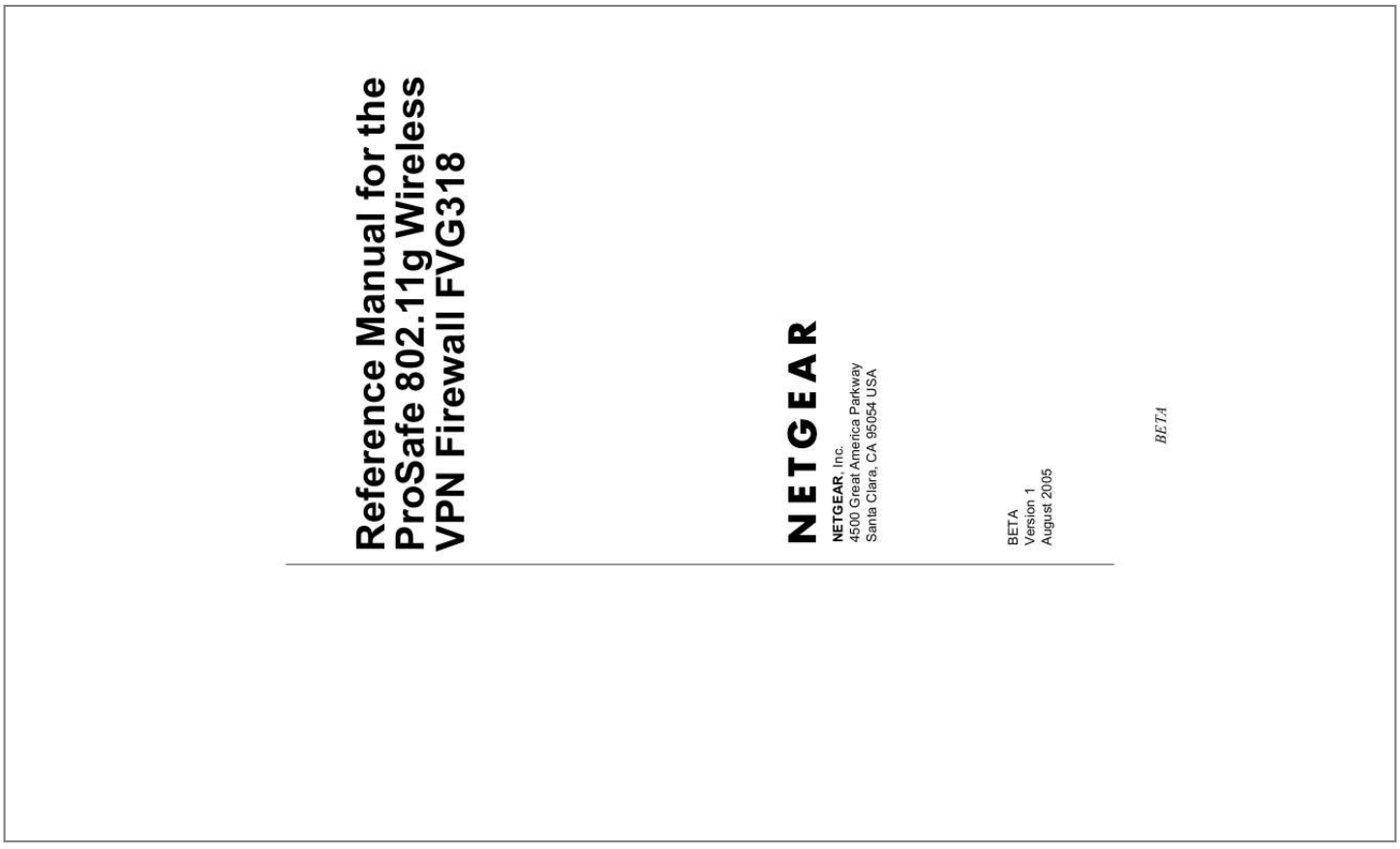

Manual abstract:

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.
EN 55 022 Declaration of Conformance This is to certify that the FVG318 ProSafe 802.11g Wireless VPN Firewall is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22). ii BETA Bestätigung des Herstellers/Importeurs Es wird hiermit bestätigt, daß das FVG318 ProSafe 802.11g Wireless VPN Firewall 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 FVG318 ProSafe 802.11g Wireless VPN Firewall 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. iii BETA Product and Publication Details Model Number: Publication Date: Product Family: Product Name: Home or Business Product: Language: English Business FVG318 ProSafe 802.11g Wireless VPN Firewall Router August 2005 FVG318 iv BETA Contents Chapter 1 About This Manual Audience, Scope, Conventions, and Formats .

.....
.....
.....
.....

.....
.....
.....
.....

...1-1 How to Use This Manual .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

.....1-2 How to Print this Manual .
.....
.....
.....

.....
.....
.....
.....

.....
.....

.....
.....
.....
.....

.....
.....
.....
.....

B-27 Configuring the VPN Tunnel .....
.....
.....
.....

.....
.....
.....
.....

