block Instant Messenger usage by employees during working hours, you can create an outbound rule to block that application from any internal IP address to any external address according to the schedule that you have created in the Schedule menu. You can also have the firewall log any attempt to use Instant Messenger during that blocked period.
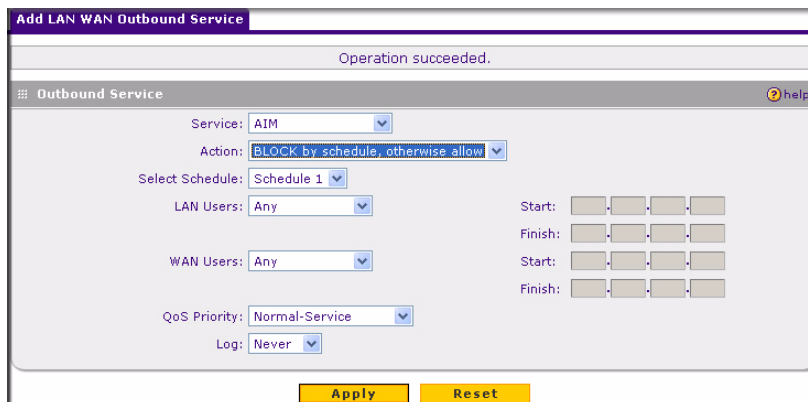
Figure 4-4

Inbound Rules (Port Forwarding)

Because the DGFV338 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.

Security and Firewall Protection   4-7

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. If you enable Translate to a Port Number, the traffic will be forwarded to a specific port based on the destination port number. This is also known as port forwarding.

This following lists all the existing rules for incoming traffic. Remember that allowing inbound services opens holes in your firewall. Only enable those ports that are necessary for your network.

A rule is defined by the following fields:

- **! (Status)**: A rule can be disabled if not in use and enabled as needed. A rule is disabled if the status light is grey and it is enabled if the status light is green. Disabling a rule does not delete the configuration, but merely de-activates the rule.

- **Service Name**: This is a unique name assigned to the service. The name usually indicates the type of traffic the rule covers such as ftp, ssh, telnet, ping, etc. Services not already in the list can be are added on the Services page.

- **Filter**: Defines an action to be taken on the enabled rule. It can be:

  - **Block Always**: Block selected service at all times.

  - **Enable Always**: Allow selected service to pass through at all times.

  - **Block by schedule, otherwise allow**: Works in conjunction with a schedule defined in the Schedule 1/2/3 pages. Selected service will be blocked during the scheduled interval and will be allowed to pass through at other times.

  - **Allow by schedule, otherwise block**: Works in conjunction with a schedule defined in the Schedule 1/2/3 pages. Selected service will be allowed to pass through during the scheduled interval and will be blocked at other times.

- **LAN Server IP Address**: An IP address and port number of a machine on the LAN which is hosting the server. It is displayed in the form: *<IP address:port number>*.

  For example, if a machine with an IP address of 192.168.1.100 on the LAN side is running a telnet server on port 2000, then the table will display 192.168.10.100:2000. If the telnet server is running on the default port (port 23), then the table will display only the IP address.

- **Destination LAN Users**: Specifies whether one or more IP addresses on the LAN will be affected by the rule. This field is only enabled when in routing mode since the LAN is accessible only in this mode.

  - **Any**: All computers on the LAN will be affected by the rule.

  - **Single Address**: A single IP address on the LAN will be affected by the rule.

– **Address Range**: A range of IP addresses on the LAN will be affected by the rule.

– **Group**: Computers that are part of the Group defined in the Network Database will be affected by the rule (groups are defined under the Network Configuration menu, LAN Groups page on the Edit Group Names tab).

WAN Users: Specifies whether all Internet addresses or specific IP addresses are included in the rule.

– **Any**: All IP addresses on the Internet are included in the rule.

– **Single Address**: A single Internet IP address that is affected by the rule.

– **Address Range**: A range of IP addresses that are affected by the rule.

• **Destination**: The WAN IP address that will map to the incoming server. It can either be the address of the ADSL or WAN Ethernet port* or another WAN IP address.

> **Note:** This field is only enabled when under NAT mode since the router needs to map traffic coming from a particular WAN port to a LAN machine.

• **Priority**: The priority assigned to IP packets of this service. The priorities are defined by "Type of Service (TOS) in the Internet Protocol Suite" standards, RFC 1349. The router marks the Type Of Service (TOS) field as defined below:

– **Normal-Service**: No special priority given to the traffic. The IP packets for services with this priority are marked with a TOS value of 0.

– **Minimize-Cost**: Used when data must be transferred over a link that has a lower "cost". The IP packets for services with this priority are marked with a TOS value of 1.

– **Maximize-Reliability**: Used when data needs to travel to the destination over a reliable link and with little or no retransmission. The IP packets for services with this priority are marked with a TOS value of 2.

– **Maximize-Throughput:** Used when the volume of data transferred during an interval is important even if the latency over the link is high. The IP packets for services with this priority are marked with a TOS value of 4.

– **Minimize-Delay**: Used when the time required (latency) for the packet to reach the destination must be low. The IP packets for services with this priority are marked with a TOS value of 8.

• **Log**: Specifies whether the packets for this rule should be logged or not. To log details for all packets that match this rule, select Always. Select Never to disable logging.

For example, if an inbound rule for a schedule is selected as Block Always, then for every packet that tries to make an outbound connection for that service, a message with the packet's source and destination addresses, along with other information will be recorded in the log. Enabling logging may generate a significant volume of log messages and is recommended for debugging purposes only.

> **Note:** See "Setting up Port Triggering" on page 4-28 for yet another way to allow certain types of inbound traffic that would otherwise be blocked by the firewall.

Additional actions that can be taken on the rules are:

- **Edit**: Modify the configuration of the selected rule.

- **Select All**: Selects all the rules in the table.

- **Delete**: Deletes the selected policy or policies.

- **Enable**: Enables the selected rule or rules.

- **Disable**: Disables the selected rule or rules.

- **Add**: Add a new rule.

To create a new inbound service rule:

1. Click **Add** under the **Inbound Services** table. The **Add LAN-WAN Inbound Service** will appear.
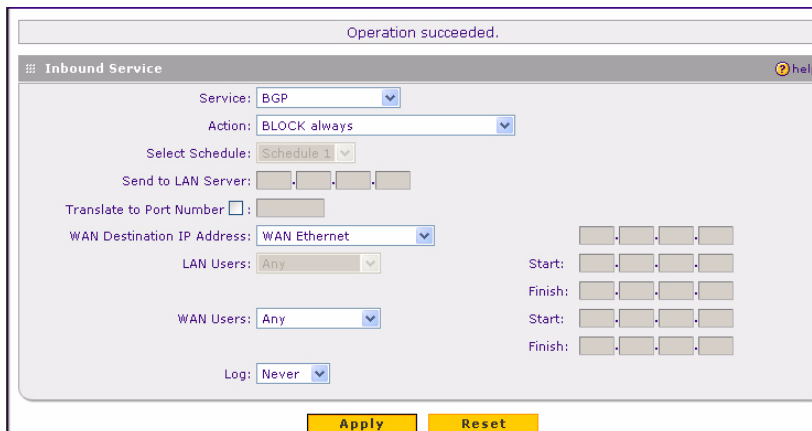
Figure 4-5

2. Complete the Inbound Service screen and click **Apply**. The new rule will be listed in the **Inbound Services** table.
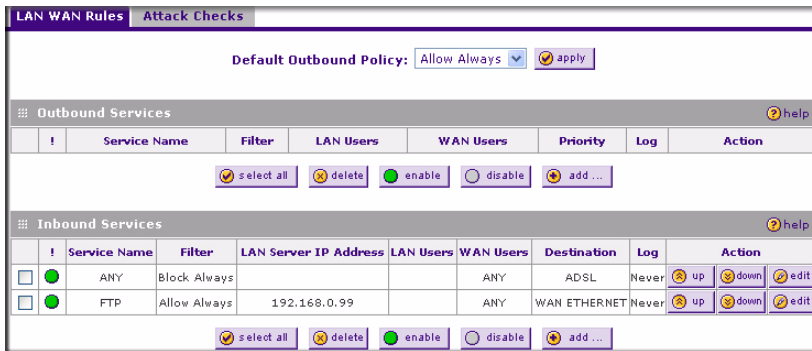
Figure 4-6

To make changes to an existing inbound service rule:

1. Select the radio button next to an row in the table.

2. Click the button for the desired actions:

- **Edit** – to make any changes to the rule definition. The Inbound Service screen will be displayed (see "Inbound Rules (Port Forwarding)" on page 4-7) with the data for the selected rule.

- **Up** or **Down** – to move the selected rule to a new position in the table. .

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

- **Delete** – to delete the selected rule.

3. Enable or disable a rule by selecting the check box in the **Status** column of the row adjacent to the rule you want to modify.

- Click **Enable** to enable the policy. The status circle will turn green.

- Click **Disable** to disable the policy. The status circle will turn gray.

Inbound Rule Example: A Local Public Web Server

If you host a public Web server on your local network, you can define a rule to allow inbound Web (HTTP) requests from any outside IP address to the IP address of your Web server at any time of day. This rule is shown in Figure 4-7:
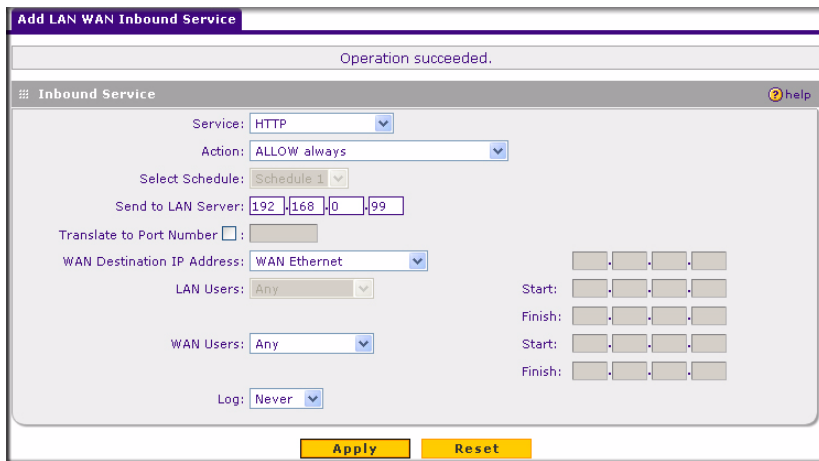
Figure 4-7

Inbound Rule Example: Allowing Videoconference from Restricted Addresses

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

Figure 4-8

Inbound Rule Example: One-to-One NAT Mapping

This application note describes how to configure multi-NAT to support multiple public IP addresses on one WAN interface of a NETGEAR ProSafe Wireless ADSL Modem VPN Firewall Router. By creating an inbound rule, we will configure the firewall to host an additional public IP addresses and associate this address with a Web server on the LAN.

IP Address Requirements – If you arrange with your ISP to have more than one public IP address for your use, you can use the additional public IP addresses to map to servers on your LAN or DMZ. One of these public IP addresses will be used as the primary IP address of the router. This address will be used to provide Internet access to your LAN PCs through NAT. The other addresses are available to map to your servers.

To configure the DGFV338 for additional IP addresses:

1. Go to the LAN-WAN Rules menu.

2. Click **Add** under the Inbound Services table to create an Inbound Services rule. The Add LAN-WAN Inbound Services screen will display.

3. From the Device pull-down menu, (see Figure 4-9), select the HTTP service for a Web server.

Figure 4-9

4. From the Action pull-down menu, select ALLOW always.

5. For Send to LAN Server, enter the local IP address of your Web server PC.

6. From the Public Destination IP Address pull-down menu, select Other Public IP Address and enter one of your public Internet addresses that will be used by clients on the Internet to reach your Web server.

7. Click **Apply**.

Your rule will now appear in the Inbound Services table of the Rules menu (see Figure 4-10). This rule is different from a normal inbound port forwarding rule in that the Destination box contains an IP Address other than your normal WAN IP Address.
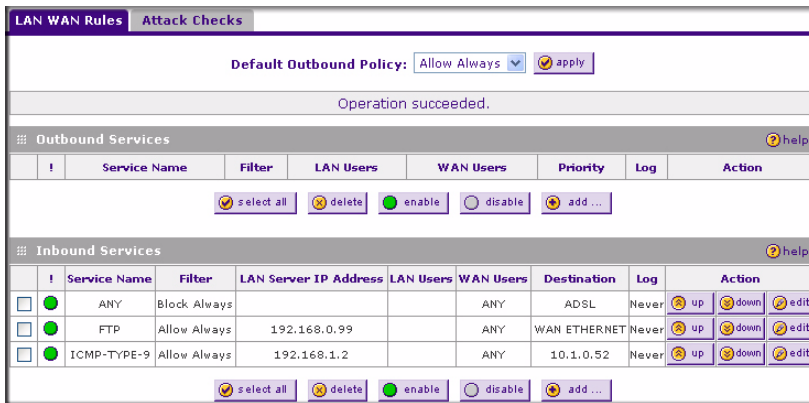
Figure 4-10

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

Inbound Rule Example: 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 haven't defined.

To expose one of the PCs on your LAN as this host (see Figure 4-11):

1. Create an inbound rule that allows all protocols.

2. Place the rule below all other inbound rules by the clicking the **Down** icon adjacent to the rule.

> **Note:** For security, NETGEAR strongly recommends that you avoid creating an exposed host. When a computer is designated as the exposed host, it loses much of the protection of the firewall and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.
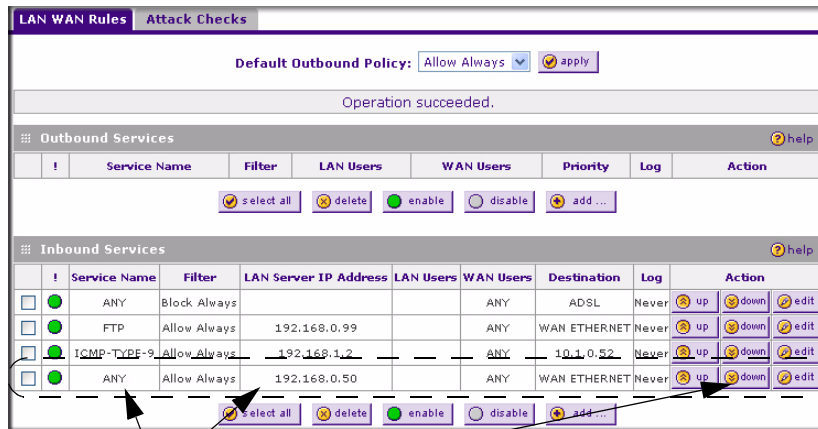
1. Select Any protocol and ALLOW Always (or Allow by Schedule)
2. Place rule below all other inbound rules by clicking the down icon

Figure 4-11

Considerations for Inbound Rules

The DHCP setup and how the PCs access the server's LAN address impact the Inbound Rules.

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

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

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

Order of Precedence for Rules

As you define new rules, they are added to the tables in the Rules menu, as shown in Figure 4-12:

	!	Service Name	Filter	LAN Server IP Address	LAN Users	WAN Users	Destination	Log	Action
☐	🟢	ANY	Block Always			ANY	ADSL	Never	up down edit
☐	🟢	FTP	Allow Always	192.168.0.99		ANY	WAN ETHERNET	Never	up down edit
☐	🟢	ICMP-TYPE-9	Allow Always	192.168.1.2		ANY	10.1.0.52	Never	up down edit
☐	🟢	ANY	Allow Always	192.168.0.50		ANY	WAN ETHERNET	Never	up down edit
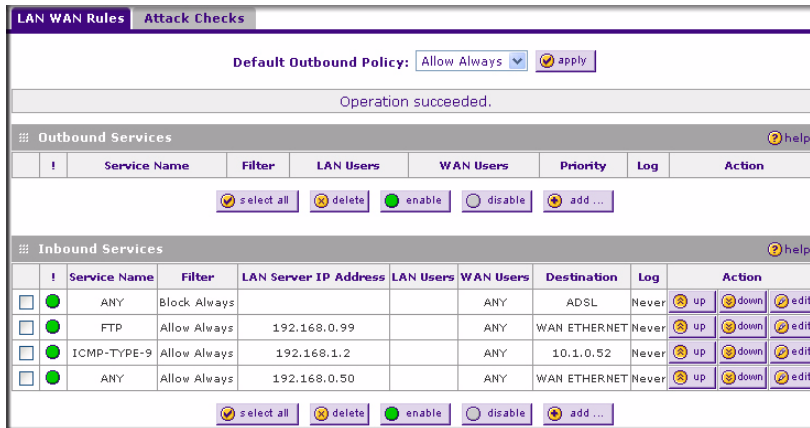
Figure 4-12

For any traffic attempting to pass through the firewall, the packet information is subjected to the rules in the order shown in the LAN WAN Rules Table, beginning at the top and proceeding to the default rules at the bottom. In some cases, the order of precedence of two or more rules may be important in determining the disposition of a packet. The **Up** and **Down** icons adjacent to each rule allows you to relocate a defined rule to a new position in the table.

Customized Services

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

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

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

Although the DGFV338 already holds a list of many service port numbers, you are not limited to these choices. Use the Services menu to add additional services and applications to the list for use in defining firewall rules. The Services menu shows a list of services that you have defined, as shown in Figure 4-13:
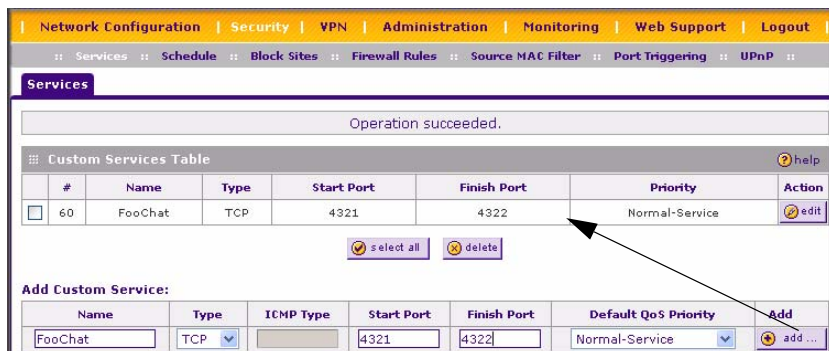

Figure 4-13

To define a new service, first you must determine which port number or range of numbers is used by the application. This information can usually be determined by contacting the publisher of the application or from user groups of newsgroups. When you have the port number information, go the Services menu and click on the Add Custom Service button. The Add Services menu will appear, as shown in Figure 4-13.

To add a service:

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

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

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

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

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

5. Click **Add**.

The new service will now appear in the Custom Services Table.

Quality of Service (QoS) Priorities

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

Outbound Rules Add Screen

QoS Priority

Figure 4-14

The QoS priority definition for a service determines the IP packets queue for outbound traffic passing through the ProSafe DGFV338 for this service. The priorities are defined by "Type of Service (TOS) in the Internet Protocol Suite" standards, RFC 1349. The router marks the Type Of Service (TOS) field as defined below:

* **Normal-Service**: No special priority is 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 though it may have a high link latency. The IP packets for this service 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 fast (low link latency). The IP packets for this service priority are marked with a TOS value of 8.

Attack Checks

This screen allows you to specify if the router should be protected against common attacks from the LAN and WAN networks. The various types of attack checks are defined below. Select the appropriate radio boxes to enable the required security measures.

- **WAN Security Checks**:

  – Respond to Ping On Internet Ports: Responds to an ICMP Echo (ping) packet coming from the Internet or WAN side. (Usually used as a diagnostic tool for connectivity problems. It is recommended that you disable this option to prevent hackers from easily discovering the router via a ping.)

  > **Note:** Under NAT mode (Network Configuration menu, WAN Mode screen), a firewall rule that directs ping requests to a particular computer on the LAN will override this option.

  – Enable Stealth Mode: If Stealth Mode is enabled, the router will not respond to port scans from the WAN or Internet, which makes it less susceptible to discovery and attacks.

  – Block TCP Flood: If this option is enabled, the router will drop all invalid TCP packets and be protected protect from a SYN flood attack.

- **LAN Security Checks:** Block UDP Flood: If this option is enabled, the router will not accept more than 20 simultaneous, active, UDP connections from a single computer on the LAN.

- **VPN Pass through**: IPSec, PPTP or L2TP: Typically, this router is used as a VPN Client or Gateway that connects to other VPN Gateways. When the router is in NAT mode, all packets going to the Remote VPN Gateway are first filtered through NAT and then encrypted, per the VPN policy.

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

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

To enable Attack Checks:

1. Select **Security** from the main menu and **Firewall Rules** from the submenu. Then click the **Attack Checks** tab.

2. Check the radio box for the types of security measures you want to enable. (See the explanation above the various WAN and LAN Security Checks.)

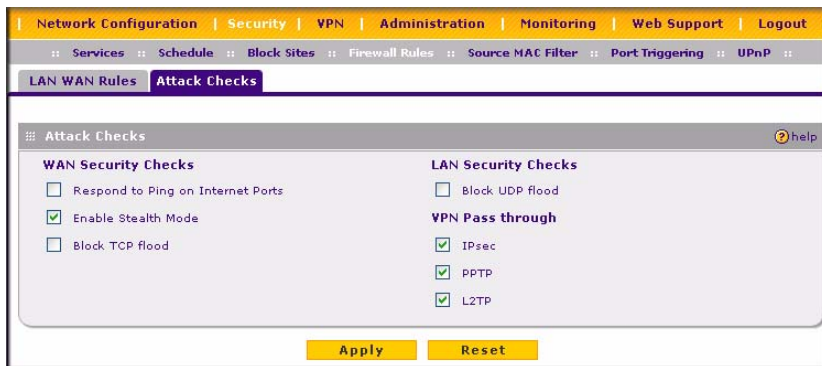3. Click **Apply** to activate the selected security checks.

Figure 4-15

Managing Groups and Hosts

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

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

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

Some advantages of the Network Database are:

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

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

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

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

- Group and Individual Control over PCs:

  - You can assign PCs to Groups and apply restrictions to each Group using the Firewall Rules screen (see "Outbound Rules (Service Blocking)" on page 4-3).

  - You can also select the Groups to be covered by the Block Sites feature (see "Blocking Internet Sites" on page 4-24).

