Reference Manual for the ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2

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

201-10301-02
May 2005

Trademarks

NETGEAR is a trademark of Netgear, Inc.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

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

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

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

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

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

FCC Caution

1. FCC RF Radiation Exposure Statement: The equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.
2. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
3. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

EN 55 022 Declaration of Conformance

This is to certify that the ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2 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).

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2 gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Certificate of the Manufacturer/Importer

It is hereby certified that the ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2 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.

Product and Publication Details

Model Number:	FWG114P v2
Publication Date:	May 2005
Product Family:	wireless access point
Product Name:	ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2
Home or Business Product:	Business
Language:	English
Publication Part Number:	201-10301-02

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 1-3

Chapter 2
Introduction

Key Features of the FWG114P v2 2-1
Full Routing on Both the Broadband and Serial Ports 2-2
802.11g and 802.11b Wireless Networking 2-2
Virtual Private Networking 2-3
Wireless Multimedia (WMM) Support 2-3
A Powerful, True Firewall with Content Filtering 2-3
Security 2-4
Autosensing Ethernet Connections with Auto Uplink 2-4
Extensive Protocol Support 2-5
Easy Installation and Management 2-6
NETGEAR Related Products 2-6
Package Contents 2-7
The FWG114P v2 Front Panel 2-7
The FWG114P v2 Rear Panel 2-8

Chapter 3
Connecting the FWG114P v2 to the Internet

What You Will Need Before You Begin 3-1
Cabling and Computer Hardware Requirements 3-1
Computer Network Configuration Requirements 3-1
Internet Configuration Requirements 3-2
Where Do I Get the Internet Configuration Parameters? 3-2
Record Your Internet Connection Information 3-3

Connecting the FWG114P v2 Wireless Firewall/Print Server 3-4
Verify That Basic Requirements Are Met 3-4
Basic Setup Troubleshooting Tips 3-10
FWG114P v2 Setup Wizard Auto Detection 3-10
Wizard-Detected Login Account Setup 3-11
Wizard-Detected Dynamic IP Account Setup 3-13
Wizard-Detected Fixed IP Account Setup 3-14
How to Configure the Serial Port as the Primary Internet Connection 3-15
Testing Your Internet Connection 3-17
Manually Configuring Your Internet Connection 3-18
How to Manually Configure the Primary Internet Connection 3-19

Chapter 4
Wireless Configuration

Observing Performance, Placement, and Range Guidelines 4-1
Implementing Appropriate Wireless Security 4-2
Understanding Wireless Settings 4-3
Default Factory Settings 4-6
Before You Change the SSID and WEP Settings 4-7
How to Set Up and Test Basic Wireless Connectivity 4-8
How to Restrict Wireless Access by MAC Address 4-9
How to Configure WEP 4-10
How to Configure WPA with Radius 4-12
How to Configure WPA2 with Radius 4-14
How to Configure WPA and WPA2 with Radius 4-16
How to Configure WPA-PSK 4-18
How to Configure WPA2-PSK 4-20
How to Configure WPA-PSK and WPA2-PSK 4-21

Chapter 5
Serial Port Configuration

Configuring a Serial Port Modem 5-2
Basic Requirements for Serial Port Modem Configuration 5-2
How to Configure a Serial Port Modem 5-2
Configuring Auto-Rollover 5-3
Basic Requirements for Auto-Rollover 5-3
How to Configure Auto-Rollover 5-3

Configuring Dial-in on the Serial Port 5-4
Basic Requirements for Dial-in 5-5
How to Configure Dial-in 5-5
Configuring LAN-to-LAN Settings 5-6
Basic Requirements for LAN-to-LAN Connections 5-6
How to Configure LAN-to-LAN Connections 5-6

Chapter 6
Firewall Protection and Content Filtering

Firewall Protection and Content Filtering Overview 6-1
Using the Block Sites Menu to Screen Content 6-1
Services and Rules Regulate Inbound and Outbound Traffic 6-3
Defining a Service 6-3
Using Inbound/Outbound Rules to Block or Allow Services 6-4
Examples of Using Services and Rules to Regulate Traffic 6-6
Inbound Rules (Port Forwarding) 6-6
Example: Port Forwarding to a Local Public Web Server 6-7
Example: Port Forwarding for Videoconferencing 6-8
Example: Port Forwarding for VPN Tunnels when NAT is Off 6-8
Outbound Rules (Service Blocking or Port Filtering) 6-9
Outbound Rule Example: Blocking Instant Messaging 6-10
Other Rules Considerations 6-10
Order of Precedence for Rules 6-11
Rules Menu Options 6-11
Using a Schedule to Block or Allow Content or Traffic 6-12
Setting the Time Zone 6-13
Getting E-Mail Notifications of Event Logs and Alerts 6-13
Viewing Logs of Web Access or Attempted Web Access 6-16
What to Include in the Event Log 6-17

Chapter 7
Print Server

Printing Options 7-1
For Windows XP and 2000, Use TCP/IP LPR Printing 7-2
For Windows 95/98/Me, Use the Netgear Printer Port Driver 7-6
Printing from the Macintosh 7-9
Windows Printer Port Management 7-10

Troubleshooting the Print Server 7-12

Chapter 8
Virtual Private Networking

Overview of FWG114P v2 Policy-Based VPN Configuration 8-1
Using Policies to Manage VPN Traffic 8-2
Using Automatic Key Management 8-2
IKE Policies’ Automatic Key and Authentication Management 8-3
VPN Policy Configuration for Auto Key Negotiation 8-6
VPN Policy Configuration for Manual Key Exchange 8-9
Using Digital Certificates for IKE Auto-Policy Authentication 8-14
Certificate Revocation List (CRL) 8-14
Walk-Through of Configuration Scenarios on the FWG114P v2 8-15
How to Use the VPN Wizard to Configure a VPN Tunnel 8-15
VPNC Scenario 1: Gateway to Gateway with Preshared Secrets 8-19
Scenario 1: FWG114P v2 to FWG114P v2 with Preshared Secrets 8-20
How to Check VPN Connections 8-24
VPNC Scenario 2: Gateway-to-Gateway with Certificates 8-25
Scenario 2: FWG114P v2 to FWG114P v2 with Certificates 8-26
Netgear VPN Client to FWG114P v2 8-32
Configuration Profile 8-32
Step-By-Step Configuration of FWG114P v2 Gateway 8-33
Step-By-Step Configuration of the Netgear VPN Client 8-38
Testing the VPN Connection 8-45
From the Client PC to the FWG114P v2 8-45
From the FWG114P v2 to the Client PC 8-46
Monitoring the PC VPN Connection 8-46
Viewing the FWG114P v2 VPN Status and Log Information 8-47

Chapter 9
Maintenance

Viewing Wireless Firewall/Print Server Status Information 9-1
Viewing a List of Attached Devices 9-6
Upgrading the Router Software 9-7
Configuration File Management 9-7
Restoring and Backing Up the Configuration 9-8
Erasing the Configuration 9-9

Changing the Administrator Password 9-9

Chapter 10
Advanced Configuration

Using the WAN Setup Options 10-1
How to Configure Dynamic DNS 10-3
Using the LAN IP Setup Options 10-5
Configuring LAN TCP/IP Setup Parameters 10-5
Using the Router as a DHCP server 10-7
Using Address Reservation 10-7
Configuring Static Routes 10-8
Enabling Remote Management Access 10-10
Using Universal Plug and Play (UPnP) 10-11
Advanced Wireless Settings 10-12

Chapter 11
Troubleshooting

Basic Functioning 11-1
Power LED Not On 11-1
LEDs Never Turn Off 11-2
LAN or Internet Port LEDs Not On 11-2
Troubleshooting the Web Configuration Interface 11-3
Troubleshooting the ISP Connection 11-4
Troubleshooting a TCP/IP Network Using a Ping Utility 11-5
Testing the LAN Path to Your Router 11-5
Testing the Path from Your Computer to a Remote Device 11-6
Restoring the Default Configuration and Password 11-7
Problems with Date and Time 11-7

Appendix A
Technical Specifications

Appendix B
Networks, Routing, and Firewall Basics

Related Publications B-1
Basic Router Concepts B-1
What is a Router? B-1
Routing Information Protocol B-2
IP Addresses and the Internet B-2
Netmask B-4

Subnet Addressing B-4
Private IP Addresses B-7
Single IP Address Operation Using NAT B-7
MAC Addresses and Address Resolution Protocol B-9
Related Documents B-9
Domain Name Server B-9
IP Configuration by DHCP B-10
Internet Security and Firewalls B-10
What is a Firewall? B-11
Stateful Packet Inspection B-11
Denial of Service Attack B-11
Ethernet Cabling B-11
Category 5 Cable Quality B-12
Inside Twisted Pair Cables B-13
Uplink Switches, Crossover Cables, and MDI/MDIX Switching B-14

Appendix C
Preparing Your Network

Preparing Your Computers for TCP/IP Networking C-1
Configuring Windows 95, 98, and Me for TCP/IP Networking C-2
Install or Verify Windows Networking Components C-2
Enabling DHCP to Automatically Configure TCP/IP Settings C-4
Selecting Windows’ Internet Access Method C-4
Verifying TCP/IP Properties C-5
Configuring Windows NT, 2000 or XP for IP Networking C-5
Installing or Verifying Windows Networking Components C-5
Verifying TCP/IP Properties C-6
Configuring the Macintosh for TCP/IP Networking C-6
MacOS 8.6 or 9.x C-6
MacOS X C-7
Verifying TCP/IP Properties for Macintosh Computers C-8
Verifying the Readiness of Your Internet Account C-9
Are Login Protocols Used? C-9
What Is Your Configuration Information? C-9
Obtaining ISP Configuration Information for Windows Computers C-10
Obtaining ISP Configuration Information for Macintosh Computers C-11

Restarting the Network C-12

Appendix D
Firewall Log Formats

Action List D-1
Field List D-1
Outbound Log D-1
Inbound Log D-2
Other IP Traffic D-2
Router Operation D-3
Other Connections and Traffic to this Router D-4
DoS Attack/Scan D-4
Access Block Site D-6
All Web Sites and News Groups Visited D-6
System Admin Sessions D-6
Policy Administration LOG D-7

Appendix E
Wireless Networking Basics

Wireless Networking Overview E-1
Infrastructure Mode E-1
Ad Hoc Mode (Peer-to-Peer Workgroup) E-2
Network Name: Extended Service Set Identification (ESSID) E-2
Authentication and WEP Data Encryption E-2
802.11 Authentication E-3
Open System Authentication E-3
Shared Key Authentication E-4
Overview of WEP Parameters E-5
Key Size E-6
WEP Configuration Options E-7
Wireless Channels E-7
WPA Wireless Security E-8
How Does WPA Compare to WEP? E-9
How Does WPA Compare to IEEE 802.11i? E-10
What are the Key Features of WPA Security? E-10
WPA Authentication: Enterprise-level User Authentication via 802.1x/EAP and RADIUS E-12
WPA Data Encryption Key Management E-14

Is WPA Perfect? E-16
Product Support for WPA E-16
Supporting a Mixture of WPA and WEP Wireless Clients is Discouraged E-16
Changes to Wireless Access Points E-17
Changes to Wireless Network Adapters E-17
Changes to Wireless Client Programs E-18

Appendix F
Virtual Private Networking

What is a VPN? F-1
What is IPSec and How Does It Work? F-2
IPSec Security Features F-2
IPSec Components F-2
Encapsulating Security Payload (ESP) F-3
Authentication Header (AH) F-4
IKE Security Association F-4
Mode F-5
Key Management F-6
Understand the Process Before You Begin F-6
VPN Process Overview F-7
Network Interfaces and Addresses F-7
Interface Addressing F-7
Firewalls F-8
Setting Up a VPN Tunnel Between Gateways F-8
VPNC IKE Security Parameters F-10
VPNC IKE Phase I Parameters F-10
VPNC IKE Phase II Parameters F-11
Testing and Troubleshooting F-11
Additional Reading F-11

Appendix G
NETGEAR VPN Configuration
FVS318 or FVM318 to FWG114P v2

Configuration Template G-1
Step-By-Step Configuration of FVS318 or FVM318 Gateway A G-2
Step-By-Step Configuration of FWG114P Gateway B G-5
Test the VPN Connection G-9

Appendix H
NETGEAR VPN Configuration
FVS318 or FVM318 with FQDN to FVS328

Configuration Template H-1
Using DDNS and Fully Qualified Domain Names (FQDN) H-2
Step-By-Step Configuration of FVS318 or FVM318 Gateway A H-3
Step-By-Step Configuration of FVS328 Gateway B H-7
Test the VPN Connection H-11
Glossary

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 website.

This guide uses the following typographical conventions:

Table 1-1. Typographical Conventions

italics	Emphasis, books, CDs, URL names
bold	User input
`fixed`	Screen text, file and server names, extensions, commands, IP addresses

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 FWG114P v2 Wireless Firewall/Print Server according to these specifications:

Table 1-2. Manual Scope

Product Version	ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2
Manual Publication Date	May 2005

Note: Product updates are available on the NETGEAR, Inc. Web site at *http://kbserver.netgear.com/products/FWG114P v2.asp*.

How to Use This Manual

The HTML version of this manual includes the following:

- Buttons, > and <, for browsing forwards or backwards through the manual one page at a time
- A TOC button that displays the table of contents and an Index 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 Knowledge Base button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

How to Print this Manual

To print this manual you can choose one of the following several options, according to your needs.

- **Printing a Page in the HTML View**.

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

- **Printing a Chapter**.

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

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

  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.

Chapter 2
Introduction

This chapter describes the features of the NETGEAR ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2.

Key Features of the FWG114P v2

The ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2, with a 4-port switch, connects your LAN to the Internet through a broadband modem. With auto fail-over connectivity through the serial port, the FWG114P v2 provides highly reliable Internet access.

The FWG114P v2 is a complete security solution that protects your network from attacks and intrusions and enables secure communications using Virtual Private Networks (VPNs). Unlike simple Internet sharing routers that rely on Network Address Translation (NAT) for security, the FWG114P v2 uses Stateful Packet Inspection for Denial of Service attack (DoS) attack protection and intrusion detection. The FWG114P v2 allows Internet access for up to 253 users. It provides multiple Web content filtering options, plus browsing activity reporting and instant alerts via e-mail. Parents or 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.

With minimum setup, you can install and use the router within minutes. The FWG114P v2 Wireless Firewall/Print Server provides the following features:

- 802.11g and 802.11b standards-based wireless networking.
- Easy, Web-based setup for installation and management.
- Supports two VPN tunnels, Content Filtering, and Site Blocking Security.
- Wireless Multimedia (WMM) support.
- Built-in 4-port 10/100 Mbps Switch and USB 2.0 Printer Port.
- Ethernet and Serial ports for connection to a WAN device, such as a broadband modem.
- Extensive Protocol Support.
- Login capability.
- Front panel LEDs for easy monitoring of status and activity.

- Flash memory for firmware upgrade.
- NAT off (classical routing).

Full Routing on Both the Broadband and Serial Ports

You can install, configure, and operate the FWG114P v2 to take full advantage of a variety of routing options on both the serial and broadband WAN ports, including:

- Internet access via either the serial or broadband port.
- Auto fail-over connectivity through an analog or ISDN modem connected to the serial port. If the broadband Internet connection fails, after waiting for an amount of time you specify, the FWG114P v2 can automatically establish a backup ISDN or dial-up Internet connection via the serial port on the firewall.
- Remote Access Server (RAS) that allows you to log in remotely through the serial port to access a server on your LAN, other LAN resources, or the Internet, based on a user name and password you define.
- LAN-to-LAN access between two FWG114P v2 wireless firewall/print servers through the serial port, with the option of enabling auto-failover Internet access across the serial LAN-to-LAN connection.

802.11g and 802.11b Wireless Networking

The FWG114P v2 Wireless Firewall/Print Server includes an 802.11g-compliant wireless access point. The access point provides:

- 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.
- 64-bit and 128-bit WEP encryption security.
- 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.

Virtual Private Networking

The FWG114P v2 Wireless Firewall/Print Server provides a secure encrypted connection between your local network and remote networks or clients. Its VPN features include:

- Support for up to 2 simultaneous VPN connections.
- Support for industry standard VPN protocols.

  The ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2 supports standard keying methods (Manual or IKE), standard authentication methods (MD5 and SHA-1), and standard encryption methods (DES, 3DES). It is compatible with many other VPN products.
- Support for up to 168 bit encryption (3DES) for maximum security.
- Support for VPN Main Mode, Aggressive mode, or Manual Keying.
- Support for Fully Qualified Domain Name (FQDN) configuration when the Dynamic DNS feature is enabled with one of the supported service providers.

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 routers, the FWG114P v2 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.
- Blocks unwanted traffic from the Internet to your LAN.
- Blocks access from your LAN to Internet locations or services that you specify as off-limits.

- Logs security incidents.

  The FWG114P v2 will log security events, such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the router to e-mail the log to you at specified intervals. You can also configure the router to send immediate alert messages to your e-mail address or e-mail pager whenever a significant event occurs.
- With its content filtering feature, the FWG114P v2 prevents objectionable content from reaching your PCs. The router allows you to control access to Internet content by screening for keywords within Web addresses. You can configure the router to log and report attempts to access objectionable Internet sites.

Security

The FWG114P v2 Wireless Firewall/Print Server 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 router 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 8-port 10/100 switch, the FWG114P v2 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 router incorporates Auto Uplink™ technology. Each Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a ‘normal’ connection, such as to a computer, or an ‘uplink’ connection, such as to a switch or hub. That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

Extensive Protocol Support

The FWG114P v2 Wireless Firewall/Print Server supports the Transmission Control Protocol/ Internet Protocol (TCP/IP) and Routing Information Protocol (RIP).

- The ability to enable or disable IP address sharing by NAT.

  The FWG114P v2 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. This feature can also be turned off completely for using the FWG114P v2 in settings where you want to manage the IP address scheme of your organization.

- Automatic configuration of attached PCs by DHCP.

  The FWG114P v2 Wireless Firewall/Print Server 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 router provides its own address as a DNS server to the attached PCs. The router 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 Entersys or WinPOET on your computer.

- PPTP login support for European ISPs, BigPond login for Telstra cable in Australia.
- Classical IP (RFC 1577).

  Some Internet service providers, in Europe for example, use Classical IP in their ADSL services. In such cases, the firewall is able to use the Classical IP address from the ISP.

Easy Installation and Management

You can install, configure, and operate the ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2 within minutes after connecting it to the network. The following features simplify installation and management tasks:

- Automatic fail-over connectivity through an analog or ISDN modem connected to the serial port. If the broadband modem Internet connection fails, after waiting for an amount of time you specify, the FWG114P v2 can automatically establish a backup ISDN or dial-up Internet connection via the serial port on the firewall.
- Browser-based management.

  Browser-based configuration allows you to easily configure your router 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 FWG114P v2 Wireless Firewall/Print Server automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- Diagnostic functions.

  The firewall incorporates built-in diagnostic functions, such as Ping, DNS lookup, and remote reboot.
- Remote management.

  The firewall allows you to log in 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 FWG114P v2 Wireless Firewall/Print Server's front panel LEDs provide an easy way to monitor its status and activity.
- Regional support, including ISPs like Telstra DSL and BigPond, or Deutsche Telekom.
- Flash memory for firmware upgrades.

NETGEAR Related Products

The following NETGEAR products are related to the ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2:

- ProSafe™ Dual Band Wireless PC Card Model WAG511
- ProSafe™ Dual Band Wireless PCI Adapter Model WAG311

- 54 Mbps Wireless PC Card Model WG511
- 54 Mbps Wireless PCI Card Model WG311
- 54 Mbps Wireless USB 2.0 Adapter Model WG121
- ProSafe™ Indoor 5 dBi Omni-directional Antenna Model ANT24O5
- ProSafe™ Indoor/Outdoor 18 dBi Patch Panel Directional Antenna Model ANT24D18
- ProSafe™ Indoor/Outdoor 9 dBi Omni-directional Antenna Model ANT2409
- Low-loss Antenna Cables

Package Contents

The product package should contain the following items:

- ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2.
- AC power adapter.
- Category 5 (Cat 5) Ethernet cable.
- FWG114P Installation Guide (201-10301-01).
- *Resource CD for the ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P (SW-10023-03)*, including:
  - — This manual.
  - — Application Notes and other helpful information.
- Registration and Warranty Card.

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the router for repair.

The FWG114P v2 Front Panel

The front panel of the FWG114P v2 contains the status LEDs. Use the LEDs to verify various operations. Viewed from left to right, Table 2-1 describes the LEDs on the front of the router.

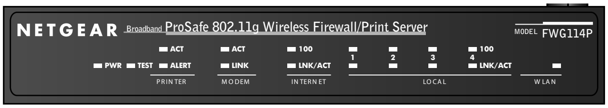


Figure 2-1: FWG114P v2 Front Panel

Table 2-1. LED Descriptions

Label	Activity	Description
POWER	On	Power is supplied to the firewall.
TEST	On Off	The system is initializing. The system is ready and running.
PRINTER		
ACT	On Blinking	The printer is connected and powered on. Data is being transmitted or received by the Printer port.
ALERT	On (Amber)	The printer has a problem, such as out of paper, out of ink, or a paper jam.
MODEM		
ACT	Blinking	Data is being transmitted or received by the Modem port.
LINK	On (Amber)	The port has detected a link with an attached device.
INTERNET	**Note:** The operation of these LEDs depends on how the WAN port is configured.	
100 (100 Mbps)	On Off	The Internet (WAN) port is operating at 100 Mbps. The Internet (WAN) port is operating at 10 Mbps.
LINK/ACT (Link/Activity)	On Blinking	The Internet port has detected a link with an attached device. Data is being transmitted or received by the Internet port.
LOCAL		
100 (100 Mbps)	On Off	The Local port is operating at 100 Mbps. The Local port is operating at 10 Mbps.
LINK/ACT (Link/Activity)	On Blinking	The Local port has detected a link with an attached device. The Local port is transmitting or receiving data.
WLAN	On Blinking	The Wireless (WLAN) port is operating. The Wireless (WLAN) port is transmitting or receiving data.

The FWG114P v2 Rear Panel

The rear panel of the FWG114P v2 Wireless Firewall/Print Server contains the port connections listed below.

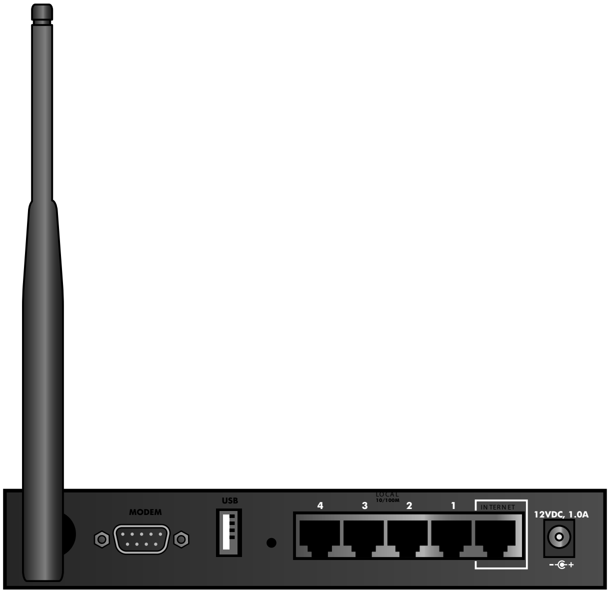


Figure 1-2: FWG114P v2 Rear Panel

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

- Wireless antenna.
- DB-9 serial port for modem connection.
- USB 2.0 Printer Port.
- Factory Default Reset push button.
- Four Ethernet LAN ports.
- Internet Ethernet WAN port for connecting the router to a broadband modem.
- AC power adapter outlet.

Chapter 3
Connecting the FWG114P v2 to the Internet

This chapter describes how to set up the router on your local area network (LAN) and connect to the Internet. You will find out how to configure your ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2 for Internet access using the Setup Wizard, or how to manually configure your Internet connection.

What You Will Need Before You Begin

You need to prepare these three things before you begin:

1. An active Internet service, such as those provided by a cable or DSL broadband account.
2. Locate the Internet Service Provider (ISP) configuration information for your broadband account.
3. Connect the router to a broadband modem and a computer as explained below.

Cabling and Computer Hardware Requirements

To use the FWG114P v2 Wireless Firewall/Print Server on your network, each computer must have an installed Ethernet Network Interface Card (NIC) and an Ethernet cable. If the computer will connect to your network at 100 Mbps, you must use a Category 5 (CAT5) cable, such as the one provided with your router.

Computer Network Configuration Requirements

The FWG114P v2 includes a built-in Web Configuration Manager. To access the configuration menus on the FWG114P v2, you must use a Java-enabled Web browser program that supports HTTP uploads, such as Microsoft Internet Explorer or Netscape Navigator. Use Internet Explorer or Netscape Navigator versions 4.0 or above. Free browser programs are readily available for Windows, Macintosh, or UNIX/Linux.

For the initial connection to the Internet and configuration of your router, you will need to connect a computer to the router that is set to automatically get its TCP/IP configuration from the router via DHCP.

The cable or DSL modem broadband access device must provide a standard 10 Mbps (10BASE-T) Ethernet interface.

Internet Configuration Requirements

Depending on how your ISP set up your Internet account, you might need one or more of these configuration parameters to connect your router to the Internet:

- Host and Domain Names.
- ISP login name and password.
- ISP Domain Name Server (DNS) Addresses.
- Fixed IP address which is also known as static IP address.

Where Do I Get the Internet Configuration Parameters?

There are several ways you can gather the required Internet connection information:

- Your ISP provides all the information needed to connect to the Internet. If you cannot locate this information, you can ask your ISP to provide it or you can try one of the options below.
- If you have a computer already connected using the active Internet access account, you can gather the configuration information from that computer.
  - For Windows 95/98/ME, open the Network control panel, select the TCP/IP entry for the Ethernet adapter, and click Properties. Record all the settings for each tab page.
  - For Windows 2000/XP, open the Local Area Network Connection, select the TCP/IP entry for the Ethernet adapter, and click Properties. Record all the settings for each tab page.
  - For Macintosh computers, open the TCP/IP or Network control panel. Record all the settings for each section.
- You may also refer to the *FWG114P v2 Resource CD* for the NETGEAR Router ISP Guide which provides Internet connection information for many ISPs.

Once you locate your Internet configuration parameters, you may want to record them on the following form:

Record Your Internet Connection Information

Print this page. Fill in the configuration parameters from your Internet Service Provider (ISP).

ISP Login Name: The login name and password are case sensitive and must be entered exactly as given by your ISP. For AOL customers, the login name is their primary screen name. Some ISPs use your full e-mail address as the login name. The Service Name is not required by all ISPs. If you connect using a login name and password, then fill in the following:

Login Name: ______________________________ Password: ____________________________

Service Name: ______________________________

Fixed or Static IP Address: If you have a static IP address, record the following information. For example, 169.254.141.148 could be a valid IP address.

Fixed or Static Internet IP Address: ______.______.______.______
Gateway IP Address: ______.______.______.______
Subnet Mask: ______.______.______.______

ISP DNS Server Addresses: If you were given DNS server addresses, fill in the following:

Primary DNS Server IP Address: ______.______.______.______

Secondary DNS Server IP Address: ______.______.______.______

Host and Domain Names: Some ISPs use a specific host or domain name like **CCA7324-A** or **home**. If you have not been given host or domain names, you can use the following examples as a guide:

- If your main e-mail account with your ISP is **aaa@yyy.com**, then use **aaa** as your host name. Your ISP might call this your account, user, host, computer, or system name.
- If your ISP's mail server is **mail.xxx.yyy.com**, then use **xxx.yyy.com** as the domain name.

ISP Host Name: _________________________ ISP Domain Name: ________________________

Serial Port Internet Access: If you use a dial-up account, record the following:
Account/User Name: _________________________ Password: __________________________
Telephone number: ______________________ Alternative number: ______________________

Connecting the FWG114P v2 Wireless Firewall/Print Server

This section provides instructions for connecting the FWG114P v2 Wireless Firewall/Print Server. Also, the *Resource CD for the ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P (SW-10023-03)*, included with your router, contains an animated Installation Assistant to help you through this procedure.

Verify That Basic Requirements Are Met

Assure that the following requirements are met:

- You have your broadband Internet service settings handy.
- The computer is configured to obtain an IP address automatically via DHCP. For instructions on how to do this, please see the *Reference Manual* on the *Resource CD for the ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P (SW-10023-03)*.

1. CONNECT THE WIRELESS FIREWALL/PRINT SERVER

   a. Turn off your computer and cable or DSL modem.

   b. Disconnect the Ethernet cable (**A**) from your computer which connects to the broadband modem.

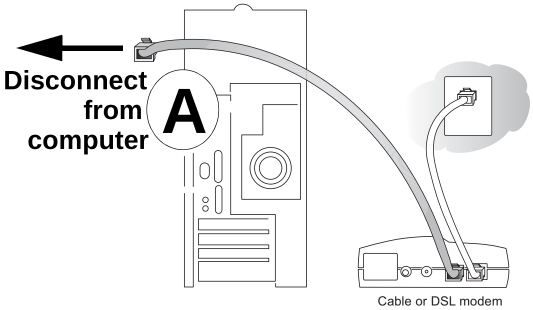


Figure 3-1: Disconnect the broadband modem

c. Securely insert the Ethernet cable from your broadband modem into the Internet port (**B)** on the FWG114P v2.

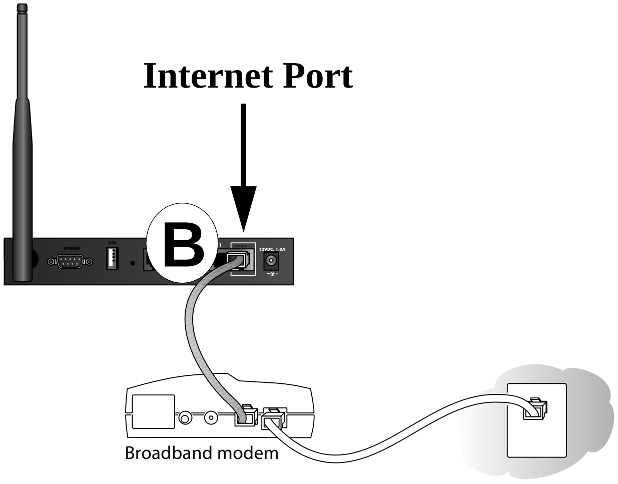


Figure 3-2: Connect the broadband modem to the router

d. Securely insert one end of the Ethernet cable that came with your wireless firewall/print server into a Local port on the router, such as Local port 4 (**C)**, and the other end into the Ethernet port of your computer (**D)**.

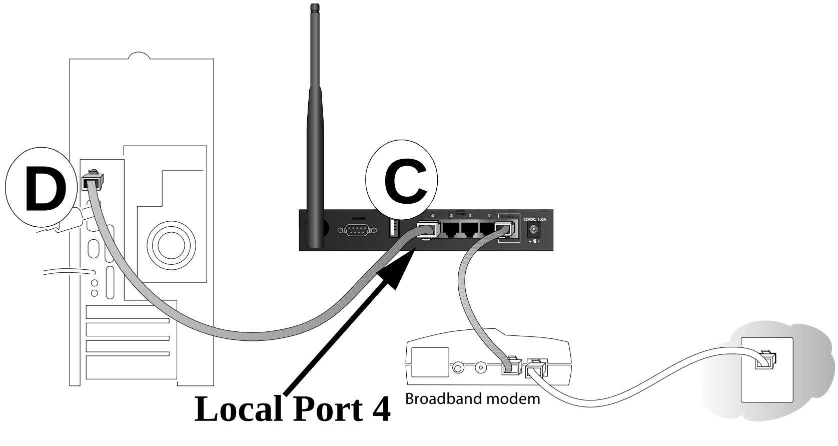


Figure 3-3: Connect the computers on your network to the router

Note: The FWG114P v2 incorporates Auto Uplink™ technology which eliminates the need to worry about crossover cables by automatically adjusting to the cable type.

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. First, turn on the broadband modem and wait 2 minutes.

b. Now, turn on your wireless firewall/print server.

c. Last, turn on your computer.
Note: If software usually logs you in to the Internet, *do not* run that software, or cancel it if it starts automatically.

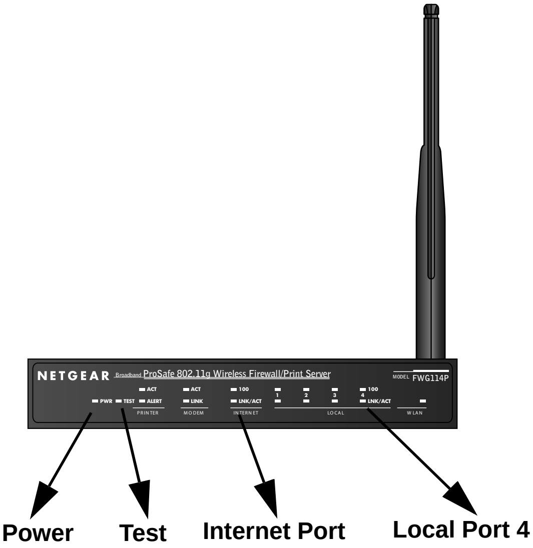


Figure 3-4: Verify the connections to the firewall

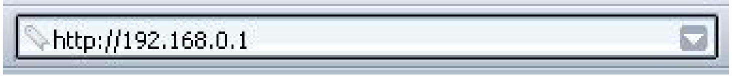
d. Check the status lights and verify the following:

- *Power*: The power light goes on when your turn the wireless firewall/print server on.
- *Test*: The test light turns on, then goes off after less than a minute.
- *Local*: A Local light on the router is lit. If no Local lights are lit, check that the Ethernet cable connecting the powered on computer to the router is securely attached at both ends.
- *Internet*: The Internet light on the wireless firewall/print server is lit. If the Internet light is not lit, make sure the Ethernet cable is securely attached to the wireless firewall/print server Internet port and the powered on modem.

3. LOG IN TO THE WIRELESS FIREWALL/PRINT SERVER

a. From your PC, launch your Internet browser. Because you are not yet connected to the Internet, your browser will display a page not found message.

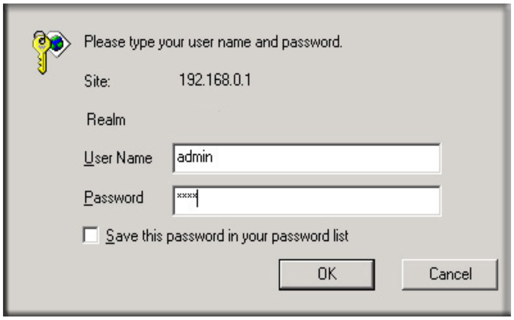
b. Connect to the wireless firewall/print server by typing **http://192.168.0.1** in the address field of Internet Explorer or Netscape® Navigator.



http://192.168.0.1

Figure 3-5: Log in to the firewall

c. Enter **admin** for the router user name and **password** for the router password, both in lower case letters.A login window opens as shown here:



Please type your user name and password.

Site: 192.168.0.1

Realm

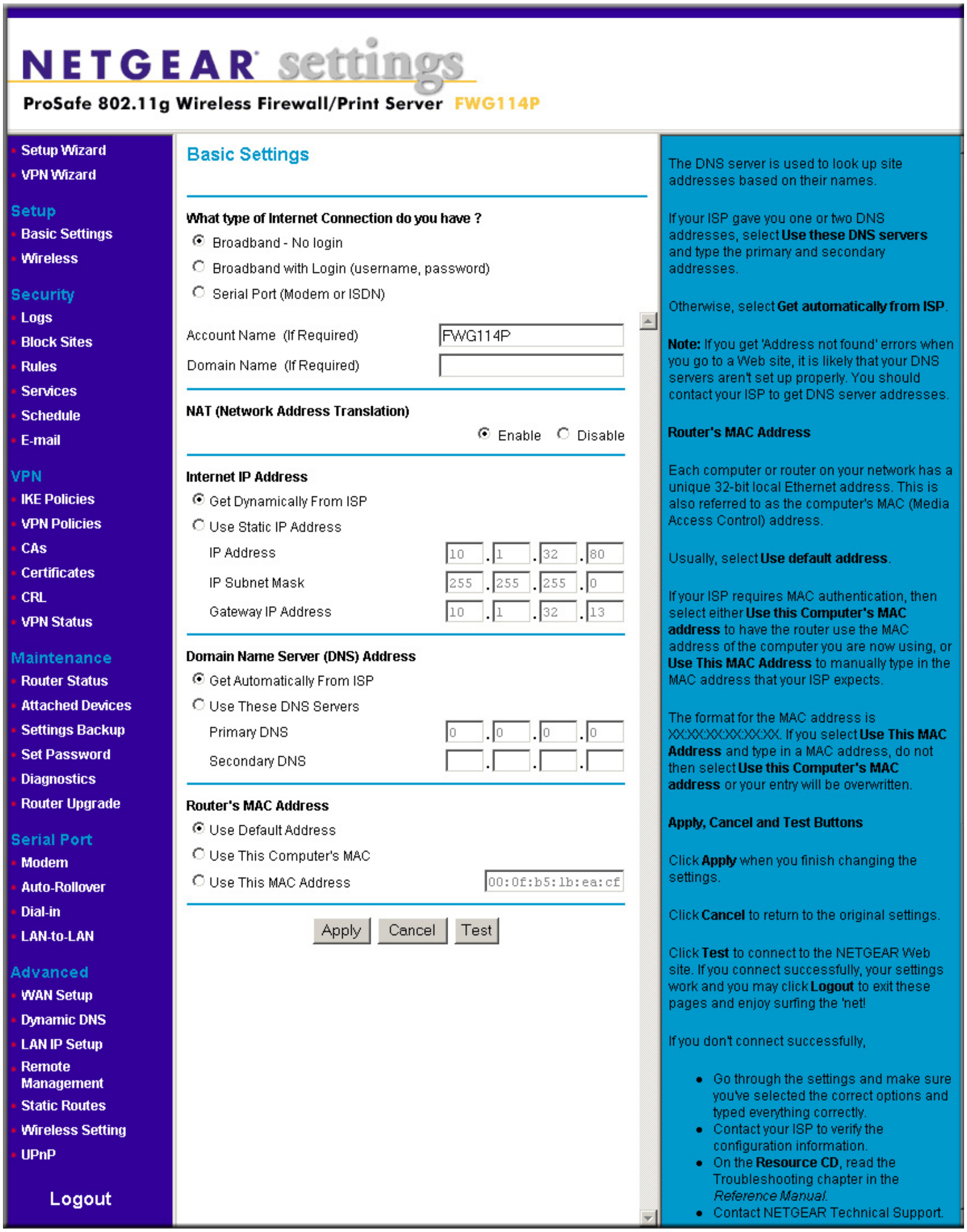
User Name: admin

Password: ****

□ Save this password in your password list

Figure 3-6: Login window

d. After logging in to the router, you will see the login result page.



NETGEAR settings

ProSafe 802.11g Wireless Firewall/Print Server FWG114P

Basic Settings

What type of Internet Connection do you have ?

● Broadband - No login

○ Broadband with Login (username, password)

○ Serial Port (Modem or ISDN)

Account Name (If Required): FWG114P

Domain Name (If Required):

NAT (Network Address Translation)

● Enable ○ Disable

Internet IP Address

● Get Dynamically From ISP

○ Use Static IP Address

IP Address: 10 . 1 . 32 . 80

IP Subnet Mask: 255 . 255 . 255 . 0

Gateway IP Address: 10 . 1 . 32 . 13

Domain Name Server (DNS) Address

● Get Automatically From ISP

○ Use These DNS Servers

Primary DNS: 0 . 0 . 0 . 0

Secondary DNS: . . .

Router's MAC Address

● Use Default Address

○ Use This Computer's MAC

○ Use This MAC Address: 00:0f:b5:1b:ea:cf

The DNS server is used to look up site addresses based on their names.

If your ISP gave you one or two DNS addresses, select **Use these DNS servers** and type the primary and secondary addresses.

Otherwise, select **Get automatically from ISP**.

Note: If you get 'Address not found' errors when you go to a Web site, it is likely that your DNS servers aren't set up properly. You should contact your ISP to get DNS server addresses.

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.

Usually, select **Use default address**.

If your ISP requires MAC authentication, then select either **Use this Computer's MAC address** to have the router 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. If you select **Use This MAC Address** and type in a MAC address, do not then select **Use this Computer's MAC address** or your entry will be overwritten.

Apply, Cancel and Test Buttons

Click **Apply** when you finish changing the settings.

Click **Cancel** to return to the original settings.

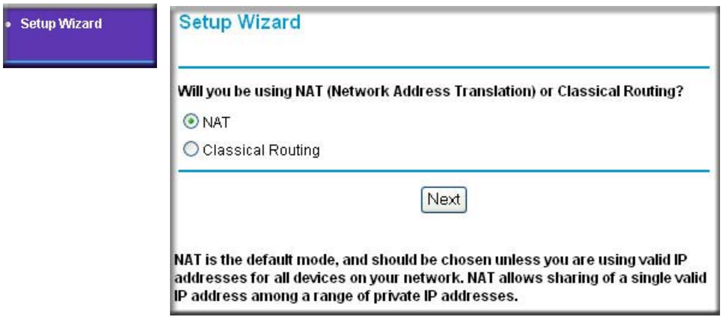
Click **Test** to connect to the NETGEAR Web site. If you connect successfully, your settings work and you may click **Logout** to exit these pages and enjoy surfing the 'net!

If you don't connect successfully,

- Go through the settings and make sure you've selected the correct options and typed everything correctly.
- Contact your ISP to verify the configuration information.
- On the **Resource CD**, read the Troubleshooting chapter in the *Reference Manual*.
- Contact NETGEAR Technical Support.

Figure 3-7: Login Result page

4. RUN THE SETUP WIZARD TO CONNECT TO THE INTERNET



Setup Wizard

Will you be using NAT (Network Address Translation) or Classical Routing?

● NAT

○ Classical Routing

NAT is the default mode, and should be chosen unless you are using valid IP addresses for all devices on your network. NAT allows sharing of a single valid IP address among a range of private IP addresses.

Figure 3-8: Setup Wizard

a. You are now connected to the router. If you do not see the menu above, click the Setup Wizard link on the upper left of the main menu.

b. Choose NAT or Classical Routing. Typically, NAT is used. NAT automatically assigns private IP addresses (192.168.0.x) to LAN connected devices. Classical routing lets you directly manage the IP addresses the FWG114P v2 uses.

   Note: If you choose not to use NAT, each computer on the LAN connected to the FWG114P v2 must have a valid public IP address in the same subnet as the Wan port of the FWG114P v2. For more information on NAT, please see "Single IP Address Operation Using NAT" on page B-7. Furthermore, if you turn NAT off and plan to use VPN, you will have to open UDP port 500 in the Security settings according to the instructions at

c. Click **Next** to proceed. Input your ISP settings, as needed.

d. At the end of the Setup Wizard, click the **Test** button to verify your Internet connection and register your product. If you have trouble connecting to the Internet, use the Troubleshooting Tips below to correct basic problems, or refer to the *Reference Manual* on the CD.

   If you were unable to connect to the firewall, please refer to Basic Functioning "Basic Functioning" on page 11-1.

You are now connected to the Internet!

Note: For wireless placement and range guidelines, and wireless configuration instructions, please see Chapter 4, "Wireless Configuration."

Basic Setup Troubleshooting Tips

Here are some tips for correcting simple problems that prevent with you from connecting to the Internet or connecting to the wireless firewall/print server.

Be sure to restart your network in the correct sequence.

Follow this sequence. Turn off the modem, wireless firewall/print server, and computer. Turn on the modem first and wait two minutes. Next, turn on the wireless firewall/print server, and finally the computer.

Make sure the Ethernet cables are securely plugged in.

- For each powered on computer connected to the wireless firewall/print server with a securely plugged in Ethernet cable, the corresponding wireless firewall/print server Local port status light will be lit. The label on the bottom of the wireless firewall/print server identifies the number of each Local port.
- The Internet port status light on the wireless firewall/print server will be lit if the Ethernet cable from the wireless firewall/print server to the modem is plugged in securely and the modem and wireless firewall/print server are turned on.

Make sure the network settings of the computer are correct.

LAN connected computers *must* be configured to obtain an IP address automatically via DHCP, unless you have turned NAT off and are managing the IP addresses directly. For instructions on these configuration settings, please see the *Reference Manual* on the *Resource CD for the ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P (SW-10023-03)*.

FWG114P v2 Setup Wizard Auto Detection

There are two ways you can configure your firewall to connect to the Internet:

- Let the FWG114P v2 auto-detect the type of Internet connection you have and configure it.
- Manually choose which type of Internet connection you have and configure it.

These options are described below. Unless your ISP uses DHCP, you will need the parameters from your ISP you entered in “Record Your Internet Connection Information” on page 3.

The Setup Wizard will can check for the following connection types:

- Dynamic IP assignment
- A login protocol, such as PPPoE

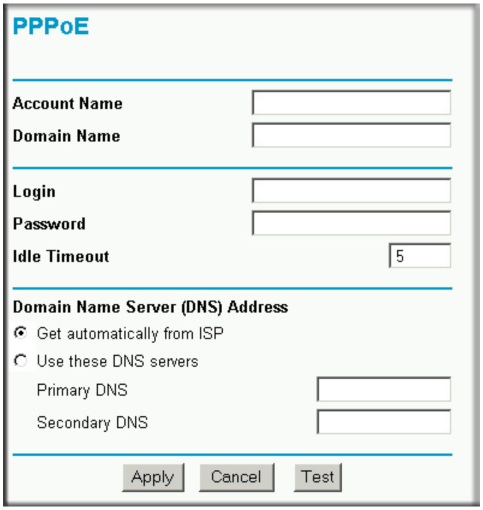
- Fixed IP address assignment

Next, the Setup Wizard will report which connection type it has discovered, and then display the appropriate configuration menu. If the Setup Wizard finds no connection, you will be prompted to check the physical connection between your firewall and the cable or DSL modem. When the connection is properly made, the firewall's Internet LED should be on.

The procedures for filling in the configuration menu for each type of connection follow below.

Wizard-Detected Login Account Setup

If the Setup Wizard determines that your Internet service account uses a login protocol, such as PPP over Ethernet (PPPoE), you will be directed to a menu like the PPPoE menu in Figure 3-9:



PPPoE

Account Name

Domain Name

Login

Password

Idle Timeout 5

Domain Name Server (DNS) Address

● Get automatically from ISP

○ Use these DNS servers

Primary DNS

Secondary DNS

Figure 3-9: Setup Wizard menu for PPPoE login accounts

1. 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. If you leave the Domain Name field blank, the firewall will attempt to learn the domain automatically from the ISP. If this is not successful, you may need to enter it manually.
2. Enter the PPPoE login user name and password provided by your ISP. These fields are case sensitive. If you wish to change the idle timeout, enter a new value in minutes.

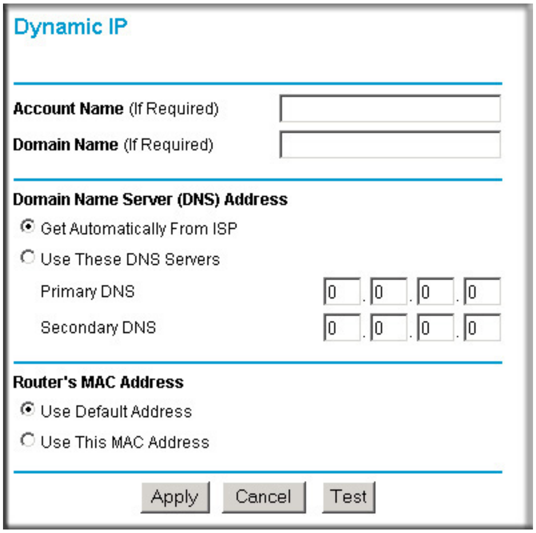
Note: You will no longer need to launch the ISP’s login program on your computer in order to access the Internet. When you start an Internet application, your firewall will automatically log you in.

3. The Idle Timeout setting determines how long to wait after there is no activity before disconnecting from the Internet. This is useful in countries where Internet service charges are based on the amount of time connected to the Internet. Whenever a computer on the network requests access to the Internet the FWG114P v2 will automatically reconnect.
4. 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: If you enter an address here, after you finish configuring the firewall, reboot your PCs so that the settings take effect.
5. Click **Apply** to save your settings.
6. Click **Test** to test your Internet connection. If the NETGEAR Web site does not appear within one minute, refer to Chapter 11, “Troubleshooting”.

Wizard-Detected Dynamic IP Account Setup

If the Setup Wizard determines that your Internet service account uses Dynamic IP assignment, you will be directed to the menu shown in Figure 3-10 below:



Dynamic IP

Account Name (If Required)

Domain Name (If Required)

Domain Name Server (DNS) Address

● Get Automatically From ISP

○ Use These DNS Servers

Primary DNS 0 . 0 . 0 . 0

Secondary DNS 0 . 0 . 0 . 0

Router's MAC Address

● Use Default Address

○ Use This MAC Address

Figure 3-10: Setup Wizard menu for Dynamic IP address

1. 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. If you leave the Domain Name field blank, the firewall will attempt to learn the domain automatically from the ISP. If this is not successful, you may need to enter it manually.
2. 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: DNS servers are required to perform the function of translating an Internet name, such as www.netgear.com to a numeric IP address. For a fixed IP address configuration, you must obtain DNS server addresses from your ISP and enter them manually here. You should reboot your PCs after configuring the firewall for these settings to take effect.
3. The Router’s MAC Address is the Ethernet MAC address that will be used by the firewall on the Internet port.

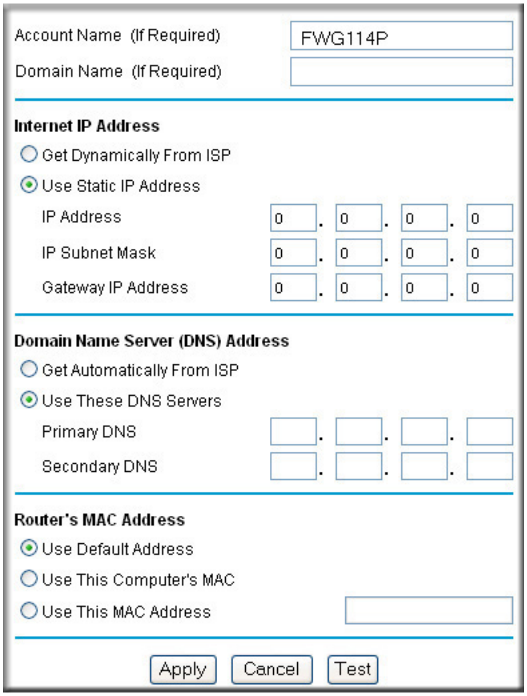
If your ISP allows access from only one specific computer’s Ethernet MAC address, select “Use this MAC address.” The firewall will then capture and use the MAC address of the computer that you are now using. You must be using the one computer that is allowed by the ISP. Otherwise, you can type in a MAC address.

Note: Some ISPs will register the Ethernet MAC address of the network interface card in your computer when your account is first opened. They will then only accept traffic from the MAC address of that computer. This feature allows your firewall to masquerade as that computer by using its MAC address.

4. Click **Apply** to save your settings.
5. Click **Test** to test your Internet connection. If the NETGEAR Web site does not appear within one minute, refer to Chapter 11, “Troubleshooting”.

Wizard-Detected Fixed IP Account Setup

If the Setup Wizard determines that your Internet service account uses Fixed IP assignment, you will be directed to the menu shown in Figure 3-11 below:



Account Name (If Required): FWG114P
Domain Name (If Required):

Internet IP Address
○ Get Dynamically From ISP
● Use Static IP Address
IP Address: 0 . 0 . 0 . 0
IP Subnet Mask: 0 . 0 . 0 . 0
Gateway IP Address: 0 . 0 . 0 . 0

Domain Name Server (DNS) Address
○ Get Automatically From ISP
● Use These DNS Servers
Primary DNS: . . .
Secondary DNS: . . .

Router's MAC Address
● Use Default Address
○ Use This Computer's MAC
○ Use This MAC Address

Figure 3-11: Setup Wizard menu for Fixed IP address

1. Enter your assigned IP Address, Subnet Mask, and the IP Address of your ISP's gateway router. This information should have been provided to you by your ISP. You will need the configuration parameters from your ISP you recorded in "Record Your Internet Connection Information" on page 3.
2. Enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

   Note: DNS servers are required to perform the function of translating an Internet name, such as www.netgear.com to a numeric IP address. For a fixed IP address configuration, you must obtain DNS server addresses from your ISP and enter them manually here. You should reboot your PCs after configuring the firewall for these settings to take effect.
3. Click **Apply** to save the settings.
4. Click **Test** to test your Internet connection. If the NETGEAR Web site does not appear within one minute, refer to Chapter 11, "Troubleshooting.

How to Configure the Serial Port as the Primary Internet Connection

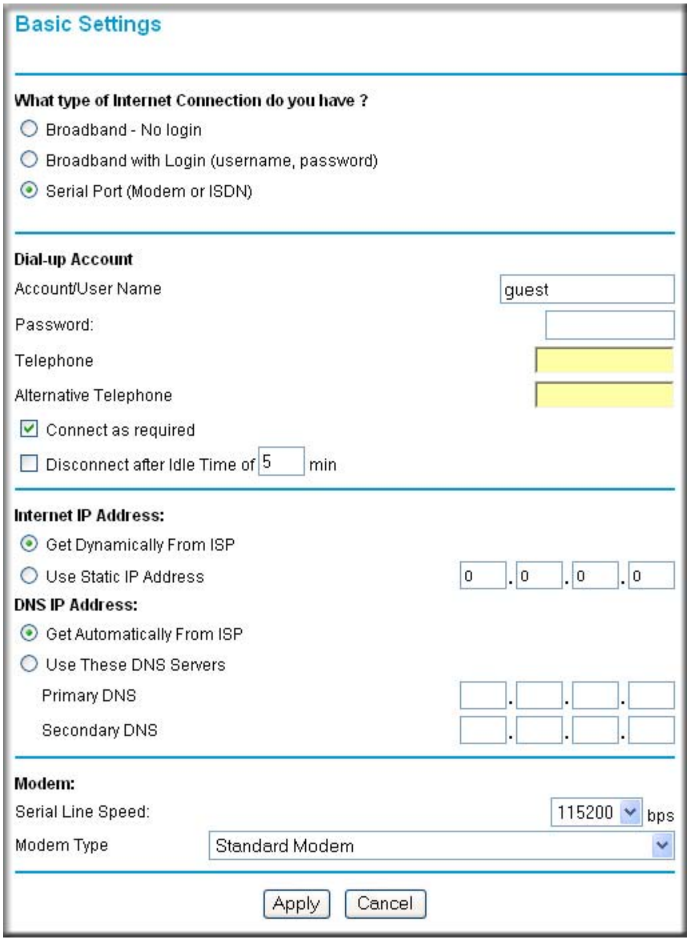
Use the procedure below to configure an Internet connection via the serial port of your firewall.

There are three steps to configuring the serial port of your firewall for an Internet connection:

1. Connect the firewall to your ISDN or dial-up analog modem.
2. Configure the firewall.
3. Connect to the Internet.

Follow the steps below to configure a serial port Internet connection on your firewall.

1. **Connect the Firewall to your ISDN or dial-up modem**
   a. Turn off your modem and connect the cable from the serial port of the FWG114P v2 to the modem.
   b. Turn on the modem and wait about 30 seconds for the lights to stop blinking.
2. **Configure the Serial Port of the Firewall**.
   a. Use a browser to log in to the firewall at http://192.168.0.1 with its default User Name of **admin** and default Password of **password**, or using whatever Password you have set up.
   b. From the Setup Basic Settings menu, click Serial Port.



Basic Settings

What type of Internet Connection do you have ?

○ Broadband - No login

○ Broadband with Login (username, password)

● Serial Port (Modem or ISDN)

Dial-up Account

Account/User Name: guest

Password:

Telephone

Alternative Telephone

☑ Connect as required

□ Disconnect after Idle Time of 5 min

Internet IP Address:

● Get Dynamically From ISP

○ Use Static IP Address 0 . 0 . 0 . 0

DNS IP Address:

● Get Automatically From ISP

○ Use These DNS Servers

Primary DNS . . .

Secondary DNS . . .

Modem:

Serial Line Speed: 115200 bps

Modem Type: Standard Modem

Figure 3-12: Serial Internet Connection configuration menu

c. Fill in the ISDN or analog ISP Internet configuration parameters as appropriate:

- For a Dial-up Account, enter the Account information. Check “Connect as required” to enable the firewall to automatically dial the number. To enable Idle Time disconnect, check the box and enter a time in minutes.
- To configure the Internet IP settings, fill in the address parameters your ISP provided.

d. Configure the Modem parameters.

Note: You can validate modem string settings by first connecting the modem directly to a computer, establishing a connection to your ISP, and then copying the modem string settings from the computer configuration and pasting them into the FWG114P v2 Modem Properties Initial String field. For more information on this procedure, please refer to the support area of the NETGEAR Web site.

- Select the Serial Line Speed. This is the maximum speed the modem will attempt to use. For ISDN permanent connections, the speeds are typically 64000 or 128000 bps. For dial-up modems, 56000 bps would be a typical setting.
- Select the Modem Type:
  - For ISDN, select "Permanent connection (leased line)."
  - For dial-up, select your modem from the list. "Standard Modem" should work in most cases.
  - If your modem is not on the list, select "User Defined" and enter the Modem Properties.

Note: If you are using the "User Defined" Modem Type, you must first use the Serial Port menu Modem link to fill in the Modem Properties settings for your modem.

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

3. **Connect to the Internet to test your configuration.**

a. If you have a broadband connection, disconnect it.

b. From a workstation, open a browser and test your serial port Internet connection.

Note: The response time of your serial port Internet connection will be slower than a broadband Internet connection.

Testing Your Internet Connection

After completing the Internet connection configuration, your can test your Internet connection. Log in to the firewall, then, from the Setup Basic Settings link, click the Test button. If the NETGEAR Web site does not appear within one minute, refer to Chapter 11, "Troubleshooting."

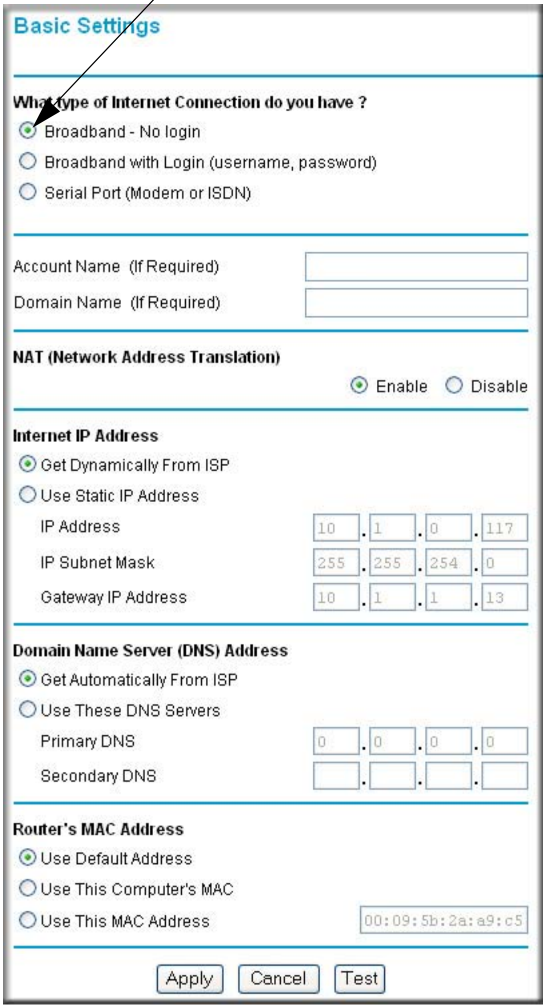
Note: Popup blocking software may block the test page from opening. Alternately, you can just open a new browser window and browse the Internet.

To access the Internet from any computer connected to your firewall, launch a browser, such as Microsoft Internet Explorer or Netscape Navigator. You should see the firewall's Internet LED blink, indicating communication to the ISP. The browser should begin to display a Web page.

Manually Configuring 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



Basic Settings

What type of Internet Connection do you have ?

● Broadband - No login
○ Broadband with Login (username, password)
○ Serial Port (Modem or ISDN)

Account Name (If Required)
Domain Name (If Required)

NAT (Network Address Translation)
● Enable ○ Disable

Internet IP Address
● Get Dynamically From ISP
○ Use Static IP Address

IP Address 10 . 1 . 0 . 117
IP Subnet Mask 255 . 255 . 254 . 0
Gateway IP Address 10 . 1 . 1 . 13

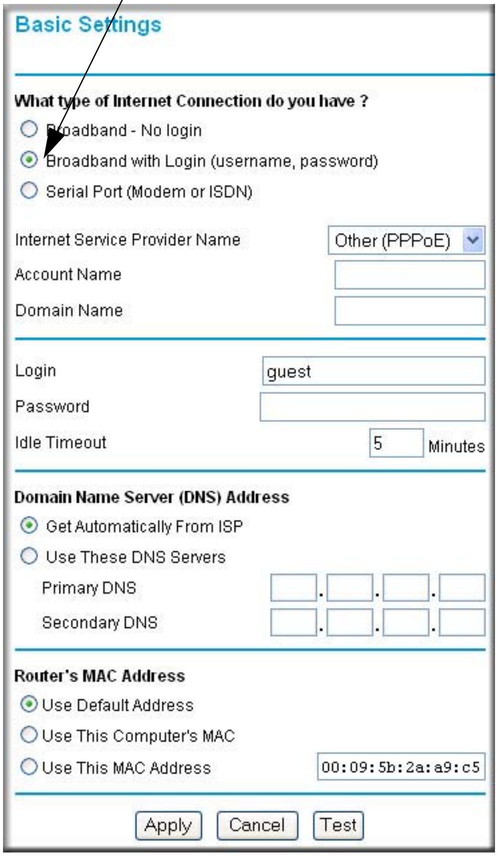
Domain Name Server (DNS) Address
● Get Automatically From ISP
○ Use These DNS Servers

Primary DNS 0 . 0 . 0 . 0
Secondary DNS

Router's MAC Address
● Use Default Address
○ Use This Computer's MAC
○ Use This MAC Address 00:09:5b:2a:a9:c5

Apply Cancel Test

ISP *Does* Require Login



Basic Settings

What type of Internet Connection do you have ?

