

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



## NETGEAR

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

202-10027-01  
Version 2.0  
March 2004

© 2004 by NETGEAR, Inc. All rights reserved.

## 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 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).

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

(1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

## **Bestätigung des Herstellers/Importeurs**

Es wird hiermit bestätigt, daß das ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P 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 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.



# Contents

## Chapter 1

### About This Manual

|                                    |     |
|------------------------------------|-----|
| Audience, Conventions, Scope ..... | 1-1 |
| How to Use this Manual .....       | 1-2 |
| How to Print this Manual .....     | 1-3 |

## Chapter 2

### Introduction

|                                                           |     |
|-----------------------------------------------------------|-----|
| Key Features of the FWG114P .....                         | 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 |
| A Powerful, True Firewall with Content Filtering .....    | 2-3 |
| Security .....                                            | 2-4 |
| Autosensing Ethernet Connections with Auto Uplink .....   | 2-4 |
| Extensive Protocol Support .....                          | 2-4 |
| Easy Installation and Management .....                    | 2-5 |
| Package Contents .....                                    | 2-6 |
| The FWG114P Front Panel .....                             | 2-7 |
| The FWG114P Rear Panel .....                              | 2-8 |

## Chapter 3

### Connecting the FWG114P 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 Wireless Firewall/Print Server ..... | 3-4 |
| Verify That Basic Requirements Are Met .....                | 3-4 |

|                                                                           |      |
|---------------------------------------------------------------------------|------|
| Basic Setup Troubleshooting Tips .....                                    | 3-9  |
| FWG114P Setup Wizard Auto Detection .....                                 | 3-9  |
| Wizard-Detected Login Account Setup .....                                 | 3-10 |
| Wizard-Detected Dynamic IP Account Setup .....                            | 3-12 |
| Wizard-Detected Fixed IP Account Setup .....                              | 3-13 |
| How to Configure the Serial Port as the Primary Internet Connection ..... | 3-14 |
| Testing Your Internet Connection .....                                    | 3-16 |
| Manually Configuring Your Internet Connection .....                       | 3-17 |
| How to Manually Configure the Primary Internet Connection .....           | 3-18 |

## **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 .....                               | 4-7  |
| Before You Change the SSID and WEP Settings .....            | 4-8  |
| How to Set Up and Test Basic Wireless Connectivity .....     | 4-9  |
| How to Restrict Wireless Access by MAC Address .....         | 4-10 |
| How to Configure WEP .....                                   | 4-11 |
| How to Configure WPA .....                                   | 4-12 |
| How to Configure WPA-PSK .....                               | 4-13 |

## **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 ..... | 7-5  |
| Printing from the Macintosh .....                               | 7-8  |
| Windows Printer Port Management .....                           | 7-9  |
| Troubleshooting the Print Server .....                          | 7-11 |

## **Chapter 8**

### **Virtual Private Networking**

|                                                          |     |
|----------------------------------------------------------|-----|
| Overview of FWG114P 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 .....        | 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 to FWG114P 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 to FWG114P with Certificates .....              | 8-26 |
| Netgear VPN Client to FWG114P .....                                 | 8-32 |
| Configuration Profile .....                                         | 8-32 |
| Step-By-Step Configuration of FWG114P 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 .....                             | 8-45 |
| From the FWG114P to the Client PC .....                             | 8-46 |
| Monitoring the PC VPN Connection .....                              | 8-46 |
| Viewing the FWG114P 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 .....                        | 9-5 |
| Upgrading the Router Software .....                             | 9-6 |
| Configuration File Management .....                             | 9-6 |
| Restoring and Backing Up the Configuration .....                | 9-7 |
| Erasing the Configuration .....                                 | 9-8 |
| Changing the Administrator Password .....                       | 9-8 |

## **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**

|                                                                |     |
|----------------------------------------------------------------|-----|
| 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 |
| <b>Glossary</b>                                      |      |
| List of Glossary Terms .....                         | G-1  |
| <b>Index</b>                                         |      |



# Chapter 1

## About This Manual

Congratulations on your purchase of the NETGEAR® ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P. This chapter introduces important features of this manual.

### Audience, Conventions, Scope

---

This reference manual assumes that the reader has basic-to-intermediate computer and Internet skills. However, basic computer network, Internet, firewall, and networking technology tutorial information is provided in the appendices.