  - If necessary, you can also create Firewall Rules to apply to a single PC (see "To block keywords or Internet domains:" on page 4-27). Because the MAC address is used to identify each PC, users cannot avoid these restrictions by changing their IP address.
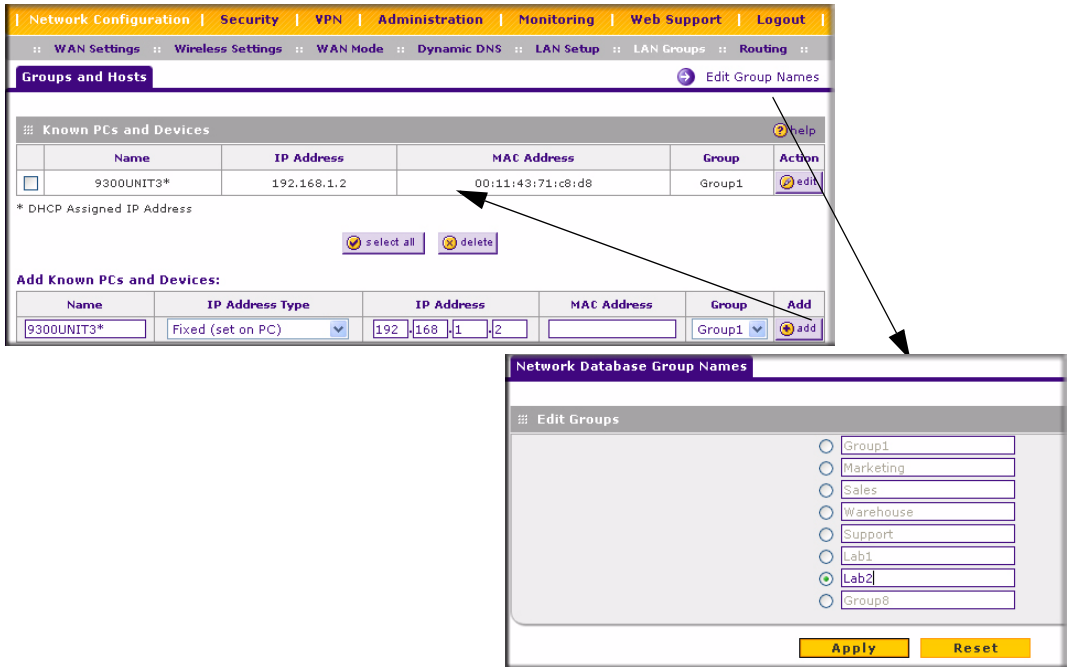
Figure 4-16

Table 4.1   Groups and Hosts

Item	Description
Known PCs and Devices	This table lists all current entries in the Network Database. For each PC or device, the following data is displayed. • Radio button – Use this to select a PC for editing or deletion. • Name – The name of the PC or device. Sometimes, this cannot be determined, and is 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 Group 1.
Operations	• Group Assignment – You can select a group for any entry by selecting **Edit**. When the **Edit Groups and Hosts** screen displays, select the desired group from the pull-down menu in the Group column. Click **Apply**. • Adding a new Entry – If a PC is not connected, using a fixed IP, or a different LAN segment, it may not be listed. In this case, you can add it by adding it to the **Add Known PCs and Devices** and clicking **Add**. • Editing an Entry – To edit an entry, click **Edit** adjacent to the entry. • Deleting an Entry – If a PC or device has been removed from your network, you can delete it from the database. Select its radio button, and click **Delete**. • Edit Group Names – To edit Group names, click the **Edit Group Names** link at the top right of the screen. By default the group names are Group1 through Group 8, with Group 1 being the default group.

Blocking Internet Sites

If you want to reduce incoming traffic by preventing access to certain sites on the Internet, you can use the wireless firewall Web Components filtering and Key Word Blocking. By default, both are disabled; all requested traffic from any Web site is allowed. When enabled, if users try to access a blocked site, they see a "Blocked by NETGEAR" message.

- Web Components filtering – 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 cause many websites to not function properly.

• Keyword (and domain name) Blocking – You can specify up to 32 words that, should they appear in the Web site name (URL) or in a newsgroup name, will cause the site or newsgroup to be blocked by the wireless firewall.

You can apply the keywords to one or more groups in the Apply Keyword Blocking to: fields. 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.

If you enter a domain name in the Trusted Domains box, keyword filtering will be bypassed. For example, if you entered www.netgear.com, keyword filtering will be bypassed for this domain; however, Web Components filtering still applies.

Keyword application examples:

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

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

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

The following screen (Figure 4-17) illustrates the use of Keyword Blocking and adding Trusted Domains.
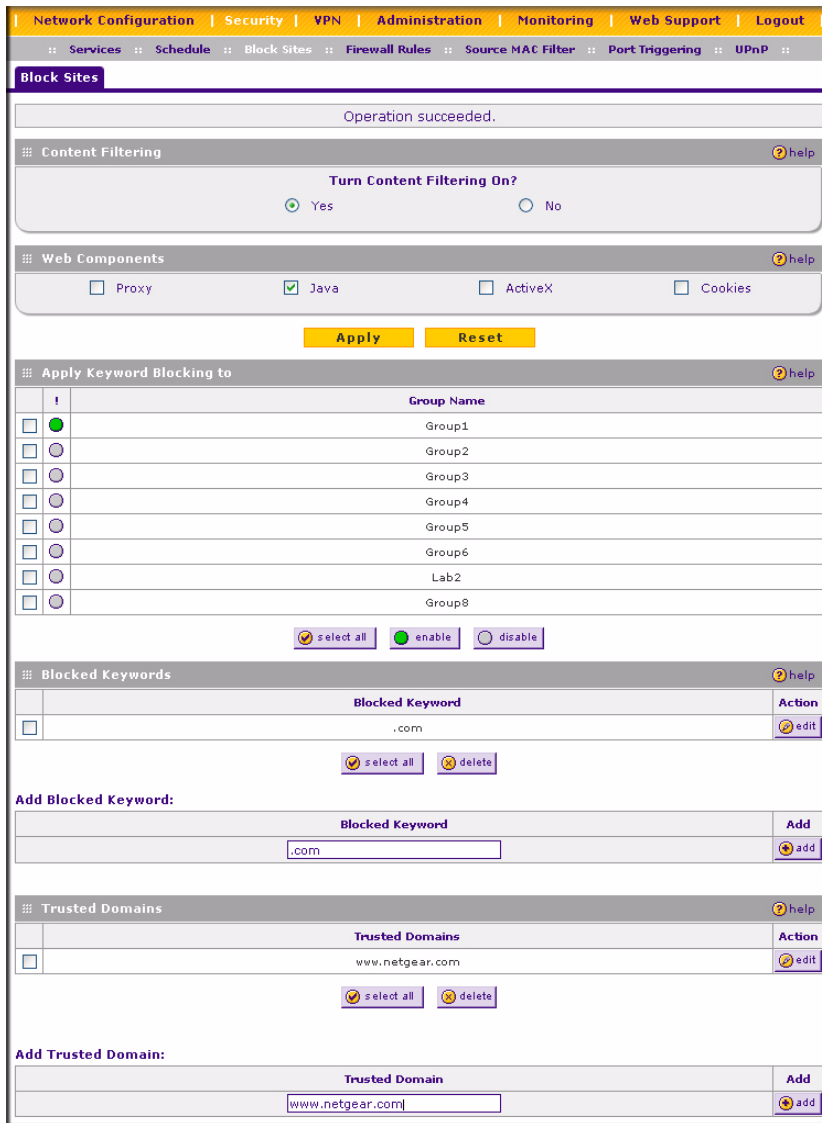
Figure 4-17

To block keywords or Internet domains:

1. Check the **Yes** radio box in the **Turn keyword blocking on?** section and click **Apply**. (The default is **No.**)

2. Select the **Web Components** you want to enable and click **Apply.**

3. Check the boxes next to the group names in the **Apply Keyword Blocking to** list to specify for which groups you want to implement Keyword Blocking. Only those PCs that are in one of the specified groups will undergo the filtering process. Click **Enable.** Only those groups names selected with show their status as enabled.

4. Enter a **Blocked Keyword** in the **Add Blocked Keyword table** and click **Add.** The word or domain name will appear in the **Blocked Keywords** table. Any number of keywords or domain names may be added to the list.

5. 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 domain name must be exact; e.g., entering www.netgear.com would be allowed as a trusted domain exempt from filtering. The Trusted Domain will appear in the **Trusted Domains** table and will be exempt from filtering.

To delete keywords or domain names:

1. Check the box adjacent to the keyword or domain name to be deleted and click **Delete.**

2. Delete all keywords or domain names by clicking **Select All** and then **Delete.**

Enabling Source MAC Filtering

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

- By default, the source MAC address filter is disabled; all the outbound traffic received from any PCs with a MAC address are allowed.

- When enabled, outbound Internet traffic will be dropped from the PCs that have a configured MAC address in the **Blacked MAC Addresses** table.

To enable the Source MAC Address Filtering:

1. Select **Security** from the main menu and **Source MAC Filter** from the submenu. The **Source MAC Filter** screen will display.

2. In the **MAC Filtering Enable** section, check the **Yes** radio box and click **Apply.**

3. Enter the MAC Address to be blocked in the **MAC Address** field and click **Add**. The MAC address will appear in the **Blocked MAC Addresses** table. Repeat this process to add additional MAC addresses.

A valid MAC address is 12 fields; 0 to 9 and a to f. For example: 00:e0:4c:69:0a:11.
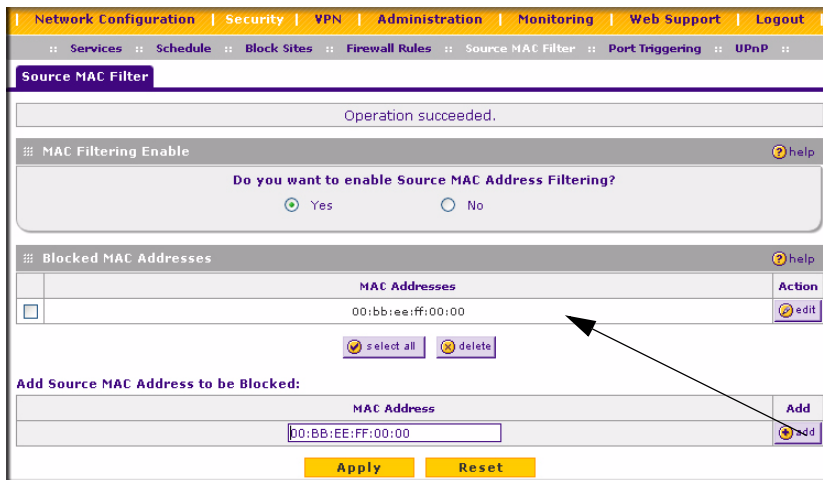
Figure 4-18

4. Click **Apply**. The outbound traffic from the specified MAC addresses will be dropped

> **Note:** For additional ways of restricting outbound traffic, see "Order of Precedence for Rules" on page 4-17.

To delete a MAC Address or all MAC addresses:

- Check the radio box adjacent to the MAC Address to be deleted and click **Delete** or

- Click **select all** to select all the MAC Addresses and click **Delete**.

Setting up Port Triggering

Port triggering is used to allow 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 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 from where the request

was made. 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, the operation is as follows:

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

- The ProSafe DGFV338 records this connection, opens the incoming port or ports associated with this entry in the Incoming Port Triggering table, and associates them with the PC.

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

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

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

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

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

> **Note:** For additional ways of allowing inbound traffic, see "Inbound Rules (Port Forwarding)" on page 4-7.

To add a new port triggering rule:

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

2. Enter the following data in the **Add Port Triggering Rule** fields:

   a. Name – Enter a suitable name for this rule (for example, the name of the application)

   b. Enable/Disable – Select the desired option from the pull-down menu.

   c. Outgoing (Trigger) Port Range – Enter the range of port numbers used by the application on the private network when it generates an outgoing request.

   d. Incoming (Response) Port Range – Enter the range of port numbers used by the remote system when it responds to the PC's request.

3.
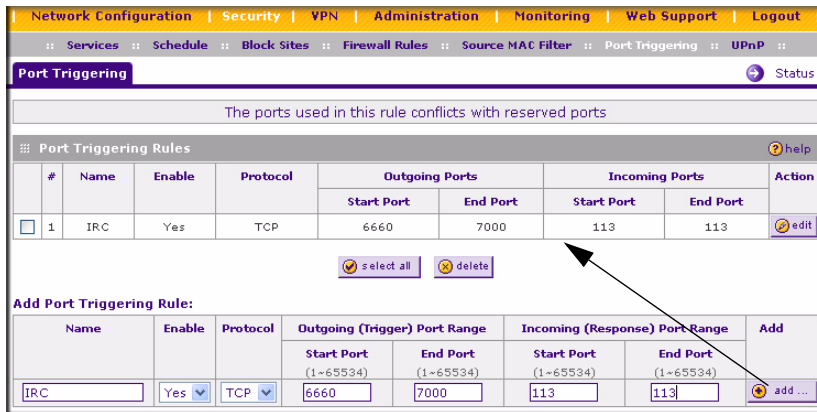
Figure 4-19

Table 4.2   Port triggering

Item	Description
Port Triggering Rules	• Enable - Indicates if the rule is enabled or disabled. Generally, there is no need to disable a rule unless it interferes with some other function such as Port Forwarding. • Name - The name for this rule. • Outgoing Ports - The port or port range for outgoing traffic. An outgoing connection using one of these ports will trigger this rule. • Incoming Ports - The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC which triggered this rule.
Adding a new Rule	• To add a new rule, click the Add and enter the following data on the resulting screen. • Name - enter a suitable name for this rule (e.g., the name of the application) • Enable/Disable - select the desired option. • Outgoing (Trigger) Port Range - enter the range of port numbers used by the application when it generates an outgoing request. • Incoming (Response) Port Range - enter the range of port numbers used by the remote system when it responds to the PC's request.

Table 4.2   Port triggering

Item	Description
Modifying or Deleting an existing Rule:	• Select the desired rule by clicking the radio button beside the rule. • Click Edit or Delete as desired.
Checking Operation and Status	To see which rules are currently being used, click the Status button. The following data will be displayed: • Rule - the name of the Rule. • LAN IP Address - The IP address of the PC currently using this rule. • Open Ports - the Incoming ports which are associated the this rule. Incoming traffic using one of these ports will be sent to the IP address above. • Time Remaining - The time remaining before this rule is released, and thus available for other PCs. This timer is restarted whenever incoming or outgoing traffic is received.

Setting a Schedule to Block or Allow Specific Traffic

If you enabled Content Filtering in the Security/Block Sites menu, or if you defined an outbound rule to use a schedule, you can set up a schedule for when blocking occurs or when access is restricted. The firewall allows you to specify when blocking will be enforced by configuring the Schedule 1, Schedule 2 or Schedule 3 screens.

The ProSafe DGFV338 uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet.

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

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

2. Schedule which Days you want by selecting either the **All Days** radio button or the **Specific Days** radio button. If you selected **Specific Days,** specify which days.

3. Select the time of day radio box: either **All Day** if you want to limit access completely for the selected days; or select a **Specific Times** to limit access during the selected days.

   If you selected **Specific Times,** enter the **Start Time** and **End Time** for this schedule in the appropriate fields.

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

> **Note:** Enter the values as 24-hour time. For example, 10:30 am would be 10 hours and 30 minutes and 10:30 pm would be 22 hours and 30 minutes.
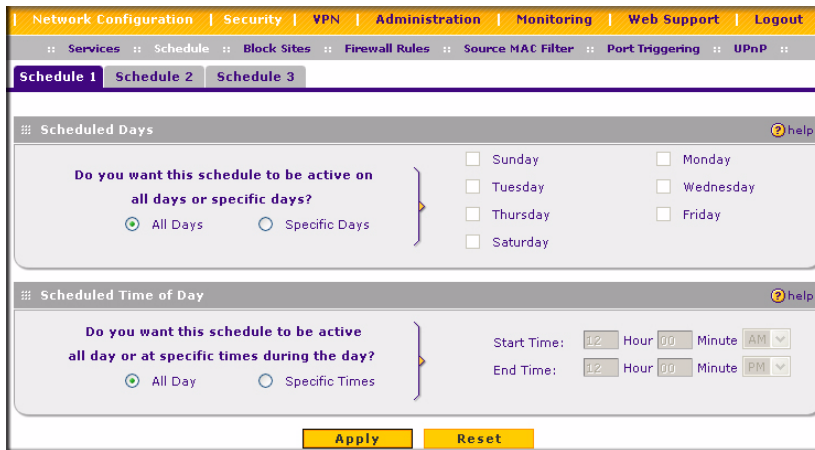
Figure 4-20

Event Logs and Alerts

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

For example, if the Default Outbound Policy is "Block Always", and Accept Packets from LAN to WAN is enabled then, if there is a firewall rule to allow ssh traffic from the LAN, whenever a LAN machine tries to make an ssh connection, those packets will be accepted and a message will be logged.

> **Note:** Make sure the log option for the firewall rule is set to log "always" (see the Security menu, Firewall Rules submenu).

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

> **Note:** Enabling logging options may generate a significant volume of log messages and is recommended for debugging purposes only.
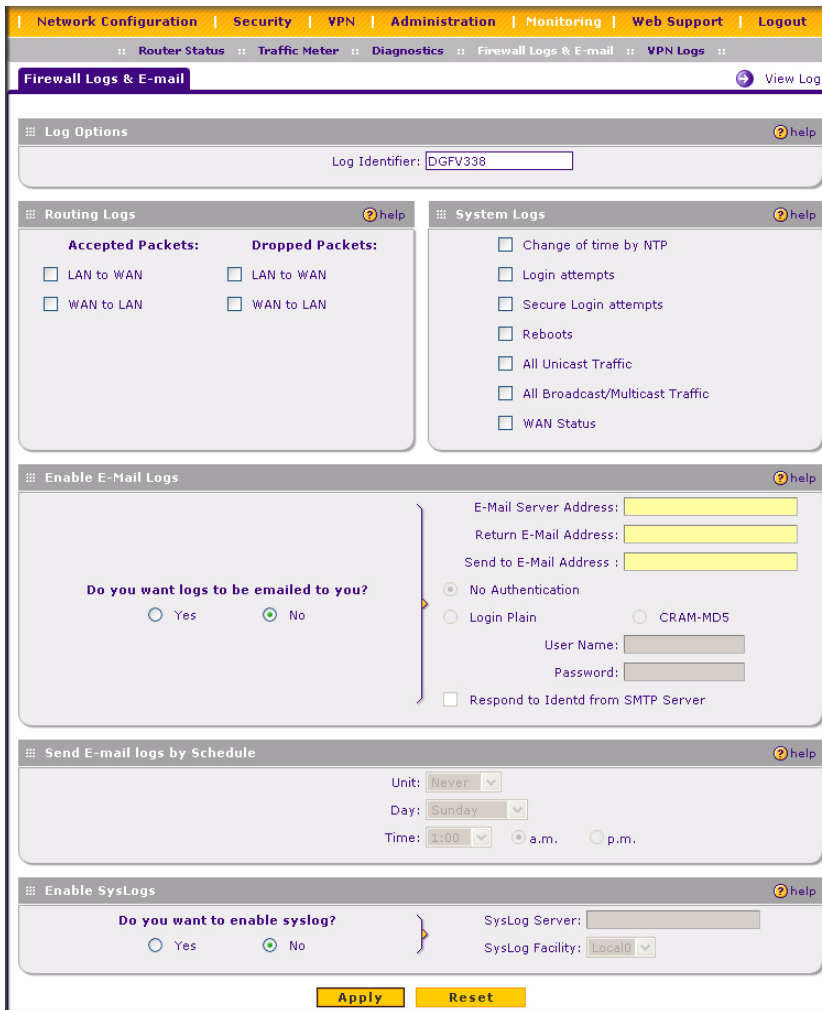
Figure 4-21

To view the Logs and E-mail screen:

1. Select **Monitoring** from the main menu and **Firewall Logs and E-mail** from the submenu. The **Firewall Logs and E-mail** screen will display.

   The **Log Options** section will display the **Log Identifier** field. A mandatory field to identify the log messages. This ID is appended to log messages.

2. From the **Routing Logs** section, check the radio boxes of the Accepted Packets and/or Dropped packets you want to log.

Security and Firewall Protection   4-33

3. From the **System Logs** section, check the radio boxes of the System Log events you want to track and record:

- **Change of Time by NTP**: Logs a message when the system time changes after a request from a Network Time server.

- **Login Attempts**: Logs a message when a login is attempted from the LAN network. Both, successful and failed login attempts will be logged.

- **Secure Login Attempt**: Logs a message when a log in is attempted using the Secure Remote Management URL. "Allow Remote Management" must be enabled (see the Administration main menu and the Remote Management submenu). Both successful and failed login attempts will be logged.

- **Reboots**: Records a message when the device has been rebooted through the Web interface.

- **All Unicast Traffic**: All unicast packets directed to the router are logged.

- **All Broadcast/Multicast Traffic:** All broadcast or multicast packets directed to the router are logged.

- **WAN Status:** WAN link status of all related logs is enabled

4. In the **Enable E-Mail Logs** section, select the Yes radio box if you want the logs e-mailed (**Enable E-Mail Logs** is disabled by default). If you selected "Yes," fill in the following fields:

- **E-mail Server address**: Enter the IP address or Internet Name of an SMTP server. The router will connect to this server to send the e-mail logs.

- **Return E-mail Address:** Type the e-mail address where the replies from the SMTP server are to be sent; for example, failure messages.

- **Send To E-mail Address:** Type the e-mail address where the logs and alerts are to be sent.

- **Authentication with SMTP server**: If the SMTP server requires authentication before accepting connections, select either **Login Plain** or **CRAM-MD5** and enter the **User Name** and **Password** to be used for authentication.

  To disable authentication, select the **No Authentication** radio box.

- **Respond to Identd from SMTP Server:** Check this radio box to configure the router to respond to an IDENT request from the SMTP server.

5. In the **Enable SysLogs** section, if you want the router to send logs to a SysLog server, select the Yes radio box and input the following fields:

- **SysLog Server:** Enter the IP address or Internet Name of the SysLog server.

6. **SysLog Facility**: Select the appropriate syslog facility (Local0 to Local7).

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

Security and Administrator Management

Consider the following operational items:

1. As an option, you can enable Remote Management if you need to manage distant sites from a central location (see "Enabling Remote Management Access" on page 6-8).