○ Broadband - No login
● Broadband with Login (username, password)
○ Serial Port (Modem or ISDN)

Internet Service Provider Name Other (PPPoE)
Account Name
Domain Name

Login guest
Password
Idle Timeout 5 Minutes

Domain Name Server (DNS) Address
● Get Automatically From ISP
○ Use These DNS Servers

Primary DNS
Secondary DNS

Router's MAC Address
● Use Default Address
○ Use This Computer's MAC
○ Use This MAC Address 00:09:5b:2a:a9:c5

Apply Cancel Test

Figure 3-13: Browser-based configuration Basic Settings menu

How to Manually Configure the Primary Internet Connection

Use these steps to manually configure the primary Internet connection in the Basic Settings menu.

1. Select your Internet connection type (broadband with or without login, or serial).

   Note: If you are a Telstra BigPond broadband customer, or if you are in an area, such as Austria that uses broadband PPTP, login is required. If so, select BigPond or PPTP from the Internet Service Type drop down box.

2. 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.

3. If needed, enter the PPPoE login user name and password provided by your ISP. These fields are case sensitive. To change the login timeout, enter a new value in minutes.

   Note: You will no longer need to run the ISP's login program on your computer in order to access the Internet. When you start an Internet application, your firewall automatically logs you in.

4. You should only disable NAT if you are sure you do not require it. NAT automatically assigns private IP addresses (for example, 192.168.0.x) to LAN connected devices. When NAT is disabled, only standard routing is performed by this router.

   Note: Disabling NAT will reboot the router and reset all the FWG114P v2 configuration settings to the factory default. Disable NAT only if you plan to install the FWG114P v2 in a setting where you will be manually administering the IP address space on the LAN side of the router.

5. Internet IP Address: If your ISP assigned you a permanent, fixed IP address for your computer, select "Use Static IP Address." Enter the IP address your ISP assigned. Also enter the IP Subnet Mask and the Gateway IP address. The Gateway is the ISP's router to which your firewall will connect.

6. Domain Name Server (DNS) Address: If 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.

   Note: A DNS server is a host on the Internet that translates Internet names (such as www.netgear.com) to numeric IP addresses. Typically your ISP transfers the IP address of one or two DNS servers to your firewall during login. If the ISP does not transfer an address, you must obtain it from the ISP and enter it manually here. If you enter an address here, you should reboot your PCs after configuring the firewall.

7. Router'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 computer when your account is first opened. They will then only accept traffic from the MAC address of that computer. This feature allows your firewall to masquerade as that computer 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 computer that you are now using. You must be using the one computer that is allowed by the ISP. Or, select "Use This MAC Address" and enter it.
8. Click **Apply** to save your settings.
9. Click **Test** to test your Internet connection. If the NETGEAR Web site does not appear within one minute, refer to Chapter 11, "Troubleshooting."

The remaining chapters in this manual describe how to configure the Advanced features of your firewall, and how to troubleshoot problems that may occur.

Chapter 4
Wireless Configuration

This chapter describes how to configure the wireless features of your FWG114P v2 Wireless Firewall/Print Server.

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 FWG114P v2 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 firewall/print server. 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 FWG114P v2 Wireless Firewall/Print Server. The latency, data throughput performance, and notebook power consumption also vary depending on your configuration choices. For best results, place your wireless firewall/print server:

- 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.

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 FWG114P v2 Wireless Firewall/Print Server provides highly effective security features which are covered in detail in this chapter.

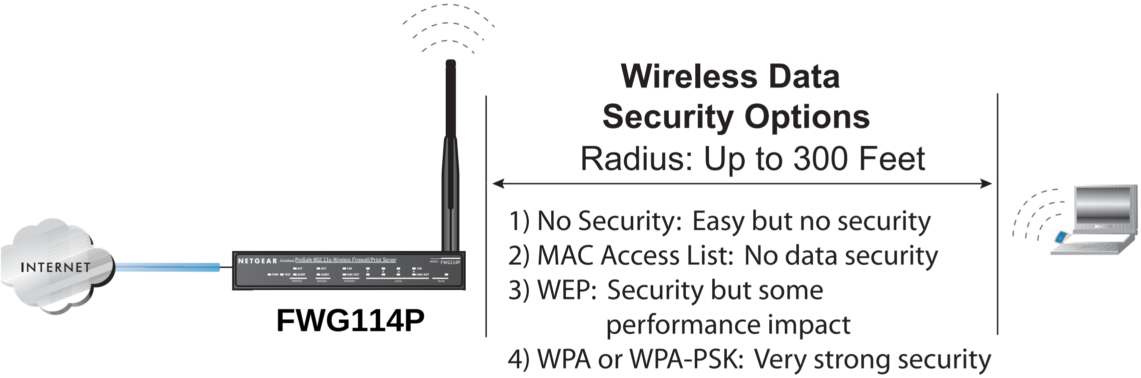

INTERNET
FWG114P
Wireless Data Security Options
Radius: Up to 300 Feet
1) No Security: Easy but no security
2) MAC Access List: No data security
3) WEP: Security but some performance impact
4) WPA or WPA-PSK: Very strong security

Figure 4-1: FWG114P v2 wireless data security options

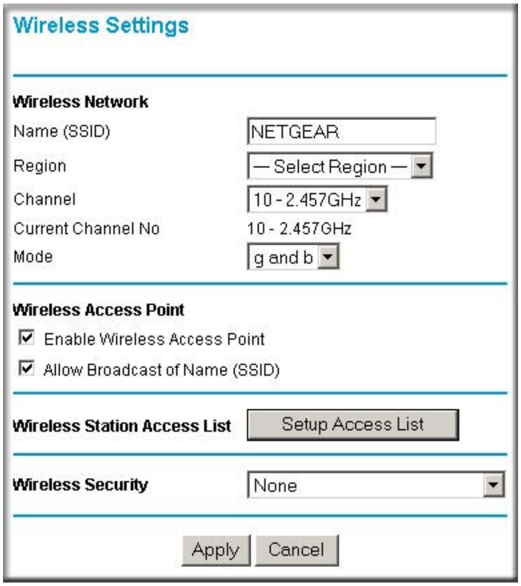
There are several ways you can enhance the security of your wireless network:

- **Restrict Access Based on MAC Address.** You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the FWG114P v2. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn Off the Broadcast of the Wireless Network Name SSID.** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies wireless network ‘discovery’ feature of some products, such as Windows XP, but the data is still exposed.
- **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption will block all but the most determined eavesdropper.

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

Understanding Wireless Settings

To configure the wireless settings of your FWG114P v2, click the Wireless link in the Setup section of the main menu. The wireless settings menu will appear, as shown below.



Wireless Settings

Wireless Network

Name (SSID): NETGEAR

Region: — Select Region —

Channel: 10 - 2.457GHz

Current Channel No: 10 - 2.457GHz

Mode: g and b

Wireless Access Point

☑ Enable Wireless Access Point

☑ Allow Broadcast of Name (SSID)

Wireless Station Access List

Wireless Security: None

Figure 4-2: Wireless Settings menu

Note: The 802.11b and 802.11g wireless networking protocols are configured in exactly the same fashion. The FWG114P v2 will automatically adjust to the 802.11g or 802.11b protocol as the device requires without compromising the speed of the other devices.

- **Wireless Network.** The station name of the FWG114P v2.
  - — **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 FWG114P v2 default SSID is: **NETGEAR**.
  - — **Region.** This field identifies the region where the FWG114P v2 can be used. It may not be legal to operate the wireless features of the wireless firewall/print server 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 FWG114P v2.
  - — **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 FWG114P v2 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**.**

- **Security Options**
  - **Disable**: No data encryption is used.
  - **WEP (Wired Equivalent Privacy)**: Use WEP 64 or 128 bit data encryption.
  - **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.

Default Factory Settings

The FWG114P v2 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 FWG114P v2 Wireless Firewall/Print Server, use the procedures below to customize any of the settings to better meet your networking needs.

FEATURE	DEFAULT FACTORY SETTINGS
SSID	**NETGEAR**
RF Channel	**11 until the region is selected**
Access Point	**Enabled**
SSID broadcast	**Enabled**
Wireless Card Access List for Access Point Connections	**All wireless stations allowed**
WEP Security	**Disabled**
Authentication Type	**Open System**

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 FWG114P v2 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 firewall/print server 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 FWG114P v2.
- **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: ________________________________

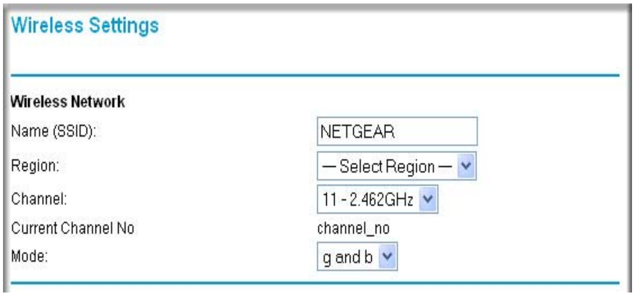
  Shared Key: ________________________________

Use the procedures described in the following sections to configure the FWG114P v2. Store this information in a safe place.

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.



Wireless Settings

Wireless Network

Name (SSID):	NETGEAR
Region:	— Select Region —
Channel:	11 - 2.462GHz
Current Channel No	channel_no
Mode:	g and b

Figure 4-3: Wireless Settings menu

2. Set the Regulatory Domain correctly.

3. 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 ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2. If they do not match, you will not get a wireless connection to the FWG114P v2.

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 firewall/print server. For more information on the wireless channel frequencies please refer to "Wireless Channels" on page E-7.

5. Depending on the types of wireless adapters you have in your computers, choose from the Mode drop-down list.

6. For initial configuration and test, leave the Wireless Card Access List set to "All Wireless Stations" and the Encryption Strength set to "Disable."

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

Note: If you are configuring the FWG114P v2 from a wireless computer and you change the wireless firewall/print server'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 FWG114P v2'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 FWG114P v2. Check that they have a wireless link and are able to obtain an IP address by DHCP from the wireless firewall/print server.

Once your PCs have basic wireless connectivity to the wireless firewall/print server, 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. 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**.
2. Click **Wireless** in the main menu of the FWG114P v2. From the Wireless Settings menu, click **Setup Access List**.

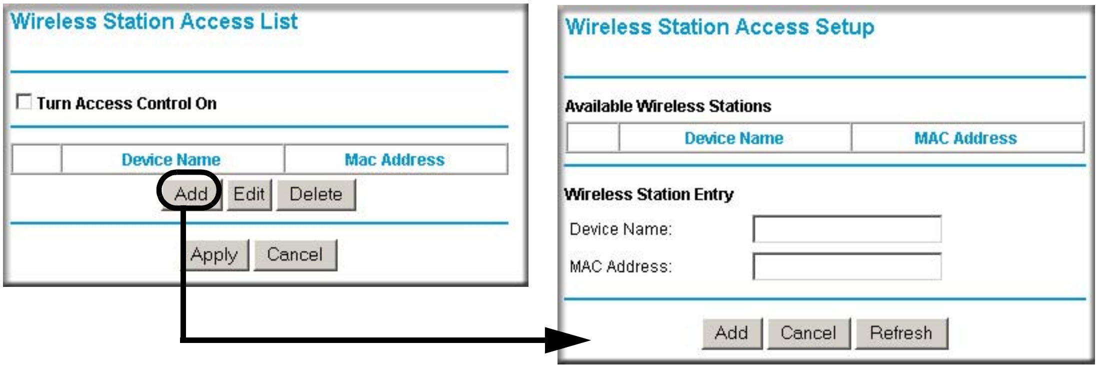


Figure 4-4: Wireless Station Access menu

3. Click the **Turn Access Control On** checkbox to enable MAC filtering.

4. Click **Add** to open the Wireless Card Access Setup menu. You can select a device from the list of available wireless cards the FWG114P v2 has discovered in your area, or you can manually enter the MAC address and Device Name (usually the NetBIOS name).
5. Click **Add** to add this device to your MAC access control list.

➡	**Note:** When configuring the FWG114P v2 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 firewall/print server from a wired computer or from a wireless computer which is on the access control list to make any further changes.

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 FWG114P v2.

To remove a MAC address from the table, click to select it, then click the Delete button.

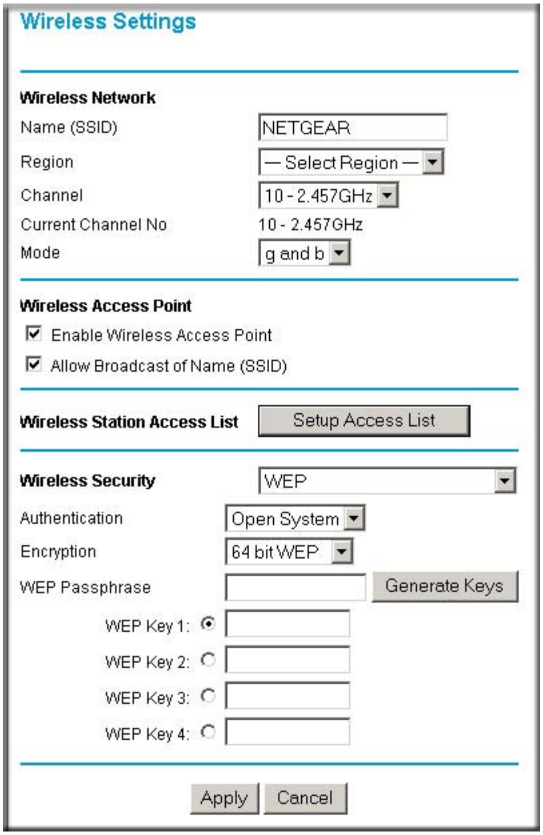
How to Configure WEP

➡	**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 firewall/print server 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.

2. Click **Wireless Settings** in the main menu of the FWG114P v2.



Wireless Settings

Wireless Network

Name (SSID): NETGEAR

Region: — Select Region —

Channel: 10 - 2.457GHz

Current Channel No: 10 - 2.457GHz

Mode: g and b

Wireless Access Point

☑ Enable Wireless Access Point

☑ Allow Broadcast of Name (SSID)

Wireless Station Access List

Wireless Security: WEP

Authentication: Open System

Encryption: 64 bit WEP

WEP Passphrase:

WEP Key 1: ●

WEP Key 2: ○

WEP Key 3: ○

WEP Key 4: ○

Figure 4-5: Wireless Settings menu (WEP)

3. Select **WEP** on the pulldown menu. The WEP options menu will open.

4. 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

- **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.

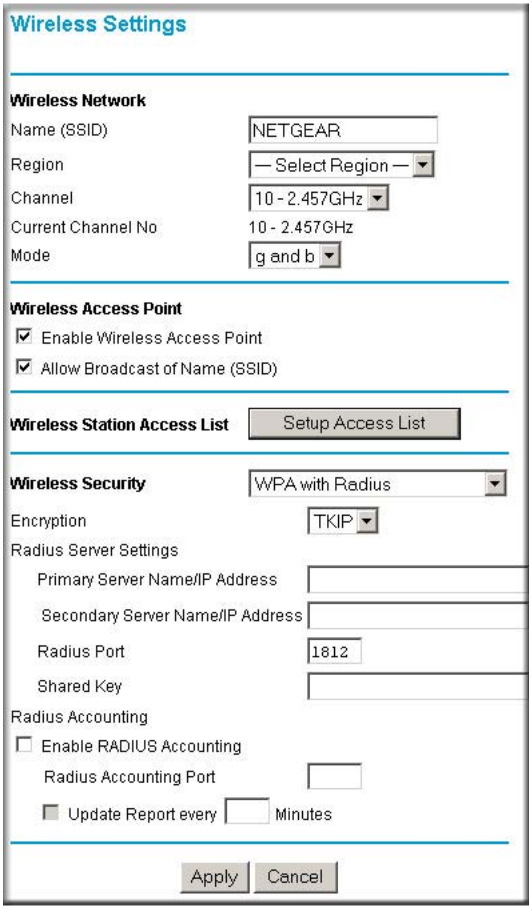
How to Configure WPA with Radius

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.

2. Click **Wireless Settings** in the main menu of the FWG114P v2.



Wireless Settings

Wireless Network

Name (SSID): NETGEAR

Region: — Select Region —

Channel: 10 - 2.457GHz

Current Channel No: 10 - 2.457GHz

Mode: g and b

Wireless Access Point

☑ Enable Wireless Access Point

☑ Allow Broadcast of Name (SSID)

Wireless Station Access List: Setup Access List

Wireless Security: WPA with Radius

Encryption: TKIP

Radius Server Settings

Primary Server Name/IP Address:

Secondary Server Name/IP Address:

Radius Port: 1812

Shared Key:

Radius Accounting

☐ Enable RADIUS Accounting

Radius Accounting Port:

☐ Update Report every ___ Minutes

Apply | Cancel

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.
   - **Secondary Radius Server Name/IP Address**: This field is optional. If you have a Secondary Radius Server on your LAN, enter its name or IP address here.

- **Radius Port**: Enter the port number used for connecting to the Radius Server.
- **Shared Key**: Enter the desired value for the Shared Key. This must match the value used on the Radius server.
- **Radius Accounting**: Enable Radius Accounting

  Enable this if you want to use the Radius Accounting system. If enabled, the following fields must be correct:
- **Radius Accounting Port**: Enter the port number used for Accounting data on the Radius Server.
- **Update Report**: Enable this if you wish to have this AP send Accounting update messages to the Radius accounting server periodically.

  If enabled, enter the desired Update Report interval in the field provided.

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

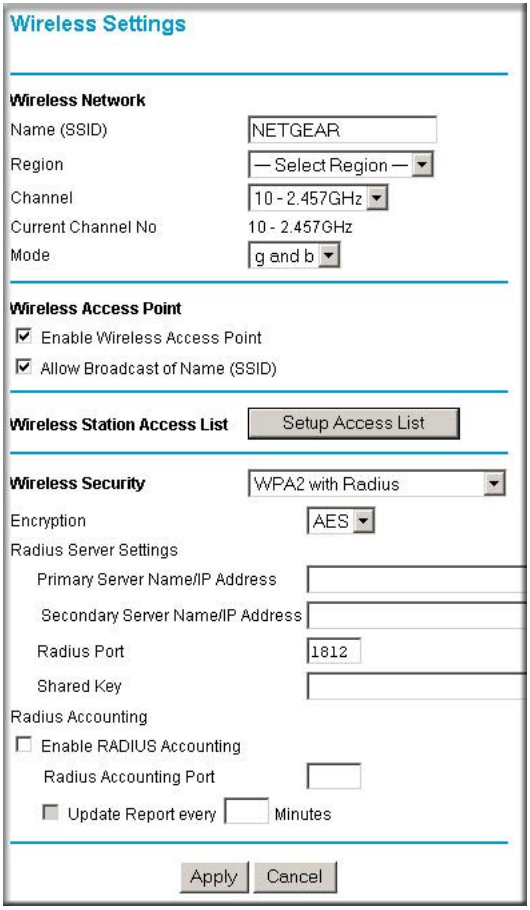
How to Configure WPA2 with Radius

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

To configure WPA2 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.

2. Click **Wireless Settings** in the main menu of the FWG114P v2.



Wireless Settings

Wireless Network

Name (SSID): NETGEAR

Region: — Select Region —

Channel: 10 - 2.457GHz

Current Channel No: 10 - 2.457GHz

Mode: g and b

Wireless Access Point

☑ Enable Wireless Access Point

☑ Allow Broadcast of Name (SSID)

Wireless Station Access List: Setup Access List

Wireless Security: WPA2 with Radius

Encryption: AES

Radius Server Settings

Primary Server Name/IP Address:

Secondary Server Name/IP Address:

Radius Port: 1812

Shared Key:

Radius Accounting

☐ Enable RADIUS Accounting

Radius Accounting Port:

☐ Update Report every ___ Minutes

Apply Cancel

Figure 4-7: Wireless Settings menu (WPA2 with Radius)

3. Select **WPA2 with Radius** on the pulldown menu. The WPA2 with Radius menu will open.

   Encryption: There is no choice for encryption; this is displayed for your information. For WPA2 with Radius, AES 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.

- **Secondary Radius Server Name/IP Address**: This field is optional. If you have a Secondary Radius Server on your LAN, enter its name or IP address here.
- **Radius Port**: Enter the port number used for connecting to the Radius Server.
- **Shared Key**: Enter the desired value for the Shared Key. This must match the value used on the Radius server.
- **Radius Accounting**: Enable Radius Accounting

  Enable this if you want to use the Radius Accounting system. If enabled, the following fields must be correct:

- **Radius Accounting Port**: Enter the port number used for Accounting data on the Radius Server.
- **Update Report**: Enable this if you wish to have this AP send Accounting update messages to the Radius accounting server periodically.

  If enabled, enter the desired Update Report interval in the field provided.

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

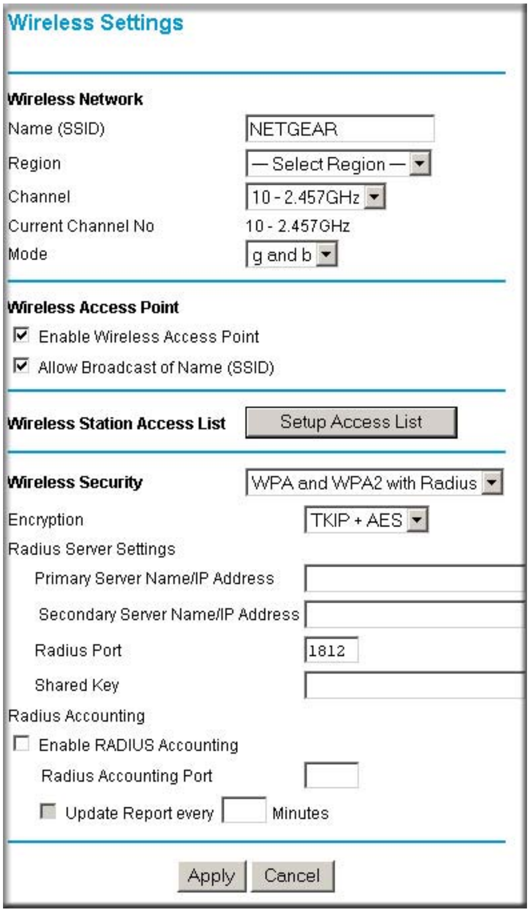
How to Configure WPA and WPA2 with Radius

Note: Not all wireless adapters support WPA and WPA2. 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 and WPA2. Nevertheless, the wireless adapter hardware and driver must also support WPA and WPA2. Consult the product document for your wireless adapter and WPA and WPA2 client software for instructions on configuring WPA and WPA2 settings.

To configure WPA and WPA2 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.

2. Click **Wireless Settings** in the main menu of the FWG114P v2.



Wireless Settings

Wireless Network

Name (SSID): NETGEAR

Region: — Select Region —

Channel: 10 - 2.457GHz

Current Channel No: 10 - 2.457GHz

Mode: g and b

Wireless Access Point

☑ Enable Wireless Access Point

☑ Allow Broadcast of Name (SSID)

Wireless Station Access List: Setup Access List

Wireless Security: WPA and WPA2 with Radius

Encryption: TKIP + AES

Radius Server Settings

Primary Server Name/IP Address:

Secondary Server Name/IP Address:

Radius Port: 1812

Shared Key:

Radius Accounting

□ Enable RADIUS Accounting

Radius Accounting Port:

□ Update Report every ____ Minutes

Apply | Cancel

Figure 4-8: Wireless Settings menu (WPA and WPA2 with Radius)

3. Select **WPA and WPA2 with Radius** on the pulldown menu. The WPA and WPA2 with Radius menu will open.

   Encryption: There is no choice for encryption; this is displayed for your information. For WPA and WPA2 with Radius, WPA clients must use TKIP, and WPA2 clients must use AES.

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.

- **Secondary Radius Server Name/IP Address**: This field is optional. If you have a Secondary Radius Server on your LAN, enter its name or IP address here.
- **Radius Port**: Enter the port number used for connecting to the Radius Server.
- **Shared Key**: Enter the desired value for the Shared Key. This must match the value used on the Radius server.
- **Radius Accounting**: Enable Radius Accounting

  Enable this if you want to use the Radius Accounting system. If enabled, the following fields must be correct:

- **Radius Accounting Port**: Enter the port number used for Accounting data on the Radius Server.
- **Update Report**: Enable this if you wish to have this AP send Accounting update messages to the Radius accounting server periodically.

  If enabled, enter the desired Update Report interval in the field provided.

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

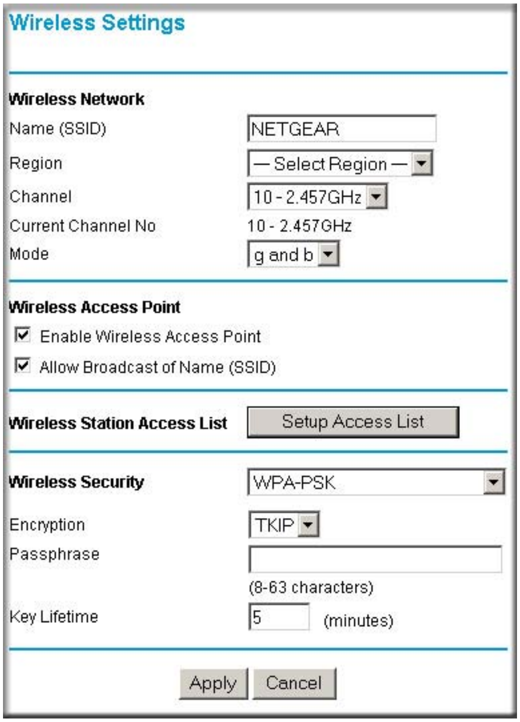
How to Configure WPA-PSK

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-PSK, 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.

2. Click **Wireless Settings** in the main menu of the FWG114P v2.



Wireless Settings

Wireless Network

Name (SSID): NETGEAR

Region: — Select Region —

Channel: 10 - 2.457GHz

Current Channel No: 10 - 2.457GHz

Mode: g and b

Wireless Access Point

☑ Enable Wireless Access Point

☑ Allow Broadcast of Name (SSID)

Wireless Station Access List: Setup Access List

Wireless Security: WPA-PSK

Encryption: TKIP

Passphrase: (8-63 characters)

Key Lifetime: 5 (minutes)

Figure 4-9: Wireless Settings menu (WPA-PSK)

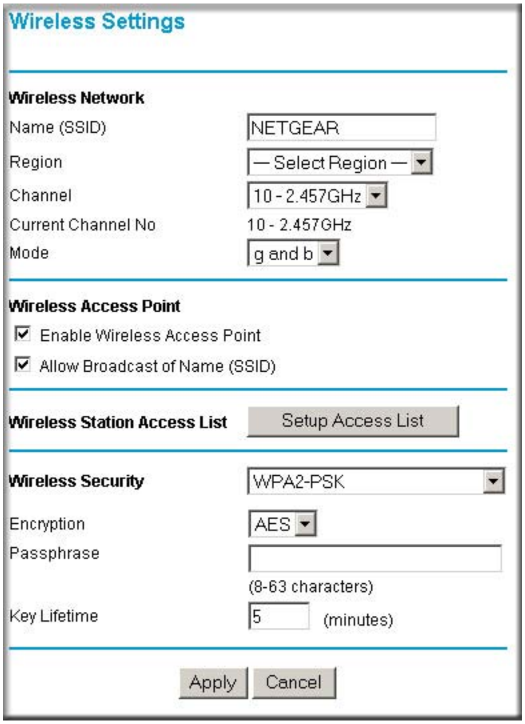
3. Select **WPA-PSK** on the pulldown menu. The WPA-PSK menu will open.
4. Select the desired Encryption method. For WPA-PSK, you can choose TKIP or AES.
5. Enter the pre-shared key in the Passphrase field. Enter a word or group of printable characters in the Passphrase box. The Passphrase must be 8 to 63 characters in length. The 256 Bit key used for encryption is generated from this passphrase.
6. Enter the Key Lifetime. This setting determines how often the encryption key is changed. Shorter periods provide greater security, but adversely affect performance. If desired, you can change the default value.
7. Click **Apply** to save your settings.

How to Configure WPA2-PSK

Note: Not all wireless adapters support WPA2. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA2. Nevertheless, the wireless adapter hardware and driver must also support WPA2. Consult the product document for your wireless adapter and WP2 client software for instructions on configuring WPA2 settings.

To configure WPA2-PSK, 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.
2. Click **Wireless Settings** in the main menu of the FWG114P v2.



Wireless Settings

Wireless Network

Name (SSID)	NETGEAR
Region	— Select Region —
Channel	10 - 2.457GHz
Current Channel No	10 - 2.457GHz
Mode	g and b

Wireless Access Point

☑ Enable Wireless Access Point

☑ Allow Broadcast of Name (SSID)

Wireless Station Access List

Wireless Security	WPA2-PSK
Encryption	AES
Passphrase	(8-63 characters)
Key Lifetime	5 (minutes)

Figure 4-10: Wireless Settings menu (WPA2-PSK)

3. Select **WPA2-PSK** on the pulldown menu. The WPA2-PSK menu will open.

4. Select the desired Encryption method. For WPA2-PSK, the only option is AES.
5. Enter the pre-shared key in the Passphrase field. Enter a word or group of printable characters in the Passphrase box. The Passphrase must be 8 to 63 characters in length. The 256 Bit key used for encryption is generated from this passphrase.
6. Enter the Key Lifetime. This setting determines how often the encryption key is changed. Shorter periods provide greater security, but adversely affect performance. If desired, you can change the default value.
7. Click **Apply** to save your settings.

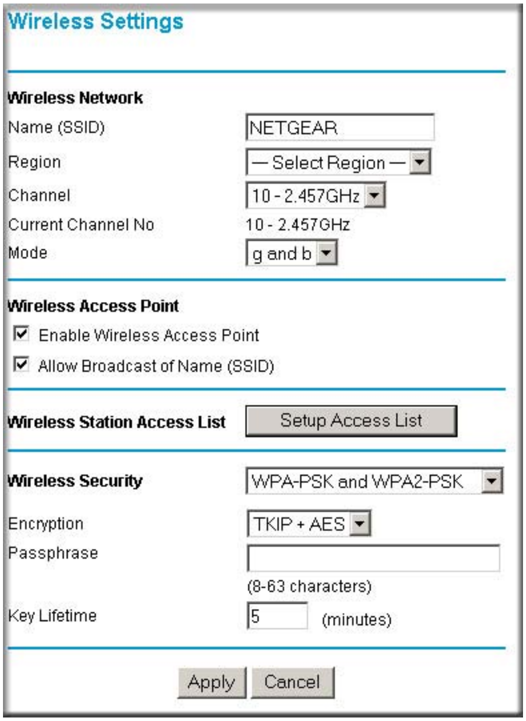
How to Configure WPA-PSK and WPA2-PSK

Note: Not all wireless adapters support WPA and WPA2. 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 and WPA2. Nevertheless, the wireless adapter hardware and driver must also support WPA and WPA2. Consult the product document for your wireless adapter and WPA and WPA2 client software for instructions on configuring WPA and WPA2 settings.

To configure WPA-PSK and WPA2-PSK, 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.

2. Click **Wireless Settings** in the main menu of the FWG114P v2.



Wireless Settings

Wireless Network

Name (SSID): NETGEAR

Region: — Select Region —

Channel: 10 - 2.457GHz

Current Channel No: 10 - 2.457GHz

Mode: g and b

Wireless Access Point

☑ Enable Wireless Access Point

☑ Allow Broadcast of Name (SSID)

Wireless Station Access List: Setup Access List

Wireless Security: WPA-PSK and WPA2-PSK

Encryption: TKIP + AES

Passphrase: (8-63 characters)

Key Lifetime: 5 (minutes)

Apply Cancel

Figure 4-11: Wireless Settings menu (WPA-PSK and WPA2-PSK)

3. Select **WPA-PSK and WPA2-PSK** on the pulldown menu. The WPA-PSK and WPA2-PSK menu will open.
4. Select the desired Encryption method. For WPA-PSK and WPA2-PSK, the only option is TKIP + AES. WPA clients must use TKIP, and WPA2 clients must use AES.
5. Enter the pre-shared key in the Passphrase field. Enter a word or group of printable characters in the Passphrase box. The Passphrase must be 8 to 63 characters in length. The 256 Bit key used for encryption is generated from this passphrase.
6. Enter the Key Lifetime. This setting determines how often the encryption key is changed. Shorter periods provide greater security, but adversely affect performance. If desired, you can change the default value.
7. Click **Apply** to save your settings.

Chapter 5
Serial Port Configuration

This chapter describes how to configure the serial port options of your ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2. The FWG114P v2 serial port lets you share the broadband connection of another FWG114P v2, share resources between two LANs, and take advantage of the routing functions on the broadband (WAN), LAN, and serial network interfaces.

Note: If you configure the serial port of the FWG114P v2 as the primary Internet connection, you will not be able to configure the other serial port options. For instructions on configuring the serial port as the primary Internet connection, please see "How to Configure the Serial Port as the Primary Internet Connection" on page 3-15.

The FWG114P v2 provides these serial port configuration options:

- **Modem**
  Use this option to configure the serial modem settings for any of the features below.
- **Auto-Rollover**
  Use this option to provide a backup connection for your broadband service. If the broadband service you configured in the Basic Settings menu fails, the FWG114P v2 will automatically connect to the Internet through the serial port. However, you will then be accessing the Internet at a slower speed than you would through your broadband service.
- **Dial-in**
  Dial-in lets a single remote computer connect to the FWG114P v2 through the serial port to gain access to LAN resources or a remote access server.
- **LAN-to-LAN**
  LAN-to-LAN enables direct communications between two FWG114P v2 wireless firewall/print servers to:
  - Share resources on the two LANs.
  - Let users on one FWG114P v2 share the Internet connection of the other FWG114P v2.
  - Let users on one FWG114P v2 connect to the Internet through the second FWG114P v2 in case the broadband connection of the first FWG114P v2 fails.

The procedures for these configuration options are presented below.

Configuring a Serial Port Modem

You can configure a serial port modem for any of the features described above.

Be sure you have prepared the basic requirements listed below, then follow the ‘how to’ procedure.

Basic Requirements for Serial Port Modem Configuration

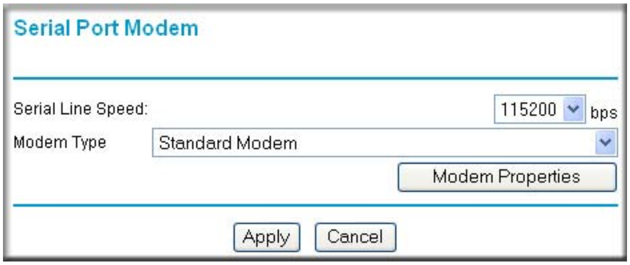
Configuring a serial port modem requires these elements:

1. A serial analog or ISDN modem.
2. A serial modem cable with a DB9 connector.
3. An active phone or ISDN line.

How to Configure a Serial Port Modem

Follow the steps below to configure a serial port modem.

1. From the main menu, click **Modem** in the Serial Port section.



Serial Port Modem

Serial Line Speed: 115200 bps

Modem Type: Standard Modem

Figure 5-1: Serial Port Modem configuration menu

2. Select the Serial Line Speed.
   This is the maximum speed the modem will attempt to use. For ISDN permanent connections, the speeds are typically 64000 or 128000 bps. For dial-up modems, 56000 bps would be a typical setting.
3. Select the Modem Type:
   — For ISDN, select “Permanent connection (leased line).”

- For dial-up, “Standard Modem” should work in most cases. Otherwise, select your modem from the list.
- If your modem is not on the list, select “User Defined” and enter the Modem Properties.

  If you are using the “User Defined” selection and configuring your own modem stings, fill in the Modem Properties settings.

  Note: You can validate modem string settings by first connecting the modem directly to a computer, establishing a connection to your ISP, and then copying the modem string settings from the computer configuration and pasting them into the FWG114P v2 Modem Properties Initial String field. For more information on this procedure, please refer to the support area of the NETGEAR Web site.

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

Configuring Auto-Rollover

You can configure the serial port of the FWG114P v2 to provide an auto-rollover backup connection for your broadband service.

Be sure you have prepared the basic requirements listed below, then follow the ‘how to’ procedure.

Basic Requirements for Auto-Rollover

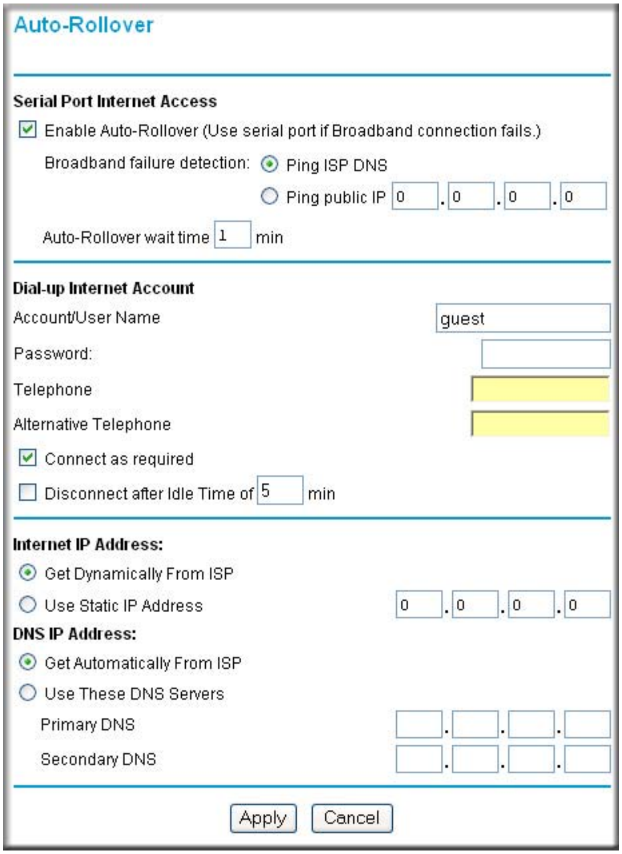
Auto-Rollover requires these elements:

1. A broadband connection to the FWG114P v2.
2. An ISDN or analog phone line with an active ISDN or dial-up ISP account.
3. A serial modem properly configured and attached to the DB9 connector on the serial port.
4. The Auto-Rollover settings configured and applied to the FWG114P v2.

How to Configure Auto-Rollover

Follow the steps below to configure a serial port auto-rollover connection.

1. Configure a serial port modem according to the instructions above.
2. From the main menu, click **Auto-rollover** in the Serial Port section.



Auto-Rollover

Serial Port Internet Access

☑ Enable Auto-Rollover (Use serial port if Broadband connection fails.)

Broadband failure detection: ● Ping ISP DNS

○ Ping public IP 0 . 0 . 0 . 0

Auto-Rollover wait time 1 min

Dial-up Internet Account

Account/User Name: guest

Password:

Telephone

Alternative Telephone

☑ Connect as required

☐ Disconnect after Idle Time of 5 min

Internet IP Address:

● Get Dynamically From ISP

○ Use Static IP Address 0 . 0 . 0 . 0

DNS IP Address:

● Get Automatically From ISP

○ Use These DNS Servers

Primary DNS . . .

Secondary DNS . . .

Figure 5-2: Auto-Rollover configuration menu

3. Configure the Auto-Rollover settings.
4. Click **Apply** for the changes to take effect.

Configuring Dial-in on the Serial Port

Dial-in lets a single remote computer connect to the FWG114P v2 through the serial port to gain access to LAN resources or a remote access server.

Be sure you have prepared the basic requirements listed below, then follow the ‘how to’ procedure.

Basic Requirements for Dial-in

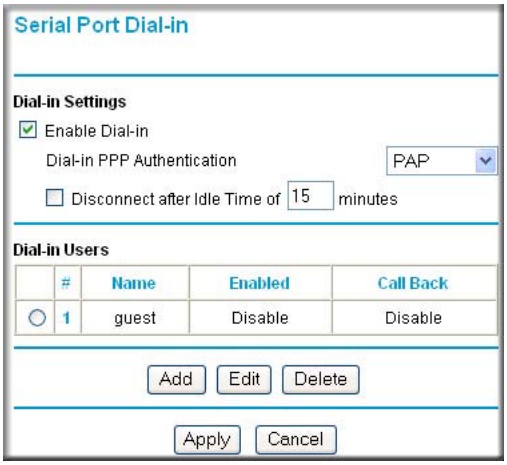
Dial-in requires these elements:

1. A broadband connection to the FWG114P v2.
2. An analog phone line.
3. A serial modem properly configured and attached to the DB9 connector on the serial port.
4. The Dial-in settings configured and applied to the FWG114P v2.

How to Configure Dial-in

Follow the steps below to configure a serial port dial-in connection.

1. Configure a serial port modem according to the instructions above.
2. From the Serial Port section of the main menu, click **Dial-in**.



Serial Port Dial-in

Dial-in Settings

☑ Enable Dial-in

Dial-in PPP Authentication: PAP

□ Disconnect after Idle Time of 15 minutes

Dial-in Users

	#	Name	Enabled	Call Back
○	1	guest	Disable	Disable

Figure 5-3: Serial Port Dial-in settings screen

3. Configure the Dial-in settings.
4. Click **Apply** for the changes to take effect.

Configuring LAN-to-LAN Settings

LAN-to-LAN enables direct communications between two FWG114P v2 wireless firewall/print servers.

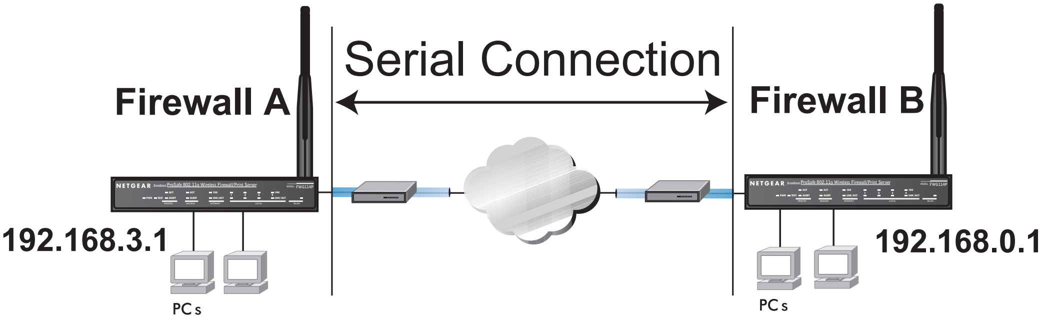


Figure 5-4: LAN-to-LAN network configuration

Basic Requirements for LAN-to-LAN Connections

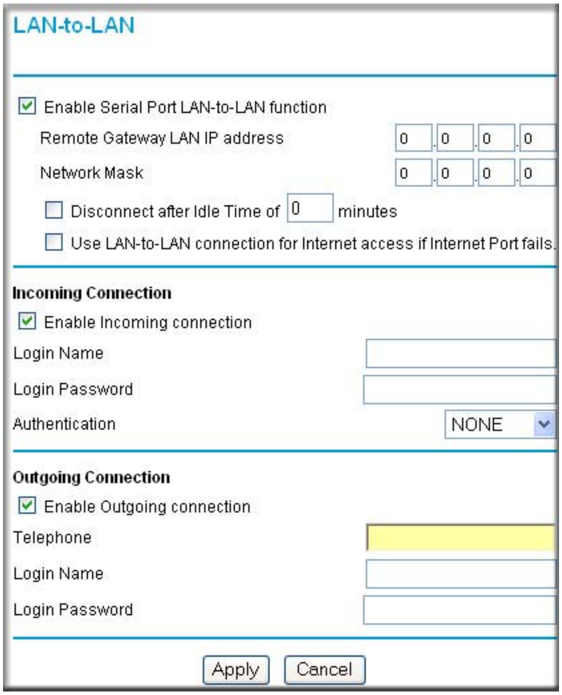
Serial port LAN-to-LAN configurations require these elements:

1. An ISDN or analog phone line with an active ISDN or dial-up ISP account.
2. A serial modem properly configured and attached to the DB9 connector on the serial port.
3. A broadband connection to one FWG114P v2 for LAN-to-LAN auto-rollover Internet access.
4. The LAN-to-LAN settings configured and applied to the two FWG114P v2 wireless firewall/print servers.

How to Configure LAN-to-LAN Connections

Follow these steps to configure a serial port LAN-to-LAN connection.

1. Configure a serial port modem.
2. From the main menu, click **LAN-to-LAN** in the Serial Port section.



LAN-to-LAN

☑ Enable Serial Port LAN-to-LAN function

Remote Gateway LAN IP address 0 . 0 . 0 . 0

Network Mask 0 . 0 . 0 . 0

□ Disconnect after Idle Time of 0 minutes

□ Use LAN-to-LAN connection for Internet access if Internet Port fails.

Incoming Connection

☑ Enable Incoming connection

Login Name

Login Password

Authentication NONE

Outgoing Connection

☑ Enable Outgoing connection

Telephone

Login Name

Login Password

Figure 5-5: LAN-to-LAN configuration menu

3. Configure the LAN-to-LAN settings.

   Note: The LAN subnet address of each FWG114P v2 must be different.

4. Click **Apply** for the changes to take effect.

Chapter 6
Firewall Protection and Content Filtering

This chapter describes how to use the content filtering features of the ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2 to protect your network. These features can be found by clicking on the Content Filtering heading in the Main Menu of the browser interface.

Firewall Protection and Content Filtering Overview

The ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2 provides you with Web content filtering options, plus browsing activity reporting and instant alerts via e-mail. Parents and network administrators can establish restricted access policies based on time-of-day, Web addresses, and Web address keywords. You can also block Internet access by applications and services, such as chat or games.

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

To configure these features of your router, click on the subheadings under the Content Filtering heading in the Main Menu of the browser interface. The subheadings are described below:

Using the Block Sites Menu to Screen Content

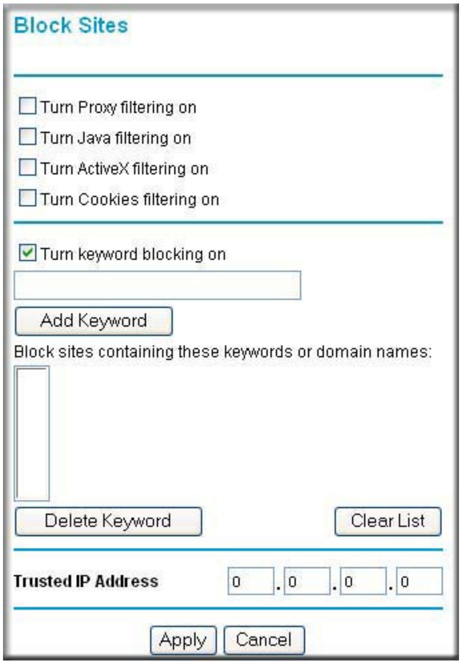
The FWG114P v2 allows you to restrict access based on the following categories:

- Use of a proxy server
- Type of file (Java, ActiveX, Cookie)

- Web addresses
- Web address keywords

These options are discussed below.

The Keyword Blocking menu is shown here.



Block Sites

□ Turn Proxy filtering on

□ Turn Java filtering on

□ Turn ActiveX filtering on

□ Turn Cookies filtering on

☑ Turn keyword blocking on

Block sites containing these keywords or domain names:

Trusted IP Address 0 . 0 . 0 . 0

Figure 6-1: Block Sites menu

To enable filtering, click the checkbox next to the type of filtering you want to enable. The filtering choices are:

- Proxy: blocks use of a proxy server
- Java: blocks use of Java applets
- ActiveX: blocks use of ActiveX components (OCX files) used by IE on Windows
- Cookies: blocks all cookies

To enable keyword blocking, check “Turn keyword blocking on”, then click Apply.

To add a keyword or domain, type it in the Keyword box, click Add Keyword, then click Apply.

To delete a keyword or domain, select it from the list, click Delete Keyword, then click Apply.

Keyword application examples:

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

Up to 255 entries are supported in the Keyword list.

To specify a Trusted User, enter that computer's IP address in the Trusted User box and click Apply. You may specify one Trusted User, which is a computer that will be exempt from blocking and logging. Since the Trusted User will be identified by an IP address, you should configure that computer with a fixed or reserved IP address.

Services and Rules Regulate Inbound and Outbound Traffic

The ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2 firewall lets you regulate what ports are available to the various TCP/IP protocols. Follow these two steps to configure inbound or outbound traffic:

1. **Define a Service**
2. **Set up an Inbound or Outbound Rule that uses the Service**

These steps are discussed below.

Defining a Service

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

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

Although the FWG114P v2 already holds a list of many service port numbers, you are not limited to these choices. Use the Services menu to add additional services and applications to the list for use in defining firewall rules. The Services menu shows a list of services that you have defined.

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

To add a service,

1. Enter a descriptive name for the service so that you will remember what it is.
2. Select whether the service uses TCP or UDP as its transport protocol.
   If you can’t determine which is used, select both.
3. Enter the lowest port number used by the service.
4. Enter the highest port number used by the service.
   If the service only uses a single port number, enter the same number in both fields.
5. Click Apply.

The new service will now appear in the Services menu, and in the Service name selection box in the Rules menu.

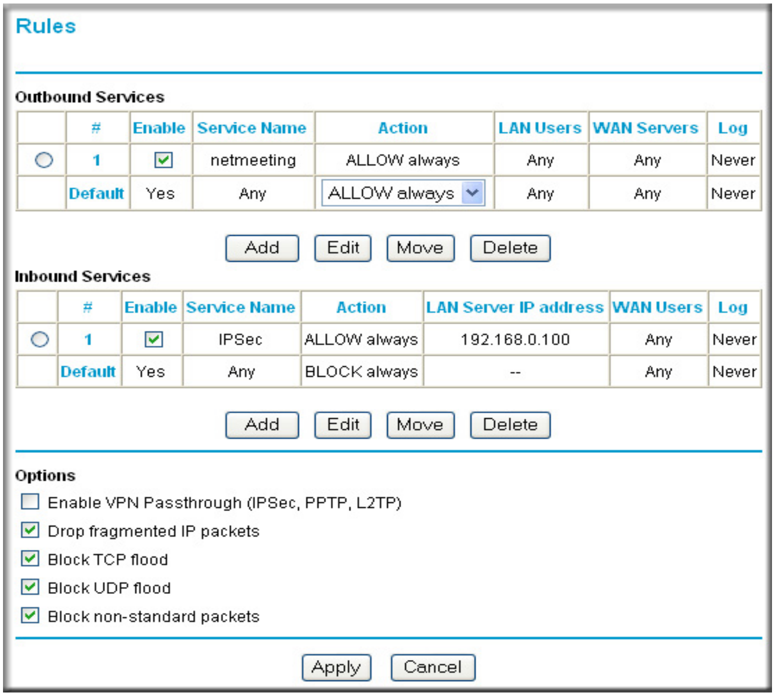
Using Inbound/Outbound Rules to Block or Allow Services

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

A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the FWG114P v2 are:

- Inbound: Block all access from outside except responses to requests from the LAN side.
- Outbound: Allow all access from the LAN side to the outside.

These default rules are shown in the Rules table of the Rules menu in Figure 6-2:



Rules

Outbound Services

	#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
○	1	☑	netmeeting	ALLOW always	Any	Any	Never
	Default	Yes	Any	ALLOW always	Any	Any	Never

Inbound Services

	#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
○	1	☑	IPSec	ALLOW always	192.168.0.100	Any	Never
	Default	Yes	Any	BLOCK always	--	Any	Never

Options

□ Enable VPN Passthrough (IPSec, PPTP, L2TP)
☑ Drop fragmented IP packets
☑ Block TCP flood
☑ Block UDP flood
☑ Block non-standard packets

Figure 6-2: Rules menu

You can define additional rules that will specify exceptions to the default rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. You can also choose to log traffic that matches or does not match the rule you have defined.

To create a new rule, click the Add button.

To edit an existing rule, select its button on the left side of the table and click Edit.

To delete an existing rule, select its button on the left side of the table and click Delete.

To move an existing rule to a different position in the table, select its button on the left side of the table and click Move. At the script prompt, enter the number of the desired new position and click OK.

An example of the menu for defining or editing a rule is shown in Figure 6-3. The parameters are:

- Service. From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the Services menu to add any additional services or applications that do not already appear.
- Action. Choose how you would like this type of traffic to be handled. You can block or allow always, or you can choose to block or allow according to the schedule you have defined in the Schedule menu.
- Source Address. Specify traffic originating on the LAN (outbound) or the WAN (inbound), and choose whether you would like the traffic to be restricted by source IP address. You can select Any, a Single address, or a Range. If you select a range of addresses, enter the range in the start and finish boxes. If you select a single address, enter it in the start box.
- Destination Address.The Destination Address will be assumed to be from the opposite (LAN or WAN) of the Source Address. As with the Source Address, you can select Any, a Single address, or a Range unless NAT is enabled and the destination is the LAN. In that case, you must enter a Single LAN address in the start box.
- Log. You can select whether the traffic will be logged. The choices are:
  - Never - no log entries will be made for this service.
  - Match - traffic of this type which matches the parameters and action will be logged.

Examples of Using Services and Rules to Regulate Traffic

Use the examples to see how you combine Services and Rules to regulate how the TCP/IP protocols are used on your firewall to enable either blocking or allowing specific Internet traffic on your wireless firewall/print server.

Inbound Rules (Port Forwarding)

Because the FWG114P v2 uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers. However, by defining an inbound rule, also known as port forwarding, you can make a local server (for example, a Web server or game server) visible and available to the Internet. The rule tells the router to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as port forwarding.

Note: Some home broadband accounts do not allow you to run any server processes (such as a Web or FTP server). Your ISP may check for servers and suspend your account if it discovers active servers at your location. If you are unsure, refer to the Acceptable Use Policy of your ISP.

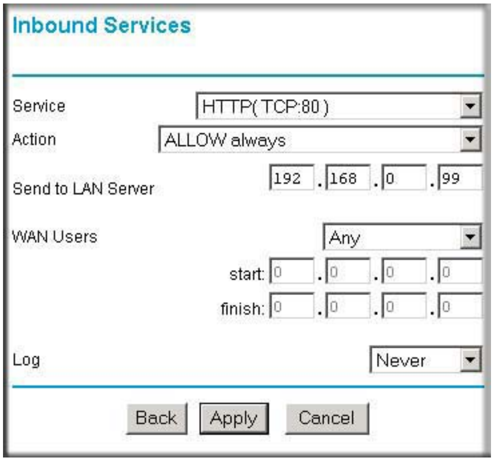
Follow these guidelines when setting up port forwarding inbound rules:

- If your external IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires. Consider using the Dyamic DNS feature in the Advanced menus so that external users can always find your network.
- If the IP address of the local server computer is assigned by DHCP, it may change when the computer is rebooted. To avoid this, use the Reserved IP address feature in the LAN IP menu to keep the computer’s IP address constant.
- Local computers must access the local server using the local LAN address of the computer. Attempts by local computers to access the server using the external WAN IP address will fail.

Remember that allowing inbound services opens holes in your FWG114P v2 Wireless Firewall/ Print Server. Only enable those ports that are necessary for your network. Following are two application examples of inbound rules:

Example: Port Forwarding to a Local Public Web Server

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



Inbound Services

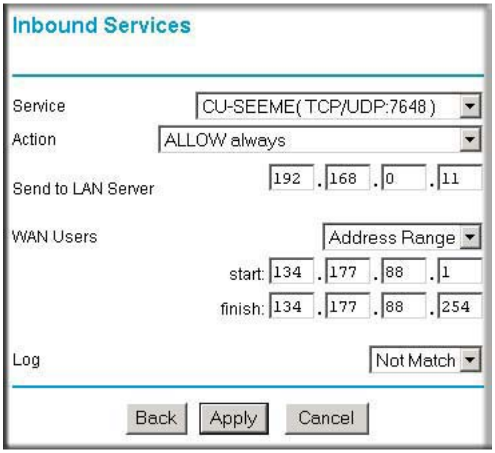
Service: HTTP(TCP:80)
Action: ALLOW always
Send to LAN Server: 192 . 168 . 0 . 99
WAN Users: Any
start: 0 . 0 . 0 . 0
finish: 0 . 0 . 0 . 0
Log: Never

Figure 6-3: Rule example: A Local Public Web Server

This rule is shown in Figure 6-3.

Example: Port Forwarding for Videoconferencing

If you want to allow incoming videoconferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office, you can create an inbound rule. In the example shown in Figure 6-4, CU-SeeMe is a predefined service and its connections are allowed only from a specified range of external IP addresses. In this case, we have also specified logging of any incoming CU-SeeMe requests that do not match the allowed parameters.



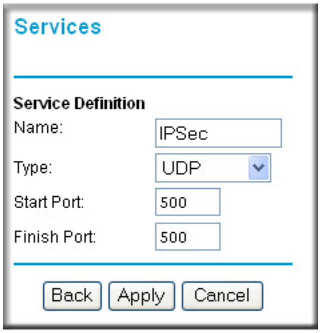
Inbound Services

Service: CU-SEEME(TCP/UDP:7648)
Action: ALLOW always
Send to LAN Server: 192 . 168 . 0 . 11
WAN Users: Address Range
start: 134 . 177 . 88 . 1
finish: 134 . 177 . 88 . 254
Log: Not Match

Figure 6-4: Rule example: Videoconference from Restricted Addresses

Example: Port Forwarding for VPN Tunnels when NAT is Off

If you want to allow incoming VPN IPSec tunnels to be initiated from outside IP addresses anywhere on the Internet when NAT is off, first create a service and then an inbound rule.



Services

Service Definition

Name: IPSec

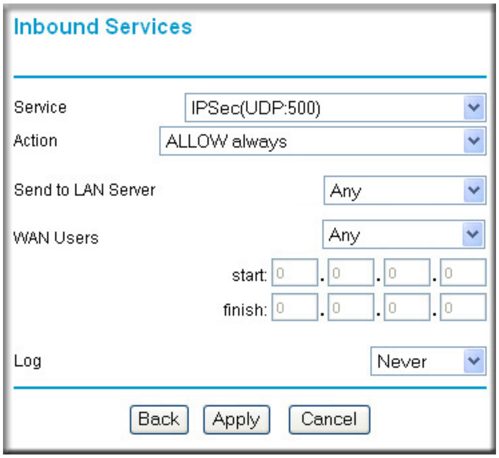
Type: UDP

Start Port: 500

Finish Port: 500

Figure 6-5: Service example: port forwarding for VPN when NAT is Off

In the example shown in Figure 6-5, UDP port 500 connections are defined as the IPSec service.



Inbound Services

Service: IPSec(UDP:500)

Action: ALLOW always

Send to LAN Server: Any

WAN Users: Any

start: 0 . 0 . 0 . 0

finish: 0 . 0 . 0 . 0

Log: Never

Figure 6-6: Inbound rule example: VPN IPSec when NAT is off

In the example shown in Figure 6-6, VPN IPSec connections are allowed for any internal LAN IP address.

Outbound Rules (Service Blocking or Port Filtering)

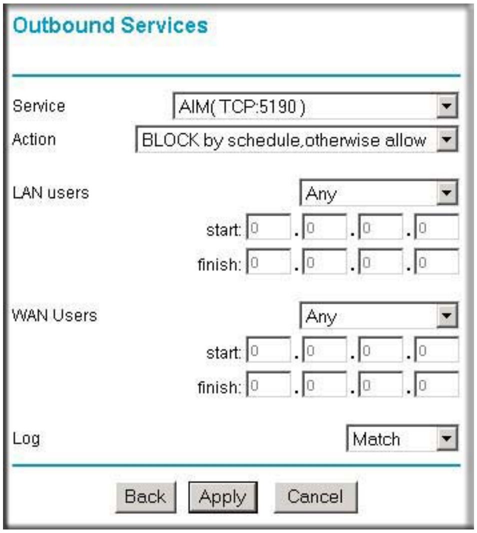
The FWG114P v2 allows you to block the use of certain Internet services by computers on your network. This is called service blocking or port filtering. You can define an outbound rule to block Internet access from a local computer based on:

- IP address of the local computer (source address)

- IP address of the Internet site being contacted (destination address)
- Time of day
- Type of service being requested (service port number)

Outbound Rule Example: Blocking Instant Messaging

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



Outbound Services

Service	AIM(TCP:5190)
Action	BLOCK by schedule,otherwise allow
LAN users	Any
start:	0 . 0 . 0 . 0
finish:	0 . 0 . 0 . 0
WAN Users	Any
start:	0 . 0 . 0 . 0
finish:	0 . 0 . 0 . 0
Log	Match

Figure 6-7: Rule example: Blocking Instant Messenger

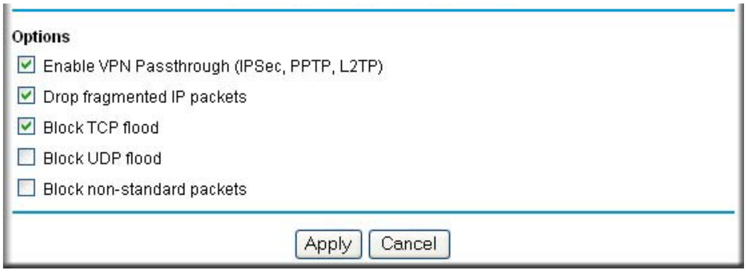
Other Rules Considerations

The order of precedence of rules is determined by the position of the rule on a list of many rules. Also, there are optional Rules settings you can configure. These topics are presented here.

Order of Precedence for Rules

As you define new rules, they are added to the tables in the Rules menu. For any traffic attempting to pass through the firewall, the packet information is subjected to the rules in the order of the entries in the Rules Table, beginning at the top and proceeding to the default rules at the bottom. In some cases, the order of precedence of two or more rules may be important in determining the disposition of a packet. The Move button allows you to relocate a defined rule to a new position in the table.