.....
.....
.....
. B-28 Initiating and Checking the VPN Connections .....

.....
.....
.....
.....

.....
.....
B-36 x BETA Contents Chapter 1 About This Manual This chapter describes the intended audience, scope, conventions, and formats of this manual. Audience, Scope, Conventions, and Formats This reference manual assumes that the reader has basic to intermediate computer and Internet skills. However, basic computer network, Internet, firewall, and VPN technologies tutorial information is provided in the Appendices and on the NETGEAR Web site. This guide uses the following typographical conventions: Table 1-1. italics bold fixed User input Screen text, file and server names, extensions, commands, IP addresses Typographical Conventions Emphasis, books, CDs, URL names This guide uses the following formats to highlight special messages: Note: This format is used to highlight information of importance or special interest.
This manual is written for the FVG318 Wireless VPN Firewall according to these specifications.: Table 1-2. Product Version Manual Publication Date Manual Scope FVG318 ProSafe 802.11g Wireless VPN Firewall August 2005 Note: Product updates are available on the NETGEAR, Inc. Web site at http://kbserver.netgear.com/products/FVG318.asp. About This Manual BETA 1-1 Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 How to Use This Manual The HTML version of this manual includes the following: · · Buttons, at a time and , for browsing forwards or backwards through the manual one page 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 product model. button to access the full NETGEAR, Inc. online Knowledge Base for the · · Links to PDF versions of the full manual and individual chapters. 1-2 BETA About This Manual Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 How to Print this Manual To print this manual you can choose one of the following several options, according to your needs. · 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. · 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. Note: 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 Web site at http://www.adobe.
com. 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. Printing a Chapter. About This Manual BETA 1-3 Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 1-4 BETA About This Manual Chapter 2 Introduction This chapter describes the features of the NETGEAR FVG318 ProSafe 802.11g Wireless VPN Firewall. Key Features of the Wireless VPN Firewall The FVG318 ProSafe 802.11g Wireless VPN Firewall with eight-port switch connects your local area network (LAN) to the Internet through an external access device such as a cable modem or DSL modem and provides 802.

11b/g wireless LAN connectivity. The FVG318 is a complete security solution that protects your network from attacks and intrusions. Unlike simple Internet sharing firewalls that rely on Network Address Translation (NAT) for security, the FVG318 uses stateful packet inspection for Denial of Service attack (DoS) protection and intrusion detection. The FVG318 allows Internet access for up to 253 users. The FVG318 Wireless VPN Firewall provides you with multiple Web content filtering options, plus browsing activity reporting and instant alerts -- both via e-mail. Parents and network administrators can establish restricted access policies based on time-of-day, Web site addresses and address keywords, and share high-speed cable/DSL Internet access for up to 253

personal computers. In addition to NAT, the built-in firewall protects you from hackers. With minimum setup, you can install and use the firewall within minutes. The FVG318 Wireless VPN Firewall provides the following features: · · · · · · · · · 802.11g and 802. 11b standards-based wireless networking.

Wireless Multimedia (WMM) support. Easy, Web-based setup for installation and management. Front panel LEDs for easy monitoring of status and activity. Content filtering and site blocking security.

Built-in eight-port 10/100 Mbps switch. Ethernet connection to a WAN device, such as a cable modem or DSL modem. Extensive protocol support. Flash memory for firmware upgrade. Introduction BETA 2-1 Reference Manual for the ProSafe 802.

11g Wireless VPN Firewall FVG318 802.11g and 802.11b Wireless Networking The FVG318 Wireless VPN Firewall includes an 802.11g-compliant wireless access point. The access point provides: · · · · · · · · WEP keys can be generated manually or by passphrase. Wireless access can be restricted by MAC Address. Wireless network name broadcast can be turned off so that only devices that have the network name (SSID) can connect. 64-bit and 128-bit WEP encryption security. 802.11b standards-based wireless networking at up to 11 Mbps.

802.11g wireless networking at up to 54 Mbps, which conforms to the 802.11g standard. WPA and WPA2 enterprise class strong security with RADIUS and certificate authentication as well as dynamic encryption key generation. WPA-PSK and WPA2-PSK pre-shared key authentication without the overhead of RADIUS servers but with all of the strong security of WPA and WPA2. Wireless Multimedia (WMM) Support WMM is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the kind of data. Time-dependent information such as video or audio will have a higher priority than normal traffic. For WMM to function correctly, wireless clients must also support WMM.

A Powerful, True Firewall with Content Filtering Unlike simple Internet sharing NAT firewalls, the FVG318 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. · · · 2-2 BETA 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. Introduction Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 The FVG318 logs security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the firewall to email the log to you at specified intervals. You can also configure the firewall to send immediate alert messages to your e-mail address or email pager whenever a significant event occurs.

