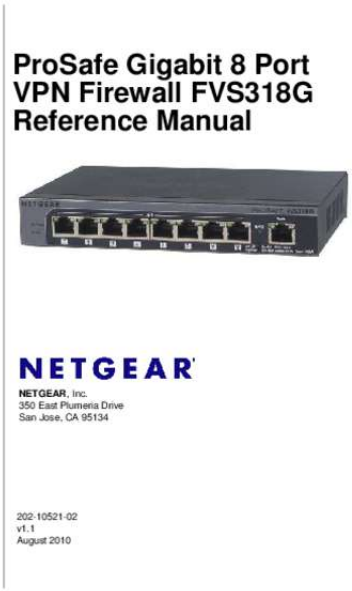

ProSafe Gigabit 8 Port
VPN Firewall FVS318G
Reference Manual

NETGEAR

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

202-10521-02
v1.1
August 2010

Manual abstract:

Support Information Phone: 1-888-NETGEAR, for US & Canada only. For other countries, see your Support information card. @@@@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: â□¢ â□¢ â□¢ â□¢ 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. Certificate of the Manufacturer/Importer It is hereby certified that the ProSafe Gigabit 8 Port VPN Firewall FVS318G 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. 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 holderâ□□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 â□□as isâ□□ with no express or implied warranties of correctness or fitness for purpose. 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: â□□This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www. The names â□□OpenSSL Toolkitâ□□ and â□□OpenSSL Projectâ□□ must not be used to endorse or promote products derived from this software without prior written permission. Products derived from this software may not be called â□□OpenSSLâ□□ nor may â□□OpenSSLâ□□ appear in their names without prior written permission of the OpenSSL Project. 6. Redistributions of any form whatsoever must retain the following acknowledgment: â□□This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www. This product includes cryptographic software written by Eric Young (eay@cryptsoft. com). This product includes software written by Tim Hudson (tjh@cryptsoft.

License to copy and use this software is granted provided that it is identified as the â□□RSA Data Security, Inc. MD5 Message-Digest Algorithmâ□□ 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 â□□derived from the 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 â□□as isâ□□ 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. 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. Interface of the zlib general purpose compression library version 1. This software is provided â□□as is,â□□ 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. The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files ftp://ds. 1-8 Chapter 2 Connecting the VPN Firewall to the Internet Understanding the Connection Steps .

4-22 Managing the Application Level Gateway for SIP Sessions . 4-42 Chapter 5 Virtual Private Networking Using the VPN Wizard for Client and Gateway Configurations . 5-39 Configuring the User Database for XAUTH . 5-45 Configuring the ProSafe VPN Client for ModeConfig . 7-5 Testing the Path from Your PC to a Remote Device . 1, August 2010 Contents About This Manual The NETGEARÂ® ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual describes how to install, configure and troubleshoot the ProSafe Gigabit 8 Port VPN Firewall FVS318G. The information in this manual is intended for readers with intermediate computer and Internet skills. Conventions, Formats and Scope The conventions, formats, and scope of this manual are described in the following paragraphs. â□¢ Typographical Conventions. This manual uses the following typographical conventions: Italics Bold Fixed italics Emphasis, books, CDs, file and server names, extensions User input, IP addresses, GUI screen text Command prompt, CLI text, code URL links â□¢ Formats. This manual uses the following formats to highlight special messages: Note: This format is used to highlight information of importance or special interest. Tip: This format is used to highlight a procedure that will save time or resources. Warning: Ignoring this type of note may result in a malfunction or damage to the equipment. danger: This is a safety warning. Failure to take heed of this notice may result in personal injury or death.

This manual is written for the VPN firewall according to these specifications. Product Version Manual Publication Date ProSafe Gigabit 8 Port VPN Firewall FVS318G August 2010 For more information about network, Internet, firewall, and VPN technologies, see the links to the NETGEAR website in Appendix C, â□□Related Documents. Â□□ Note: Product updates are available on the NETGEAR, Inc. How to Print This Manual To print this manual, your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe website at http://www.

*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. 0 April 2010 Added the following new features for the April 2010 firmware maintenance release: â□¢ Connection reset and delay options on the Broadband ISP Settings screen (see â□□Manually Configuring Your Internet Connectionâ□□). Â□¢ Support for an address range for inbound LAN rules on the Add LAN WAN Inbound Service screen (see â□□Inbound Rules (Port Forwarding)â□□ and â□□Inbound Rules Examplesâ□□). Â□¢ Support for new log options such as Resolved DNS Names and VPN on the Firewall Logs & E-mail screen (see â□□Activating Notification of Events and Alertsâ□□). In addition, made the following substantial changes to the book: â□¢ Provided new screen captures for better viewing. â□¢ Made minor corrections throughout the manual. Â□¢ Removed the â□□Managing Users, Authentication, and Certificatesâ□□ chapter and included the material in other chapters. Â□¢ Made the following change to Chapter 2, â□□Connecting the VPN Firewall to the Internetâ□□: * Updated the Broadband ISP Settings screen (Figure 2-2) and the ISP Type options in the â□□â□□Manually Configuring Your Internet Connectionâ□□ section. Â□¢ Made the following changes and addition to Chapter 3, â□□LAN Configurationâ□□: * Updated the LAN Setup screen (Figure 3-1), added LDAP information and the Enable ARP Broadcast paragraph to the â□□Configuring the LAN Setup Optionsâ□□ section, and revised this section for more clarity. * Updated the LAN Multi-homing screen (Figure 3-4) and revised the â□□Configuring Multi Home LAN IP Addressesâ□□ section for more clarity.*