2. Although by using Rules (see "Using Rules to Block or Allow Specific Kinds of Traffic" on page 4-1) is the basic or most typical way to manage the traffic through your system, you can further refine your control by using these features of the ProSafe DGFV338:

   – Groups and Hosts (see "Managing Groups and Hosts" on page 4-21)

   – Services (see "Customized Services" on page 4-17)

   – Schedules (see "Setting a Schedule to Block or Allow Specific Traffic" on page 4-31)

   – Block Sites (see "Blocking Internet Sites" on page 4-24)

   – Source MAC Filtering (see "Enabling Source MAC Filtering" on page 4-27)

   – Port Triggering (see "Setting up Port Triggering" on page 4-28)

Chapter 5
Virtual Private Networking

This chapter describes how to use the virtual private networking (VPN) features of the ProSafe DGFV338. VPN tunnels provide secure, encrypted communications between your local network and a remote network or computer.

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

Dual WAN Port Systems

The ADSL port and the Ethernet port of the ProSafe DGFV338 can be configured for auto-rollover mode for increased system reliability (if both ports are configured) or, if only one of the ports is configured, they can be configured as either Dedicated ADSL or Dedicated Ethernet. This WAN mode choice then impacts how the VPN features must be configured.

Table 5-1. IP addressing requirements for VPNs in dual WAN port systems

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

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

Setting up a VPN Connection using the VPN Wizard

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

To set up a Gateway VPN Tunnel using the VPN Wizard:

1. Select **Gateway** as your **VPN tunnel connection**. The wizard needs to know if you are planning to connect to a remote Gateway or setting up the connection for a remote client/PC to establish a secure connection to this device.

2. Select a **Connection Name**. Enter an appropriate name for the connection. This name is not supplied to the remote VPN Endpoint. It is used to help you manage the VPN settings.

3. Enter a **Pre-shared Key**. The key must be entered both here and on the remote VPN Gateway, or the remote VPN Client. This key length should be minimum 8 characters and should not exceed 49 characters. This method does not require using a CA (Certificate Authority).

4. Check the radio box for the **WAN interface** that will act as one end of this VPN tunnel: ADSL or WAN Ethernet.

5. Enter the **Remote WAN IP Address or Internet Name** of the gateway you want to connect to.

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

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

6. Enter the **Local WAN IP Address or Internet Name** of your gateway.

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

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

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

8. Click the **VPN Wizard Default Values** link at the top right of the screen to view the recommended VPNC parameters (see Figure 5-1).

9. Click **Apply** to save your settings. The **VPN Policies** screen will display showing the policy "Offsite" as enabled. Click **Edit** in the **Action** column adjacent to the policy to confirm your policy settings.
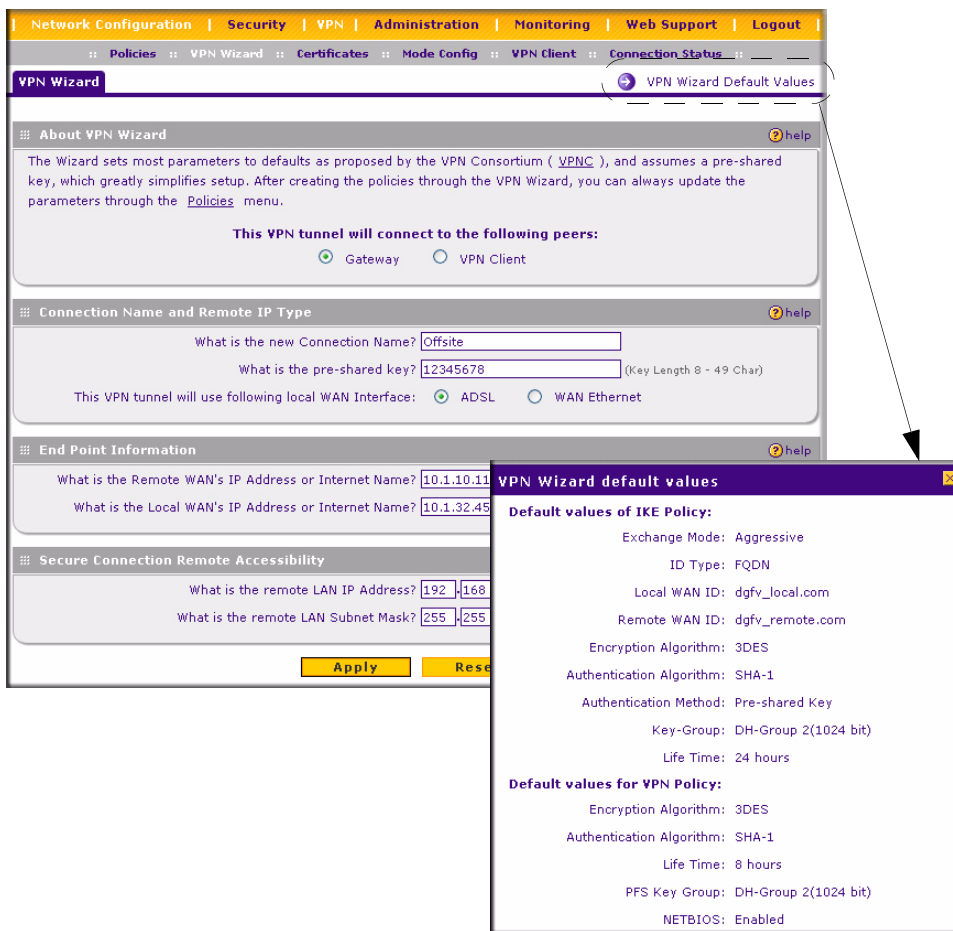
Figure 5-1
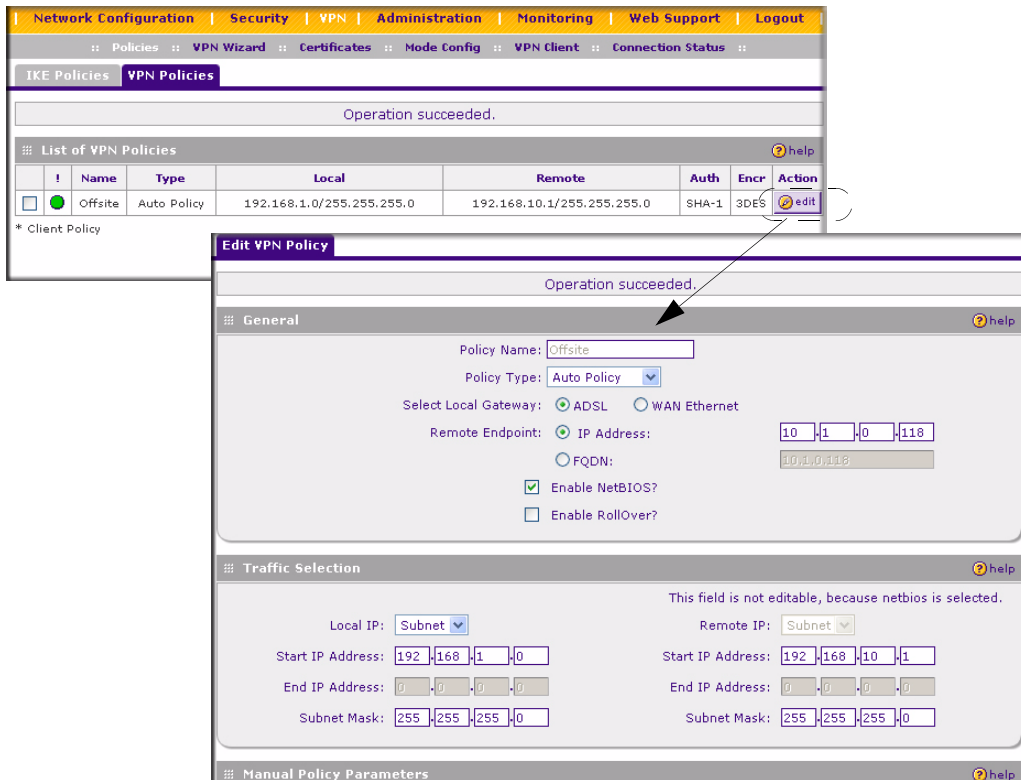
Figure 5-2

You can also view the status of your IKE Policies by clicking the **IKE Policies** tab. The **IKE Policies screen** will display. Then view or edit the parameters of the "Offsite" policy by clicking **Edit** in the **Action** column adjacent to the policy. The **Edit IKE Policy** screen will display.
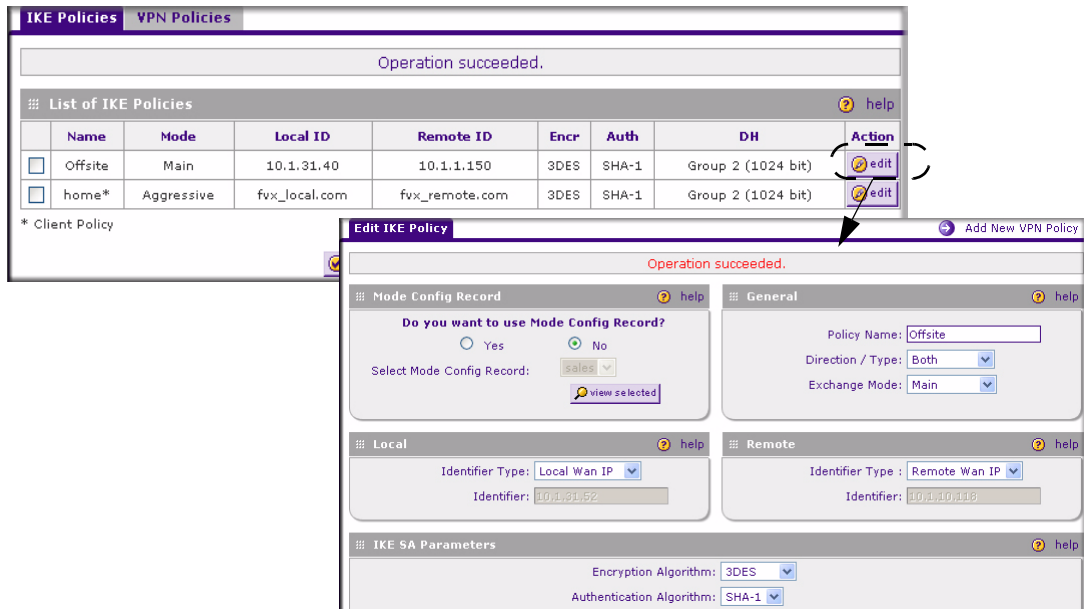
Figure 5-3

VPN Tunnel Policies

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

IKE Policy

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.

Managing IKE Policies

IKE Policies are activated when:

1. The VPN Policy Selector determines that some traffic matches an existing VPN Policy. If the VPN policy is of type "Auto", then the **Auto Policy Parameters** defined in the VPN Policy are accessed which specify which IKE Policy to use.

2. If the VPN Policy is a "Manual" policy, then the **Manual Policy Parameters** defined in the VPN Policy are accessed and the first matching IKE Policy is used to start negotiations with the remote VPN Gateway.

   • If negotiations fail, the next matching IKE Policy is used.

   • If none of the matching IKE Policies are acceptable to the remote VPN Gateway, then a VPN tunnel cannot be established.

3. An IKE session is established, using the SA (Security Association) parameters specified in a matching IKE Policy:

   • Keys and other parameters are exchanged.

   • An IPSec SA (Security Association) is established, using the parameters in the VPN Policy.

   The VPN tunnel is then available for data transfer.

IKE Policy Table

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

• **Name**. Uniquely identifies each IKE policy. The name is chosen by you and used for the purpose of managing your policies; it is not supplied to the remote VPN Server.

• **Mode**. Two modes are available: either "Main" or "Aggressive".

  – Main Mode is slower but more secure.

  – Aggressive mode is faster but less secure.

• **Local ID**. The IKE/ISAKMP identify of this device. (The remote VPN must have this value as their "Remote ID".)

• **Remote ID**. The IKE/ISAKMP identify of the remote VPN Gateway. (The remote VPN must have this value as their "Local ID".)

- **Encr**. Encryption Algorithm used for the IKE SA. The default setting using the VPN Wizard is 3DES. (This setting must match the Remote VPN.)

- **Auth**. Authentication Algorithm used for the IKE SA. The default setting using the VPN Wizard is SHA1. (This setting must match the Remote VPN.)

- **DH**. Diffie-Hellman Group. The Diffie-Hellman algorithm is used when exchanging keys. The DH Group sets the number of bits. The VPN Wizard default setting is Group 2. (This setting must match the Remote VPN.)

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

VPN Policy

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

- **Manual**. All settings (including the keys) for the VPN tunnel are manually input at each end (both VPN Endpoints). No third party server or organization is involved.

- **Auto**. Some parameters for the VPN tunnel are generated automatically by using the IKE (Internet Key Exchange) protocol to perform negotiations between the two VPN Endpoints (the Local ID Endpoint and the Remote ID Endpoint).

In addition, a CA (Certificate Authority) can also be used to perform authentication (see "Certificate Authorities" on page 5-22). To use a CA, each VPN Gateway must have a Certificate from the CA. For each Certificate, there is both a "Public Key" and a "Private Key". The "Public Key" is freely distributed, and is used to encrypt data. The receiver then uses their "Private Key" to decrypt the data (without the Private Key, decryption is impossible). CAs can be beneficial since using them reduces the amount of data entry required on each VPN Endpoint.

Managing VPN Policies

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.

VPN Policy Table

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 radio box adjacent to the circle and click **Enable** or **Disable**, as required.

- **Name**. Each policy is given a unique name (the Connection Name when using the VPN Wizard).

- **Type**. The Type is "Auto" or "Manual" as described previously (Auto is used during VPN Wizard configuration).

- **Local**. IP address (either a single address, range of address or subnet address) on your local LAN. Traffic must be from (or to) these addresses to be covered by this policy. (The Subnet address is supplied as the default IP address when using the VPN Wizard).

- **Remote**. IP address or address range of the remote network. Traffic must be to (or from) these addresses to be covered by this policy. (The VPN Wizard default requires the remote LAN IP address and subnet mask).

- **AH**. Authentication Header. This specifies the authentication protocol for the VPN header (VPN Wizard default is disabled).

- **ESP**. Encapsulating Security Payload. This specifies the encryption protocol used for the VPN data (VPN Wizard default is enabled).

- **Action.** Allows you to access individual policies to make any changes or modifications.

VPN Tunnel Connection Status

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

- **Policy Name.** The name of the VPN policy associated with this SA.

- **Endpoint**. The IP address on the remote VPN Endpoint.

- **Tx (KBytes)**. The amount of data transmitted over this SA.

- **Tx (Packets).** The number of packets transmitted over this SA.

- **State**. The current state of the SA. Phase 1 is "Authentication phase" and Phase 2 is "Key Exchange phase".

- **Action**. Allows you to terminate or build the SA (connection), if required.

Creating a VPN Connection: Between FVX538 and DGFV338

This section describes how to configure a VPN connection between a NETGEAR FVX538 VPN Firewall and the ProSafe Wireless ADSL Modem VPN Firewall Router.

Using each firewall's VPN Wizard, we will create a set of policies (IKE and VPN) that will allow the two firewalls to connect from locations with fixed IP addresses. Either firewall can initiate the connection.

To graphically illustrate this process, we will assume the following:

- NETGEAR FVX538 VPN Firewall with:

  – WAN IP address is 10.1.32.40

  – LAN IP address subnet is 192.168.1.1/255.255.255.0

- NETGEAR ProSafe DGFV338 with:

  – WAN IP address is 10.1.1.150

  – LAN IP address subnet is 192.168.2.1/255.255.255.0

Configuring the ProSafe DGFV338

To configure the ProSafe DGFV338:

1. Select **VPN** from the main menu. The **Policies** submenu will display showing the **IKE Policies** screen

2. Select **VPN Wizard**. The **VPN Wizard** screen will display.

3. Select the **VPN Tunnel** connection type; in this case, the Gateway radio box is selected.

4. Give the gateway connection a name, such as `to_fvx`.

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

6. Select ADSL as the local WAN interface for your VPN tunnel connection.

Virtual Private Networking 5-9

7. Enter the WAN IP address of the remote FVX538 and then enter the WAN IP address of the local DGFV338. (Both local and remote ends must define the address as either an IP address or a FQDN. A combination of IP address and FQDN is not permissible.)**.**

Figure 5-4

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

9. Click **Apply** to create the "to_fvx" IKE and VPN policies. The VPN Policies screen will display showing the "to_fvx" policy as enabled in the **List of VPN Policies** table.
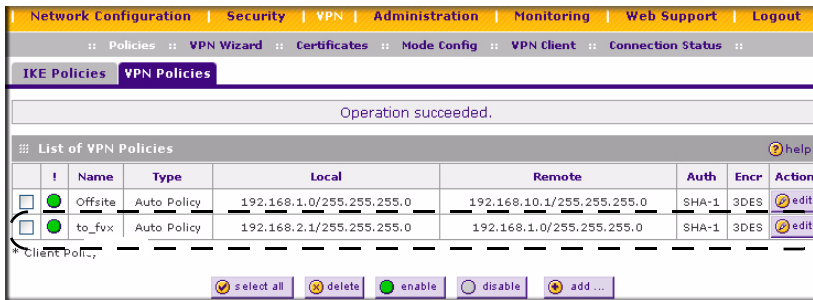
Figure 5-5

To view the VPN Policy parameters:

1. Click **Edit** in the **Action** column adjacent to the "to_fvx" policy. The **Edit VPN Policy** screen will display. (It should not be necessary to make any changes.

2. View the IKE Policy statistics associated with this policy by clicking **View Selected.**
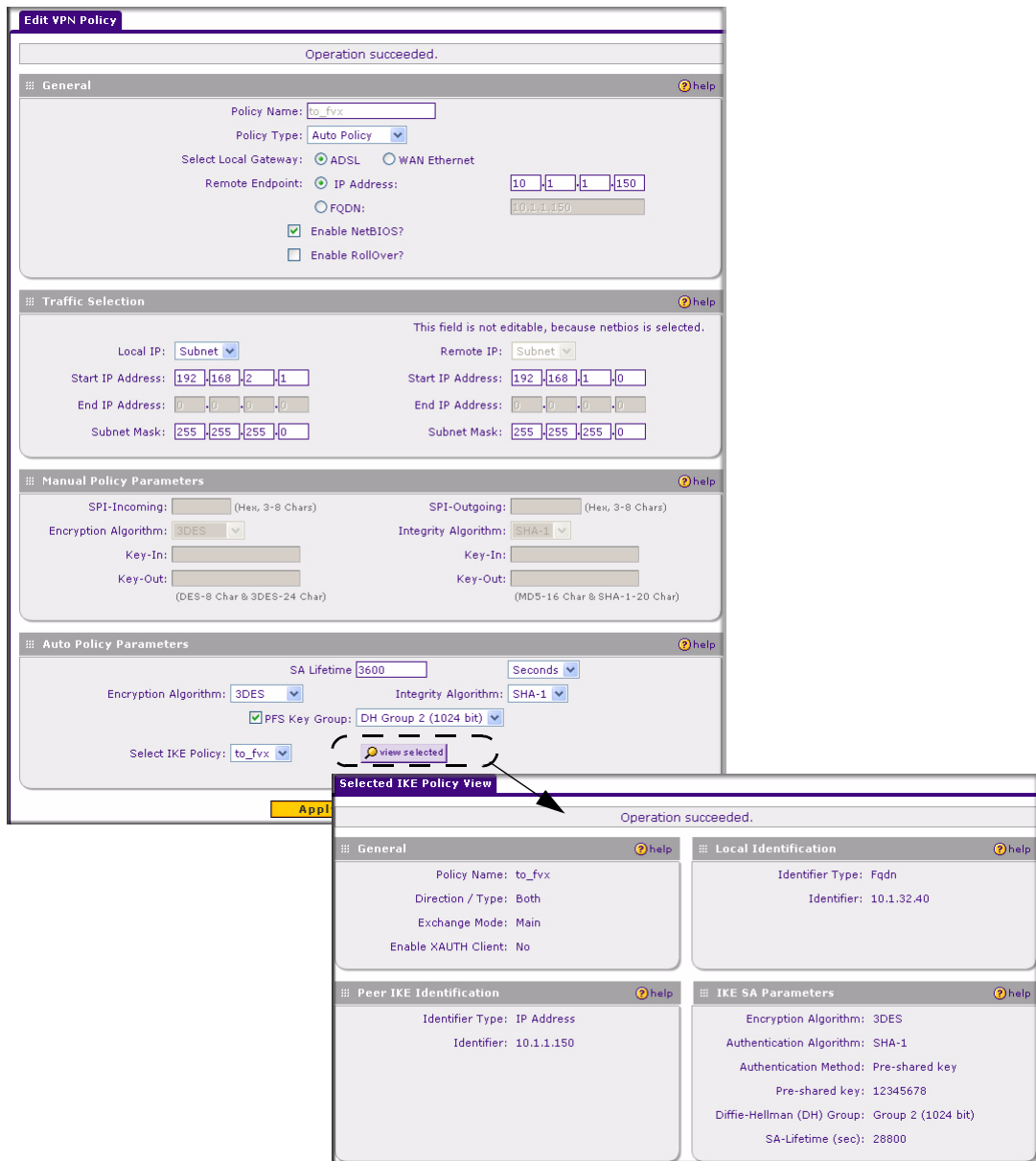
Figure 5-6

To view the IKE Policy Configuration parameters:

1. Select the **IKE Policies** tab. The **IKE Policies** table will display.

2. Select "to_FVX" and click **Edit**. It should not be necessary to make any changes)
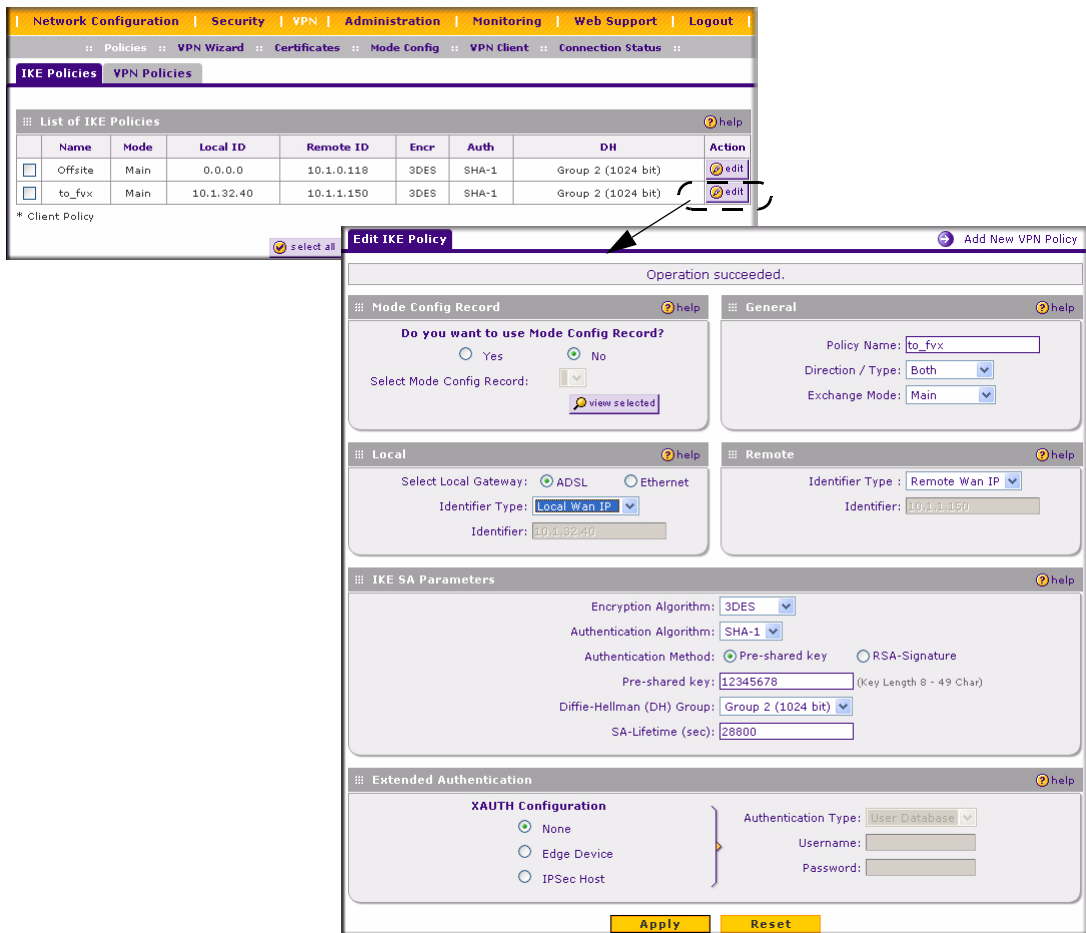
Figure 5-7

> → | **Note:** When XAUTH is enabled as an Edge Device, incoming VPN connections are authenticated against the DGFV338 User Database first; then, if configured, a RADIUS server is checked. If IPSec Host is enabled, users are authenticated by the remote host.

