NETGEAR

ProSafe Wireless - 802.11 b/g/n VPN Firewall FVS318N

350 East Plumeria Drive
San Jose, CA 95134
USA

April 2011
202-10804-01
1.0

Technical Support

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

NETGEAR, INC. Support Information

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

Email: support@netgear.com

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

Trademarks

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

Statement of Conditions

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

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

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

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

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

EU Regulatory Compliance Statement

The ProSafe Wireless - 802.11 b/g/n VPN Firewall FVS318N is compliant with the following EU Council Directives: 89/336/EEC and LVD 73/23/EEC. Compliance is verified by testing to the following standards: EN55022 Class B, EN55024 and EN60950-1.

Visit the NETGEAR EU Declarations of Conformity website at:
http://kb.netgear.com/app/answers/detail/a_id/11621/sno/0

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.
This device complies with Part 15 of the 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.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.
Caution: Change/ modifications not approved by the manufacturer could void the user's authority to operate equipment.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das ProSafe Wireless - 802.11 b/g/n VPN Firewall FVS318N 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 - 802.11 b/g/n VPN Firewall FVS318N has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

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

Voluntary Control Council for Interference (VCCI) Statement

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

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

Read instructions for correct handling.

Additional Copyrights

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

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

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

Product and Publication Details

Model Number:	FVS318N
Publication Date:	April 2011
Product Family:	VPN Firewall
Product Name:	ProSafe Wireless - 802.11 b/g/n VPN Firewall FVS318N
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10837-01
Publication Version Number	1.0

1 Introduction

The ProSafe Wireless - 802.11 b/g/n VPN Firewall FVS318N with eight 10/100/1000 Mbps Gigabit Ethernet LAN ports and one 10/100/1000 Mbps Gigabit Ethernet WAN port connects your local area network (LAN) to the Internet through an external access device such as a cable modem or DSL modem.

The FVS318N is a complete security solution that protects your network from attacks and intrusions. For example, the FVS318N provides support for Stateful Packet Inspection, Denial of Service (DoS) attack protection and multi-NAT support. The VPN firewall supports multiple Web content filtering options, plus browsing activity reporting and instant alerts—both via email. Network administrators can establish restricted access policies based on time-of-day, website addresses and address keywords.

The FVS318N is a plug-and-play device that can be installed and configured within minutes.

This chapter contains the following sections:

- *Key Features* ” on this page
- “Package Contents” on page 1-10
- “VPN Firewall Front and Rear Panels” on page 1-10
- “Default IP Address, Login Name, and Password” on page 1-12
- “Qualified Web Browsers” on page 1-12

Key Features

The FVS318N provides the following features:

- One 10/100/1000 Mbps Ethernet WAN port for connection to a WAN device, such as a cable modem or DSL modem.
- Built-in eight-port 10/100/1000 Mbps Gigabit Ethernet LAN switch for extremely fast data transfer between local network resources.
- Support for up to 253 internal LAN users.
- Advanced VPN support for IPsec.
- SNMP Manageable, optimized for the NETGEAR ProSafe Network Management Software (NMS100).
- Easy, Web-based setup for installation and management.

- Advanced SPI Firewall and Multi-NAT support.
- Extensive Protocol Support.
- Login capability.
- One console port for local management.
- Front panel LEDs for easy monitoring of status and activity.
- Flash memory for firmware upgrade.

Advanced VPN Support for IPsec

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

IPsec VPN delivers full network access between a central office and branch offices, or between a central office and telecommuters. Remote access by telecommuters requires the installation of VPN client software on the remote computer.

- IPsec VPN with broad protocol support for secure connection to other IPsec gateways and clients.
- Bundled with a single-user license of the NETGEAR ProSafe VPN Client software (VPN01L)
- Supports 5 concurrent IPsec VPN tunnels.