** Added the â□□Configuring and Enabling the DMZ Portâ□□ section. Â□¢ Reorganized Chapter 4, â□□Firewall Protection and Content Filteringâ□□ and added the following sections to this chapter: * â□□Configuring DMZ WAN Rulesâ□□ * â□□Configuring LAN DMZ Rulesâ□□ * â□□Managing the Application Level Gateway for SIP Sessionsâ□□ * â□□Configuring UPnP (Universal Plug and Play)â□□ â□¢ Made the following changes to Chapter 5, â□□Virtual Private Networkingâ□□: * Revised the â□□Managing VPN Policiesâ□□ section * Revised the â□□Managing Certificatesâ□□ section â□¢ Added the following section to Chapter 6, â□□VPN Firewall and Network Managementâ□□: * â□□Monitoring System Performanceâ□□ 202-10521-02 1. 1, August 2010 About This Manual Chapter 1 Intro 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. Â□¢ â□¢ Autosensing Ethernet Connections with Auto Uplink With its internal 8-port 10/100/1000 Mbps switch and 10/100/1000 WAN port, the FVS318G 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 UplinkTM technology.*

Each Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a â□□normalâ□□ connection such as to a PC or an â□□uplinkâ□□ 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. For further information about TCP/IP, see the â□□TCP/IP Networking Basicsâ□□ document that you can access from the link in â□□Related Documentsâ□□ in Appendix C.

â□¢ 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. Â□¢ â□¢ â□¢ â□¢ Easy Installation and Management You can install, configure, and operate the FVS318G within minutes after connecting it to the network. the following features simplify installation and management tasks: â□¢ 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. 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. 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 firewallâ□□s front panel LEDs provide an easy way to monitor its status and activity.
Â□¢ â□¢ â□¢ Maintenance and Support NETGEAR offers the following features to help you maximize your use of the FVS318G: â□¢ Flash memory for firmware upgrade â□¢ 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 â□¢ â□¢ â□¢ â□¢ â□¢ â□¢ â□¢ The product package should contain the following items: FVS318G ProSafe Gigabit 8 Port VPN Firewall FVS318G AC power cable Rubber feet Category 5 (Cat5) Ethernet cable ProSafe Gigabit 8 Port VPN Firewall FVS318G Installation Guide Resource CD, including: â□¢ Application Notes and other helpful information. Â□¢ ProSafe VPN Client software (one user license) Warranty and Support Information Card â□¢ 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. introduction v1.
1, August 2010 1-5 ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual VPN Firewall Front and Rear Panels The FVS318G 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. 4 1 6 7 1 2 3 Figure 1-1 5 Table 1-1 describes each item on the front panel and its operation. Blinking (Green) Data is being transmitted or received by the port. Power is not supplied to the VPN firewall. The Internet connection is down The WAN port is either not enabled or has no link.
Activity Description The rear panel of the FVS318G includes a cable lock receptacle, a Factory Defaults button, and a DC power connection. 1 Figure 1-2 2 3 Viewed from left to right, the rear panel contains the following elements: 1. Factory Defaults button: Using a sharp object, press and hold this button for about ten seconds until the front panel TEST light flashes to reset the VPN firewall to factory default settings. All configuration settings will be lost and the default password will be restored. 1, August 2010 1-7 ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual Default IP Address, Login Name, and Password Check the label on the bottom of the FVS318Gâ□□s enclosure if you forget the following factory default information: â□¢ IP Address: http://192. When the login 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 FVS318G, you must use a Web browser such as Internet Explorer 5. 1, August 2010 Introduction Chapter 2 Connecting the VPN Firewall to the Internet This section provides instructions for connecting the ProSafe Gigabit 8 Port VPN Firewall FVS318G, including these topics: â□¢ â□¢ â□¢ â□¢ â□¢ â□¢ â□¢ â□□Understanding the Connection Stepsâ□□ on this page â□□Logging into the VPN Firewallâ□□ on page 2-2 â□□Navigating the Menusâ□□ on page 2-3 â□□Configuring the Internet Connection to Your ISPâ□□ on page 2-4 â□□Configuring the WAN Modeâ□□ on page 2-9 â□□Configuring Dynamic DNSâ□□ on page 2-11 â□□Configuring the Advanced Broadband Optionsâ□□ on page 2-13 Setting up VPN tunnels is covered in Chapter 5, â□□Virtual Private Networking. Â□□ Understanding the Connection Steps Typically, six steps are required to complete the basic Internet connection of your VPN firewall. 1.

Connect the VPN firewall physically to your network. Connect the cables and restart your network according to the instructions in the installation guide. See the ProSafe Gigabit 8 Port VPN Firewall FVS318G Installation Guide for complete steps. A PDF of the Installation Guide is on the NETGEAR website at: http://kbserver. After logging in, you are ready to set up and configure your VPN firewall. You can also change your password and enable remote management at this time.

See â□□Logging into the VPN Firewallâ□□ on page 2-2. 3. Configure the Internet connection to your ISP. During this phase, you will connect to your ISP. See â□□Configuring the Internet Connection to Your ISPâ□□ on page 2-4. See â□□Configuring the WAN Modeâ□□ on page 2-9. As an option, configure your fully qualified domain names during this phase. As an option, change the VPN firewallâ□□s Media Access Control (MAC) address, the factory default MTU size, and the port speed. However, these are advanced features and changing them is not usually required.