Rules Menu Options



Options

☑ Enable VPN Passthrough (IPSec, PPTP, L2TP)

☑ Drop fragmented IP packets

☑ Block TCP flood

□ Block UDP flood

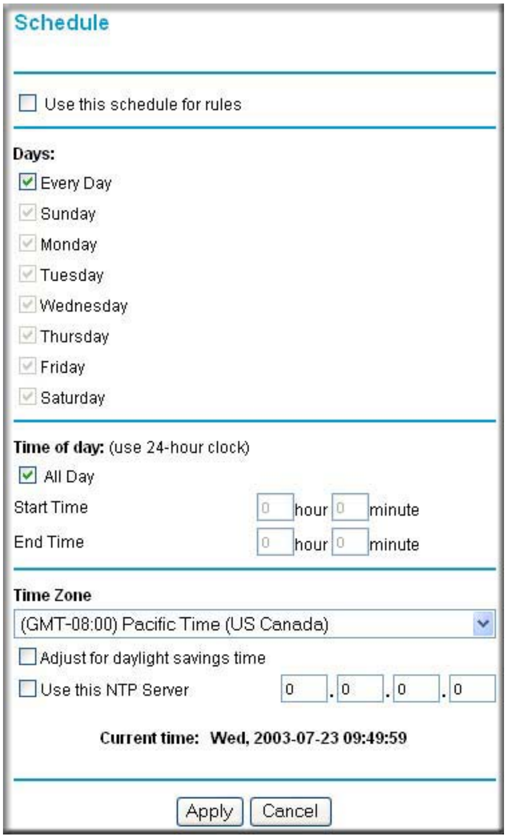
□ Block non-standard packets

Use the Options checkboxes to enable the following:

- **Enable VPN Passthrough (IPSec, PPTP, L2TP)**
  If LAN users need to use VPN (Virtual Private Networking) software on their computer, and connect to remote sites or servers, enable this checkbox. This will allow the VPN protocols (IPSec, PPTP, L2TP) to be used. If this checkbox is not checked, these protocols are blocked.
- **Drop fragmented IP packets**
  If checked, all fragmented IP packets will be dropped (discarded). Normally, this should NOT be checked.
- **Block TCP flood**
  If checked, when a TCP flood attack is detected, the port used will be closed, and no traffic will be able to use that port.
- **Block UDP flood**
  If checked, when a UDP flood attack is detected, all traffic from that IP address will be blocked.
- **Block non-standard packets**
  If checked, only known packet types will be accepted; other packets will be blocked. The known packet types are TCP, UDP, ICMP, ESP, and GRE. Note that these are packet types, not protocols.

Using a Schedule to Block or Allow Content or Traffic

If you enabled content filtering in the Block Sites menu, or if you defined an outbound rule to use a schedule, you can set up a schedule for when blocking occurs or when access is restricted. The router allows you to specify when blocking will be enforced by configuring the Schedule tab shown below.



Schedule

☐ Use this schedule for rules

Days:

☑ Every Day
☑ Sunday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday

Time of day: (use 24-hour clock)

☑ All Day

Start Time 0 hour 0 minute
End Time 0 hour 0 minute

Time Zone

(GMT-08:00) Pacific Time (US Canada)

☐ Adjust for daylight savings time
☐ Use this NTP Server 0 . 0 . 0 . 0

Current time: Wed, 2003-07-23 09:49:59

Figure 6-8: Schedule menu

To block keywords or Internet domains based on a schedule, select Every Day or select one or more days. If you want to limit access completely for the selected days, select All Day. Otherwise, If you want to limit access during certain times for the selected days, type a Start Time and an End Time.

Note: Enter the values in 24-hour time format. For example, 10:30 am would be 10 hours and 30 minutes and 10:30 pm would be 22 hours and 30 minutes.

Be sure to click Apply when you have finished configuring this menu.

Setting the Time Zone

The FWG114P v2 Wireless Firewall/Print Server uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet. In order to localize the time for your log entries, you must specify your Time Zone:

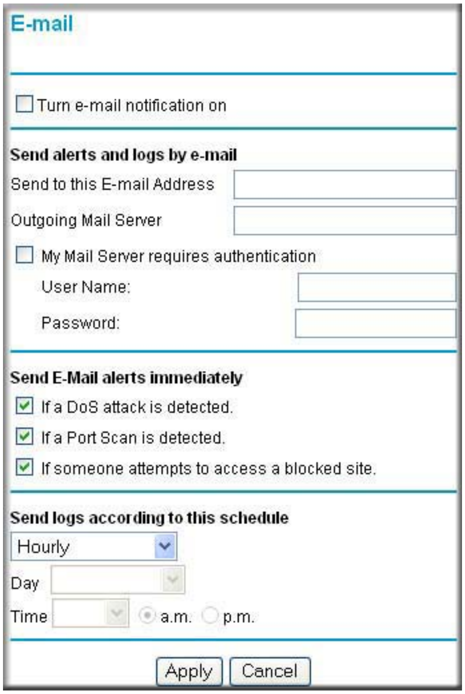
- Time Zone. Select your local time zone. This setting will be used for the blocking schedule and for time-stamping log entries.
- Daylight Savings Time. Select this check box for daylight savings time.

  Note: If your region uses Daylight Savings Time, you must manually select Adjust for Daylight Savings Time on the first day of Daylight Savings Time, and unselect it at the end. Enabling Daylight Savings Time will add one hour to the standard time.

Be sure to click Apply when you have finished configuring this menu.

Getting E-Mail Notifications of Event Logs and Alerts

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



E-mail

□ Turn e-mail notification on

Send alerts and logs by e-mail

Send to this E-mail Address

Outgoing Mail Server

□ My Mail Server requires authentication

User Name:

Password:

Send E-Mail alerts immediately

☑ If a DoS attack is detected.

☑ If a Port Scan is detected.

☑ If someone attempts to access a blocked site.

Send logs according to this schedule

Hourly

Day

Time ● a.m. ○ p.m.

Figure 6-9: E-mail menu

- **Turn e-mail notification on.** Select this check box if you want to receive e-mail logs and alerts from the router.
- **Send alerts and logs by e-mail.** If you enable e-mail notification, these boxes cannot be blank. Enter the name or IP address of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You may be able to find this information in the configuration menu of your e-mail program. Enter the e-mail address to which logs and alerts will be sent. This e-mail address will also be used as the From address. If you leave this box blank, log and alert messages will not be sent via e-mail. Check "My Mail Server requires authentication" if you need to log in to your SMTP server in order to send e-mail. If this is checked, you must enter the login name and password for your mail server.

  Tip: You used this information when you set up your e-mail program. If you cannot remember it, check the settings in your e-mail program.
- **Send E-mail alerts immediately.** You can specify that logs are immediately sent to the specified e-mail address when any of the following events occur:

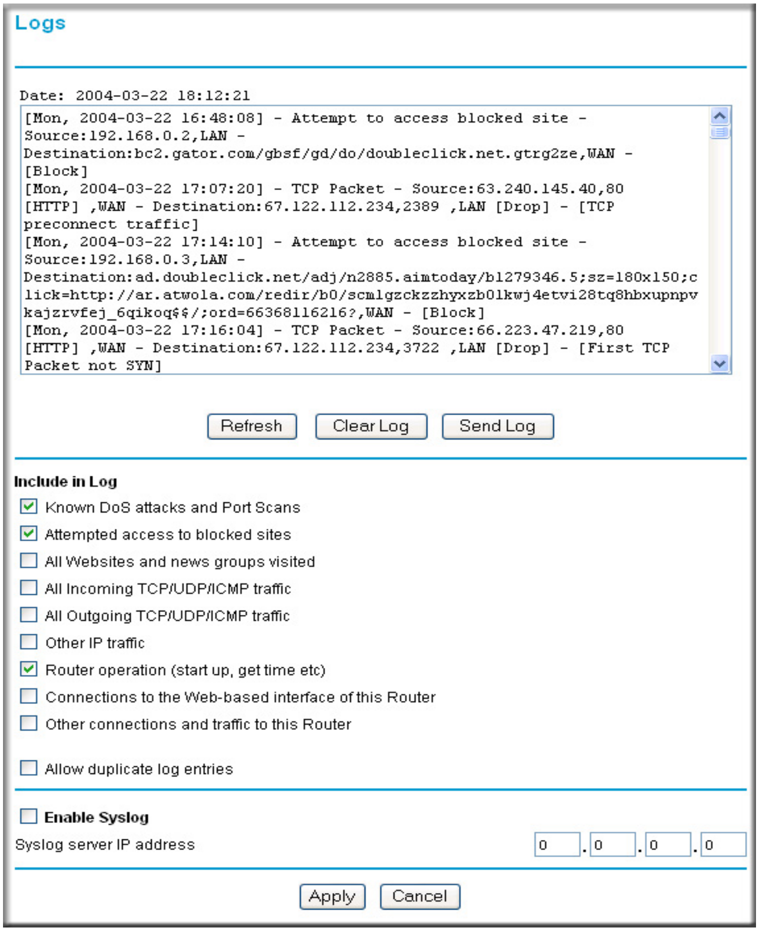
  - If a Denial of Service attack is detected.
  - If a Port Scan is detected.
  - If a user on your LAN attempts to access a website that you blocked using Keyword blocking.
- **Send logs according to this schedule.** You can specify that logs are sent to you according to a schedule. Select whether you would like to receive the logs Hourly, Daily, Weekly, When Full, or None for no logs. Depending on your selection, you may also need to specify:
  - Day for sending log
    Relevant when the log is sent weekly or daily.
  - Time for sending log
    Relevant when the log is sent daily or weekly.

  If the Weekly, Daily or Hourly option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, the log is cleared from the router's memory. If the router cannot e-mail the log file, the log buffer may fill up. In this case, the router overwrites the log and discards its contents.

Be sure to click Apply when you have finished configuring this menu.

Viewing Logs of Web Access or Attempted Web Access

The router will log security-related events, such as denied incoming and outgoing service requests, hacker probes, and administrator logins. If you enable content filtering in the Block Sites menu, the Log page will also show you when someone on your network tries to access a blocked site. If you enabled e-mail notification, you will receive these logs in an e-mail message. If you do not have e-mail notification enabled, you can view the logs here.



```
Date: 2004-03-22 18:12:21
[Mon, 2004-03-22 16:48:08] - Attempt to access blocked site -
Source:192.168.0.2,LAN -
Destination:bc2.gator.com/gbsf/gd/do/doubleclick.net.gtrg2ze,WAN -
[Block]
[Mon, 2004-03-22 17:07:20] - TCP Packet - Source:63.240.145.40,80
[HTTP] ,WAN - Destination:67.122.112.234,2389 ,LAN [Drop] - [TCP
preconnect traffic]
[Mon, 2004-03-22 17:14:10] - Attempt to access blocked site -
Source:192.168.0.3,LAN -
Destination:ad.doubleclick.net/adj/n2885.aimtoday/b1279346.5;sz=180x150;c
lick=http://ar.atwola.com/redir/b0/scmlgzckzzhyxzb0lkwj4etvi28tq8hbxupnpv
kajzrvfej_6qikoq$$/;ord=66368116216?,WAN - [Block]
[Mon, 2004-03-22 17:16:04] - TCP Packet - Source:66.223.47.219,80
[HTTP] ,WAN - Destination:67.122.112.234,3722 ,LAN [Drop] - [First TCP
Packet not SYN]
```

Include in Log

- ☑ Known DoS attacks and Port Scans
- ☑ Attempted access to blocked sites
- □ All Websites and news groups visited
- □ All Incoming TCP/UDP/ICMP traffic
- □ All Outgoing TCP/UDP/ICMP traffic
- □ Other IP traffic
- ☑ Router operation (start up, get time etc)
- □ Connections to the Web-based interface of this Router
- □ Other connections and traffic to this Router

□ Allow duplicate log entries

□ **Enable Syslog**

Syslog server IP address 0 . 0 . 0 . 0

Figure 6-10: Logs menu

See Appendix D, “Firewall Log Formats” for a full explanation of log entry formats.

Log action buttons are described in Table 6-1.

Table 6-1. Log action buttons

Field	Description
Refresh	Refreshes the log screen.
Clear Log	Clears the log entries.
Send Log	E-mails the log immediately.

What to Include in the Event Log

Use these checkboxes to determine which events are included in the log. Checking all options will increase the size of the log, so it is good practice to disable any events which are not really required.

- All Websites and news groups visited - If checked, all visited websites and newsgroups are logged.
- All Incoming TCP/UDP/ICMP traffic - If checked, all incoming TCP/UDP/ICMP connections and traffic is logged.
- All Outgoing TCP/UDP/ICMP traffic - If checked, all outgoing TCP/UDP/ICMP connections and traffic is logged.
- Other IP traffic - If checked, all other traffic (IP packets which are not TCP, UDP, or ICMP) is logged.
- Router operation (start up, get time, etc.) - If checked, Router operations, such as starting up and getting the time from the Internet Time Server, are logged.
- Connection to the Web-based interface of this Router - If checked, Administrator connections to the Web-based interface will be logged.
- Other connections and traffic to this Router - If checked, this will log traffic sent to this Router (rather than through this Router to the Internet).
- Allow duplicate log entries - If checked, then events or packets which fall within more than one (1) category above will have a log entry for each category in which they belong. This will generate a large number of log entries. If unchecked, then events or packets will only be logged once. Usually, this should be left unchecked.

Logging programs are available for Windows, Macintosh, and Linux computers.

Enable one of these three options, as required:

- Disable - select this if you do not have a Syslog server.
- Broadcast on LAN - the Syslog data is broadcast, rather than sent to a specific Syslog server. Use this if your Syslog Server does not have a fixed IP address.
- Send to this Syslog server IP address - If your Syslog server has a fixed IP address, select this option, and enter the IP address of your Syslog server.

Chapter 7
Print Server

This chapter describes how to install and configure the print server in your ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2.

Printing Options

The FWG114P v2 supports these methods for printing:

- **For Windows XP and 2000 Only: TCP/IP Line Printer Remote (LPR) Printing**
  - No software needs to be installed
  - Windows XP or 2000 users can print directly to the firewall. Print jobs are spooled (queued) on each computer. The computer sends the print job directly to the LAN IP address of the FWG114P v2.
- **For Windows 95/98/Me, NT4.0, 2000, and XP: Netgear Printer Port Driver**
  - Install the Netgear Printer Port Driver on Each computer.
  - After installing the Print Port Driver from the *Resource CD for the ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P (SW-10023-03)* Windows users can print directly to the firewall. Print jobs are spooled (queued) on each computer.
- **For Macintosh computers: LPR printing**
  - No software needs to be installed
  - LPR printing can be set up on any Macintosh that has Desktop Printing installed or available. Desktop Printing is supported on MacOS versions beginning from 8.1. LaserWriter8 version 8.5.1 or higher is also required.
- **For Windows NT 4.0 Server or 2000 Server: LPD/LPR Printing**
  - No software needs to be installed
  - If using Windows NT 4.0 Server or Windows 2000 Server, LPD/LPR printing can be used. No software needs to be installed on either the Windows Server or each client computer. Print jobs will be spooled (queued) on the Windows Server, and can be managed using the standard Windows Server tools.

For Windows XP and 2000, Use TCP/IP LPR Printing

Follow these instructions to set up TCP/IP printing on your Windows XP and 2000 PCs.

1

Install the FWG114P v2, connect your printer to the USB port on the FWG114P v2, and run the Windows Add Printer Wizard.

a. Follow the instructions in the printed Installation Guide or this manual to install your FWG114P v2. Connect your printer to the USB port on the back of the FWG114P v2.

b. From the Windows Start menu of a computer connected to the FWG114P v2, click **Printers and Faxes**.

c. Click **Add a printer**. Click **Next** to proceed.

d. Be sure to choose the **Local printer attached to this computer** option.

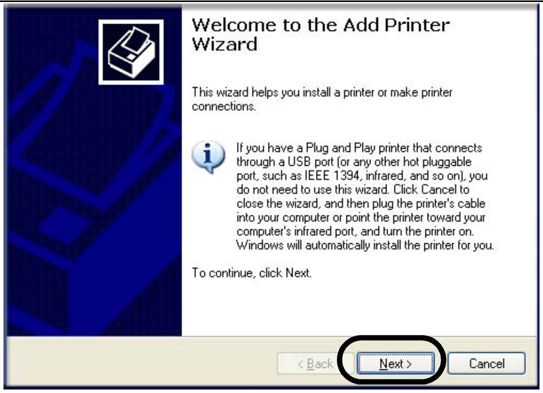
Click **Next** to proceed.

e. On the Select a Printer Port screen, be sure to choose the **Create a new port:** option.

From the Type of port: drop-down list, be sure to select **Standard TCP/IP Port**.

Click **Next** to proceed.

This will start the Add Standard TCP/IP Printer Port Wizard.



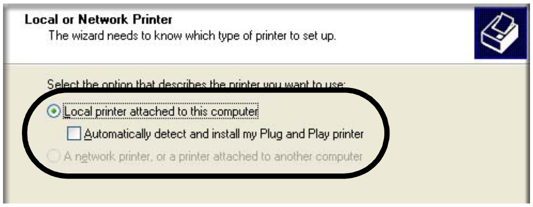
Welcome to the Add Printer Wizard

This wizard helps you install a printer or make printer connections.

If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.

To continue, click Next.

Add Printer Wizard



Local or Network Printer
The wizard needs to know which type of printer to set up.

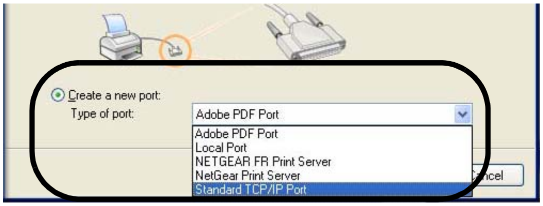
Select the option that describes the printer you want to use:

● Local printer attached to this computer

□ Automatically detect and install my Plug and Play printer

○ A network printer, or a printer attached to another computer

Local or Network Printer screen



● Create a new port:

Type of port: Adobe PDF Port

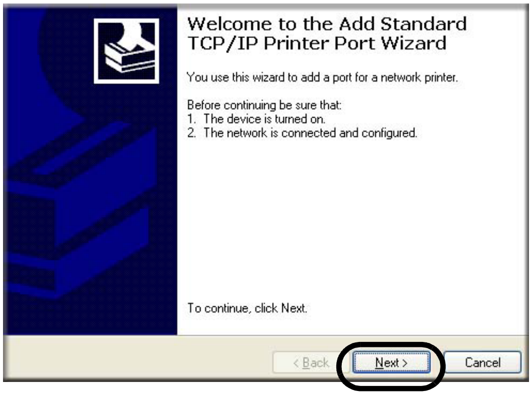
Adobe PDF Port
Local Port
NETGEAR FR Print Server
NetGear Print Server
Standard TCP/IP Port

Select a Printer Port screen

2

Complete the Add Standard TCP/IP Printer Port Wizard.

a. Click **Next** to proceed with the Add Standard TCP/IP Printer Port Wizard. The Add Port screen will display.



Welcome to the Add Standard TCP/IP Printer Port Wizard

You use this wizard to add a port for a network printer.

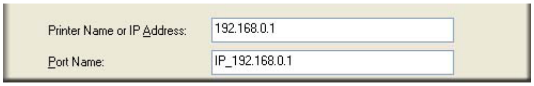
Before continuing be sure that:
1. The device is turned on.
2. The network is connected and configured.

To continue, click Next.

Add Standard TCP/IP Printer Port Wizard

b. From the Add Port screen, enter **192.168.0.1**, the FWG114P v2 default LAN IP address, in the IP Address field. **Note**: If you changed the default LAN IP Address of the FWG114P v2, be sure to use the address you assigned here. The Port Name is automatically filled in.

Click **Next** to proceed.

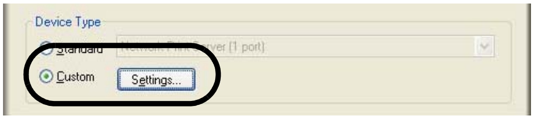


Printer Name or IP Address: 192.168.0.1

Port Name: IP_192.168.0.1

Add Port Screen

c. In the Device Type section of the Additional Port Information Required screen, select **Custom**.



Device Type

○ Standard Network Print Server (1 port)

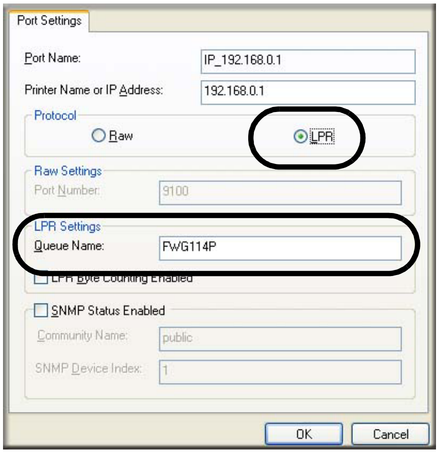
● Custom

Additional Port Information Required

d. In the Custom selection, click **Settings.**

e. The Port Settings tab page opens. In the Protocol section, select the **LPR** radio button, and enter **FWG114P** as the Queue Name in the LPR Settings section. Click **OK** to close this tab page.

Click **Next** to proceed.



Port Settings

Port Name: IP_192.168.0.1

Printer Name or IP Address: 192.168.0.1

Protocol

○ Raw ● LPR

Raw Settings

Port Number: 9100

LPR Settings

Queue Name: FWG114P

□ LPR Byte Counting Enabled

□ SNMP Status Enabled

Community Name: public

SNMP Device Index: 1

Additional Port Information Required

The Add Printer Wizard will now prompt you to install the software for the printer you attached to the FWG114P v2.

3

Identify the printer connected to FWG114P v2 USB printer port.

a. From the Install Printer Software screen selection lists, find the manufacturer and model of the printer you connected to the USB port on the FWG114P v2.

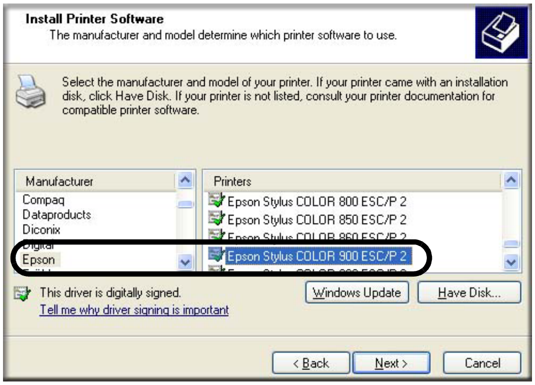
Click **Next** to proceed.

If the printer software is already installed on this computer, the Add Printer Wizard will inform you and let you keep the existing driver.

b. The Name Your Printer screen prompts for a descriptive name and if you want it to be the default. Enter your choices.

Click **Next** to proceed.

c. On the Printer Sharing screen, accept the “Do not share this printer” option and click **Next** to proceed.



Install Printer Software

The manufacturer and model determine which printer software to use.

Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for compatible printer software.

This driver is digitally signed.

Tell me why driver signing is important

Manufacturer
Compaq
Dataproducts
Diconix
Digital
Epson
Printers
Epson Stylus COLOR 800 ESC/P 2
Epson Stylus COLOR 850 ESC/P 2
Epson Stylus COLOR 860 ESC/P 2
Epson Stylus COLOR 900 ESC/P 2
Windows Update
Have Disk...
< Back
Next >
Cancel

Add Printer Wizard Install Printer Software page

If you do not see your make and model printer in the lists, and you are connected to the Internet, you can click the Windows Update button to download additional printer software from the Microsoft Web site, or you can click the Have Disk button to install the printer software from a disk you have.

4

Print a test page to verify successful printing on your network.

a. Upon completion of the Add Printer Wizard, you will be prompted to print a test page.

b. Check the printer attached to the FWG114P v2 to see that the test page printed successfully.

If you are unable to print a test page, see “Troubleshooting the Print Server“ on page -12.

➡	**Note:** If two long files are sent to the printer at once, Windows will pop up a print failure error message. This message can be ignored. The file will print once the printer finishes printing the first file.

For Windows 95/98/Me, Use the Netgear Printer Port Driver

Follow these instructions to set up the Netgear Printer Port Drive on Windows 9x PCs.

1

Install the Netgear Printer Port Driver and configuration utility software.

a. Follow the instructions in the printed Installation Guide or this manual to install your FWG114P v2.

b. Connect your printer to the USB port on the back of the FWG114P v2.

c. Insert the Resource CD for the FWG114P v2 into the CD-ROM drive of a computer connected to the FWG114P v2.

The CD main page shown at the right will load.

d. Click the **Print Server** button.

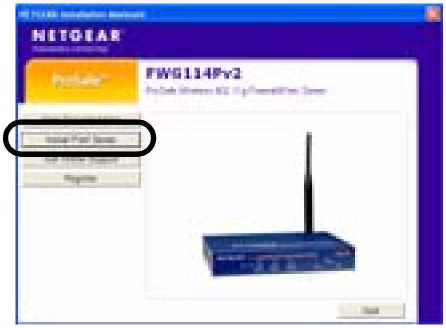
Follow the instructions for running the setup utility.

e. Click **Next** to proceed through the Netgear Printer Port Installation Wizard steps.

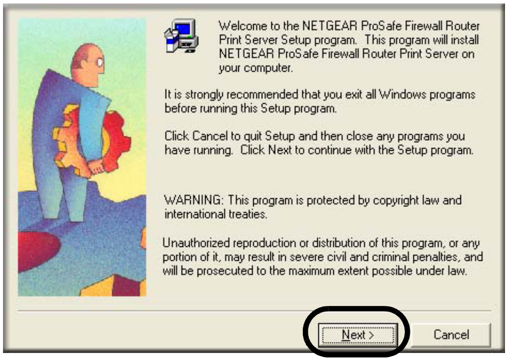
Note: Windows 2000 or XP may require you to be logged on with administrator rights.

Warning: If you are installing the Netgear printer port driver on a Windows computer where an Epson printer had been installed, you must disable the Epson Spool Manager. Failure to disable Epson Spool Manager software will prevent the Netgear printer port driver from operating.

To disable the Epson Spool Manager, run the Epson Spool Manager, select **Queue Setup** from the menu, click **Use Print Manager for this port**, and click **OK** to exit.



FWG114P v2 Resource CD



Welcome to the NETGEAR ProSafe Firewall Router Print Server Setup program. This program will install NETGEAR ProSafe Firewall Router Print Server on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

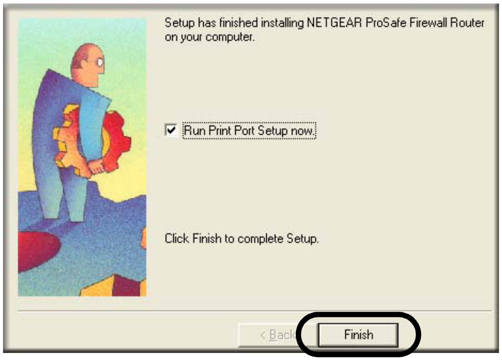
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Netgear Printer Port Installation Wizard

2

Set up the Netgear printer port driver.

a. Click **Finish** when the Installation Wizard is done.



Setup has finished installing NETGEAR ProSafe Firewall Router on your computer.

☑ Run Print Port Setup now.

Click Finish to complete Setup.

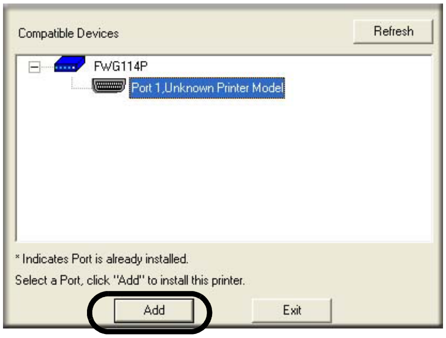
Netgear Printer Port Installation Wizard

The Printer Port Setup utility displays, and queries the network to locate the print server in the FWG114P v2.

After a short delay, the Printer Port Setup utility will display the port it finds in the FWG114P v2 print server.

Note: Under Windows 95, you may receive an error message stating that SETUPAPI.DLL was not found. In this case, you should upgrade your Internet Explorer to version 5 or later.

b. Click **Add** to add this printer port to your computer.



Compatible Devices

FWG114P

Port 1,Unknown Printer Model

* Indicates Port is already installed.

Select a Port, click "Add" to install this printer.

Netgear Printer Port Setup Utility

The Printer Port Setup utility will report that Port FWG114P_P1 has been added to the computer.

c. Click **Exit** to exit the Printer Port Setup utility.

The Windows Add Printer Wizard automatically runs.

3

Identify the printer connected to the FWG114P v2 USB printer port.

a. From the Add Printer Wizard screen selection lists, find the manufacturer and model of the printer you connected to the USB port on the FWG114P v2.

Click **Next** to proceed.

If the printer software is already installed on this PC, the Add Printer Wizard will inform you and let you keep the existing driver.

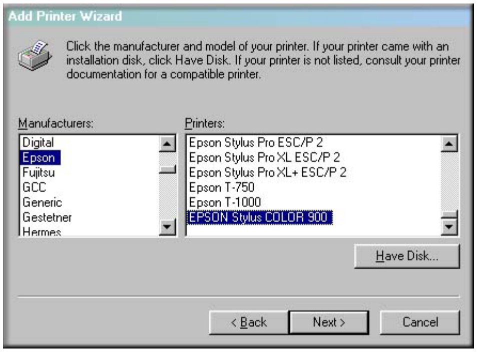
b. Be sure to select the **FWG114P_P1** port in the Add Printer Wizard.

Click **Next.**

c. The Name Your Printer screen prompts for a descriptive name and if you want it to be the default. Enter your choices.

If prompted about Sharing, do not enable Sharing.

Click **Next** to proceed and finish the Add Printer Wizard steps.



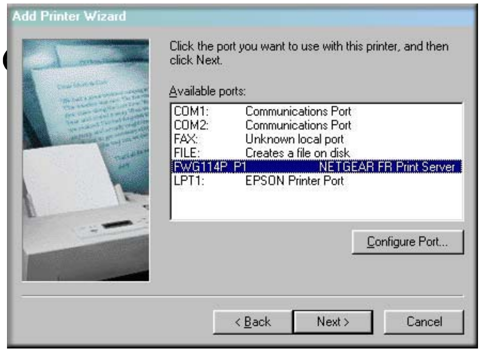
Add Printer Wizard

Click the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

Manufacturers:	Printers:
Digital	Epson Stylus Pro ESC/P 2
Epson	Epson Stylus Pro XL ESC/P 2
Fujitsu	Epson Stylus Pro XL+ ESC/P 2
GCC	Epson T-750
Generic	Epson T-1000
Gestetner	EPSON Stylus COLOR 900
Hermes	

Windows Add Printer Wizard

If you do not see your make and model printer in the lists, and you are connected to the Internet, you can click the Windows Update button to download additional printer software from the Microsoft Web site, or you can click the Have Disk button to install the printer software from a disk you have.



Add Printer Wizard

Click the port you want to use with this printer, and then click Next.

Available ports:

COM1:	Communications Port
COM2:	Communications Port
FAX:	Unknown local port
FILE:	Creates a file on disk
FWG114P_P1	NETGEAR FR Print Server
LPT1:	EPSON Printer Port

Windows Add Printer Wizard

4

Print a test page to verify successful printing on your network.

a. Upon completion of the Add Printer Wizard, print a test page.
   - From the Windows Start menu, select Setup > Printers.
   - Highlight the printer you just added.
   - Right-click and the select **Properties**.
     The printer properties dialog box opens to the General tab page.
   - On the General tab page, click **Print Test Page**.

b. Check the printer attached to the FWG114P v2 to see that the test page printed successfully.

If you are unable to print a test page, see “Troubleshooting the Print Server“ on page -12.

Printing from the Macintosh

Macintosh computers can connect to a TCP/IP network printer using the Line Printer Remote (LPR) protocol. LPR printing can be set up on any Macintosh that has Desktop Printing installed or available. Desktop Printing is supported on MacOS versions beginning from 8.1. LaserWriter8 version 8.5.1 or higher is also required.

To configure the Macintosh to use the print server, follow these steps:

1. From the Apple Extras folder, under Apple LaserWriter Software, launch the Desktop Printing Utility. A new window titled New Desktop Printer appears.
2. Select LaserWriter 8 in the “With” drop-down menu.
3. Select Printer (LPR) and click OK. A new window called Untitled 1 will open.
4. If the PostScript Printer Description does not match your printer, click Change... and select your actual printer.
   If your printer model does not appear, click the Generic button.
5. Click OK to return to the Untitled 1 window.

6. In the LPR Printer Selection box, click Change...
7. In the Printer Address field, type the name or IP address of the FWG114P v2 Wireless Firewall/Print Server.
   The IP address will usually be 192.168.0.1.
   You can leave the Queue Name blank.

   Click Verify to make sure your computer can see the printer.
   You should see the IP address displayed above the button. If no IP Address appears, check that you have correctly typed the queue name or IP Address.

   Click OK to return to the Untitled 1 window.
8. At the bottom of the Untitled 1 dialog box, click Create....

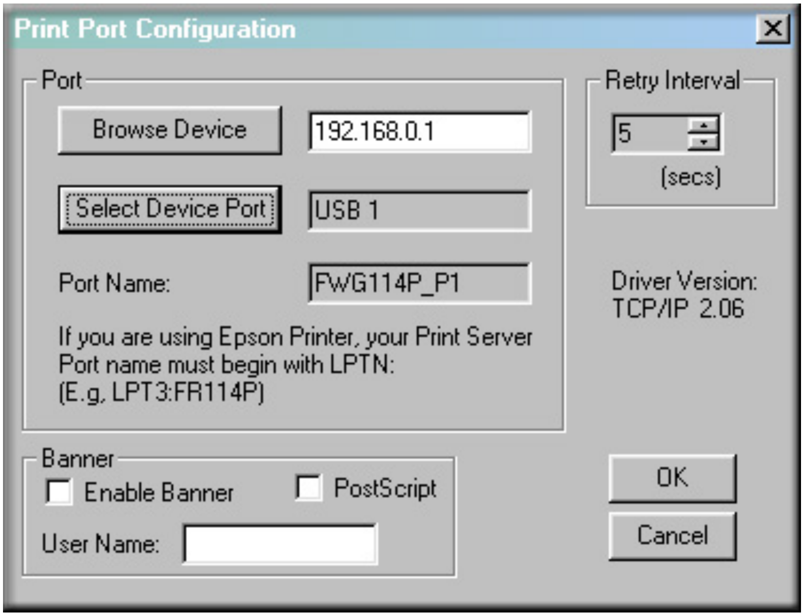
   When prompted, rename the printer with a descriptive name and click Save.
   A printer icon should now appear on your desktop.
9. Quit the Desktop Printer Utility.

Windows Printer Port Management

- Print jobs can be managed from Windows. Open the Printers folder (Start -> Settings -> Printers) and double-click any printer to see the current print jobs.
- To delete a port created by this setup program, use the Windows Delete Port facility:
  a. Right-click any printer in the Printers folder, and select Properties.
  b. Highlight the port you want to delete.
  c. Use the Delete Port button to delete the port. This button is on either the Details or Ports tab, depending on your version of Windows.
- If you change the printer attached to the FWG114P v2, run the Add Port program again and select the new printer.

The options for the Print Port Driver are accessed via the Windows Port Settings button.

Use Start -> Settings -> Printers to open the Printers folder, then right-click the Printer and select Properties. The Port Settings button is on either the Details or Port tab, depending on your version of Windows. An example screen is shown below:



Print Port Configuration

Port

Browse Device: 192.168.0.1

Select Device Port: USB 1

Port Name: FWG114P_P1

If you are using Epson Printer, your Print Server Port name must begin with LPTN:
(E.g, LPT3:FR114P)

Retry Interval: 5 (secs)

Driver Version:
TCP/IP 2.06

Banner

□ Enable Banner □ PostScript

User Name:

Figure 7-1: Print Port Configuration menu

Items shown on this screen are as follows:

- Port

  If desired, click Browse Device to select a different device. The Select Device Port button supports multi-port models, but the FWG114P v2 Wireless Firewall/Print Server is a single-port print server. The Port Name is shown in the Printer's Properties.

- Banner

  Check this option to print a banner page before each print job. The User Name you enter will be printed on the banner page. If using a PostScript Printer, check the PostScript box.

- Retry Interval

  Determines how often Windows will poll the print server to establish a connection when the printer is busy.

Troubleshooting the Print Server

Note: When the TCP/IP LPR configuration is used, if two long files are sent to the printer at once, Windows will pop up a print failure error message. This message can be ignored. The file will print once the printer finishes printing the first file. This does not happen when the Netgear Printer Port driver is used.

Question: When I tried to install the Printer Driver for Peer-to-Peer printing, I received an error message and the installation was aborted.

Answer: This may be caused by an existing installation of the printer port software. Before attempting another installation, remove the existing installation and restart your PC.

To remove an existing printer port installation:

a. Open Start -> Settings -> Control Panel -> Add/Remove Programs.

b. Look for an entry with a name like “NETGEAR ProSafe Firewall Router”, “NETGEAR Print Server”, "Print Server Driver" or "Print Server Port".

c. Select this item, click Add/Remove, and confirm the deletion.

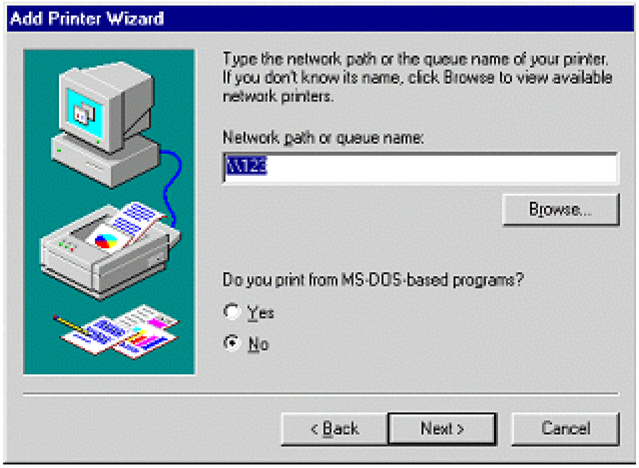
Question: I am using Windows 95. The Printer Driver installed and ran, but when I selected a port and clicked Add, the printer was not installed.

Answer: Try installing the printer using the standard Windows tools, as follows:

a. From Start -> Settings, open the Printers folder, and start the Add Printer Wizard.

b. When prompted, select Network Printer and click Next.

c. For Network Path or Queue, enter a dummy value, such as \\123, as shown below. Select NO for “Do you print from MS-DOS-based programs?”.



Add Printer Wizard

Type the network path or the queue name of your printer. If you don't know its name, click Browse to view available network printers.

Network path or queue name: \\123

Do you print from MS-DOS-based programs?

○ Yes

● No

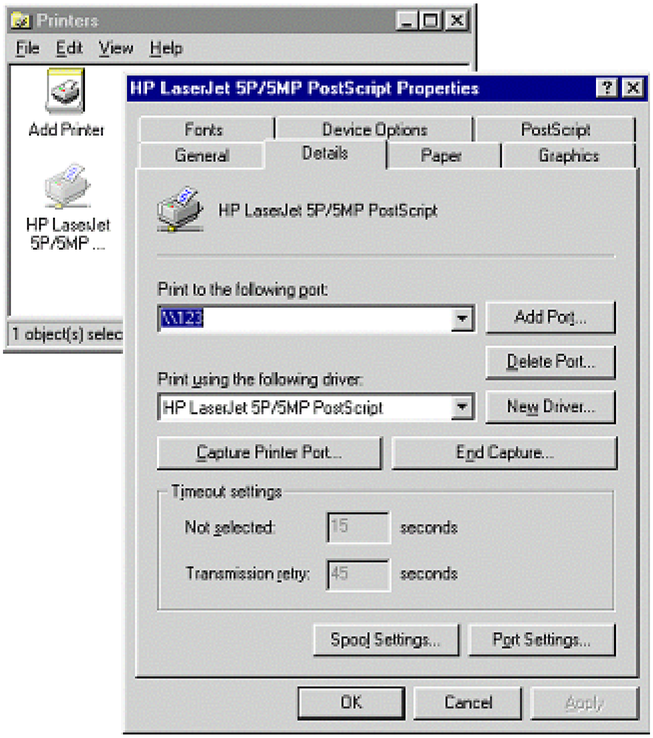
d. Click Next.

Figure 7-2: Windows Add Printer Wizard

e. The printer wizard will display a message stating that "The Network Printer is off-line". This is OK. Continue the Add Printer Wizard until finished.

f. When finished, go to Start -> Settings -> Printers. The new printer icon will be grayed out indicating the printer is not ready.

g. Right-click the new printer and select Properties. Then select the Details tab, as shown below.



HP LaserJet 5P/5MP PostScript Properties

HP LaserJet 5P/5MP PostScript

Print to the following port: \\123

Print using the following driver: HP LaserJet 5P/5MP PostScript

Timeout settings

Not selected: 15 seconds

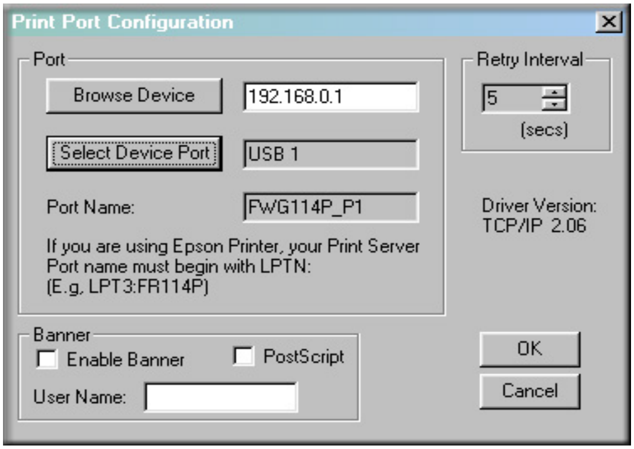
Transmission retry: 45 seconds

Figure 7-3: Windows Printer Properties

h. Click the Add Port button. On the resulting screen, select Other, then select the NETGEAR Print Server Port as the port to add.

i. Click OK to see the Print Port Configuration screen.

j. Click the Browse Device button, select the firewall, and click OK.



Print Port Configuration

Port

192.168.0.1

USB 1

Port Name: FWG114P_P1

If you are using Epson Printer, your Print Server Port name must begin with LPTN: (E.g. LPT3:FR114P)

Retry Interval: 5 (secs)

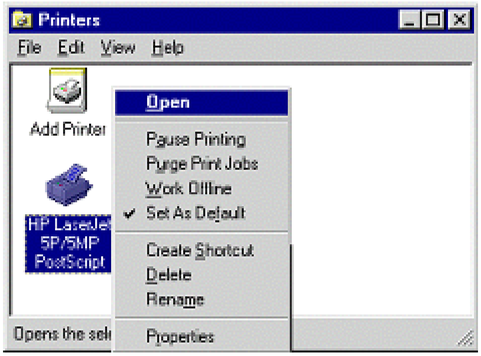
Driver Version: TCP/IP 2.06

Banner

□ Enable Banner □ PostScript

User Name:

k. Click OK to return to the Printers folders, and right-click on the new printer. Make sure that the Work Offline option is NOT checked.



l. From the printer Properties page, General tab, print a test page to confirm that the settings work.

m. The new printer icon should no longer be grayed out, and the printer is ready for use.

Chapter 8
Virtual Private Networking

This chapter describes how to use the virtual private networking (VPN) features of the FWG114P v2 Wireless Firewall/Print Server. VPN tunnels provide secure, encrypted communications between your local network and a remote network or computer. The FWG114P v2 supports 2 VPN tunnels.

Overview of FWG114P v2 Policy-Based VPN Configuration

The FWG114P v2 uses state-of-the-art firewall and security technology to facilitate controlled and actively monitored VPN connectivity. Since the FWG114P v2 strictly conforms to IETF standards, it is interoperable with devices from major network equipment vendors.

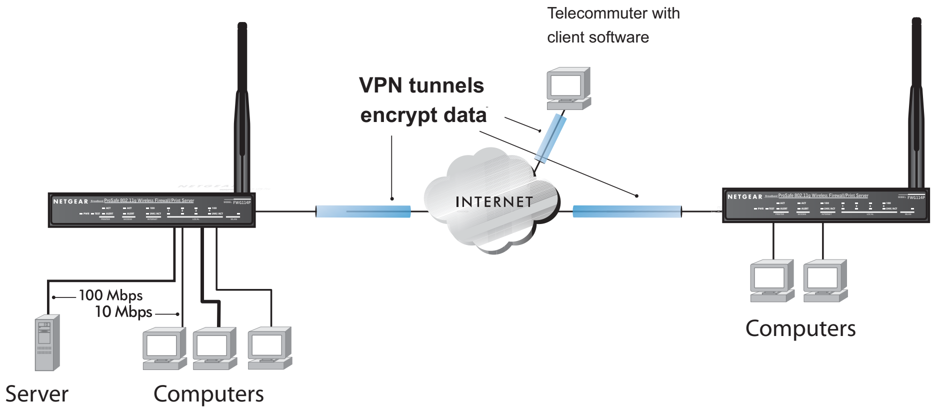


Figure 8-1: Secure access through FWG114P v2 VPN routers

Using Policies to Manage VPN Traffic

You create policy definitions to manage VPN traffic on the FWG114P v2. There are two kinds of policies:

- **IKE Policies**: Define the authentication scheme and automatically generate the encryption keys. As an alternative option, to further automate the process, you can create an IKE policy which uses a trusted certificate authority to provide the authentication while the IKE policy still handles the encryption.
- **VPN Policies**: Apply the IKE policy to specific traffic which requires a VPN tunnel. Or, you can create a VPN policy which does not use an IKE policy but in which you manually enter all the authentication and key parameters.

Since the VPN policies use the IKE policies, you define the IKE policy first. The FWG114P v2 also allows you to manually input the authentication scheme and encryption key values. In the case of manual key management there will not be any IKE policies.

In order to establish secure communication over the Internet with the remote site you need to configure matching VPN policies on both the local and remote FWG114P v2 Wireless Firewall/ Print Servers. The outbound VPN policy on one end must match to the inbound VPN policy on other end, and vice versa.

When the network traffic enters into the FWG114P v2 from the LAN network interface, if there is no VPN policy found for a type of network traffic, then that traffic passes through without any change. However, if the traffic is selected by a VPN policy, then the IPSec authentication and encryption rules will be applied to it as defined in the VPN policy.

By default, a new VPN policy is added with the least priority, that is, at the end of the VPN policy table.

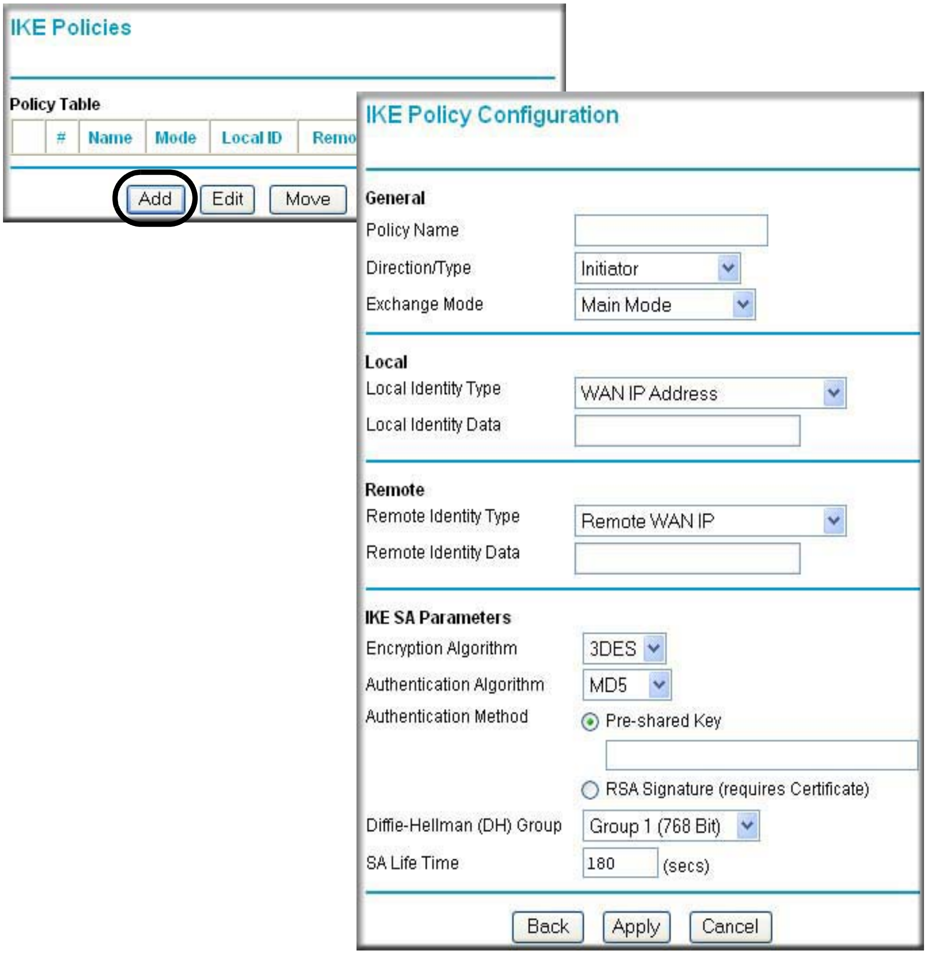
Using Automatic Key Management

The most common configuration scenarios will use IKE policies to automatically manage the authentication and encryption keys. Based on the IKE policy, some parameters for the VPN tunnel are generated automatically. The IKE protocols perform negotiations between the two VPN endpoints to automatically generate required parameters.

Some organizations will use an IKE policy with a Certificate Authority (CA) to perform authentication. Typically, CA authentication is used in large organizations which maintain their own internal CA server. This requires that each VPN gateway has a certificate from the CA. Using CAs reduces the amount of data entry required on each VPN endpoint.

IKE Policies’ Automatic Key and Authentication Management

Click the IKE Policies link from the VPN section of the main menu, and then click the Add button of the IKE Policies screen to display the IKE Policy Configuration menu shown in Figure 8-2.



IKE Policies

Policy Table

	#	Name	Mode	Local ID	Remo

IKE Policy Configuration

General

Policy Name	
Direction/Type	Initiator
Exchange Mode	Main Mode

Local

Local Identity Type	WAN IP Address
Local Identity Data	

Remote

Remote Identity Type	Remote WAN IP
Remote Identity Data	

IKE SA Parameters

Encryption Algorithm	3DES
Authentication Algorithm	MD5
Authentication Method	● Pre-shared Key ○ RSA Signature (requires Certificate)
Diffie-Hellman (DH) Group	Group 1 (768 Bit)
SA Life Time	180 (secs)

Figure 8-2: IKE - Policy Configuration Menu

The IKE Policy Configuration fields are defined in the following table.

Table 8-1. IKE Policy Configuration Fields

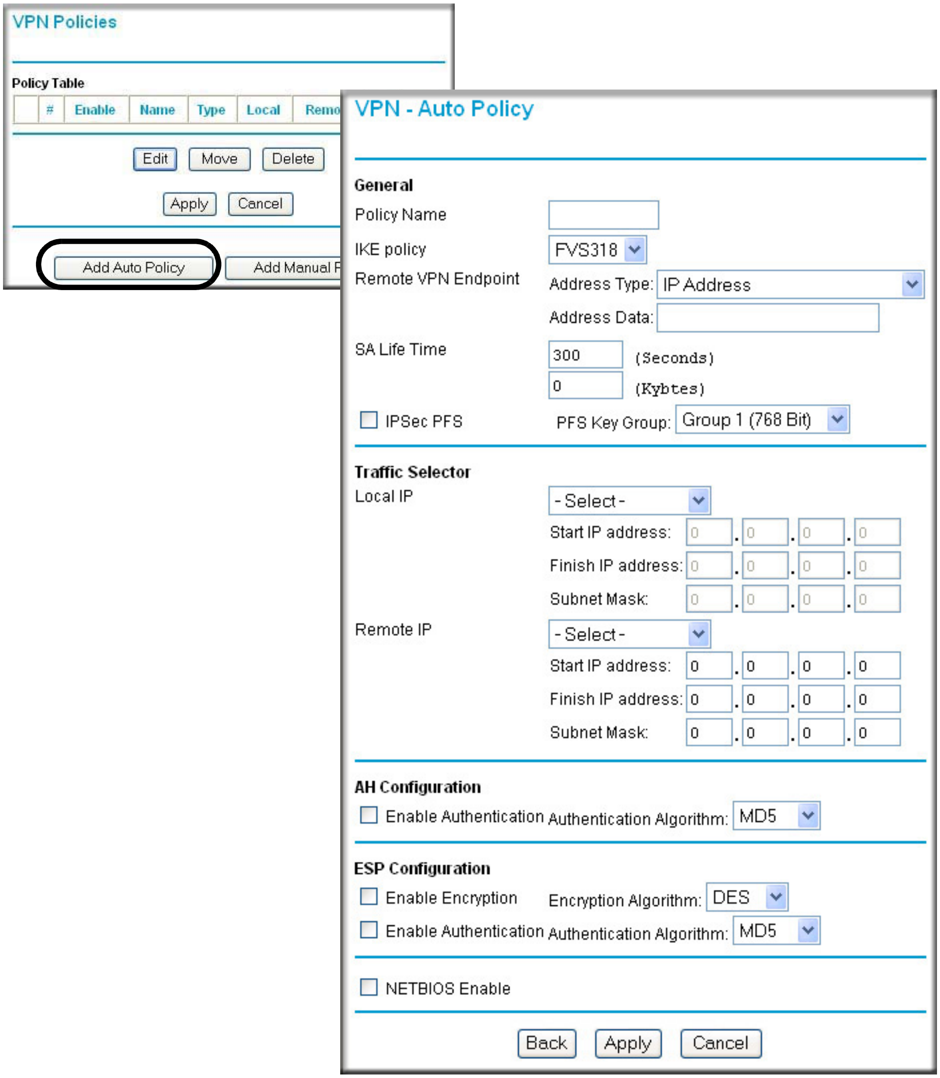
Field	Description
General	These settings identify this policy and determine its major characteristics.
Policy Name	The descriptive name of the IKE policy. Each policy should have a unique policy name. This name is not supplied to the remote VPN endpoint. It is only used to help you identify IKE policies.
Direction/Type	This setting is used when determining if the IKE policy matches the current traffic. The drop-down menu includes the following: • Initiator – Outgoing connections are allowed, but incoming are blocked. • Responder – Incoming connections are allowed, but outgoing are blocked. • Both Directions – Both outgoing and incoming connections are allowed. • Remote Access – This is to allow only incoming client connections, where the IP address of the remote client is unknown. If Remote Access is selected, the “Exchange Mode” MUST be “Aggressive,” and the ‘Identities’ below (both Local and Remote) MUST be “Name.” On the matching VPN Policy, the IP address of the remote VPN endpoint should be set to 0.0.0.0.
Exchange Mode	Main Mode or Aggressive Mode. This setting must match the setting used on the remote VPN endpoint. • Main Mode is slower but more secure. Also, the “Identity” below must be established by IP address. • Aggressive Mode is faster but less secure. The “Identity” below can be by name (host name, domain name, e-mail address, and so on) instead of by IP address.
Local	These parameters apply to the Local FWG114P v2 Wireless Firewall/Print Server.
Local Identity Type	Use this field to identify the local FWG114P v2. You can choose one of the following four options from the drop-down list: • By its Internet (WAN) port IP address. • By its Fully Qualified Domain Name (FQDN) -- your domain name. • By a Fully Qualified User Name -- your name, E-mail address, or other ID. • By DER ASN.1 DN -- the binary DER encoding of your ASN.1 X.500 Distinguished Name.
Local Identity Data	This field lets you identify the local FWG114P v2 by name.

Table 8-1. IKE Policy Configuration Fields

Field	Description
Remote	These parameters apply to the target remote FWG114P v2, VPN gateway, or VPN client.
Remote Identity Type	Use this field to identify the remote FWG114P v2. You can choose one of the following four options from the drop-down list: • By its Internet (WAN) port IP address. • By its Fully Qualified Domain Name (FQDN) — your domain name. • By a Fully Qualified User Name — your name, e-mail address, or other ID. • By DER ASN.1 DN — the binary DER encoding of your ASN.1 X.500 Distinguished Name.
Remote Identity Data	This field lets you identify the target remote FWG114P v2 by name.
IKE SA Parameters	These parameters determine the properties of the IKE Security Association.
Encryption Algorithm	Choose the encryption algorithm for this IKE policy: • DES is the default. • 3DES is more secure.
Authentication Algorithm	If you enable Authentication Header (AH), this menu lets you to select from these authentication algorithms: • MD5 is the default. • SHA-1 is more secure.
Authentication Method	You may select Pre-Shared Key or RSA Signature.
Pre-Shared Key	Specify the key according to the requirements of the Authentication Algorithm you selected. • For MD5, the key length should be 16 bytes. • For SHA-1, the key length should be 20 bytes.
RSA Signature	RSA Signature requires a certificate.
Diffie-Hellman (D-H) Group	The DH Group setting determines the bit size used in the key exchange. This must match the value used on the remote VPN gateway or client.
SA Life Time	The amount of time in seconds before the Security Association expires; over an hour (3600) is common.

VPN Policy Configuration for Auto Key Negotiation

An already defined IKE policy is required for VPN - Auto Policy configuration. From the VPN Policies section of the main menu, you can navigate to the VPN - Auto Policy configuration menu.



VPN Policies

Policy Table

	#	Enable	Name	Type	Local	Remo

VPN - Auto Policy

General

Policy Name:

IKE policy: FVS318

Remote VPN Endpoint: Address Type: IP Address; Address Data:

SA Life Time: 300 (Seconds); 0 (Kybtes)

□ IPSec PFS — PFS Key Group: Group 1 (768 Bit)

Traffic Selector

Local IP: - Select -
Start IP address: 0 . 0 . 0 . 0
Finish IP address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0

Remote IP: - Select -
Start IP address: 0 . 0 . 0 . 0
Finish IP address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0

AH Configuration

□ Enable Authentication — Authentication Algorithm: MD5

ESP Configuration

□ Enable Encryption — Encryption Algorithm: DES

□ Enable Authentication — Authentication Algorithm: MD5

□ NETBIOS Enable

Figure 8-3: VPN - Auto Policy Menu

The VPN Auto Policy fields are defined in the following table.

Table 8-1. VPN Auto Policy Configuration Fields

Field	Description
General	These settings identify this policy and determine its major characteristics.
Policy Name	The descriptive name of the VPN policy. Each policy should have a unique policy name. This name is not supplied to the remote VPN endpoint. It is only used to help you identify VPN policies.
IKE Policy	The existing IKE policies are presented in a drop-down list. **Note:** Create the IKE policy BEFORE creating a VPN - Auto policy.
Remote VPN Endpoint	The address used to locate the remote VPN firewall or client to which you wish to connect. The remote VPN endpoint must have this FWG114P v2's Local IP values entered as its "Remote VPN Endpoint." • By its Fully Qualified Domain Name (FQDN) — your domain name. • By its IP Address.
Address Type	The address type used to locate the remote VPN firewall or client to which you wish to connect. • By its Fully Qualified Domain Name (FQDN) — your domain name. • By its IP Address.
Address Data	The address used to locate the remote VPN firewall or client to which you wish to connect. The remote VPN endpoint must have this FWG114P v2's Local Identity Data entered as its "Remote VPN Endpoint." • By its Fully Qualified Domain Name (FQDN) — your domain name. • By its IP Address.
SA Life Time	The duration of the Security Association before it expires. • Seconds - the amount of time before the SA expires. Over an hour is common (3600). • Kbytes - the amount of traffic before the SA expires. One of these can be set without setting the other.
IPSec PFS	If enabled, security is enhanced by ensuring that the key is changed at regular intervals. Also, even if one key is broken, subsequent keys are no easier to break. Each key has no relationship to the previous key.
PFS Key Group	If PFS is enabled, this setting determines the DH group bit size used in the key exchange. This must match the value used on the remote gateway.