This guide uses the following typographical conventions:

**Table 1.        Typographical conventions**

|                           |                                                                        |
|---------------------------|------------------------------------------------------------------------|
| <i>italics</i>            | Emphasis, books, CDs, URL names                                        |
| <b>bold times roman</b>   | User input                                                             |
| <code>courier font</code> | Screen text, file and server names, extensions, commands, IP addresses |

This guide uses the following formats to highlight special messages:

|                                                                                     |                                                                                              |
|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
|  | <b>Note:</b> This format is used to highlight information of importance or special interest. |
|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|

This manual is written according to these specifications.

**Table 1-1.        Manual Specifications**

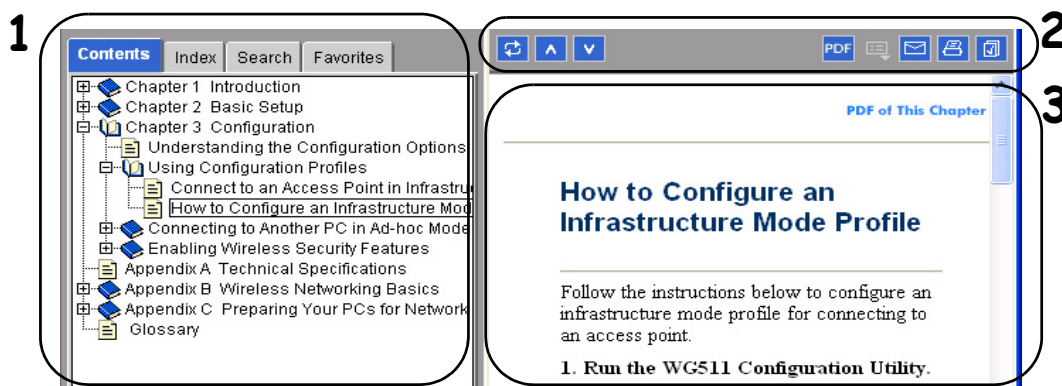
|                                     |                                                                 |
|-------------------------------------|-----------------------------------------------------------------|
| Product Version                     | ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P v2 |
| Firmware Version                    | Version 2 Release 06                                            |
| Manual Version and Publication Date | Manual Version 2.0, March 2004                                  |

|                                                                                     |                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <b>Note:</b> Product updates are available on the NETGEAR, Inc. Web site at <a href="http://kbserver.netgear.com/products/FWG114P.asp">http://kbserver.netgear.com/products/FWG114P.asp</a> . |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## How to Use this Manual

---

The HTML version of this manual includes a variety of navigation features as well as links to PDF versions of the full manual and individual chapters.



**Figure Preface -2: HTML version of this manual**

1. **Left pane.** Use the left pane to view the Contents, Index, Search, and Favorites tabs.

To view the HTML version of the manual, you must have a version 4 or later IE or Netscape browser with JavaScript enabled.

2. **Toolbar buttons.** Use the toolbar buttons across the top to navigate, print pages, and more.



The Show in Contents button locates the current topic in the Contents tab.



Previous/Next buttons display the previous or next topic.



The PDF button links to a PDF version of the full manual.



The Print button prints the current topic. Using this button when a step-by-step procedure is displayed will send the entire procedure to your printer. You do not have to worry about specifying the correct range of pages.

3. **Right pane.** Use the right pane to view the contents of the manual. Also, each page of the manual includes a [PDF of This Chapter](#) link at the top right which links to a PDF file containing just the currently selected chapter of the manual.

## How to Print this Manual

---

To print this manual you may choose one of the following options, according to your needs:

- **Printing a “How To” Sequence of Steps in the HTML View.** Use the *Print* button  on the upper right of the toolbar to print the currently displayed topic. Using this button when a step-by-step procedure is displayed will send the entire procedure to your printer. You do not have to worry about specifying the correct range of pages.
- **Printing a Chapter.** Use the [PDF of This Chapter](#) link at the top right 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 PDF button in the toolbar at the top right of the browser window.
  - Click the PDF button  on the upper right of the toolbar. The PDF version of the chapter you were viewing opens in a browser window.
  - Click the print icon in the upper left of the window.

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



# Chapter 2

## Introduction

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

### Key Features of the FWG114P

---

The ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P, 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 provides highly reliable Internet access.

The FWG114P 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 uses Stateful Packet Inspection for Denial of Service attack (DoS) attack protection and intrusion detection. The FWG114P 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 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.
- 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 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 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 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 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 enterprise class strong security with RADIUS and certificate authentication as well as dynamic encryption key generation.
- WPA-PSK pre-shared key authentication without the overhead of RADIUS servers but with all of the strong security of WPA.
- 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 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 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.