See â□□Configuring the Advanced Broadband Optionsâ□□ on page 2-13. Each of these tasks is detailed separately in this chapter. the configuration of firewall and VPN features is described in later chapters. Note: In this manual, â□□WAN portâ□□ and â□□broadband portâ□□ both indicate the same port through which the VPN firewall connects to the Internet. Logging into the VPN Firewall To connect to the VPN firewall, your computer needs to be configured to obtain an IP address automatically via DHCP.

If you need instructions on how to configure you computer for DHCP, refer to the â□□Preparing Your Networkâ□□ document that you can access from the link in Appendix C, â□□Related Documents. 1 in the address field of your browser. figure 2-1 2. When prompted, enter admin for the VPN firewall user name and password for the VPN firewall password, both in lower case letters. (The VPN firewall user name and password are not the same as any user name or password you may use to log in to your Internet connection.) 2-2 Connecting the VPN Firewall to the Internet v1. For more information about this screen, see â□□Viewing the VPN Firewall Configuration and System Statusâ□□ on page 6-30. Note: You might want to enable remote management at this time so that you can log in remotely in the future to manage the VPN firewall (see â□□Configuring an External Server for Authenticationâ□□ on page 6-11). If you enable remote management, NETGEAR strongly advises you to change your password (see â□□Changing Passwords and Settingsâ□□ on page 6-8). Navigating the Menus The Web Configuration Manager menus are organized in a layered structure of main categories and submenus: â□¢ Main menu.

The horizontal orange bar near the top of the page is the main menu, containing the primary configuration categories. Clicking on a primary category changes the contents of the submenu bar. submenu. The horizontal grey bar immediately below the main menu is the submenu, containing subcategories of the currently selected primary category. tab. Immediately below the submenu bar, at the top of the menu active window, are one or more tabs, further subdividing the currently selected subcategory if necessary. option arrow. To the right of the tabs on some menus are one or more blue dots with an arrow in the center. Clicking an option arrow brings up either a popup window or an advanced option menu. Tip: In the instructions in this manual, we may refer to a menu using the notation primary | subcategory, such as Network Configuration | WAN Settings.

In this example, Network is the selected primary category (in the main menu) and WAN Settings is the selected subcategory (in the submenu). You can now proceed to the first configuration task, configuring the VPN firewallâ□□s Internet connection. Â□¢ â□¢ â□¢ Connecting the VPN Firewall to the Internet v1. 1, August 2010 2-3 ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual Configuring the Internet Connection to Your ISP To automatically configure the broadband port and connect to the Internet: 1. Select Network Configuration from the main menu and Broadband ISP Settings from the submenu.

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. 2-4 Connecting the VPN Firewall to the Internet v1. 1, August 2010 ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual When Auto Detect successfully detects an active Internet service, it reports which connection type it discovered. The options are described in Table 2-1.

Note: When you click Auto Detect while the WAN port already has a connection, you might lose the connection because the VPN firewall will enter its detection mode. Fixed (Static) IP Static IP address, Subnet, and Gateway IP; and related data supplied by your ISP. If Auto Detect does not find a connection, you will be prompted to check the physical connection between your VPN firewall and the cable or DSL line or to check your VPN firewallâ□□s MAC address (see â□□Manually Configuring Your Internet Connectionâ□□ on page 2-6). 3. Click the Broadband Status option arrow at the top right of the screen to verify the WAN port connection status. click Connect if there is no connection. Figure 2-3 Connecting the VPN Firewall to the Internet v1. 1, August 2010 2-5 ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual The Connection Status window should show a valid IP address and gateway. If the configuration was not successful, skip ahead to â□□Manually Configuring Your Internet Connection following this section, or see â□□Troubleshooting the ISP Connectionâ□□ on page 7-4. Note: If the configuration process was successful, you are connected to the Internet through the WAN port.

If your WAN ISP configuration was successful, you can skip ahead to â□□Manually Configuring Your Internet Connectionâ□□ on page 2-6. Manually Configuring Your Internet Connection If you know your ISP connection type, you can bypass the Auto Detect feature and connect your VPN firewall manually. Ensure that you have all of the relevant connection information such as IP addresses, account information, type of ISP connection, and so on, before you begin. Unless your ISP automatically assigns your configuration automatically via DHCP, you will need these configuration settings from your ISP. to manually configure your broadband ISP settings: 1. Select Network Configuration from the main menu and Broadband ISP Settings from the submenu. The Broadband ISP Settings screen displays (see Figure 2-2 on page 2-4 for the entire screen). 2. In the ISP Login section, choose one of these options: â□¢ â□¢ If your ISP requires an initial login to establish an Internet connection, click Yes (this is the default). If a login is not required, click No and ignore the Login and Password fields.

figure 2-4 3. If you clicked Yes, enter the ISP-provided Login and Password information. 2-6 Connecting the VPN Firewall to the Internet v1. 1 , August 2010 ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual 4.

In the ISP Type section, select the type of ISP connection you use from the two listed options.
If you have installed login software such as WinPoET or Ethernet, then your connection type is PPPoE. configure the following fields: â□□ â□□ â□□ Account Name. Valid account name for the PPPoE connection. domain Name. Name of your ISPâ□□s domain or your domain name if your ISP has assigned one.
In most cases, you may leave this field blank. idle Timeout. Select Keep Connected, to keep the connection always on. To logout after the connection is idle for a period of time, click Idle Time and in the timeout field enter the number of minutes to wait before disconnecting. connection Reset. Select this checkbox to to specify a time when the PPPoE WAN connection is reset, that is, the connection is disconnected momentarily and then reestablished. Enter the hour and minutes in the Disconnect Time fields to specify when the connection should be disconnected. Enter the seconds in the Delay field to specify the period after which the connection should be re-established. â□□ â□¢ PPTP. Select this option if your ISP is Austria Telecom or any other ISP that uses PPTP as a login protocol.