Table 8-1. VPN Auto Policy Configuration Fields

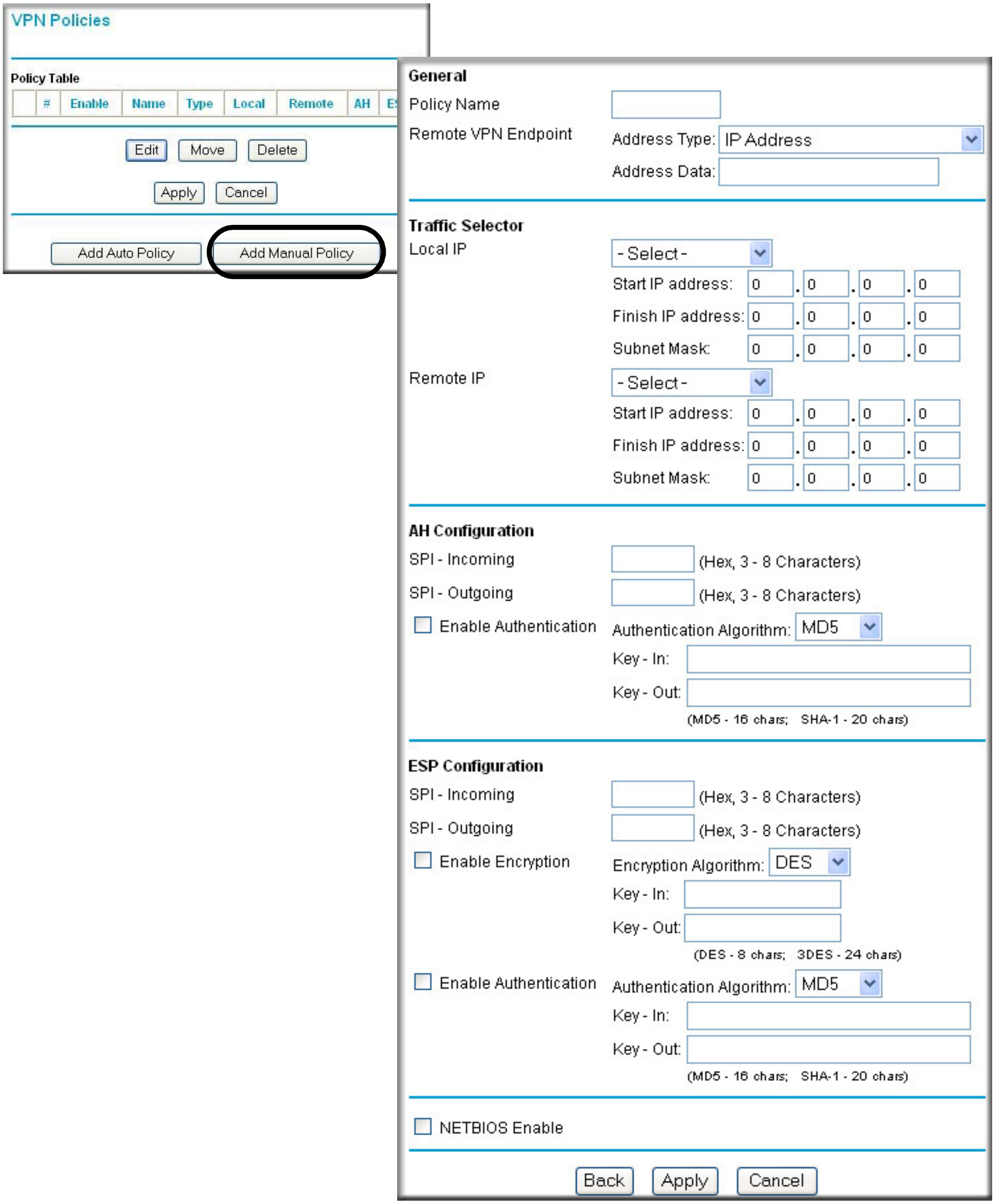
Field	Description
Traffic Selector	These settings determine if and when a VPN tunnel will be established. If network traffic meets *all* criteria, then a VPN tunnel will be created.
Local IP	The drop-down menu allows you to configure the source IP address of the outbound network traffic for which this VPN policy will provide security. Usually, this address will be from your network address space. The choices are: • Default: ANY for all valid IP addresses in the Internet address space **Note:** Selecting ANY means all traffic goes through the IPSec tunnel and prevents access to the Internet. • Single IP Address • Range of IP Addresses • Subnet Address
Remote IP	The drop-down menu allows you to configure the destination IP address of the outbound network traffic for which this VPN policy will provide security. Usually, this address will be from the remote site's corporate network address space. The choices are: • ANY for all valid IP addresses in the Internet address space **Note:** Selecting ANY means all traffic goes through the IPSec tunnel and prevents access to the Internet. • Single IP Address • Range of IP Addresses • Subnet Address
Authenticating Header (AH) Configuration	AH specifies the authentication protocol for the VPN header. These settings must match the remote VPN endpoint.
Enable Authentication	Use this checkbox to enable or disable AH for this VPN policy.
Authentication Algorithm	If you enable AH, then select the authentication algorithm: • MD5 is the default. • SHA1 is more secure.
Encapsulated Security Payload (ESP) Configuration	ESP provides security for the payload (data) sent through the VPN tunnel. Generally, you will want to enable both Encryption and Authentication. Two ESP modes are available: • Plain ESP encryption • ESP encryption with authentication These settings must match the remote VPN endpoint.

Table 8-1. VPN Auto Policy Configuration Fields

Field	Description
Enable Encryption	Use this checkbox to enable or disable ESP Encryption.
Encryption Algorithm	If you enable ESP encryption, then select the encryption algorithm: • DES is the default. • 3DES is more secure.
Enable Authentication	Use this checkbox to enable or disable ESP transform for this VPN policy. You can also select the ESP mode with this menu. Two ESP modes are available: • Plain ESP • ESP with authentication
Authentication Algorithm	If you enable AH, then use this menu to select which authentication algorithm will be employed. The choices are: • MD5 is the default. • SHA1 is more secure.
NETBIOS Enable	Check this if you wish NETBIOS traffic to be forwarded over the VPN tunnel. The NETBIOS protocol is used by Microsoft Networking for such features as Network Neighborhood.

VPN Policy Configuration for Manual Key Exchange

With Manual Key Management, you will not use an IKE policy. You must manually type in all the required key information. Click the VPN Policies link from the VPN section of the main menu to display the menu shown below.



VPN Policies

Policy Table

	#	Enable	Name	Type	Local	Remote	AH	E

Edit | Move | Delete

Apply | Cancel

Add Auto Policy | Add Manual Policy

General

Policy Name

Remote VPN Endpoint — Address Type: IP Address

Address Data:

Traffic Selector

Local IP: - Select -

Start IP address: 0 . 0 . 0 . 0

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Remote IP: - Select -

Start IP address: 0 . 0 . 0 . 0

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

AH Configuration

SPI - Incoming (Hex, 3 - 8 Characters)

SPI - Outgoing (Hex, 3 - 8 Characters)

□ Enable Authentication — Authentication Algorithm: MD5

Key - In:

Key - Out:

(MD5 - 16 chars;   SHA-1 - 20 chars)

ESP Configuration

SPI - Incoming (Hex, 3 - 8 Characters)

SPI - Outgoing (Hex, 3 - 8 Characters)

□ Enable Encryption — Encryption Algorithm: DES

Key - In:

Key - Out:

(DES - 8 chars;   3DES - 24 chars)

□ Enable Authentication — Authentication Algorithm: MD5

Key - In:

Key - Out:

(MD5 - 16 chars;   SHA-1 - 20 chars)

□ NETBIOS Enable

Back | Apply | Cancel

Figure 8-4: VPN - Manual Policy Menu

The VPN Manual Policy fields are defined in the following table.

Table 8-1. VPN Manual Policy Configuration Fields

Field	Description
General	These settings identify this policy and determine its major characteristics.
Policy Name	The name of the VPN policy. Each policy should have a unique policy name. This name is not supplied to the remote VPN Endpoint. It is used to help you identify VPN policies.
Remote VPN Endpoint	The WAN Internet IP address of the remote VPN firewall or client to which you wish to connect. The remote VPN endpoint must have this FWG114P v2's WAN Internet IP address entered as its "Remote VPN Endpoint."
Traffic Selector	These settings determine if and when a VPN tunnel will be established. If network traffic meets *all* criteria, then a VPN tunnel will be created.
Local IP	The drop down menu allows you to configure the source IP address of the outbound network traffic for which this VPN policy will provide security. Usually, this address will be from your network address space. The choices are: • ANY for all valid IP addresses in the Internet address space **Note:** Selecting ANY means all traffic goes through the IPSec tunnel and prevents access to the Internet. • Single IP Address • Range of IP Addresses • Subnet Address
Remote IP	The drop down menu allows you to configure the destination IP address of the outbound network traffic for which this VPN policy will provide security. Usually, this address will be from the remote site's corporate network address space. The choices are: • ANY for all valid IP addresses in the Internet address space **Note:** Selecting ANY means all traffic goes through the IPSec tunnel and prevents access to the Internet. • Single IP Address • Range of IP Addresses • Subnet Address
Authenticating Header (AH) Configuration	AH specifies the authentication protocol for the VPN header. These settings must match the remote VPN endpoint. **Note:** The "Incoming" settings here must match the "Outgoing" settings on the remote VPN endpoint, and the "Outgoing" settings here must match the "Incoming" settings on the remote VPN endpoint.

Table 8-1. VPN Manual Policy Configuration Fields

Field	Description
SPI - Incoming	Enter a Hex value (3 - 8 chars). Any value is acceptable, provided the remote VPN endpoint has the same value in its "Outgoing SPI" field.
SPI - Outgoing	Enter a Hex value (3 - 8 chars). Any value is acceptable, provided the remote VPN endpoint has the same value in its "Incoming SPI" field.
Enable Authentication	Use this checkbox to enable or disable AH. Authentication is often not used. In this case, leave the checkbox unchecked.
Authentication Algorithm	If you enable AH, then select the authentication algorithm: • MD5 is the default. • SHA1 is more secure. Enter the keys in the fields provided. For MD5, the keys should be 16 characters. For SHA-1, the keys should be 20 characters.
Key - In	Enter the keys. • For MD5, the keys should be 16 characters. • For SHA-1, the keys should be 20 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Authentication Algorithm "Key - Out" field.
Key - Out	Enter the keys in the fields provided. • For MD5, the keys should be 16 characters. • For SHA-1, the keys should be 20 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Authentication Algorithm "Key - In" field.
Encapsulated Security Payload (ESP) Configuration	ESP provides security for the payload (data) sent through the VPN tunnel. Generally, you will want to enable both encryption and authentication when you use ESP. Two ESP modes are available: • Plain ESP encryption • ESP encryption with authentication These settings must match the remote VPN endpoint.
SPI - Incoming	Enter a Hex value (3 - 8 chars). Any value is acceptable, provided the remote VPN endpoint has the same value in its "Outgoing SPI" field.
SPI - Outgoing	Enter a Hex value (3 - 8 chars). Any value is acceptable, provided the remote VPN endpoint has the same value in its "Incoming SPI" field.
Enable Encryption	Use this checkbox to enable or disable ESP Encryption.

Table 8-1. VPN Manual Policy Configuration Fields

Field	**Description**
Encryption Algorithm	If you enable ESP Encryption, then select the Encryption Algorithm: • DES is the default. • 3DES is more secure.
Key - In	Enter the key in the fields provided. • For DES, the key should be 8 characters. • For 3DES, the key should be 24 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Encryption Algorithm "Key - Out" field.
Key - Out	Enter the key in the fields provided. • For DES, the key should be 8 characters. • For 3DES, the key should be 24 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Encryption Algorithm "Key - In" field.
Enable Authentication	Use this checkbox to enable or disable ESP authentication for this VPN policy.
Authentication Algorithm	If you enable authentication, then use this menu to select the algorithm: • MD5 is the default. • SHA1 is more secure.
Key - In	Enter the key. • For MD5, the key should be 16 characters. • For SHA-1, the key should be 20 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Authentication Algorithm "Key - Out" field.
Key - Out	Enter the key in the fields provided. • For MD5, the key should be 16 characters. • For SHA-1, the key should be 20 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Authentication Algorithm "Key - In" field.
NETBIOS Enable	Check this if you wish NETBIOS traffic to be forwarded over the VPN tunnel. The NETBIOS protocol is used by Microsoft Networking for such features as Network Neighborhood.

Using Digital Certificates for IKE Auto-Policy Authentication

Digital certificates are strings generated using encryption and authentication schemes which cannot be duplicated by anyone without access to the different values used in the production of the string. They are issued by Certification Authorities (CAs) to authenticate a person or a workstation uniquely. The CAs are authorized to issue these certificates by Policy Certification Authorities (PCAs), who are in turn certified by the Internet Policy Registration Authority (IPRA). The FWG114P v2 is able to use certificates to authenticate users at the end points during the IKE key exchange process.

The certificates can be obtained from a certificate server an organization might maintain internally or from the established public CAs. The certificates are produced by providing the particulars of the user being identified to the CA. The information provided may include the user's name, e-mail ID, domain name, and so on.

Each CA has its own certificate. The certificates of a CA are added to the FWG114P v2 and can then be used to form IKE policies for the user. Once a CA certificate is added to the FWG114P v2 and a certificate is created for a user, the corresponding IKE policy is added to the FWG114P v2. Whenever the user tries to send traffic through the FWG114P v2, the certificates are used in place of pre-shared keys during initial key exchange as the authentication and key generation mechanism. Once the keys are established and the tunnel is set up the connection proceeds according to the VPN policy.

Certificate Revocation List (CRL)

Each Certification Authority (CA) maintains a list of the revoked certificates. The list of these revoked certificates is known as the Certificate Revocation List (CRL).

Whenever an IKE policy receives the certificate from a peer, it checks for this certificate in the CRL on the FWG114P v2 obtained from the corresponding CA. If the certificate is not present in the CRL it means that the certificate is not revoked. IKE can then use this certificate for authentication. If the certificate is present in the CRL it means that the certificate is revoked, and the IKE will not authenticate the client.

You must manually update the FWG114P v2 CRL regularly in order for the CA-based authentication process to remain valid.

Walk-Through of Configuration Scenarios on the FWG114P v2

There are a variety of configurations you might implement with the FWG114P v2. The scenarios listed below illustrate typical configurations you might use in your organization.

In order to help make it easier to set up an IPsec system, the following two scenarios are provided. These scenarios were developed by the VPN Consortium (*http://www.vpnc.org*). The goal is to make it easier to get the systems from different vendors to interoperate. NETGEAR is providing you with both of these scenarios in the following two formats:

- VPN Consortium Scenarios without Any Product Implementation Details as presented in "VPNC Scenario 1: Gateway to Gateway with Preshared Secrets" on page 8-19 and "VPNC Scenario 2: Gateway-to-Gateway with Certificates" on page 8-25.
- VPN Consortium Scenarios Based on the FWG114P v2 User Interface as presented in "Scenario 1: FWG114P v2 to FWG114P v2 with Preshared Secrets" on page 8-20 and "Scenario 2: FWG114P v2 to FWG114P v2 with Certificates" on page 8-26.

The purpose of providing these two versions of the same scenarios is to help you determine where the two vendors use different vocabulary. Seeing the examples presented in these different ways will reveal how systems from different vendors do the same thing.

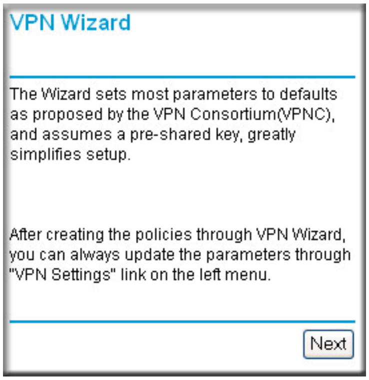
How to Use the VPN Wizard to Configure a VPN Tunnel

➡	**Note:** If you have turned NAT off, before configuring VPN IPSec tunnels you must first open UDP port 500 for inbound traffic as explained in "Example: Port Forwarding for VPN Tunnels when NAT is Off" on page 6-8.

Follow this procedure to configure a VPN tunnel using the VPN Wizard.

Note: The LAN IP address ranges of each VPN endpoint must be different. The connection will fail if both are using the NETGEAR default address range of 192.168.0.x.

1. Log in to the FVS318 on LAN A at its default LAN address of *http://192.168.0.1* with its default user name of **admin** and password of **password**. Click the VPN Wizard link in the main menu to display this screen. Click **Next** to proceed.



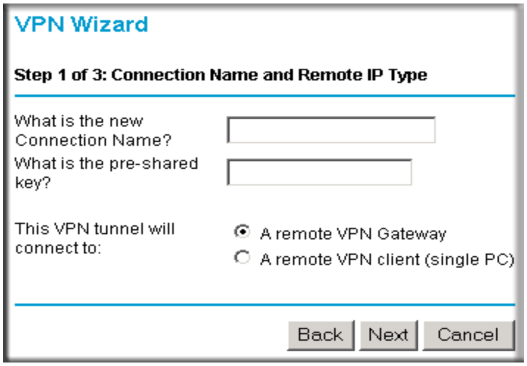
VPN Wizard

The Wizard sets most parameters to defaults as proposed by the VPN Consortium(VPNC), and assumes a pre-shared key, greatly simplifies setup.

After creating the policies through VPN Wizard, you can always update the parameters through "VPN Settings" link on the left menu.

Figure 8-5: VPN Wizard Start Screen

2. Fill in the Connection Name, pre-shared key, and select the type of target end point, and click **Next** to proceed.



VPN Wizard

Step 1 of 3: Connection Name and Remote IP Type

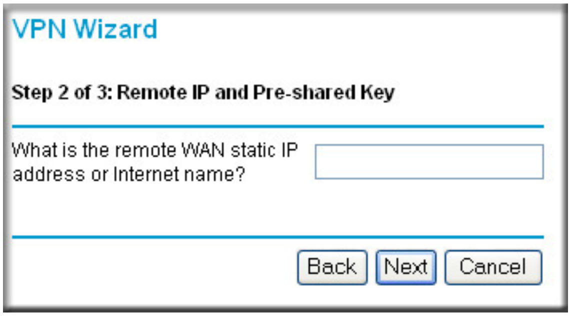
What is the new Connection Name?

What is the pre-shared key?

This VPN tunnel will connect to: ● A remote VPN Gateway ○ A remote VPN client (single PC)

Figure 8-6: Connection Name and Remote IP Type

3. Fill in the IP Address or FQDN for the target VPN endpoint WAN connection and click **Next**.



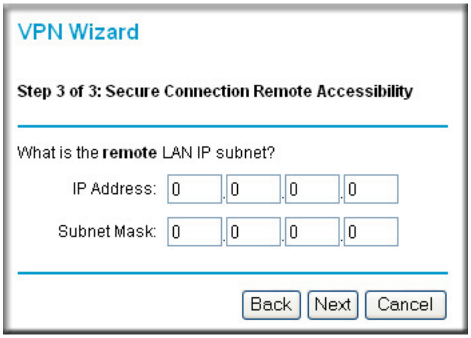
VPN Wizard

Step 2 of 3: Remote IP and Pre-shared Key

What is the remote WAN static IP address or Internet name?

Figure 8-7: Remote IP

4. Identify the IP addresses at the target endpoint which can use this tunnel, and click **Next**.



VPN Wizard

Step 3 of 3: Secure Connection Remote Accessibility

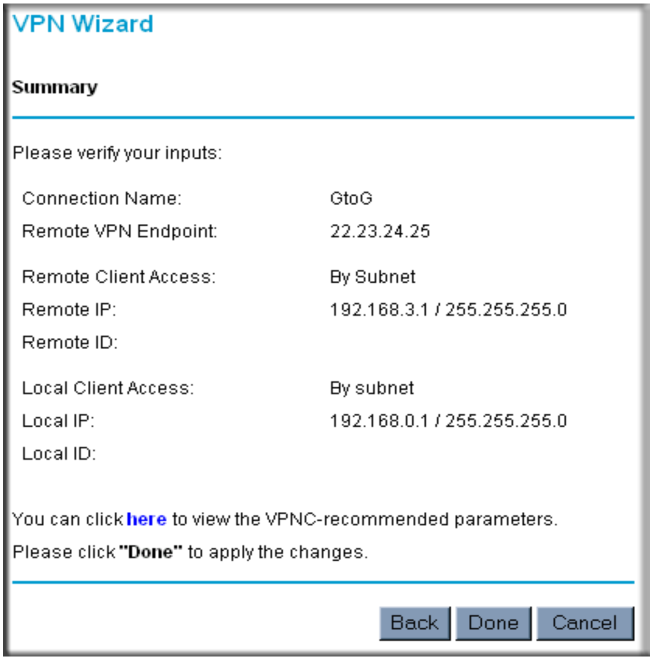
What is the **remote** LAN IP subnet?

IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Figure 8-8: Secure Connection Remote Accessibility

The Summary screen below displays.



VPN Wizard

Summary

Please verify your inputs:

Connection Name:	GtoG
Remote VPN Endpoint:	22.23.24.25
Remote Client Access:	By Subnet
Remote IP:	192.168.3.1 / 255.255.255.0
Remote ID:	
Local Client Access:	By subnet
Local IP:	192.168.0.1 / 255.255.255.0
Local ID:	

You can click **here** to view the VPNC-recommended parameters.

Please click **"Done"** to apply the changes.

Figure 8-9: VPN Wizard Summary

To view the VPNC recommended authentication and encryption Phase 1 and Phase 2 settings the VPN Wizard used, click the "**here**" link.

5. Click **Done** to complete the configuration procedure. The VPN Settings menu displays showing that the new tunnel is enabled

   To view or modify the tunnel settings, select the radio button next to the tunnel entry and click Edit.

VPNC Scenario 1: Gateway to Gateway with Preshared Secrets

The following is a typical gateway-to-gateway VPN that uses a preshared secret for authentication.

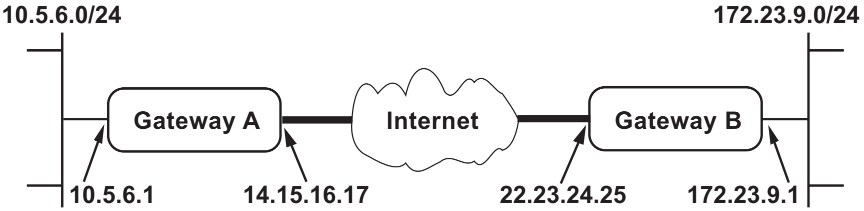


Figure 8-10: VPN Consortium Scenario 1

Gateway A connects the internal LAN 10.5.6.0/24 to the Internet. Gateway A's LAN interface has the address 10.5.6.1, and its WAN (Internet) interface has the address 14.15.16.17.

Gateway B connects the internal LAN 172.23.9.0/24 to the Internet. Gateway B's WAN (Internet) interface has the address 22.23.24.25. Gateway B's LAN interface address, 172.23.9.1, can be used for testing IPsec but is not needed for configuring Gateway A.

The IKE Phase 1 parameters used in Scenario 1 are:

- Main mode
- TripleDES
- SHA-1
- MODP group 2 (1024 bits)
- pre-shared secret of "hr5xb84l6aa9r6"
- SA lifetime of 28800 seconds (eight hours) with no kbytes rekeying

The IKE Phase 2 parameters used in Scenario 1 are:

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying
- Selectors for all IP protocols, all ports, between 10.5.6.0/24 and 172.23.9.0/24, using IPv4 subnets

Scenario 1: FWG114P v2 to FWG114P v2 with Preshared Secrets

Note: This scenario assumes all ports are open on the FWG114P v2. You can verify this by reviewing the security settings as seen in the "Rules menu" on page 6-5.

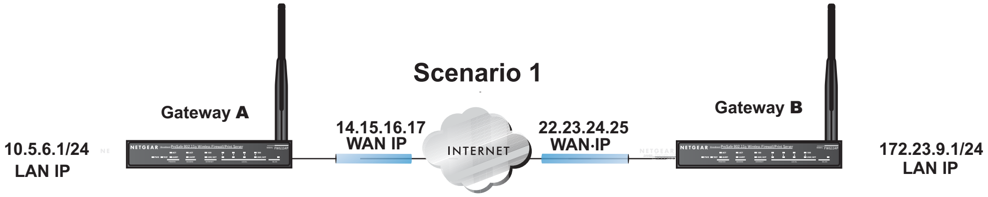


Figure 8-11: LAN to LAN VPN access from an FWG114P v2 to an FWG114P v2

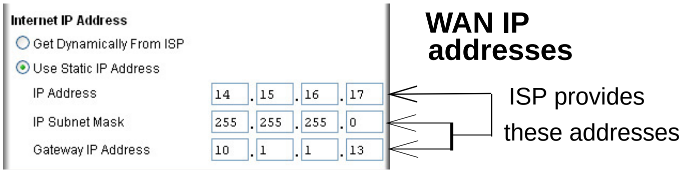
Use this scenario illustration and configuration screens as a model to build your configuration.

1. **Log in to the FWG114P v2 labeled Gateway A as in the illustration.**

   Log in at the default address of *http://192.168.0.1* with the default user name of **admin** and default password of **password**, or using whatever password and LAN address you have chosen.

2. **Configure the WAN (Internet) and LAN IP addresses of the FWG114P v2.**

   a. From the main menu Setup section, click on the Basic Setup link.



Internet IP Address

○ Get Dynamically From ISP

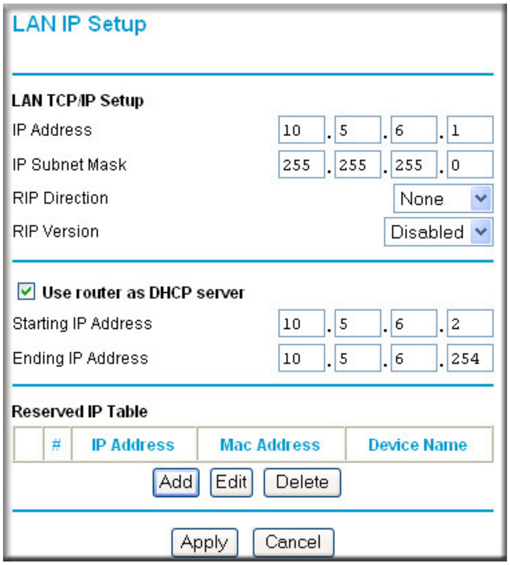
● Use Static IP Address

IP Address	14 . 15 . 16 . 17
IP Subnet Mask	255 . 255 . 255 . 0
Gateway IP Address	10 . 1 . 1 . 13

Figure 8-12: FWG114P v2 Internet IP Address menu

   b. Configure the WAN Internet Address according to the settings above and click Apply to save your settings. For more information on configuring the WAN IP settings in the Basic Setup topics, please see "Manually Configuring Your Internet Connection" on page 3-18.

c. From the main menu Advanced section, click on the LAN IP Setup link.



LAN IP Setup

LAN TCP/IP Setup

IP Address	10 . 5 . 6 . 1
IP Subnet Mask	255 . 255 . 255 . 0
RIP Direction	None
RIP Version	Disabled

☑ Use router as DHCP server

Starting IP Address	10 . 5 . 6 . 2
Ending IP Address	10 . 5 . 6 . 254

Reserved IP Table

	#	IP Address	Mac Address	Device Name

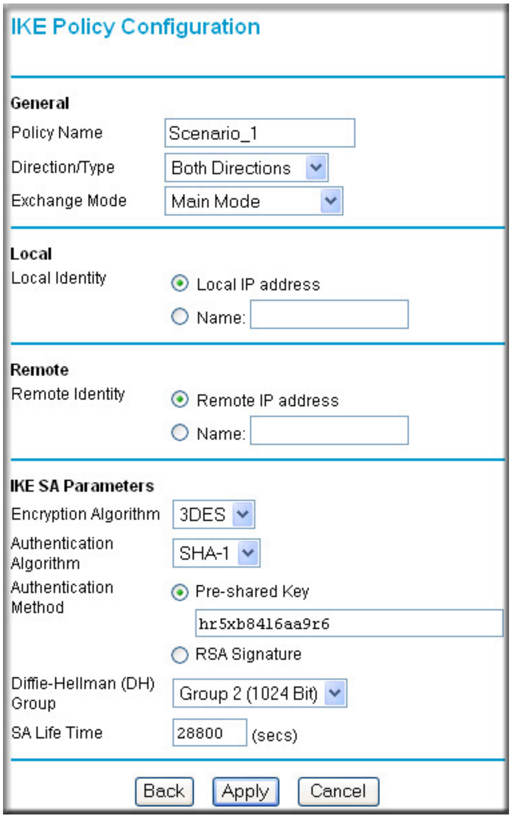
Figure 8-13: LAN IP configuration menu

d. Configure the LAN IP address according to the settings above and click Apply to save your settings. For more information on LAN TCP/IP setup topics, please see "Using the LAN IP Setup Options" on page 10-5.

Note: After you click Apply to change the LAN IP address settings, your workstation will be disconnected from the FWG114P v2. You will have to log on with *http://10.5.6.1*, which is now the address you use to connect to the built-in web-based configuration manager of the FWG114P v2.

3. Set up the IKE Policy illustrated below on the FWG114P v2.

a. From the main menu VPN section, click on the IKE Policies link, and then click the Add button to display the screen below.



IKE Policy Configuration

General

Policy Name: Scenario_1

Direction/Type: Both Directions

Exchange Mode: Main Mode

Local

Local Identity: ● Local IP address ○ Name:

Remote

Remote Identity: ● Remote IP address ○ Name:

IKE SA Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

Authentication Method: ● Pre-shared Key hr5xb8416aa9r6 ○ RSA Signature

Diffie-Hellman (DH) Group: Group 2 (1024 Bit)

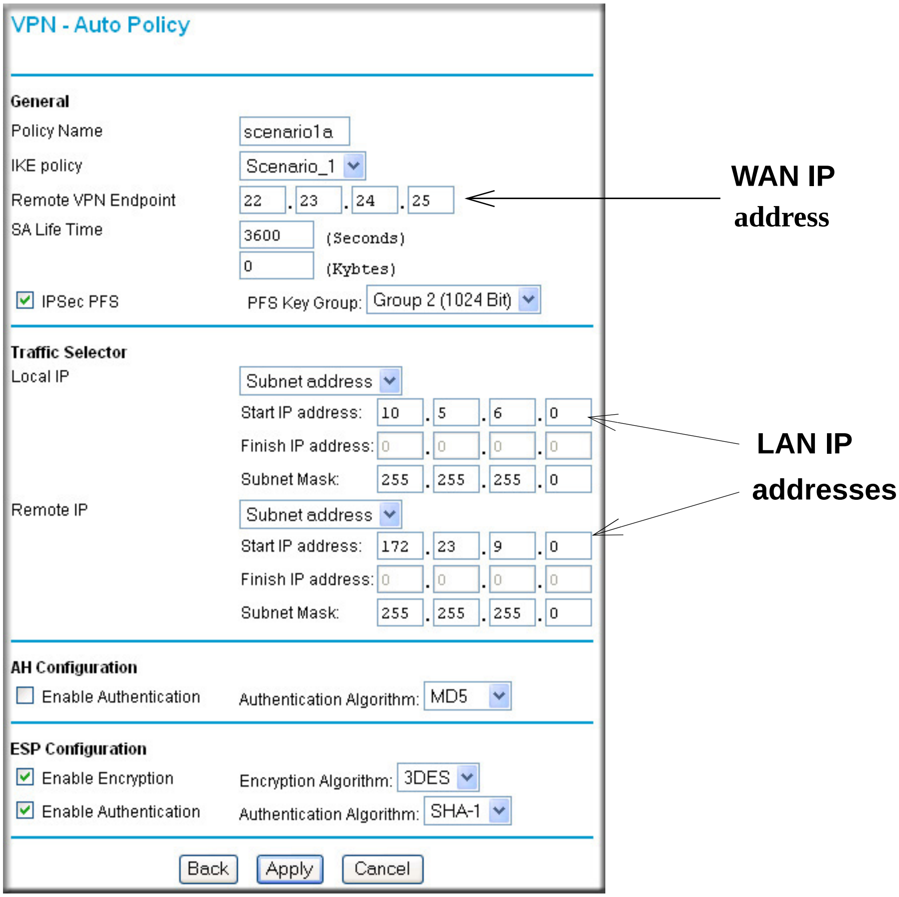
SA Life Time: 28800 (secs)

Figure 8-14: Scenario 1 IKE Policy

b. Configure the IKE Policy according to the settings in the illustration above and click Apply to save your settings. For more information on IKE Policy topics, please see “IKE Policies’ Automatic Key and Authentication Management” on page 8-3.

4. **Set up the FWG114P v2 VPN -Auto Policy illustrated below.**

   a. From the main menu VPN section, click on the VPN Policies link, and then click on the Add Auto Policy button.



VPN - Auto Policy

General

Policy Name: scenario1a

IKE policy: Scenario_1

Remote VPN Endpoint: 22 . 23 . 24 . 25

SA Life Time: 3600 (Seconds)

0 (Kybtes)

☑ IPSec PFS — PFS Key Group: Group 2 (1024 Bit)

Traffic Selector

Local IP: Subnet address

Start IP address: 10 . 5 . 6 . 0

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Remote IP: Subnet address

Start IP address: 172 . 23 . 9 . 0

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

AH Configuration

☐ Enable Authentication — Authentication Algorithm: MD5

ESP Configuration

☑ Enable Encryption — Encryption Algorithm: 3DES

☑ Enable Authentication — Authentication Algorithm: SHA-1

Figure 8-15: Scenario 1 VPN - Auto Policy

   b. Configure the IKE Policy according to the settings in the illustration above and click Apply to save your settings. For more information on IKE Policy topics, please see "IKE Policies' Automatic Key and Authentication Management" on page 8-3.
   Note: Selecting ANY for the Traffic Selectors means all traffic goes through the IPSec tunnel and prevents access to the Internet.

5. After applying these changes, all traffic from the range of LAN IP addresses specified on FWG114P v2 A and FWG114P v2 B will flow over a secure VPN tunnel.

How to Check VPN Connections

You can test connectivity and view VPN status information on the FWG114P v2.

1. To test connectivity between the Gateway A FWG114P v2 LAN and the Gateway B LAN, follow these steps:
   a. Using our example, from a PC attached to the FWG114P v2 on LAN A, on a Windows PC click the Start button on the taskbar and then click Run.
   b. Enter **`ping -t 172.23.9.1`**, and then click OK.
   c. This will cause a continuous ping to be sent to the LAN interface of Gateway B. After between several seconds and two minutes, the ping response should change from “timed out” to “reply.”
   d. At this point the connection is established.
2. To test connectivity between the FWG114P v2 Gateway A and Gateway B WAN ports, follow these steps:
   a. Using our example, log in to the FWG114P v2 on LAN A, go to the main menu Maintenance section and click the Diagnostics link.
   b. To test connectivity to the WAN port of Gateway B, enter **`22.23.24.25`**, and then click Ping.
   c. This will cause a ping to be sent to the WAN interface of Gateway B. After between several seconds and two minutes, the ping response should change from “timed out” to “reply.” You may have to run this test several times before you get the “reply” message back from the target FWG114P v2.
   d. At this point the connection is established.

   Note: If you want to ping the FWG114P v2 as a test of network connectivity, be sure the FWG114P v2 is configured to respond to a ping on the Internet WAN port by checking the checkbox seen in “Rules menu” on page 6-5. However, to preserve a high degree of security, you should turn off this feature when you are finished with testing.
3. To view the FWG114P v2 event log and status of Security Associations, follow these steps:
   a. Go to the FWG114P v2 main menu VPN section and click the VPN Status link.
   b. The log screen will display a history of the VPN connections, and the IPSec SA and IKE SA tables will report the status and data transmission statistics of the VPN tunnels for each policy.

VPNC Scenario 2: Gateway-to-Gateway with Certificates

The following is a typical gateway-to-gateway VPN that uses PKIX certificates for authentication.

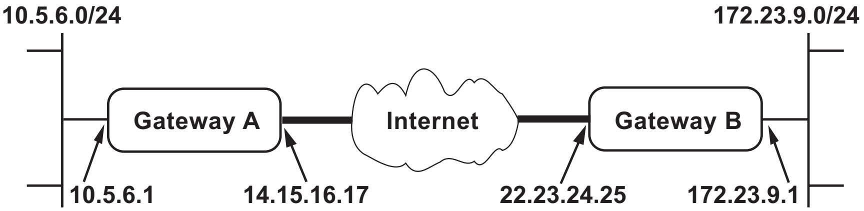


Figure 8-16: VPN Consortium Scenario 2

Gateway A connects the internal LAN 10.5.6.0/24 to the Internet. Gateway A's LAN interface has the address 10.5.6.1, and its WAN (Internet) interface has the address 14.15.16.17.

Gateway B connects the internal LAN 172.23.9.0/24 to the Internet. Gateway B's WAN (Internet) interface has the address 22.23.24.25. Gateway B's LAN interface address, 172.23.9.1, can be used for testing IPsec but is not needed for configuring Gateway A.

The **IKE Phase 1 parameters** used in Scenario 2 are:

- Main mode
- TripleDES
- SHA-1
- MODP group 2 (1024 bits)
- Authentication with signatures authenticated by PKIX certificates; both Gateway A and Gateway B have end-entity certificates that chain to a root authority called "Trusted Root CA."
- SA lifetime of 28800 seconds (eight hours) with no kbytes rekeying

The **IKE Phase 2 parameters** used in Scenario 2 are:

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying

- Selectors for all IP protocols, all ports, between 10.5.6.0/24 and 172.23.9.0/24, using IPv4 subnets

Scenario 2: FWG114P v2 to FWG114P v2 with Certificates

The following is a typical gateway-to-gateway VPN that uses Public Key Infrastructure x.509 (PKIX) certificates for authentication. The network setup is identical to the one given in scenario 1. The IKE Phase 1 and Phase 2 parameters are identical to the ones given in scenario 1, with the exception that the identification is done with signatures authenticated by PKIX certificates.

Note: Before completing this configuration scenario, make sure the correct Time Zone is set on the FWG114P v2. For instructions on this topic, please see, “Setting the Time Zone” on page 6-13.

1. **Obtain a root certificate.**
   a. Obtain the root certificate (which includes the public key) from a Certificate Authority (CA)

      Note: The procedure for obtaining certificates differs from a CA like Verisign and a CA, such as a Windows 2000 certificate server, which an organization operates for providing certificates for its members. For example, an administrator of a Windows 2000 certificate server might provide it to you via e-mail.

   b. Save the certificate as a text file called *trust.txt*.
2. **Install the trusted CA certificate for the Trusted Root CA.**
   a. Log in to the FWG114P v2.

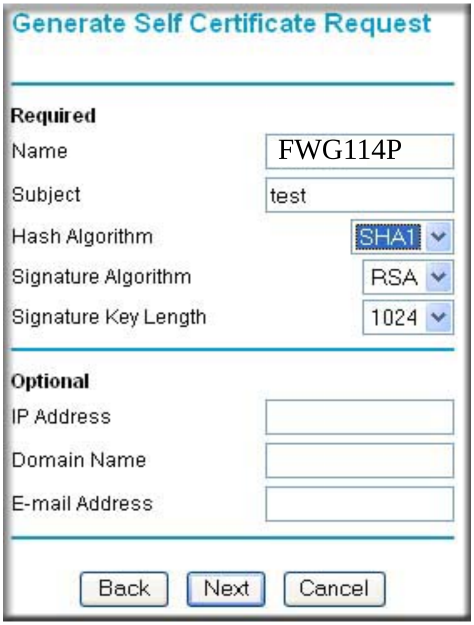
   b. From the main menu VPN section, click on the CA’s link.

   c. Click Add to add a CA.

   d. Click Browse to locate the *trust.txt* file.

   e. Click Upload.
3. **Create a certificate request for the FWG114P v2.**
   a. From the main menu VPN section, click the Certificates link.

b. Click the Generate Request button to display the screen illustrated in Figure 8-17 below.



Generate Self Certificate Request

Required

Name	FWG114P
Subject	test
Hash Algorithm	SHA1
Signature Algorithm	RSA
Signature Key Length	1024

Optional

IP Address	
Domain Name	
E-mail Address	

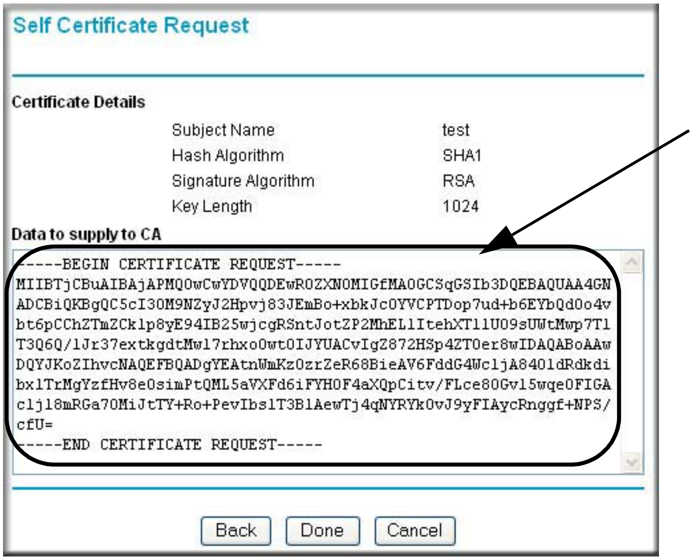
Figure 8-17: Generate Self Certificate Request menu

c. Fill in the fields on the Add Self Certificate screen.

- Required
  - Name. Enter a name to identify this certificate.
  - Subject. This is the name which other organizations will see as the holder (owner) of this certificate. This should be your registered business name or official company name. Generally, all certificates should have the same value in the Subject field.
  - Hash Algorithm. Select the desired option: MD5 or SHA1.
  - Signature Algorithm. Select the desired option: DSS or RSA.
  - Signature Key Length. Select the desired option: 512, 1024, or 2048.
- Optional
  - IP Address. If you use “IP type” in the IKE policy, you should input the IP Address here. Otherwise, you should leave this blank.
  - Domain Name. If you have a domain name, you can enter it here. Otherwise, you should leave this blank.

– E-mail Address. You can enter your e-mail address here.

d. Click the Next button to continue. The FWG114P v2 generates a Self Certificate Request as shown below.



Self Certificate Request

Certificate Details

Subject Name	test
Hash Algorithm	SHA1
Signature Algorithm	RSA
Key Length	1024

Data to supply to CA

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBTjCBuAIBAjAPMQ0wCwYDVQQDEwR0ZXN0MIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQC5cI30M9NZyJ2Hpvj83JEmBo+xbkJc0YVCPTDop7ud+b6EYbQd0o4v
bt6pCChZTmZCk1p8yE94IB25wjcgRSntJotZP2MhEL1ItehXT11U09sUWtMwp7T1
T3Q6Q/1Jr37extkgdtMw17rhxo0wt0IJYUACvIgZ872HSp4ZT0er8wIDAQABoAAw
DQYJKoZIhvcNAQEFBQADgYEAtnWmKz0zrZeR68BieAV6FddG4Wc1jA8401dRdkdi
bx1TrMgYzfHv8e0simPtQML5aVXFd6iFYH0F4aXQpCitv/FLce80Gv15wqe0FIGA
c1j18mRGa70MiJtTY+Ro+PevIbs1T3B1AewTj4qNYRYk0vJ9yFIAycRnggf+NPS/
cfU=
-----END CERTIFICATE REQUEST-----
```

Highlight, copy and paste this data into a text file.

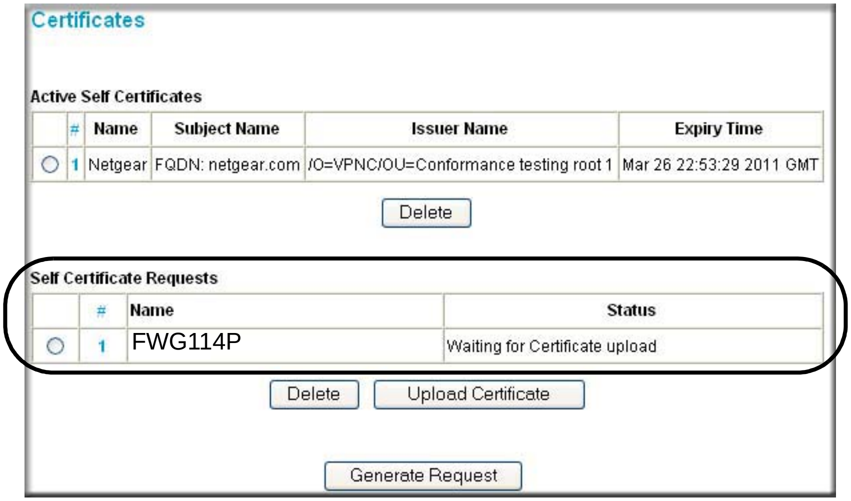
Figure 8-18: Self Certificate Request data

4. Transmit the Self Certificate Request data to the Trusted Root CA.

a. Highlight the text in the Data to supply to CA area, copy it, and paste it into a text file.

b. Give the certificate request data to the CA. In the case of a Windows 2000 internal CA, you might simply e-mail it to the CA administrator. The procedures of a CA like Verisign and a CA, such as a Windows 2000 certificate server administrator will differ. Follow the procedures of your CA.

c. When you have finished gathering the Self Certificate Request data, click the Done button. You will return to the Certificates screen where your pending "FWG114P v2" Self Certificate Request will be listed, as illustrated in Figure 8-19 below.



Certificates

Active Self Certificates

	#	Name	Subject Name	Issuer Name	Expiry Time
○	1	Netgear	FQDN: netgear.com	/O=VPNC/OU=Conformance testing root 1	Mar 26 22:53:29 2011 GMT

Self Certificate Requests

	#	Name	Status
○	1	FWG114P	Waiting for Certificate upload

Figure 8-19: Self Certificate Requests table

5. **Receive the certificate back from the Trusted Root CA and save it as a text file.**

   Note: In the case of a Windows 2000 internal CA, the CA administrator might simply e-mail it to back to you. Follow the procedures of your CA. Save the certificate you get back from the CA as a text file called *final.txt*.

6. **Upload the new certificate.**

   a. From the main menu VPN section, click on the Certificates link.

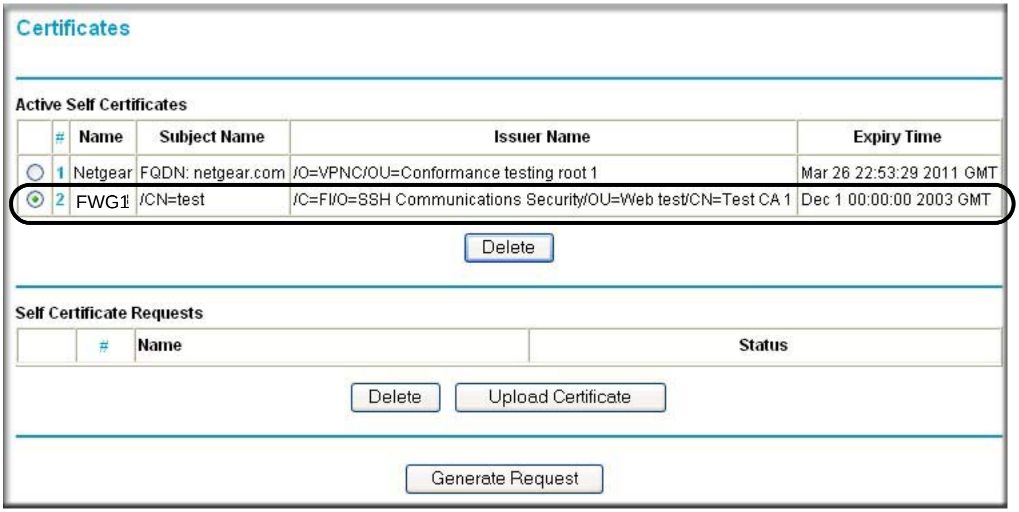
   b. Click the radio button of the Self Certificate Request you want to upload.

   c. Click the Upload Certificate button.

   d. Browse to the location of the file you saved in step 5 above which contains the certificate from the CA.

   e. Click the Upload button.

f. You will now see the "FWG114P v2" entry in the Active Self Certificates table and the pending "FWG114P v2" Self Certificate Request is gone, as illustrated below.



Certificates

Active Self Certificates

	#	Name	Subject Name	Issuer Name	Expiry Time
○	1	Netgear	FQDN: netgear.com	/O=VPNC/OU=Conformance testing root 1	Mar 26 22:53:29 2011 GMT
●	2	FWG1	/CN=test	/C=FI/O=SSH Communications Security/OU=Web test/CN=Test CA 1	Dec 1 00:00:00 2003 GMT

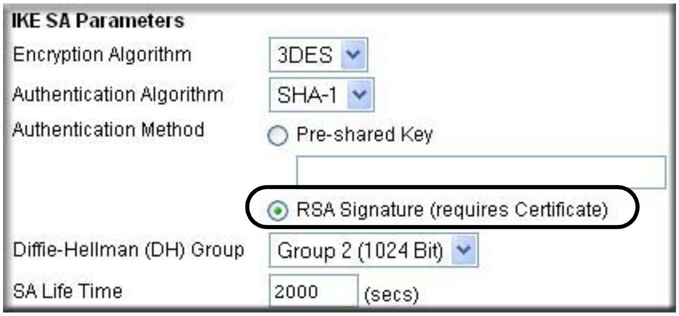
Self Certificate Requests

	#	Name	Status

Figure 8-20: Self Certificates table

7. Associate the new certificate and the Trusted Root CA certificate on the FWG114P v2.

a. Create a new IKE policy called **Scenario_2** with all the same properties of **Scenario_1** (see "Scenario 1 IKE Policy" on page 8-22) except now use the RSA Signature instead of the shared key.



IKE SA Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

Authentication Method: ○ Pre-shared Key

● RSA Signature (requires Certificate)

Diffie-Hellman (DH) Group: Group 2 (1024 Bit)

SA Life Time: 2000 (secs)

Figure 8-21: IKE policy using RSA Signature

b. Create a new VPN Auto Policy called **scenario2a** with all the same properties as **scenario1a** except that it uses the IKE policy called Scenario_2.

Now, the traffic from devices within the range of the LAN subnet addresses on FWG114P v2 A and Gateway B will be authenticated using the certificates rather than via a shared key.

8. **Set up Certificate Revocation List (CRL) checking.**
   a. Get a copy of the CRL from the CA and save it as a text file.

      Note: The procedure for obtaining a CRL differs from a CA like Verisign and a CA, such as a Windows 2000 certificate server, which an organization operates for providing certificates for its members. Follow the procedures of your CA.

   b. From the main menu VPN section, click on the CRL link.

   c. Click Add to add a CRL.

   d. Click Browse to locate the CRL file.

   e. Click Upload.

   Now expired or revoked certificates will not be allowed to use the VPN tunnels managed by IKE policies which use this CA.

   Note: You must update the CRLs regularly in order to maintain the validity of the certificate-based VPN policies.

Netgear VPN Client to FWG114P v2

Follow these procedures to configure a VPN tunnel from a NETGEAR ProSafe VPN Client to an FWG114P v2. This case study follows the Virtual Private Network Consortium (VPNC) interoperability profile guidelines. The menu options for the FVS328, FVL328, FWAG114, and FWG114P v2 are the same.

Configuration Profile

The configuration in this document follows the addressing and configuration mechanics defined by the VPN Consortium. Gather all the necessary information before you begin the configuration process. Verify whether the firmware is up to date, all of the addresses that will be necessary, and all of the parameters that need to be set on both sides. Check that there are no firewall restrictions.

Table 8-1. Summary

VPN Consortium Scenario:		Scenario 1
Type of VPN		PC/Client-to-Gateway
Security Scheme:		IKE with Preshared Secret/Key (not Certificate-based)
Date Tested:		December 2003
Model/Firmware Tested:		
	Gateway	FWG114P firmware v 2.2
	Client	NETGEAR ProSafe VPN Client v10.1
IP Addressing:		
	Gateway	Static IP address
	Client	Dynamic

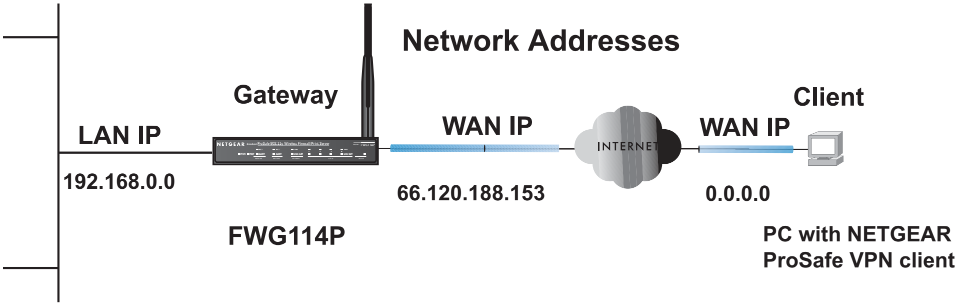


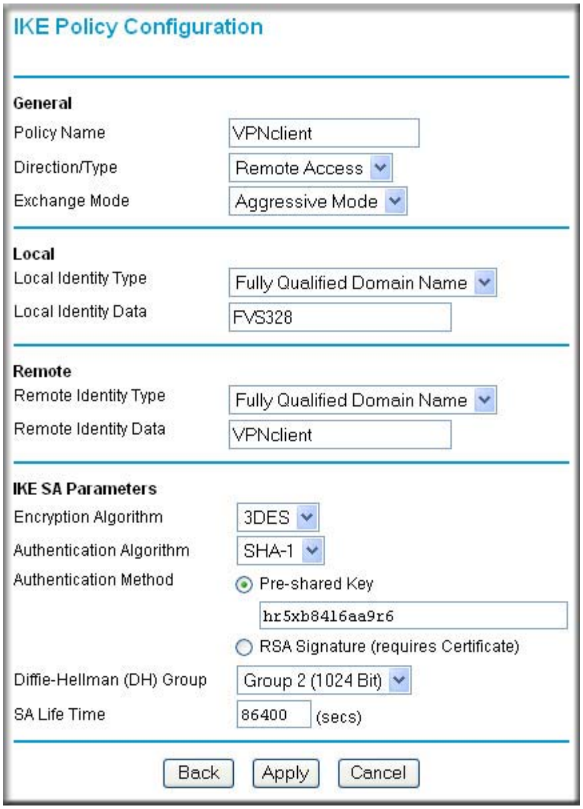
Figure 8-22: Addressing and Subnet Used for Examples

Step-By-Step Configuration of FWG114P v2 Gateway

1. Log in to the FWG114P v2 gateway as in the illustration.

   Out of the box, the FWG114P v2 is set for its default LAN address of *http://192.168.0.1,* with its default user name of **admin** and default password of **password**.

2. Click **IKE Policies** under the VPN menu and click **Add** on the IKE Policies Menu.



IKE Policy Configuration

General

Policy Name	VPNclient
Direction/Type	Remote Access
Exchange Mode	Aggressive Mode

Local

Local Identity Type	Fully Qualified Domain Name
Local Identity Data	FVS328

Remote

Remote Identity Type	Fully Qualified Domain Name
Remote Identity Data	VPNclient

IKE SA Parameters

Encryption Algorithm	3DES
Authentication Algorithm	SHA-1
Authentication Method	● Pre-shared Key hr5xb8416aa9r6 ○ RSA Signature (requires Certificate)
Diffie-Hellman (DH) Group	Group 2 (1024 Bit)
SA Life Time	86400 (secs)

Figure 8-23: NETGEAR FWG114P v2 IKE Policy Configuration

– Enter a descriptive name for the policy in the Policy Name field. This name is not supplied to the remote VPN endpoint. It is used to help you manage the IKE policies. In our example, we used **VPNclient** as the Policy Name.

– From the Direction/Type drop-down box, select **Remote Access**.

– From the Exchange Mode drop-down box, select **Aggressive Mode**. This will also be selected in the VPN Client My Identity ID Type fields, as seen in “Security Policy” on page 8-41.

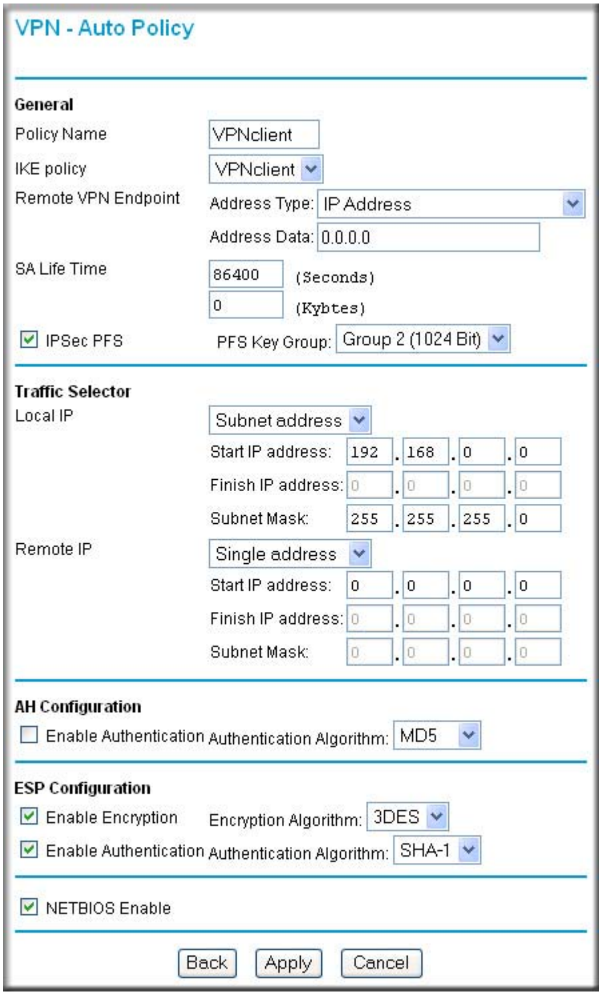
– From the Local Identity drop-down box, select **Fully Qualified Domain Name** (the actual WAN IP address of the FWG114P v2 will also be used in the Connection ID Type fields of the VPN Client as seen in “Security Policy Editor New Connection” on page 8-39).

– For this example we typed **FWG114P v2** in the Local Identity Data field.

- From the Remote Identity drop-down box, select **Fully Qualified Domain Name**.
- Type **VPNclient** in the Remote Identity Data. This will also be entered in the VPN Client My Identity ID Type fields, as seen in "My Identity" on page 8-40.
- From the Encryption Algorithm drop-down box, select **3DES**. This will also be selected in the VPN Client Security Policy Authentication Phase 1 Proposal 1 Encrypt Alg field, as seen in "Connection Security Policy Authentication (Phase 1)" on page 8-42.
- From the Authentication Algorithm drop-down box, select **SHA-1**.This will also be selected in the VPN Client Security Policy Authentication Phase 1 Proposal 1 Hash Alg field, as seen in "Connection Security Policy Authentication (Phase 1)" on page 8-42.
- From the Authentication Method radio button, select **Pre-shared Key**. This will also be selected in the VPN Client Security Policy Authentication Phase 1 Proposal 1 Authentication Method field, as seen in "Connection Security Policy Authentication (Phase 1)" on page 8-42.
- In the Pre-Shared Key field, type **hr5xb84l6aa9r6**. You must make sure the key is the same for both the client and the FWG114P v2 Wireless Firewall/Print Server. This will also be selected in the VPN client Security Policy Authentication Phase 1 Proposal 1 Encrypt Alg field, as seen in "Connection Identity Pre-Shared Key" on page 8-41.
- From the Diffie-Hellman (DH) Group drop-down box, select **Group 2 (1024 Bit)**. This will also be selected in the VPN Client Security Policy Authentication Phase 1 Proposal 1 Key Group field, as seen in "Connection Security Policy Authentication (Phase 1)" on page 8-42.
- In the SA Life Time field, type **86400**.

Click **Apply**. This will bring you back to the IKE Policies Menu.The FWG114P v2 IKE Policy is now displayed in the IKE Policies page.

3. Click the **VPN Policies** link under the VPN category on the left side of the main menu. This will take you to the VPN Policies Menu page. Click **Add Auto Policy**. This will open a new screen titled VPN – Auto Policy.



VPN - Auto Policy

General

Policy Name: VPNclient

IKE policy: VPNclient

Remote VPN Endpoint: Address Type: IP Address; Address Data: 0.0.0.0

SA Life Time: 86400 (Seconds); 0 (Kybtes)

☑ IPSec PFS — PFS Key Group: Group 2 (1024 Bit)

Traffic Selector

Local IP: Subnet address
- Start IP address: 192.168.0.0
- Finish IP address: 0.0.0.0
- Subnet Mask: 255.255.255.0

Remote IP: Single address
- Start IP address: 0.0.0.0
- Finish IP address: 0.0.0.0
- Subnet Mask: 0.0.0.0

AH Configuration

☐ Enable Authentication — Authentication Algorithm: MD5

ESP Configuration

☑ Enable Encryption — Encryption Algorithm: 3DES

☑ Enable Authentication — Authentication Algorithm: SHA-1

☑ NETBIOS Enable

Figure 8-24: VPN – Auto Policy settings

- – Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. In our example, we use **VPNclient** as the Policy Name.
- – From the IKE policy drop-down box, select **VPNclient** which is the IKE Policy that was set up in the earlier step.

- From the Remote VPN Endpoint Address Type drop-down box, select **IP Address**.
- Type **0.0.0.0** as the Address Data of the client because we are assuming the remote PC will have a dynamically assigned IP address. This will also be entered in the VPN Client Internal Network IP Address field, as seen in "My Identity" on page 8-40.
- Type **86400** in the SA Life Time (Seconds) field.
- Type **0** in the SA Life Time (Kbytes) field.
- Check the **IPSec PFS** check box to enable Perfect Forward Secrecy. This will also be entered in the VPN Client Security Policy Enable Perfect Forward Secrecy check box, as seen in "Security Policy" on page 8-41.
- From the PFS Key Group drop-down box, select **Group 2 (1024 Bit)**. This will also be entered in the VPN Client Security Policy PFS Key Group drop-down selection box, as seen in "Security Policy" on page 8-41.
- From the Traffic Selector Local IP drop-down box, select **Subnet addresses**. This will also be entered in the VPN Client Connection Remote Party Identity and Addressing ID Type field, as seen in "Security Policy Editor New Connection" on page 8-39.
  Note: Selecting ANY for the Traffic Selectors means all traffic goes through the IPSec tunnel and prevents access to the Internet.
- Type the starting LAN IP Address of the FWG114P v2 in the Local IP Start IP Address field. For this example, we used **192.168.0.0** which is the default LAN IP address of the FWG114P v2**.** This will also be entered in the VPN Client Connection Remote Party Identity and Addressing Subnet field, as seen in "Security Policy Editor New Connection" on page 8-39.
- Type the LAN Subnet Mask of the FWG114P v2 (**255.255.255.0** in our example) in the Local IP Subnet Mask field. This will also be entered in the VPN Client Connection Remote Party Identity and Addressing Mask field, as seen in "Security Policy Editor New Connection" on page 8-39.
- From the Traffic Selector Remote IP drop-down box, select **Single addresses**.
- Type **0.0.0.0** as the start IP Address of the in the Remote IP Start IP Address field because we are assuming the remote PC will have a dynamically assigned IP address. This will also be entered in the VPN Client My Identity Internal Network IP Address field, as seen in "My Identity" on page 8-40.
- Select the **Enable Encryption** check box. This will also be selected in the VPN Client Security Policy Key Exchange (Phase 2) Encapsulation Protocol (ESP) check box, as seen in "Connection Security Policy Key Exchange (Phase 2)" on page 8-43.
- From the ESP Configuration Encryption Algorithm drop-down box, select **3DES**. This will also be entered in the VPN Client Security Policy Key Exchange (Phase 2) Encrypt Alg field, as seen in "Connection Security Policy Key Exchange (Phase 2)" on page 8-43.

- Select **Enable Authentication** in the ESP Configuration Enable Authentication check box.
  Note: Do not confuse this with the Authentication Protocol (AH) option. Using the AH option will prevent clients behind a home NAT router from connecting.
- From the ESP Configuration Authentication Algorithm drop-down box, select **SHA-1**. This will also be entered in the VPN Client Security Policy Key Exchange (Phase 2) Hash Alg field, as seen in "Connection Security Policy Key Exchange (Phase 2)" on page 8-43.
- Select the **NETBIOS Enable** check box to enable networking features like Windows Network Neighborhood.

Click **Apply** to save your changes. You will be taken back to the VPN Policies Menu page.

4. When the screen returns to the VPN Policies, make sure the Enable check box is selected. Click **Apply** to save your changes.

Step-By-Step Configuration of the Netgear VPN Client

➡	**Note:** The Netgear ProSafe VPN Client has the ability to "Import" a predefined configuration profile. The FWG114P v2.SPD file on the ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2 *Resource CD for the ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P (SW-10023-03)* includes all the settings identified in this procedure. Whenever importing policy settings, you should first export any existing settings you may have configured to prevent the new imported settings from replacing an existing working configuration. To import this policy, use the Security Policy Editor File menu to select Import Policy, and select the FWG114P v2.SPD file at D:\Software\Policies where D is the drive letter of your CD-ROM drive.

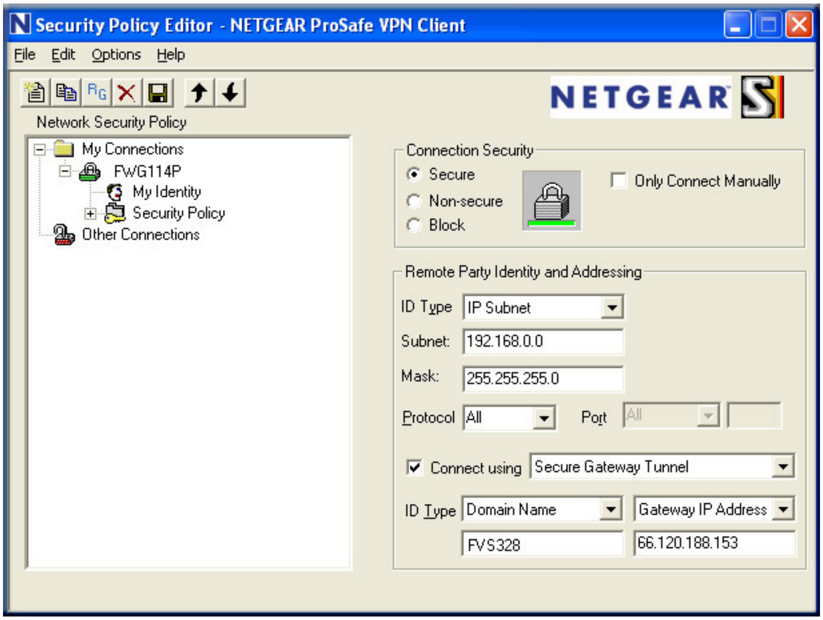
This procedure describes linking a remote PC and a LAN. The LAN will connect to the Internet using an FWG114P v2 with a static IP address. The PC can be directly connected to the Internet through dialup, cable or DSL modem, or other means, and we will assume it has a dynamically assigned IP address.

1. Install the Netgear VPN Client Software on the PC.

➡	**Note:** Before installing the Netgear VPN Client software, be sure to turn off any virus protection or firewall software you may be running on your PC.

- You may need to insert your Windows CD to complete the installation.
- Reboot your PC after installing the client software.

2. Configure the Connection Network Settings.



Connection Security
● Secure
○ Non-secure
○ Block
□ Only Connect Manually

Remote Party Identity and Addressing
ID Type: IP Subnet
Subnet: 192.168.0.0
Mask: 255.255.255.0
Protocol: All   Port: All
☑ Connect using: Secure Gateway Tunnel
ID Type: Domain Name   Gateway IP Address
FVS328   66.120.188.153

Figure 8-25: Security Policy Editor New Connection

a. Run the Security Policy Editor program and create a VPN Connection.

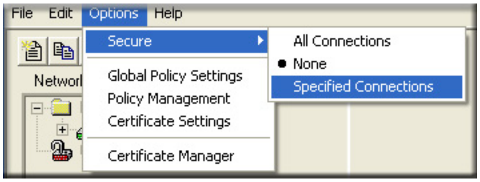


Figure 8-26: Security Policy Editor Options menu

Note: If the configuration settings on this screen are not available for editing, go to the Options menu, select Secure, and Specified Options to enable editing these settings.

From the Edit menu of the Security Policy Editor, click **Add**, then **Connection**. A “New Connection” listing appears. Rename the “New Connection” to **FWG114P v2**.

b. Ensure that the following settings are configured:

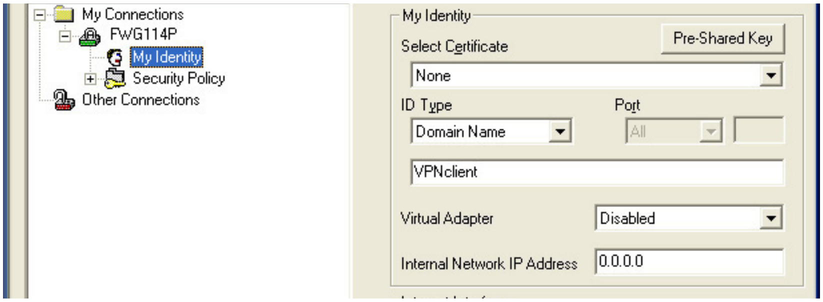
– In the Connection Security box, Secure is selected.
– In the Protocol menu, All is selected.
– The Connect using Secure Gateway Tunnel check box is selected.

c. In this example, select IP Subnet as the ID Type, **192.168.0.0** in the Subnet field (the Subnet address is the LAN IP Address of the FWG114P v2 with 0 as the last number), and **255.255.255.0** in the Mask field, which is the LAN Subnet Mask of the FWG114P v2.

d. In the ID Type menus, select **Domain Name** and **Gateway IP Address**. Enter **FWG114P v2** in the Domain Name field. In this example, **66.120.188.153** would be used for the Gateway IP Address, which is the static IP address for the FWG114P v2 WAN port.

3. Configure the Connection Identity Settings.

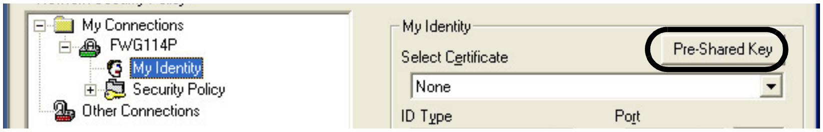
a. In the Network Security Policy list, click the My Identity subheading.



Select Certificate: None
ID Type: Domain Name
VPNclient
Virtual Adapter: Disabled
Internal Network IP Address: 0.0.0.0

Figure 8-27: My Identity

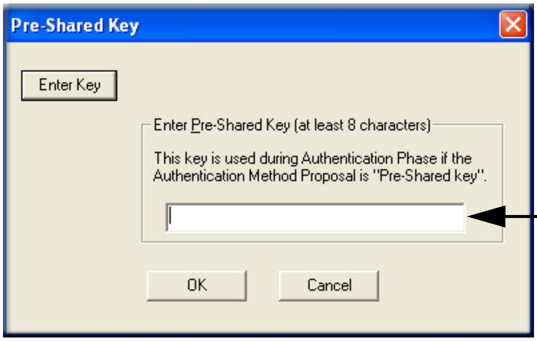
In this example, select Domain Name as the ID Type, and enter **VPNclient**. Also, accept the default Internal Network IP Address of 0.0.0.0.



Select Certificate: None

Figure 8-28: My Identity Pre-Shared Key

b. Click **Pre-Shared Key**.



Pre-Shared Key

Enter Key

Enter Pre-Shared Key (at least 8 characters)

This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".

In this example, enter this pre-shared key in this field: **hr5xb84l6aa9r6**

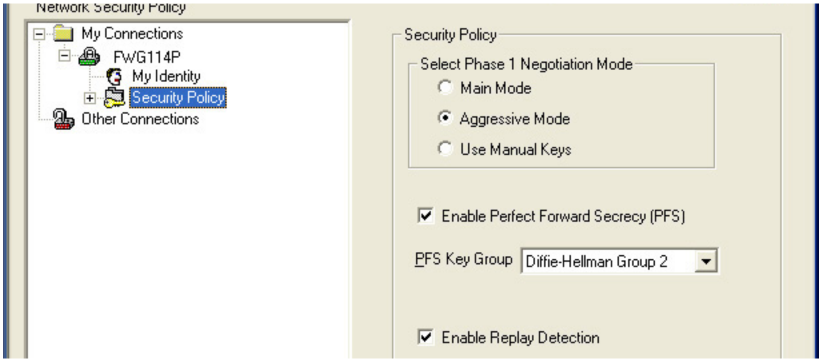
Figure 8-29: Connection Identity Pre-Shared Key

c. Enter **hr5xb84l6aa9r6,** which is the same Pre-Shared Key entered in the FWG114P v2.

d. Click **OK**.

4. Configure the Connection Identity Settings.

a. In the Network Security Policy list, click the Security Policy subheading.



Network Security Policy

Security Policy

Select Phase 1 Negotiation Mode

○ Main Mode

● Aggressive Mode

○ Use Manual Keys

☑ Enable Perfect Forward Secrecy (PFS)

PFS Key Group: Diffie-Hellman Group 2

☑ Enable Replay Detection

Figure 8-30: Security Policy

b. For this example, ensure that the following settings are configured:

– In the Select Phase 1 Negotiation Mode menu, select **Aggressive Mode**.

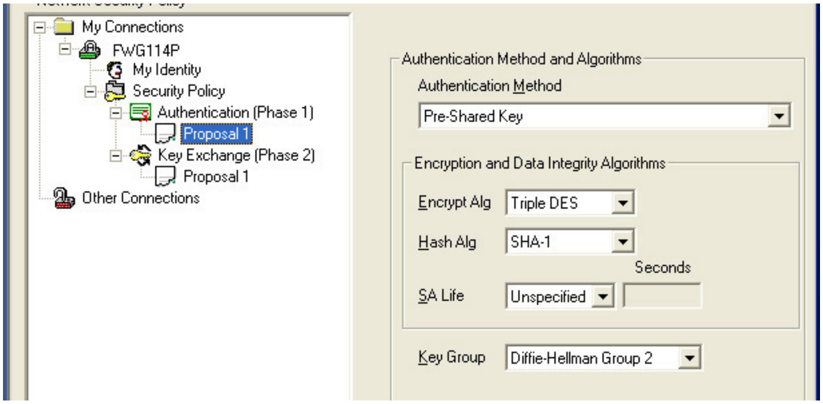
– Select the **Enable Perfect Forward Secrecy (PFS)** check box.

– In the PFS Key Group drop-down list, **Diffie-Hellman Group 2**.

– Select the Enable Replay Detection check box.

5. **Configure the Connection Security Policy**

In this step, you will provide the authentication (IKE Phase 1) settings, and the key exchange (Phase 2) settings. The setting choices in this procedure follow the VPNC guidelines.



Authentication Method and Algorithms

Authentication Method: Pre-Shared Key

Encryption and Data Integrity Algorithms

Encrypt Alg: Triple DES

Hash Alg: SHA-1

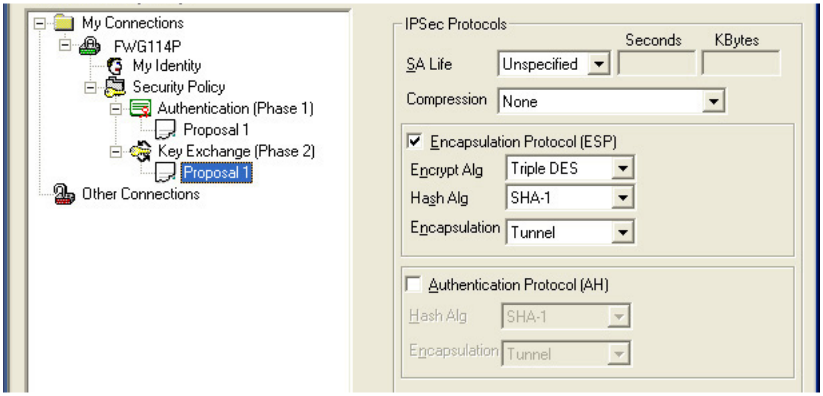
SA Life: Unspecified Seconds

Key Group: Diffie-Hellman Group 2

Figure 8-31: Connection Security Policy Authentication (Phase 1)

a. Configure the Authentication (Phase 1) Settings.

- Expand the Security Policy heading, then expand the Authentication (Phase 1) heading, and click on Proposal 1.
- For this example, ensure that the following settings are configured:
  - In the Encrypt Alg menu, select **Triple DES**.
  - In the Hash Alg, select **SHA-1**.
  - In the SA Life, select Unspecified.
  - In the Key Group menu, select **Diffie-Hellman Group 2**.



SA Life: Unspecified

Compression: None

☑ Encapsulation Protocol (ESP)

Encrypt Alg: Triple DES

Hash Alg: SHA-1

Encapsulation: Tunnel

☐ Authentication Protocol (AH)

Hash Alg: SHA-1

Encapsulation: Tunnel

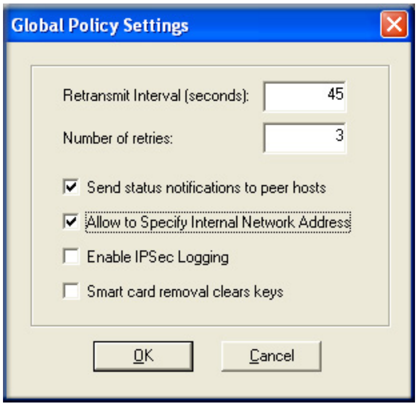
Figure 8-32: Connection Security Policy Key Exchange (Phase 2)

b. Configure the Key Exchange (Phase 2).

- Expand the Key Exchange (Phase 2) heading, and click on Proposal 1.
- For this example, ensure that the following settings are configured:
  - In the SA Life menu, select **Unspecified**.
  - In the Compression menu, select **None**.
  - Check the **Encapsulation Protocol (ESP)** check box.
  - In the Encrypt Alg menu, select **Triple DES**.
  - In the Hash Alg, select **SHA-1**.
  - In the Encapsulation menu, select **Tunnel**.

6. **Configure the Global Policy Settings.**

   a. From the Options menu at the top of the Security Policy Editor window, select **Global Policy Settings**.



Global Policy Settings

Retransmit Interval (seconds): 45

Number of retries: 3

☑ Send status notifications to peer hosts

☑ Allow to Specify Internal Network Address

☐ Enable IPSec Logging

☐ Smart card removal clears keys

Figure 8-33: Security Policy Editor Global Policy Options

   b. Increase the Retransmit Interval period to **45** seconds.

   c. Select the Allow to Specify Internal Network Address check box and click **OK**.

7. **Save the VPN Client Settings.**

   From the File menu at the top of the Security Policy Editor window, select Save.

   After you have configured and saved the VPN client information, your PC will automatically open the VPN connection when you attempt to access any IP addresses in the range of the remote VPN router’s LAN.

➡	**Note:** Whenever you make changes to a Security Policy, save them first, then deactivate the security policy, reload the security policy, and finally activate the security policy. This ensures that your new settings will take effect.

Testing the VPN Connection

You can test the VPN connection in several ways:

- From the client PC to the FWG114P v2
- From the FWG114P v2 to the client PC

These procedures are explained below.

⇨	**Note:** Virus protection or firewall software can interfere with VPN communications. Be sure such software is not running on the remote PC with the Netgear ProSafe VPN Client and that the firewall features of the FWG114P v2 are not set in such a way as to prevent VPN communications.

From the Client PC to the FWG114P v2

To check the VPN Connection, you can initiate a request from the remote PC to the FWG114P v2 by using the “Connect” option of the FWG114P v2 Wireless Firewall/Print Server popup menu.

1. Open the popup menu by right-clicking on the system tray icon.
2. Select **Connect** to open the My Connections list.
3. Choose **FWG114P v2**.

   The FWG114P v2 Wireless Firewall/Print Server will report the results of the attempt to connect.

Once the connection is established, you can access resources of the network connected to the FWG114P v2.

Another method is to ping from the remote PC to the LAN IP address of the FWG114P v2. To perform a ping test using our example, start from the remote PC:

1. Establish an Internet connection from the PC.
2. On the Windows taskbar, click the Start button, and then click Run.
3. Type **`ping -t 192.168.0.1`** and click OK.

   This will cause a continuous ping to be sent to the first FWG114P v2. After a period of up to two minutes, the ping response should change from “timed out” to “reply.”

To test the connection to a computer connected to the FWG114P v2, simply ping the IP address of that computer.

Once connected, you can open a browser on the remote PC and enter the LAN IP Address of the FWG114P v2, which is http://192.168.0.1 in this example. After a short wait, you should see the login screen of the FWG114P v2.

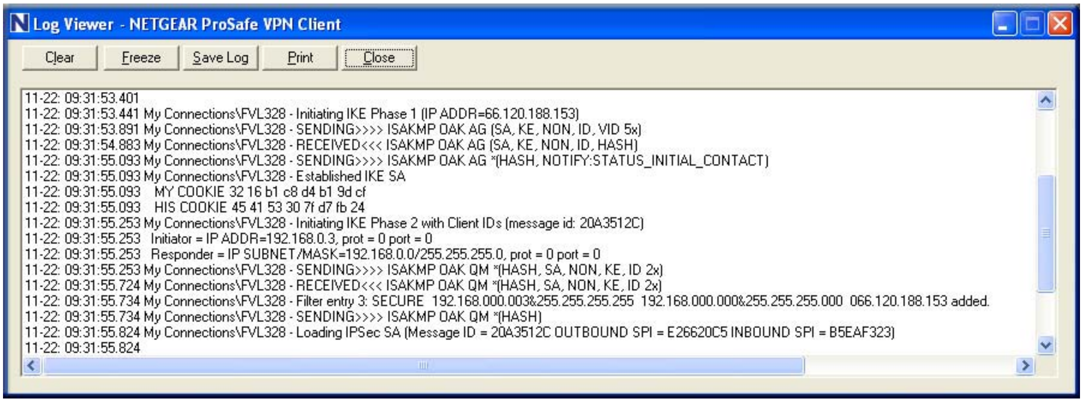
From the FWG114P v2 to the Client PC

You can use the FWG114P v2 Diagnostic utilities to test the VPN connection from the FWG114P v2 to the client PC. Run ping tests from the Diagnostics link of the FWG114P v2 main menu.

Monitoring the PC VPN Connection

Information on the progress and status of the VPN client connection can be viewed by opening the Netgear ProSafe VPN Client Connection Monitor or Log Viewer. To launch these functions, click on the Windows Start button, then select Programs, then Netgear ProSafe VPN Client, then either the Connection Monitor or Log Viewer.

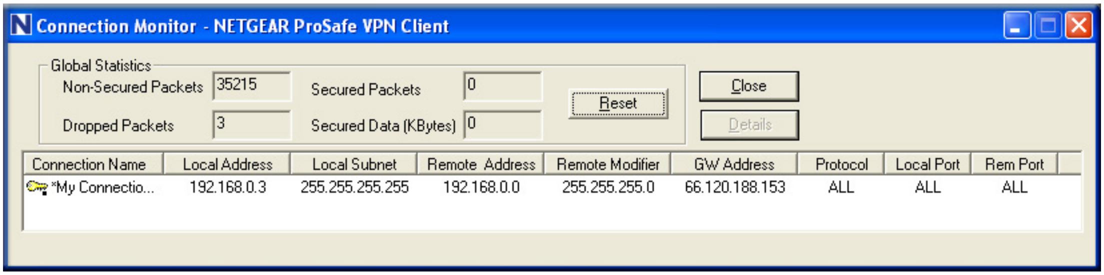
The Log Viewer screen for a successful connection is similar to the one shown below:



```
11-22: 09:31:53.401
11-22: 09:31:53.441 My Connections\FVL328 - Initiating IKE Phase 1 (IP ADDR=66.120.188.153)
11-22: 09:31:53.891 My Connections\FVL328 - SENDING>>>> ISAKMP OAK AG (SA, KE, NON, ID, VID 5x)
11-22: 09:31:54.883 My Connections\FVL328 - RECEIVED<<< ISAKMP OAK AG (SA, KE, NON, ID, HASH)
11-22: 09:31:55.093 My Connections\FVL328 - SENDING>>>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT)
11-22: 09:31:55.093 My Connections\FVL328 - Established IKE SA
11-22: 09:31:55.093    MY COOKIE 32 16 b1 c8 d4 b1 9d cf
11-22: 09:31:55.093    HIS COOKIE 45 41 53 30 7f d7 fb 24
11-22: 09:31:55.253 My Connections\FVL328 - Initiating IKE Phase 2 with Client IDs (message id: 20A3512C)
11-22: 09:31:55.253   Initiator = IP ADDR=192.168.0.3, prot = 0 port = 0
11-22: 09:31:55.253   Responder = IP SUBNET/MASK=192.168.0.0/255.255.255.0, prot = 0 port = 0
11-22: 09:31:55.253 My Connections\FVL328 - SENDING>>>> ISAKMP OAK QM *(HASH, SA, NON, KE, ID 2x)
11-22: 09:31:55.724 My Connections\FVL328 - RECEIVED<<< ISAKMP OAK QM *(HASH, SA, NON, KE, ID 2x)
11-22: 09:31:55.734 My Connections\FVL328 - Filter entry 3: SECURE  192.168.000.003&255.255.255.255  192.168.000.000&255.255.255.000  066.120.188.153 added.
11-22: 09:31:55.734 My Connections\FVL328 - SENDING>>>> ISAKMP OAK QM *(HASH)
11-22: 09:31:55.824 My Connections\FVL328 - Loading IPSec SA (Message ID = 20A3512C OUTBOUND SPI = E26620C5 INBOUND SPI = B5EAF323)
11-22: 09:31:55.824
```

Figure 8-34: Log Viewer screen

A sample Connection Monitor screen for a different connection is shown below:



Connection Monitor - NETGEAR ProSafe VPN Client

Global Statistics

Non-Secured Packets 35215
Secured Packets 0
Dropped Packets 3
Secured Data (KBytes) 0

Connection Name	Local Address	Local Subnet	Remote Address	Remote Modifier	GW Address	Protocol	Local Port	Rem Port
*My Connectio...	192.168.0.3	255.255.255.255	192.168.0.0	255.255.255.0	66.120.188.153	ALL	ALL	ALL

Figure 8-35: Connection Monitor screen

In this example the following connection options apply:

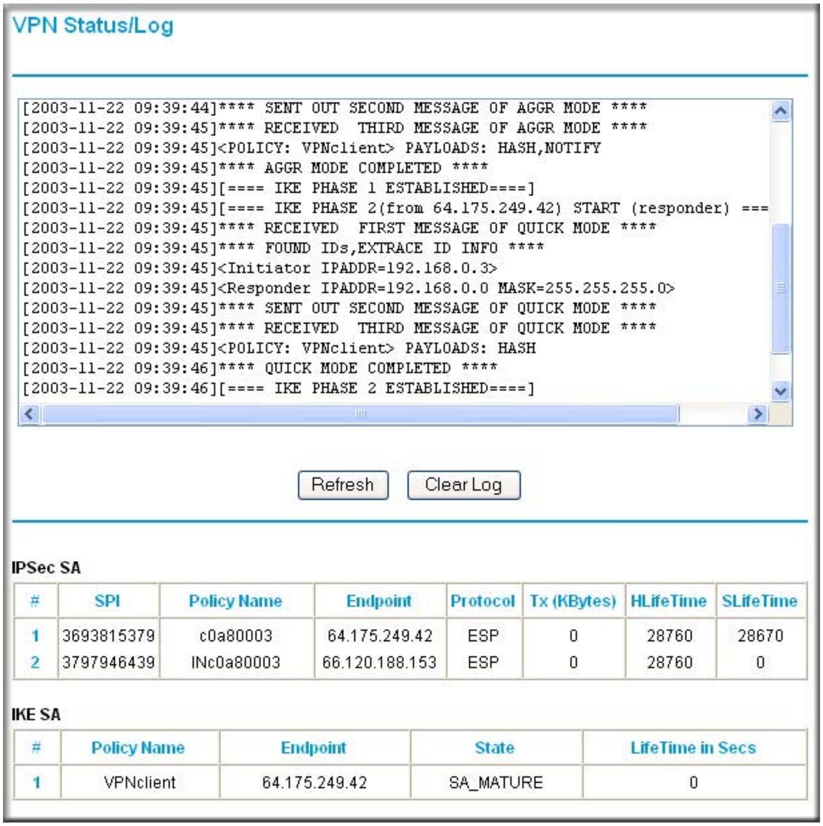
- The FWG114P v2 has a public IP WAN address of 66.120.188.153
- The FWG114P v2 has a LAN IP address of 192.168.0.1
- The VPN client PC is behind a home NAT router and has a dynamically assigned address of 192.168.0.3

While the connection is being established, the Connection Name field in this menu will say “SA” before the name of the connection. When the connection is successful, the “SA” will change to the yellow key symbol shown in the illustration above.

Viewing the FWG114P v2 VPN Status and Log Information

Information on the status of the VPN client connection can be viewed by opening the FWG114P v2 VPN Status screen. To view this screen, click the VPN Status link on the FWG114P v2 main menu.

The FWG114P v2 VPN Status screen for a successful connection is shown below:



VPN Status/Log

```
[2003-11-22 09:39:44]**** SENT OUT SECOND MESSAGE OF AGGR MODE ****
[2003-11-22 09:39:45]**** RECEIVED  THIRD MESSAGE OF AGGR MODE ****
[2003-11-22 09:39:45]<POLICY: VPNclient> PAYLOADS: HASH,NOTIFY
[2003-11-22 09:39:45]**** AGGR MODE COMPLETED ****
[2003-11-22 09:39:45][==== IKE PHASE 1 ESTABLISHED====]
[2003-11-22 09:39:45][==== IKE PHASE 2(from 64.175.249.42) START (responder) ===
[2003-11-22 09:39:45]**** RECEIVED  FIRST MESSAGE OF QUICK MODE ****
[2003-11-22 09:39:45]**** FOUND IDs,EXTRACE ID INFO ****
[2003-11-22 09:39:45]<Initiator IPADDR=192.168.0.3>
[2003-11-22 09:39:45]<Responder IPADDR=192.168.0.0 MASK=255.255.255.0>
[2003-11-22 09:39:45]**** SENT OUT SECOND MESSAGE OF QUICK MODE ****
[2003-11-22 09:39:45]**** RECEIVED  THIRD MESSAGE OF QUICK MODE ****
[2003-11-22 09:39:45]<POLICY: VPNclient> PAYLOADS: HASH
[2003-11-22 09:39:46]**** QUICK MODE COMPLETED ****
[2003-11-22 09:39:46][==== IKE PHASE 2 ESTABLISHED====]
```

IPSec SA

#	SPI	Policy Name	Endpoint	Protocol	Tx (KBytes)	HLifeTime	SLifeTime
1	3693815379	c0a80003	64.175.249.42	ESP	0	28760	28670
2	3797946439	INc0a80003	66.120.188.153	ESP	0	28760	0

IKE SA

#	Policy Name	Endpoint	State	LifeTime in Secs
1	VPNclient	64.175.249.42	SA_MATURE	0

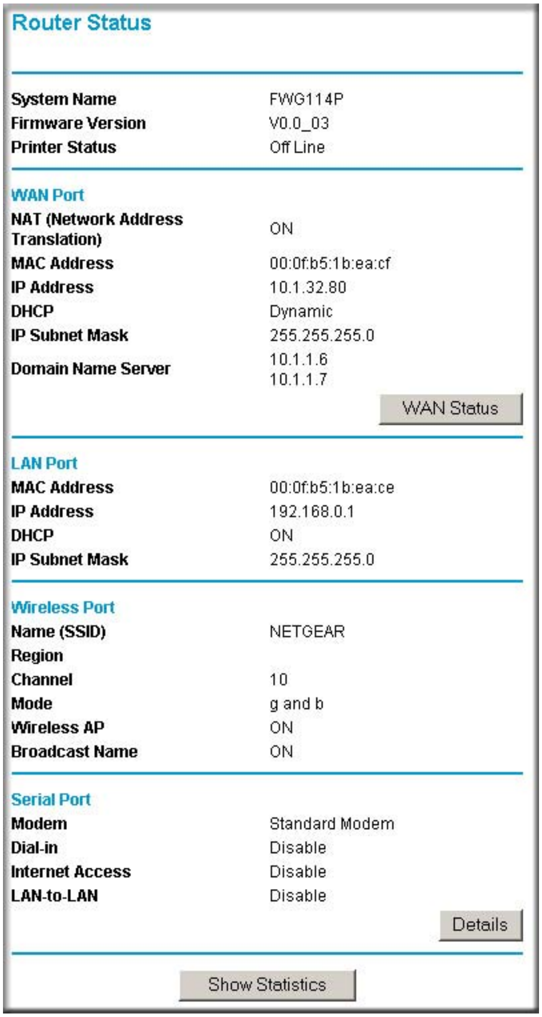
Figure 8-36: FWG114P v2 VPN Status screen

Chapter 9
Maintenance

This chapter describes how to use the maintenance features of your ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2. These features are accessed via the Main Menu Maintenance heading.

Viewing Wireless Firewall/Print Server Status Information

The Router Status menu provides status and usage information. From the main menu of the browser interface, click on Maintenance, then select Router Status to view this screen.



Router Status

System Name	FWG114P
Firmware Version	V0.0_03
Printer Status	Off Line

WAN Port

NAT (Network Address Translation)	ON
MAC Address	00:0f:b5:1b:ea:cf
IP Address	10.1.32.80
DHCP	Dynamic
IP Subnet Mask	255.255.255.0
Domain Name Server	10.1.1.6 10.1.1.7

LAN Port

MAC Address	00:0f:b5:1b:ea:ce
IP Address	192.168.0.1
DHCP	ON
IP Subnet Mask	255.255.255.0

Wireless Port

Name (SSID)	NETGEAR
Region	
Channel	10
Mode	g and b
Wireless AP	ON
Broadcast Name	ON

Serial Port

Modem	Standard Modem
Dial-in	Disable
Internet Access	Disable
LAN-to-LAN	Disable

Figure 9-1: Router Status screen

The Router Status screen shows the following parameters:

Table 9-1.   Status Fields

Field	Description
System Name	The System Name assigned to the router.
Firmware Version	The router firmware version.

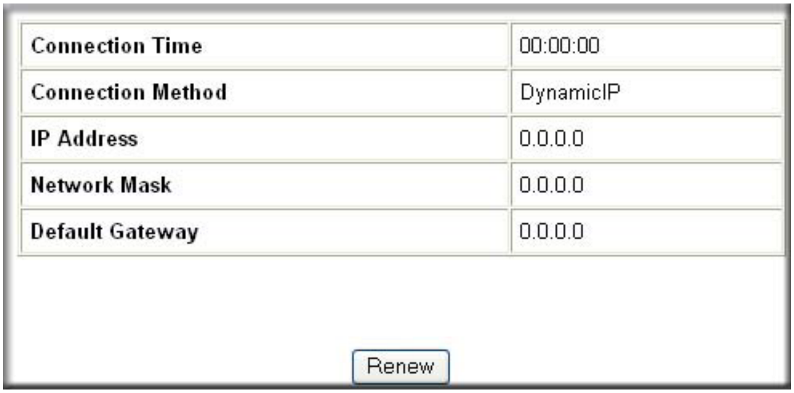
Table 9-1. Status Fields

Field	Description
Printer Status	The printer status.
WAN Port	These parameters apply to the Internet (WAN) port of the router.
MAC Address	This field displays the MAC address being used by the Internet (WAN) port of the router.
IP Address	This field displays the IP address being used by the Internet (WAN) port of the router. If no address is shown, the router cannot connect to the Internet.
DHCP	This field if the WAN port DHCP settings are dynamic or static.
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Internet (WAN) port of the router.
Domain Name Server	Identifies the IP address of the DNS server(s).
LAN Port	
MAC Address	The Media Access Control address being used by the LAN port of the router.
IP Address	The IP address being used by the Local (LAN) port of the router. The default is 192.168.0.1.
DHCP	Identifies if the router’s built-in DHCP server is active for the LAN attached devices.
IP Subnet Mask	The IP Subnet Mask being used by the Local (LAN) port of the router. The default is 255.255.255.0.
Wireless Port	
Name (SSID)	This field displays the wireless network name (SSID) being used by the wireless port of the router. The default is Wireless.
Region	This field displays the MAC address being used by the wireless port of the router.
Channel/Frequency	Identifies the channel the wireless port is using. See “Wireless Channels” on page E-7 for the frequencies used on each channel.
Mode	Identifies if the channel the wireless port is set for 802.11b, 802.11g, or both.
Wireless AP	Identifies if the wireless access point is on or off.
Broadcast Name	Identifies if the Name (SSID) is being broadcast.
Serial Port	
Status	The status of the serial port. Click the Details button to view the Serial Port Log, Port Status, Physical Link, PPP Link, PPP IP Address, Phone Line Speed, and Serial Line Speed.

Table 9-1. Status Fields

Field	Description
Modem	The status of the modem port.
Dial-In	The status of the Dial-In port.
Internet Access	The status of the serial Internet connection.
Lan-to-LAN	The status of the serial LAN-to-LAN connection.

Click “WAN Status” to display the WAN connection status.



Connection Time	00:00:00
Connection Method	DynamicIP
IP Address	0.0.0.0
Network Mask	0.0.0.0
Default Gateway	0.0.0.0

Figure 9-2: Connection Status screen

This screen shows the following statistics:.

Table 9-1. Connection Status Fields

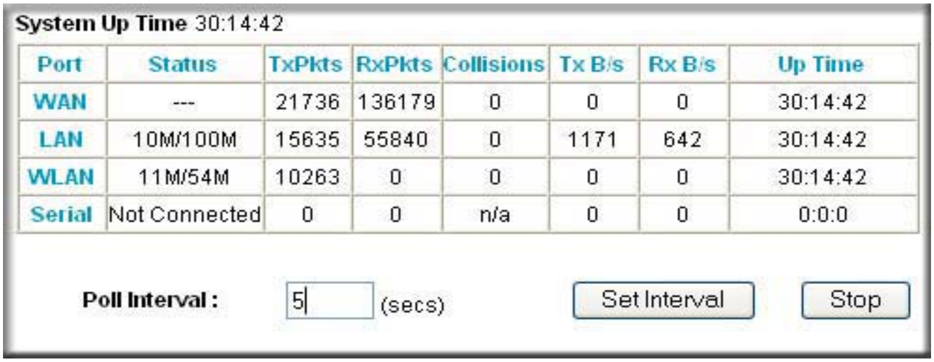
Field	Description
Connection Time	The length of time the router has been connected to your Internet service provider’s network.
Connection Method	The method used to obtain an IP address from your Internet service provider.
IP Address	The WAN (Internet) IP Address assigned to the router.
Network Mask	The WAN (Internet) Subnet Mask assigned to the router.
Default Gateway	The WAN (Internet) default gateway the router communicates with.

Log action buttons are described in Table 9-2.

Table 9-2. Connection Status action buttons

Field	Description
Renew	Click the Renew button to renew the DHCP lease.

Click “Show Statistics” to display router usage statistics.



System Up Time 30:14:42

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	---	21736	136179	0	0	0	30:14:42
LAN	10M/100M	15635	55840	0	1171	642	30:14:42
WLAN	11M/54M	10263	0	0	0	0	30:14:42
Serial	Not Connected	0	0	n/a	0	0	0:0:0

Poll Interval : 5 (secs)

Figure 9-3: Router Statistics screen

This screen shows the following statistics:

Table 9-1. Router Statistics Fields

Field	Description
interface	The statistics for the WAN (Internet), LAN (local), Wireless, and Serial interfaces. For each interface, the screen displays:
Status	The link status of the interface.
TxPkts	The number of packets transmitted on this interface since reset or manual clear.
RxPkts	The number of packets received on this interface since reset or manual clear.
Collisions	The number of collisions on this interface since reset or manual clear.
Tx B/s	The current transmission (outbound) bandwidth used on the interfaces.
Rx B/s	The current reception (inbound) bandwidth used on the interfaces.
Up Time	The amount of time since the router was last restarted.

Table 9-1. Router Statistics Fields (continued)

Field	**Description**
Serial Up Time	The time elapsed since this port acquired the link.
Poll Interval	Specifies the intervals at which the statistics are updated in this window. Click on Stop to freeze the display.

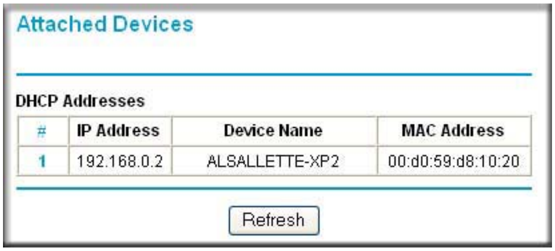
WAN Status action buttons are described in Table 9-2.

Table 9-2. Connection Status action buttons

Field	**Description**
Set Interval	Enter a time and click the button to set the polling frequency.
Stop	Click the Stop button to freeze the polling information.

Viewing a List of Attached Devices

The Attached Devices menu contains a table of all IP devices that the router has discovered on the local network. From the Main Menu of the browser interface, under the Maintenance heading, select Attached Devices to view the table shown below:



Attached Devices

DHCP Addresses

#	IP Address	Device Name	MAC Address
1	192.168.0.2	ALSALLETTE-XP2	00:d0:59:d8:10:20

Figure 9-4: Attached Devices menu

For each device, the table shows the IP address, Device Name (if available), and Ethernet MAC address. Note that if the router is rebooted, the table data is lost until the router rediscovers the devices. To force the router to look for attached devices, click the Refresh button.

Upgrading the Router Software

The routing software of the FWG114P v2 Wireless Firewall/Print Server is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR. Upgrade files can be downloaded from Netgear's Web site. If the upgrade file is compressed (.ZIP file), you must first extract the binary file before sending it to the router. The upgrade file can be sent to the router using your browser.

Note: The Web browser used to upload new firmware into the FWG114P v2 Wireless Firewall/Print Server must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer or Netscape Navigator 3.0, or above.

From the Main Menu of the browser interface, under the Maintenance heading, select the Router Upgrade heading.

To upload new firmware:

1. Download and unzip the new software file from NETGEAR.
2. In the Router Upgrade menu, click the Browse button and browse to the location of the binary (.IMG) upgrade file.
3. Click Upload.

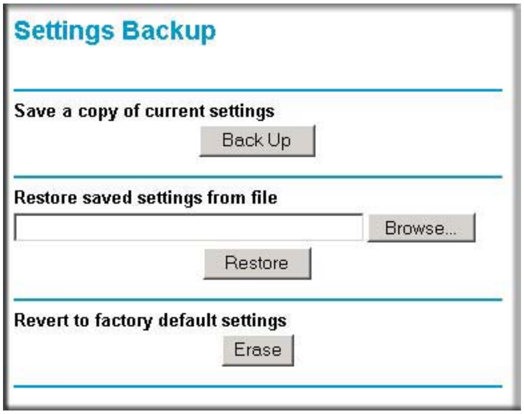
   Note: When uploading software to the FWG114P v2, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it may corrupt the software. When the upload is complete, your router will automatically restart. The upgrade process will typically take about one minute.

In some cases, you may need to reconfigure the router after upgrading.

Configuration File Management

The configuration settings of the FWG114P v2 Wireless Firewall/Print Server are stored within the router in a configuration file. This file can be saved (backed up) to a user’s computer, retrieved (restored) from the user’s computer, or cleared to the factory default settings.

From the Main Menu of the browser interface, under the Maintenance heading, select the Settings Backup heading to bring up the menu shown below.



Settings Backup

Save a copy of current settings

Restore saved settings from file

Revert to factory default settings

Figure 9-5: Settings Backup menu

Three options are available, and are described in the following sections.

Restoring and Backing Up the Configuration

The Restore and Backup options in the Settings Backup menu allow you to save and retrieve a file containing your router’s configuration settings.

To save your settings, click Backup. Your browser will extract the configuration file from the router and will prompt you for a location on your computer to store the file. You can give the file a meaningful name at this time, such as SBC.cfg.

To restore your settings from a saved configuration file, enter the full path to the file on your computer or click the Browse button to locate the file. When you have located it, click the Restore button to send the file to the router. The router will then reboot automatically.

Erasing the Configuration

It is sometimes desirable to restore the router to a known blank condition. This can be done by using the Erase function, which will restore all factory settings. After an erase, the router's password will be **password**, the LAN IP address will be 192.168.0.1, and the router's DHCP client will be enabled.

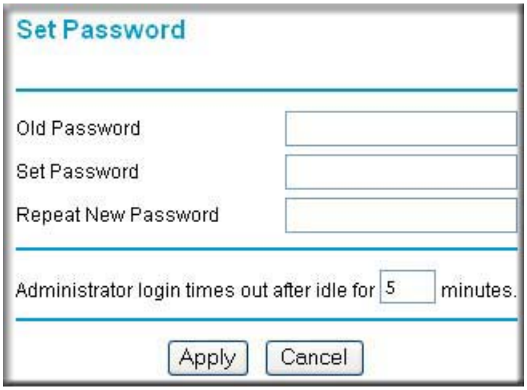
To erase the configuration, click the Erase button.

To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the router. See "Restoring the Default Configuration and Password" on page 11-7.

Changing the Administrator Password

The default password for the router's Web Configuration Manager is **password**. Netgear recommends that you change this password to a more secure password.

From the main menu of the browser interface, under the Maintenance heading, select Set Password to bring up this menu.



Set Password

Old Password

Set Password

Repeat New Password

Administrator login times out after idle for 5 minutes.

Figure 9-6: Set Password menu

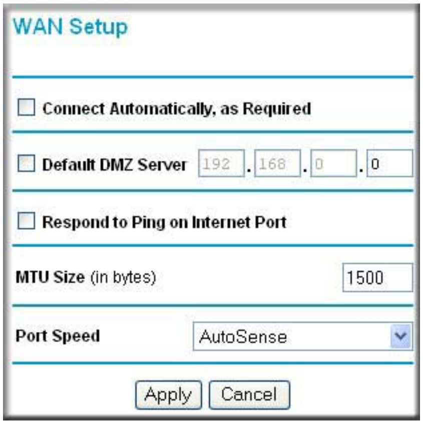
To change the password, first enter the old password, and then enter the new password twice. Click Apply. To change the login idle timeout, change the number of minutes and click Apply.

Chapter 10
Advanced Configuration

This chapter describes how to configure the advanced features of your ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2. These features can be found under the Advanced heading in the Main Menu of the browser interface.

Using the WAN Setup Options

The first feature category under the Advanced heading is WAN Setup. This menu allows configuration of a DMZ server, MTU size, port speed, and so on. From the Main Menu of the browser interface, under Advanced, click on WAN IP Setup to view the WAN IP Setup menu, shown below.



WAN Setup

□ Connect Automatically, as Required

□ Default DMZ Server 192 . 168 . 0 . 0

□ Respond to Ping on Internet Port

MTU Size (in bytes) 1500

Port Speed AutoSense

Figure 10-1: WAN Setup Menu

The WAN Setup options let you configure a DMZ server, change the MTU size, and set the WAN port speed. These options are discussed below.

- **Connect Automatically, as Required**

Normally, this option is Enabled, so that an Internet connection will be made automatically whenever Internet-bound traffic is detected. In locations where Internet access is billed by the minute, if this causes high connection costs, you can disable this setting.

If disabled, you must connect manually, using the sub-screen accessed from the Router Status menu "Show WAN Status" screen.

- **Setting Up a Default DMZ Server**

Note: DMZ servers pose a security risk. A computer designated as the default DMZ server loses much of the protection of the firewall, and is exposed to attacks from the Internet. If compromised, the DMZ server can be used to attack your network.

The use of the term 'DMZ' has become common, although it is a misnomer. In traditional firewalls, a DMZ is actually a separate physical network port. A true DMZ port is for connecting servers that require greater access from the outside, and will therefore be provided with a different level of security by the firewall. A better term for our application is Exposed Host.

The default DMZ server feature is helpful when using some online games and videoconferencing applications that are incompatible with NAT. The router 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, one local computer can run the application properly if that computer's IP address is entered as the default DMZ server.

Incoming traffic from the Internet is normally discarded by the router unless the traffic is a response to one of your local computers or a service that you have configured in the Ports menu. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the Default DMZ Server.

The WAN Setup menu lets you configure a Default DMZ Server.

To assign a computer or server to be a Default DMZ server, follow these steps:

1. Click WAN Setup link on the Advanced section of the main menu.
2. Type the IP address for that server. To remove the default DMZ server, replace the IP address numbers with all zeros.
3. Click Apply.

- **Respond to Ping on Internet WAN Port**

If you want the router to respond to a 'ping' from the Internet, click the 'Respond to Ping on Internet WAN Port' check box. This should only be used as a diagnostic tool, since it allows your router to be discovered. Do not check this box unless you have a specific reason to do so.

- **Setting the MTU Size**

  The default MTU size is usually fine. The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs, particularly those using PPPoE, you may need to reduce the MTU. This should not be done unless you are sure it is necessary for your ISP.

  Any packets sent through the router that are larger than the configured MTU size will be repackaged into smaller packets to meet the MTU requirement. To change the MTU size, under MTU Size, enter a new size between 64 and 1500. Then, click Apply to save the new configuration.

- **Setting the WAN Port Speed**

  In most cases, your router can automatically determine (AutoSense) the connection speed of the Internet (WAN) port. If you cannot establish an Internet connection and the Internet LED blinks continuously, you may need to manually select the port speed.

  If you know that the Ethernet port on your broadband modem supports 100BaseT, select 100M; otherwise, select 10M.

How to Configure Dynamic DNS

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial dynamic DNS service, which will allow you to register your domain to their IP address, and will forward traffic directed to your domain to your frequently-changing IP address.

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

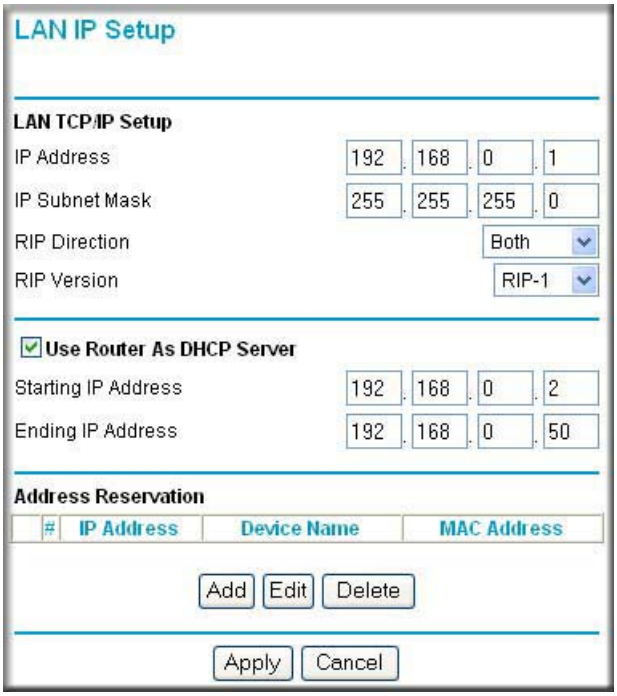
1. Log in to the router at its default LAN address of *http://192.168.0.1,* with its default user name of **admin**, default password of **password**, or using whatever password and LAN address you have chosen for the router.
2. From the Main Menu of the browser interface, under Advanced, click on Dynamic DNS.

3. Access the website of one of the dynamic DNS service providers whose names appear in the ‘Select Service Provider’ box, and register for an account.
   For example, for dyndns.org, go to *www.dyndns.org*.
4. Select the “Use a dynamic DNS service” check box.
5. Select the name of your dynamic DNS Service Provider.
6. Type the host name that your dynamic DNS service provider gave you.
   The dynamic DNS service provider may call this the domain name. If your URL is myName.dyndns.org, then your host name is “myName.”
7. Type the user name for your dynamic DNS account.
8. Type the password (or key) for your dynamic DNS account.
9. If your dynamic DNS provider allows the use of wildcards in resolving your URL, you may select the Use wildcards check box to activate this feature.
   For example, the wildcard feature will cause *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org
10. Click Apply to save your configuration.

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

Using the LAN IP Setup Options

The second feature category under the Advanced heading is LAN IP Setup. This menu allows configuration of LAN IP services, such as DHCP and RIP. From the Main Menu of the browser interface, under Advanced, click on LAN IP Setup to view the LAN IP Setup menu, shown below.



LAN IP Setup

LAN TCP/IP Setup

IP Address 192 . 168 . 0 . 1

IP Subnet Mask 255 . 255 . 255 . 0

RIP Direction Both

RIP Version RIP-1

☑ Use Router As DHCP Server

Starting IP Address 192 . 168 . 0 . 2

Ending IP Address 192 . 168 . 0 . 50

Address Reservation

	#	IP Address	Device Name	MAC Address

Figure 10-2: LAN IP Setup Menu

Configuring LAN TCP/IP Setup Parameters

The router is shipped preconfigured to use private IP addresses on the LAN side, and to act as a DHCP server. The router’s default LAN IP configuration is:

- LAN IP addresses—192.168.0.1
- Subnet mask—255.255.255.0

These addresses are part of the IETF-designated private address range for use in private networks, and should be suitable in most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in this menu.

The LAN IP parameters are:

- IP Address
  This is the LAN IP address of the router.
- IP Subnet Mask
  This is the LAN Subnet Mask of the router. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.
- RIP Direction
  RIP (Router Information Protocol) allows a router to exchange routing information with other routers. The RIP Direction selection controls how the router sends and receives RIP packets. Both is the default.
  - When set to Both or Out Only, the router will broadcast its routing table periodically.
  - When set to Both or In Only, it will incorporate the RIP information that it receives.
  - When set to None, it will not send any RIP packets and will ignore any RIP packets received.
- RIP Version
  This controls the format and the broadcasting method of the RIP packets that the router sends. (It recognizes both formats when receiving.) By default, this is set for RIP-1.
  - RIP-1 is universally supported. RIP-1 is probably adequate for most networks, unless you have an unusual network setup.
  - RIP-2 carries more information. RIP-2B uses subnet broadcasting.

Note: If you change the LAN IP address of the router 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.

Using the Router as a DHCP server

By default, the router will function as a DHCP (Dynamic Host Configuration Protocol) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the router's LAN. The assigned default gateway address is the LAN address of the router. IP addresses will be assigned to the attached PCs from a pool of addresses specified in this menu. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications, the default DHCP and TCP/IP settings of the router are satisfactory.

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 ‘Use router as DHCP server’ check 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 router’s LAN IP address. Using the default addressing scheme, you should define a range between 192.168.0.2 and 192.168.0.253, although you may wish to save part of the range for devices with fixed addresses.

The router will deliver the following parameters to any LAN device that requests DHCP:

- An IP Address from the range you have defined.
- Subnet Mask.
- Gateway IP Address (the router’s LAN IP address).
- Primary DNS Server (if you entered a Primary DNS address in the Basic Settings menu; otherwise, the router’s LAN IP address).
- Secondary DNS Server (if you entered a Secondary DNS address in the Basic Settings menu).

Using Address Reservation

When you specify a reserved IP address for a computer on the LAN, that computer will always receive the same IP address each time it access the router’s DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.

To reserve an IP address:

1. Click the Add button.
2. In the IP Address box, type the IP address to assign to the computer or server.
(choose an IP address from the router’s LAN subnet, such as 192.168.0.X)

3. Type the MAC Address of the computer or server.
   (Tip: If the computer is already present on your network, you can copy its MAC address from the Attached Devices menu and paste it here.)
4. Click Apply to enter the reserved address into the table.

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

To edit or delete a reserved address entry:

1. Click the button next to the reserved address you want to edit or delete.
2. Click Edit or Delete.

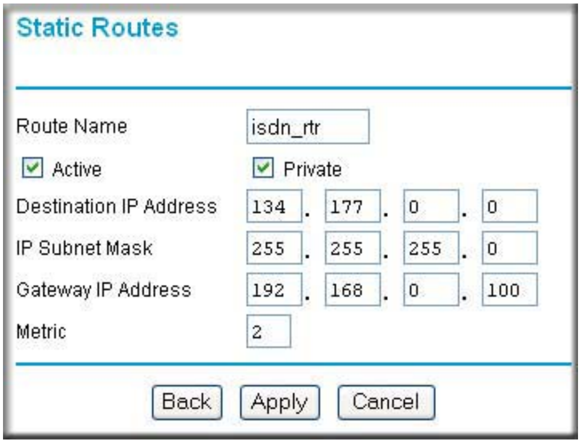
Configuring Static Routes

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

From the Main Menu of the browser interface, under Advanced, click on Static Routes to view the Static Route menu.

To add or edit a Static Route:

1. Click the Add button to open the Static Routes menu.



Static Routes

Route Name: isdn_rtr

☑ Active ☑ Private

Destination IP Address: 134 . 177 . 0 . 0

IP Subnet Mask: 255 . 255 . 255 . 0

Gateway IP Address: 192 . 168 . 0 . 100

Metric: 2

Figure 10-3. Static Route Entry and Edit Menu

2. Type a route name for this static route in the Route Name box.
   (This is for identification purpose only.)
3. Select Active to make this route effective.
4. Select Private if you want to limit access to the LAN only. The static route will not be reported in RIP.
5. Type the Destination IP Address of the final destination.
6. Type the IP Subnet Mask for this destination.
   If the destination is a single host, type 255.255.255.254.
7. Type the Gateway IP Address, which must be a router on the same LAN segment as the router.
8. Type a number between 1 and 15 as the Metric value.
   This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.
9. Click Apply to have the static route entered into the table.

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.0.100.

- Your company’s network is 134.177.0.0.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router will forward your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company’s firewall.

In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100. The static route would look like Figure 10-3.

In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Gateway IP Address fields specifies that all traffic for these addresses should be forwarded to the ISDN router at 192.168.0.100.
- A Metric value of 1 will work since the ISDN router is on the LAN.
- Private is selected only as a precautionary security measure in case RIP is activated.

Enabling Remote Management Access

Using the Remote Management page, you can allow a user or users on the Internet to configure, upgrade and check the status of your FWG114P v2 Wireless Firewall/Print Server.

> **Note:** Be sure to change the router's default configuration password to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both upper and lower case), numbers, and symbols. Your password can be up to 30 characters.

To configure your router for Remote Management:

1. Select the Turn Remote Management On check box.
2. Specify what external addresses will be allowed to access the router’s remote management. **Note:** For enhanced security, restrict access to as few external IP addresses as practical.
   a. To allow access from any IP address on the Internet, select Everyone.

b. To allow access from a range of IP addresses on the Internet, select IP address range. Enter a beginning and ending IP address to define the allowed range.

c. To allow access from a single IP address on the Internet, select Only this computer. Enter the IP address that will be allowed access.

3. Specify the Port Number that will be used for accessing the management interface.

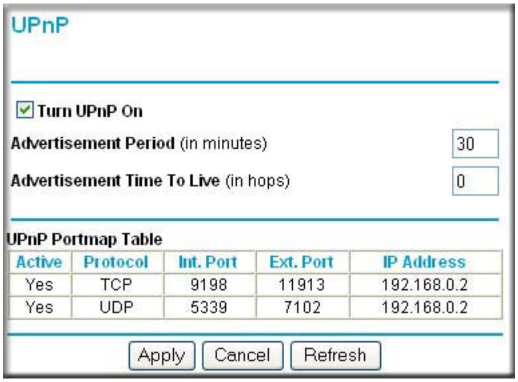
   Web browser access normally uses the standard HTTP service port 80. For greater security, you can change the remote management Web interface to a custom port by entering that number in the box provided. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

4. Click Apply to have your changes take effect.

Note: When accessing your router from the Internet, you will type your router's WAN IP address into your browser's Address (in IE) or Location (in Netscape) box, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, you must enter in your browser: http://134.177.0.123:8080

Using Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.



UPnP

☑ Turn UPnP On

Advertisement Period (in minutes) 30

Advertisement Time To Live (in hops) 0

UPnP Portmap Table

Active	Protocol	Int. Port	Ext. Port	IP Address
Yes	TCP	9198	11913	192.168.0.2
Yes	UDP	5339	7102	192.168.0.2

Figure 10-4. UPnP Menu

Turn UPnP On: UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is enabled. If disabled, the router will not allow any device to automatically control the resources, such as port forwarding (mapping), of the router.

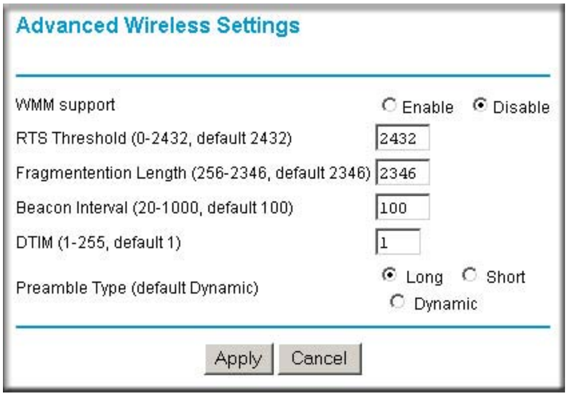
Advertisement Period: The Advertisement Period is how often the router will broadcast its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations will ensure that control points have current device status at the expense of additional network traffic. Longer durations may compromise the freshness of the device status but can significantly reduce network traffic.

Advertisement Time To Live: The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. The time to live hop count is the number of steps a broadcast packet is allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it may be necessary to increase this value a little.

UPnP Portmap Table: The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the router and which ports (Internal and External) that device has opened. The UPnP Portmap Table also displays what type of port is opened and if that port is still active for each IP address.

Advanced Wireless Settings

Note: Incorrectly changing these settings can prevent the wireless functions from working.



Advanced Wireless Settings

WMM support	○ Enable ● Disable
RTS Threshold (0-2432, default 2432)	2432
Fragmentention Length (256-2346, default 2346)	2346
Beacon Interval (20-1000, default 100)	100
DTIM (1-255, default 1)	1
Preamble Type (default Dynamic)	● Long ○ Short ○ Dynamic

Figure 10-5: Advanced Wireless Settings menu

These settings normally do not need to be changed.

- **WMM support**

  WMM (Wireless Multimedia) 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, like video or audio, will have a higher priority than normal traffic. For WMM to function correctly, wireless clients must also support WMM. The default is Disable.

- **RTS Threshold**

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

- **Fragmentation Length**

  This is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be larger than the RTS Threshold value.

- **Beacon Interval**

  Specifies the data beacon rate between 20 and 1000.

- **DTIM**

  The Delivery Traffic Indication Message. Specifies the data beacon rate between 1 and 255.

- **Preamble Type**

  A long transmit preamble may provide a more reliable connection or slightly longer range. A short transmit preamble gives better performance.

Chapter 11
Troubleshooting

This chapter gives information about troubleshooting your ProSafe Wireless 802.11g Firewall/ Print Server Model FWG114P v2. After each problem description, instructions are provided to help you diagnose and solve the problem.

Basic Functioning

After you turn on power to the router, the following sequence of events should occur:

1. When power is first applied, verify that the PWR LED is on.
2. After approximately 10 seconds, verify that:
   a. The TEST LED is not lit.
   b. The LAN port LEDs are lit for any local ports that are connected.

      If a port’s LED is lit, a link has been established to the connected device. If a LAN port is connected to a 100 Mbps device, verify that the port’s LED is green. If the port is 10 Mbps, the LED will be OFF.

   c. The Internet port LED is lit.

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

Power LED Not On

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

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

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

LEDs Never Turn Off

When the router is turned on, the LEDs turns on for about 10 seconds and then turns off. If all the LEDs stay on, there is a fault within the router.

If all LEDs are still on one minute after power up:

- Cycle the power to see if the router recovers.
- Clear the router’s configuration to the factory defaults. This will set the router’s IP address to 192.168.0.1. This procedure is explained in “Restoring the Default Configuration and Password” on page 11-7.

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

LAN or Internet Port LEDs Not On

If either the LAN LEDs or the Internet LED do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.
- Be sure you are using the correct cable:

  When connecting the router’s Internet port to a broadband modem, use the cable that was supplied with the broadband modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

Troubleshooting the Web Configuration Interface

If you are unable to access the router's Web Configuration interface from a computer on your local network, check the following:

- Check the Ethernet connection between the computer and the router as described in the previous section.
- Make sure your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.0.2 to 192.168.0.254.

  Note: If your computer's IP address is shown as 169.254.x.x: Recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router and reboot your computer.
- If your router's IP address has been changed and you do not know the current IP address, clear the router's configuration to the factory defaults. This will set the router's IP address to 192.168.0.1. This procedure is explained in "Restoring the Default Configuration and Password" on page 11-7.
- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

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

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

Troubleshooting the ISP Connection

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

To check the WAN IP address:

1. Launch your browser and select an external site, such as www.netgear.com.
2. Access the Main Menu of the router’s configuration at http://192.168.0.1.
3. Under the Maintenance heading, select Router Status.
4. Check that an IP address is shown for the WAN Port.
   If 0.0.0.0 is shown, your router has not obtained an IP address from your ISP.

If your router is unable to obtain an IP address from the ISP, you may need to force your broadband modem to recognize your new router by performing the following procedure:

1. Turn off power to the broadband modem.
2. Turn off power to your router.
3. Wait five minutes and reapply power to the broadband modem.
4. When the modem’s LEDs indicate that it has reacquired sync with the ISP, reapply power to your router.

If your router is still unable to obtain an IP address from the ISP, the problem may be one of the following:

- Your ISP may require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, you may have incorrectly set the login name and password.
- Your ISP may check for your computer's host name.
  Assign the computer Host Name of your ISP account as the Account Name in the Basic Settings menu.
- Your ISP only allows one Ethernet MAC address to connect to Internet, and may check for your computer’s MAC address. In this case:

  Inform your ISP that you have bought a new network device and ask them to use the router’s MAC address.

OR

Configure your router to spoof your computer’s MAC address. This can be done in the Basic Settings menu. Refer to “Manually Configuring Your Internet Connection” on page 3-18.

If your router can obtain an IP address, but your computer is unable to load any Web pages from the Internet:

- Your computer may not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. Alternatively, you may configure your computer manually with DNS addresses, as explained in your operating system documentation.

- Your computer may not have the router configured as its TCP/IP gateway.

  If your computer obtains its information from the router by DHCP, reboot the computer and verify the gateway address.

Troubleshooting a TCP/IP Network Using a Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. Troubleshooting a TCP/IP network is made very easy by using the ping utility in your computer or workstation.

Testing the LAN Path to Your Router

You can ping the router from your computer to verify that the LAN path to your router is set up correctly.

To ping the router from a computer running Windows 95 or later:

1. From the Windows toolbar, click on the Start button and select Run.
2. In the field provided, type Ping followed by the IP address of the router, as in this example:

   ```
   ping 192.168.0.1
   ```

3. Click on OK.

   You should see a message like this one:

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

   If the path is working, you see this message:

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

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