· With its content filtering feature, the FVG318 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 FVG318 Wireless VPN Firewall is equipped with several features designed to maintain security, as described in this section. · PCs Hidden by NAT NAT opens a temporary path to the Internet for requests originating from the local network. Requests originating from outside the LAN are discarded, preventing users outside the LAN from finding and directly accessing the PCs on the LAN. Port Forwarding with NAT Although NAT prevents Internet locations from directly accessing the PCs on the LAN, the firewall allows you to direct incoming traffic to specific PCs based on the service port number of the incoming request, or to one designated "DNS" host computer. You can specify forwarding of single ports or ranges of ports. · Autosensing Ethernet Connections with Auto Uplink With its internal eight-port 10/100 switch, the FVG318 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 UplinkTM technology. Each Ethernet port automatically senses 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 then configures 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. Introduction BETA 2-3 Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 Extensive Protocol Support The FVG318 Wireless VPN Firewall supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). For further information about TCP/IP, refer to Appendix B, "Network, Routing, and Firewall Basics." · IP Address Sharing by NAT The FVG318 Wireless 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 FVG318 Wireless VPN Firewall dynamically assigns network configuration information, including IP, gateway, and Domain Name Server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP).

This feature greatly simplifies configuration of PCs on your local network. DNS Proxy When DHCP is enabled and no DNS addresses are specified, the firewall provides its own address as a DNS server to the attached PCs. The firewall obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN. Point-to-Point Protocol 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 Entersys or WinPOET on your PC.

· · · Easy Installation and Management You can install, configure, and operate the FVG318 ProSafe 802.11g Wireless VPN Firewall 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 FVG318 Wireless VPN Firewall automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.

2-4 BETA Introduction Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 · Diagnostic functions The firewall incorporates built-in diagnostic functions such as Ping, DNS lookup, and remote reboot.

Remote management The firewall allows you to login to the Web Management Interface from a remote location on the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses, and you can choose a nonstandard port number. Visual monitoring The FVG318 Wireless 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 FVG318 Wireless VPN Firewall: · · Flash memory for firmware upgrade. Free technical support seven days a week, 24 hours a day. Note: The FVS318v3 firmware is not backward compatible with earlier versions of the FVS318 firewall. Introduction BETA 2-5 Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 Package Contents The product package should contain the following items: · · · · · -- This guide.

-- Application Notes and other helpful information. · Registration and Warranty Card. FVG318 ProSafe 802.11g Wireless VPN Firewall. AC power adapter. Category 5 (Cat 5) Ethernet cable. Installation Guide. Resource CD, including: 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. 2-6 BETA Introduction Reference Manual for the ProSafe 802.

11g Wireless VPN Firewall FVG318 The FVG318 Front Panel The front panel of the FVG318 Wireless VPN Firewall contains the status LEDs described below. Figure 2-1: FVG318 front panel You can use some of the LEDs to verify connections. Viewed from left to right, Table 2-1 describes the LEDs on the front panel of the firewall. These LEDs are green when lit. Table 2-1.

LED Label PWR TEST INTERNET 100 (100 Mbps) LINK/ACT (Link/Activity) LOCAL 100 (100 Mbps) LINK/ACT (Link/Activity) WLAN On Off On Blinking On/Blink Off The Local port is operating at 100 Mbps. The Local port is operating at 10 Mbps. The Local port has detected a link with an attached device. Data is being transmitted or received by the Local port. The wireless interface is on/data transmission in progress.

The wireless interface is off. On Off On Blinking The Internet (WAN) port is operating at 100 Mbps. The Internet (WAN) port is operating at 10 Mbps. The Internet port has detected a link with an attached device. Data is being transmitted or received by the Internet port. On Off On Activity LED Descriptions Description Power is supplied to the firewall. The system is initializing. The system is ready and running. Introduction BETA 2-7 Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 The FVG318 Rear Panel The rear panel of the FVG318 Wireless VPN Firewall contains the port connections listed below.

Antenna FACTORY Reset Button LOCAL Ports INTERNET Port Power Figure 2-2: FVG318 rear panel Viewed from left to right, the rear panel contains the following features: · · · · · Detachable wireless antenna Factory default reset push button Eight Ethernet LAN ports Internet Ethernet WAN port for connecting the firewall to a cable or DSL modem DC power input 2-8 BETA Introduction Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 NETGEAR-Related Products NETGEAR products related to the FVG318 are listed in the following table: Table 2-2. Category Notebooks WAG511 108 Mbps Dual Band PC Card WG511T 108 Mbps PC Card WG511 54 Mbps PC Card WG111 54 Mbps USB 2.0 Adapter MA521 802.11b PC Card MA111 802.11b USB Adapter WAG311 108 Mbps Dual Band PCI Adapter WG311T 108 Mbps PCI Adapter WG311 54 Mbps PCI Adapter WG111 54 Mbps USB 2.0 Adapter MA111 802.11b USB Adapter MA701 802.11b Compact Flash Card ANT24O5 5 dBi Antenna ANT2409 Indoor/Outdoor 9 dBi Antenna ANT24D18 Indoor/Outdoor 18 dBi Antenna Antenna Cables1.5, 3, 5, 10, and 30 m lengths VPN01L and VPN05L ProSafe VPN Client Software Wireless Wired FA511 CardBus Adapter FA120 USB 2.