) Enter the valid account name for the PPTP connection (usually your email name as assigned by your ISP). Some ISPs require entering your full email address here. domain Name. Your domain name or workgroup name assigned by your ISP, or your ISPs domain name. You may leave this field blank. Â□□ Connecting the VPN Firewall to the Internet v1. 1 , August 2010 2-7 ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual â□□ Idle Timeout. Check the Keep Connected radio box to keep the connection always on. To logout after the connection is idle for a period of time, click Idle Time and enter the number of minutes to wait before disconnecting in the timeout field. This is useful if your ISP charges you based on the amount of time you have logged in. my IP Address. IP address assigned by the ISP to make the connection with the ISP server. server IP Address. IP address of the PPTP server. Figure 2-6 â□¢ Get Dynamically from ISP.
If your ISP has not assigned a static IP address, select this radio button. The ISP will automatically assign an IP address to the VPN firewall using DHCP network protocol. The IP address and subnet mask fields will be inactivated. As an option, you can select the following checkboxes: â□□ â□□ Client Identifier. Select this checkbox if your ISP requires the Client Identifier information to assign an IP address using DHCP.
vendor Class Identifier. Select this checkbox if your ISP requires the Vendor Class Identifier information to assign an IP address using DHCP. â□¢ Use Static IP Address. If your ISP has assigned a fixed (static) IP address, select this radio button, and configure the following fields: â□□ â□□ â□□ IP Address. Enter the Static IP address assigned to you, that identifies the VPN firewall to your ISP. subnet Mask. Enter the mask provided by the ISP or your network administrator. gateway IP Address. Enter the IP address of the ISPâ□□s gateway, provided by the ISP or your network administrator. 2-8 Connecting the VPN Firewall to the Internet v1.

Figure 2-7 â□¢ â□¢ If your ISP has not assigned any Domain Name Servers (DNS) addresses, click Get Dynamically from ISP. If your ISP (or your IT department) has assigned DNS addresses, click Use These DNS Servers and enter the DNS server IP addresses provided to you in the fields. 7. Click Apply to save any changes to the broadband settings. (Or click Reset to discard any changes and revert to the previous settings. The VPN firewall will attempt to connect to the NETGEAR website. if a successful connection is made , NETGEARâ□□s website appears. Configuring the WAN Mode To access the WAN Mode screen, select Network Configuration from the main menu and WAN Settings from the submenu. the WAN Mode screen displays. Figure 2-8 Connecting the VPN Firewall to the Internet v1.
1, August 2010 2-9 ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual The WAN Mode screen allows you to configure how the VPN firewalll uses the external Internet connection. This screen gives you two choices for accessing the external Internet connection. â□¢ Network Address Translation (NAT). This technique allows several computers on a LAN to share the same Internet connection (IP address) while using private IP address on the LAN, which are hidden from the Internet. classical Routing.
This method allows the VPN firewall to perform the routing, but requires separate valid static Internet IP address for each PC on your LAN. Â□¢ Network Address Translation Network Address Translation (NAT) allows all PCs on your LAN to share a single public Internet IP address. From the Internet, there is only a single device (the VPN firewall) and a single IP address. PCs on your LAN can use any private IP address range, and these IP addresses are not visible from the Internet. Â□¢ â□¢ â□¢ The VPN firewall uses NAT to select the correct PC (on your LAN) to receive any incoming data.
If you only have a single public Internet IP address, you MUST use NAT. (the default setting). If your ISP has provided you with multiple public IP addresses, you can use one address as the primary shared address for Internet access by your PCs, and you can map incoming traffic on the other public IP addresses to specific PCs on your LAN. This one-to-one inbound mapping is configured using an inbound firewall rule. Classical Routing In classical routing mode, the VPN firewall performs routing, but without NAT. To gain Internet access, each PC on your LAN must have a valid static Internet IP address. If your ISP has allocated a number of static IP addresses to you, and you have assigned one of these addresses to each PC, you can choose classical routing. Or, you can use classical routing for routing private IP addresses within a campus environment. To learn the status of the WAN port, you can view the Router Status screen (see â□□Viewing the VPN Firewall Configuration and System Statusâ□□ on page 6-30) or look at the LEDs on the front panel (see â□□VPN Firewall Front and Rear Panelsâ□□ on page 1-6). 2-10 Connecting the VPN Firewall to the Internet v1.

1, August 2010 ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual Configuring Dynamic DNS Dynamic DNS (DDNS) is an Internet service that allows routers with varying public IP addresses to be located using Internet domain names. To use DDNS, you must setup an account with a DDNS provider such as DynDNS. Links to DynDNS, TZO, Oray, and 3322 are provided for your convenience on the Dynamic DNS Configuration screen. The VPN firewall firmware includes software that notifies dynamic DNS servers of changes in the WAN IP address, so that the services running on this network can be accessed by others on the Internet.