## A Powerful, True Firewall with Content Filtering

Unlike simple Internet sharing NAT routers, the FWG114P 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 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 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 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 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 Wireless Firewall/Print Server supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). For further information about TCP/IP, refer to [Appendix B, “Network, Routing, and Firewall Basics.”](#)

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

The FWG114P 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 in settings where you want to manage the IP address scheme of your organization.

- Automatic configuration of attached PCs by DHCP.

The FWG114P 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 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 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 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 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.

## Package Contents

---

The product package should contain the following items:

- ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P.
- AC power adapter.
- Category 5 (Cat 5) Ethernet cable.
- FWG114P Installation Guide (M-10150-02).
- *Resource CD for the ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P (SW-10023-02)*, 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 Front Panel

The front panel of the FWG114P 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 Front Panel**

**Table 2-1. LED Descriptions**

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

## The FWG114P Rear Panel

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



**Figure 1-2: FWG114P 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 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 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 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 includes a built-in Web Configuration Manager. To access the configuration menus on the FWG114P, 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.

**Note:** For help with DHCP configuration, please refer to [Appendix C, “Preparing Your Network.”](#)

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 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 Wireless Firewall/Print Server

---

This section provides instructions for connecting the FWG114P Wireless Firewall/Print Server. Also, the *Resource CD for the ProSafe Wireless 802.11g Firewall/Print Server Model FWG114P (SW-10023-02)*, included with your router, contains an animated Installation Assistant to help you through this procedure.

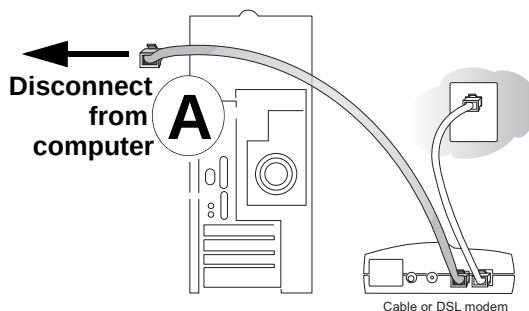
### Verify That Basic Requirements Are Met

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-10023-02)*.

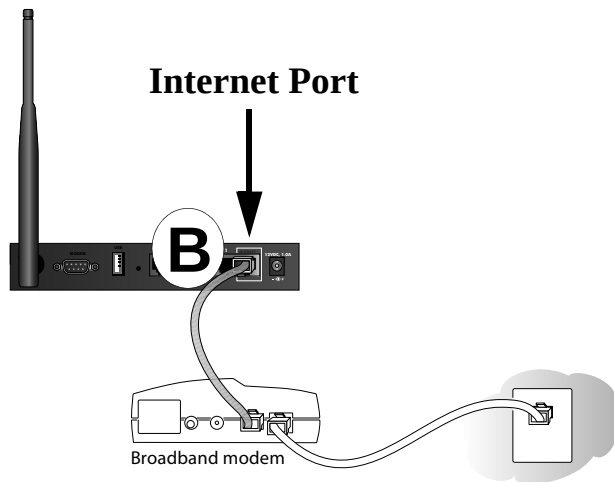
#### 1. CONNECT THE WIRELESS FIREWALL/PRINT SERVER

- 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.



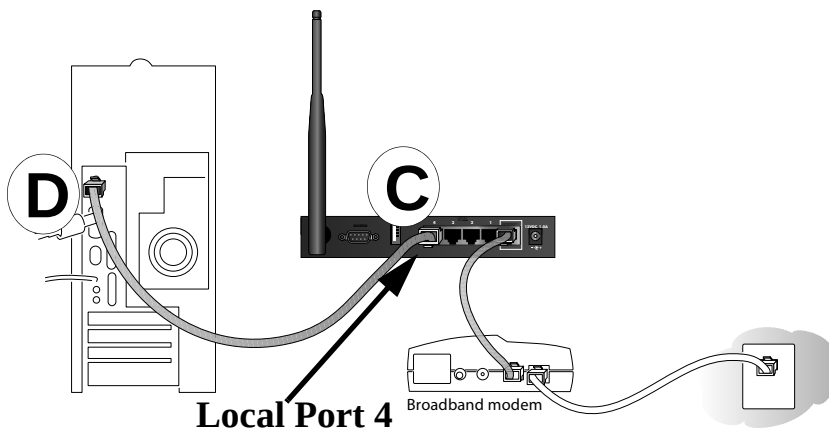
**Figure 3-1: Disconnect the broadband modem**