0 Adapter NETGEAR-Related Products Desktops FA311 PCI Adapter FA120 USB 2.0 Adapter PDAs Antennas and Accessories NETGEAR Product Registration, Support, and Documentation Register your product at http://www.NETGEAR.com/register. Registration is required before you can use our telephone support service.

Product updates and Web support are always available by going to: http://kbserver.netgear.com. Documentation is available on the Resource CD and at http://kbserver.netgear.

com. When the wireless VPN firewall is connected to the Internet, click the Knowledge Base or the Documentation link under the Web Support menu to view support information or the documentation for the wireless VPN firewall. Introduction BETA 2-9 Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 2-10 BETA Introduction Chapter 3 Connecting the Firewall to the Internet This chapter describes how to set up the firewall on your LAN, connect to the Internet, perform basic configuration of your FVG318 ProSafe 802.11g Wireless VPN Firewall using the Setup Wizard, or how to manually configure your Internet connection. Follow these instructions to set up your firewall. Prepare to Install Your FVG318 · · For Cable Modem Service: When you set up the wireless VPN firewall, be sure to use the computer you first registered with your cable modem service provider. For DSL Service: You may need information such as the DSL login name and password in order to complete the wireless VPN firewall setup. First, Connect the FVG318 1. a.

b. c. Connect the wireless VPN firewall to your computer and modem Turn off and unplug your cable or DSL modem. Turn off your computer. At the computer end only, disconnect the Ethernet cable (point A in the illustration) that connects your computer to the cable or DSL modem. A Connecting the Firewall to the Internet BETA 3-1 Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 d. Securely insert the Ethernet cable from your modem into the FVG318 Internet port (point B in the illustration). Securely insert one end of the blue NETGEAR cable that came with your FVG318 into a Local port on the router such as port 4 (point C in the illustration), and the other end into the Ethernet port of your computer (point D in the illustration) . e. B D C 2. Restart your network in the correct sequence Warning: Failure to restart your network in the correct sequence could prevent you from connecting to the Internet. a. b. c.

First, plug in and turn on the cable or DSL modem.Wait about 2 minutes. Now, plug in the power cord to your FVG318 and wait about 30 seconds. Last, turn on your computer. Note: For DSL customers, if ISP-provided software logs you in to the Internet, do not run that software.

You may need to go to the Internet Explorer® Tools menu, Internet Options, Connections tab page where you can select the "Never dial a connection" radio button and click Apply.

d. Check the status lights and verify the following: 3-2 BETA Connecting the Firewall to the Internet Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 Power Test Internet Port Local Port 4 Wireless · · · Power: The power light should be lit. If after 2 minutes the power light turns solid amber, see the Troubleshooting Tips in this guide. Test: The test light blinks when the FVG318 is first turned on. If after 2 minutes it is still on, see the Troubleshooting Tips in this guide. Internet: The Internet light on the FVG318 should be lit. If not, make sure the Ethernet cable is securely attached to the wireless VPN firewall Internet port and the powered on modem. Wireless: The WLAN light should be lit.

If the Wireless light is not lit, see the Troubleshooting Tips in this guide. LOCAL: A LOCAL light should be lit. · · Now, Configure the FVG318 for Internet Access and Wireless Connectivity Use the Smart Wizard configuration assistant to configure the FVG318. 1. From the Ethernet connected computer you just set up, open a browser. With the FVG318 in its factory default state, your browser will display the NETGEAR Smart Wizard welcome page. Note: If you do not see this page, type http:// www.routerlogin.net in the browser address bar and click Enter. If you still cannot connect to the FVG318, verify your computer networking setup.

Your computer should be set to obtain both IP and DNS server addresses automatically, which is usually so. For help with this, please see the Reference Manual or animated tutorials on the Resource CD. Connecting the Firewall to the Internet BETA 3-3 Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 Click OK to proceed. 2.

3. 4. Follow the Smart Wizard prompts to connect to the Internet and set up wireless connectivity. Click Done on the Success screen and, if prompted, click OK to finish and close the screen. Verify wireless connectivity.

Connect to the Internet or log in to the FVG318 from a computer with a wireless adapter. For wireless connectivity problems, see the Troubleshooting Tips below or in the Reference Manual on the CD. Note: The configuration wizard only appears when the FVG318 is in its factory default state. After you configure the FVG318, it will not appear again. You can always connect to the router configuration menu to change its settings. To do so, open a browser and go to http://www.routerlogin.net. Then, when prompted, enter admin as the user name and password for the password both in lower case letters. Troubleshooting Tips Here are some tips for correcting simple problems you may have.