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will not know in advance what your IP address will be, and the address can change frequentlyâ□□hence, the need for a commercial DDNS service, which allows you to register an extension to its domain, and restores DNS requests for the resulting FQDN to your frequently-changing IP address. After you have configured your account information on the VPN firewall, whenever your ISP-assigned IP address changes, your VPN firewall will automatically contact your DDNS service provider, log in to your account, and register your new IP address. Note: If your ISP assigns a private WAN IP address such as 192. X, the dynamic DNS service will not work because private addresses will not be routed on the Internet. to configure Dynamic DNS: 1.

Select Network Configuration from the main menu and Dynamic DNS from the submenu. the Dynamic DNS screen displays (see Figure 2-9 on page 2-12). Connecting the VPN Firewall to the Internet v1. 1 , August 2010 2-11 ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual Figure 2-9 2. Click the tab of the DNS service you want to enable.

each DNS service provider requires registration. After registration you can configure the required settings on the corresponding screen for the DNS service. 3. Access the website of one of the DNS service providers and set up an account. A link to each DNS service provider is located to the right of the tabs (see the option arrow).

*After setting up your account, return to the screen for the DNS service. 4. On the screen for the DNS service, select the Yes radio button, and complete the required fields for the DNS service that you selected: a. In the Host and Domain Name field, enter the entire FQDN name that your DNS service provider gave you (for example: <yourname>. Enter the account information for the service you have chosen (for example, user name, password, key, or domain). c. If your DNS service provider allows the use of wild cards in resolving your URL, you may check the Use wildcards checkbox to activate this feature. For example, the wildcard feature will cause *. Org to be aliased to the same IP address as yourhost. If your WAN IP address does not change often, you may need to force a periodic update to the DDNS service to prevent your account from expiring.*

If it appears, you can select the Update every 30 days checkbox to enable a periodic update. 5. Click Apply to save your configuration or click Reset to return to the previous settings. 2-12 Connecting the VPN Firewall to the Internet v1. 1, August 2010 ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual Configuring the Advanced Broadband Options To configure the advanced broadband options: 1. Select Network Configuration from the main menu and Broadband ISP Settings from the submenu. Click the Advanced option arrow at the right of the tabs to display the Broadband Advanced Options screen. figure 2-10 3. Edit the default information you want to change. â□¢ MTU Size.

The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 Bytes, or 1492 Bytes for PPPoE connections. For some ISPs you may have to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection. port Speed. In most cases, your VPN firewall can automatically determine the connection speed of the Internet (WAN) port.

If you cannot establish an Internet connection and the Internet LED blinks continuously, you may have to manually select the port speed. autoSense is the default. If you know that the Ethernet port on your broadband modem supports 100BaseT, select 100BaseT Half_Duplex; otherwise, select 10BaseT Half_Duplex. Use the half-duplex settings unless you are sure you need full duplex. Connecting the VPN Firewall to the Internet v1.

1 , August 2010 2-13 â□¢ ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual â□¢ Router's MAC Address. Each computer or router on your network has a unique 32-bit local Ethernet address. This is also referred to as the computer's MAC (Media Access Control) address. the default is Use Default Address. However, if your ISP requires MAC authentication, then select either â□□ â□□ Use this Computerâ□□s MAC address to enable the VPN firewall to use the MAC address of the computer you are now using, or Use This MAC Address to manually type in the MAC address that your ISP expects. The format for the MAC address is XX:XX:XX:XX:XX:XX (numbers 0-9 and either uppercase or lowercase letters A-F). If you select Use This MAC Address and then type in a MAC address, your entry will be overwritten. Additional WAN Related Configuration â□¢ If you want the ability to manage the VPN firewalll remotely, enable remote management at this time (see â□□Enabling Remote Management Accessâ□□ on page 6-14). If you enable remote management, NETGEAR strongly recommends that you change your password (see â□□Changing Passwords and Settingsâ□□ on page 6-8). At this point, you can set up the traffic meter for each WAN, if desired.

See â□□Enabling the Traffic Meterâ□□ on page 6-27. Â□¢ 2-14 Connecting the VPN Firewall to the Internet v1. 1, August 2010 Chapter 3 LAN Configuration This chapter describes how to configure the advanced LAN features of your ProSafe Gigabit 8 Port VPN Firewall FVS318G, including the following sections: â□¢ â□□Choosing the VPN Firewall DHCP Optionsâ□□ on this page â□¢ â□□Configuring the LAN Setup Optionsâ□□ on page 3-2 â□¢ â□□Managing Groups and Hosts (LAN Groups)â□□ on page 3-5 â□¢ â□□Configuring Multi Home LAN IP Addressesâ□□ on page 3-10 â□¢ â□□Configuring and Enabling the DMZ Portâ□□ on page 3-11 â□¢ â□□Configuring Static Routesâ□□ on page 3-14 â□¢ â□□Configuring Routing Information Protocol (RIP)â□□ on page 3-17 Choosing the VPN Firewall DHCP Options By default, the VPN firewall will function as a DHCP (Dynamic Host Configuration Protocol) server, allowing it to assign IP, DNS server, WINS Server, and default gateway addresses to all computers connected to the VPN firewall LAN. The assigned default gateway address is the LAN address of the VPN firewall. IP addresses will be assigned to the attached PCs from a pool of addresses that you must specify. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN. The DHCP options are available for both the LAN and DMZ settings. For most applications, the default DHCP and TCP/IP settings of the VPN firewall are satisfactory.

See the link to â□□TCP/IP Networking Basicsâ□□ in Appendix C, â□□Related Documents for an explanation of DHCP and information about how to assign IP addresses for your network. If another device on your network will be the DHCP server, or if you will manually configure the network settings of all of your computers, clear the Enable DHCP server radio box by selecting the Disable DHCP Server radio box.