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



**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**

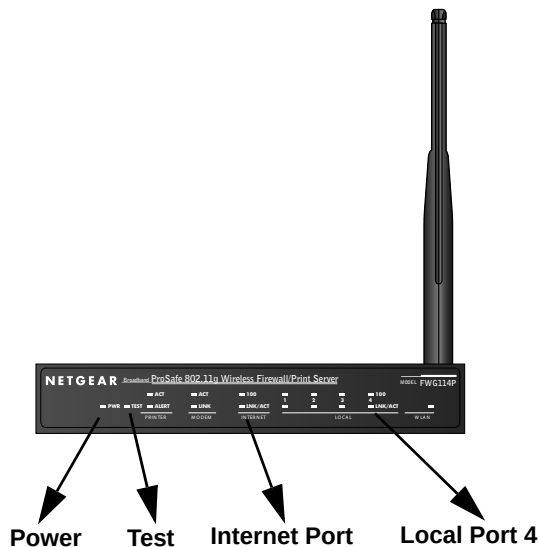
**Note:** The FWG114P incorporates Auto Uplink™ technology which eliminates the need to worry about crossover cables by automatically adjusting to the cable type.

## 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.

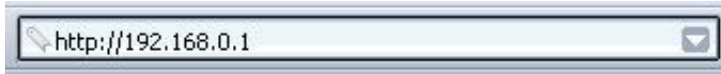


**Figure 3-4: Verify the connections to the firewall**

- 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.



**Figure 3-5: Log in to the firewall**

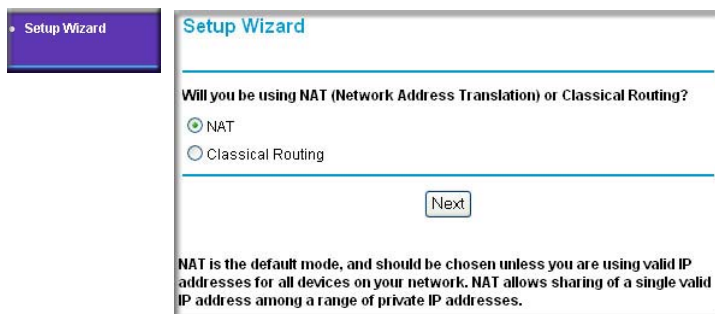
- c. Enter **admin** for the router user name and **password** for the router password, both in lower case letters. A login window opens as shown here:



**Figure 3-6: Login window**

- d. After logging in to the router, you will see the Internet connection Setup Wizard on the settings main page.

## 4. RUN THE SETUP WIZARD TO CONNECT TO THE INTERNET



**Figure 3-7: 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 uses.

**Note:** If you choose not to use NAT, each computer on the LAN connected to the FWG114P must have a valid public IP address in the same subnet as the Wan port of the FWG114P. 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-10023-02)*.

## FWG114P Setup Wizard Auto Detection

---

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

- Let the FWG114P 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

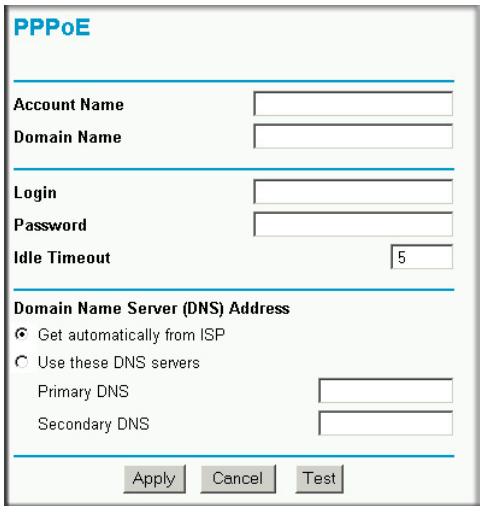
- Fixed IP address assignment

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 3-8](#):



The screenshot shows a web-based configuration window titled "PPPoE". It contains several input fields and a section for DNS settings. The fields are: "Account Name", "Domain Name", "Login", "Password", and "Idle Timeout" (with a value of 5). Below these is a section titled "Domain Name Server (DNS) Address" with two radio buttons: "Get automatically from ISP" (selected) and "Use these DNS servers". Under the second radio button are fields for "Primary DNS" and "Secondary DNS". At the bottom are three buttons: "Apply", "Cancel", and "Test".