```
Request timed out
```

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

- Wrong physical connections
  - — Make sure the LAN port LED is on. If the LED is off, follow the instructions in "LAN or Internet Port LEDs Not On" on page 11-2.
  - — Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
- Wrong network configuration
  - — Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer or workstation.
  - — Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your computer to a remote device. From the Windows run menu, type:

```
PING -n 10 <IP address>
```

where <*IP address*> is the IP address of a remote device, such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

— Check that your computer has the IP address of your router listed as the default gateway. If the IP configuration of your computer is assigned by DHCP, this information will not be visible in your computer's Network Control Panel. Verify that the IP address of the router is listed as the default gateway.

— Check to see that the network address of your computer (the portion of the IP address specified by the netmask) is different from the network address of the remote device.

— Check that your broadband modem is connected and functioning.

— If your ISP assigned a host name to your computer, enter that host name as the Account Name in the Basic Settings menu.

— Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If this is the case, you must configure your router to “clone” or “spoof” the MAC address from the authorized computer. Refer to “Manually Configuring Your Internet Connection” on page 3-18.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router’s administration password to **password** and the IP address to 192.168.0.1. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the router (see “Erasing the Configuration” on page 9-9).
- Use the Default Reset button on the rear panel of the router. Use this method for cases when the administration password or IP address is not known.

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

1. Press and hold the Default Reset button until the Test LED turns on (about 10 seconds).
2. Release the Default Reset button and wait for the router to reboot.

Problems with Date and Time

The E-Mail menu in the Content Filtering section displays the current date and time of day. The FWG114P v2 Wireless Firewall/Print Server uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000. Cause: The router has not yet successfully reached a Network Time Server. Check that your Internet access settings are configured correctly. If you have just completed configuring the router, wait at least five minutes and check the date and time again.
- Time is off by one hour. Cause: The router does not automatically sense Daylight Savings Time. In the E-Mail menu, check or uncheck the box marked “Adjust for Daylight Savings Time”.

Appendix A
Technical Specifications

This appendix provides technical specifications for the ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2.

Network Protocol and Standards Compatibility	
Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP PPP over Ethernet (PPPoE)
VPN	
Protocols:	IPSec, SHA-1, MD5, DES, 3DES, ESP, DH1, DH2
Tunnels:	2 IPSec Tunnels
Power Adapter	
North America:	120V, 60 Hz, input
United Kingdom, Australia:	240V, 50 Hz, input
Europe:	230V, 50 Hz, input
Japan:	100V, 50/60 Hz, input
All regions (output):	12 V DC @ 1.2 A output, 18W maximum
Physical Specifications	
Dimensions:	H: 32 x L: 188 x W: 124 mm (1.25 x 7.4 x 4.9 in.)
Weight:	0.64 kg (1.4 lb)
Environmental Specifications	
Operating temperature:	0° to 40° C (32º to 104º F)
Operating humidity:	90% maximum relative humidity, noncondensing

Electromagnetic Emissions			
For North America and Australia	FCC Part 15 Class B		
For Japan	VCCI Class B		
For Europe	EN 300 328, EN 301 489-17, EN 301 489-1, EN 60950		
Interface Specifications			
LAN:	10BASE-T or 100BASE-Tx, RJ-45		
WAN:	10BASE-T or 100BASE-Tx		
Printer:	USB v1.1		
Serial:	RS-232 male DB-9 connector		
Wireless			
Data Encoding:	802.11b: Direct Sequence Spread Spectrum (DSSS) 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)		
Maximum Computers Per Wireless Network:	Limited by the amount of wireless network traffic generated by each node. Typically 30-70 nodes.		
802.11b and g Radio Data Rate	1, 2, 5.5, 6, 9, 12, 18, 24, 36, 48, and 54 Mbps (Auto-rate capable)		
802.11b and g Transmit Power and Receive Sensitivity		Maximum Transmit Power / Receive Sensitivity	
	54 Mbps, 11g	14.5 dBm typical	- 72 dBm typical
	48 Mbps, 11g	14.5 dBm typical	- 75 dBm typical
	36 Mbps, 11g	15.5 dBm typical	- 80dBm typical
	24 Mbps, 11g	15.5 dBm typical	- 82 dBm typical
	18Mbps, 11g	16.5 dBm typical	- 84 dBm typical
	12 Mbps, 11g	16.5 dBm typical	- 85 dBm typical
	6 Mbps, 11g	16.5 dBm typical	- 86 dBm typical
	11 Mbps, 11b	17.5 dBm typical	- 83 dBm typical
	5.5 Mbps, 11b	17.5 dBm typical	- 86 dBm typical
	2 Mbps, 11b	17.5 dBm typical	- 89 dBm typical
	1Mbps, 11b	17.5 dBm typical	- 92 dBm typical
	Note: For Europe, the maximum transmit power does not exceed +15 dBm		
Antenna:	External detachable 5 dBi omnidirectional		
802.11 Security	40-bits (also called 64-bits), 128-bits WEP data encryption, and WPA		

Appendix B
Networks, Routing, and Firewall Basics

This appendix provides an overview of IP networks, routing, and firewalls.

Related Publications

As you read this document, you may be directed to various RFC documents for further information. An RFC is a Request For Comment (RFC) published by the Internet Engineering Task Force (IETF), an open organization that defines the architecture and operation of the Internet. The RFC documents outline and define the standard protocols and procedures for the Internet. The documents are listed on the World Wide Web at *www.ietf.org* and are mirrored and indexed at many other sites worldwide.

Basic Router Concepts

Large amounts of bandwidth can be provided easily and relatively inexpensively in a local area network (LAN). However, providing high bandwidth between a local network and the Internet can be very expensive. Because of this expense, Internet access is usually provided by a slower-speed wide-area network (WAN) link, such as a cable or DSL modem. In order to make the best use of the slower WAN link, a mechanism must be in place for selecting and transmitting only the data traffic meant for the Internet. The function of selecting and forwarding this data is performed by a router.

What is a Router?

A router is a device that forwards traffic between networks based on network layer information in the data and on routing tables maintained by the router. In these routing tables, a router builds up a logical picture of the overall network by gathering and exchanging information with other routers in the network. Using this information, the router chooses the best path for forwarding network traffic.

Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connection they support.

Routing Information Protocol

One of the protocols used by a router to build and maintain a picture of the network is the Routing Information Protocol (RIP). Using RIP, routers periodically update one another and check for changes to add to the routing table.

The FWG114P v2 Wireless Firewall/Print Server supports both the older RIP-1 and the newer RIP-2 protocols. Among other improvements, RIP-2 supports subnet and multicast protocols. RIP is not required for most home applications.

IP Addresses and the Internet

Because TCP/IP networks are interconnected across the world, every machine on the Internet must have a unique address to make sure that transmitted data reaches the correct destination. Blocks of addresses are assigned to organizations by the Internet Assigned Numbers Authority (IANA). Individual users and small organizations may obtain their addresses either from the IANA or from an Internet service provider (ISP). You can contact IANA at www.iana.org.

The Internet Protocol (IP) uses a 32-bit address structure. The address is usually written in dot notation (also called dotted-decimal notation), in which each group of eight bits is written in decimal form, separated by decimal points.

For example, the following binary address:

```
11000011  00100010  00001100  00000111
```

is normally written as:

```
195.34.12.7
```

The latter version is easier to remember and easier to enter into your computer.

In addition, the 32 bits of the address are subdivided into two parts. The first part of the address identifies the network, and the second part identifies the host node or station on the network. The dividing point may vary depending on the address range and the application.

There are five standard classes of IP addresses. These address classes have different ways of determining the network and host sections of the address, allowing for different numbers of hosts on a network. Each address type begins with a unique bit pattern, which is used by the TCP/IP software to identify the address class. After the address class has been determined, the software can correctly identify the host section of the address. The following figure shows the three main address classes, including network and host sections of the address for each address type.

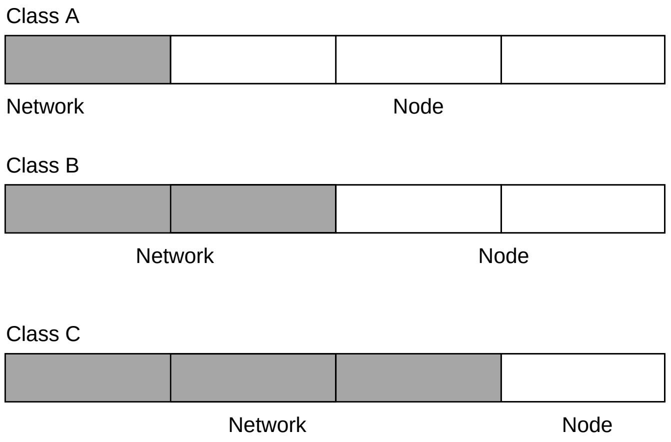


Figure 11-1: Three Main Address Classes

The five address classes are:

- Class A
  Class A addresses can have up to 16,777,214 hosts on a single network. They use an eight-bit network number and a 24-bit node number. Class A addresses are in this range:

  1.x.x.x to 126.x.x.x.

- Class B
  Class B addresses can have up to 65,354 hosts on a network. A Class B address uses a 16-bit network number and a 16-bit node number. Class B addresses are in this range:

  128.1.x.x to 191.254.x.x.

- Class C
  Class C addresses can have 254 hosts on a network. Class C addresses use 24 bits for the network address and eight bits for the node. They are in this range:

  192.0.1.x to 223.255.254.x.

- Class D
  Class D addresses are used for multicasts (messages sent to many hosts). Class D addresses are in this range:

  224.0.0.0 to 239.255.255.255.

- Class E
  Class E addresses are for experimental use.

This addressing structure allows IP addresses to uniquely identify each physical network and each node on each physical network.

For each unique value of the network portion of the address, the base address of the range (host address of all zeros) is known as the network address and is not usually assigned to a host. Also, the top address of the range (host address of all ones) is not assigned, but is used as the broadcast address for simultaneously sending a packet to all hosts with the same network address.

Netmask

In each of the address classes previously described, the size of the two parts (network address and host address) is implied by the class. This partitioning scheme can also be expressed by a netmask associated with the IP address. A netmask is a 32-bit quantity that, when logically combined (using an AND operator) with an IP address, yields the network address. For instance, the netmasks for Class A, B, and C addresses are 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively.

For example, the address 192.168.170.237 is a Class C IP address whose network portion is the upper 24 bits. When combined (using an AND operator) with the Class C netmask, as shown here, only the network portion of the address remains:

```
11000000  10101000  10101010  11101101 (192.168.170.237)
```

combined with:

```
11111111  11111111  11111111  00000000 (255.255.255.0)
```

Equals:

```
11000000  10101000  10101010  00000000 (192.168.170.0)
```

As a shorter alternative to dotted-decimal notation, the netmask may also be expressed in terms of the number of ones from the left. This number is appended to the IP address, following a backward slash (/), as “/n.” In the example, the address could be written as 192.168.170.237/24, indicating that the netmask is 24 ones followed by 8 zeros.

Subnet Addressing

By looking at the addressing structures, you can see that even with a Class C address, there are a large number of hosts per network. Such a structure is an inefficient use of addresses if each end of a routed link requires a different network number. It is unlikely that the smaller office LANs would have that many devices. You can resolve this problem by using a technique known as subnet addressing.

Subnet addressing allows us to split one IP network address into smaller multiple physical networks known as subnetworks. Some of the node numbers are used as a subnet number instead. A Class B address gives us 16 bits of node numbers translating to 64,000 nodes. Most organizations do not use 64,000 nodes, so there are free bits that can be reassigned. Subnet addressing makes use of those bits that are free, as shown below.

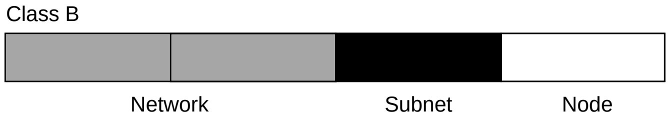


Figure 11-2: Example of Subnetting a Class B Address

A Class B address can be effectively translated into multiple Class C addresses. For example, the IP address of 172.16.0.0 is assigned, but node addresses are limited to 255 maximum, allowing eight extra bits to use as a subnet address. The IP address of 172.16.97.235 would be interpreted as IP network address 172.16, subnet number 97, and node number 235. In addition to extending the number of addresses available, subnet addressing provides other benefits. Subnet addressing allows a network manager to construct an address scheme for the network by using different subnets for other geographical locations in the network or for other departments in the organization.

Although the preceding example uses the entire third octet for a subnet address, note that you are not restricted to octet boundaries in subnetting. To create more network numbers, you need only shift some bits from the host address to the network address. For instance, to partition a Class C network number (192.68.135.0) into two, you shift one bit from the host address to the network address. The new netmask (or subnet mask) is 255.255.255.128. The first subnet has network number 192.68.135.0 with hosts 192.68.135.1 to 129.68.135.126, and the second subnet has network number 192.68.135.128 with hosts 192.68.135.129 to 192.68.135.254.

➡	**Note:** The number 192.68.135.127 is not assigned because it is the broadcast address of the first subnet. The number 192.68.135.128 is not assigned because it is the network address of the second subnet.

The following table lists the additional subnet mask bits in dotted-decimal notation. To use the table, write down the original class netmask and replace the 0 value octets with the dotted-decimal value of the additional subnet bits. For example, to partition your Class C network with subnet mask 255.255.255.0 into 16 subnets (4 bits), the new subnet mask becomes 255.255.255.240.

Table 11-1. Netmask Notation Translation Table for One Octet

Number of Bits	Dotted-Decimal Value
1	128
2	192
3	224
4	240
5	248
6	252
7	254
8	255

The following table displays several common netmask values in both the dotted-decimal and the masklength formats.

Table 11-2. Netmask Formats

Dotted-Decimal	Masklength
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31
255.255.255.255	/32

NETGEAR strongly recommends that you configure all hosts on a LAN segment to use the same netmask for the following reasons:

- So that hosts recognize local IP broadcast packets.

  When a device broadcasts to its segment neighbors, it uses a destination address of the local network address with all ones for the host address. In order for this scheme to work, all devices on the segment must agree on which bits comprise the host address.

- So that a local router or bridge recognizes which addresses are local and which are remote.

Private IP Addresses

If your local network is isolated from the Internet (for example, when using NAT), you can assign any IP addresses to the hosts without problems. However, the IANA has reserved the following three blocks of IP addresses specifically for private networks:

```
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255
```

NETGEAR recommends that you choose your private network number from this range. The DHCP server of the FWG114P v2 Wireless Firewall/Print Server is preconfigured to automatically assign private addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines explained here. For more information about address assignment, refer to RFC 1597, *Address Allocation for Private Internets,* and RFC 1466, *Guidelines for Management of IP Address Space*. The Internet Engineering Task Force (IETF) publishes RFCs on its Web site at *www.ietf.org*.

Single IP Address Operation Using NAT

In the past, if multiple computers on a LAN needed to access the Internet simultaneously, you had to obtain a range of IP addresses from the ISP. This type of Internet account is more costly than a single-address account typically used by a single user with a modem, rather than a router. The FWG114P v2 Wireless Firewall/Print Server employs an address-sharing method called Network Address Translation (NAT). This method allows several networked computers to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your ISP.

The router accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. The internal LAN IP addresses can be either private addresses or registered addresses. For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

The following figure illustrates a single IP address operation.

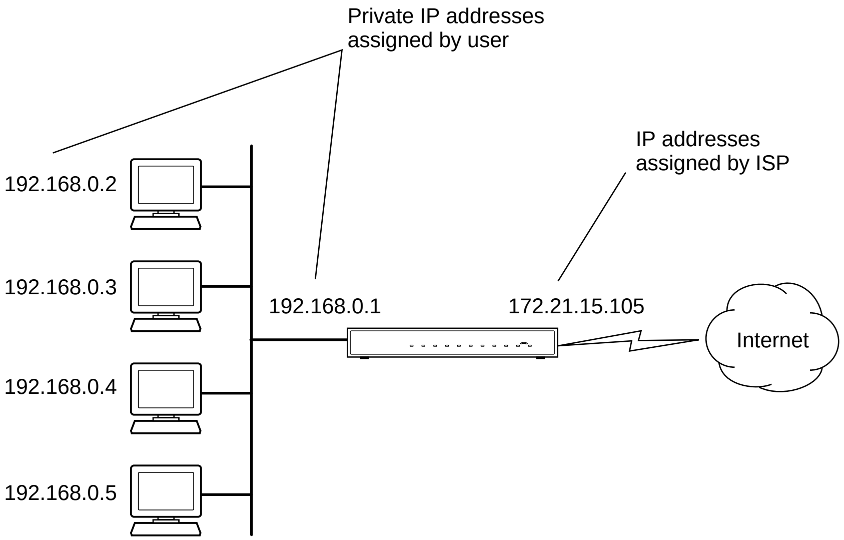


Figure 11-3: Single IP Address Operation Using NAT

This scheme offers the additional benefit of firewall-like protection because the internal LAN addresses are *not* available to the Internet through the translated connection. All incoming inquiries are filtered out by the router. This filtering can prevent intruders from probing your system. However, using port forwarding, you can allow one PC (for example, a Web server) on your local network to be accessible to outside users.

MAC Addresses and Address Resolution Protocol

An IP address alone cannot be used to deliver data from one LAN device to another. To send data between LAN devices, you must convert the IP address of the destination device to its media access control (MAC) address. Each device on an Ethernet network has a unique MAC address, which is a 48-bit number assigned to each device by the manufacturer. The technique that associates the IP address with a MAC address is known as address resolution. Internet Protocol uses the Address Resolution Protocol (ARP) to resolve MAC addresses.

If a device sends data to another station on the network and the destination MAC address is not yet recorded, ARP is used. An ARP request is broadcast onto the network. All stations on the network receive and read the request. The destination IP address for the chosen station is included as part of the message so that only the station with this IP address responds to the ARP request. All other stations discard the request.

Related Documents

The station with the correct IP address responds with its own MAC address directly to the sending device. The receiving station provides the transmitting station with the required destination MAC address. The IP address data and MAC address data for each station are held in an ARP table. The next time data is sent, the address can be obtained from the address information in the table.

For more information about address assignment, refer to the IETF documents RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*.

For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT).*

Domain Name Server

Many of the resources on the Internet can be addressed by simple descriptive names, such as *www.NETGEAR.com*. This addressing is very helpful at the application level, but the descriptive name must be translated to an IP address in order for a user to actually contact the resource. Just as a telephone directory maps names to phone numbers, or as an ARP table maps IP addresses to MAC addresses, a domain name system (DNS) server maps descriptive names of network resources to IP addresses.

When a PC accesses a resource by its descriptive name, it first contacts a DNS server to obtain the IP address of the resource. The PC sends the desired message using the IP address. Many large organizations, such as ISPs, maintain their own DNS servers and allow their customers to use the servers to look up addresses.

IP Configuration by DHCP

When an IP-based local area network is installed, each PC must be configured with an IP address. If the computers need to access the Internet, they should also be configured with a gateway address and one or more DNS server addresses. As an alternative to manual configuration, there is a method by which each PC on the network can automatically obtain this configuration information. A device on the network may act as a Dynamic Host Configuration Protocol (DHCP) server. The DHCP server stores a list or pool of IP addresses, along with other information (such as gateway and DNS addresses) that it may assign to the other devices on the network. The FWG114P v2 Wireless Firewall/Print Server has the capacity to act as a DHCP server.

The FWG114P v2 Wireless Firewall/Print Server also functions as a DHCP client when connecting to the ISP. The firewall can automatically obtain an IP address, subnet mask, DNS server addresses, and a gateway address if the ISP provides this information by DHCP.

Internet Security and Firewalls

When your LAN connects to the Internet through a router, an opportunity is created for outsiders to access or disrupt your network. A NAT router provides some protection because by the very nature of the Network Address Translation (NAT) process, the network behind the NAT router is shielded from access by outsiders on the Internet. However, there are methods by which a determined hacker can possibly obtain information about your network or at the least can disrupt your Internet access. A greater degree of protection is provided by a firewall router.

What is a Firewall?

A firewall is a device that protects one network from another, while allowing communication between the two. A firewall incorporates the functions of the NAT router, while adding features for dealing with a hacker intrusion or attack. Several known types of intrusion or attack can be recognized when they occur. When an incident is detected, the firewall can log details of the attempt, and can optionally send e-mail to an administrator notifying them of the incident. Using information from the log, the administrator can take action with the ISP of the hacker. In some types of intrusions, the firewall can fend off the hacker by discarding all further packets from the hacker’s IP address for a period of time.

Stateful Packet Inspection

Unlike simple Internet sharing routers, a firewall uses a process called stateful packet inspection to ensure secure firewall filtering to protect your network from attacks and intrusions. Since user-level applications, such as FTP and Web browsers can create complex patterns of network traffic, it is necessary for the firewall to analyze groups of network connection "states." Using stateful packet inspection, an incoming packet is intercepted at the network layer and then analyzed for state-related information associated with all network connections. A central cache within the firewall keeps track of the state information associated with all network connections. All traffic passing through the firewall is analyzed against the state of these connections in order to determine whether or not it will be allowed to pass through or be rejected.

Denial of Service Attack

A hacker may be able to prevent your network from operating or communicating by launching a Denial of Service (DoS) attack. The method used for, such an attack can be as simple as merely flooding your site with more requests than it can handle. A more sophisticated attack may attempt to exploit some weakness in the operating system used by your router or gateway. Some operating systems can be disrupted by simply sending a packet with incorrect length information.

Ethernet Cabling

Although Ethernet networks originally used thick or thin coaxial cable, most installations currently use unshielded twisted pair (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. A normal straight-through UTP Ethernet cable follows the EIA568B standard wiring as described below in Table B-1

.

Table B-1. UTP Ethernet cable wiring, straight-through

Pin	Wire color	Signal
1	Orange/White	Transmit (Tx) +
2	Orange	Transmit (Tx) -
3	Green/White	Receive (Rx) +
4	Blue	
5	Blue/White	
6	Green	Receive (Rx) -
7	Brown/White	
8	Brown	

Category 5 Cable Quality

Category 5 distributed cable that meets ANSI/EIA/TIA-568-A building wiring standards can be a maximum of 328 feet (ft.) or 100 meters (m) in length, divided as follows:

20 ft. (6 m) between the hub and the patch panel (if used)

295 ft. (90 m) from the wiring closet to the wall outlet

10 ft. (3 m) from the wall outlet to the desktop device

The patch panel and other connecting hardware must meet the requirements for 100 Mbps operation (Category 5). Only 0.5 inch (1.5 cm) of untwist in the wire pair is allowed at any termination point.

A twisted pair Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or Cat 5, by the Electronic Industry Association (EIA). This rating will be printed on the cable jacket. A Category 5 cable will meet specified requirements regarding loss and crosstalk. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

Inside Twisted Pair Cables

For two devices to communicate, the transmitter of each device must be connected to the receiver of the other device. The crossover function is usually implemented internally as part of the circuitry in the device. Computers and workstation adapter cards are usually media-dependent interface ports, called MDI or uplink ports. Most repeaters and switch ports are configured as media-dependent interfaces with built-in crossover ports, called MDI-X or normal ports. Auto Uplink technology automatically senses which connection, MDI or MDI-X, is needed and makes the right connection.

Figure B-1 illustrates straight-through twisted pair cable.

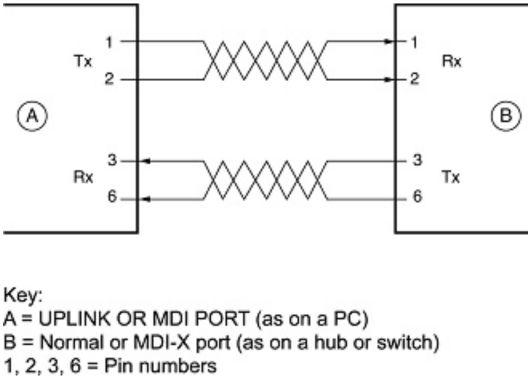

1
Tx
2
A
3
Rx
6
1
Rx
2
B
3
Tx
6
Key:
A = UPLINK OR MDI PORT (as on a PC)
B = Normal or MDI-X port (as on a hub or switch)
1, 2, 3, 6 = Pin numbers

Figure B-1: Straight-Through Twisted-Pair Cable

Figure B-2 illustrates crossover twisted pair cable.

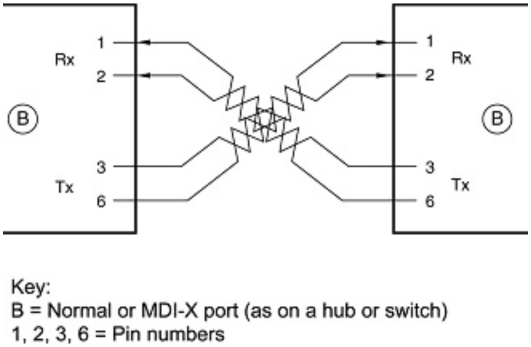


Figure B-2: Crossover Twisted-Pair Cable

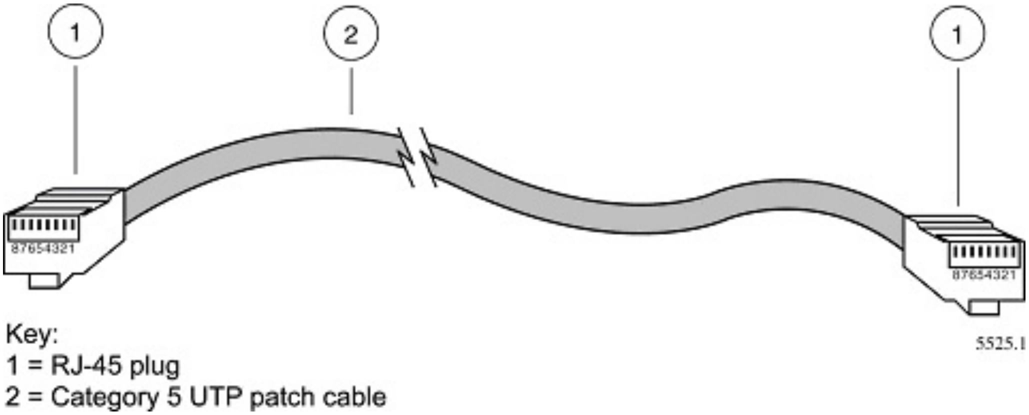


Figure B-3: Category 5 UTP Cable with Male RJ-45 Plug at Each End

Note: Flat “silver satin” telephone cable may have the same RJ-45 plug. However, using telephone cable results in excessive collisions, causing the attached port to be partitioned or disconnected from the network.

Uplink Switches, Crossover Cables, and MDI/MDIX Switching

In the wiring table above, the concept of transmit and receive are from the perspective of the PC, which is wired as Media Dependant Interface (MDI). In this wiring, the PC transmits on pins 1 and 2. At the hub, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X).

When connecting a PC to a PC, or a hub port to another hub port, the transmit pair must be exchanged with the receive pair. This exchange is done by one of two mechanisms. Most hubs provide an Uplink switch which will exchange the pairs on one port, allowing that port to be connected to another hub using a normal Ethernet cable. The second method is to use a crossover cable, which is a special cable in which the transmit and receive pairs are exchanged at one of the two cable connectors. Crossover cables are often unmarked as such, and must be identified by comparing the two connectors. Since the cable connectors are clear plastic, it is easy to place them side by side and view the order of the wire colors on each. On a straight-through cable, the color order will be the same on both connectors. On a crossover cable, the orange and blue pairs will be exchanged from one connector to the other.

The FWG114P v2 Wireless Firewall/Print Server incorporates Auto Uplink™ technology (also called MDI/MDIX). Each LOCAL Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a normal connection (e.g. connecting to a PC) or an uplink connection (e.g. connecting to a router, 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.

Appendix C
Preparing Your Network

This appendix describes how to prepare your network to connect to the Internet through the ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2 and how to verify the readiness of broadband Internet service from an Internet service provider (ISP).

➡	**Note:** If an ISP technician configured your computer during the installation of a broadband modem, or if you configured it using instructions provided by your ISP, you may need to copy the current configuration information for use in the configuration of your firewall. Write down this information before reconfiguring your computers. Refer to "Obtaining ISP Configuration Information for Windows Computers" on page C-10 or "Obtaining ISP Configuration Information for Macintosh Computers" on page C-11 for further information.

Preparing Your Computers for TCP/IP Networking

Computers access the Internet using a protocol called TCP/IP (Transmission Control Protocol/ Internet Protocol). Each computer on your network must have TCP/IP installed and selected as its networking protocol. If a Network Interface Card (NIC) is already installed in your PC, then TCP/ IP is probably already installed as well.

Most operating systems include the software components you need for networking with TCP/IP:

- Windows® 95 or later includes the software components for establishing a TCP/IP network.
- Windows 3.1 does not include a TCP/IP component. You need to purchase a third-party TCP/ IP application package, such as NetManage Chameleon.
- Macintosh Operating System 7 or later includes the software components for establishing a TCP/IP network.
- All versions of UNIX® or Linux® include TCP/IP components. Follow the instructions provided with your operating system or networking software to install TCP/IP on your computer.

In your IP network, each PC and the firewall must be assigned unique IP addresses. Each PC must also have certain other IP configuration information, such as a subnet mask (netmask), a domain name server (DNS) address, and a default gateway address. In most cases, you should install TCP/IP so that the PC obtains its specific network configuration information automatically from a DHCP server during bootup. For a detailed explanation of the meaning and purpose of these configuration items, refer to "Appendix B, "Networks, Routing, and Firewall Basics.""

The FWG114P v2 Wireless Firewall/Print Server is shipped preconfigured as a DHCP server. The firewall assigns the following TCP/IP configuration information automatically when the computers are rebooted:

- PC or workstation IP addresses—192.168.0.2 through 192.168.0.254
- Subnet mask—255.255.255.0
- Gateway address (the firewall)—192.168.0.1

These addresses are part of the IETF-designated private address range for use in private networks.

Configuring Windows 95, 98, and Me for TCP/IP Networking

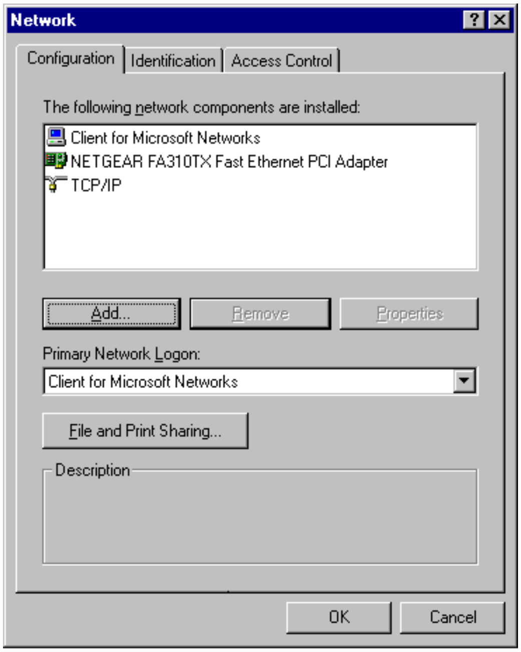
As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Install or Verify Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.

   The Network window opens, which displays a list of installed components:



The following network components are installed:

- Client for Microsoft Networks
- NETGEAR FA310TX Fast Ethernet PCI Adapter
- TCP/IP

Primary Network Logon: Client for Microsoft Networks

You must have an Ethernet adapter, the TCP/IP protocol, and Client for Microsoft Networks.

Note: It is not necessary to remove any other network components shown in the Network window in order to install the adapter, TCP/IP, or Client for Microsoft Networks.

If you need to install a new adapter, follow these steps:

a. Click the Add button.

b. Select Adapter, and then click Add.

c. Select the manufacturer and model of your Ethernet adapter, and then click OK.

If you need TCP/IP:

a. Click the Add button.

b. Select Protocol, and then click Add.

c. Select Microsoft.

d. Select TCP/IP, and then click OK.

If you need Client for Microsoft Networks:

a. Click the Add button.

b. Select Client, and then click Add.

c. Select Microsoft.

d. Select Client for Microsoft Networks, and then click OK.

3. Restart your PC for the changes to take effect.

Enabling DHCP to Automatically Configure TCP/IP Settings

After the TCP/IP protocol components are installed, each PC must be assigned specific information about itself and resources that are available on its network. The simplest way to configure this information is to allow the PC to obtain the information from the internal DHCP server of the FWG114P v2 Wireless Firewall/Print Server. To use DHCP with the recommended default addresses, follow these steps:

1. Connect all computers to the firewall, then restart the firewall and allow it to boot.
2. On each attached PC, open the Network control panel (refer to the previous section) and select the Configuration tab.
3. From the components list, select TCP/IP->(your Ethernet adapter) and click Properties.
4. In the IP Address tab, select “Obtain an IP address automatically”.
5. Select the Gateway tab.
6. If any gateways are shown, remove them.
7. Click OK.
8. Restart the PC.

Repeat steps 2 through 8 for each PC on your network.

Selecting Windows’ Internet Access Method

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Internet Options icon.
3. Select “I want to set up my Internet connection manually” or “I want to connect through a Local Area Network” and click Next.
4. Select “I want to connect through a Local Area Network” and click Next.

5. Uncheck all boxes in the LAN Internet Configuration screen and click Next.
6. Proceed to the end of the Wizard.

Verifying TCP/IP Properties

After your PC is configured and has rebooted, you can check the TCP/IP configuration using the utility *winipcfg.exe*:

1. On the Windows taskbar, click the Start button, and then click Run.
2. Type **`winipcfg`**, and then click OK.

   The IP Configuration window opens, which lists (among other things), your IP address, subnet mask, and default gateway.
3. From the drop-down box, select your Ethernet adapter.

   The window is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

   - The IP address is between 192.168.0.2 and 192.168.0.254
   - The subnet mask is 255.255.255.0
   - The default gateway is 192.168.0.1

Configuring Windows NT, 2000 or XP for IP Networking

As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Installing or Verifying Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network and Dialup Connections icon.
3. If an Ethernet adapter is present in your PC, you should see an entry for Local Area Connection. Double-click that entry.
4. Select Properties.

5. Verify that ‘Client for Microsoft Networks’ and ‘Internet Protocol (TCP/IP)’ are present. If not, select Install and add them.
6. Select ‘Internet Protocol (TCP/IP)’, click Properties, and verify that “Obtain an IP address automatically is selected.
7. Click OK and close all Network and Dialup Connections windows.
8. Make sure your PC is connected to the firewall, then reboot your PC.

Verifying TCP/IP Properties

To check your PC’s TCP/IP configuration:

1. On the Windows taskbar, click the Start button, and then click Run.

   The Run window opens.
2. Type **`cmd`** and then click OK.

   A command window opens
3. Type **`ipconfig /all`**

   Your IP Configuration information will be listed, and should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

   - The IP address is between 192.168.0.2 and 192.168.0.254
   - The subnet mask is 255.255.255.0
   - The default gateway is 192.168.0.1
4. Type **`exit`**

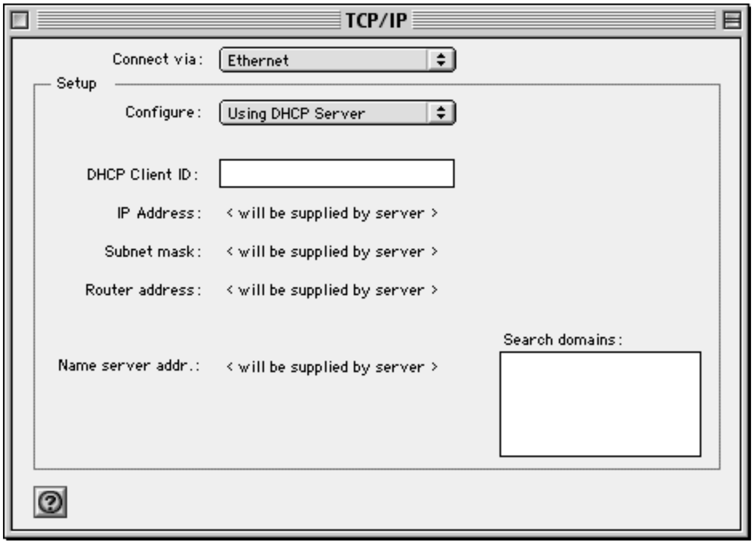
Configuring the Macintosh for TCP/IP Networking

Beginning with Macintosh Operating System 7, TCP/IP is already installed on the Macintosh. On each networked Macintosh, you will need to configure TCP/IP to use DHCP.

MacOS 8.6 or 9.x

1. From the Apple menu, select Control Panels, then TCP/IP.

The TCP/IP Control Panel opens:



TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Name server addr.: < will be supplied by server >

Search domains:

2. From the “Connect via” box, select your Macintosh’s Ethernet interface.
3. From the “Configure” box, select Using DHCP Server.

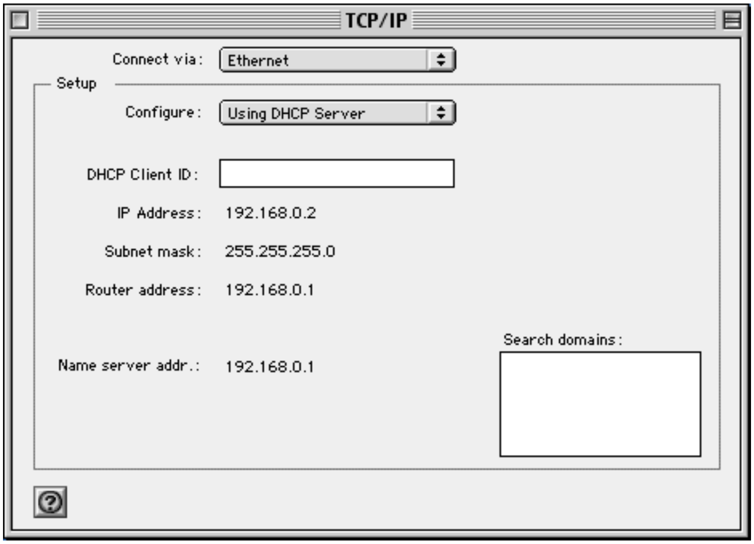
   You can leave the DHCP Client ID box empty.
4. Close the TCP/IP Control Panel.
5. Repeat this for each Macintosh on your network.

MacOS X

1. From the Apple menu, choose System Preferences, then Network.
2. If not already selected, select Built-in Ethernet in the Configure list.
3. If not already selected, Select Using DHCP in the TCP/IP tab.
4. Click Save.

Verifying TCP/IP Properties for Macintosh Computers

After your Macintosh is configured and has rebooted, you can check the TCP/IP configuration by returning to the TCP/IP Control Panel. From the Apple menu, select Control Panels, then TCP/IP.



Connect via: Ethernet

Configure: Using DHCP Server

DHCP Client ID:

IP Address: 192.168.0.2

Subnet mask: 255.255.255.0

Router address: 192.168.0.1

Name server addr.: 192.168.0.1

The panel is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

- The IP Address is between 192.168.0.2 and 192.168.0.254
- The Subnet mask is 255.255.255.0
- The Router address is 192.168.0.1

If you do not see these values, you may need to restart your Macintosh or you may need to switch the "Configure" setting to a different option, then back again to "Using DHCP Server".

Verifying the Readiness of Your Internet Account

For broadband access to the Internet, you need to contract with an Internet service provider (ISP) for a single-user Internet access account using a cable modem or DSL modem. This modem must be a separate physical box (not a card) and must provide an Ethernet port intended for connection to a Network Interface Card (NIC) in a computer. Your firewall does not support a USB-connected broadband modem.

For a single-user Internet account, your ISP supplies TCP/IP configuration information for one computer. With a typical account, much of the configuration information is dynamically assigned when your PC is first booted up while connected to the ISP, and you will not need to know that dynamic information.

In order to share the Internet connection among several computers, your firewall takes the place of the single PC, and you need to configure it with the TCP/IP information that the single PC would normally use. When the firewall’s Internet port is connected to the broadband modem, the firewall appears to be a single PC to the ISP. The firewall then allows the computers on the local network to masquerade as the single PC to access the Internet through the broadband modem. The method used by the firewall to accomplish this is called Network Address Translation (NAT) or IP masquerading.

Are Login Protocols Used?

Some ISPs require a special login protocol, in which you must enter a login name and password in order to access the Internet. If you normally log in to your Internet account by running a program, such as WinPOET or EnterNet, then your account uses PPP over Ethernet (PPPoE).

When you configure your router, you will need to enter your login name and password in the router’s configuration menus. After your network and firewall are configured, the firewall will perform the login task when needed, and you will no longer need to run the login program from your PC. It is not necessary to uninstall the login program.

What Is Your Configuration Information?

More and more, ISPs are dynamically assigning configuration information. However, if your ISP does not dynamically assign configuration information but instead uses fixed configurations, your ISP should have given you the following basic information for your account:

- An IP address and subnet mask
- A gateway IP address, which is the address of the ISP's router
- One or more domain name server (DNS) IP addresses
- Host name and domain suffix

  For example, your account's full server names may look like this:

  `mail.xxx.yyy.com`

  In this example, the domain suffix is `xxx.yyy.com`.

If any of these items are dynamically supplied by the ISP, your firewall automatically acquires them.

If an ISP technician configured your PC during the installation of the broadband modem, or if you configured it using instructions provided by your ISP, you need to copy the configuration information from your PC's Network TCP/IP Properties window or Macintosh TCP/IP Control Panel before reconfiguring your PC for use with the firewall. These procedures are described next.

Obtaining ISP Configuration Information for Windows Computers

As mentioned above, you may need to collect configuration information from your PC so that you can use this information when you configure the FWG114P v2 Wireless Firewall/Print Server. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the firewall for Internet access:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.

   The Network window opens, which displays a list of installed components.
3. Select TCP/IP, and then click Properties.

   The TCP/IP Properties dialog box opens.
4. Select the IP Address tab.

   If an IP address and subnet mask are shown, write down the information. If an address is present, your account uses a fixed (static) IP address. If no address is present, your account uses a dynamically-assigned IP address. Click "Obtain an IP address automatically".
5. Select the Gateway tab.

If an IP address appears under Installed Gateways, write down the address. This is the ISP's gateway address. Select the address and then click Remove to remove the gateway address.

6. Select the DNS Configuration tab.

   If any DNS server addresses are shown, write down the addresses. If any information appears in the Host or Domain information box, write it down. Click Disable DNS.

7. Click OK to save your changes and close the TCP/IP Properties dialog box.

   You are returned to the Network window.

8. Click OK.

9. Reboot your PC at the prompt. You may also be prompted to insert your Windows CD.

Obtaining ISP Configuration Information for Macintosh Computers

As mentioned above, you may need to collect configuration information from your Macintosh so that you can use this information when you configure the FWG114P v2 Wireless Firewall/Print Server. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the firewall for Internet access:

1. From the Apple menu, select Control Panels, then TCP/IP.

   The TCP/IP Control Panel opens, which displays a list of configuration settings. If the “Configure” setting is “Using DHCP Server”, your account uses a dynamically-assigned IP address. In this case, close the Control Panel and skip the rest of this section.

2. If an IP address and subnet mask are shown, write down the information.

3. If an IP address appears under Router address, write down the address. This is the ISP's gateway address.

4. If any Name Server addresses are shown, write down the addresses. These are your ISP's DNS addresses.

5. If any information appears in the Search domains information box, write it down.

6. Change the “Configure” setting to “Using DHCP Server”.

7. Close the TCP/IP Control Panel.

Restarting the Network

Once you have set up your computers to work with the firewall, you must reset the network for the devices to be able to communicate correctly. Restart any computer that is connected to the firewall.

After configuring all of your computers for TCP/IP networking and restarting them, and connecting them to the local network of your FWG114P v2 Wireless Firewall/Print Server, you are ready to access and configure the firewall.

Appendix D
Firewall Log Formats

Action List

Drop:	Packet dropped by Firewall current inbound or outbound rules.
Reset:	TCP session reset by Firewall.
Forward:	Packet forwarded by Firewall to the next hop based on matching the criteria in the rules table.
Receive:	Packet was permitted by the firewall rules and modified prior to being forwarded and/or replied to.

Field List

<DATE><TIME>:	Log's date and time
<EVENT>:	Event is that access the device or access other host via the device
<PKT_TYPE>:	Packet type pass Firewall
<SRC_IP><DST_IP>:	IP address in the packet
<SRC_PORT><DST_PORT>:	Port in the packet
<SRC_INF><DST_INF>:	Include `LAN` and `WAN` (optional)
<ACTION>:	As `Action List` referenced
<DESCRIPTION>:	A complement to the log (optional)
<DIRECTION>:	Inbound and Outbound
<SERVICE>:	Firewall costumed service

Outbound Log

Outgoing packets that match the Firewall rules are logged.

The format is:

```
<DATE> <TIME> <PKT_TYPE> <SRC_IP> <SRC_INF> <DST_IP > <DST_INF>
<ACTION><DESCRIPTION>

[Fri, 2003-12-05 22:19:42] - UDP Packet - Source:172.31.12.233,138 ,WAN -
Destination:172.31.12.255,138 ,LAN [Drop] - [Inbound Default rule match]
[Fri, 2003-12-05 22:35:04] - TCP Packet - Source:172.31.12.156,34239 ,WAN -
Destination:192.168.0.10,21[FTP Control] ,LAN [Forward] - [Inbound Rule(1)
match]
[Fri, 2003-12-05 22:35:11] - UDP Packet - Source:172.31.12.200,138 ,WAN -
Destination:172.31.12.255,138 ,LAN [Forward] - [Inbound Rule(1) not match]

Notes:
SRC_INF = WAN
DST_INF = LAN
DESCRIPTION = "Inbound rule match", "Inbound Default rule match"
PKT_TYPE = "UDP packet", "TCP connection", "ICMP packet"
```

Inbound Log

Incoming packets that match the Firewall rules are logged.

The format is:

```
<DATE> <TIME> <PKT_TYPE> <SRC_IP> <SRC_INF> <DST_IP > <DST_INF>
<ACTION><DESCRIPTION>

[Fri, 2003-12-05 22:59:56] - ICMP Packet [Echo Request] - Source:192.168.0.10,LAN
- Destination:192.168.0.1,WAN [Forward] - [Outbound Default rule match]

[Fri, 2003-12-05 23:00:58] - ICMP Packet [Echo Request] - Source:192.168.0.10,LAN
- Destination:172.31.12.200,WAN [Forward] - [Outbound Default rule match]

[Fri, 2003-12-05 23:02:30] - TCP Packet - Source:192.168.0.10,3472 ,LAN -
Destination:216.239.39.99,80[HTTP] ,WAN [Forward] - [Outbound Default rule
match]

Notes:
SRC_INF = LAN
DST_INF = WAN
DESCRIPTION = "Outbound rule match", "Outbound Default rule match"
PKT_TYPE = "UDP packet", "TCP connection", "ICMP packet"
```

Other IP Traffic

Some special packets matching the Firewall rules, like VPN connection, etc. are logged.

The format is:

```
<DATE><TIME><PKT_TYPE>< SRC_IP><SRC_PORT ><SRC_INF>< DST_IP><DST_PORT
><DST_PORT><ACTION><DESCRIPTION>

<DATE><TIME> <PKT_TYPE> <SRC_IP> <SRC_INF> <DST_IP> <DST_INF> <ACTION>
<DESCRIPTION>

[Wed, 2003-07-30 17:43:28] - IPSEC Packet - Source: 64.3.3.201, 37180 WAN -
Destination: 10.10.10.4,80[HTTP] LAN - [Drop] [VPN Packet]

[Wed, 2003-07-30 18:44:50] - IP Packet [Type Field: 321] - Source 18.7.21.69
192.168.0.3 - [Drop]

Notes:
DESCRIPTION = "VPN Packet"
PKT_TYPE = "GRE", "AH", "ESP", "IP packet [Type Field: Num]", "IPSEC"
ACTION = "Forward", "Drop"
```

Router Operation

Operations that the router initiates are logged.

The format is:

```
<DATE><TIME><EVENT>

[Wed, 2003-07-30 16:30:59] - Log emailed
[Wed, 2003-07-30 13:38:31] - NETGEAR activated
[Wed, 2003-07-30 13:42:01] - NTP Reply Invalid
```

The format is:

```
<DATE><TIME><EVENT><DST_IP>
<DATE><TIME><EVENT><SRC_IP>

[Wed, 2003-07-30 16:32:33] - Send out NTP Request to 207.46.130.100
[Wed, 2003-07-30 16:35:27] - Receive NTP Reply from 207.46.130.100
```

Other Connections and Traffic to this Router

The format is:

```
<DATE><TIME>< PKT_TYPE ><SRC_IP><DST_IP><ACTION>
```

```
[Fri, 2003-12-05 22:31:27] - ICMP Packet[Echo Request] - Source: 192.168.0.10 -
Destination: 192.168.0.1 - [Receive]
[Wed, 2003-07-30 16:34:56] - ICMP Packet[Type: 238]  - Source:  64.3.3.201 -
Destination: 192.168.0.3 - [Drop]
[Fri, 2003-12-05 22:59:56] - ICMP Packet[Echo Request] - Source:192.168.0.10 -
Destination:192.168.0.1 - [Receive]
```

The format is:

```
<DATE><TIME><EVENT>< SRC_IP><SRC_PORT ><SRC_INF><
DST_IP><DST_PORT><DST_INF><ACTION>
```

```
[Wed, 2003-07-30 16:24:23] - UDP Packet - Source: 207.46.130.100 WAN -
Destination: 10.10.10.4,1234 LAN - [Drop]
[Wed, 2003-07-30 17:48:09] - TCP Packet[SYN] - Source: 64.3.3.201,65534 WAN -
Destination: 10.10.10.4,1765 LAN - [Receive]
[Fri, 2003-12-05 22:07:11] - IP Packet [Type Field:8], from 20.97.173.18 to
172.31.12.157 - [Drop]
```

```
Notes:
ACTION = "Drop", "Receive"
EVENT = "ICMP Packet", "UDP Packet", "TCP Packet", "IP Packet"
```

DoS Attack/Scan

Common attacks and scans are logged.

The format is:

```
<DATE><TIME><PKT_TYPE>< SRC_IP><SRC_PORT ><SRC_INF>< DST_IP><DST_PORT
><DST_PORT><ACTION><DESCRIPTION>
<DATE> <TIME> <PKT_TYPE> <SRC_IP> <SRC_INF> <DST_IP> <DST_INF> <ACTION>
<DESCRIPTION>

[Fri, 2003-12-05 21:22:07] - TCP Packet - Source:172.31.12.156,54611 ,WAN -
Destination:172.31.12.157,134 ,LAN [Drop] - [FIN Scan]
[Fri, 2003-12-05 21:22:38] - TCP Packet - Source:172.31.12.156,59937 ,WAN -
Destination:172.31.12.157,670 ,LAN [Drop] - [Nmap Xmas Scan]
[Fri, 2003-12-05 21:23:06] - TCP Packet - Source:172.31.12.156,39860 ,WAN -
Destination:172.31.12.157,18000 ,LAN [Drop] - [Null Scan]
[Fri, 2003-12-05 21:27:55] - TCP Packet - Source:172.31.12.156,38009 ,WAN -
Destination:172.31.12.157,15220 ,LAN [Drop] - [Full Sapu Scan]
[Fri, 2003-12-05 21:28:56] - TCP Packet - Source:172.31.12.156,35128 ,WAN -
Destination:172.31.12.157,38728 ,LAN [Drop] - [Full Xmas Scan]
[Fri, 2003-12-05 21:30:30] - IP Packet - Source:227.113.223.77,WAN -
Destination:172.31.12.157,LAN [Drop] - [Fragment Attack]
[Fri, 2003-12-05 21:30:30] - IP Packet - Source:20.97.173.18,WAN -
Destination:172.31.12.157,LAN [Drop] - [Targa3 Attack]
[Fri, 2003-12-05 21:30:30] - TCP Packet - Source:3.130.176.84,37860 ,WAN -
Destination:172.31.12.157,63881 ,LAN [Drop] - [Vecna Scan]
[Fri, 2003-12-05 21:30:31] - ICMP Packet [Type 238]  - Source:100.110.182.63,WAN
- Destination:172.31.12.157,LAN [Drop] - [ICMP Flood]
[Fri, 2003-12-05 21:33:52] - UDP Packet - Source:127.0.0.1,0 ,WAN -
Destination:172.31.12.157,0 ,LAN [Drop] - [Fragment Attack]
[Fri, 2003-12-05 19:20:00] - TCP Session - Source:54.148.179.175,58595 ,LAN -
Destination:192.168.0.1,20[FTP Data] ,WAN [Reset] - [SYN Flood]
[Fri, 2003-12-05 19:21:22] - UDP Packet - Source:172.31.12.156,7 ,LAN -
Destination:172.31.12.157,7 ,WAN [Drop] - [UDP Flood]
[Fri, 2003-12-05 20:59:08] - ICMP Echo Request packet - Source:192.168.0.5,LAN -
Destination:172.31.12.99,WAN [Drop] - [ICMP Flood]
[Fri, 2003-12-05 18:07:29] - TCP Packet - Source:192.168.0.10,1725 ,LAN -
Destination:61.177.58.50,1352 ,WAN [Drop] - [TCP incomplete sessions overflow]
[Fri, 2003-12-05 21:11:24] - TCP Packet - Source:192.168.0.10,2342 ,LAN -
Destination:61.177.58.50,1352 ,WAN [Drop] - [First TCP Packet not SYN]

Notes:
DESCRIPTION = "SYN Flood", "UDP Flood", "ICMP Flood", "IP Spoofing", "TearDrop",
"Brute Force", "Ping of Death", "Fragment Attack", "Targa3 Attack", "Big Bomb"
"SYN with Data", "Full Xmas Scan", "Full Head Scan", "Full Sapu Scan", "FIN
Scan", "SYN FIN Scan", "Null Scan", "Nmap Xmas Scan", "Vecna Scan", "Tcp SYN RES
Set", "Other Scan"
"TCP incomplete sessions overflow", "TCP preconnect traffic", "TCP invalid
traffic", "First TCP Packet not SYN", "First TCP Packet with no SYN"

<DATE><TIME><PKT_TYPE>< SRC_IP >< DST_IP><ACTION>

[Wed, 2003-07-30 17:45:17] - TCP Packet [Malformed, Length=896] - Source:
64.3.3.201 - Destination: 10.10.10.4 - [Drop]
[Wed, 2003-07-30 17:45:17] - TCP Packet [Malformed, Length=1000] - Source:
64.3.3.201- Destination:  10.10.10.4 - [Forward]

Notes:
PKT_TYPE = "TCP", "UDP", "ICMP", "Proto: Number"
```

Access Block Site

If keyword blocking is enabled and a keyword is specified, attempts to access a site whose URL contains a specified keyword are logged.

The format is

```
<DATE> <TIME> <EVENT> <SRC_IP> <SRC_INF> <DST_IP> <DST_INF> <ACTION>

[Fri, 2003-12-05 23:01:47] - Attempt to access blocked sites -
Source:192.168.0.10,LAN - Destination:www.google.com/,WAN - [Drop]

Notes:
EVENT = Attempt to access blocked sites
SRC_INF = LAN
DST_INF = WAN
```

All Web Sites and News Groups Visited

All Web sites and News groups that you visit are logged.

The format is

```
<DATE> <TIME> <EVENT> <SRC_IP> <SRC_INF> <DST_IP> <DST_INF> <ACTION>

[Fri, 2003-12-05 23:03:49] - Access site - Source:192.168.0.10,LAN -
Destination:euro.allyes.com,WAN - [Forward]

Notes:
EVENT = Attempt to access blocked sites
SRC_INF = LAN or WAN
DST_INF = WAN or LAN
```

System Admin Sessions

Administrator session logins and failed attempts are logged, as well as manual or idle-time logouts.

The format is:

```
<DATE><TIME><EVENT ><SRC_IP>
<DATE><TIME><EVENT ><SRC_IP><SRC_PORT><DST_IP><DST_PORT><ACTION>

[Fri, 2003-12-05 21:07:43] - Administrator login successful - IP:192.168.0.10
[Fri, 2003-12-05 21:09:16] - Administrator logout - IP:192.168.0.10
[Fri, 2003-12-05 21:09:31] - Administrator login fail, Username error -
IP:192.168.0.10
[Fri, 2003-12-05 21:09:25] - Administrator login fail, Password error -
IP:192.168.0.10
[Fri, 2003-12-05 21:16:15] - Login screen timed out - IP:192.168.0.10
[Fri, 2003-12-05 21:07:43] - Administrator Interface Connecting[TCP] - Source
192.168.0.10,2440 - Destination 192.168.0.1,80 - [Receive]

Notes:
ACTION: Receive or Drop
```

Policy Administration LOG

```
<DATE> <TIME> <EVENT> <DIRECTION> <SERVICE>< DESCRIPTION >

[Fri, 2003-12-05 21:48:41] - Administrator Action - Inbound Policy to Service
[BGP] is Added
[Fri, 2003-12-05 21:49:41] - Administrator Action - Outbound Policy to Service
[BGP] is Added
[Fri, 2003-12-05 21:50:14] - Administrator Action - Inbound Policy to Service
[BGP] is Modified
[Fri, 2003-12-05 21:50:57] - Administrator Action - Outbound Policy to Service
[BGP] is Modified
[Fri, 2003-12-05 21:51:14] - Administrator Action - Inbound Policy to Service
[BGP] is Deleted
[Fri, 2003-12-05 21:52:12] - Administrator Action - Inbound Policy to Service
[BGP] is Moved to Index [0]
[Fri, 2003-12-05 21:54:41] - Administrator Action - Outbound Policy to Service
[FTP] is Moved to Index [1]
[Fri, 2003-12-05 22:01:47] - Administrator Action - Inbound Policy to Service
[BGP] is changed to Disable
[Fri, 2003-12-05 22:02:14] - Administrator Action - Inbound Policy to Service
[BGP] is changed to Enable
[Fri, 2003-12-05 22:02:35] - Administrator Action - Outbound Policy to Service
[NFS] is changed to Disable
[Fri, 2003-12-05 22:02:52] - Administrator Action - Outbound Policy to Service
[NFS] is changed to Enable