A Powerful, True Firewall with Content Filtering

Unlike simple Internet sharing NAT routers, the FVS318N is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- DoS protection. Automatically detects and thwarts DoS attacks such as Ping of Death, SYN Flood, LAND Attack, and IP Spoofing.
- Secure Firewall. Blocks unwanted traffic from the Internet to your LAN.
- Block Sites. Blocks access from your LAN to Internet locations or services that you specify as off-limits.
- Logs security incidents. The FVS318N will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the VPN firewall to
  email the log to you at specified intervals. You can also configure the VPN firewall to send immediate alert messages to your email address or email pager whenever a significant event occurs.
- Keyword Filtering. With its URL keyword filtering feature, the FVS318N prevents objectionable content from reaching your PCs. The VPN firewall allows you to control access to Internet content by screening for keywords within Web addresses. You can configure the VPN firewall to log and report attempts to access objectionable Internet sites.

Security Features

The FVS318N is equipped with several features designed to maintain security, as described in this section.

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

Autosensing Ethernet Connections with Auto Uplink

With its internal 8-port 10/100/1000 Mbps switch and 10/100/1000 WAN port, the FVS318N can connect to either a 10 Mbps standard Ethernet network, a 100 Mbps Fast Ethernet network, or a 1000 Mbps Gigabit Ethernet network. The LAN and WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

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

Extensive Protocol Support

The FVS318N supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). For further information about TCP/IP, see the “TCP/IP Networking Basics” document that you can access from the link in “Related Documents” in Appendix C.

- IP Address Sharing by NAT. The VPN firewall allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as NAT, allows the use of an inexpensive single-user ISP account.
- Automatic Configuration of Attached PCs by DHCP. The VPN firewall dynamically assigns network configuration information, including IP, gateway, and domain name server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host

Configuration Protocol (DHCP). This feature greatly simplifies configuration of PCs on your local network.

- DNS Proxy. When DHCP is enabled and no DNS addresses are specified, the VPN firewall provides its own address as a DNS server to the attached PCs. The VPN firewall obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.
- PPP over Ethernet (PPPoE). PPPoE is a protocol for connecting remote hosts to the Internet over a DSL connection by simulating a dial-up connection. This feature eliminates the need to run a login program such as EnterNet or WinPOET on your PC.
- Quality of Service (QoS). QoS support for traffic prioritization.

Easy Installation and Management

You can install, configure, and operate the FVS318N within minutes after connecting it to the network. The following features simplify installation and management tasks:

- Browser-Based Management. Browser-based configuration allows you to easily configure your VPN firewall from almost any type of personal computer, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided and online help documentation is built into the browser-based Web Management Interface.
- Auto Detect. The VPN firewall automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- VPN Wizard. The VPN firewall includes the NETGEAR VPN Wizard to easily configure VPN tunnels according to the recommendations of the Virtual Private Network Consortium (VPNC) to ensure the VPN tunnels are interoperable with other VPNC-compliant VPN routers and clients.
- SNMP. The VPN firewall supports the Simple Network Management Protocol (SNMP) to let you monitor and manage log resources from an SNMP-compliant system manager. The SNMP system configuration lets you change the system variables for MIB2.
- Diagnostic Functions. The VPN firewall incorporates built-in diagnostic functions such as Ping, Trace Route, DNS lookup, and remote reboot.
- Remote Management. The VPN firewall allows you to login to the Web Management Interface from a remote location on the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses.
- Visual monitoring. The VPN firewall's front panel LEDs provide an easy way to monitor its status and activity.

Maintenance and Support

NETGEAR offers the following features to help you maximize your use of the FVS318N:

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

Package Contents

- The product package should contain the following items:
- ProSafe Wireless - 802.11 b/g/n VPN Firewall FVS318N
- AC power cable
- Rubber feet
- Category 5 (Cat5) Ethernet cable
- *ProSafe Gigabit 8 Port VPN Firewall FVS318N Installation Guide*
- *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 VPN firewall for repair.