Otherwise, leave it checked. Specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the VPN firewallâ□□s LAN IP address. Using the default addressing scheme, you should define a range between 192. 100, although you may wish to save part of the range for devices with fixed addresses.

3-1 v1. 1, August 2010 ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual The VPN firewall will deliver the following settings to any LAN device that requests DHCP: â□¢ â□¢ â□¢ â□¢ â□¢ An IP address from the range that you have defined. WINS server (if you entered a WINS server address in the DHCP section of the LAN Setup screen). lease time (date obtained and duration of lease). DHCP Relay options allow you to make the VPN firewall a DHCP relay agent.

The DHCP Relay Agent makes it possible for DHCP broadcast messages to be sent over routers that do not support forwarding of these types of messages. The DHCP Relay Agent is therefore the routing protocol that enables DHCP clients to obtain IP addresses from a DHCP server on a remote subnet, or which is not located on the local subnet. If you have no configured DHCP Relay Agent, your clients would only be able to obtain IP addresses from the DHCP server which is on the same subnet. To enable clients to obtain IP addresses from a DHCP server on a remote subnet, you have to configure the DHCP Relay Agent on the subnet that contains the remote clients, so that it can relay DHCP broadcast messages to your DHCP server. When the DNS Proxy option is enabled, the VPN firewall will act as a proxy for all DNS requests and communicates with the ISPâ□□s DNS servers (as configured on the Broadband ISP Settings screen). All DHCP clients will receive the primary and/or secondary DNS IP address along with the IP address where the DNS proxy is running, that is, the VPN firewallâ□□s LAN IP address. When disabled, all DHCP clients will receive the DNS IP addresses of the ISP excluding the DNS proxy IP address. Configuring the LAN Setup Options The LAN Setup screen allows configuration of LAN IP services such as DHCP and allows you to configure a secondary or â□□multi-homeâ□□ LAN IP setup in the LAN. The default values are suitable for most users and situations. Note: If you enable the DNS Relay feature, you will not use the VPN firewall as a DHCP server but rather as a DHCP relay agent for a DHCP server somewhere else on your network.

Select Network Configuration from the main menu and LAN Settings from the submenu. In the LAN TCP/IP Setup section, configure the following settings: â□¢ IP Address. The LAN address of your VPN firewall (factory default: 192. Note: If you change the LAN IP address of the VPN firewall while connected through the browser, you will be disconnected. You must then open a new connection to the new IP address and log in again. For example, if you change the default IP address 192. 1, you must now enter https://10. 1 in your browser to reconnect to the Web Configuration Manager. The subnet mask specifies the network number portion of an IP address. Your VPN firewall will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use 255. (Always make sure that the LAN port IP address and DMZ port IP address are in different subnets. By default, the VPN firewall will function as a DHCP server, providing TCP/IP configuration settings for all computers connected to the VPN firewallâ□□s LAN. If another device on your network will be the DHCP server, or if you will manually configure all devices, click Disable DHCP Server. If the VPN firewall will function as a DHCP relay agent, select DHCP Relay and enter the IP address of the DHCP relay gateway in the Relay Gateway field.

If the DHCP server is enabled, enter the following settings: â□¢ â□¢ Domain Name. Specifies the first of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN will be assigned an IP address between this address and the Ending IP Address. The IP address 192. Specifies the last of the contiguous addresses in the IP address pool.

The IP address 192. Note: The starting and ending DHCP addresses should be in the same subnet as the LAN IP address of the VPN firewall (the IP address that is configured in the LAN TCP/IP Setup section of the LAN Setup screen). â□¢ Primary DNS Server. (Optional) If an IP address is specified, the VPN firewall will provide this address as the primary DNS server IP address. If no address is specified, the VPN firewall will provide its own LAN IP address as the primary DNS server IP address. secondary DNS Server. (Optional) If an IP address is specified, the VPN firewall will provide this address as the secondary DNS server IP address. wINS Server. (Optional) Specifies the IP address of a local Windows NetBIOS Server if one is present in your network. lease Time.

This specifies the duration for which IP addresses will be leased to clients. â□¢ â□¢ â□¢ â□¢ 3-4 v1. 1, August 2010 LAN Configuration ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual If you will use a Lightweight Directory Access Protocol (LDAP) authentication server for network-validated domain-based authentication, select Enable LDAP Information to enable the DHCP server to provide LDAP server information. enter the following settings: â□¢ â□¢ LDAP Server. Specifies the name or the IP address of the device that hosts the LDAP server. search Base. Specifies the distinguished name (dn) at which to start the search, specified as a sequence of relative distinguished names (rdn), connected with commas and without any blank spaces. For most users, the search base is a variation of the domain name. For example, if your domain is yourcompany. Com, your search base dn might be as follows: dc=yourcompany,dc=com.

port. Specifies the port number that the LDAP server is using. Leave this field blank for the default port. â□¢ 4. In the Advanced Settings section, configure the following settings: â□¢ Enable DNS Proxy.

If the DNS proxy is enabled (which is the default setting), the DHCP server will provide the VPN firewallâ□□s LAN IP address as the DNS server for address name resolution. If this box is unchecked, the DHCP server will provide the ISPâ□□s DNS server IP addresses.