Be sure to restart your network in the correct sequence. Always follow this sequence: 1) Unplug and turn off the modem, FVG318, and computer; 2) plug in and turn on the modem, wait two minutes; 3) plug in the FVG318 and wait 30 seconds; 4) turn on the computer. Make sure the Ethernet cables are securely plugged in. · For each powered on computer connected to the wireless VPN firewall with a securely plugged in Ethernet cable, the corresponding wireless VPN firewall LAN port status light will be lit. The label on the bottom of the wireless VPN firewall identifies the number of each LAN port. · The Internet port status light on the wireless VPN firewall will be lit if the Ethernet cable from the FVG318 to the modem is plugged in securely and the modem and wireless VPN firewall are turned on. 3-4 BETA Connecting the Firewall to the Internet Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 Make sure the computer & router wireless settings match exactly. The Wireless Network Name (SSID) and security settings (WEP/WPA, MAC access control list) of the FVG318 and wireless computer must match exactly. Make sure the network settings of the computer are correct.

· · LAN and wirelessly connected computers must be configured to obtain an IP address automatically via DHCP. Some cable modem ISPs require you to use the MAC address of the computer registered on the account. If so, in the Router MAC Address section of the Basic Settings menu, select, "Use this Computer's MAC Address." The router will then capture and use the MAC address of the computer that you are now using. You must be using the computer that is registered with the ISP.

Click Apply to save your settings. Restart the network in the correct sequence. Check the router status lights to verify correct router operation. · · If the Power light does not turn solid green within 2 minutes after turning the router on, reset the router according to the instructions in the Reference Manual on the CD. If the Wireless light does not come on, verify that the wireless feature is turned on according to the instructions in the Reference Manual on the CD. Connecting the Firewall to the Internet BETA 3-5 Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 Overview of How to Access the FVG318 Wireless VPN Firewall The table below describes how you access the wireless VPN firewall, depending on the state of the wireless VPN firewall. Table 3-1. Firewall State Factory Default Automatic Access via the Smart Wizard Configuration Assistant Access Options Description Any time a browser is opened on any computer connected to the wireless VPN firewall, the wireless VPN firewall will automatically connect to that browser and display the Configuration Assistant welcome page. There is no need to enter the wireless VPN firewall URL in the browser, or provide the login user name and password. Manually enter a URL You can bypass the Smart Wizard Configuration Assistant to bypass the Smart feature by typing Wizard Configuration http://www.routerlogin.net/basicsetting.htm in the browser address bar and pressing Enter. You will not Assistant be prompted for a user name or password.

This will enable you to manually configure the wireless VPN firewall even when it is in the factory default state. When manually configuring the firewall, you must complete the configuration by clicking Apply when you finish entering your settings. If you do not do so, a browser on any PC connected to the firewall will automatically display the firewall's Configuration Assistant welcome page rather than the browser's home page. Ways to access the firewall Note: The wireless VPN firewall is supplied in the factory default state. Also, the factory default state is restored when you use the factory reset button. See "Backing Up the Configuration" on page 8-7 for more information on this feature. 3-6 BETA Connecting the Firewall to the Internet Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 Table 3-1. Firewall State Configuration Settings Have Been Applied Enter the standard URL to access the wireless VPN firewall Access Options Description Connect to the wireless VPN firewall by typing either of these URLs in the address field of your browser, then press Enter: Ways to access the firewall (continued) http://www.

routerlogin.

net http://www.routerlogin.com The wireless VPN firewall will prompt you to enter the user name of admin and the password. The default password is password. Enter the IP address of the wireless VPN firewall Connect to the wireless VPN firewall by typing the IP address of the wireless VPN firewall in the address field of your browser, then press Enter.

192.168.0.1 is the default IP address of the wireless VPN firewall. The wireless VPN firewall will prompt you to enter the user name of admin and the password.

The default password is password. How to Log On to the FVG318 After Configuration Settings Have Been Applied 1. Connect to the wireless VPN firewall by typing http://www.routerlogin.net in the address field of your browser, then press Enter. Figure 3-1: Login URL 2. For security reasons, the firewall has its own user name and password. When prompted, enter admin for the firewall user name and password for the firewall password, both in lower case letters. To change the password, see "Changing the Administrator Password" on page 8-8 Note: The 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. A login window like the one shown below opens: Connecting the Firewall to the Internet BETA 3-7 Reference Manual for the ProSafe 802.

11g Wireless VPN Firewall FVG318 Figure 3-2: Login window Once you have entered your user name and password, your Web browser should find the FVG318 Wireless VPN Firewall and display the home page as shown below. Figure 3-3: Login result: FVG318 home page NEED NEW SCREEN When the wireless VPN firewall is connected to the Internet, click the Knowledge Base or the Documentation link under the Web Support menu to view support information or the documentation for the wireless VPN firewall. If you do not click Logout, the wireless VPN firewall will wait five minutes after there is no activity before it automatically logs you out. How to Bypass the Configuration Assistant 1. When the wireless VPN firewall is in the factory default state, type http://www.routerlogin.net/basicsetting.htm in your browser, then press Enter. 3-8 BETA Connecting the Firewall to the Internet Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 When the wireless VPN firewall is in the factory default state, a user name and password are not required. 2. The browser then displays the FVG318 settings home page shown in "Login result: FVG318 home page NEED NEW SCREEN" on page 3-8. If you do not click Logout, the wireless VPN firewall waits five minutes after there is no activity before it automatically logs you out. Using the Smart Setup Wizard You can use the Smart Setup Wizard to assist with manual configuration or to verify the Internet connection. The Smart Setup Wizard is not the same as the Smart Wizard Configuration Assistant (as illustrated in Figure 3-5) that only appears when the firewall is in its factory default state.