VPN Firewall Front and Rear Panels

The FVS318N front panel includes eight LAN ports, one WAN port, and four groups of status indicator light-emitting diodes (LEDs), including Power and Test, LAN, and WAN LEDs.

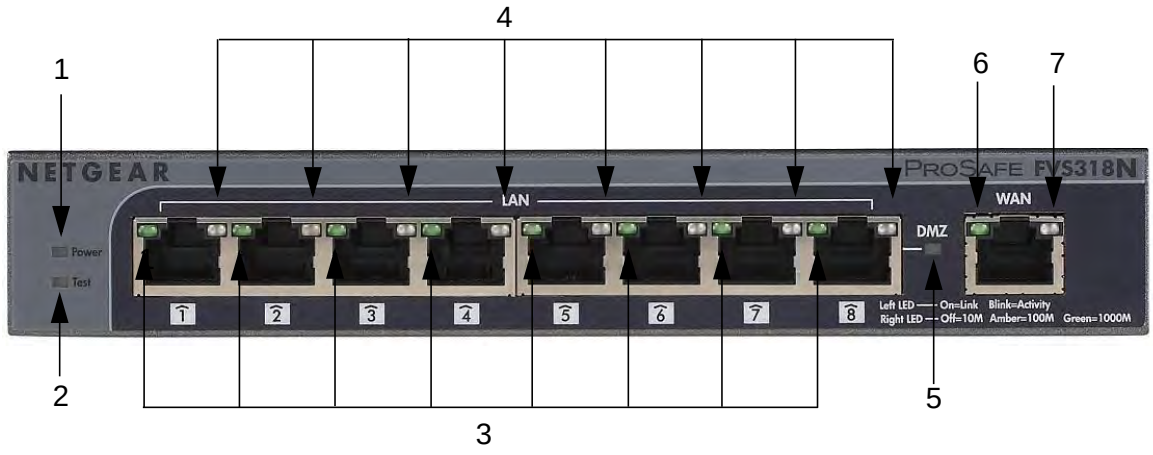

Figure 1-1

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

Table 1-1. LED Descriptions

Object	Activity	Description
1. Power	On (Green) Off	Power is supplied to the VPN firewall. Power is not supplied to the VPN firewall.
2. Test	On (Amber) Off	Test mode: The system is initializing or the initialization has failed. The system has booted successfully.
Eight LAN Ports		
3. Link and Activity (left side of port)	On (Green) Blinking (Green) Off	The port has detected a link with a connected Ethernet device. Data is being transmitted or received by the port. The port has no link.
4. Speed (right side of port)	On (Green) On (Amber) Off	The LAN port is operating at 1,000 Mbps. The LAN port is operating at 100 Mbps. The LAN port is operating at 10 Mbps.
5. DMZ	On (Green) Off	LAN port 8 is enabled as a DMZ port. LAN port 8 is not enabled as a DMZ port.
One WAN Port		
6. Active (left side of port)	On (Green) Off)	The WAN port is connected. The Internet connection is down The WAN port is either not enabled or has no link.
7. Speed (right side of port)	On (Green) On (Amber) Off	The port is operating at 1,000 Mbps. The port is operating at 100 Mbps. The port is operating at 10 Mbps.

The rear panel of the FVS318N includes a cable lock receptacle, a Factory Defaults button, and a DC power connection.