The VPN firewall will still service DNS requests sent to its LAN IP address unless you disable DNS Proxy in the VPN firewall settings (see â□□Attack Checksâ□□ on page 4-20). enable ARP Broadcast. If ARP broadcast is enabled (which is the default setting), the Address Resolution Protocol (ARP) is broadcasted on the LAN so that IP addresses can be mapped to physical addresses (that is, MAC addresses).

â□¢ 5. Click Apply to save your settings or click Reset to discard any changes and revert to the previous configuration. Note: Once you have completed the LAN IP setup, all outbound traffic is allowed and all inbound traffic is discarded. To change these traffic rules, refer to Chapter 4, â□□Firewall Protection and Content Filtering. Â□□ Managing Groups and Hosts (LAN Groups) The Known PCs and Devices table on the Groups and Hosts screen contains a list of all known PCs and network devices, as well as hosts, that are assigned dynamic IP addresses by this VPN firewall. Collectively, these entries make up the Network Database. By default, the DHCP server in this VPN firewall is enabled, and will accept and respond to DHCP client requests from PCs and other network devices. These requests also generate an entry in the Network Database. Because of this, leaving the DHCP Server feature (on the LAN screen) enabled is strongly recommended. scanning the Network.

The local network is scanned using standard methods such as ARP. This will detect active devices which are not DHCP clients. However, sometimes the name of the PC or device cannot be accurately determined, and will be shown as Unknown. manual Entry. You can manually enter information about a network device. Â□¢ â□¢ Creating the Network Database Some advantages of the Network Database are: â□¢ â□¢ Generally, you do not need to enter either IP address or MAC addresses. Instead, you can just select the desired PC or device. No need to reserve an IP address for a PC in the DHCP Server. All IP address assignments made by the DHCP Server will be maintained until the PC or device is removed from the database, either by expiry (inactive for a long time) or by you. No need to use a fixed IP address on PCs.

Because the address allocated by the DHCP Server will never change, you do not need to assign a fixed IP address to a PC to ensure it always has the same IP address. mAC level control over PCs. The Network Database uses the MAC address to identify each PC or device. So changing a PCâ□□s IP address does not affect any restrictions on that PC. group and individual control over PCs.

Â□□ â□□ â□□ You can assign PCs to groups and apply restrictions to each group using the Firewall Rules screen (see â□□Using Rules to Block or Allow Specific Kinds of Traffic â□□ on page 4-2). You can also select the groups to be covered by the Block Sites feature (see â□□Blocking Internet Sites (Content Filtering)â□□ on page 4-30). If necessary, you can also create firewall rules to apply to a single PC (see â□□Configuring Source MAC Filteringâ□□ on page 4-33). Because the MAC address is used to identify each PC, users cannot avoid these restrictions by changing their IP address. Â□¢ â□¢ â□¢ â□¢ A computer is identified by its MAC addressâ□□not its IP address.

Hence, changing a computerâ□□s IP address does not affect any restrictions applied to that PC. 3-6 v1. 1, August 2010 LAN Configuration ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual Viewing the Network Database To view the Network Database, follow these steps: 1. Select Network Configuration from the main menu and LAN Settings from the submenu. Figure 3-2 The Known PCs and Devices table lists the entries in the Network Database. For each computer or device, the following fields are displayed: â□¢ Name. The name of the computer or device. Computers that do not support the NetBIOS protocol will be listed as Unknown. In this case, the name can be edited manually for easier management. If the computer was assigned an IP address by the DHCP server, then an asterisk is be appended to the name.

iP Address. The current IP address of the computer. For DHCP clients of the VPN firewall, this IP address will not change. If a computer is assigned a static IP address, you must to update this entry manually when the IP address of the computer changes. mAC Address. The MAC address of the computerâ□□s network interface. group. Each PC or device can be assigned to a single group. By default, a computer is assigned to the first group (Group 1). To change the group assignment by selecting the Edit button in the Action column.

1, August 2010 3-7 ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual Adding Devices to the Network Database To add devices manually to the network database: 1. To add computers to the network database manually, make the following selections: â□¢ â□¢ Name: The name of the PC or device. iP Address Type. From the pull-down menu, choose how this device receives its IP address: â□□ â□□ Select Fixed (Set on PC) if the IP address is statically assigned on the computer. Select Reserved (DHCP Client) to direct the VPN firewall to reserve the IP address for allocation by the DHCP server (see â□□Setting Up DHCP Address Reservationâ□□ on page 3-9).

Note: When assigning a reserved IP address to a client, the IP address selected must be outside the range of addresses allocated to the DHCP server pool. â□¢ IP Address. Enter the IP address that this computer or device is assigned. If the IP Address Type is Reserved (DHCP Client), the VPN firewall will reserve the IP address for the associated MAC address. mAC Address.

Enter the MAC address of the computerâ□□s network interface. The MAC address format is six colon-separated pairs of hexadecimal characters (0-9 and A-F), such as 01:23:45:67:89:AB. group. From the pull-down menu, select the group to which the computer has to be assigned. Click Add to add the new entry to the network database. 3. As an optional step: To enable DHCP address reservation for the entry that you just added to the Known PCs and Devices table, select the checkbox for the table entry, and click Save Binding to bind the IP address to the MAC address for DHCP assignment. 3-8 v1. 1, August 2010 LAN Configuration ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual Changing Group Names in the LAN Groups Database By default, the LAN Groups are named Group1 through Group8. You can rename these group names to be more descriptive, such as Engineering or Marketing.

To edit the names of any of the eight available groups: 1. From the LAN Groups screen, click the Edit Group Names option arrow to the right of the tabs. Select the radio button next to any group name to make that name active for editing.