Configuring the FVX538

To configure the FVX538 VPN Wizard:

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

2. Check the **Gateway** radio box for the type of VPN tunnel connection.

3. Give the new connection a name, such as **to_dgfv**..

Figure 5-8

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

5. Enter the WAN IP address of the remote DGFV338.

6. Enter the WAN IP address of the FVX538.

7. Enter the LAN IP address and subnet mask of the remote DGFV338.

8. Click **Apply** to create the "to_dgfv" IKE and VPN policies. The **VPN Policies** screen will display.

Testing the Connection

To test the VPN gateway tunnel:

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

2. For additional status and troubleshooting information, view VPN Logs and VPN Connections Status screens in the FVX538 or DGFV338.

Creating a VPN Client Connection: VPN Client to DGFV338

This section describes how to configure a VPN connection between a Windows PC and the ProSafe DGFV338.

Using the DGFV338's VPN Wizard, we will create a single set of VPN Client policies (IKE and VPN) that will allow up to 50 remote PCs to connect from locations in which their IP addresses are unknown in advance. The PCs may be directly connected to the Internet or may be behind NAT routers. If more PCs are to be connected, an additional policy or policies must be created.

Each PC will use Netgear's ProSafe VPN Client software. Since the PC's IP address is assumed to be unknown, the PC must always be the Initiator of the connection.

This procedure was developed and tested using:

- Netgear ProSafe Wireless ADSL Modem VPN Firewall Router

- Netgear ProSafe VPN Client

- NAT router: Netgear FR114P

Configuring the DGFV338

1. Select the VPN Wizard.

2. Select the **VPN Client** radio button for type of VPN connection.

3. Give the client connection a name, such as "home".

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

5. Check either the ADSL or WAN Ethernet radio box to select the WAN interface tunnel.

Virtual Private Networking
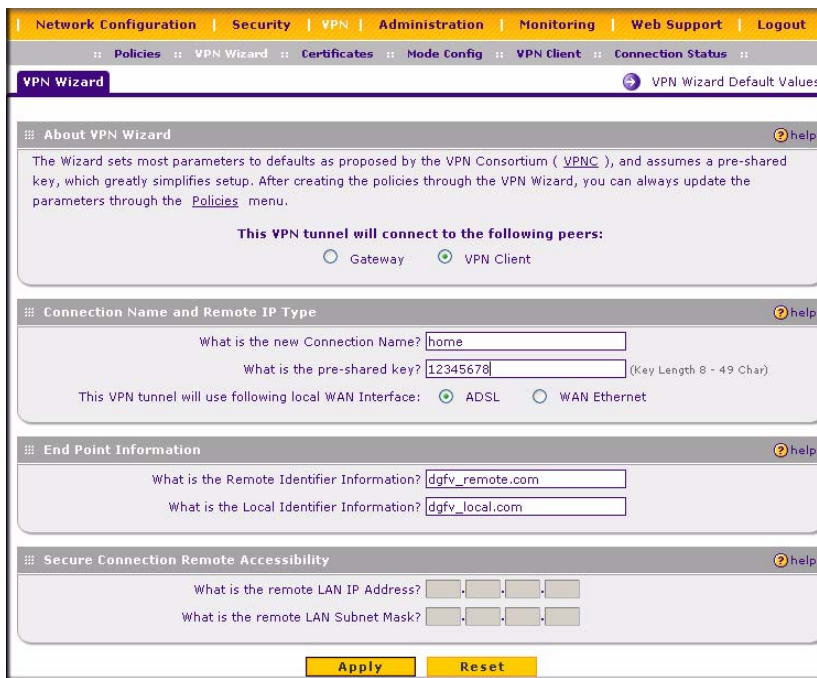
Figure 5-9

6. Enter he remote WAN's IP Address or Internet Name and then enter the local WAN's IP Address or Internet Name. In this example, we are using their FQDNs. (Both the local and remote addresses must be of the same type—either both must be FQDN or both must be an IP address.)

7. Click **Apply** to create the "home" VPN Client. The **VPN Policies** screen will display showing the VPN Client policy as enabled.

8. Click the **IKE Policies** tab to display the **IKE Policies** table and click **Edit** adjacent to the "home" policy to view the "home" policy details.

   You can also augment user authentication security by enabling the XAUTH server by selecting the **Edge Device** radio box and then adding users to the User Database (see "Extended Authentication (XAUTH) Configuration" on page 5-26 and "User Database Configuration" on page 5-29, respectively). Alternatively, you can also choose to selection either a RADIUS-CHAP or RADIUS-PAP server.

Configuring the VPN Client

From a PC with the Netgear Prosafe VPN Client installed, you can configure a VPN client policy to connect to the DGFV338.

To configure your VPN client:

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

2. In the upper left of the Policy Editor window, click the New Document icon to open a New Connection.Give the New Connection a name, such as **to_dgfv.**
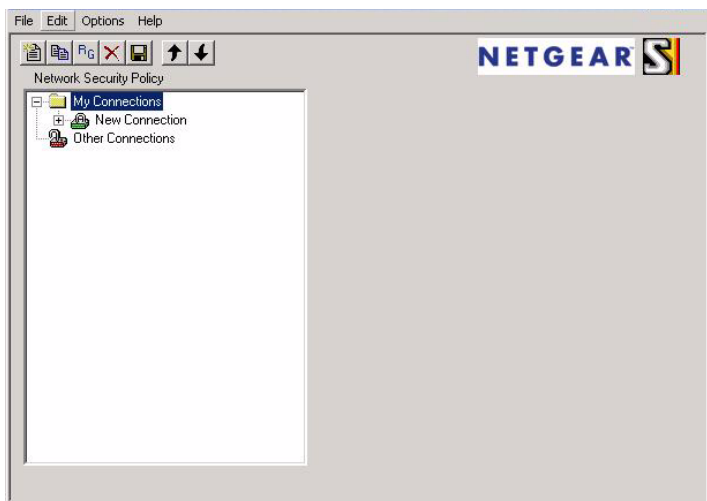
Figure 5-10

3. From the **ID Type** pull-down menu, select **IP Subnet**.

4. Enter the LAN IP **Subnet Address** and **Subnet Mask** of the DGFV338 LAN.Check the **Connect using** radio box and select **Secure Gateway Tunnel** from the pull-down menu.

5. From the first **ID Type** pull-down menus, select **Domain Name** and enter the FQDN address of the DGFV338.

6. From the second **ID Type** pull-down menu, select **Gateway IP Address** and enter the WAN IP Gateway address of the DGFV338.
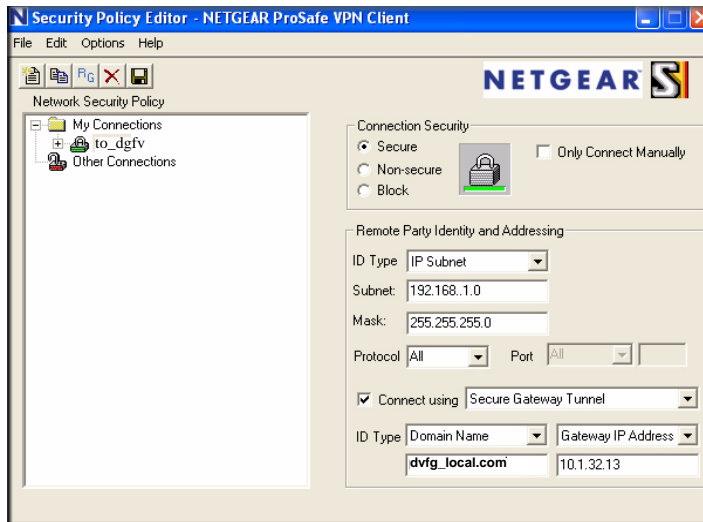
Figure 5-11

7. In the left frame, click **My Identity**.

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

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

The value entered under Domain Name is ".dvfg_remote.com". In this example, we have entered **dvfg_remote.com**. Up to 50 users can be served by one policy.

10. Leave **Virtual Adapter** disabled, and select your computer's Network Adapter. Your current IP address will appear.
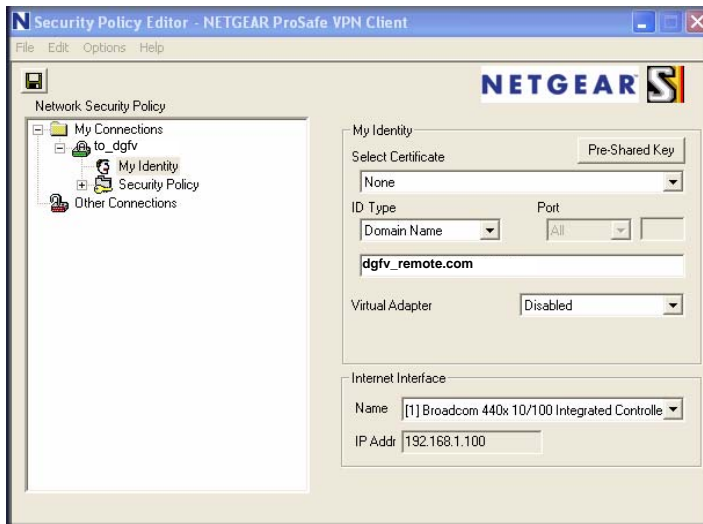
Figure 5-12

5. Before leaving the My Identity menu, click **Pre-Shared Key**.

6. Click **Enter Key** and then enter your preshared key, and click **OK**. This key will be shared by all users of the DGFV338 policy "home".
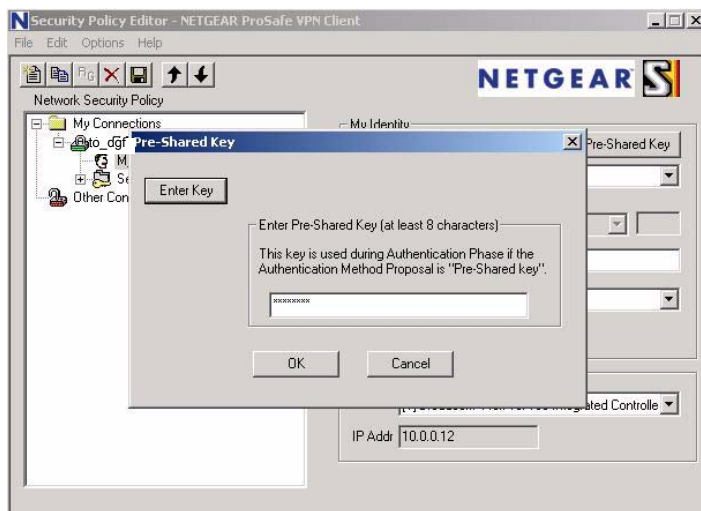
Figure 5-13

7. In the left frame, select **Security Policy.**

8. For the **Phase 1 Negotiation Mode**, check the **Aggressive Mode** radio box.

9. **PFS** should be enabled, and **Enable Replay Detection** should be enabled.
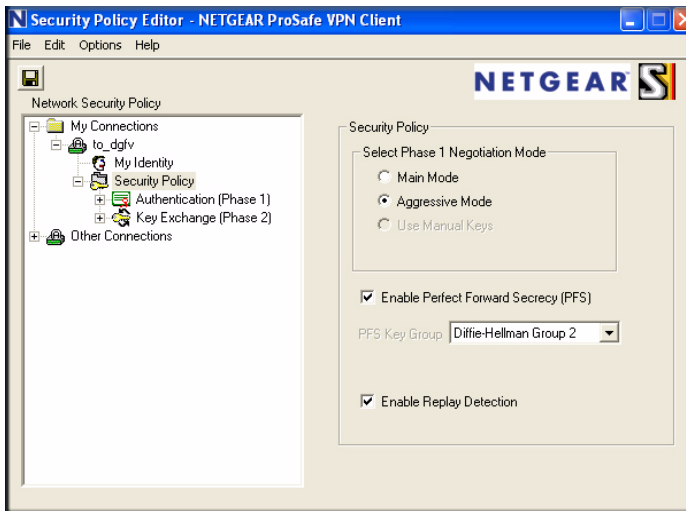
Figure 5-14

10. In the left frame, expand **Authentication (Phase 1)** and select **Proposal 1**. The Proposal 1
    fields should mirror those in the following figure. No changes should be necessary.
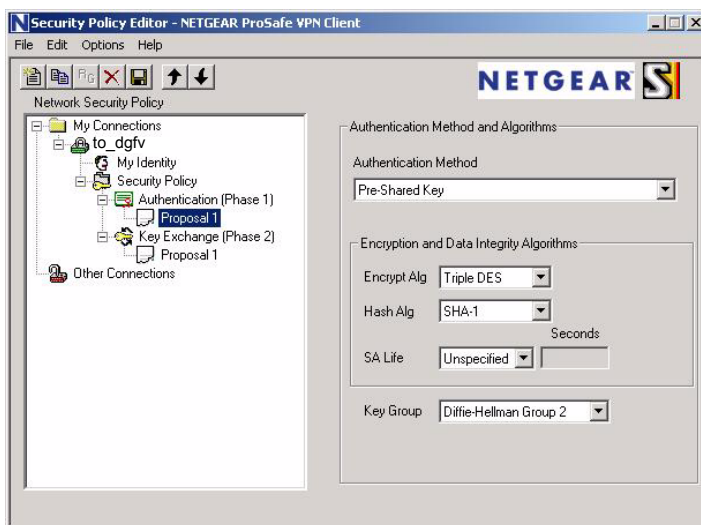
Figure 5-15

11. In the left frame, expand **Key Exchange (Phase 2)** and select **Proposal 1**. The fields in this proposal should also mirror those in the following figure. No changes should be necessary.

12. In the upper left of the window, click the disk icon to save the policy.
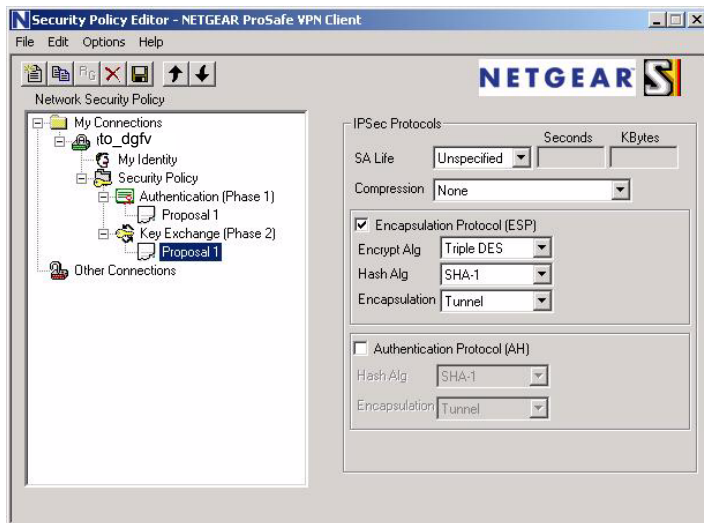
Figure 5-16

Testing the Connection

1. From your PC, right-click on the VPN client icon in your Windows toolbar and select **Connect...**, then **My Connections\to_dgfv**.

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

2. For additional status and troubleshooting information, right-click on the VPN client icon Logs and Connection Status screens in the DGFV338.
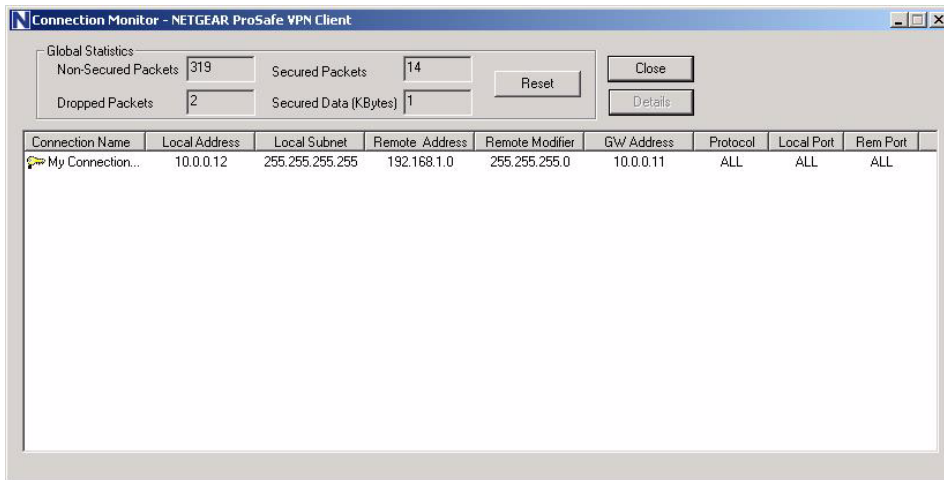
Figure 5-17

Certificate Authorities

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

Each CA also issues a CA Identity certificate shown in the **Trusted Certificates (CA Certificates)** table. This Certificate is required in order to validate communication with the CA. It is a three-step process. First, you generate a CA request; then, when the request is granted, you upload the Self Certificate (shown in the **Active Self Certificates** table) and then you upload the CA Identity certificate (shown in the **Trusted Certificates** table.

The **Trusted Certificates** table lists the certificates generated and signed by a publicly known organization or authority called the Certificate Authority. The table lists the certificates of each CA 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

5-22   Virtual Private Networking

The Active Self Certificates table shows the Certificates issued to you by the various CAs (Certification Authorities), and available for use. For each Certificate, the following data is listed:

- **Name**. The name you used to identify this Certificate.

- **Subject Name**. This is the name which other organizations will see as the Holder (owner) of this Certificate. This should be your registered business name or official company name. Generally, all Certificates should have the same value in the Subject field.

- **Serial Number**. It 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 which issued the Certificate.

- **Expiry Time**. The date on which the Certificate expires. You should renew the Certificate before it expires.

Generating a Self Certificate Request

To use a Certificate, you must first request the certificate from the CA, then download and activate the certificate on your system.

To request a Certificate from the CA:

1. From the main menu under **VPN**, select the **Certificates** submenu. The Certificates screen will display.

2. In the **Generate Self Certificate Request,** enter the required data:

   - **Name** – Enter a name that will identify this Certificate.

   - **Subject** – This is the name which other organizations will see as the Holder (owner) of the Certificate. Since this name will be seen by other organizations, you should use your registered business name or official company name. (Using the same name, or a derivation of the name, in the Title field would be useful.)

   - From the pull-down menus, select the following values:

     – Hash Algorithm: MD5 or SHA2.

     – Signature Algorithm: RSA.

     – Signature Key Length: 512, 1024, 2048. (Larger key sizes may improve security, but may also impact performance.)

3. Complete the Optional fields, if desired, with the following information:

   - **IP Address** – If you have a fixed IP address, you may enter it here. Otherwise, you should leave this field blank.

Virtual Private Networking   5-23
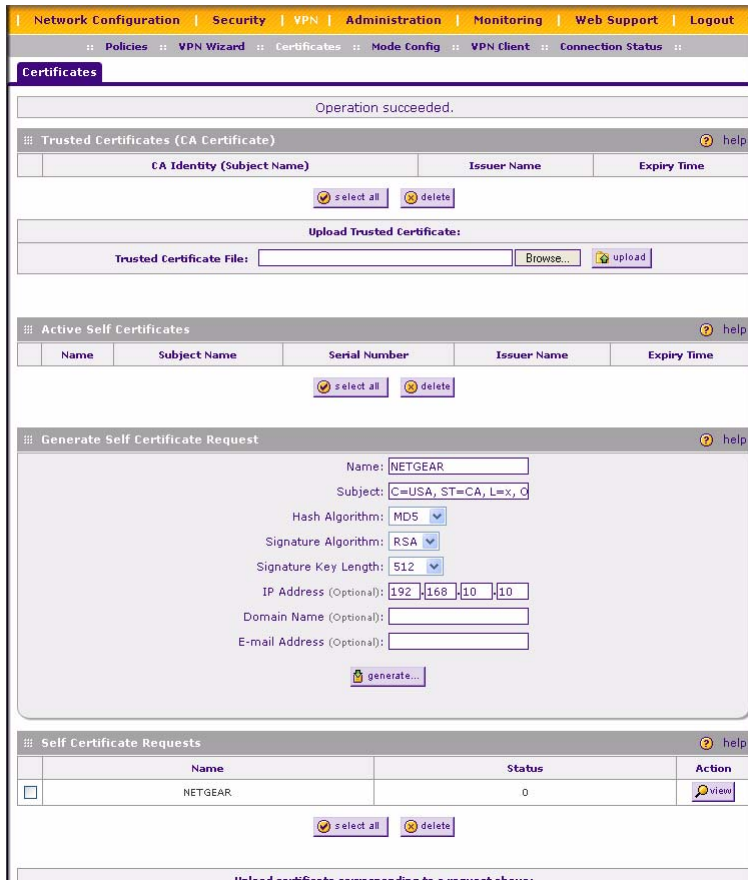
Figure 5-18

- **Domain Name** – If you have a Domain name, you can enter it here. Otherwise, you should leave this field blank.