After you configure the wireless VPN firewall, the Smart Wizard Configuration Assistant will not appear again. To use the Smart Setup Wizard to assist with manual configuration or to verify the Internet connection settings, follow this procedure. 1. 2. Connect to the wireless VPN firewall by typing http://www.routerlogin.net in the address field of your browser, then press Enter. For security reasons, the firewall has its own user name and password. When prompted, enter admin for the firewall user name and password for the firewall password, both in lower case letters. To change the password, see "Changing the Administrator Password" on page 8-8 Note: The 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. Once you have entered your user name and password, your Web browser should find the FVG318 Wireless VPN Firewall and display the home page as shown in Figure 3-3. 3. 4. 5. Click Setup Wizard on the upper left of the main menu.

Click Next to proceed. Input your ISP settings, as needed. At the end of the Setup Wizard, click the Test button to verify your Internet connection. If you have trouble connecting to the Internet, use the Troubleshooting Tips "Troubleshooting Tips" on page 3-4 to correct basic problems, or refer to Chapter 10, "Troubleshooting." Connecting the Firewall to the Internet BETA 3-9 Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 How to Manually Configure Your Internet Connection You can manually configure your firewall using the menu below, or you can allow the Setup Wizard to determine your configuration as described in the previous section. ISP Does Not Require Login ISP Does Require Login Figure 3-4: Browser-based configuration Basic Settings menu NEED NEW SCREENs 3-10 BETA Connecting the Firewall to the Internet Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 You can manually configure the firewall using the Basic Settings menu shown in Figure 3-4 using these steps: 1. 2. 3. Log in to the firewall at its default address of http://www.routerlogin.net using a browser like Internet Explorer or Netscape® Navigator. Click the Basic Settings link under the Setup section of the main menu. If your Internet connection does not require a login, click No at the top of the Basic Settings menu and fill in the settings according to the instructions below.

If your Internet connection does require a login, click Yes, and skip to step 4. a. Account: Enter your Account Name (may also be called Host Name) and Domain Name. These parameters may be necessary to access your ISP's services such as mail or news servers. Internet IP Address: If your ISP has assigned you a permanent, fixed (static) IP address for your PC, select "Use static IP address".

Enter the IP address that your ISP assigned. Also enter the netmask and the Gateway IP address. The Gateway is the ISP's firewall to which your firewall will connect. Domain Name Server (DNS) Address: If you know that your ISP does not automatically transmit DNS addresses to the firewall during login, select "Use these DNS servers" and enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also. Note: After completing the DNS configuration, restart the computers on your network so that these settings take effect. b. c. d. Firewall's MAC Address: This section determines the Ethernet MAC address that will be used by the firewall on the Internet port.

Some ISPs will register the Ethernet MAC address of the network interface card in your PC when your account is first opened. They will then only accept traffic from the MAC address of that PC. This feature allows your firewall to masquerade as that PC by "cloning" its MAC address. To change the MAC address, select "Use this Computer's MAC address.

" The firewall will then capture and use the MAC address of the PC that you are now using. You must be using the one PC that is allowed by the ISP. Or, select "Use this MAC address" and enter it. e. Click Apply to save your settings. Connecting the Firewall to the Internet BETA 3-11 Reference Manual for the ProSafe 802.

11g Wireless VPN Firewall FVG318 4. If your Internet connection does require a login, fill in the settings according to the instructions below. Select Yes if you normally must launch a login program such as Enternet or WinPOET in order to access the Internet. Note: After you finish setting up your firewall, you will no longer need to launch the ISP's login program on your PC in order to access the Internet. When you start an Internet application, your firewall will automatically log you in.

a. For connections that require a login using protocols such as PPPoE, PPTP, Telstra Bigpond Cable broadband connections, select your Internet service provider from the drop-down list. Figure 3-5: Basic Settings ISP list b. c. d.

The screen will change according to the ISP settings requirements of the ISP you select. Fill in the parameters for your ISP according to the Wizard-detected procedures starting on page 3-9. Click Apply to save your settings. 3-12 BETA Connecting the Firewall to the Internet Chapter 4 Wireless Configuration This chapter describes how to configure the wireless features of your FVG318 Wireless VPN Firewall. Observing Performance, Placement, and Range Guidelines In planning your wireless network, you should consider the level of security required. You should also select the physical placement of your FVG318 in order to maximize the network speed. For further information on wireless networking, refer to in Appendix E, "Wireless Networking Basics." Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the wireless VPN firewall. For complete range and performance specifications, please see Appendix A, "Technical Specifications." The operating distance or range of your wireless connection can vary significantly based on the physical placement of the FVG318 Wireless VPN Firewall.