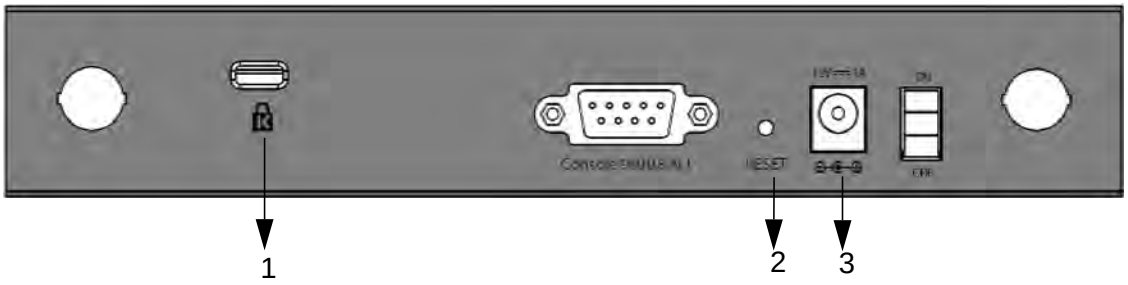

Figure 1-2

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

1. Cable security lock receptacle.
2. Factory Defaults button: Using a sharp object, press and hold this button for about ten seconds until the front panel TEST light flashes to reset the VPN firewall to factory default settings. All configuration settings will be lost and the default password will be restored.
3. DC power receptacle: 12V @ 1.0A.

Default IP Address, Login Name, and Password

Check the label on the bottom of the FVS318N's enclosure if you forget the following factory default information:

- IP Address: http://192.168.1.1
- User name: admin
- Password: password

When FVS318N is connected, log in by going to go to http://192.168.1.1. When the login

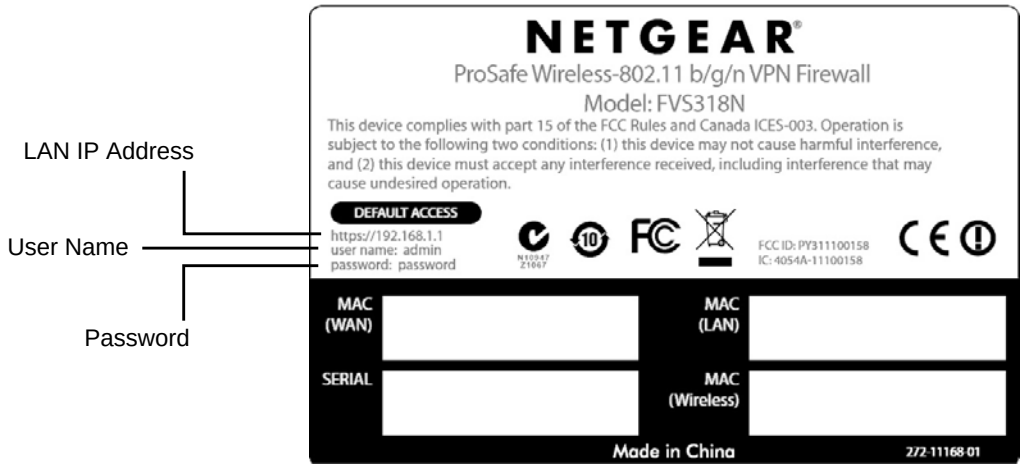

Figure 1-3

screen displays (see Figure 2-1 on page 2-2), enter admin for the user name and the password for password.

Qualified Web Browsers

To configure the FVS318N, you must use a Web browser such as Internet Explorer 5.1 or higher, Apple Safari 1.2 or higher, or Mozilla Firefox l.x Web browser with JavaScript, and cookies enabled.

Appendix A
Default Settings and Technical Specifications

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

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

Table A-1. VPN firewall Default Configuration Settings

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

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

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

Technical specifications for the ProSafe Gigabit 8 Port VPN Firewall FVS318N are listed in the following table.

Table A-2. VPN firewall Technical Specifications

Feature		Specifications
Network Protocol and Standards Compatibility		
	Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP PPP over Ethernet (PPPoE)
Power Adapter		
	North America:	120V, 60 Hz, input
	United Kingdom, Australia:	240V, 50 Hz, input
	Europe:	230V, 50 Hz, input
	Japan:	100V, 50/60 Hz, input
	All regions (output)	12 V DC @ 1.0 A output, 12 W maximum
Physical Specifications		
	Dimensions:	32 x 189 x 123 mm (1.6 x 10 x 7 in)
	Weight:	590 g (1.3 lb)

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

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