**Figure 3-8: 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.

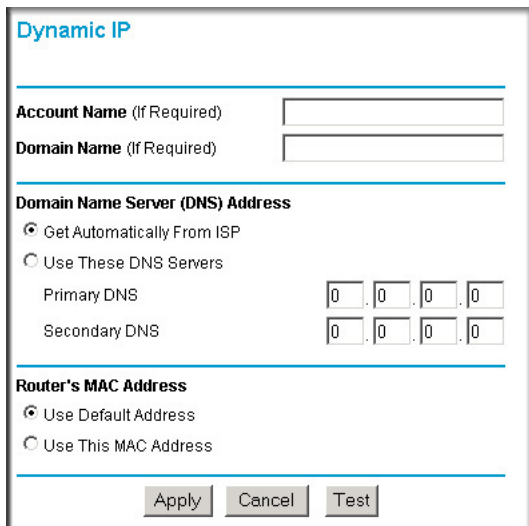
3. The Idle Timeout setting determines how long to wait after there is no activity before disconnecting from the Internet. This is useful in countries where Internet service charges are based on the amount of time connected to the Internet. Whenever a computer on the network requests access to the Internet the FWG114P 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 3-9](#) below:



The screenshot shows a window titled "Dynamic IP" with a light blue header. Below the header, there are two text input fields: "Account Name (If Required)" and "Domain Name (If Required)". Below these is a section titled "Domain Name Server (DNS) Address" with two radio buttons: "Get Automatically From ISP" (selected) and "Use These DNS Servers". Under "Use These DNS Servers", there are two rows of IP address input fields: "Primary DNS" and "Secondary DNS", each with four boxes for the octets. Below this is a section titled "Router's MAC Address" with two radio buttons: "Use Default Address" (selected) and "Use This MAC Address". At the bottom of the window are three buttons: "Apply", "Cancel", and "Test".

**Figure 3-9: 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](http://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 3-10](#) below:

The screenshot shows a configuration window titled "Internet IP Address" with the following sections:

- Account Name (If Required):** A text box containing "FWG114P".
- Domain Name (If Required):** An empty text box.
- Internet IP Address:**
  - ☐ Get Dynamically From ISP
  - ☒ Use Static IP Address
  - IP Address:** Four text boxes, each containing "0".
  - IP Subnet Mask:** Four text boxes, each containing "0".
  - Gateway IP Address:** Four text boxes, each containing "0".
- Domain Name Server (DNS) Address:**
  - ☐ Get Automatically From ISP
  - ☒ Use These DNS Servers
  - Primary DNS:** Four text boxes, each empty.
  - Secondary DNS:** Four text boxes, each empty.
- Router's MAC Address:**
  - ☒ Use Default Address
  - ☐ Use This Computer's MAC
  - ☐ Use This MAC Address: An empty text box.

At the bottom are three buttons: "Apply", "Cancel", and "Test".

**Figure 3-10: 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](http://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 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.

The screenshot shows a web-based configuration interface titled "Basic Settings". It contains several sections for configuring an internet connection:

- 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:
  - Password:
  - Telephone:
  - Alternative Telephone:
  - ☒ Connect as required
  - ☐ Disconnect after Idle Time of  min
- Internet IP Address:**
  - ☒ Get Dynamically From ISP
  - ☐ Use Static IP Address:
- DNS IP Address:**
  - ☒ Get Automatically From ISP
  - ☐ Use These DNS Servers
    - Primary DNS:
    - Secondary DNS:
- Modem:**
  - Serial Line Speed:  bps
  - Modem Type:

At the bottom are "Apply" and "Cancel" buttons.

**Figure 3-11: 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 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, you 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

IP Subnet Mask

Gateway IP Address

---

**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

---

### 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

Account Name

Domain Name

---

Login

Password

Idle Timeout  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

---

Figure 3-12: 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 configuration settings to the factory default. Disable NAT only if you plan to install the FWG114P 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 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 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 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.