The latency, data throughput performance, and notebook power consumption also vary depending on your configuration choices. For best results, place your wireless VPN firewall: · Near the center of the area in which your PCs will operate. · In an elevated location, such as a high shelf where the wirelessly 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 sources of interference, such as PCs, microwaves, and 2.4 GHz cordless phones. · Away from large metal surfaces. 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. Wireless Configuration BETA 4-1 Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 Implementing Appropriate Wireless Security 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 FVG318 Wireless VPN Firewall provides highly effective security features which are covered in detail in this chapter. FVG318 Figure 4-1: FVG318 wireless data security options 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 FVG318. 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. 4-2 BETA Wireless Configuration Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 · 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 To configure the wireless settings of your FVG318, click the Wireless link in the Setup section of the main menu. The wireless settings menu will appear, as shown below. Figure 4-2: Wireless Settings menu Note: The 802.11b and 802.11g wireless networking protocols are configured in exactly the same fashion. The FVG318 will automatically adjust to the 802.11g or 802.11b protocol as the device requires without compromising the speed of the other devices. Wireless Configuration BETA 4-3 Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 · Wireless Network.

The station name of the FVG318. -- 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 FVG318 default SSID is: NETGEAR. -- Region. This field identifies the region where the FVG318 can be used.

It may not be legal to operate the wireless features of the wireless VPN firewall in a region other than one of those identified in this field. Unless you select a region, you will only be able to use Channel 11. -- Channel. 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. For more information on the wireless channel frequencies, please refer to "Wireless Channels" on page E-7. -- Mode. Select the desired wireless mode. The options are: · · · g & b - Both 802.

11g and 802.

11b wireless stations can be used. g only - Only 802.11g wireless stations can be used. b only - All 802.11b wireless stations can be used. 802.11g wireless stations can still be used if they can operate in 802.11b mode. The default is "g & b" which allows both 802.11g and 802.
11b wireless stations to access this device. · Wireless Access Point -- Enable Wireless Access Point. Enables the wireless radio. When disabled, there are no wireless communications through the FVG318. -- Allow Broadcast of Name (SSID).
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 Card Access List Lets you restrict wireless connections according to a list of Trusted PCs MAC addresses. When the Trusted PCs Only radio button is selected, the FVG318 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, click the Set up Access List button and update the MAC access control list. 4-4 BETA Wireless Configuration Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 · WEP (Wired Equivalent Privacy): Use WEP 64 or 128 bit data encryption. Disable: No data encryption is used. Security Options 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. If selected, you must configure the Radius Server Settings. WPA-PSK (Wi-Fi Protected Access Pre-Shared Key): Use WPA-PSK standard encryption WPA2-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. Wireless Configuration BETA 4-5 Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 Default Factory Settings The FVG318 default factory settings shown below. You can restore these defaults with the Factory Default Restore button on the rear panel as seen in the illustration "FWG114P v2 Rear Panel" on page 2-9.
After you install the FVG318 Wireless VPN Firewall, use the procedures below to customize any of the settings to better meet your networking needs. FEATURE SSID RF Channel Access Point SSID broadcast Wireless Card Access List for Access Point Connections WEP Security Authentication Type Disabled Open System Enabled All wireless stations allowed Enabled NETGEAR 11 until the region is selected DEFAULT FACTORY SETTINGS 4-6 BETA Wireless Configuration Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 Before You Change the SSID and WEP Settings Take the following steps: 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. Wireless is the default FVG318 SSID. However, you may customize it by using up to 32 alphanumeric characters. Write your customized SSID on the line below. Note: The SSID in the wireless VPN firewall is the SSID you configure in the wireless adapter card. All wireless nodes in the same network must be configured with the same SSID: Authentication Circle one: Open System or Shared Key. Choose "Shared Key" for more security. Note: If you select shared key, the other devices in the network will not connect unless they are set to Shared Key as well and have the same keys in the same positions as those in the FVG318. WEP Encryption Keys For all four 802.11b keys, choose the Key Size.

Circle one: 64 or 128 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: _____ Use the procedures described in the following sections to configure the FVG318. Store this information in a safe place. Wireless Configuration BETA 4-7 Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 How to Set Up and Test Basic Wireless Connectivity Follow the instructions below to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs. 1. Log in using the default LAN address of http://192.168.0.1 with the default user name of admin and default password of password, or using whatever LAN address and password you have set up.
Figure 4-3: Wireless Settings menu 2. 3. Set the Regulatory Domain correctly. Choose a suitable descriptive name for the wireless network name (SSID). In the SSID box, enter a value of up to 32 alphanumeric characters.
The default SSID is NETGEAR. Note: The characters are case sensitive. An access point always functions in infrastructure mode. The SSID for any wireless device communicating with the access point must match the SSID configured in the FVG318 ProSafe 802.11g Wireless VPN Firewall.
If they do not match, you will not get a wireless connection to the FVG318. 4. Set the Channel. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless router or access point.