- **E-mail Address** – Enter your e-mail address in this field.

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

5. Click **View** under the **Action** column to view the request.

6. Copy the contents of the **Data to supply to CA** text box into a file, including all of the data contained in "----BEGIN CERTIFICATE REQUEST---" and "---END CERTIFICATE REQUEST---"Click **Done.** You will return to the Certificate screen and your Request details will be displayed in the **Self Certificates Requests** table showing a Status of "Waiting for Certificate upload"

To submit your Certificate request to a CA:

1. Connect to the Website of the CA.

2. Start the Self Certificate request procedure.

3. When prompted for the requested data, copy the data from your saved data file (including "----BEGIN CERTIFICATE REQUEST---" and "---END CERTIFICATE REQUEST').

4. Submit the CA form. If no problems ensue, the Certificate will be issued.

Uploading a Trusted Certificate

After obtaining a new Certificate from the CA, you must upload the certificate to this device and add it to your Trusted Certificates:

To upload your new certificate:

1. From the main menu, under **VPN**, select **Certificates**. The Certificates screen will display. Scroll down to the **Self Certificate Requests** section.

2. Click **Browse**, and locate the certificate file on your PC. Select the file name in the "File to upload" field and click **Upload**. The certificate file will be uploaded to this device.

3. Scroll back to the **Active Self Certificates** table. The new Certificate will appear in the **Active Self Certificates** list.

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

Managing your Certificate Revocation List (CRL)

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

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

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

- CA 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.

To upload a Certificate Identify to the CRL:

1. From the main menu under VPN, select **Certificates**. The **Certificates** screen will display showing the CRL (Certificate Revocation List) table at the bottom of the screen.

2. Click **Browse**, and then locate the file you previously downloaded from a CA.

3. Select the Certificate Identify file. The name will appear in the "File to upload" field. Click **Upload.**

Click **Back** to return to the CRL list. The new Certificate Identify will appear in the CRL Table. If you have a previous CA Identity from the same CA, it should now be deleted.

Figure 5-19

Extended Authentication (XAUTH) Configuration

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

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

- **Edge Device.** If this is selected, the router is used as a VPN concentrator where one or more gateway tunnels terminate. If this option is chosen, you must specify the authentication type to be used in verifying credentials of the remote VPN gateways: User Database, RADIUS-PAP, or RADIUS-CHAP.

- **IPSec Host.** If you want authentication by the remote gateway, enter a User Name and Password to be associated with this IKE policy. If this option is chosen, the remote gateway must specify the user name and password used for authenticating this gateway.

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

Configuring XAUTH for VPN Clients

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

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

To enable and configure XAUTH:

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

2. You can 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.**

3. In the **Extended Authentication** section check the **Edge Device** radio box to use this router as a VPN concentrator where one or more gateway tunnels terminate. You then must specify the authentication type to be used in verifying credentials of the remote VPN gateways. (Either the User Database or RADIUS Client must be configured when XAUTH is enabled.)

4. In the **Extended Authentication** section, select the **Authentication Type** from the pull-down menu which will be used to verify user account information. Select

   - **Edge Device** to use this router as a VPN concentrator where one or more gateway tunnels terminate. When this option is chosen, you will need to specify the authentication type to be used in verifying credentials of the remote VPN gateways.

     – **User Database** to verify against the router's user database. Users must be added through the User Database screen (see "User Database Configuration" on page 5-29).

– **RADIUS–CHAP** or **RADIUS–PAP** (depending on the authentication mode accepted by the RADIUS server) to add a RADIUS server. If RADIUS–PAP is selected, the router will first check in the User Database to see if the user credentials are available. If the user account is not present, the router will then connect to the RADIUS server (see "RADIUS Client Configuration" on page 5-30).

• **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.
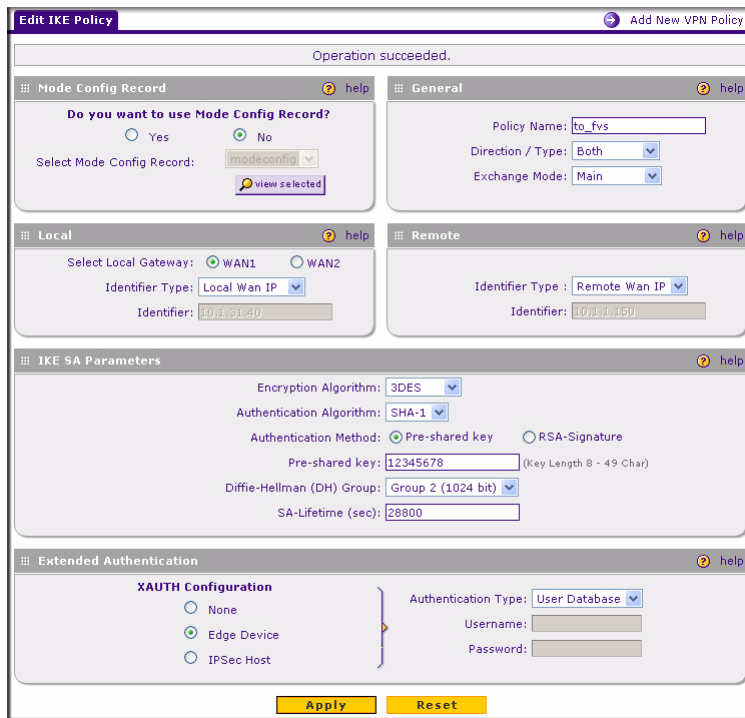
Figure 5-20

User Database Configuration

The **User Database** screen is used to configure and administer users when Extended Authentication is enabled as an Edge Device. Whether or not you use an external RADIUS server, you may want some users to be authenticated locally. These users must be added to the **User Database Configured Users** table.

To add a new user:

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

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

3. Enter a **Password** for the user, and reenter the password in the **Confirm Password** field.

4. Click **Add.** The User Name will be added to the Configured Users table.
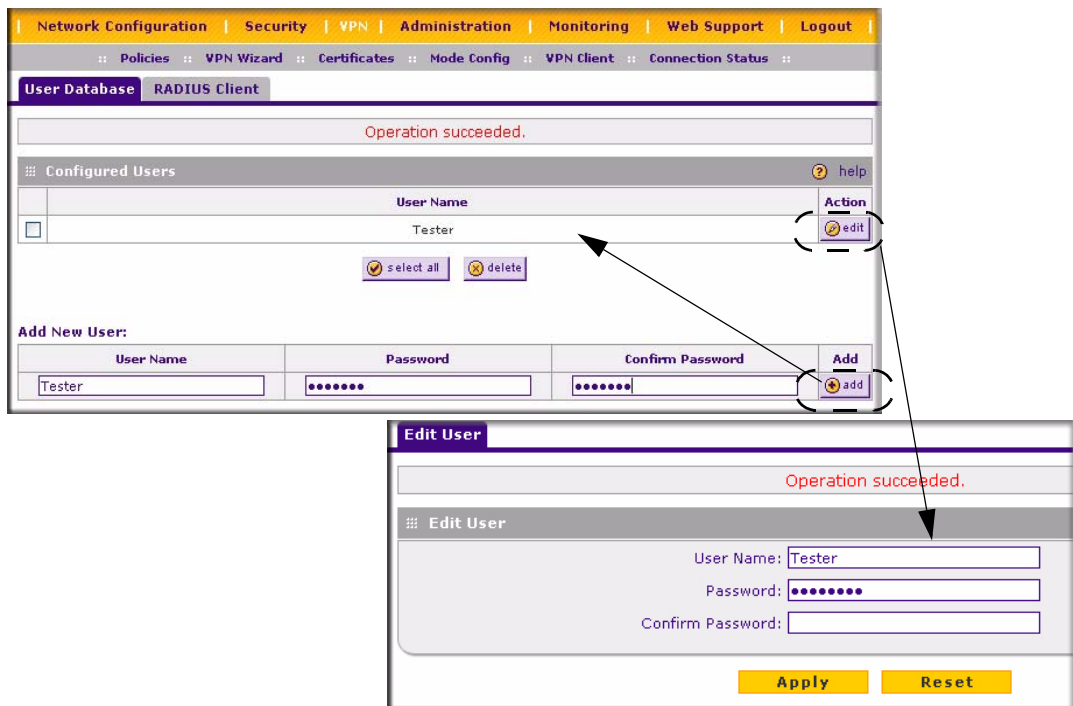
Figure 5-21

To edit the user name or password:

1. Click **Edit** opposite the user's name. The **Edit User** screen will display.

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

RADIUS Client Configuration

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

To configure the Primary RADIUS Server:

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

2. Enable the Primary RADIUS server by checking the **Yes** radio box

Figure 5-22

3. Enter the Primary **RADIUS Server IP address**.

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

5. Enter the **Primary Server NAS Identifier** (Network Access Server). This Identifier MUST be present in a RADIUS request. Ensure that NAS Identifier is configured as the same on both client and server.

The DGFV338 is acting as a NAS (Network Access Server), allowing network access to external users after verifying their authentication information. In a RADIUS transaction, the NAS must provide some NAS Identifier information to the RADIUS Server. Depending on the configuration of the RADIUS Server, the router's IP address may be sufficient as an identifier, or the Server may require a name, which you would enter here. This name would also be configured on the RADIUS Server, although in some cases it should be left blank on the RADIUS Server.

6. Enable a Backup RADIUS Server (if required) by following steps 2 through 5.

7. Set the **Time Out Period**, in seconds, that the router should wait for a response from the RADIUS server.

8. Set the **Maximum Retry Count.** This is the number of tries the router will make to the RADIUS server before giving up.

9. Click **Reset** to cancel any changes and revert to the previous settings.

10. Click **Apply** to save the settings.

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

Manually Assigning IP Addresses to Remote Users (ModeConfig)

To simply the process of connecting remote VPN clients to the DGFV338, the ModeConfig module can be used to assign IP addresses to remote users, including a network access IP address, subnet mask, and name server addresses from the router. Remote users are given IP addresses available in secured network space so that remote users appear as seamless extensions of the network.

In the following example, we configured the ProSafe DGFV338 using ModeConfig, and then configured a PC running ProSafe VPN Client software using these IP addresses.

- NETGEAR ProSafe Wireless ADSL Modem VPN Firewall Router

    – 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 ProSafe DGFV338

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

To configure the Mode Config menu:

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

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

3. Enter a descriptive **Record Name** such as "Sales".

4. Assign at least one range of IP Pool addresses in the First IP Pool field to give to remote VPN clients.

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

5. If you have a WINS Server on your local network, enter its IP address.

6. Enter one or two DNS Server IP addresses to be used by remote VPN clients.

7. If you enable Perfect Forward Secrecy (PFS), select DH Group 1 or 2. This setting must match exactly the configuration of the remote VPN client,

8. Specify the Local IP Subnet to which the remote client will have access. Typically, this is your router's LAN subnet, such as 192.168.2.1/255.255.255.0. (If not specified, it will default to the LAN subnet of the router.)

9. Specify the VPN policy settings. These settings must match the configuration of the remote VPN client. Recommended settings are:
   • SA Lifetime: 3600 seconds
   • Authentication Algorithm: SHA-1
   • Encryption Algorithm: 3DES

10. Click **Apply**. The new record should appear in the VPN Remote Host Mode Config Table (a sample record is shown below).
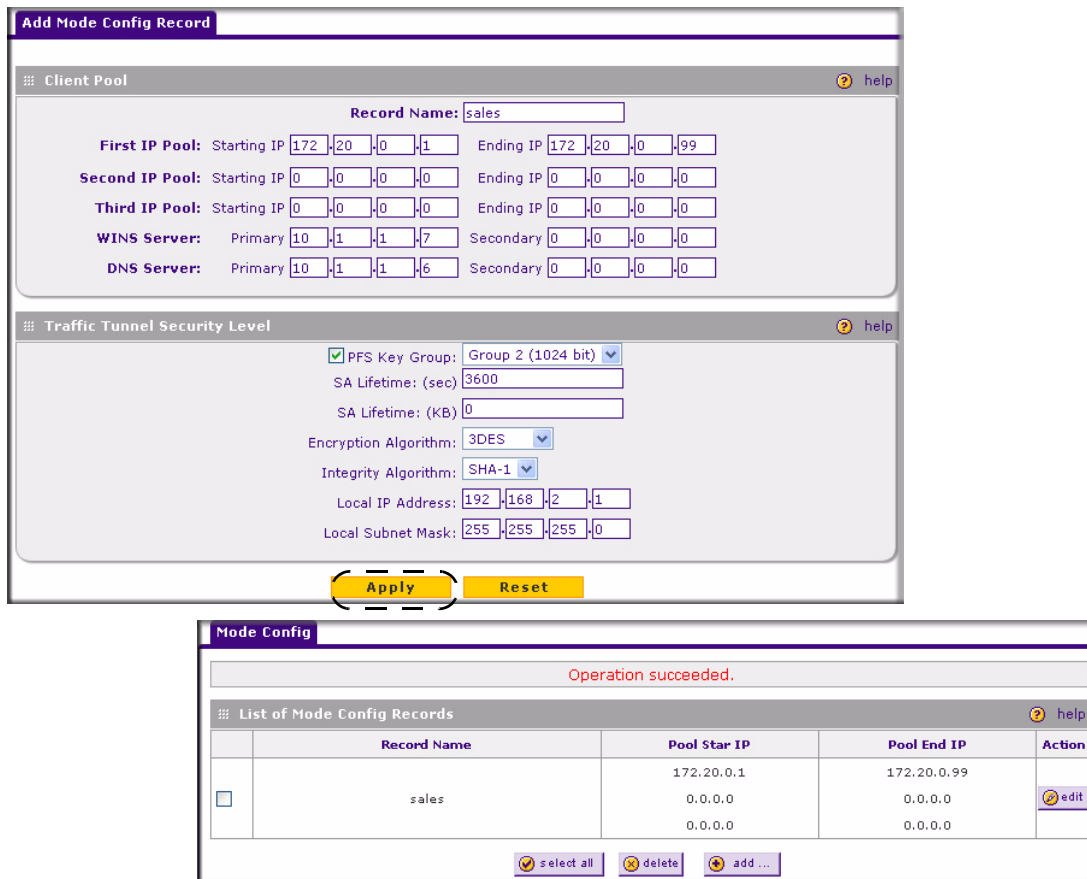
Figure 5-23

To configure an IKE Policy:

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

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

3. Enable **Mode Config** by checking the **Yes** radio box and selecting the Mode Config record you just created from the pull-down menu. (You can view the parameters of the selected record by clicking the **View selected** radio box.)

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

4. In the **General** section:

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

   b. Set Direction/Type to Responder.

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

5. For Local information:

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

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

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

   • Encryption Algorithm: 3DES

   • Authentication Algorithm: SHA-1

   • Diffie-Hellman: Group 2

   • SA Lifetime: 3600 seconds

7. Enter a Pre-Shared Key that will also be configured in the VPN client.

8. XAUTH is disabled by default. To enable XAUTH, select:

   • **Edge Device** to use this router as a VPN concentrator where one or more gateway tunnels terminate. (If selected, you must specify the **Authentication Type** to be used in verifying credentials of the remote VPN gateways.)

   • **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).

9. If Edge Device was enabled, select the **Authentication Type** from the pull down menu which will be used to verify account information: User Database, RADIUS-CHAP or RADIUS-PAP. Users must be added through the User Database screen (see "User Database Configuration" on page 5-29 or "RADIUS Client Configuration" on page 5-30).

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

10. Click **Apply.** The new policy will appear in the IKE Policies Table (a sample policy is shown below)
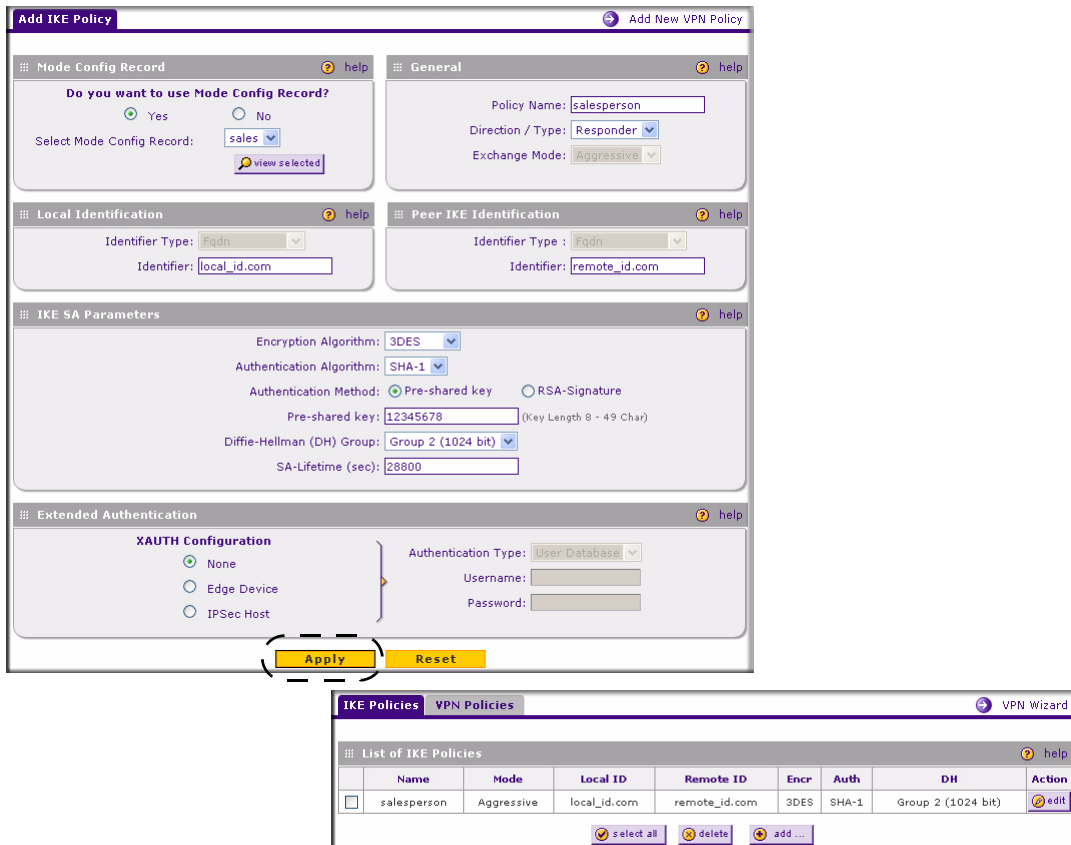
Figure 5-24

Configuring the ProSafe VPN Client for ModeConfig

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

To configure the client PC:

1. Right-click the VPN client icon in the Windows toolbar. In the upper left of the Policy Editor window, click the New Policy editor icon.

a. Give the connection a descriptive name such as "modecfg_test" (this name will only be used internally).

b. From the ID Type pull-down menu, select IP Subnet.

c. Enter the IP Subnet and Mask of the ProSafe DGFV338 (this is the LAN network IP address of the gateway).

d. Check the Connect using radio button and select Secure Gateway Tunnel from the pull-down menu.

e. From the ID Type pull-down menu, select Domain name and enter the FQDN of the ProSafe DGFV338; in this example it is "local_id.com".

f. Select Gateway IP Address from the second pull-down menu and enter the WAN IP address of the ProSafe DGFV338; in this example it is "172.21.4.1".
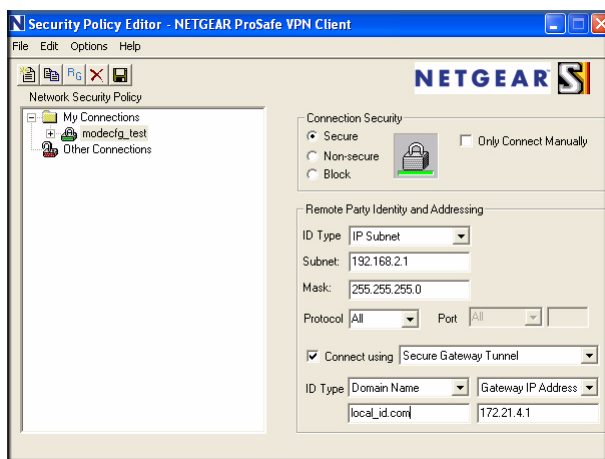
Figure 5-25

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 DGFV338 IKE menu.

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

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

Virtual Private Networking   5-37

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

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

e. Select your Internet Interface adapter from the Name pull-down menu.
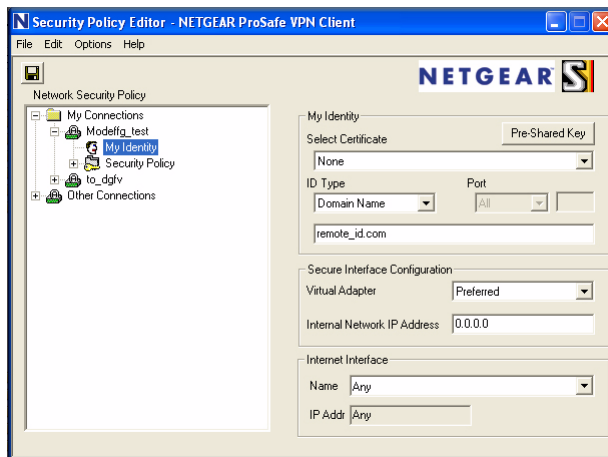
Figure 5-26

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

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

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

   c. Enable Replay Detection should be checked.