Notes:
DIRECTION: Inbound or Outbound
SERVICE: Supported service name
```

Appendix E
Wireless Networking Basics

This chapter provides an overview of Wireless networking.

Wireless Networking Overview

The FWG114P v2 Wireless Firewall/Print Server conforms to the Institute of Electrical and Electronics Engineers (IEEE) 802.11b and 802.11g standards for wireless LANs (WLANs). On an 802.11b or g wireless link, data is encoded using direct-sequence spread-spectrum (DSSS) technology and is transmitted in the unlicensed radio spectrum at 2.5GHz. The maximum data rate for the 802.11b wireless link is 11 Mbps, but it will automatically back down from 11 Mbps to 5.5, 2, and 1 Mbps when the radio signal is weak or when interference is detected. The 802.11g auto rate sensing rates are 1, 2, 5.5, 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

The 802.11 standard is also called Wireless Ethernet or Wi-Fi by the Wireless Ethernet Compatibility Alliance (WECA, see *http://www.wi-fi.net*), an industry standard group promoting interoperability among 802.11 devices. The 802.11 standard offers two methods for configuring a wireless network - ad hoc and infrastructure.

Infrastructure Mode

With a wireless Access Point, you can operate the wireless LAN in the infrastructure mode. This mode provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage, interacting with wireless nodes via an antenna.

In the infrastructure mode, the wireless access point converts airwave data into wired Ethernet data, acting as a bridge between the wired LAN and wireless clients. Connecting multiple Access Points via a wired Ethernet backbone can further extend the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one Access Point domain to another and still maintain seamless network connection.

Ad Hoc Mode (Peer-to-Peer Workgroup)

In an ad hoc network, computers are brought together as needed; thus, there is no structure or fixed points to the network - each node can generally communicate with any other node. There is no Access Point involved in this configuration. This mode enables you to quickly set up a small wireless workgroup and allows workgroup members to exchange data or share printers as supported by Microsoft networking in the various Windows operating systems. Some vendors also refer to ad hoc networking as peer-to-peer group networking.

In this configuration, network packets are directly sent and received by the intended transmitting and receiving stations. As long as the stations are within range of one another, this is the easiest and least expensive way to set up a wireless network.

Network Name: Extended Service Set Identification (ESSID)

The Extended Service Set Identification (ESSID) is one of two types of Service Set Identification (SSID). In an ad hoc wireless network with no access points, the Basic Service Set Identification (BSSID) is used. In an infrastructure wireless network that includes an access point, the ESSID is used, but may still be referred to as SSID.

An SSID is a thirty-two character (maximum) alphanumeric key identifying the name of the wireless local area network. Some vendors refer to the SSID as network name. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.

The ESSID is usually broadcast in the air from an access point. The wireless station sometimes can be configured with the ESSID **ANY.** This means the wireless station will try to associate with whichever access point has the stronger radio frequency (RF) signal, providing that both the access point and wireless station use Open System authentication.

Authentication and WEP Data Encryption

The absence of a physical connection between nodes makes the wireless links vulnerable to eavesdropping and information theft. To provide a certain level of security, the IEEE 802.11 standard has defined these two types of authentication methods:

- **Open System**. With Open System authentication, a wireless computer can join any network and receive any messages that are not encrypted.

- **Shared Key**. With Shared Key authentication, only those PCs that possess the correct authentication key can join the network. By default, IEEE 802.11 wireless devices operate in an Open System network.

Wired Equivalent Privacy (WEP) data encryption is used when the wireless devices are configured to operate in Shared Key authentication mode.

802.11 Authentication

The 802.11 standard defines several services that govern how two 802.11 devices communicate. The following events must occur before an 802.11 Station can communicate with an Ethernet network through an access point, such as the one built in to the FWG114P v2:

1. Turn on the wireless station.
2. The station listens for messages from any access points that are in range.
3. The station finds a message from an access point that has a matching SSID.
4. The station sends an authentication request to the access point.
5. The access point authenticates the station.
6. The station sends an association request to the access point.
7. The access point associates with the station.
8. The station can now communicate with the Ethernet network through the access point.

An access point must authenticate a station before the station can associate with the access point or communicate with the network. The IEEE 802.11 standard defines two types of authentication: Open System and Shared Key.

- Open System Authentication allows any device to join the network, assuming that the device SSID matches the access point SSID. Alternatively, the device can use the “ANY” SSID option to associate with any available Access Point within range, regardless of its SSID.
- Shared Key Authentication requires that the station and the access point have the same WEP Key to authenticate. These two authentication procedures are described below.

Open System Authentication

The following steps occur when two devices use Open System Authentication:

1. The station sends an authentication request to the access point.

2. The access point authenticates the station.
3. The station associates with the access point and joins the network.

This process is illustrated below.

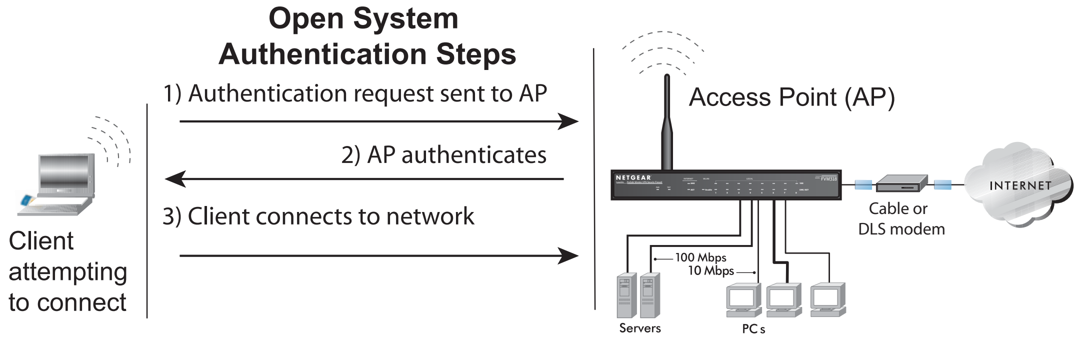


Figure E-1: Open system authentication

Shared Key Authentication

The following steps occur when two devices use Shared Key Authentication:

1. The station sends an authentication request to the access point.
2. The access point sends challenge text to the station.
3. The station uses its configured 64-bit or 128-bit default key to encrypt the challenge text, and sends the encrypted text to the access point.
4. The access point decrypts the encrypted text using its configured WEP Key that corresponds to the station’s default key. The access point compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, then the access point and the station share the same WEP Key and the access point authenticates the station.
5. The station connects to the network.

If the decrypted text does not match the original challenge text (the access point and station do not share the same WEP Key), then the access point will refuse to authenticate the station and the station will be unable to communicate with either the 802.11 network or Ethernet network.

This process is illustrated below.

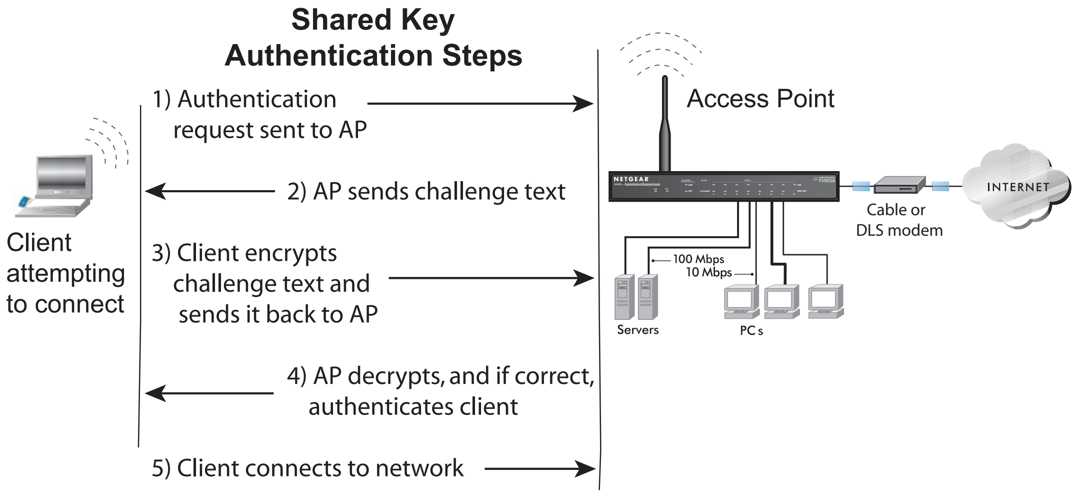

Shared Key
Authentication Steps
1) Authentication request sent to AP
2) AP sends challenge text
3) Client encrypts challenge text and sends it back to AP
4) AP decrypts, and if correct, authenticates client
5) Client connects to network
Client attempting to connect
Access Point
NETGEAR
100 Mbps
10 Mbps
Servers
PC s
Cable or DLS modem
INTERNET

Figure E-2: Shared key authentication

Overview of WEP Parameters

Before enabling WEP on an 802.11 network, you must first consider what type of encryption you require and the key size you want to use. Typically, there are three WEP Encryption options available for 802.11 products:

1. **Do Not Use WEP:** The 802.11 network does not encrypt data. For authentication purposes, the network uses Open System Authentication.

2. **Use WEP for Encryption:** A transmitting 802.11 device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving device decrypts the data using the same WEP Key. For authentication purposes, the network uses Open System Authentication.

3. **Use WEP for Authentication and Encryption:** A transmitting 802.11 device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving device decrypts the data using the same WEP Key. For authentication purposes, the wireless network uses Shared Key Authentication.

Note: Some 802.11 access points also support **Use WEP for Authentication Only** (Shared Key Authentication without data encryption).

Key Size

The IEEE 802.11 standard supports two types of WEP encryption: 40-bit and 128-bit.

The 64-bit WEP data encryption method allows for a five-character (40-bit) input. Additionally, 24 factory-set bits are added to the forty-bit input to generate a 64-bit encryption key. The 24 factory-set bits are not user-configurable). This encryption key will be used to encrypt/decrypt all data transmitted via the wireless interface. Some vendors refer to the 64-bit WEP data encryption as 40-bit WEP data encryption since the user-configurable portion of the encryption key is 40 bits wide.

The 128-bit WEP data encryption method consists of 104 user-configurable bits. Similar to the forty-bit WEP data encryption method, the remaining 24 bits are factory set and not user configurable. Some vendors allow passphrases to be entered instead of the cryptic hexadecimal characters to ease encryption key entry.

128-bit encryption is stronger than 40-bit encryption, but 128-bit encryption may not be available outside of the United States due to U.S. export regulations.

When configured for 40-bit encryption, 802.11 products typically support up to four WEP Keys. Each 40-bit WEP Key is expressed as 5 sets of two hexadecimal digits (0-9 and A-F). For example, “12 34 56 78 90” is a 40-bit WEP Key.

When configured for 128-bit encryption, 802.11 products typically support four WEP Keys but some manufacturers support only one 128-bit key. The 128-bit WEP Key is expressed as 13 sets of two hexadecimal digits (0-9 and A-F). For example, “12 34 56 78 90 AB CD EF 12 34 56 78 90” is a 128-bit WEP Key.

Table E-1: Encryption Key Sizes

Encryption Key Size	# of Hexadecimal Digits	Example of Hexadecimal Key Content
64-bit (24+40)	10	4C72F08AE1
128-bit (24+104)	26	4C72F08AE19D57A3FF6B260037

Note: Typically, 802.11 access points can store up to four 128-bit WEP Keys but some 802.11 client adapters can only store one. Therefore, make sure that your 802.11 access and client adapters’ configurations match.

WEP Configuration Options

The WEP settings must match on all 802.11 devices that are within the same wireless network as identified by the SSID. In general, if your mobile clients will roam between access points, then all of the 802.11 access points and all of the 802.11 client adapters on the network must have the same WEP settings.

Note: Whatever keys you enter for an AP, you must also enter the same keys for the client adapter in the same order. In other words, WEP key 1 on the AP must match WEP key 1 on the client adapter, WEP key 2 on the AP must match WEP key 2 on the client adapter, and so on.

Note: The AP and the client adapters can have different default WEP Keys as long as the keys are in the same order. In other words, the AP can use WEP key 2 as its default key to transmit while a client adapter can use WEP key 3 as its default key to transmit. The two devices will communicate as long as the AP's WEP key 2 is the same as the client's WEP key 2 and the AP's WEP key 3 is the same as the client's WEP key 3.

Wireless Channels

The wireless frequencies used by 802.11b/g networks are discussed below.

IEEE 802.11b/g wireless nodes communicate with each other using radio frequency signals in the ISM (Industrial, Scientific, and Medical) band between 2.4 GHz and 2.5 GHz. Neighboring channels are 5 MHz apart. However, due to spread spectrum effect of the signals, a node sending signals using a particular channel will utilize frequency spectrum 12.5 MHz above and below the center channel frequency. As a result, two separate wireless networks using neighboring channels (for example, channel 1 and channel 2) in the same general vicinity will interfere with each other. Applying two channels that allow the maximum channel separation will decrease the amount of channel cross-talk, and provide a noticeable performance increase over networks with minimal channel separation.

The radio frequency channels used in 802.11b/g networks are listed in Table E-2:

Table E-2: 802.11b/g Radio Frequency Channels

Channel	Center Frequency	Frequency Spread
1	2412 MHz	2399.5 MHz - 2424.5 MHz
2	2417 MHz	2404.5 MHz - 2429.5 MHz
3	2422 MHz	2409.5 MHz - 2434.5 MHz

Table E-2: 802.11b/g Radio Frequency Channels

Channel	Center Frequency	Frequency Spread
4	2427 MHz	2414.5 MHz - 2439.5 MHz
5	2432 MHz	2419.5 MHz - 2444.5 MHz
6	2437 MHz	2424.5 MHz - 2449.5 MHz
7	2442 MHz	2429.5 MHz - 2454.5 MHz
8	2447 MHz	2434.5 MHz - 2459.5 MHz
9	2452 MHz	2439.5 MHz - 2464.5 MHz
10	2457 MHz	2444.5 MHz - 2469.5 MHz
11	2462 MHz	2449.5 MHz - 2474.5 MHz
12	2467 MHz	2454.5 MHz - 2479.5 MHz
13	2472 MHz	2459.5 MHz - 2484.5 MHz

Note: The available channels supported by the wireless products in various countries are different. For example, Channels 1 to 11 are supported in the U.S. and Canada, and Channels 1 to 13 are supported in Europe and Australia.

The preferred channel separation between the channels in neighboring wireless networks is 25 MHz (5 channels). This means that you can apply up to three different channels within your wireless network. There are only 11 usable wireless channels in the United States. It is recommended that you start using channel 1 and grow to use channel 6, and 11 when necessary, as these three channels do not overlap.

WPA Wireless Security

Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancements that increase the level of data protection and access control for existing and future wireless LAN systems.

The IEEE introduced the WEP as an optional security measure to secure 802.11b (Wi-Fi) WLANs, but inherent weaknesses in the standard soon became obvious. In response to this situation, the Wi-Fi Alliance announced a new security architecture in October 2002 that remedies the shortcomings of WEP. This standard, formerly known as Safe Secure Network (SSN), is designed to work with existing 802.11 products and offers forward compatibility with 802.11i, the new wireless security architecture being defined in the IEEE.

WPA offers the following benefits:

- Enhanced data privacy
- Robust key management
- Data origin authentication
- Data integrity protection

The Wi-Fi Alliance is now performing interoperability certification testing on Wi-Fi Protected Access products. Starting August of 2003, all new Wi-Fi certified products will have to support WPA. NETGEAR will implement WPA on client and access point products and make this available in the second half of 2003. Existing Wi-Fi certified products will have one year to add WPA support or they will lose their Wi-Fi certification.

The 802.11i standard is currently in draft form, with ratification due at the end of 2003. While the new IEEE 802.11i standard is being ratified, wireless vendors have agreed on WPA as an interoperable interim standard.

How Does WPA Compare to WEP?

WEP is a data encryption method and is not intended as a user authentication mechanism. WPA user authentication is implemented using 802.1x and the Extensible Authentication Protocol (EAP). Support for 802.1x authentication is required in WPA. In the 802.11 standard, 802.1x authentication was optional. For details on EAP specifically, refer to IETF's RFC 2284.

With 802.11 WEP, all access points and client wireless adapters on a particular wireless LAN must use the same encryption key. A major problem with the 802.11 standard is that the keys are cumbersome to change. If you do not update the WEP keys often, an unauthorized person with a sniffing tool can monitor your network for less than a day and decode the encrypted messages. Products based on the 802.11 standard alone offer system administrators no effective method to update the keys.

For 802.11, WEP encryption is optional. For WPA, encryption using Temporal Key Integrity Protocol (TKIP) is required. TKIP replaces WEP with a new encryption algorithm that is stronger than the WEP algorithm, but that uses the calculation facilities present on existing wireless devices to perform encryption operations. TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. Through these enhancements, TKIP addresses all of known WEP vulnerabilities.

How Does WPA Compare to IEEE 802.11i?

WPA will be forward compatible with the IEEE 802.11i security specification currently under development. WPA is a subset of the current 802.11i draft and uses certain pieces of the 802.11i draft that are ready to bring to market today, such as 802.1x and TKIP. The main pieces of the 802.11i draft that are not included in WPA are secure IBSS (Ad-Hoc mode), secure fast handoff (for specialized 802.11 VoIP phones), as well as enhanced encryption protocols, such as AES-CCMP. These features are either not yet ready for market or will require hardware upgrades to implement.

What are the Key Features of WPA Security?

The following security features are included in the WPA standard:

- WPA Authentication
- WPA Encryption Key Management
  - Temporal Key Integrity Protocol (TKIP)
  - Michael message integrity code (MIC)
  - AES Support (to be phased in)
- Support for a Mixture of WPA and WEP Wireless Clients, but mixing WEP and WPA is discouraged

These features are discussed below.

WPA addresses most of the known WEP vulnerabilities and is primarily intended for wireless infrastructure networks as found in the enterprise. This infrastructure includes stations, access points, and authentication servers (typically RADIUS servers). The RADIUS server holds (or has access to) user credentials (for example, user names and passwords) and authenticates wireless users before they gain access to the network.

The strength of WPA comes from an integrated sequence of operations that encompass 802.1X/EAP authentication and sophisticated key management and encryption techniques. Its major operations include:

- Network security capability determination. This occurs at the 802.11 level and is communicated through WPA information elements in Beacon, Probe Response, and (Re) Association Requests. Information in these elements includes the authentication method (802.1X or Pre-shared key) and the preferred cipher suite (WEP, TKIP, or AES).

The primary information conveyed in the Beacon frames is the authentication method and the cipher suite. Possible authentication methods include 802.1X and Pre-shared key. Pre-shared key is an authentication method that uses a statically configured pass phrase on both the stations and the access point. This obviates the need for an authentication server, which in many home and small office environments will not be available nor desirable. Possible cipher suites include: WEP, TKIP, and AES (Advanced Encryption Standard). We talk more about TKIP and AES when addressing data privacy below.

- Authentication. EAP over 802.1X is used for authentication. Mutual authentication is gained by choosing an EAP type supporting this feature and is required by WPA. 802.1X port access control prevents full access to the network until authentication completes. 802.1X EAPOL-Key packets are used by WPA to distribute per-session keys to those stations successfully authenticated.

  The supplicant in the station uses the authentication and cipher suite information contained in the information elements to decide which authentication method and cipher suite to use. For example, if the access point is using the pre-shared key method then the supplicant need not authenticate using full-blown 802.1X. Rather, the supplicant must simply prove to the access point that it is in possession of the pre-shared key. If the supplicant detects that the service set does not contain a WPA information element then it knows it must use pre-WPA 802.1X authentication and key management in order to access the network.

- Key management. WPA features a robust key generation/management system that integrates the authentication and data privacy functions. Keys are generated after successful authentication and through a subsequent 4-way handshake between the station and Access Point (AP).
- Data Privacy (Encryption). Temporal Key Integrity Protocol (TKIP) is used to wrap WEP in sophisticated cryptographic and security techniques to overcome most of its weaknesses.
- Data integrity. TKIP includes a message integrity code (MIC) at the end of each plaintext message to ensure messages are not being spoofed.

WPA Authentication: Enterprise-level User Authentication via 802.1x/EAP and RADIUS

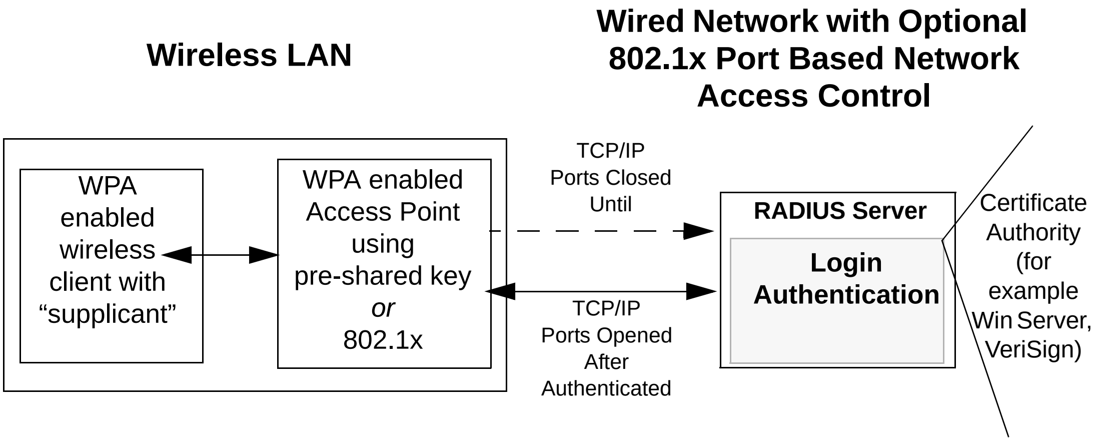

Wireless LAN
Wired Network with Optional 802.1x Port Based Network Access Control
WPA enabled wireless client with "supplicant"
WPA enabled Access Point using pre-shared key *or* 802.1x
TCP/IP Ports Closed Until
TCP/IP Ports Opened After Authenticated
RADIUS Server
Login Authentication
Certificate Authority (for example Win Server, VeriSign)

Figure E-3: WPA Overview

IEEE 802.1x offers an effective framework for authenticating and controlling user traffic to a protected network, as well as providing a vehicle for dynamically varying data encryption keys via EAP from a RADIUS server, for example. This framework enables using a central authentication server, which employs mutual authentication so that a rogue wireless user does not join the network.

It is important to note that 802.1x does not provide the actual authentication mechanisms. When using 802.1x, the EAP type, such as Transport Layer Security (EAP-TLS), or EAP Tunneled Transport Layer Security (EAP-TTLS), defines how the authentication takes place.

Note: For environments with a Remote Authentication Dial-In User Service (RADIUS) infrastructure, WPA supports Extensible Authentication Protocol (EAP). For environments without a RADIUS infrastructure, WPA supports the use of a pre-shared key.

Together, these technologies provide a framework for strong user authentication.

Windows XP implements 802.1x natively, and several NETGEAR switch and wireless access point products support 802.1x.

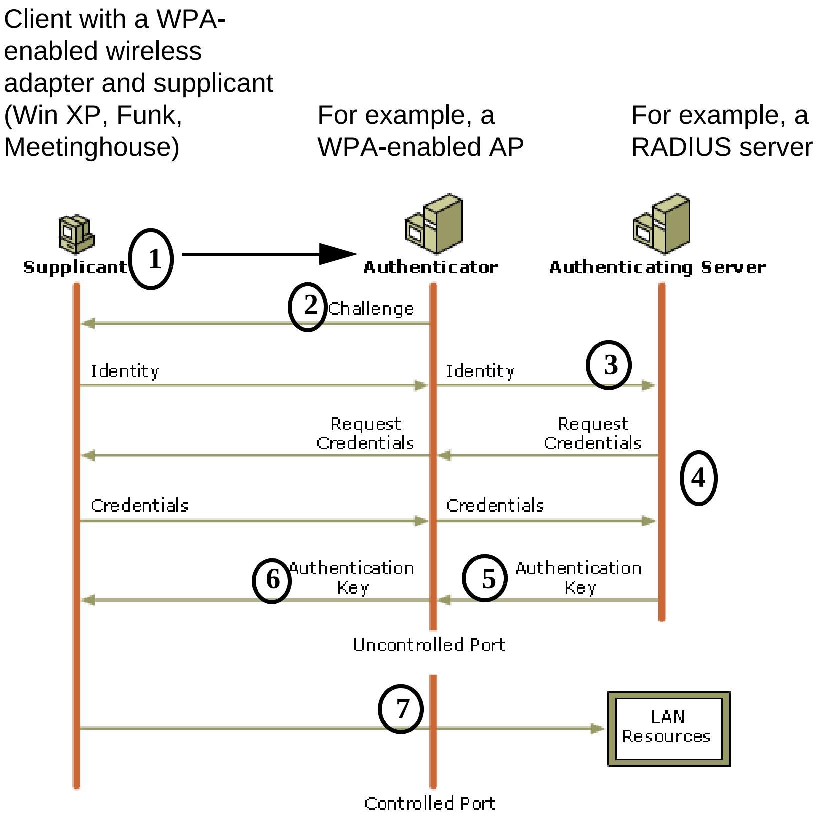


Figure E-4: 802.1x Authentication Sequence

The AP sends Beacon Frames with WPA information element to the stations in the service set. Information elements include the required authentication method (802.1x or Pre-shared key) and the preferred cipher suite (WEP, TKIP, or AES). Probe Responses (AP to station) and Association Requests (station to AP) also contain WPA information elements.

1. Initial 802.1x communications begin with an unauthenticated supplicant (client device) attempting to connect with an authenticator (802.11 access point). The client sends an EAP-start message. This begins a series of message exchanges to authenticate the client.
2. The access point replies with an EAP-request identity message.

3. The client sends an EAP-response packet containing the identity to the authentication server. The access point responds by enabling a port for passing only EAP packets from the client to an authentication server located on the wired side of the access point. The access point blocks all other traffic, such as HTTP, DHCP, and POP3 packets, until the access point can verify the client's identity using an authentication server (for example, RADIUS).
4. The authentication server uses a specific authentication algorithm to verify the client's identity. This could be through the use of digital certificates or some other EAP authentication type.
5. The authentication server will either send an accept or reject message to the access point.
6. The access point sends an EAP-success packet (or reject packet) to the client.
7. If the authentication server accepts the client, then the access point will transition the client's port to an authorized state and forward additional traffic.

The important part to know at this point is that the software supporting the specific EAP type resides on the authentication server and within the operating system or application “supplicant” software on the client devices. The access point acts as a “pass through” for 802.1x messages, which means that you can specify any EAP type without needing to upgrade an 802.1x-compliant access point. As a result, you can update the EAP authentication type to such devices as token cards (Smart Cards), Kerberos, one-time passwords, certificates, and public key authentication, or as newer types become available and your requirements for security change.

WPA Data Encryption Key Management

With 802.1x, the rekeying of unicast encryption keys is optional. Additionally, 802.11 and 802.1x provide no mechanism to change the global encryption key used for multicast and broadcast traffic. With WPA, rekeying of both unicast and global encryption keys is required.

For the unicast encryption key, the Temporal Key Integrity Protocol (TKIP) changes the key for every frame, and the change is synchronized between the wireless client and the wireless access point (AP). For the global encryption key, WPA includes a facility (the Information Element) for the wireless AP to advertise the changed key to the connected wireless clients.

If configured to implement dynamic key exchange, the 802.1x authentication server can return session keys to the access point along with the accept message. The access point uses the session keys to build, sign and encrypt an EAP key message that is sent to the client immediately after sending the success message. The client can then use contents of the key message to define applicable encryption keys. In typical 802.1x implementations, the client can automatically change encryption keys as often as necessary to minimize the possibility of eavesdroppers having enough time to crack the key in current use.

Temporal Key Integrity Protocol (TKIP)

WPA uses TKIP to provide important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. TKIP also provides for the following:

- The verification of the security configuration after the encryption keys are determined.
- The synchronized changing of the unicast encryption key for each frame.
- The determination of a unique starting unicast encryption key for each preshared key authentication.

Michael

With 802.11 and WEP, data integrity is provided by a 32-bit *integrity check value* (ICV) that is appended to the 802.11 payload and encrypted with WEP. Although the ICV is encrypted, you can use cryptanalysis to change bits in the encrypted payload and update the encrypted ICV without being detected by the receiver.

With WPA, a method known as *Michael* specifies a new algorithm that calculates an 8-byte message integrity check (MIC) using the calculation facilities available on existing wireless devices. The MIC is placed between the data portion of the IEEE 802.11 frame and the 4-byte ICV. The MIC field is encrypted together with the frame data and the ICV.

Michael also provides replay protection. A new frame counter in the IEEE 802.11 frame is used to prevent replay attacks.

Optional AES Support to be Phased In

One of the encryption methods supported by WPA, besides TKIP, is the advanced encryption standard (AES), although AES support will not be required initially for Wi-Fi certification. This is viewed as the optimal choice for security conscience organizations, but the problem with AES is that it requires a fundamental redesign of the NIC's hardware in both the station and the access point. TKIP is a pragmatic compromise that allows organizations to deploy better security while AES capable equipment is being designed, manufactured, and incrementally deployed.

Is WPA Perfect?

WPA is not without its vulnerabilities. Specifically, it is susceptible to denial of service (DoS) attacks. If the access point receives two data packets that fail the message integrity code (MIC) within 60 seconds of each other, then the network is under an active attack, and as a result, the access point employs counter measures, which include disassociating each station using the access point. This prevents an attacker from gleaning information about the encryption key and alerts administrators, but it also causes users to lose network connectivity for 60 seconds. More than anything else, this may just prove that no single security tactic is completely invulnerable. WPA is a definite step forward in WLAN security over WEP and has to be thought of as a single part of an end-to-end network security strategy.

Product Support for WPA

Starting in August, 2003, NETGEAR, Inc. wireless Wi-Fi certified products will support the WPA standard. NETGEAR, Inc. wireless products that had their Wi-Fi certification approved before August, 2003 will have one year to add WPA so as to maintain their Wi-Fi certification.

WPA requires software changes to the following:

- Wireless access points
- Wireless network adapters
- Wireless client programs

Supporting a Mixture of WPA and WEP Wireless Clients is Discouraged

To support the gradual transition of WEP-based wireless networks to WPA, a wireless AP can support both WEP and WPA clients at the same time. During the association, the wireless AP determines which clients use WEP and which clients use WPA. The disadvantage to supporting a mixture of WEP and WPA clients is that the global encryption key is not dynamic. This is because WEP-based clients cannot support it. All other benefits to the WPA clients, such as integrity, are maintained.

However, a mixed mode supporting WPA and non-WPA clients would offer network security that is no better than that obtained with a non-WPA network, and thus this mode of operation is discouraged.

Changes to Wireless Access Points

Wireless access points must have their firmware updated to support the following:

- **The new WPA information element**
  To advertise their support of WPA, wireless APs send the beacon frame with a new 802.11 WPA information element that contains the wireless AP's security configuration (encryption algorithms and wireless security configuration information).
- **The WPA two-phase authentication**
  Open system, then 802.1x (EAP with RADIUS or preshared key).
- **TKIP**
- **Michael**
- **AES** (optional)

To upgrade your wireless access points to support WPA, obtain a WPA firmware update from your wireless AP vendor and upload it to your wireless AP.

Changes to Wireless Network Adapters

Wireless networking software in the adapter, and possibly in the OS or client application, must be updated to support the following:

- **The new WPA information element**
  Wireless clients must be able to process the WPA information element and respond with a specific security configuration.
- **The WPA two-phase authentication**
  Open system, then 802.1x supplicant (EAP or preshared key).
- **TKIP**
- **Michael**
- **AES** (optional)

To upgrade your wireless network adapters to support WPA, obtain a WPA update from your wireless network adapter vendor and update the wireless network adapter driver.

For Windows wireless clients, you must obtain an updated network adapter driver that supports WPA. For wireless network adapter drivers that are compatible with Windows XP (Service Pack 1) and Windows Server 2003, the updated network adapter driver must be able to pass the adapter's WPA capabilities and security configuration to the Wireless Zero Configuration service.

Microsoft has worked with many wireless vendors to embed the WPA firmware update in the wireless adapter driver. So, to update your Microsoft Windows wireless client, all you have to do is obtain the new WPA-compatible driver and install the driver. The firmware is automatically updated when the wireless network adapter driver is loaded in Windows.

Changes to Wireless Client Programs

Wireless client programs must be updated to permit the configuration of WPA authentication (and preshared key) and the new WPA encryption algorithms (TKIP and the optional AES component).

To obtain the Microsoft WPA client program, visit the Microsoft Web site.

Appendix F
Virtual Private Networking

There have been many improvements in the Internet, including Quality of Service, network performance, and inexpensive technologies, such as DSL. But one of the most important advances has been in Virtual Private Networking (VPN) Internet Protocol security (IPSec). IPSec is one of the most complete, secure, and commercially available, standards-based protocols developed for transporting data.

What is a VPN?

A VPN is a shared network, where private data is segmented from other traffic, so that only the intended recipient has access. The term VPN was originally used to describe a secure connection over the Internet. Today, however, VPN is also used to describe private networks, such as Frame Relay, Asynchronous Transfer Mode (ATM), and Multiprotocol Label Switching (MPLS).

A key aspect of data security is that the data flowing across the network is protected by encryption technologies. Private networks lack data security, which allows data attackers to tap directly into the network and read the data. IPSec-based VPNs use encryption to provide data security, which increases the network's resistance to data tampering or theft.

IPSec-based VPNs can be created over any type of IP network, including the Internet, Frame Relay, ATM, and MPLS, but only the Internet is ubiquitous and inexpensive.

VPNs are traditionally used for:

- **Intranets:** Intranets connect an organization's locations. These locations range from the headquarters offices, to branch offices, to a remote employee's home. Often this connectivity is used for e-mail and for sharing applications and files. While Frame Relay, ATM, and MPLS accomplish these tasks, the shortcomings of each limits connectivity. The cost of connecting home users is also very expensive compared to Internet-access technologies, such as DSL or cable. Because of this, organizations are moving their networks to the Internet, which is inexpensive, and using IPSec to create these networks.

- **Remote Access:** Remote access enables telecommuters and mobile workers to access e-mail and business applications. A dial-up connection to an organization's modem pool is one method of access for remote workers, but is expensive because the organization must pay the associated long distance telephone and service costs. Remote access VPNs greatly reduce expenses by enabling mobile workers to dial a local Internet connection and then set up a secure IPSec-based VPN communications to their organization.
- **Extranets**: Extranets are secure connections between two or more organizations. Common uses for extranets include supply-chain management, development partnerships, and subscription services. These undertakings can be difficult using legacy network technologies due to connection costs, time delays, and access availability. IPSec-based VPNs are ideal for extranet connections. IPSec-capable devices can be quickly and inexpensively installed on existing Internet connections.

What is IPSec and How Does It Work?

IPSec is an Internet Engineering Task Force (IETF) standard suite of protocols that provides data authentication, integrity, and confidentiality as data is transferred between communication points across IP networks. IPSec provides data security at the IP packet level. A packet is a data bundle that is organized for transmission across a network, and includes a header and payload (the data in the packet). IPSec emerged as a viable network security standard because enterprises wanted to ensure that data could be securely transmitted over the Internet. IPSec protects against possible security exposures by protecting data while in transit.

IPSec Security Features

IPSec is the most secure method commercially available for connecting network sites. IPSec was designed to provide the following security features when transferring packets across networks:

- **Authentication:** Verifies that the packet received is actually from the claimed sender.
- **Integrity:** Ensures that the contents of the packet did not change in transit.
- **Confidentiality:** Conceals the message content through encryption.

IPSec Components

IPSec contains the following elements:

- **Encapsulating Security Payload (ESP)**: Provides confidentiality, authentication, and integrity.
- **Authentication Header (AH)**: Provides authentication and integrity.
- **Internet Key Exchange (IKE)**: Provides key management and Security Association (SA) management.

Encapsulating Security Payload (ESP)

ESP provides authentication, integrity, and confidentiality, which protect against data tampering and, most importantly, provides message content protection.

IPSec provides an open framework for implementing industry standard algorithms, such as SHA and MD5. The algorithms IPSec uses produce a unique and unforgeable identifier for each packet, which is a data equivalent of a fingerprint. This fingerprint allows the device to determine if a packet has been tampered with. Furthermore, packets that are not authenticated are discarded and not delivered to the intended receiver.

ESP also provides all encryption services in IPSec. Encryption translates a readable message into an unreadable format to hide the message content. The opposite process, called decryption, translates the message content from an unreadable format to a readable message. Encryption/decryption allows only the sender and the authorized receiver to read the data. In addition, ESP has an option to perform authentication, called ESP authentication. Using ESP authentication, ESP provides authentication and integrity for the payload and not for the IP header.

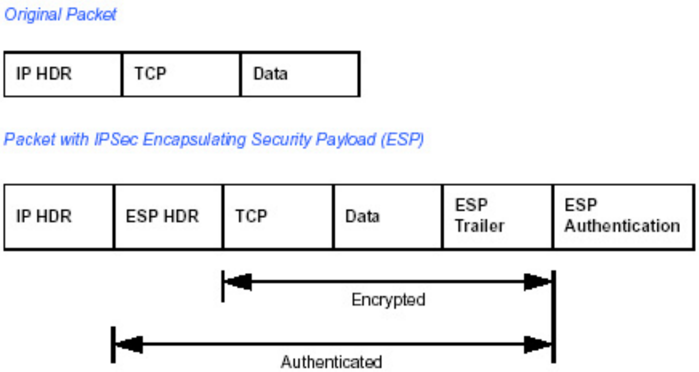


Figure F-1: Original packet and packet with IPSec Encapsulated Security Payload

The ESP header is inserted into the packet between the IP header and any subsequent packet contents. However, because ESP encrypts the data, the payload is changed. ESP does not encrypt the ESP header, nor does it encrypt the ESP authentication.

Authentication Header (AH)

AH provides authentication and integrity, which protect against data tampering, using the same algorithms as ESP. AH also provides optional anti-replay protection, which protects against unauthorized retransmission of packets. The authentication header is inserted into the packet between the IP header and any subsequent packet contents. The payload is not touched.

Although AH protects the packet's origin, destination, and contents from being tampered with, the identity of the sender and receiver is known. In addition, AH does not protect the data's confidentiality. If data is intercepted and only AH is used, the message contents can be read. ESP protects data confidentiality. For added protection in certain cases, AH and ESP can be used together. In the following table, IP HDR represents the IP header and includes both source and destination IP addresses.

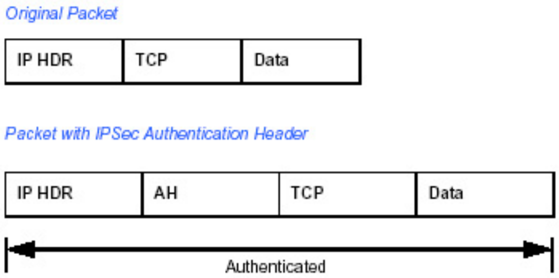


Figure F-2: Original packet and packet with IPSec Authentication Header

IKE Security Association

IPSec introduces the concept of the Security Association (SA). An SA is a logical connection between two devices transferring data. An SA provides data protection for unidirectional traffic by using the defined IPSec protocols. An IPSec tunnel typically consists of two unidirectional SAs, which together provide a protected, full-duplex data channel.

The SAs allow an enterprise to control exactly what resources may communicate securely, according to security policy. To do this an enterprise can set up multiple SAs to enable multiple secure VPNs, as well as define SAs within the VPN to support different departments and business partners.

Mode

SAs operate using modes. A mode is the method in which the IPSec protocol is applied to the packet. IPSec can be used in tunnel mode or transport mode. Typically, the tunnel mode is used for gateway-to-gateway IPSec tunnel protection, while transport mode is used for host-to-host IPSec tunnel protection. A gateway is a device that monitors and manages incoming and outgoing network traffic and routes the traffic accordingly. A host is a device that sends and receives network traffic.

- **Transport Mode:** The transport mode IPSec implementation encapsulates only the packet's payload. The IP header is not changed. After the packet is processed with IPSec, the new IP packet contains the old IP header (with the source and destination IP addresses unchanged) and the processed packet payload. Transport mode does not shield the information in the IP header; therefore, an attacker can learn where the packet is coming from and where it is going to. The previous packet diagrams show a packet in transport mode.
- **Tunnel Mode:** The tunnel mode IPSec implementation encapsulates the entire IP packet. The entire packet becomes the payload of the packet that is processed with IPSec. A new IP header is created that contains the two IPSec gateway addresses. The gateways perform the encapsulation/decapsulation on behalf of the hosts. Tunnel mode ESP prevents an attacker from analyzing the data and deciphering it, as well as knowing who the packet is from and where it is going.

Note: AH and ESP can be used in both transport mode or tunnel mode.

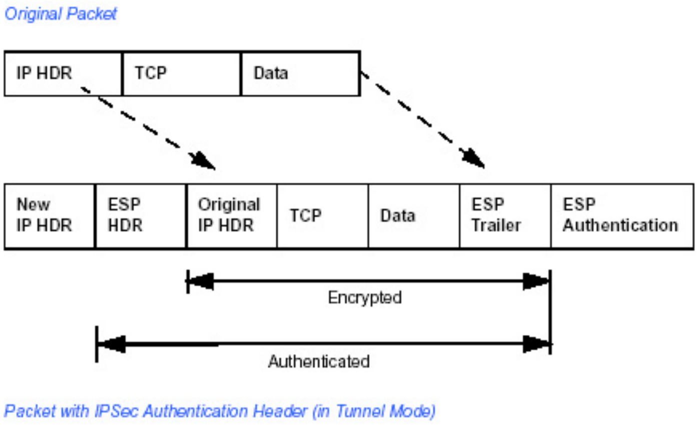


Figure F-3: Original packet and packet with IPSec ESP in Tunnel mode

Key Management

IPSec uses the Internet Key Exchange (IKE) protocol to facilitate and automate the SA setup and the exchange of keys between parties transferring data. Using keys ensures that only the sender and receiver of a message can access it.

IPSec requires that keys be re-created, or refreshed, frequently, so that the parties can communicate securely with each other. IKE manages the process of refreshing keys; however, a user can control the key strength and the refresh frequency. Refreshing keys on a regular basis ensures data confidentiality between sender and receiver.

Understand the Process Before You Begin

This document provides case studies on how to configure secure IPSec VPN tunnels. This document assumes the reader has a working knowledge of NETGEAR management systems.

NETGEAR is a member of the VPN Consortium, a group formed to facilitate IPSec VPN vendor interoperability. The VPN Consortium has developed specific scenarios to aid system administrators in the often confusing process of connecting two different vendor implementations of the IPSec standard. The case studies in this appendix follow the addressing and configuration mechanics defined by the VPN Consortium. Additional information regarding inter-vendor interoperability may be found at *http://www.vpnc.org/interop.html*.

It is a good idea to gather all the necessary information required to establish a VPN before you begin the configuration process. You should understand whether the firmware is up to date, all of the addresses that will be necessary, and all of the parameters that need to be set on both sides. Try to understand any incompatibilities before you begin, so that you minimize any potential complications which may arise from normal firewall or WAN processes.

If you are not a full-time system administrator, it is a good idea to familiarize yourself with the mechanics of a VPN. The brief description in this appendix will help. Other good sources include:

- The NETGEAR VPN Tutorial – *http://www.netgear.com/planetvpn/pvpn_2.html*
- The VPN Consortium – *http://www.vpnc.org/*
- The VPN bibliography in “Additional Reading“ on page F-11.

VPN Process Overview

Even though IPSec is standards-based, each vendor has its own set of terms and procedures for implementing the standard. Because of these differences, it may be a good idea to review some of the terms and the generic processes for connecting two gateways before diving into the specifics.

Network Interfaces and Addresses

The VPN gateway is aptly named because it functions as a "gatekeeper" for each of the computers connected on the Local Area Network behind it.

In most cases, each Gateway will have a "public" facing address (WAN side) and a "private" facing address (LAN side). These addresses are referred to as the "network interface" in documentation regarding the construction of VPN communication. Please note that the addresses used in the example do not use full TCP/IP notation.

Interface Addressing

This TechNote uses example addresses provided the VPN Consortium. It is important to understand that you will be using addresses specific to the devices that you are attempting to connect via IPSec VPN.

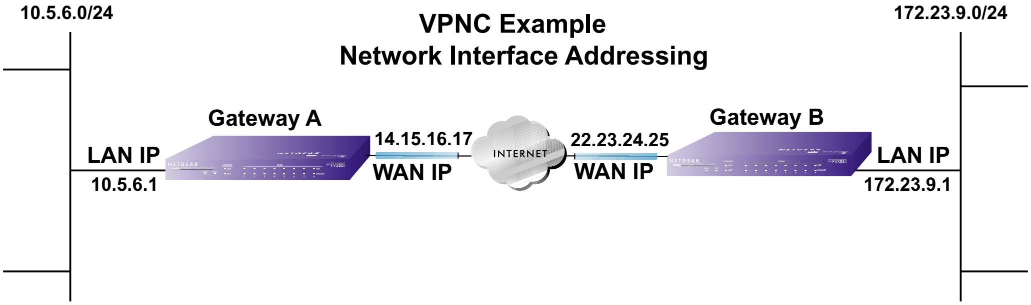


Figure F-4: VPNC Example Network Interface Addressing

It is also important to make sure the addresses do not overlap or conflict. That is, each set of addresses should be separate and distinct.

Table 5-3. WAN (Internet/Public) and LAN (Internal/Private) Addressing

Gateway	LAN or WAN	VPNC Example Address
Gateway A	LAN (Private)	10.5.6.1
Gateway A	WAN (Public)	14.15.16.17
Gateway B	LAN (Private)	22.23.24.25
Gateway B	WAN (Public)	172.23.9.1

It will also be important to know the subnet mask of both gateway LAN Connections.

Table 5-4. Subnet Addressing

Gateway	LAN or WAN	Interface Name	Example Subnet Mask
Gateway A	LAN (Private)	Subnet Mask A	255.255.255.0
Gateway B	LAN (Private)	Subnet Mask B	255.255.255.0

Firewalls

It is important to understand that many gateways are also firewalls. VPN tunnels cannot function properly if firewall settings disallow all incoming traffic. Please refer to the firewall instructions for both gateways to understand how to open specific protocols, ports, and addresses that you intend to allow.

Setting Up a VPN Tunnel Between Gateways

An SA, frequently called a tunnel, is the set of information that allows two entities (networks, PCs, routers, firewalls, gateways) to “trust each other” and communicate securely as they pass information over the Internet.

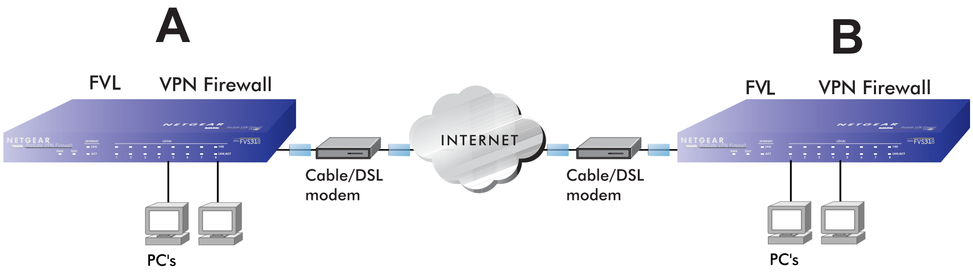


Figure F-5: VPN Tunnel SA

The SA contains all the information necessary for gateway A to negotiate a secure and encrypted communication stream with gateway B. This communication is often referred to as a “tunnel.” The gateways contain this information so that it does not have to be loaded onto every computer connected to the gateways.

Each gateway must negotiate its Security Association with another gateway using the parameters and processes established by IPSec. As illustrated below, the most common method of accomplishing this process is via the Internet Key Exchange (IKE) protocol which automates some of the negotiation procedures. Alternatively, you can configure your gateways using manual key exchange, which involves manually configuring each paramter on both gateways.

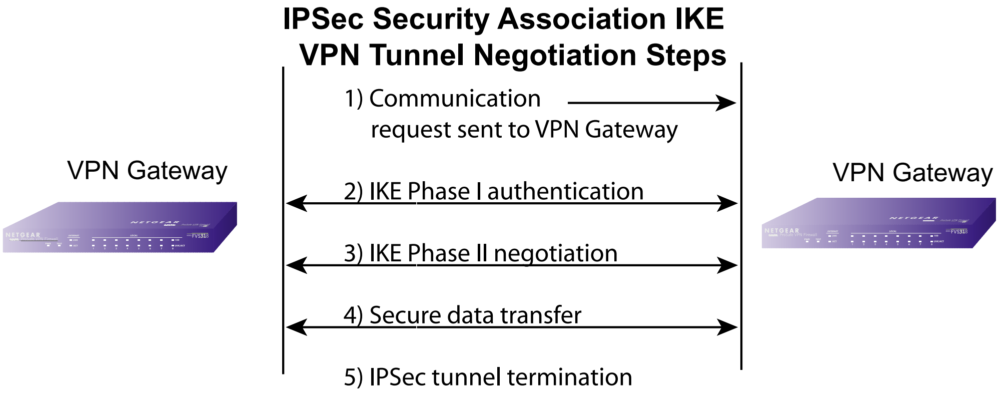

IPSec Security Association IKE
VPN Tunnel Negotiation Steps
1) Communication
request sent to VPN Gateway
VPN Gateway
VPN Gateway
2) IKE Phase I authentication
3) IKE Phase II negotiation
4) Secure data transfer
5) IPSec tunnel termination

Figure F-6: IPSec SA negotiation

1. **The IPSec software on Host A initiates the IPSec process in an attempt to communicate with Host B.** The two computers then begin the Internet Key Exchange (IKE) process.

2. **IKE Phase I.**
   a. The two parties negotiate the encryption and authentication algorithms to use in the IKE SAs.
   b. The two parties authenticate each other using a predetermined mechanism, such as preshared keys or digital certificates.
   c. A shared master key is generated by the Diffie-Hellman Public key algorithm within the IKE framework for the two parties. The master key is also used in the second phase to derive IPSec keys for the SAs.
3. **IKE Phase II.**
   a. The two parties negotiate the encryption and authentication algorithms to use in the IPSec SAs.
   b. The master key is used to derive the IPSec keys for the SAs. Once the SA keys are created and exchanged, the IPSec SAs are ready to protect user data between the two VPN gateways.
4. **Data transfer.** Data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.
5. **IPSec tunnel termination.** IPSec SAs terminate through deletion or by timing out.

VPNC IKE Security Parameters

It is important to remember that both gateways must have the identical parameters set for the process to work correctly. The settings in these examples follow the examples given for Scenario 1 of the VPN Consortium.

VPNC IKE Phase I Parameters

The IKE Phase 1 parameters used:

- Main mode
- TripleDES
- SHA-1
- MODP group 1
- Ppre-shared secret of "hr5xb84l6aa9r6"
- SA lifetime of 28800 seconds (eight hours)

VPNC IKE Phase II Parameters

The IKE Phase 2 parameters used in Scenario 1 are:

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 1
- Perfect forward secrecy for rekeying
- SA lifetime of 28800 seconds (one hour)

Testing and Troubleshooting

Once you have completed the VPN configuration steps you can use PCs, located behind each of the gateways, to ping various addresses on the LAN side of the other gateway.

You can troubleshoot connections using the VPN status and log details on the NETGEAR gateway to determine if IKE negotiation is working. Common problems encountered in setting up VPNs include:

- Parameters may be configured differently on Gateway A vs. Gateway B.
- Two LANs set up with similar or overlapping addressing schemes.
- So many required configuration parameters mean errors such as mistyped information or mismatched parameter selections on either side are more likely to happen.

Additional Reading

- *Building and Managing Virtual Private Networks*, Dave Kosiur, Wiley & Sons; ISBN: 0471295264
- *Firewalls and Internet Security: Repelling the Wily Hacker*, William R. Cheswick and Steven M. Bellovin, Addison-Wesley; ISBN: 0201633574
- *VPNs A Beginners Guide*, John Mains, McGraw Hill; ISBN: 0072191813
- [FF98] Floyd, S., and Fall, K., Promoting the Use of End-to-End Congestion Control in the Internet. IEEE/ACM Transactions on Networking, August 1999.

Relevant RFCs listed numerically:

- [RFC 791] *Internet Protocol DARPA Internet Program Protocol Specification*, Information Sciences Institute, USC, September 1981.
- [RFC 1058] *Routing Information Protocol*, C Hedrick, Rutgers University, June 1988.
- [RFC 1483] *Multiprotocol Encapsulation over ATM Adaptation Layer 5*, Juha Heinanen, Telecom Finland, July 1993.
- [RFC 2401] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol, RFC 2401, November 1998.
- [RFC 2407] D. Piper, The Internet IP Security Domain of Interpretation for ISAKMP, November 1998.
- [RFC 2474] K. Nichols, S. Blake, F. Baker, D. Black, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998.
- [RFC 2475] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, An Architecture for Differentiated Services, December 1998.
- [RFC 2481] K. Ramakrishnan, S. Floyd, A Proposal to Add Explicit Congestion Notification (ECN) to IP, January 1999.
- [RFC 2408] D. Maughan, M. Schertler, M. Schneider, J. Turner, Internet Security Association and Key Management Protocol (ISAKMP).
- [RFC 2409] D. Harkins, D.Carrel, Internet Key Exchange (IKE) protocol.
- [RFC 2401] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol.

Appendix G
NETGEAR VPN Configuration
FVS318 or FVM318 to FWG114P v2

This appendix provides a case study on how to configure a secure IPSec VPN tunnel between a NETGEAR FVS318 or FVM318 to a FWG114P v2. The configuration options and screens for the FVS318 and FVM318 are the same.

Configuration Template

The configuration in this document follows the addressing and configuration mechanics defined by the VPN Consortium. Gather all the necessary information before you begin the configuration process. Verify whether the firmware is up to date, all of the addresses that will be necessary, and all of the parameters that need to be set on both sides. Check that there are no firewall restrictions.

Table G-1. Summary

VPN Consortium Scenario:		Scenario 1
Type of VPN		LAN-to-LAN or Gateway-to-Gateway (not PC/Client-to-Gateway)
Security Scheme:		IKE with Preshared Secret/Key (not Certificate-based)
Date Tested:		December 2003
Model/Firmware Tested:		
	NETGEAR-Gateway A	FVS318 firmware version A1.4 or 2.0; FVM318 firmware version 1.1
	NETGEAR-Gateway B	FWG114P with firmware version 2 Release 2
IP Addressing:		
	NETGEAR-Gateway A	Static IP address
	NETGEAR-Gateway B	Static IP address

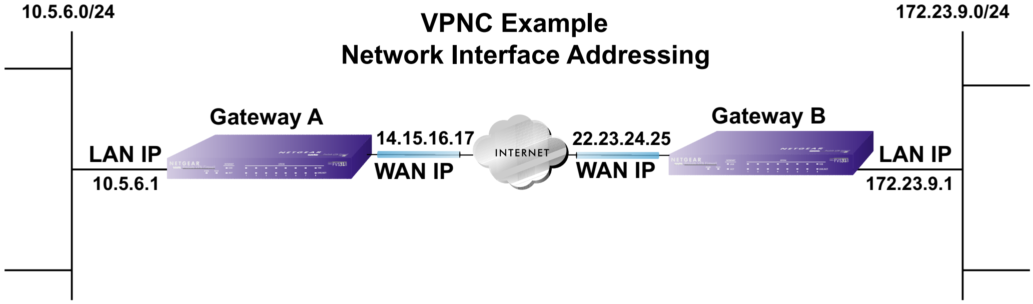
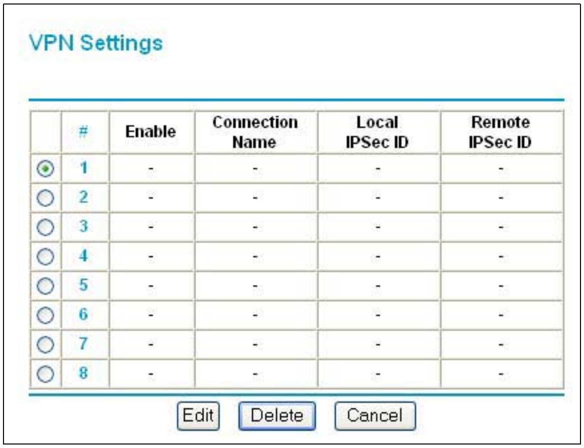


Figure G-1: Addressing and Subnet Used for Examples

Step-By-Step Configuration of FVS318 or FVM318 Gateway A

1. Log in to the FVS318 or FVM318 labeled Gateway A as in the illustration.

   Out of the box, the FVS318 or FVM318 is set for its default LAN address of *http://192.168.0.1* with its default user name of **admin** and default password of **password**. For this example we will assume you have set the local LAN address as 10.5.6.1 for Gateway A and have set your own password.

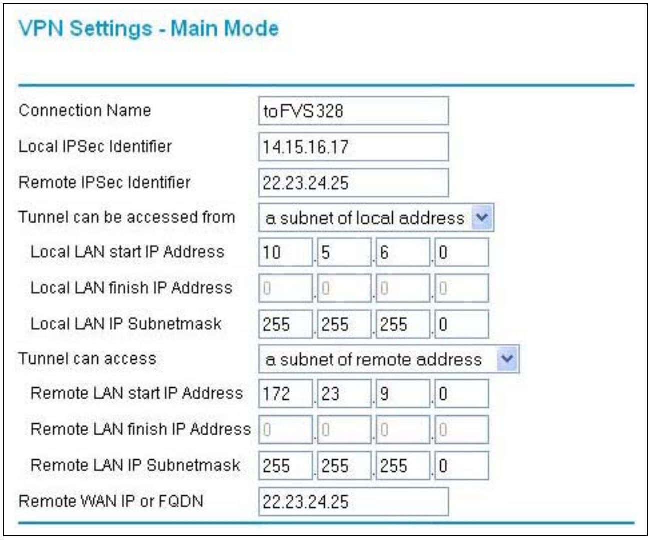


VPN Settings

	#	Enable	Connection Name	Local IPSec ID	Remote IPSec ID
●	1	-	-	-	-
○	2	-	-	-	-
○	3	-	-	-	-
○	4	-	-	-	-
○	5	-	-	-	-
○	6	-	-	-	-
○	7	-	-	-	-
○	8	-	-	-	-

Figure G-2: NETGEAR FVS318 VPN Settings Pre-Configuration

2. Click the VPN Settings link on the left side of the Settings management GUI. Click the radio button of the first available VPN leg (all 8 links are available in the example). Click the Edit button below. This will take you to the VPN Settings – Main Mode Menu.



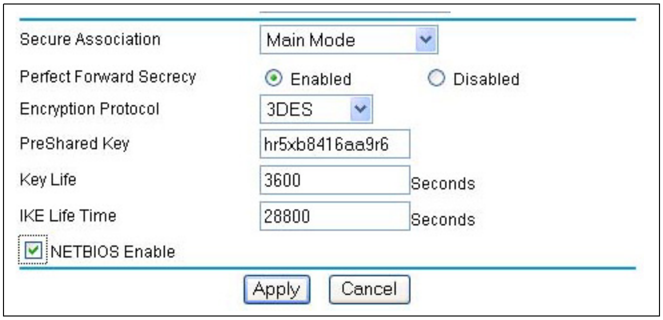
VPN Settings - Main Mode

Connection Name	toFVS328
Local IPSec Identifier	14.15.16.17
Remote IPSec Identifier	22.23.24.25
Tunnel can be accessed from	a subnet of local address
Local LAN start IP Address	10 . 5 . 6 . 0
Local LAN finish IP Address	0 . 0 . 0 . 0
Local LAN IP Subnetmask	255 . 255 . 255 . 0
Tunnel can access	a subnet of remote address
Remote LAN start IP Address	172 . 23 . 9 . 0
Remote LAN finish IP Address	0 . 0 . 0 . 0
Remote LAN IP Subnetmask	255 . 255 . 255 . 0
Remote WAN IP or FQDN	22.23.24.25

Figure G-3: Figure 3 – NETGEAR FVS318 VPN Settings (part 1) – Main Mode

- In the Connection Name box, enter in a unique name for the VPN tunnel to be configured between the NETGEAR devices. For this example we have used **toFVS328**.
- Enter a Local IPSec Identifier name for the NETGEAR FVS318 Gateway A. This name must be entered in the other endpoint as Remote IPSec Identifier. In this example we used **14.15.16.17** as the local identifier.
- Enter a Remote IPSec Identifier name for the remote NETGEAR FWG114P v2 Gateway B. This name must be entered in the other endpoint as Local IPSec Identifier. In this example we used **22.23.24.25** as the remote identifier.
- Choose a subnet from local address from the “Tunnel can be accessed from” pull-down menu.
- Type the starting LAN IP Address of Gateway A (**10.5.6.1** in our example) in the Local IP Local LAN start IP Address field.
- Type the finishing LAN IP Address of Gateway A (**0.0.0.0** in our example) in the Local IP Local LAN finish IP Address field.
- Type the LAN Subnet Mask of Gateway A (**255.255.255.0** in our example) in the Local LAN IP Subnetmask field.

- Choose a subnet from local address from the “Tunnel can access” pull-down menu.
- Type the starting LAN IP Address of Gateway B (**172.23.9.1** in our example) in the Local IP Remote LAN Start IP Address field.
- Type the finishing LAN IP Address of Gateway B (**0.0.0.0** in our example) in the Local IP Remote LAN Finish IP Address field.
- Type the LAN Subnet Mask of Gateway B (**255.255.255.0** in our example) in the Remote LAN IP Subnetmask field.
- Type the WAN IP address (**22.23.24.25** in our example) of Gateway B in the Remote WAN IP or FQDN field.



Secure Association	Main Mode	
Perfect Forward Secrecy	● Enabled	○ Disabled
Encryption Protocol	3DES	
PreShared Key	hr5xb8416aa9r6	
Key Life	3600	Seconds
IKE Life Time	28800	Seconds

☑ NETBIOS Enable

Figure G-4: Figure 4 – NETGEAR FVS318 VPN Settings (part 2) – Main Mode

- From the Secure Association drop-down box, select Main Mode.
- Next to Perfect Forward Secrecy, select the Enabled radio button.
- From the Encryption Protocol drop-down box, select 3DES.
- In the PreShared Key box, type a unique text string to be used as the shared key between Gateway A and Gateway B. In this example we used **hr5xb84l6aa9r6**. You must make sure the key is the same for both gateways.
- In the Key Life box, enter in 3600 seconds.
- In the IKE Life Time, enter 28800 seconds.
- Check the NETBIOS Enable box if you wish to pass NetBIOS traffic over the VPN tunnel, allowing functions, such as Microsoft Network Neighborhood browsing.

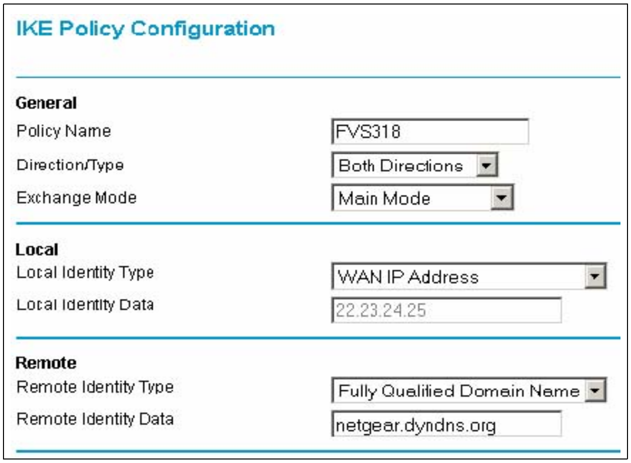
3. Click the Apply button in the lower center of the screen to save all changes and return to the VPN Settings screen.
4. When the screen returns to the VPN Settings, make sure the Enable check box is selected.

Step-By-Step Configuration of FWG114P Gateway B

1. Log in to the NETGEAR FVS328 labeled Gateway B as in the illustration.

   Out of the box, the FVS328 is set for its default LAN address of *http://192.168.0.1,* with its default user name of **admin** and default password of **password**. For this example we will assume you have set the local LAN address as 172.23.9.1 for Gateway B and have set your own user name and password.

2. Click the IKE Policies link under the VPN category link on the left side of the Settings management GUI. This will open the IKE Policies Menu. Click Add. This will open a new screen titled IKE Policy Configuration.



IKE Policy Configuration

General	
Policy Name	FVS318
Direction/Type	Both Directions
Exchange Mode	Main Mode
Local	
Local Identity Type	WAN IP Address
Local Identity Data	22.23.24.25
Remote	
Remote Identity Type	Fully Qualified Domain Name
Remote Identity Data	netgear.dyndns.org

Figure G-5: NETGEAR FVS328 IKE Policy Configuration – Part 1