Select a channel that is not being used by any other wireless networks within several hundred feet of your wireless VPN firewall. For more information on the wireless channel frequencies please refer to "Wireless Channels" on page E-7. 5. 6. Depending on the types of wireless adapters you have in your computers, choose from the Mode drop-down list. For initial configuration and test, leave the Wireless Card Access List set to "All Wireless Stations" and the Encryption Strength set to "Disable.

" 4-8 BETA Wireless Configuration Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 7. Click Apply to save your changes. Note: If you are configuring the FVG318 from a wireless computer and you change the wireless VPN firewall's SSID, channel, or security settings, you will lose your wireless connection when you click on Apply. You must then change the wireless settings of your computer to match the FVG318's new settings. 8. Configure and test your PCs for wireless connectivity. Program the wireless adapter of your PCs to have the same SSID that you configured in the FVG318. Check that they have a wireless link and are able to obtain an IP address by DHCP from the wireless VPN firewall. Once your PCs have basic wireless connectivity to the wireless VPN firewall, then you can configure the advanced options and wireless security functions.

How to Restrict Wireless Access by MAC Address To restrict access based on MAC addresses, follow these steps: 1. 2. Log in at the default LAN address of http://192.168.0.

1 with the default user name of admin and default password of password. Click Wireless in the main menu of the FVG318. From the Wireless Settings menu, click Setup Access List. Figure 4-4: Wireless Station Access menu 3. Click the Turn Access Control On checkbox to enable MAC filtering.

Wireless Configuration BETA 4-9 Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 4. Click Add to open the Wireless Card Access Setup menu. You can select a device from the list of available wireless cards the FVG318 has discovered in your area, or you can manually enter the MAC address and Device Name (usually the NetBIOS name). Click Add to add this device to your MAC access control list. Note: When configuring the FVG318 from a wireless computer whose MAC address is not in the access control list, if you select Turn Access Control On, you will lose your wireless connection when you click Apply. You must then access the wireless VPN firewall from a wired computer or from a wireless computer which is on the access control list to make any further changes. 5. 6. Be sure to click Apply to save your trusted wireless PCs list settings.

Now, only devices on this list will be allowed to wirelessly connect to the FVG318. To remove a MAC address from the table, click to select it, then click the Delete button. How to Configure WEP Note: When changing the wireless settings from a wireless computer, you will lose your wireless connection when you click Apply. You must then either configure your wireless adapter to match the new wireless settings or access the wireless VPN firewall from a wired computer to make any further changes. To configure WEP data encryption, follow these steps: 1. Log in at the default LAN address of http://192.168.0.1 with the default user name of admin and default password of password, or using whatever LAN address and password you set up. 4-10 BETA Wireless Configuration Reference Manual for the ProSafe 802.

11g Wireless VPN Firewall FVG318 2. Click Wireless Settings in the main menu of the FVG318. Figure 4-5: Wireless Settings menu (WEP) 3. 4. Select WEP on the pulldown menu.

The WEP options menu will open. Choose the Authentication Type and Encryption Strength options. You can manually or automatically program the four data encryption keys. These values must be identical on all PCs and Access Points in your network. Authentication Type: Normally this can be left at the default value of "Automatic.

" If set to "Open System" or "Shared Key", wireless stations must use the same method. Encryption: Select the desired WEP Encryption: · · 64-bit (sometimes called 40-bit) encryption 128-bit encryption Wireless Configuration BETA 4-11 Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 WEP Keys: If using WEP, you can manually or automatically program the four data encryption keys. These values must be identical on all PCs and Access Points in your network. · Automatic Key Generation (Passphrase): Enter a word or group of printable characters (this phrase is case sensitive) in the Passphrase box and click the "Generate Keys" button to automatically configure the WEP Key(s). · If encryption is set to 64 bit, then each of the four key boxes will automatically be populated with key values. If encryption is set to 128 bit, then only the selected WEP key box will automatically be populated with a key value. Manual Entry Mode: Enter ten hexadecimal digits (any combination of 0-9, a-f, or A-F). These hex values are not case sensitive. Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key box.

For 64 bit WEP: Enter ten hexadecimal digits (any combination of 0-9, A-F). For 128 bit WEP: Enter twenty-six hexadecimal digits (any combination of 0-9, A-F). Please refer to "Overview of WEP Parameters" on page E-5 for a full explanation of each of these options, as defined by the IEEE 802.11b wireless communication standard. 5. Click Apply to save your settings. How to Configure WPA with Radius Note: Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 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, follow these steps: 1. Log in at the default LAN address of http://192.168.0.

1 with the default user name of admin and default password of password, or using whatever LAN address and password you have set up. 4-12 BETA Wireless Configuration Reference Manual for the ProSafe 802.11g Wireless VPN Firewall FVG318 2. Click Wireless Settings in the main menu of the FVG318. Figure 4-6: Wireless Settings menu (WPA with Radius) 3.

Select WPA with Radius on the pulldown menu. The WPA with Radius menu will open. Encryption: There is no choice for encryption; this is displayed for your information. For WPA with Radius, TKIP is used. 4. Enter the Radius settings. · · Primary Server Name/IP Address: This field is required. Enter the name or IP address of the primary Radius Server on your LAN.