4. Click on Authentication (Phase 1) on the left-side of the menu and select Proposal 1. Enter the Authentication values to match those in the ProSafe DGFV338 ModeConfig Record menu.
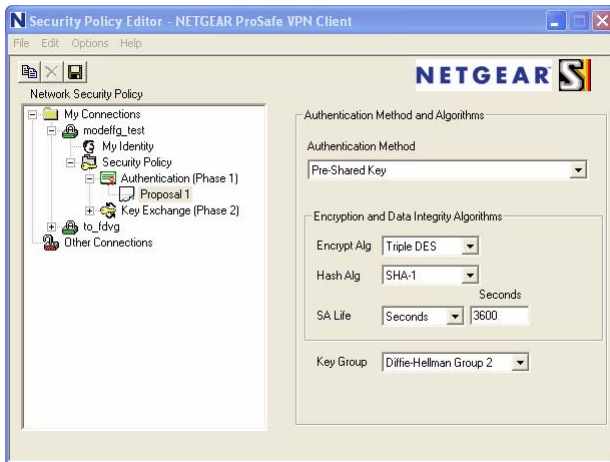
Figure 5-27

5. Click on Key Exchange (Phase 2) on the left-side of the menu and select Proposal 1. Enter the values to match your configuration of the ProSafe DGFV338 ModeConfig Record menu. (The SA Lifetime can be longer, such as 8 hours (28800 seconds)).
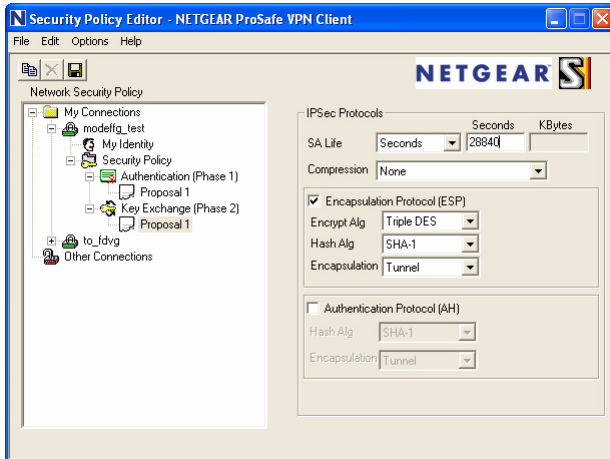
Figure 5-28

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

To test the connection:

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

2. Click on the connection. Within 30 seconds the message "Successfully connected to MyConnections/modecfg_test will display and the VPN client icon in the toolbar will read "On".

3. From the client PC, ping a computer on the ProSafe DGFV338 LAN.

.

Chapter 6
Router and Network Management

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

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

Performance Management

Performance management consists of controlling the traffic through the ProSafe DGFV338 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 ProSafe DGFV338 has the necessary features and tools to help the network manager accomplish these goals.

Wireless Firewall Features That Reduce Traffic

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

• Service blocking

• Block sites

• Source MAC filtering

Service Blocking

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

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

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

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

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

- **LAN users**. These settings determine which computers on your network are affected by this rule. Select the desired options:
    - Any: All PCs and devices on your LAN.
    - Single address: The rule will be applied to the address of a particular PC.
    - Address range: The rule is applied to a range of addresses.
    - Groups: The rule is applied to a Group. You use the Network Database to assign PCs to Groups (see "Groups and Hosts" on page 6-3).

- **WAN Users**. These settings determine which Internet locations are covered by the rule, based on their IP address.
    - Any: The rule applies to all Internet IP address.
    - Single address: The rule applies to a single Internet IP address.
    - Address range: The rule is applied to a range of Internet IP addresses.

- **Services**. You can specify the desired Services or applications to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see "Services" on page 6-3).

- **Schedule**. You can specify whether the rule is to be applied on the Schedule 1, Schedule 2, or Schedule 3 time schedule (see "Schedule" on page 6-3).

See "Using Rules to Block or Allow Specific Kinds of Traffic" on page 4-1 for the procedure on how to use this feature.

Services. The Rules menu contains a list of predefined Services for creating firewall rules. If a service does not appear in the predefined Services list, you can define the service. The new service will then appear in the Rules menu's Services list. See "Quality of Service (QoS) Priorities" on page 4-19 for the procedure on how to use this feature.

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

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

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

See "Managing Groups and Hosts" on page 4-21 for the procedure on how to use this feature.

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

See "Setting a Schedule to Block or Allow Specific Traffic" on page 4-31 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 wireless firewall 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 wireless 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" on page 4-24 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 "To block keywords or Internet domains:" on page 4-27 for the procedure on how to use this feature.

Wireless Firewall Features That Increase Traffic

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

• Port forwarding
• Port triggering
• VPN tunnels

Port Forwarding

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

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

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

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

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

You can also enable a check on special rules:

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

- Drop fragmented IP packets – Enable this to drop the fragmented IP packets.

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

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

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

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

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

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

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

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

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

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

- **Destination Address.** These settings determine the destination IP address for this rule which will be applicable to incoming traffic. This rule is applied only when the destination IP address of the incoming packet matches the IP address of the selected WAN interface or the specific IP address entered in this field. Selecting ANY enables the rule for any IP in the destination field.

- **Services**. You can specify the desired Services or applications to be covered by this rule. If the desired service or application does not appear in the list, you must define it using the Services menu (see "Services" on page 6-3).

- **Schedule**. You can specify whether the rule is to be applied on the Schedule 1, Schedule 2, or Schedule 3 time schedule (see "Schedule" on page 6-3).

See "Using Rules to Block or Allow Specific Kinds of Traffic" on page 4-1 for the procedure on how to use this feature.

Port Triggering

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

Once configured, operation is as follows:

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

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

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

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

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

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

See "Setting up Port Triggering" on page 4-28 for the procedure on how to use this feature.

VPN Tunnels

The wireless firewall permits up to 50 VPN tunnels at a time. Each tunnel requires extensive processing for encryption and authentication.

See Chapter 5, "Virtual Private Networking" for the procedure on how to use this feature.

Using QoS to Shift the Traffic Mix

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

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

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

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

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

See "Quality of Service (QoS) Priorities" on page 4-19 for the procedure on how to use this feature.

Tools for Traffic Management

The ProSafe Wireless ADSL Modem VPN Firewall Router includes several tools that can be used to monitor the traffic conditions of the firewall and control who has access to the Internet and the types of traffic they are allowed to have. See "Monitoring" on page 6-12 for a discussion of the tools.

Administrator and Guest Access Authorization

You can change the administrator and guest passwords, administrator login time-out, and enable remote management. Administrator access is read/write and guest access is read-only.

Changing the Passwords and Login Time-out

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

To change the password:

1. Select **Administration** from the main menu and **Set Password** from the submenu. The **Set Password** screen will display.

2. Enter a **New User Name** if desired.

> **Note:** You can change the Administrator account name; however, you cannot change it to "root", as this is a Telnet account that already exists on the system.
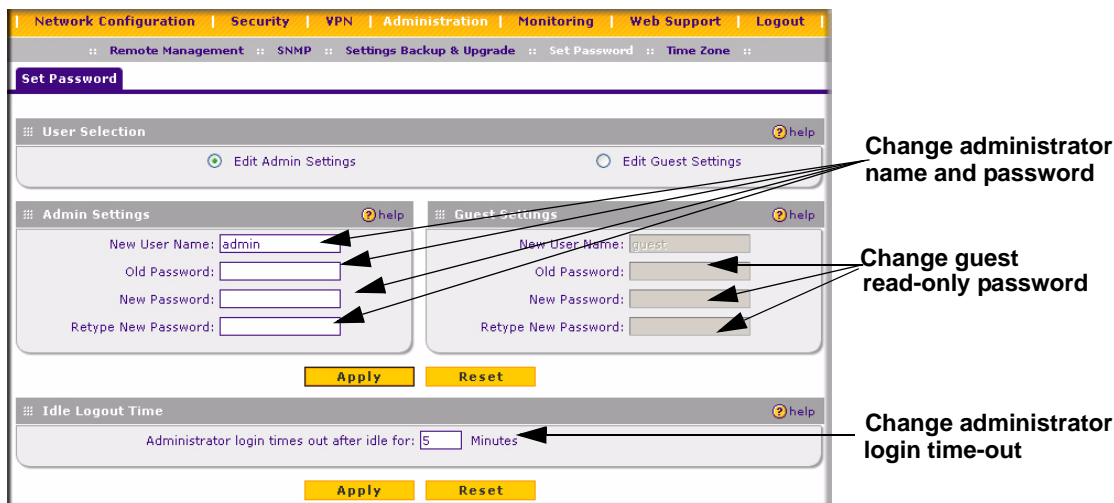
Figure 6-1

3. First enter the old password, and then enter the new password—twice. Click **Apply**.

4. Change the login idle time-out by changing the number of minutes. Click **Apply**.

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

The password and time-out values you entered will revert back to **password** and **5** minutes, respectively, after a factory default reset.

Enabling Remote Management Access

Using the Remote Management page, you can allow an administrator on the Internet to configure, upgrade, and check the status of your ProSafe DGFV338. You must be logged in locally to enable remote management (see "Logging in and Configuring your Internet Connection" on page 2-3).

> → **Note:** Be sure to change the firewall default configuration password to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both upper and lower case), numbers, and symbols. Your password can be up to 30 characters. See "Changing the Passwords and Login Time-out" on page 6-7 for the procedure on how to do this.

Figure 7.2 shows the Remote Management screen that is invoked when you select Remote Management under Management on the main menu.
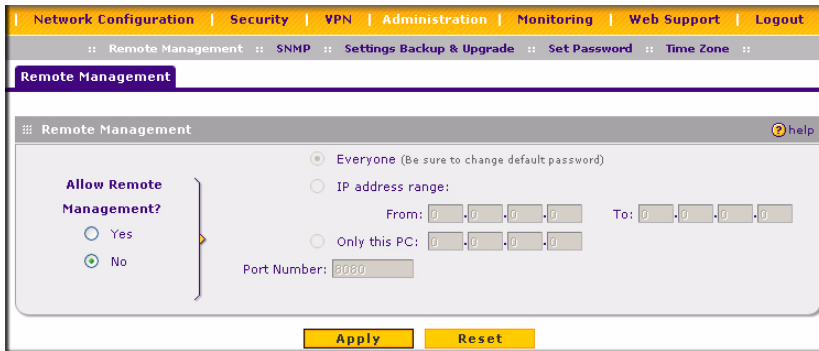
Figure 6-2

To configure your firewall for Remote Management:

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

2. Under **Allow Remote Management,** check the **Yes** radio box.

3. Specify which external addresses will be allowed to access the firewall's remote management.

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

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

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

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

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

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

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

When accessing your firewall from the Internet, the Secure Sockets Layer (SSL) will be enabled. Enter *https:// and* type your firewall WAN IP address into your browser, followed by a colon (:) and the custom port number. For example, if your WAN IP address is 172.21.4.1 and you use port number 8080, type the following in your browser:

https://172.21.4.1:8080

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

If you do not use the SSL *https://address*, but rather use *http://address*, the DGFV338 will automatically attempt to redirect to the *https://address*.

> **Note:** The first time you remotely connect the DGFV338 with a browser via SSL, you may receive a message regarding the SSL certificate. If you are using a Windows computer with Internet Explorer 5.5 or higher, simply click Yes to accept the certificate.

> **Tip:** If you are using a dynamic DNS service such as TZO, you can always identify the IP address of your DGFV338 by running `tracert` from the Windows Start menu Run option. For example, `tracert your DGFV338.mynetgear.net` and you will see the IP address your ISP assigned to the DGFV338.

Command Line Interface

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

You can access the command line interface (CLI) either by using telnet or by connecting a terminal to the console port on the front of the unit.

To access the CLI from a communications terminal when the ProSafe DGFV338 is still set to its factory defaults (or use your own settings if you have changed them), do the following:

1. From the 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).

> **Note:** No password protection exists when using the console port to access the unit.

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.

Event Alerts

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

Traffic Limits Reached

Figure 6-3 shows the **Internet Traffic** screen that is invoked by clicking **Internet Traffic** under **WAN Setup** on the Main Menu bar. The ADSL and Ethernet ports are programmed separately. A WAN port shuts down once its traffic limit is reached when this feature is enabled.

Each WAN port is programmed separately.

WAN port shuts down once the traffic limit is reached. An email alert can be sent when this shutdown happens.
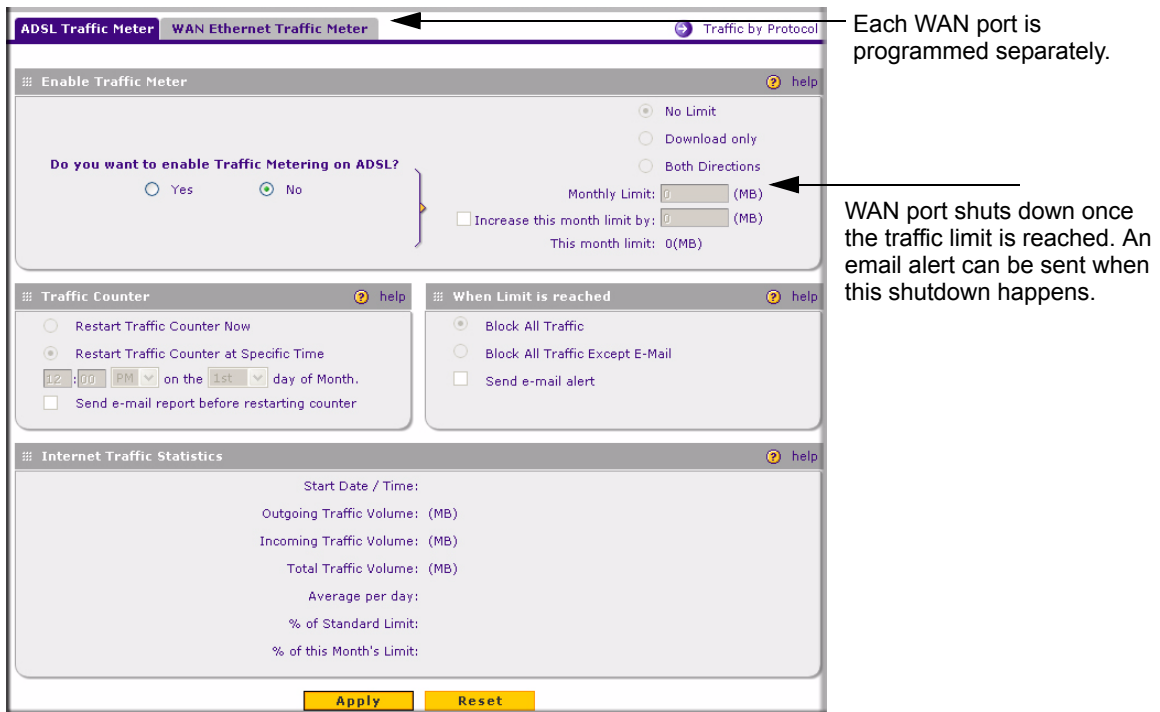
Figure 6-3

Monitoring

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

Router Status

The Router Status menu provides status and usage information on the LAN port, the ADSL configuration and the Ethernet configuration. From the main menu of the browser interface under Management, select Router Status to view this screen.
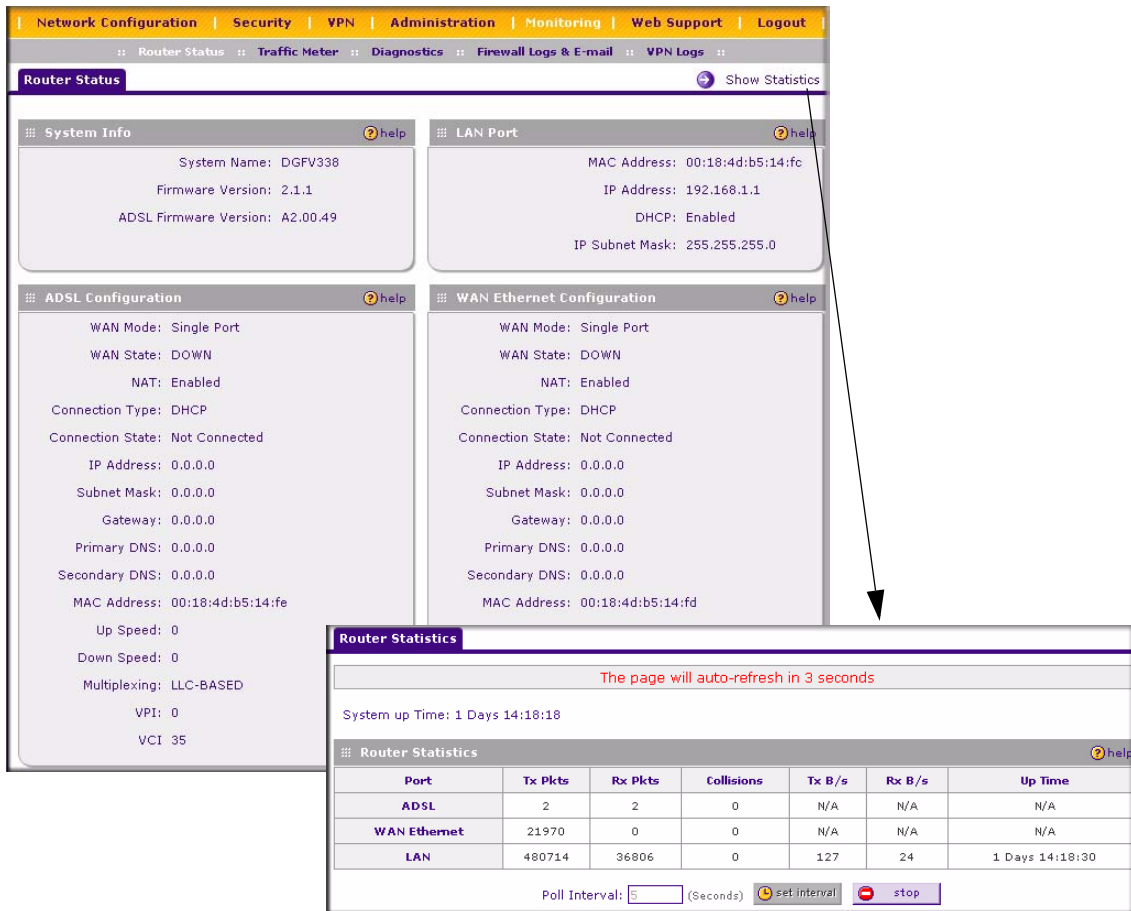
Figure 6-4

Table 6-1. Router Status

Item	Description
System Name	This is the Account Name that you entered in the Basic Settings page.
Firmware Version	This is the current software the router is using. This will change if you upgrade your router.

Table 6-1.   Router Status (continued)

Item	Description
LAN Port Information	These are the current settings for MAC address, IP address, DHCP role and Subnet Mask that you set in the LAN IP Setup page. DHCP can be either Server or None.
WAN Port Information	This indicates whether rollover mode is enabled and which LAN connection is primary and which is secondary. It also notes whether NAT is Enabled or Disabled; displays the current settings for MAC address, IP address, DHCP role and Subnet Mask that you set in the Basic Settings page. DHCP can be either Client or None.

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

WAN Ports

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

To monitor each WAN Port connection status:

1. Select **Network Configuration** from the main menu, **WAN Setup** from the submenu and click either the ADSL ISP Settings or the Ethernet ISP Settings tab. Then select the l. The ISP settings screen for the selected settings will display.

2. Click either the **Ethernet Status** or **ADSL Status** link. The current connection status for the selected connection will display.
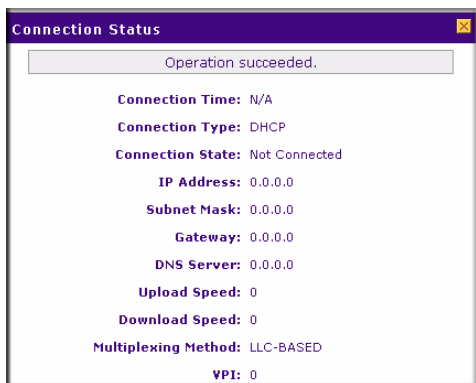
Figure 6-5

To check Dynamic DNS status:

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

2. Check the DNS provider radio box on the WAN port for which you have service.

3. Click the link at the top of the page for the dynamic DNS service you want to access. Click **Show Status.** The Status screen for the selected service will display.

Internet Traffic

The Internet Traffic screen provides the following information:

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

- Traffic by Protocol – Clicking Traffic by Protocol will show more details of the Internet Traffic. The volume of traffic for each protocol will be displayed in a sub-window. Traffic counters are updated in MBytes scale and the counter starts only when traffic passed is at least 1 MB
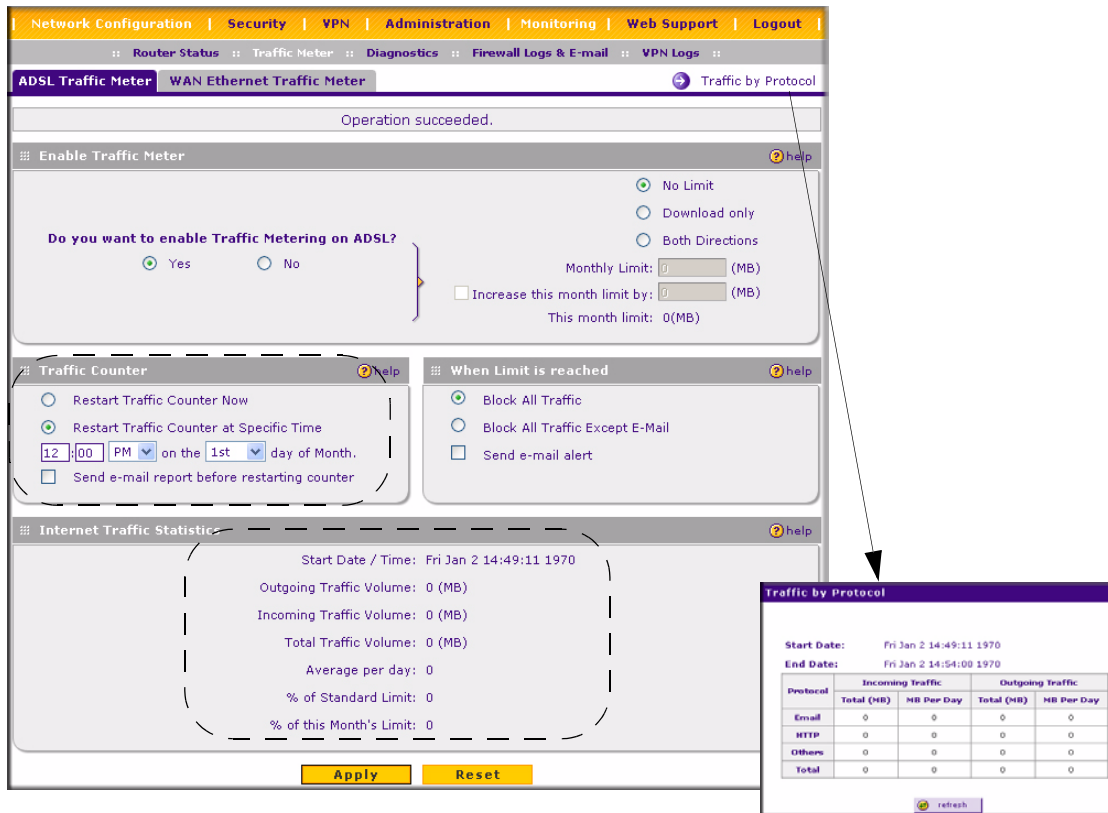
Figure 6-6

LAN Ports and Attached Devices

Known PCs and Devices

The Known PCs and Devices table contains a table of all IP devices that the firewall has discovered on the local network. This screen is accessible from the **Administration** main menu and the **LAN Groups** submenu. The Groups and Hosts screen will display showing the Known PCs and Devices table shown below:.