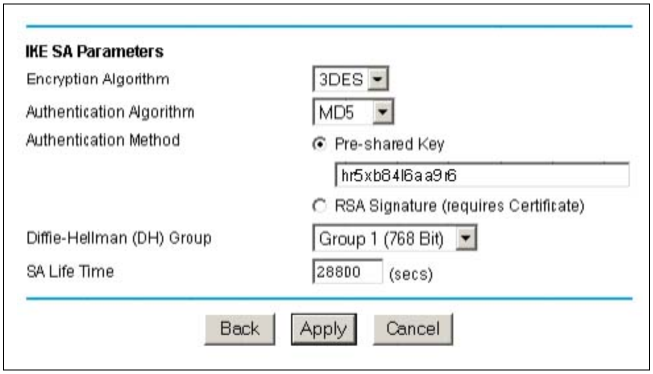
– Enter an appropriate name for the policy in the Policy Name field. This name is not supplied to the remote VPN Endpoint. It is used to help you manage the IKE policies. In our example we have used FVS318 as the Policy Name. In the Policy Name field type **FVS318**.

– From the Direction/Type drop-down box, select Both Directions.

– From the Exchange Mode drop-down box, select Main Mode.

– From the Local Identity drop-down box, select WAN IP Address (WAN IP address will automatically be populated into the Local Identity Data field after policy is applied).

– From the Remote Identity drop-down box, select Remote WAN IP (WAN IP address will automatically be populated into the Local Identity Data field after policy is applied).



IKE SA Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: MD5

Authentication Method: ● Pre-shared Key

hr5xb84l6aa9r6

○ RSA Signature (requires Certificate)

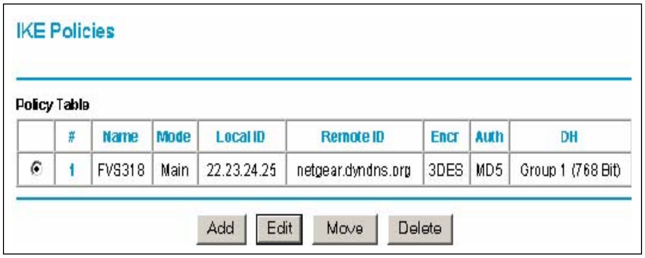
Diffie-Hellman (DH) Group: Group 1 (768 Bit)

SA Life Time: 28800 (secs)

Figure G-6: NETGEAR FVS328 IKE Policy Configuration – Part 2

- From the Encryption Algorithm drop-down box, select 3DES.
- From the Authentication Algorithm drop-down box, select MD5.
- From the Authentication Method radio button, select Pre-shared Key.
- In the Pre-Shared Key field, type **hr5xb84l6aa9r6**. You must make sure the key is the same for both gateways.
- From the Diffie-Hellman (DH) Group drop-down box, select Group 1 (768 Bit).
- In the SA Life Time field, type 28800.

3. Click the Apply Button. This will bring you back to the IKE Policies Menu.



IKE Policies

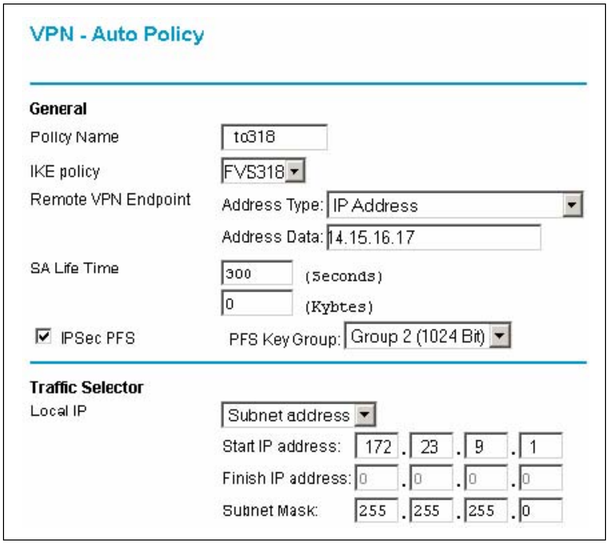
Policy Table

	#	Name	Mode	Local ID	Remote ID	Encr	Auth	DH
●	1	FVS318	Main	22.23.24.25	netgear.dyndns.org	3DES	MD5	Group 1 (768 Bit)

Figure G-7: NETGEAR FVS328 IKE Policies (Post Configuration)

The FVS318 IKE Policy is now displayed in the IKE Policies page.

4. Click the VPN Policies link under the VPN category link on the left side of the Settings management GUI. This will take you to the VPN Policies Menu page. Click Add Auto Policy. This will open a new screen titled VPN – Auto Policy.



VPN - Auto Policy

General

Policy Name: to318

IKE policy: FVS318

Remote VPN Endpoint: Address Type: IP Address

Address Data: 14.15.16.17

SA Life Time: 300 (Seconds)

0 (Kybtes)

☑ IPSec PFS   PFS Key Group: Group 2 (1024 Bit)

Traffic Selector

Local IP: Subnet address

Start IP address: 172 . 23 . 9 . 1

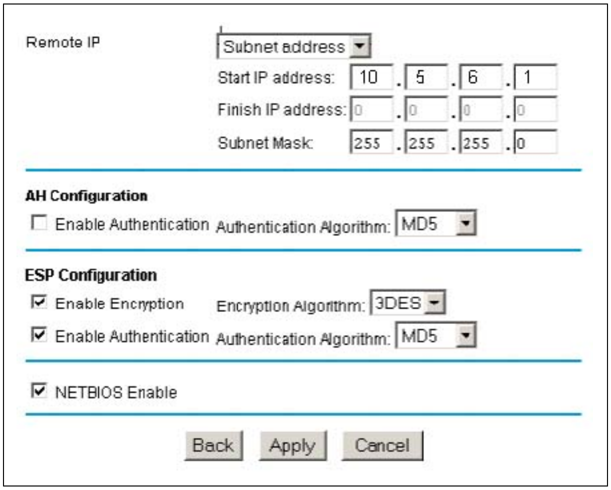
Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Figure G-8: NETGEAR FVS328 VPN – Auto Policy (part 1)

- Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. In our example we have used **to318** as the Policy Name. In the Policy Name field type **to318**.
- From the IKE policy drop-down box, select the IKE Policy that was set up in the earlier step – this being the FVS318 IKE Policy.
- From the Remote VPN Endpoint Address Type drop-down box, select IP Address.
- Type the WAN IP Address of Gateway A (**14.15.16.17** in our example) in the **Remote** VPN Endpoint Address Data field.
- Type **300** in the SA Life Time (Seconds) field.
- Type **0** in the SA Life Time (Kbytes) field.
- Check the IPSec PFS check box.
- From the PFS Key Group drop-down box, select Group 2 (1024 Bit).
- From the Traffic Selector Local IP drop-down box, select Subnet address.
- Type the starting LAN IP Address of Gateway B (**172.23.9.1** in our example) in the Local IP Start IP Address field.
- Type the finishing LAN IP Address of Gateway B (**0.0.0.0** in our example) in the Local IP Finish IP Address field.

– Type the LAN Subnet Mask of Gateway B (**255.255.255.0** in our example) in the Local IP Subnet Mask field.



Remote IP: Subnet address

Start IP address: 10 . 5 . 6 . 1

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

AH Configuration

□ Enable Authentication Authentication Algorithm: MD5

ESP Configuration

☑ Enable Encryption Encryption Algorithm: 3DES

☑ Enable Authentication Authentication Algorithm: MD5

☑ NETBIOS Enable

Figure G-9: NETGEAR FWG114P v2 VPN – Auto Policy (part 2)

– From the Traffic Selector Remote IP drop-down box, select Subnet address.

– Type the starting LAN IP Address of Gateway A (**10.5.6.1** in our example) in the Remote IP Start IP Address field.

– Type the finishing LAN IP Address of Gateway A (**0.0.0.0** in our example) in the Remote IP Finish IP Address field.

– Type the LAN Subnet Mask of Gateway A (**255.255.255.0** in our example) in the Remote IP Subnet Mask field.

– From the AH Configuration Authentication Algorithm drop-down box, select MD5.

– Select Enable Encryption in the ESP Configuration Enable Encryption check box.

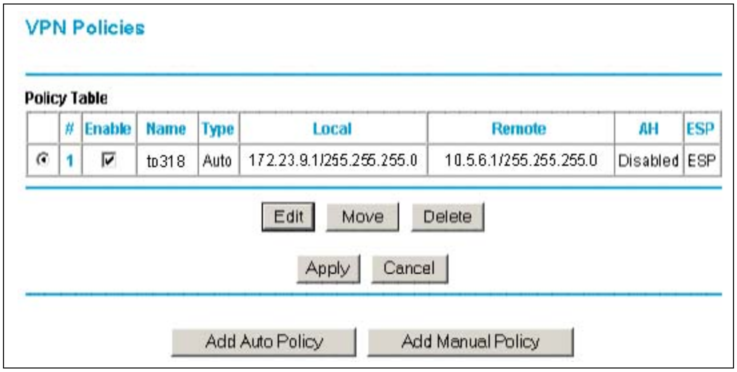
– From the ESP Configuration Encryption Algorithm drop-down box, select 3DES.

– Select Enable Authentication in the ESP Configuration Enable Authentication check box.

– From the ESP Configuration Authentication Algorithm drop-down box, select MD5.

– Select NETBIOS Enable in the NETBIOS Enable check box.

5. Click the Apply Button. You will be taken back to the VPN Policies Menu page.



VPN Policies

Policy Table

	#	Enable	Name	Type	Local	Remote	AH	ESP
●	1	☑	to318	Auto	172.23.9.1/255.255.255.0	10.5.6.1/255.255.255.0	Disabled	ESP

Figure G-10: NETGEAR FWG114P v2 VPN Policies Menu (Post Configuration)

6. When the screen returns to the **VPN Policies**, make sure the **Enable** check box is selected. Click the **Apply** button.

Test the VPN Connection

1. From a PC behind the NETGEAR FVS318 or FVM318 gateway A attempt to ping the remote FWG114P v2 gateway B LAN Interface address (example address 172.23.9.1).
2. From a PC behind the FWG114P v2 gateway B attempt to ping the remote NETGEAR FVS318 or FVM318 gateway A LAN Interface address (example address 10.5.6.1).
3. Click the Broadband Status link on the left side of the FWG114P v2 Settings management GUI. Click the Show VPN Status button below. This will take you to the IPSec Connection Status Screen. If the connection is functioning properly, the State fields will show “Estab.”
4. Click the Router Status link on the left side of the FVS318 Settings management GUI. Click the Show VPN Logs button below. NETGEAR log files should be similar to the example below.

Appendix H
NETGEAR VPN Configuration
FVS318 or FVM318 with FQDN to FVS328

This appendix provides a case study on how to configure a VPN tunnel between a NETGEAR FVS318 or FVM318 to a FWG114P v2 using a Fully Qualified Domain Name (FQDN) to resolve the public address of one or both routers. The configurations screens and settings for the FVS318 and FVM318 are the same.

Configuration Template

The configuration in this document follows the addressing and configuration mechanics defined by the VPN Consortium. Gather all the necessary information before you begin the configuration process. Verify whether the firmware is up to date, all of the addresses that will be necessary, and all of the parameters that need to be set on both sides. Check that there are no firewall restrictions.

Table H-1. Summary

VPN Consortium Scenario:		Scenario 1
Type of VPN		LAN-to-LAN or Gateway-to-Gateway (not PC/Client-to-Gateway)
Security Scheme:		IKE with Preshared Secret/Key (not Certificate-based)
Date Tested:		December 2003
Model/Firmware Tested:		
	NETGEAR-Gateway A	FVS318 firmware version A1.4 or 2.0; FVM318 firmware version 1.1
	NETGEAR-Gateway B	FVS328 with firmware version 1.0 Release 00
IP Addressing:		
	NETGEAR-Gateway A	Fully Qualified Domain Name (FQDN)
	NETGEAR-Gateway B	Static IP address

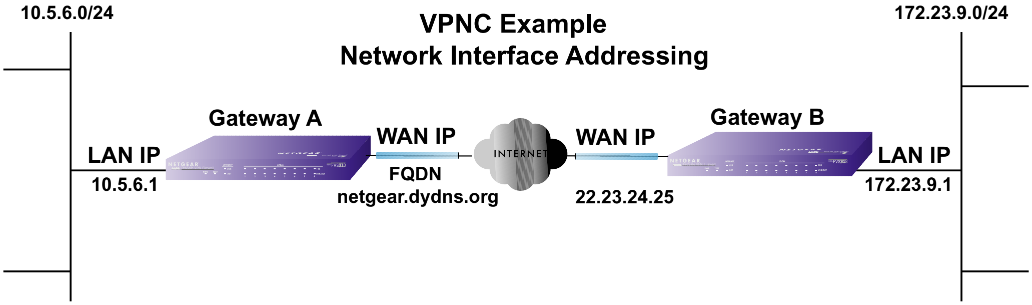


Figure H-1: Addressing and Subnet Used for Examples

Using DDNS and Fully Qualified Domain Names (FQDN)

Many ISPs (Internet Service Providers) provide connectivity to their customers using dynamic instead of static IP addressing. This means that a user's IP address does not remain constant over time, which presents a challenge for gateways attempting to establish VPN connectivity.

A Dynamic DNS (DDNS) service allows a user whose public IP address is dynamically assigned to be located by a host or domain name. It provides a central public database where information (such as e-mail addresses, host names and IP addresses) can be stored and retrieved. Now, a gateway can be configured to use a 3rd party service in lieu of a permanent and unchanging IP address to establish bi-directional VPN connectivity.

To use DDNS, you must register with a DDNS service provider. Example DDNS Service Providers include:

Table H-1. Example DDNS Service Providers

DynDNS	www.dyndns.org
TZO.com	netgear.tzo.com
ngDDNS	ngddns.iego.net

In this example, Gateway A is configured using an example FQDN provided by a DDNS Service provider. In this case we established the hostname **netgear.dyndns.org** for Gateway A using the

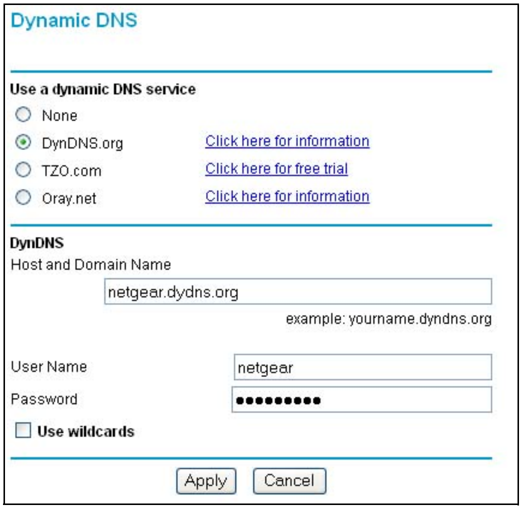
DynDNS service. Gateway B will use the DDNS Service Provider when establishing a VPN tunnel.

In order to establish VPN connectivity Gateway A must be configured to use Dynamic DNS, and Gateway B must be configured to use a DNS hostname to find Gateway A provided by a DDNS Service Provider. Again, the following step-by-step procedures assume that you have already registered with a DDNS Service Provider and have the configuration information necessary to set up the gateways.

Step-By-Step Configuration of FVS318 or FVM318 Gateway A

1. Log in to the FVS318 or FVM318 labeled Gateway A as in the illustration.

   Out of the box, the FVS318 or FVM318 is set for its default LAN address of *http://192.168.0.1*, with its default user name of **admin** and default password of **password**. For this example we will assume you have set the local LAN address as 10.5.6.1 for Gateway A and have set your own password.
2. Click **Dynamic DNS** on the left side of the Settings management GUI.
3. Access the Web site of one of the dynamic DNS service providers whose names appear in the 'Use a dynamic DNS service' list, and register for an account.
   For example, for dyndns.org, click the link or go to www.dyndns.org.



Dynamic DNS

Use a dynamic DNS service

○ None
● DynDNS.org — Click here for information
○ TZO.com — Click here for free trial
○ Oray.net — Click here for information

DynDNS

Host and Domain Name: netgear.dydns.org

example: yourname.dyndns.org

User Name: netgear

Password: ●●●●●●●●●

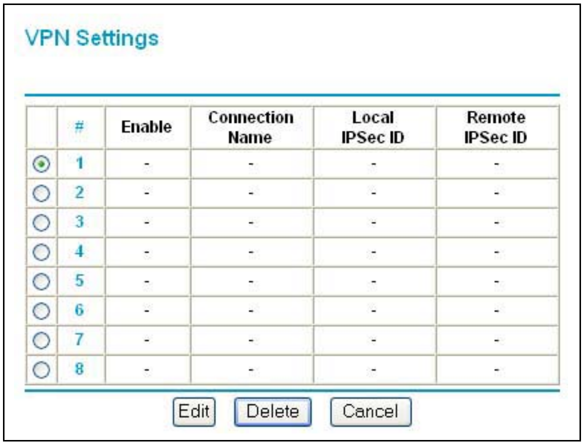
□ Use wildcards

Figure H-2: Dynamic DNS Setup menu

4. Select the **Use a dynamic DNS service** radio button for the service you are using. In this example we are using www.DynDNS.org as the service provider.
   – Type the Host Name that your dynamic DNS service provider gave you.
     The dynamic DNS service provider may call this the domain name. In this example we are using dyndns.org as the domain suffix.
   – Type the User Name for your dynamic DNS account. In this example we used netgear as the Host Name. This means that the complete FQDN we are using is netgear.dyndns.org and the Host Name is "netgear."
   – Type the Password (or key) for your dynamic DNS account.
5. Click **Apply** to save your configuration.

Note: The router supports only basic DDNS and the login and password may not be secure. If your ISP assigns a private WAN IP address, such as 192.168.x.x or 10.x.x.x, the dynamic DNS service will not work because private addresses will not be routed on the Internet.

6. Click **VPN Settings** on the left side of the Settings management GUI.

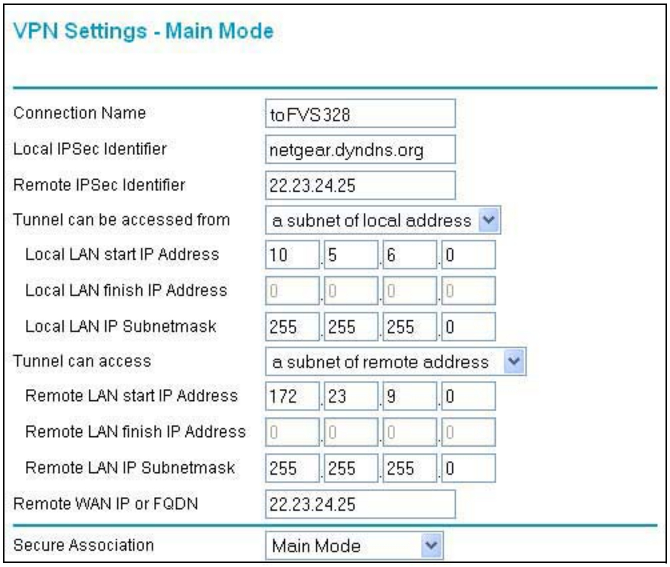


VPN Settings

	#	Enable	Connection Name	Local IPSec ID	Remote IPSec ID
●	1	-	-	-	-
○	2	-	-	-	-
○	3	-	-	-	-
○	4	-	-	-	-
○	5	-	-	-	-
○	6	-	-	-	-
○	7	-	-	-	-
○	8	-	-	-	-

Figure H-3: NETGEAR FVS318 VPN Settings Pre-Configuration

7. Click the radio button of first available VPN leg (all 8 links are available in the example). Click **Edit**. This will take you to the VPN Settings – Main Mode Menu.



VPN Settings - Main Mode

Connection Name	toFVS328
Local IPSec Identifier	netgear.dyndns.org
Remote IPSec Identifier	22.23.24.25
Tunnel can be accessed from	a subnet of local address
Local LAN start IP Address	10 . 5 . 6 . 0
Local LAN finish IP Address	0 . 0 . 0 . 0
Local LAN IP Subnetmask	255 . 255 . 255 . 0
Tunnel can access	a subnet of remote address
Remote LAN start IP Address	172 . 23 . 9 . 0
Remote LAN finish IP Address	0 . 0 . 0 . 0
Remote LAN IP Subnetmask	255 . 255 . 255 . 0
Remote WAN IP or FQDN	22.23.24.25
Secure Association	Main Mode

Figure H-4: NETGEAR FVS318 VPN Settings (part 1) – Main Mode

– In the Connection Name box, enter in a unique name for the VPN tunnel to be configured between the NETGEAR devices. For this example we have used **toFVS328**.

– Enter a Local IPSec Identifier name for the NETGEAR FVS318 Gateway A. This name must be entered in the other endpoint as Remote IPSec Identifier. In this example we used **netgear.dyndns.org** (the FQDN) as the local identifier.

– Enter a Remote IPSec Identifier name for the remote NETGEAR FVS328 Gateway B. This name must be entered in the other endpoint as Local IPSec Identifier. In this example we used **22.23.24.25** as the remote identifier.

– Choose a subnet from local address from the “Tunnel can be accessed” from pull-down menu.

– Type the starting LAN IP Address of Gateway A (**10.5.6.1** in our example) in the Local IP Local LAN start IP Address field.

– Type the finishing LAN IP Address of Gateway A (**0.0.0.0** in our example) in the Local IP Local LAN finish IP Address field.

– Type the LAN Subnet Mask of Gateway A (**255.255.255.0** in our example) in the **Local** LAN IP Subnetmask field.

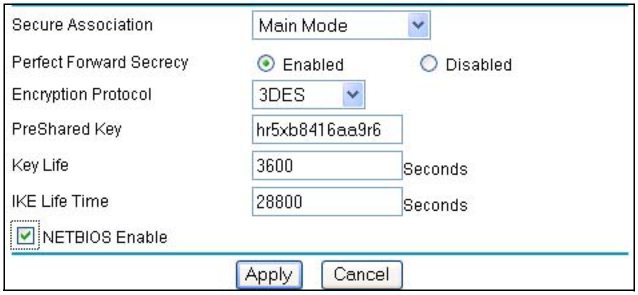
– Choose a subnet from local address from the “Tunnel can access” pull-down menu.

– Type the starting LAN IP Address of Gateway B (**172.23.9.1** in our example) in the Local IP Remote LAN Start IP Address field.

– Type the finishing LAN IP Address of Gateway B (**0.0.0.0** in our example) in the Local IP Remote LAN Finish IP Address field.

– Type the LAN Subnet Mask of Gateway B (**255.255.255.0** in our example) in the Remote LAN IP Subnetmask field.

– Type the WAN IP address (**22.23.24.25** in our example) of Gateway B in the Remote WAN IP or FQDN field.



Secure Association	Main Mode	
Perfect Forward Secrecy	● Enabled	○ Disabled
Encryption Protocol	3DES	
PreShared Key	hr5xb8416aa9r6	
Key Life	3600	Seconds
IKE Life Time	28800	Seconds
☑ NETBIOS Enable		

Figure H-5: Figure 4 – NETGEAR FVS318 VPN Settings (part 2) – Main Mode

– From the Secure Association drop-down box, select Main Mode.

– Next to Perfect Forward Secrecy, select the Enabled radio button.

– From the Encryption Protocol drop-down box, select 3DES.

– In the PreShared Key box, type a unique text string to be used as the shared key between Gateway A and Gateway B. In this example we used **hr5xb84l6aa9r6**. You must make sure the key is the same for both gateways.

– In the Key Life box, enter in 3600 seconds.

– In the IKE Life Time, enter 28800 seconds.

– Check the NETBIOS Enable box if you wish to pass NetBIOS traffic over the VPN tunnel, allowing functions, such as Microsoft Network Neighborhood browsing.

8. Click the Apply button in the lower center of the screen to save all changes and return to the VPN Settings screen.

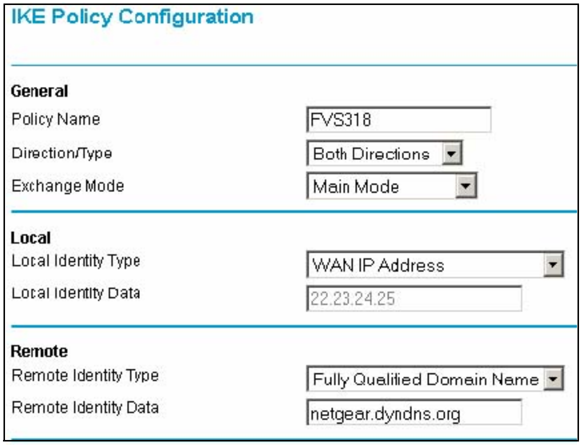
9. When the screen returns to the VPN Settings, make sure the Enable check box is selected.

Step-By-Step Configuration of FVS328 Gateway B

1. Log in to the NETGEAR FVS328, labeled Gateway B in the illustration.

   Out of the box, the FVS328 is set for its default LAN address of *http://192.168.0.1,* with its default user name of **admin** and default password of **password**. For this example we will assume you have set the local LAN address as 172.23.9.1 for Gateway B.

2. Click IKE Policies link under the VPN category and click Add on the IKE Policies Menu.



IKE Policy Configuration

General

Policy Name: FVS318

Direction/Type: Both Directions

Exchange Mode: Main Mode

Local

Local Identity Type: WAN IP Address

Local Identity Data: 22.23.24.25

Remote

Remote Identity Type: Fully Qualified Domain Name

Remote Identity Data: netgear.dyndns.org

Figure H-6: NETGEAR FVS328 IKE Policy Configuration – Part 1

– Enter an appropriate name for the policy in the Policy Name field. This name is not supplied to the remote VPN Endpoint. It is used to help you manage the IKE policies. In our example we have used FVS318 as the Policy Name. In the Policy Name field type **FVS318**.

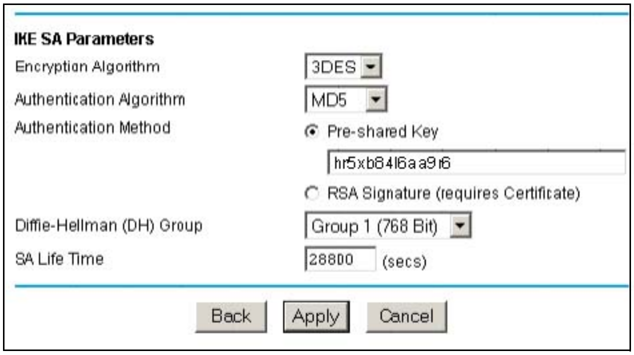
– From the Direction/Type drop-down box, select Both Directions.

– From the Exchange Mode drop-down box, select Main Mode.

– From the Local Identity drop-down box, select WAN IP Address (WAN IP address will automatically be populated into the Local Identity Data field after policy is applied).

– From the Remote Identity drop-down box, select Fully Qualified Domain Name.

– Type the FQDN (**netgear.dnydns.org** in our example) in the Remote Identity Data field.



IKE SA Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: MD5

Authentication Method: ● Pre-shared Key

hr5xb84l6aa9r6

○ RSA Signature (requires Certificate)

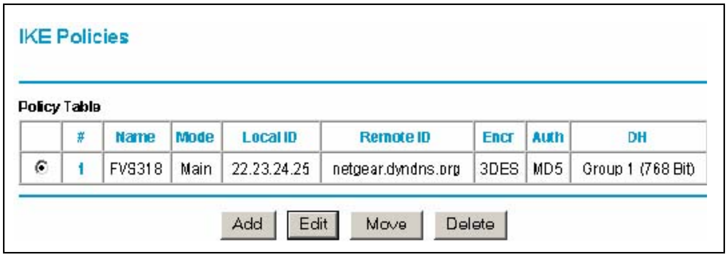
Diffie-Hellman (DH) Group: Group 1 (768 Bit)

SA Life Time: 28800 (secs)

Figure H-7: NETGEAR FVS328 IKE Policy Configuration – Part 2

- – From the Encryption Algorithm drop-down box, select 3DES.
- – From the Authentication Algorithm drop-down box, select MD5.
- – From the Authentication Method radio button, select Pre-shared Key.
- – In the Pre-Shared Key field, type **hr5xb84l6aa9r6**. You must make sure the key is the same for both gateways.
- – From the Diffie-Hellman (DH) Group drop-down box, select Group 1 (768 Bit).
- – In the SA Life Time field, type 28800.

3. Click Apply. This will bring you back to the IKE Policies Menu.



IKE Policies

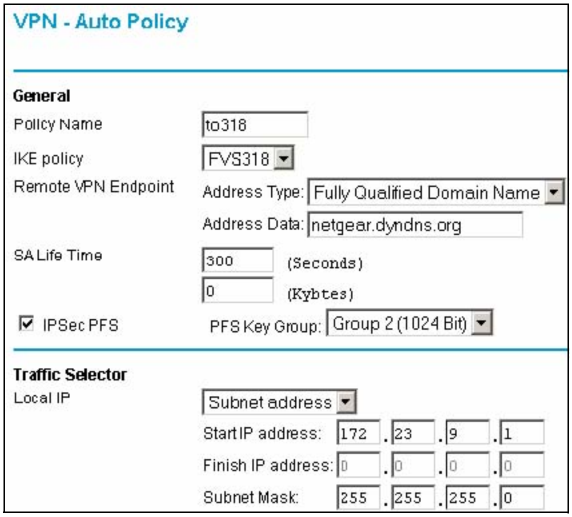
Policy Table

	#	Name	Mode	Local ID	Remote ID	Encr	Auth	DH
●	1	FVS318	Main	22.23.24.25	netgear.dyndns.org	3DES	MD5	Group 1 (768 Bit)

Figure H-8: NETGEAR FWG114P v2 IKE Policies (Post Configuration)

The FVS318 IKE Policy is now displayed in the IKE Policies page.

4. Click the VPN Policies link under the VPN category on the left side of the Settings management GUI. This will take you to the VPN Policies Menu page. Click Add Auto Policy. This will open a new screen titled VPN – Auto Policy.



VPN - Auto Policy

General

Policy Name: to318

IKE policy: FVS318

Remote VPN Endpoint: Address Type: Fully Qualified Domain Name

Address Data: netgear.dyndns.org

SA Life Time: 300 (Seconds)

0 (Kybtes)

☑ IPSec PFS — PFS Key Group: Group 2 (1024 Bit)

Traffic Selector

Local IP: Subnet address

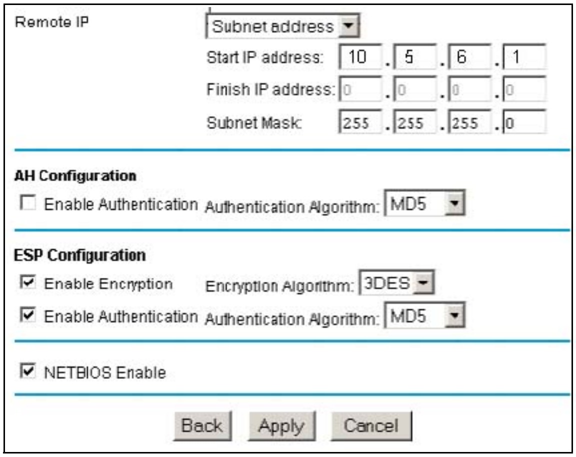
Start IP address: 172 . 23 . 9 . 1

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Figure H-9: NETGEAR FVS328 VPN – Auto Policy (part 1)

- Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. In our example we have used to318 as the Policy Name. In the Policy Name field type **to318**.
- From the IKE policy drop-down box, select the IKE Policy that was set up in the earlier step – the FVS318 IKE Policy.
- From the Remote VPN Endpoint Address Type drop-down box, select IP Address.
- Type the WAN IP Address of Gateway A (**14.15.16.17** in our example) in the Remote VPN Endpoint Address Data field.
- Type **300** in the SA Life Time (Seconds) field.
- Type **0** in the SA Life Time (Kbytes) field.
- Check the IPSec PFS check box.
- From the PFS Key Group drop-down box, select Group 2 (1024 Bit).
- From the Traffic Selector Local IP drop-down box, select Subnet address.
- Type the starting LAN IP Address of Gateway B (**172.23.9.1** in our example) in the Local IP Start IP Address field.
- Type the finishing LAN IP Address of Gateway B (**0.0.0.0** in our example) in the Local IP Finish IP Address field.
- Type the LAN Subnet Mask of Gateway B (**255.255.255.0** in our example) in the Local IP Subnet Mask field.



Remote IP: Subnet address

Start IP address: 10 . 5 . 6 . 1

Finish IP address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

AH Configuration

□ Enable Authentication Authentication Algorithm: MD5

ESP Configuration

☑ Enable Encryption Encryption Algorithm: 3DES

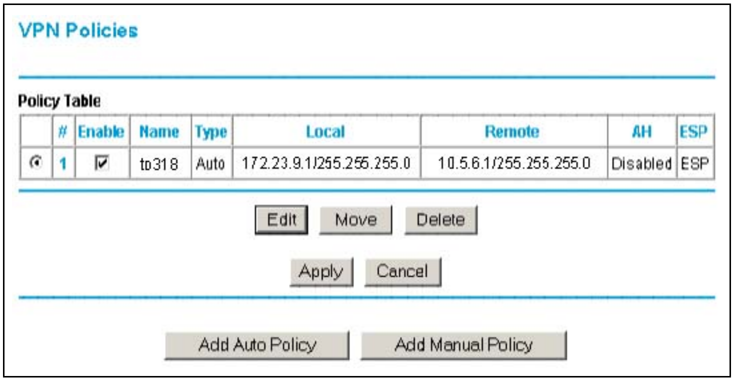
☑ Enable Authentication Authentication Algorithm: MD5

☑ NETBIOS Enable

Figure H-10: NETGEAR FVS328 VPN – Auto Policy (part 2)

- From the Traffic Selector Remote IP drop-down box, select Subnet address.
- Type the starting LAN IP Address of Gateway A (**10.5.6.1** in our example) in the Remote IP Start IP Address field.
- Type the finishing LAN IP Address of Gateway A (**0.0.0.0** in our example) in the Remote IP Finish IP Address field.
- Type the LAN Subnet Mask of Gateway A (**255.255.255.0** in our example) in the Remote IP Subnet Mask field.
- From the AH Configuration Authentication Algorithm drop-down box, select MD5.
- Select the Enable Encryption check box.
- From the ESP Configuration Encryption Algorithm drop-down box, select 3DES.
- Select the Enable Authentication check box.
- From the ESP Configuration Authentication Algorithm drop-down box, select MD5.
- Select the NETBIOS Enable check box.

5. Click the Apply Button. You will be taken back to the VPN Policies Menu page.



VPN Policies

Policy Table

	#	Enable	Name	Type	Local	Remote	AH	ESP
●	1	☑	to318	Auto	172.23.9.1/255.255.255.0	10.5.6.1/255.255.255.0	Disabled	ESP

Figure H-11: NETGEAR FVS328 VPN Policies Menu (Post Configuration)

6. When the screen returns to the VPN Policies, make sure the Enable check box is selected. Click the Apply button.

Test the VPN Connection

1. From a PC behind the NETGEAR FVS318 or FVM318 Gateway A, attempt to ping the remote FWG114P v2 Gateway B LAN Interface address (example address 172.23.9.1).
2. From the FVS318 or FVM318, click the Router Status link on the left side of the Settings management menu. Click the Show VPN Status button. This will take you to the IPSec Connection Status Screen. If the connection is functioning properly, the State fields will show "Estab."
3. From the FVS328, click the VPN Status link under the VPN section of the main menu. The VPN Logs and status are displayed.

Glossary

Use the list below to find definitions for technical terms used in this manual.

802.11 Standard

802.11, or IEEE 802.11, is a type of radio technology used for wireless local area networks (WLANs). It is a standard that has been developed by the IEEE (Institute of Electrical and Electronic Engineers), *http://standards.ieee.org*. The IEEE is an international organization that develops standards for hundreds of electronic and electrical technologies. The organization uses a series of numbers, like the Dewey Decimal system in libraries, to differentiate between the various technology families.

The 802 subgroup (of the IEEE) develops standards for local and wide area networks with the 802.11 section reviewing and creating standards for wireless local area networks.

Wi-Fi , 802.11, is composed of several standards operating in different radio frequencies: 802.11b is a standard for wireless LANs operating in the 2.4 GHz spectrum with a bandwidth of 11 Mbps; 802.11a is a different standard for wireless LANs, and pertains to systems operating in the 5 GHz frequency range with a bandwidth of 54 Mbps. Another standard, 802.11g, is for WLANS operating in the 2.4 GHz frequency but with a bandwidth of 54 Mbps.

802.11a Standard

An IEEE specification for wireless networking that operates in the 5 GHz frequency range (5.15 GHz to 5.85 GHz) with a maximum 54 Mbps data transfer rate. The 5 GHz frequency band is not as crowded as the 2.4 GHz frequency, because the 802.11a specification offers more radio channels than the 802.11b. These additional channels can help avoid radio and microwave interference.

802.11b Standard

International standard for wireless networking that operates in the 2.4 GHz frequency range (2.4 GHz to 2.4835 GHz) and provides a throughput of up to 11 Mbps. This is a very commonly used frequency. Microwave ovens, cordless phones, medical and scientific equipment, as well as Bluetooth devices, all work within the 2.4 GHz frequency band.

802.11d Standard

802.11d is an IEEE standard supplementary to the Media Access Control (MAC) layer in 802.11 to promote worldwide use of 802.11 WLANs. It will allow access points to communicate information on the permissible radio channels with acceptable power levels for client devices. The devices will automatically adjust based on geographic requirements.

The purpose of 11d is to add features and restrictions to allow WLANs to operate within the rules of these countries. Equipment manufacturers do not want to produce a wide variety of country-specific products and users that travel do not want a bag full of country-specific WLAN PC cards. The outcome will be country-specific firmware solutions.

802.11e Standard

802.11e is a proposed IEEE standard to define quality of service (QoS) mechanisms for wireless gear that gives support to bandwidth-sensitive applications such as voice and video.

802.11g Standard

Similar to 802.11b, this physical layer standard provides a throughput of up to 54 Mbps. It also operates in the 2.4 GHz frequency band but uses a different radio technology in order to boost overall bandwidth.

802.11i

This is the name of the IEEE Task Group dedicated to standardizing WLAN security. The 802.11i Security has a frame work based on RSN (Robust Security Mechanism). RSN consists of two parts: 1) The Data Privacy Mechanism and 2) Security Association Management.

The Data Privacy Mechanism supports two proposed schemes: TKIP and AES. TKIP (Temporal Key Integrity) is a short-term solution that defines software patches to WEP to provide a minimally adequate level of data privacy. AES or AES-OCB (Advanced Encryption Standard and Offset Codebook) is a robust data privacy scheme and is a longer-term solution.

Security Association Management is addressed by a) RSN Negotiation Procedures, b) IEEE 802.1x Authentication and c) IEEE 802.1x Key management.

The standards are being defined to naturally co-exist with pre-RSN networks that are currently deployed.

802.11n Standard

A recently formed (Oct 2003) IEEE official task group referred to as: 802.11n or "TGn" for the 100 Mbps wireless physical layer standard protocol. Current published ratification date is December 2005. As of February 2004, no draft specification has been written - It is expected to use both the 2.4 and 5GHz frequencies.

AES (Advanced Encryption Standard)

A symmetric 128-bit block data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES works at multiple network layers simultaneously. The National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce selected the algorithm, called Rijndael (pronounced Rhine Dahl or Rain Doll), out of a group of five algorithms under consideration, including one called MARS from a large research team at IBM. AES is expected to replace WEP as a WLAN encryption method in 2003.

Access Point (AP)

A wireless LAN transceiver or "base station" that can connect a wired LAN to one or many wireless devices. Access points can also bridge to each other.

There are various types of access points, also referred to as base stations, used in both wireless and wired networks. These include bridges, hubs, switches, routers and gateways. The differences between them are not always precise, because certain capabilities associated with one can also be added to another. For example, a router can do bridging, and a hub may also be a switch. But they are all involved in making sure data is transferred from one location to another.

A bridge connects devices that all use the same kind of protocol. A router can connect networks that use differing protocols. It also reads the addresses included in the packets and routes them to the appropriate computer station, working with any other routers in the network to choose the best path to send the packets on. A wireless hub or access point adds a few capabilities such as roaming and provides a network connection to a variety of clients, but it does not allocate bandwidth. A switch is a hub that has extra intelligence: It can read the address of a packet and send it to the appropriate computer station. A wireless gateway is an access point that provides additional capabilities such as NAT routing, DHCP, firewalls, security, etc.

Ad-Hoc mode

A client setting that provides independent peer-to-peer connectivity in a wireless LAN. An alternative set-up is one where PCs communicate with each other through an AP. See access point and Infrastructure mode.

Bandwidth

The amount of transmission capacity that is available on a network at any point in time. Available bandwidth depends on several variables such as the rate of data transmission speed between networked devices, network overhead, number of users, and the type of device used to connect PCs to a network. It is similar to a pipeline in that capacity is determined by size: the wider the pipe, the more water can flow through it; the more bandwidth a network provides, the more data can flow through it. Standard 802.11b provides a bandwidth of 11 Mbps; 802.11a and 802.11g provide a bandwidth of 54 Mbps.

Bits per second (bps)

A measure of data transmission speed over communication lines based on the number of bits that can be sent or received per second. Bits per second—bps—is often confused with bytes per second—Bps. While "bits" is a measure of transmission speed, "bytes" is a measure of storage capability. 8 bits make a byte, so if a wireless network is operating at a bandwidth of 11 megabits per second (11 Mbps or 11 Mbits/sec), it is sending data at 1.375 megabytes per second (1.375 Mbps).

Bluetooth Wireless Technology

A technology specification for linking portable computers, personal digital assistants (PDAs) and mobile phones for short-range transmission of voice and data across a global radio frequency band without the need for cables or wires. Bluetooth is a frequency-hopping technology in the 2.4 GHz frequency spectrum, with a range of 30 feet and up to 11Mbps raw data throughput.

Bridge

A product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, wireless, Ethernet or token ring). Wireless bridges are commonly used to link buildings in campuses.

Client or Client devices

Any computer connected to a network that requests services (files, print capability) from another member of the network. Clients are end users. Wi-Fi client devices include PC Cards that slide into laptop computers, mini-PCI modules embedded in laptop computers and mobile computing devices, as well as USB and PCI/

ISA bus Wi-Fi radios. Client devices usually communicate with hub devices like access points and gateways.

Collision avoidance

A network node characteristic for proactively detecting that it can transmit a signal without risking a collision, thereby ensuring a more reliable connection.

Crossover cable

A special cable used for networking two computers without the use of a hub. Crossover cables may also be required for connecting a cable or DSL modem to a wireless gateway or access point. Instead of the signals transferring in parallel paths from one set of plugs to another, the signals "crossover." If an eight-wire cable was being used, for instance, the signal would start on pin one at one end of the cable and end up on pin eight at the other end. They "cross-over" from one side to the other.

CSMA-CA (Carrier Sense Multiple Action)

CSMA/CA is the principle medium access method employed by IEEE 802.11 WLANs. It is a "listen before talk": method of minimizing (but not eliminating) collisions caused by simultaneous transmission by multiple radios. IEEE 802.11 states collision avoidance method rather than collision detection must be used, because the standard employs half duplex radios—radios capable of transmission or reception—but not both simultaneously.

Unlike conventional wired Ethernet nodes, a WLAN station cannot detect a collision while transmitting. If a collision occurs, the transmitting station will not receive an ACKnowledge packet from the intended receive station. For this reason, ACK packets have a higher priority than all other network traffic. After completion of a data transmission, the receive station will begin transmission of the ACK packet before any other node can begin transmitting a new data packet. All other stations must wait a longer pseudo randomized period of time before transmitting. If an ACK packet is not received, the transmitting station will wait for a subsequent opportunity to retry transmission

CSMA-CD (Carrier Sense Multiple Action/Collision Detection)

A method of managing traffic and reducing noise on an Ethernet network. A network device transmits data after detecting that a channel is available. However, if two devices transmit data simultaneously, the sending devices detect a collision and retransmit after a random time delay.

DHCP (Dynamic Host Configuration Protocol)

A utility that enables a server to dynamically assign IP addresses from a predefined list and limit their time of use so that they can be reassigned. Without DHCP, an IT Manager would have to manually enter in all the IP addresses of all the computers on the network. When DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned to it.

Diversity: antenna

A type of antenna system that uses two antennas to maximize reception and transmission quality and reduce interference

DNS (Domain Name System)
A program that translates URLs to IP addresses by accessing a database maintained on a collection of Internet servers. The program works behind the scenes to facilitate surfing the Web with alpha versus numeric addresses. A DNS server converts a name like mywebsite.com to a series of numbers like 107.22.55.26. Every website has its own specific IP address on the Internet.

Encryption Key
An alphanumeric (letters and/or numbers) series that enables data to be encrypted and then decrypted so it can be safely shared among members of a network. WEP uses an encryption key that automatically encrypts outgoing wireless data. On the receiving side, the same encryption key enables the computer to automatically decrypt the information so it can be read.

Enhanced Data Encryption through TKIP
To improve data encryption, Wi-Fi Protected Access utilizes its Temporal Key Integrity Protocol (TKIP). TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. Through these enhancements, TKIP addresses all WEP known vulnerabilities.

Enterprise-level User Authentication via 802.1x and EAP
WEP has almost no user authentication mechanism. To strengthen user authentication, Wi-Fi Protected Access implements 802.1x and the Extensible Authentication Protocol (EAP). Together, these implementations provide a framework for strong user authentication. This framework utilizes a central authentication server, such as RADIUS, to authenticate each user on the network before they join it, and also employs "mutual authentication" so that the wireless user doesn’t accidentally join a rogue network that might steal its network credentials.

ESSID (more commonly referred to as SSID – Short Set Identifier)
The identifying name of an 802.11 wireless network. When you specify your correct ESSID in your client setup you ensure that you connect to your wireless network rather than another network in range. (See SSID.) The ESSID can be called by different terms, such as Network Name, Preferred Network, SSID or Wireless LAN Service Area.

Ethernet
International standard networking technology for wired implementations. Basic 10BaseT networks offer a bandwidth of about 10 Mbps. Fast Ethernet (100 Mbps) and Gigabit Ethernet (1000 Mbps) are becoming popular.

Firewall
A system that secures a network and prevents access by unauthorized users. Firewalls can be software, hardware or a combination of both. Firewalls can prevent unrestricted access into a network, as well as restrict data from flowing out of a network.

Gateway

In the wireless world, a gateway is an access point with additional software capabilities such as providing NAT and DHCP. Gateways may also provide VPN support, roaming, firewalls, various levels of security, etc.

Hot Spot (also referred to as Public Access Location)

A place where you can access Wi-Fi service. This can be for free or for a fee. HotSpots can be inside a coffee shop, airport lounge, train station, convention center, hotel or any other public meeting area. Corporations and campuses are also implementing HotSpots to provide wireless Internet access to their visitors and guests. In some parts of the world, HotSpots are known as CoolSpots.

Hub

A multiport device used to connect PCs to a network via Ethernet cabling or via Wi-Fi. Wired hubs can have numerous ports and can transmit data at speeds ranging from 10 Mbps to multigigabyte speeds per second. A hub transmits packets it receives to all the connected ports. A small wired hub may only connect 4 computers; a large hub can connect 48 or more. Wireless hubs can connect hundreds.

HZ (‘hertz”)

The international unit for measuring frequency, equivalent to the older unit of cycles per second. One megahertz (MHz) is one million hertz. One gigahertz (GHz) is one billion hertz. The standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 535—1605 kHz, the FM broadcast radio frequency band is 88—108 MHz, and wireless 802.11b LANs operate at 2.4 GHz.

IEEE (Institute of Electrical and Electronics Engineers)

A membership organization (*www.ieee.org*) that includes engineers, scientists and students in electronics and allied fields. It has more than 300,000 members and is involved with setting standards for computers and communications.

IEEE 802.11

A set of specifications for LANs from The Institute of Electrical and Electronics Engineers (IEEE). Most wired networks conform to 802.3, the specification for CSMA/CD based Ethernet networks or 802.5, the specification for token ring networks. 802.11 defines the standard for wireless LANs encompassing three incompatible (non-interoperable) technologies: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and Infrared. WECA’s (Wireless Ethernet Compatibility Alliance – now Wi-Fi Alliance) focus is on 802.11b, an 11 Mbps high-rate DSSS standard for wireless networks.

Infrastructure mode

A client setting providing connectivity to an access point (AP). As compared to Ad-Hoc mode, whereby PCs communicate directly with each other, clients set in Infrastructure Mode all pass data through a central AP. The AP not only mediates wireless network traffic in the immediate neighborhood, but also provides communication with the wired network. See Ad-Hoc and AP.

IP (Internet Protocol) address

A 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network.

ISO Network Model

A network model developed by the International Standards Organization (ISO) that consists of seven different levels, or layers. By standardizing these layers, and the interfaces in between, different portions of a given protocol can be modified or changed as technologies advance or systems requirements are altered. The seven layers are:

- Physical
- Data Link
- Network
- Transport
- Session
- Presentation
- Application

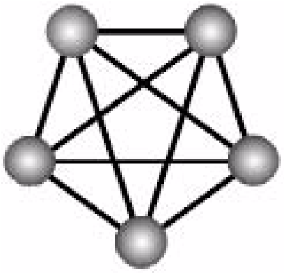
The IEEE 802.11 Standard encompasses the physical layer (PHY) and the lower portion of the data link layer. The lower portion of the data link layer is often referred to as the Medium Access Controller (MAC) sublayer.

MAC (Media Access Control)

Every wireless 802.11 device has its own specific MAC address hard-coded into it. This unique identifier can be used to provide security for wireless networks. When a network uses a MAC table, only the 802.11 radios that have had their MAC addresses added to that network's MAC table will be able to get onto the network.

Mesh Networks

Also called mesh topology, mesh is a network topology in which devices are connected with many redundant interconnections between network nodes. In a full mesh topology every node has a connection to every other node in the network. Mesh networks may be wired or wireless.



Mesh network

In a wireless mesh example, each of the spheres below represent a mesh router. Corporate servers and printers may be shared by attaching to each mesh router. For wireless access to the mesh, an access point must be attached to any one of the mesh routers.

Multiple Input Multiple Output (MIMO)

MIMO refers to radio links with multiple antennas at the transmitter and the receiver side to improve the performance of the wireless link.

NAT (Network Address Translation)

A network capability that enables a houseful of computers to dynamically share a single incoming IP address from a dial-up, cable or xDSL connection. NAT takes the single incoming IP address and creates new IP address for each client computer on the network.

Network name

Identifies the wireless network for all the shared components. During the installation process for most wireless networks, you need to enter the network name or SSID. Different network names are used when setting up your individual computer, wired network or workgroup.

NIC (Network Interface Card)

A type of PC adapter card that either works without wires (Wi-Fi) or attaches to a network cable to provide two-way communication between the computer and network devices such as a hub or switch. Most office wired NICs operate at 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet) or 10/100 Mbps dual speed. High-speed Gigabit and 10 Gigabit NIC cards are also available. See PC Card.

PC card (also called PCMCIA)

A removable, credit-card-sized memory or I/O (input/output) device that fits into a Type 2 PCMCIA standard slot, PC Cards are used primarily in PCs, portable computers, PDAs and laptops. PC Card peripherals include Wi-Fi cards, memory cards, modems, NICs, hard drives, etc.

PCI adapter

A high-performance I/O computer bus used internally on most computers. Other bus types include ISA and AGP. PCIs and other computer buses enable the addition of internal cards that provide services and features not supported by the motherboard or other connectors.

Peer-to-peer network (also called Ad-Hoc in WLANs)

A wireless or wired computer network that has no server or central hub or router. All the networked PCs are equally able to act as a network server or client, and each client computer can talk to all the other wireless computers without having to go through an access point or hub. However, since there is no central base station to monitor traffic or provide Internet access, the various signals can collide with each other, reducing overall performance.

PHY

The lowest layer within the OSI Network Model. It deals primarily with transmission of the raw bit stream over the PHYsical transport medium. In the case of wireless LANs, the transport medium is free space. The

PHY defines parameters such as data rates, modulation method, signaling parameters, transmitter/receiver synchronization, etc. Within an actual radio implementation, the PHY corresponds to the radio front end and baseband signal processing sections.

Plug and Play

A computer system feature that provides for automatic configuration of add-ons and peripheral devices such as wireless PC Cards, printers, scanners and multimedia devices.

Proxy server

Used in larger companies and organizations to improve network operations and security, a proxy server is able to prevent direct communication between two or more networks. The proxy server forwards allowable data requests to remote servers and/or responds to data requests directly from stored remote server data

Range

The distance away from your access point that your wireless network can reach. Most Wi-Fi systems will provide a range of a hundred feet or more. Depending on the environment and the type of antenna used, Wi-Fi signals can have a range of up to mile

Residential gateway

A wireless device that connects multiple PCs, peripherals and the Internet on a home network. Most Wi-Fi residential gateways provide DHCP and NAT as well.

RJ-45

Standard connectors used in Ethernet networks. Even though they look very similar to standard RJ-11 telephone connectors, RJ-45 connectors can have up to eight wires, whereas telephone connectors have only four.

Roaming

Moving seamlessly from one AP coverage area to another with your laptop or desktop with no loss in connectivity.

Rogue Access Point

"Rogue AP" is a term used to describe an unauthorized access point that is connected on the main home or corporate network or operating in a stand-alone mode (in a parking lot or in a neighbor's building). Rogue APs, by definition, are not under the management of network administrators and do not conform to network security policies and may present a severe security risk. Ideally, it is best to have some type of WLAN system that does not allow rogue access points to easily be added to an existing WLAN.

Router

A device that forwards data packets from one local area network (LAN) or wide area network (WAN) to another. Based on routing tables and routing protocols, routers can read the network address in each transmitted frame and make a decision on how to send it via the most efficient route based on traffic load, line costs, speed, bad connections, etc.

Satellite broadband

A wireless high-speed Internet connection provided by satellites. Some satellite broadband connections are two-way—up and down. Others are one-way, with the satellite providing a high-speed downlink and then using a dial-up telephone connection or other land-based system for the uplink to the Internet.

Server

A computer that provides its resources to other computers and devices on a network. These include print servers, Internet servers and data servers. A server can also be combined with a hub or router.

Site survey

The process whereby a wireless network installer inspects a location prior to putting in a wireless network. Site surveys are used to identify the radio- and client-use properties of a facility so that access points can be optimally placed.

SSID (also called ESSID)

A 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS. (Also called ESSID.) The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID.

A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet, it does not supply any security to the network. An SSID is also referred to as a Network Name because essentially it is a name that identifies a wireless network.

SSL (Secure Sockets Layer)

Commonly used encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions. When an SSL session begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server in order to have a secret key exchange for that session.

Subnetwork or Subnet

Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect to the central network through a router, hub or gateway. Each individual wireless LAN will probably use the same subnet for all the local computers it talks to.

Switch

A type of hub that efficiently controls the way multiple devices use the same network so that each can operate at optimal performance. A switch acts as a networks traffic cop: rather than transmitting all the packets it receives to all ports as a hub does, a switch transmits packets to only the receiving port.

TCP (Transmission Control Protocol)

A protocol used along with the Internet Protocol (IP) to send data in the form of individual units (called packets) between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet.

For example, when a web page is downloaded from a web server, the TCP program layer in that server divides the file into packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network. At the other end, TCP reassembles the individual packets and waits until they have all arrived to forward them as a single file.

TCP/IP

The underlying technology behind the Internet and communications between computers in a network. The first part, TCP, is the transport part, which matches the size of the messages on either end and guarantees that the correct message has been received. The IP part is the user's computer address on a network. Every computer in a TCP/IP network has its own IP address that is either dynamically assigned at startup or permanently assigned. All TCP/IP messages contain the address of the destination network as well as the address of the destination station. This enables TCP/IP messages to be transmitted to multiple networks (subnets) within an organization or worldwide.

TKIP

A security feature that is a WEP enhancement: Temporal Key Integrity Protocol and Message Integrity Check (MIC) is a modification of WEP to defend against known attacks (WEP+ four patches for key mixing, message integrity, rekeying, initialization vector protection)

USB (Universal Serial Bus)

A high-speed bidirectional serial connection between a PC and a peripheral that transmits data at the rate of 12 megabits per second. The new USB 2.0 specification provides a data rate of up to 480 Mbps, compared to standard USB at only 12 Mbps. 1394, FireWire and iLink all provide a bandwidth of up to 400 Mbps.

VoIP (Voice over IP)

Voice transmission using Internet Protocol to create digital packets distributed over the Internet. VoIP can be less expensive than voice transmission using standard analog packets over POTS (Plain Old Telephone Service).

VPN (Virtual Private Network)

A type of technology designed to increase the security of information transferred over the Internet. VPN can work with either wired or wireless networks, as well as with dial-up connections over POTS. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate servers and database.

War Chalking

The act of making chalk marks on outdoor surfaces (walls, sidewalks, buildings, sign posts, trees) to indicate the existence of an open wireless network connection, usually offering an Internet connection so that others can benefit from the free wireless access. The open connections typically come from the access points of wireless networks located within buildings to serve enterprises. The chalk symbols indicate the type of access point that is available at that specific spot.

There are three basic designs that are currently used: a pair of back-to-back semicircles, which denotes an open node; a closed circle, which denotes a closed node; a closed circle with a “W” inside, which denotes a node equipped with WEP. Warchalkers also draw identifiers above the symbols to indicate the password that can be used to access the node, which can easily be obtained with sniffer software.

As a recent development, the debate over the legality of warchalking is still going on.

The practice stems from the U.S. Depression-era culture of wandering hobos who would make marks outside of homes to indicate to other wanderers whether the home was receptive to drifters or was inhospitable.

War Driving

War driving is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, you need a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.

Some people have made a sport out of war driving, in part to demonstrate the ease with which wireless LANs can be compromised. With an omnidirectional antenna and a geophysical positioning system (GPS), the war driver can systematically map the locations of 802.11b wireless access points.

WEP (Wired Equivalent Privacy)

Basic wireless security provided by Wi-Fi. In some instances, WEP may be all a home or small-business user needs to protect wireless data. WEP is available in 40-bit (also called 64-bit), or in 108-bit (also called 128-bit) encryption modes. As 108-bit encryption provides a longer algorithm that takes longer to decode, it can provide better security than basic 40-bit (64-bit) encryption.

Wi-Fi (Wireless Fidelity)

Another name for IEEE 802.11b. Products certified as Wi-Fi are interoperable with each other even if they are from different manufacturers. A user with a Wi-Fi product can use any brand of access point with any other brand of client hardware that is built to the Wi-Fi standard.

Wi-Fi Alliance (formerly WECA – Wireless Ethernet Compatibility Alliance)

The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification. Currently the Wi-Fi Alliance has 193 member companies from around the world, and 509 products have received Wi-Fi certification since certification began in March of 2000. The goal of the Wi-Fi Alliance's members is to enhance the user experience through product interoperability (*www.weca.net*).

Wi-Fi Protected Access (WPA)

WPA is a security technology for wireless networks that improves on the authentication and encryption features of WEP (Wired Equivalent Privacy). In fact, WPA was developed by the networking industry in response to the shortcomings of WEP.

One of the key technologies behind WPA is the Temporal Key Integrity Protocol (TKIP). TKIP addresses the encryption weaknesses of WEP. Another key component of WPA is built-in authentication that WEP does not offer. With this feature, WPA provides roughly comparable security to VPN tunneling with WEP,

with the benefit of easier administration and use. This is similar to 802.1x support and requires a RADIUS server in order to implement. The Wi-Fi Alliance will call this, 'WPA-Enterprise.'
One variation of WPA is called WPA Pre Shared Key or WPA-PSK for short - this provides an authentication alternative to an expensive RADIUS server. WPA-PSK is a simplified but still powerful form of WPA most suitable for home Wi-Fi networking. To use WPA-PSK, a person sets a static key or "passphrase" as with WEP. But, using TKIP, WPA-PSK automatically changes the keys at a preset time interval, making it much more difficult for hackers to find and exploit them. The Wi-Fi Alliance will call this, 'WPA-Personal.'

Wi-Fi Protected Access and IEEE 802.11i Comparison

Wi-Fi Protected Access will be forward-compatible with the IEEE 802.11i security specification currently under development by the IEEE. Wi-Fi Protected Access is a subset of the current 802.11i draft, taking certain pieces of the 802.11i draft that are ready to bring to market today, such as its implementation of 802.1x and TKIP. These features can also be enabled on most existing Wi-Fi CERTIFIED products as a software upgrade. The main pieces of the 802.11i draft that are not included in Wi-Fi Protected Access are secure IBSS, secure fast handoff, secure de-authentication and disassociation, as well as enhanced encryption protocols such as AES-CCMP. These features are either not yet ready for market or will require hardware upgrades to implement.

Wi-Fi Protected Access for the Enterprise

Wi-Fi Protected Access effectively addresses the WLAN security requirements for the enterprise and provides a strong encryption and authentication solution prior to the ratification of the IEEE 802.11i standard. In an enterprise with IT resources, Wi-Fi Protected Access should be used in conjunction with an authentication server such as RADIUS to provide centralized access control and management. With this implementation in place, the need for add-on solutions such as VPNs may be eliminated, at least for the express purpose of securing the wireless link in a network.

Wi-Fi Protected Access for Home/SOHO

In a home or Small Office/ Home Office (SOHO) environment, where there are no central authentication servers or EAP framework, Wi-Fi Protected Access runs in a special home mode. This mode, also called Pre-Shared Key (PSK), allows the use of manually-entered keys or passwords and is designed to be easy to set up for the home user. All the home user needs to do is enter a password (also called a master key) in their access point or home wireless gateway and each PC that is on the Wi-Fi wireless network. Wi-Fi Protected Access takes over automatically from that point. First, the password allows only devices with a matching password to join the network, which keeps out eavesdroppers and other unauthorized users. Second, the password automatically kicks off the TKIP encryption process, described above.

Wi-Fi Protected Access for Public Access

The intrinsic encryption and authentication schemes defined in Wi-Fi Protected Access may also prove useful for Wireless Internet Service Providers (WISPs) offering Wi-Fi public access in "hot spots" where secure transmission and authentication is particularly important to users unknown to each other. The authentication capability defined in the specification enables a secure access control mechanism for the service providers and for mobile users not utilizing VPN connections.

Wi-Fi Protected Access in "Mixed Mode" Deployment

In a large network with many clients, a likely scenario is that access points will be upgraded before all the Wi-Fi clients. Some access points may operate in a "mixed mode", which supports both clients running Wi-Fi Protected Access and clients running original WEP security. While useful for transition, the net effect of supporting both types of client devices is that security will operate at the less secure level (WEP), common to all the devices. Therefore, organizations will benefit by accelerating the move to Wi-Fi Protected Access for all Wi-Fi clients and access points.

WiMAX

An IEEE 802.16 Task Group that provides a specification for fixed broadband wireless access systems employing a point-to-multipoint (PMP) architecture. Task Group 1 of IEEE 802.16 developed a point-to-multipoint broadband wireless access standard for systems in the frequency range 10-66 GHz. The standard covers both the Media Access Control (MAC) and the physical (PHY) layers. Ratification is expected in second half of 2004.

Wireless Multimedia (WMM)

WMM (Wireless Multimedia) 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, like video, audio, or voice will have a higher priority than normal traffic. For WMM to function correctly, wireless clients must also support WMM.

Wireless Networking

Wireless Networking refers to the infrastructure enabling the transmission of wireless signals. A network ties things together and enables resource sharing.

WLAN (Wireless LAN)

Also referred to as LAN. A type of local-area network that uses wireless or high-frequency radio waves rather than wires to communicate between nodes.