3. Type a new name in the field. 4. Select and edit other group names if desired. Setting Up DHCP Address Reservation When you specify a reserved IP address for a device on the LAN (based on the MAC address of the device), that computer or device will always receive the same IP address each time it accesses the VPN firewallâ□□s DHCP server. Reserved IP addresses should be assigned to servers or access points that require permanent IP settings. The Reserved IP address that you select must be outside of the DHCP Server pool.

To reserve an IP address, manually enter the device on the LAN Groups screen, specifying Reserved (DHCP Client), as described in â□□Adding Devices to the Network Databaseâ□□ on page 38. lAN Configuration v1. 1, August 2010 3-9 ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual Note: The reserved address will not be assigned until the next time the PC contacts the VPN firewall's DHCP server. Reboot the PC or access its IP configuration and force a DHCP release and renew. Configuring Multi Home LAN IP Addresses If you have computers on your LAN using different IP address ranges (for example, 172.

0), you can add â□□aliasesâ□□ to the LAN port, giving computers on those networks access to the Internet through the VPN firewall. This allows the VPN firewall to act as a gateway to additional logical subnets on your LAN. You can assign the VPN firewall an IP address on each additional logical subnet. to add a secondary LAN IP address: 1. Select Network Configuration from the main menu and LAN Settings from the submenu.

Figure 3-4 The Available Secondary LAN IPs table lists the secondary LAN IP addresses added to the VPN firewall. â□¢ IP Address. The IP address alias added to the LAN port of the VPN firewall. This is the gateway for computers that need to access the Internet. The Edit button allows you to make changes to the selected entry. In the Add Secondary LAN IP Address section, enter the additional IP address and subnet mask to be assigned to the LAN port of the VPN firewall. The secondary LAN IP address will be added to the Available Secondary LAN IPs table. To make changes to the Available Secondary LAN IPs table, use the following buttons: â□¢ Select All. Selects all the entries in the Available Secondary LAN IPs table. Note: Additional IP addresses cannot be configured in the DHCP server.

The hosts on the secondary subnets must be manually configured with the IP addresses, gateway IP and DNS server IPs. Warning: Make sure that the secondary IP addresses are different from the LAN, WAN, DMZ, and any other subnet addresses that are attached to the VPN firewall. Example of correct addresses: WAN IP address: 10. 0 Configuring and Enabling the DMZ Port The De-Militarized Zone (DMZ) is a network which, when compared to the LAN, has fewer firewall restrictions, by default. This zone can be used to host servers (such as a Web server, FTP server, or email server, for example) and give public access to them. The eighth LAN ports on the VPN firewall can be dedicated as a hardware DMZ port for safely providing services to the Internet, without compromising security on your LAN. The DMZ port feature is also helpful when using some online games and videoconferencing applications that are incompatible with NAT. The VPN firewall is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, local PCs can run the application properly if those PCs are used on the DMZ port. A separate firewall security profile is provided for the DMZ port that is hardware independent of the standard firewall security used for the LAN.

lAN Configuration v1. 1, August 2010 3-11 ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual The DMZ Setup screen allows you to set up the DMZ port. It permits you to enable or disable the hardware DMZ port (LAN port 8, see â□□VPN Firewall Front and Rear Panelsâ□□ on page 1-6) and configure an IP address and Mask for the DMZ port. to enable and configure the DMZ port: 1. From the main menu, select Network Configuration and then select DMZ Setup from the submenu.

In the DMZ Port Setup section, under Do you want to enable DMZ Port? Enter an IP address and the subnet mask for the DMZ port. Make sure that the DMZ port IP address and LAN Port IP address are in different subnets (for example, an address outside the LAN Address pool, such as 192. In the DHCP for DMZ Connected Computers section, select one of the following three radio buttons: â□¢ Disable DHCP Server. The DHCP server is disabled, which is the default setting. Select this radio button if another device on your DMZ network will be the DHCP server, or if you will manually configure all devices.

enable DHCP Server. The DHCP server provide a TCP/IP configuration for all computers connected to the VPN firewallâ□□s DMZ network. Specifies the first of the contiguous addresses in the IP address pool. Any new DHCP client joining the LAN will be assigned an IP address between this address and the Ending IP Address. The IP address 192. Specifies the last of the contiguous addresses in the IP address pool. The IP address 192. Note: The starting and ending DHCP addresses should be in the same subnet as the LAN IP address of the VPN firewall (the IP address that is configured in the LAN TCP/IP Setup section of the screen). â□□ Primary DNS Server. (Optional) If an IP address is specified, the VPN firewall will provide this address as the primary DNS server IP address.

If no address is specified, the VPN firewall will provide its own LAN IP address as the primary DNS server IP address. secondary DNS Server. (Optional) If an IP address is specified, the VPN firewall will provide this address as the secondary DNS server IP address. wINS Server. (Optional) Specifies the IP address of a local Windows NetBIOS Server if one is present in your network. lease Time. This specifies the duration for which IP addresses will be leased to clients. â□¢ â□□ â□□ â□□ â□□ LAN Configuration v1. 1, August 2010 3-13 ProSafe Gigabit 8 Port VPN Firewall FVS318G Reference Manual If you will use a Lightweight Directory Access Protocol (LDAP) authentication server for network-validated domain-based authentication, select Enable LDAP Information to enable the DHCP server to provide LDAP server information. enter the following settings: â□□ â□□ LDAP Server.

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

Com, your search base dn might be as follows: dc=yourcompany,dc=com.