Figure 6-7

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

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

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

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

Table 6-2. Known PCs and Devices table

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

Note: If the firewall is rebooted, the table data is lost until the firewall rediscovers the devices. To force the firewall to look for attached devices, click the Refresh button.

DHCP Log

The **DHCP Log** is accessible from the **DHCP Log** link on the **LAN Setup** screen, located under **Network Configuration** on the main menu.
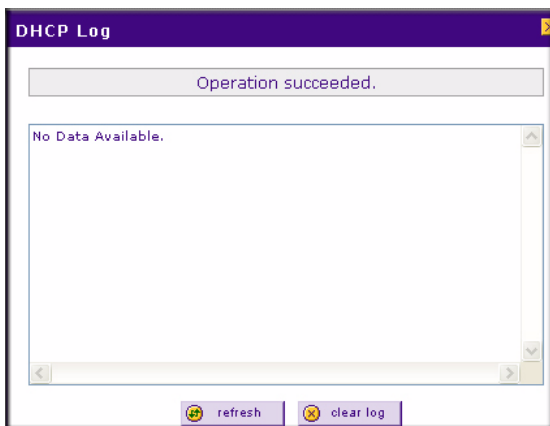
Figure 6-8

Port Triggering Status

The **Port Triggering Status** screen is available from the **Port Triggering** screen accessible under **Security** on the main menu. Only one PC can use a Port Triggering application at any time. When the PC has finished using the application, a time-out period occurs before another PC can use the Port triggering. You can check status using the Port Triggering Status screen. For a description of the fields, see the following field descriptions in Table 6-3.
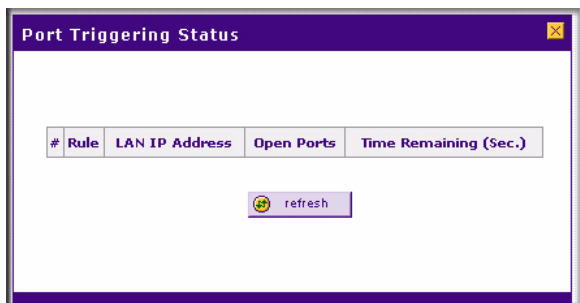
Figure 6-9

Table 6-3.   Port Triggering Status data

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

Firewall Security

A log of the firewall activities can be viewed, saved to a syslog server, and sent to an email address.

Figure 6-10 shows the **Log** screen that is invoked by clicking **Logs and Email** under **Security** on the Main Menu bar.
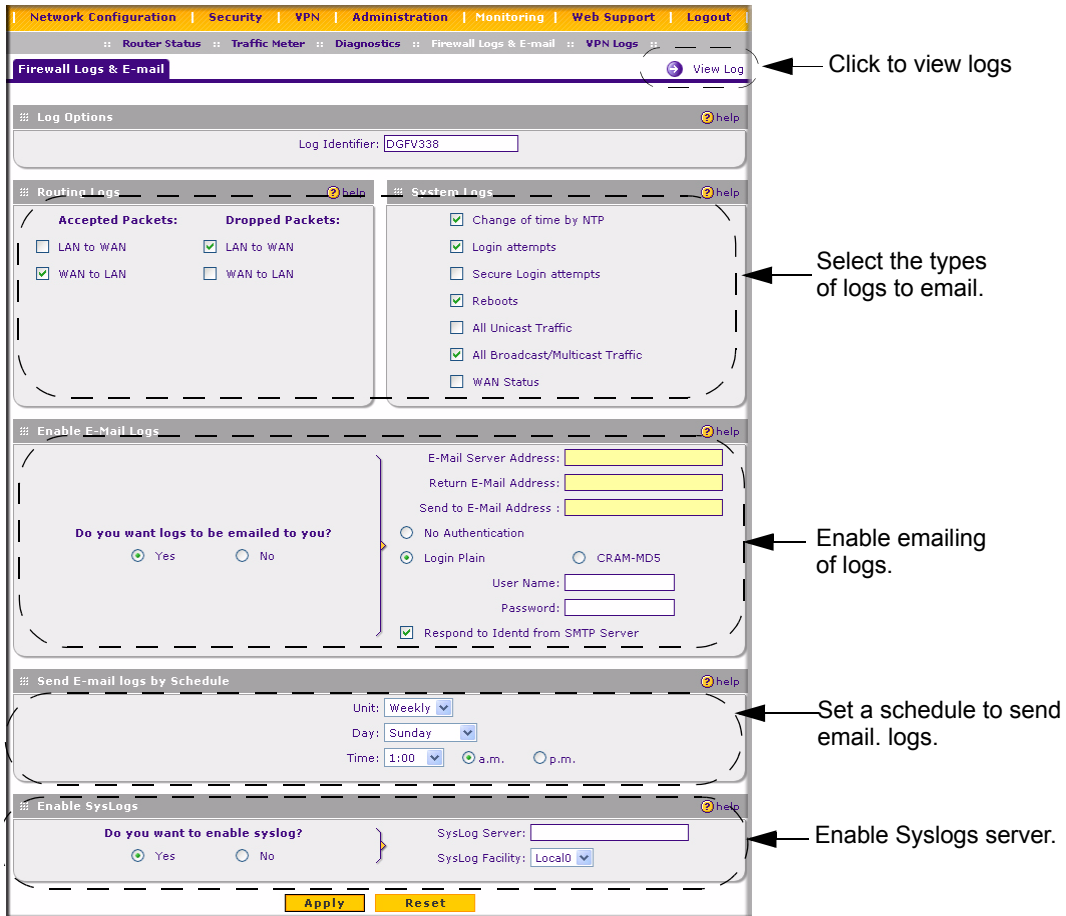
Figure 6-10

To invoke the Log screen, click the **View Log** link on the Logs and E-mail screen.
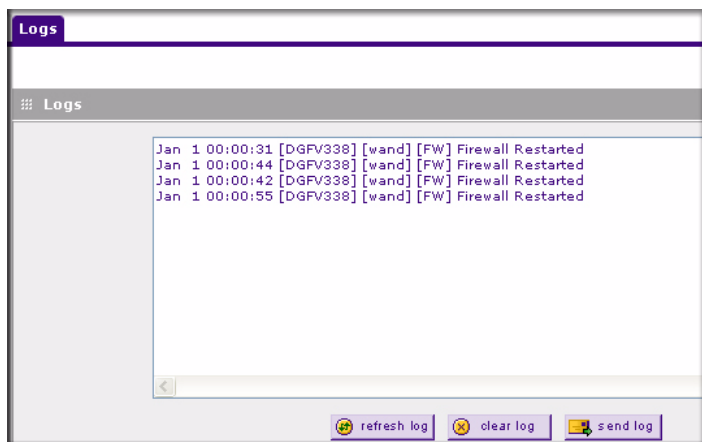
Figure 6-11

VPN Tunnels

You can view the VPN Logs by selecting **Monitoring** on the main menu and **VPN Logs** on the submenu. The VPN Logs screen displays the log contents generated by all VPN policies.

• Click **Refresh** to view entries made after this screen was invoked.

• Click **Clear Log** to delete all entries.
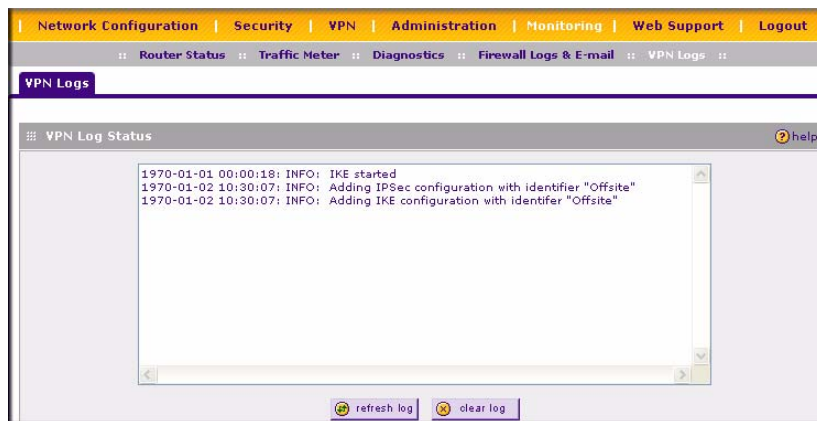
Figure 6-12

Select **VPN** from the main menu and **Connection Status** from the submenu to display the status of IPSec connections. You can change the status of a connection; to either establish or drop the Security Association (SA). Clicking on the VPN Status will show the IPSec Connection status of each VPN tunnel. The field descriptions for the data in the IPSec Connection Status table are in the following Table 6-4.
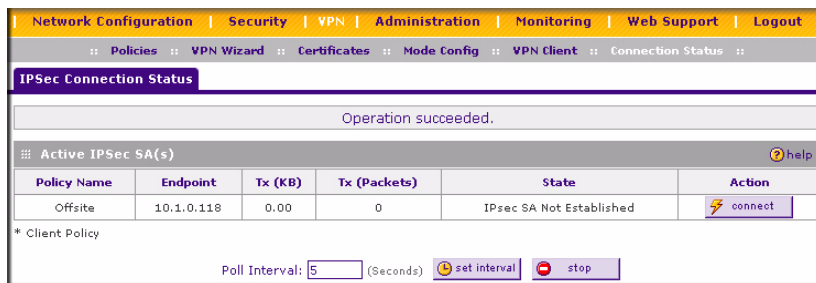
Figure 6-13

Table 6-4.   VPN Status Data

Item	Description
Policy Name	The name of the VPN policy associated with this SA.
Endpoint	The IP address on the remote VPN Endpoint.
Tx (KBytes)	The amount of data transmitted over this SA.
Tx (Packets)	The number of packets transmitted over the SA.
State	The current status of the SA for IKE Policies. The status can be either Not Connected or IPSec SA Established.
Action	Click **Connect** to build the SA (connection) or **Drop** to terminate the SA (connection).
Poll Interval	Time, in seconds, after which this screen will automatically reload.
Set Interval	Enter a new value in the Poll Interval field and click Set Interval to set a new interval value.
Stop	Disables the automatic page refresh feature.

Using a SNMP Manager

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

The SNMP Configuration table lists the SNMP configurations by:

- **IP Address**: The IP address of the SNMP manager.

- **Port**: The trap port of the configuration.

- **Community**: The trap community string of the configuration.

To create a new SNMP configuration entry:

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

2. Under **Create New SNMP Configuration Entry,** enter the IP Address of the SNMP manager in the **IP Address** field and the Subnet Mask in the **Subnet Mask** field.

   - If you want to allow only the host address to access the wireless firewall and receive traps (for example, see Figure 6-14), enter an IP Address of, for example, 192.168.1.100 with a Subnet Mask of 255.255.255.**255**.

   - If you want to allow a subnet access to the wireless firewall through SNMP, enter an IP address of, for example,192.168.1.100 with a Subnet Mask of 255.255.255.**0**. The traps will still be received on 192.168.1.100, but the entire subnet will have access through the community string.

   - If you want to make the wireless firewall globally accessible using the community string, but still receive traps on the host, enter 0.0.0.0 as the Subnet Mask and an IP Address for where the traps will be received.

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

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

5. Click **Add** to create the new configuration. The entry will display in the **SNMP Configuration** table.

6. Click **Edit** in the **Action** column adjacent to the entry to modify or change the selected configuration.
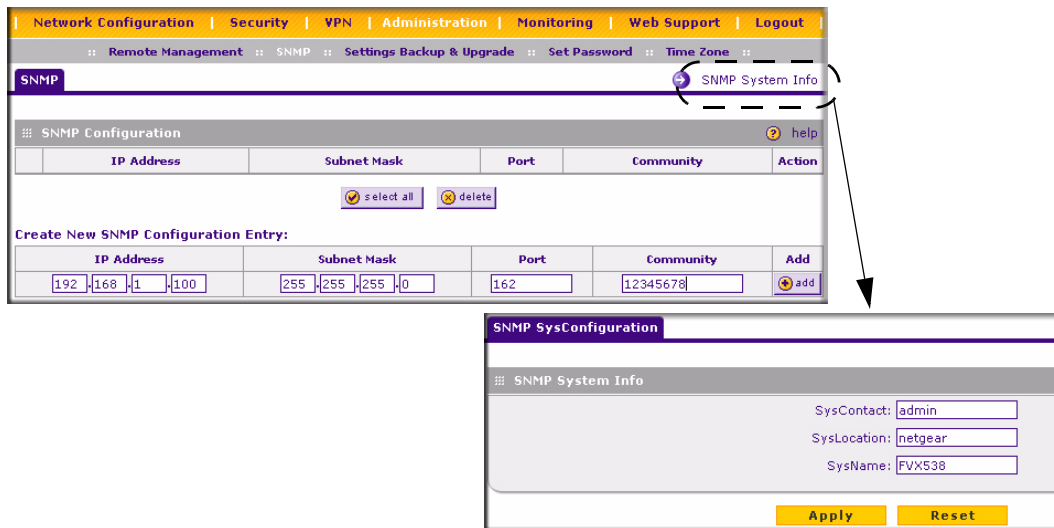
Figure 6-14

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

To modify the SNMP System contact information:

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

2. Modify any of the contact information that you want the SNMP Manager to use.

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

Diagnostics

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

> **Note:** For normal operation, diagnostics are not required

Select **Monitoring** from the main menu and **Diagnostics** from the submenu. The Diagnostics screen will display.
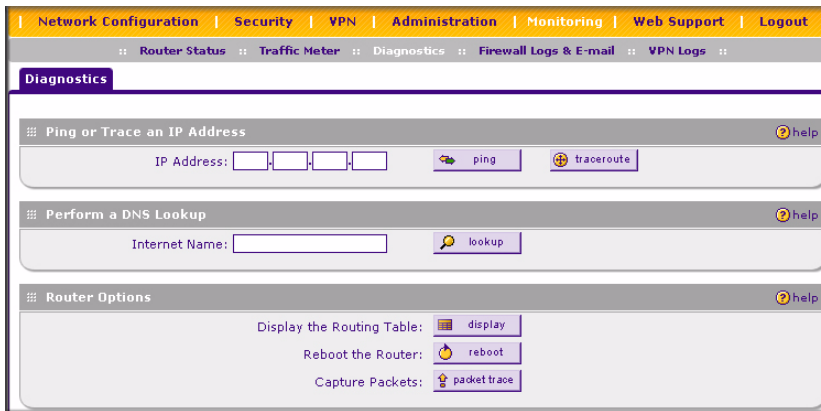
Figure 6-15

.The functionality of the each diagnostic tool is described in the following Table 6-5.

Table 6-5.   Diagnostics

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

Table 6-5. Diagnostics (continued)

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

Configuration File Management

The configuration settings of the ProSafe DGFV338 are stored within the firewall in a configuration file. This file can be saved (backed up) to a user's PC, retrieved (restored) from the user's PC, or cleared to factory default settings. You can also upgrade the firewall software with the latest version from NETGEAR.

Settings Backup and Firmware Upgrade

Once you have installed the wireless firewall and have it working properly, you should back up a copy of your setting so that it is if something goes wrong. When you backup the settings, they are saved as a file on your computer. You can then restore the wireless 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 wireless firewall firmware from a saved file on your hard disk to use a different firmware version.

Backup and Restore Settings

To backup and restore settings:

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

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

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

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

To restore settings from a backup file:

1. Click **Browse**. Locate and select the previously saved backup file (by default, netgear.cfg).

2. When you have located the file, click **restore**.

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

To reset the router to the original factory default settings:

Click **default**

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

> ⚠ **Warning:** When you click **default,** your router settings will be erased. All firewall rules, VPN policies, LAN/WAN settings and other settings will be lost. Please backup your settings if you intend on using them!
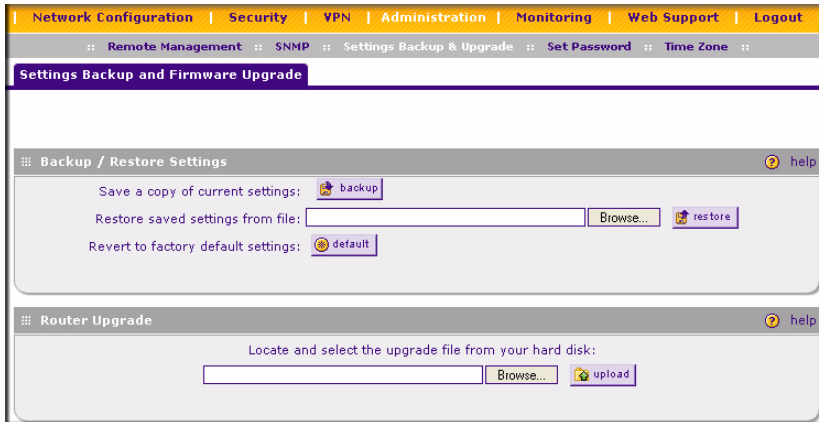
Figure 6-16

Router Upgrade

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

To download a firmware version:

1. Go to the NETGEAR Web site at *http://www.netgear.com/support* and click on **Downloads.**

2. From the **Product Selection** pull-down menu, select your product. Select the software version and follow the **To Install** steps to download your software.

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

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

To upgrade router software:

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

2. Click **Browse** in the **Router Upgrade** section.

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

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

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

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

Setting the Time Zone

Date, time and NTP Server designations can be input on the **Time Zone** screen. Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock times in a network of computers Select **Administration** from the main menu and **Time Zone** from the submenu. The **Time Zone** screen will display.

To set Time, Date and NTP servers:

1. From the **Date/Time** pull-down menu, select the Local Time Zone. This is required in order for scheduling to work correctly. The wireless firewall includes a Real-Time Clock (RTC), which it uses for scheduling.

2. If supported in your region, check the **Automatically Adjust for Daylight Savings Time** radio box.

3. Select a NTP Server option by checking one of the following radio boxes:

   • **Use Default NTP Servers**: If this is enabled, then the RTC (Real-Time Clock) is updated regularly by contacting a Default Netgear NTP Server on the Internet.

- **Use Custom NTP Servers**: If you prefer to use a particular NTP server, enable this instead and enter the name or IP address of an NTP Server in the **Server 1 Name/IP Address** field.

  If required, you can also enter the address of another NTP server in the **Server 2 Name/IP Address** field. If you select this option and leave either the Server 1 or Server 2 fields empty, they will be set to the Default Netgear NTP servers.

4. Click **Apply** to save your settings or click **Cancel** to revert to your previous settings.
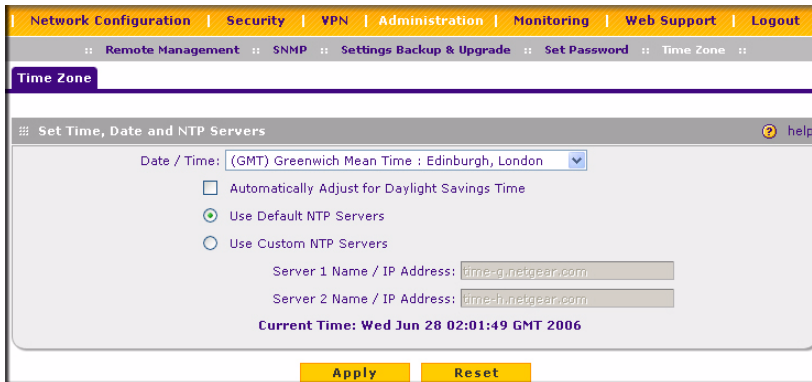
Figure 6-17

This chapter describes how to configure the advanced LAN features of your ProSafe Wireless ADSL Modem VPN Firewall Router. These features can be found by selecting Network Configuration from the primary menu and LAN Setup from the submenu of the browser interface.

Using the Firewall as a DHCP server

By default, the firewall will function as a DHCP (Dynamic Host Configuration Protocol) server, allowing it to provide an IP address, DNS server address, WINS Server address, and default gateway address 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.

For most applications, the default DHCP and TCP/IP settings of the firewall are satisfactory. See the link to "Preparing a Computer for Network Access" in Appendix B, "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).

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. These are advanced settings most usually configured by a network administrator.

To change the LAN IP services:

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

Figure 7-1

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

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

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

4. **DHCP** Server. By default, the router will function as a DHCP server, providing TCP/IP configuration for all computers connected to the router's LAN. If another device on your network will be the DHCP server, or if you will manually configure all devices, select the **Disable DHCP Server** radio button. If the **Enable DHCP Server** radio button is selected, complete the following fields:

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

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

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

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

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

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

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

Using Address Reservation

When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time it access the firewall's DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings
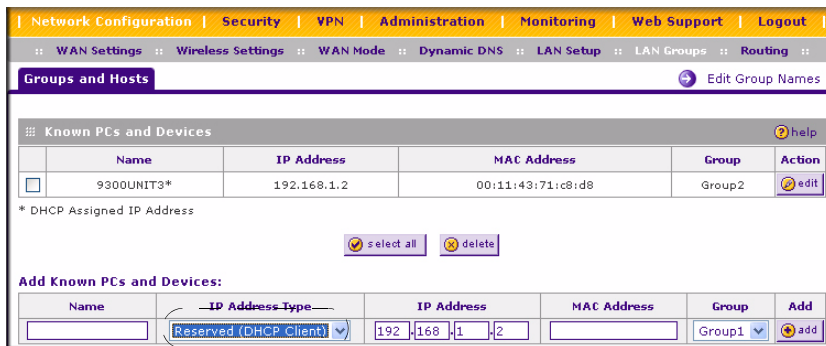
Figure 7-2

To reserve an IP address:

1. Select **Network Configuration** from the main menu and **LAN Groups** from the submenu. THe **Groups and Hosts** screen will display.

2. From the **IP Address Type** pull-down menu, select **Reserve** as the address type.

3. Fill in the remaining fields in the **Add Known PCs and Devices** table and click **Add.** The Reserved IP address will be added to your **Known PCs and Devices** table (see the Groups and Hosts Entry screen (see "Managing Groups and Hosts" on page 4-21).

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

Configuring Multi Home LAN IPs

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

- The **Available Secondary LAN IPs** table lists the secondary LAN IP addresses added to the router.

- The **IP Address** is the "alias" added to the LAN port of the router. This will be the gateway for computers that need to access the Internet.

- The **Subnet Mask** is the IPv4 Subnet Mask.

To add a secondary LAN IP address:

1. Enter the IP Address and the Subnet Mask in the respective fields of the **Add Secondary LAN IP Address** section.

2. Click **Add.** The new Secondary LAN IP address will appear in the **Available Secondary LAN IPs** table.

To delete any or all entries in the Available Secondary LAN IPs table:

1. Select the entries using one of the following methods:

    •   Click **Select all** to select all the entries in the table. All the radio buttons are selected.

    •   Check the individual radio button of each entry you want to delete.

2. Click **Delete** to delete the entries with checked radio buttons from the Available Secondary LAN IPs table.

To make changes to the selected entry:

1. Click **Edit** in the Action column adjacent to the selected entry. The **Edit Secondary LAN IP Setup** screen will display.

2. Modify the **IP Address** and **Subnet Mask** fields and click **Apply.**

3. Click **Reset** to discard any changes and revert to the previous settings.

> **Tip:** The Secondary LAN IP address will be assigned to the LAN interface of the router and can be used as a gateway by the secondary subnet.
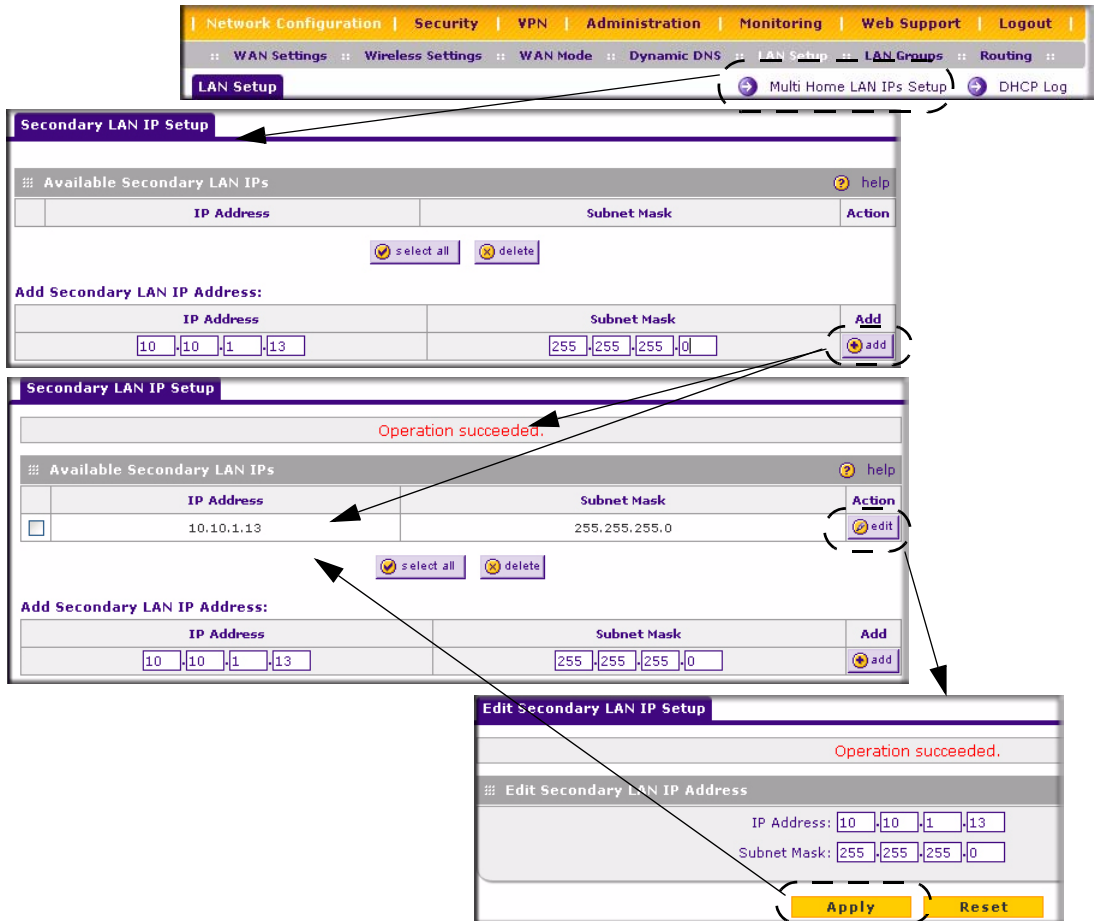
Figure 7-3

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

Configuring Static Routes

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

Adding or Editing a Static Route

To add or edit a static route:

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

2. Click **Add**. The **Add Static Route** menu, shown below, will display.

3. Enter a route name for this static route in the **Route Name** field (for identification and management).
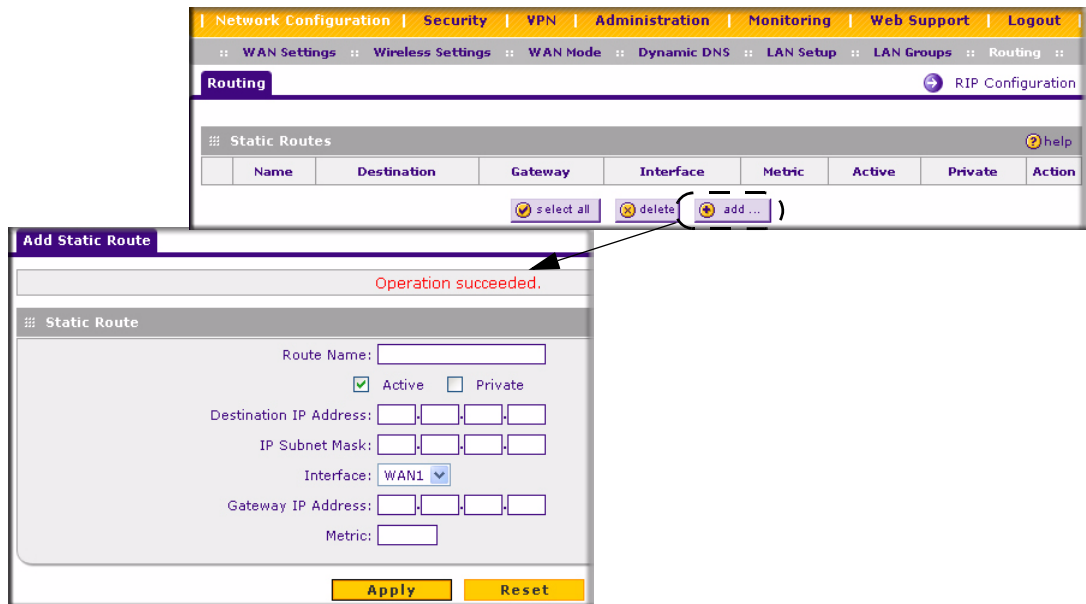
Figure 7-4

4. Select Active to make this route effective.

5. Select Private if you want to limit access to the LAN only. The private 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 Route table.

12. Click **Reset** to discard any changes and revert to the previous settings.

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

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** from the main menu and **Routing** from the submenu. When the **Routing** screen displays, click **RIP Configuration.** The **RIP Configuration** screen will display.

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

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

- **Both** – The router broadcasts its routing table and also processes RIP information received from other routers.

- **Out Only** – The router broadcasts its routing table periodically but does not accept RIP information from other routers.

- **In Only** – The router accepts RIP information from other routers, but does not broadcast its routing table.
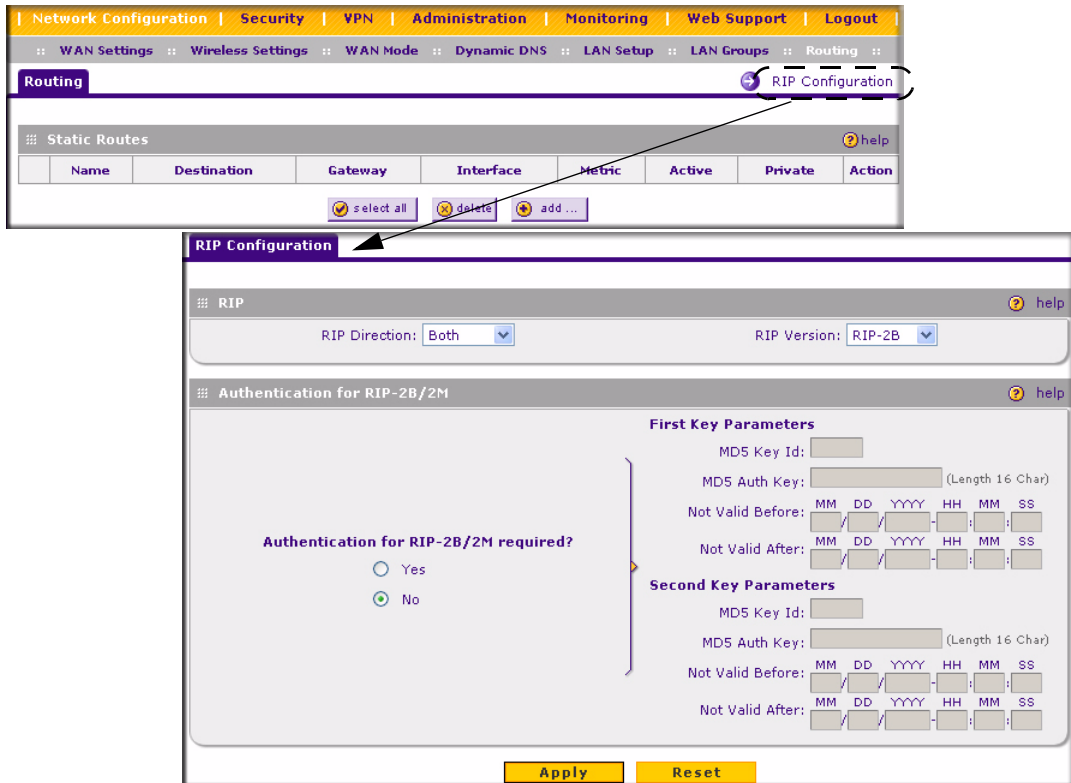
Figure 7-5

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

- **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.

4. Authentication for RIP2B/2M required? If you selected RIP-2B or RIP-2M, check the **YES** radio box to enable the feature, and input the **First Key Parameters** and **Second Key Parameters** MD-5 keys to authenticate between routers.

LAN Configuration 7-9

5. Click **Reset** to discard any changes and revert to the previous settings.

6. Click **Save** to save your settings.

Static Route Example

For example, you may require a static route if:

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

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

• Your company's network is 134.177.0.0.

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

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

In this example:

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

• The Gateway IP Address fields specifies that all traffic for these addresses should be forwarded to the ISDN firewall at 192.168.1.100.

• A Metric value of 1 will work since the ISDN firewall is on the LAN.

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

Enabling Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP) can improve the overall networking experience through automatic discovery and device interoperability. UPnP helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

By default, UPnP is disabled. When disabled, the router will not allow any device to automatically control the resources of the router; for example, port forwarding. When enabled, you must set the Advertisement Period and the Advertisement Time to Live according to the following criteria:

• **Advertisement Period**. Determines how often the router will advertise (broadcast) its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations will ensure that control points have current device status, but this can create additional network traffic. Longer durations may compromise the freshness of the device status but can significantly reduce network traffic.

• **Advertisement Time To Live**. The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. A hop is the number of steps allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it may be necessary to increase this value a little.

The UPnP Portmap Table shows IP addresses and other settings of UPnP devices that have accessed this wireless gateway. These settings are described in the following Portmap table.

Table 7-1.   UPnP Portmap Table settings

Settings	Description
Active	Yes or No indicates whether or not the port of the UPnP device that established a connection is currently active.
Protocol	The network protocol (for example, HTTP, FTP, etc.) that the device is using to connect to this wireless gateway.
Int. Port (Internal Port)	Which, if any, internal ports are opened by the UPnP device.
Ext. Port (External Port)	Which, if any, external ports are opened by the UPnP device.
IP Address	The IP address of the UPnP device that is accessing this gateway.
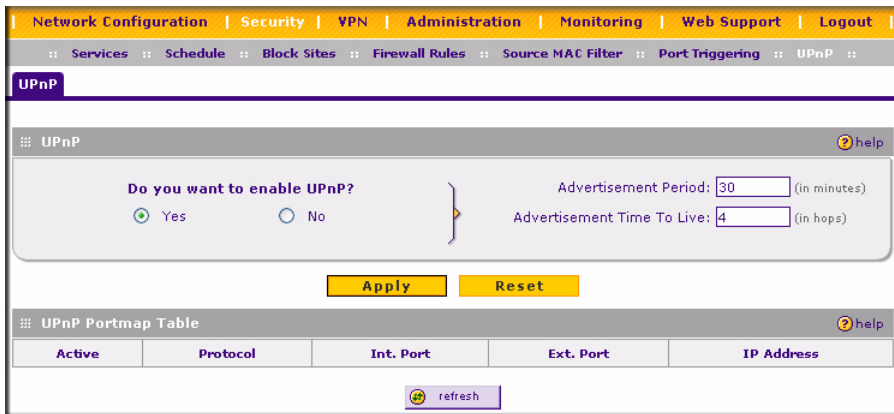
Figure 7-6

To turn on and set up UPnP:

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

2. Enable the UPnP radio by selecting the **Yes** radio box.

3. Modify the default **Advertisement Period** and **Advertisement Time to Live** settings, if desired. The defaults are 30 minutes and 4 hops, respectively.

4. Click **Apply** to save the new settings. Devices attached to the router can now use the router resources.

5. Click **Refresh** to update the Portmap table to show active ports currently opened by UPnP devices.

Chapter 8
Troubleshooting

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

Basic Functions

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

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

2. After approximately 60 to 90 seconds, verify that:

   a. The TEST LED is not lit.

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

   c. The Internet port LED is lit.

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

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

Power LED Not On

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

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

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

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

LEDs Never Turn Off

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

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

- Cycle the power to see if the firewall recovers.

- Clear the firewall's configuration to factory defaults. This will set the firewall's IP address to 192.168.1.1. This procedure is explained in "Restoring the Default Configuration and Password" on page 8-7.

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

LAN or Internet Port LEDs Not On

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

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

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

- Be sure you are using the correct cable:

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

Troubleshooting the Web Configuration Interface

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

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

- Check the PC's wireless settings and radio settings (if accessing the firewall using the wireless features). Also check the Network Authentication scheme.

- Make sure your PC's IP address is on the same subnet as the firewall. If you are using the recommended addressing scheme, your PC's address should be in the range of 192.168.1.2 to 192.168.1.254.

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

- If your firewall's IP address has been changed and you don't know the current IP address, clear the firewall's configuration to factory defaults. This will set the firewall's IP address to 192.168.1.1. This procedure is explained in "Restoring the Default Configuration and Password" on page 8-7.

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

- Try quitting the browser and launching it again.

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

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

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

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

Troubleshooting the ISP Connection

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

To check the WAN IP address:

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

---

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

3. Under the Management heading, select Router Status

4. Check that an IP address is shown for the ADSL or Ethernet WAN Port (whichever port you configured.)
If 0.0.0.0 is shown, your firewall has not obtained an IP address from your ISP.

If your firewall is unable to obtain an IP address from the ISP on the Ethernet port, you may need to force your cable or DSL modem to recognize your new firewall by performing the following procedure:

1. Turn off power to the cable or DSL modem.

2. Turn off power to your firewall.

3. Wait 5 minutes and reapply power to the cable or DSL modem.

4. When the modem's LEDs indicate that it has reacquired sync with the ISP, reapply power to your firewall.

If your firewall is unable to obtain an IP address from the ISP on the ADSL port, you may need to force your internal ADSL modem to recognize your new firewall by performing the following procedure:

1. Turn off power to your firewall.

2. Wait 5 minutes and reapply power to your firewall.

If your firewall is still unable to obtain an Ethernet IP address or an ADSL 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 a PPP over Ethernet (PPPoE) or some other type of login. (If ADSL, ask if they require either a PPPoE or a PPPoA login.)

• If your ISP requires a login, you may have incorrectly set the login name and password.

• Your ISP may check for your PC's host name.
Assign the PC Host Name of your ISP account as the Account Name in the Basic Settings menu.

• Your ISP only allows one Ethernet MAC address to connect to Internet, and may check for your PC's MAC address. In this case:

Inform your ISP that you have bought a new network device, and ask them to use the firewall's MAC address.

OR

Configure your firewall to spoof your PC's MAC address. This can be done in the Basic Settings menu. Refer to "Manually Configuring your ADSL Connection" on page 2-6 or "Manually Configuring your Ethernet Connection" on page 2-8.

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

- Your PC may not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. You may configure your PC manually with DNS addresses, as explained in your operating system documentation.

- Your PC may not have the firewall configured as its TCP/IP gateway.

Troubleshooting a TCP/IP Network Using a Ping Utility

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

Testing the LAN Path to Your Firewall

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

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

1. From the Windows toolbar, click on the Start button and select Run.

2. In the field provided, type Ping followed by the IP address of the firewall, as in this example:

   ping 192.168.1.1

3. Click on OK.

   You should see a message like this one:

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

   If the path is working, you see this message:

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

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

```
Request timed out
```

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

- Wrong physical connections
  - Make sure the LAN port LED is on. If the LED is off, follow the instructions in "LAN or Internet Port LEDs Not On" on page 8-2.
  - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and firewall.
- Wrong network configuration
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
  - Verify that the IP address for your firewall and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your PC to a Remote Device

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

PING -n 10 *<IP address>*

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

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

- Check that your PC has the IP address of your firewall listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC's Network Control Panel.
- Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- If configuring your Ethernet port, check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your PC, enter that host name as the Account Name in the Basic Settings menu.

- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your firewall to "clone" or "spoof" the MAC address from the authorized PC. Refer to "Manually Configuring your ADSL Connection" on page 2-6 or "Manually Configuring your Ethernet Connection" on page 2-8.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the firewall's administration password to **password** and the IP address to 192.168.1.1. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the firewall (see "Backup and Restore Settings" on page 6-26).
- Use the reset button on the rear panel of the firewall. Use this method for cases when the administration password or IP address is not known.

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

1. Press and hold the reset button until the Test LED turns on and begins to blink (about 10 seconds).

2. Release the reset button and wait for the firewall to reboot.

Problems with Date and Time

The E-Mail menu in the Content Filtering section displays the current date and time of day. The ProSafe DGFV338 uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000. Cause: The firewall has not yet successfully reached a Network Time Server. Check that your Internet access settings are configured correctly. If you have just completed configuring the firewall, wait at least five minutes and check the date and time again.

- Time is off by one hour. Cause: The firewall does not automatically sense Daylight Savings Time. In the E-Mail menu, check or uncheck the box marked "Adjust for Daylight Savings Time".

Appendix A
Default Settings and Technical Specifications

Default Factory Settings

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

- To perform a hard reset, push and hold the reset button for approximately 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. Default Configuration Settings

Feature		Default Behavior
Router Login		
	User Login URL	http://192.168.1.1
	User Name (case sensitive)	admin
	Login Password (case sensitive)	password
Internet Connection		
	WAN MAC Address (Ethernet)	Use Default address
	WAN MAC Address (ADSL)	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
	Gateway Address	0.0.0.0
	RIP Direction	None
	RIP Version	Disabled
	RIP Authentication	None

Table A-1. Default Configuration Settings (continued)

Feature		Default Behavior
	DHCP Server	Enabled
	DHCP Starting IP Address	192.168.1.2
	DHCP Ending IP Address	192.168.1.254
	UPnP	Disabled
	Time Zone	GMT
	Time Zone Adjusted for Daylight Saving Time	Disabled
	SNMP	Disabled
Firewall		
	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the http port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled
Wireless		
	Wireless Communication	Disaabled
	SSID Name	NETGEAR
	Security	Disabled
	Broadcast SSID	Enabled
	Transmission Speed	Auto[a]
	Country/Region	Auto
	RF Channel	11 until the region is selected
	Operating Mode	Auto
	Data Rate	Best

Table A-1. Default Configuration Settings (continued)

Feature		Default Behavior
	Output Power	Full
	Access Point	Disabled
	Authentication Type	Open System
	Wireless Card Access List	All wireless stations allowed

a. Maximum Wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

Technical Specifications

This appendix provides technical specifications for the ProSafe Wireless ADSL Modem VPN Firewall Router.

Table A-2. Technical Specifications

Specification		Description
Network Protocol and Standards Compatibility		
	Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP, PPP over Ethernet (PPPoE) PPP over ATM (PPPoA)
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:	9.92 x 7.1 x 1.57 in. (252 mm x 180 mm x 40 mm)
	Weight:	3.6 lbs. (1.63 kg)
	Environmental Specifications	
	Operating temperature:	0° to 40° C (32° to 104° F)
	Operating humidity:	90% maximum relative humidity, noncondensing

Table A-2. Technical Specifications

Specification		Description
Electromagnetic Emissions		
	Meets requirements of:	FCC Part 15 Class B
		VCCI Class B
		EN 55 022 (CISPR 22), Class B
Interface Specifications		
	LAN:	10BASE-T or 100BASE-Tx, RJ-45
	WAN:	10BASE-T or 100BASE-Tx or ADSL

Appendix B
Related Documents

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

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

Index

Numerics

B

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com