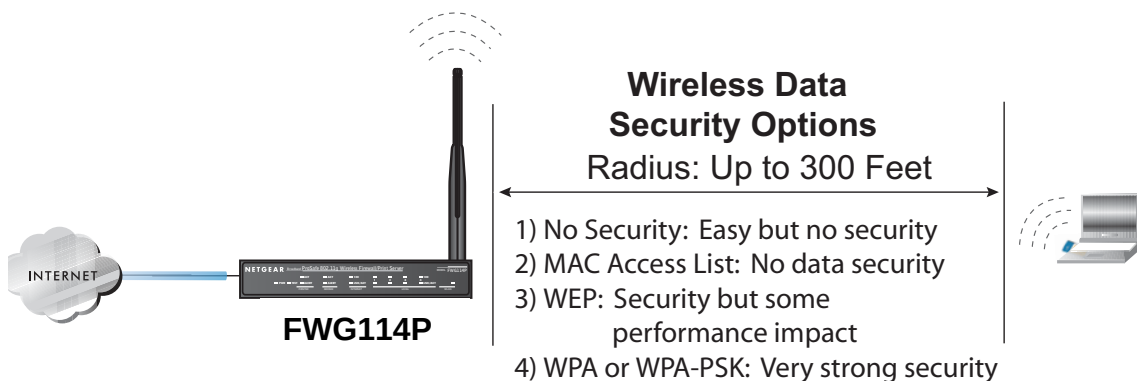
## Implementing Appropriate Wireless Security

---



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



**Figure 4-1: FWG114P 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. 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 or WPA-PSK.** Wi-Fi Protected Access (WPA) data encryption provides data security. The very strong authentication along with dynamic per frame rekeying of WPA 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, click the Wireless link in the Setup section of the main menu. The wireless settings menu will appear, as shown below.

The screenshot shows the 'Wireless Settings' window. It has a title bar 'Wireless Settings' in blue. Below the title bar, there are four sections separated by horizontal lines. The first section is 'Wireless Network' with fields for 'Name (SSID):' (text box with 'NETGEAR'), 'Region:' (dropdown menu with '— Select Region —'), 'Channel:' (dropdown menu with '11 - 2.462GHz'), 'Current Channel No' (text box with 'channel\_no'), and 'Mode:' (dropdown menu with 'g and b'). The second section is 'Wireless Access Point' with two checked checkboxes: 'Enable Wireless Access Point' and 'Allow Broadcast of Name (SSID)'. The third section is 'Wireless Card Access List' with a 'Setup Access List' button. The fourth section is 'Security Options' with four radio buttons: 'Disable' (selected), 'WEP (Wired Equivalent Privacy)', 'WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)', and 'WPA'. At the bottom of the window are 'Apply' and 'Cancel' buttons.

**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 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.
  - **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 default SSID is: **NETGEAR**.
  - **Region.** This field identifies the region where the FWG114P 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.
  - **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 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**

**Table 4-1. Wireless Security Options**

| Field                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Disable</b>                        | Wireless security is not used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>WEP (Wired Equivalent Privacy)</b> | <p>You can select the following WEP options:</p> <p><b>Authentication Type</b></p> <ul style="list-style-type: none"><li>• Open: the FWG114P does not perform any authentication.</li><li>• Shared: WEP shared key authentication. For a full explanation of WEP shared key, see <a href="#">“Authentication and WEP Data Encryption” on page E-2</a>.</li></ul> <p><b>Encryption Strength</b></p> <ul style="list-style-type: none"><li>• If Shared or Open Network Authentication is enabled, you can choose 64- or 128-bit WEP data encryption.</li></ul> <p><b>Note:</b> With Open Network Authentication and 64- or 128-bit WEP Data Encryption, the FWG114P <i>does</i> perform 64- or 128-bit data encryption but <i>does not</i> perform any authentication.</p> <p><b>Security Encryption (WEP) Key</b></p> <p>These key values must be identical on all wireless devices in your network (key 1 must be the same for all, key 2 must be the same for all, and so on).</p> <p>The FWG114P provides two methods for creating WEP encryption keys:</p> <ul style="list-style-type: none"><li>• Passphrase. These characters <i>are</i> case sensitive. Enter a word or group of printable characters in the Passphrase box and click the Generate button.</li></ul> <p><b>Note:</b> Not all wireless adapters support passphrase key generation.</p> <ul style="list-style-type: none"><li>• Manual. These values <i>are not</i> case sensitive.</li></ul> <p>64-bit WEP: enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F).</p> <p>128-bit WEP: enter 26 hexadecimal digits (any combination of 0-9, a-f, or A-F).</p> |

**Table 4-1. Wireless Security Options**

| Field                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WPA-PSK</b><br>(Wi-Fi Protected Access Pre-Shared Key) | <p>WPA Pre-Shared-Key uses a pre-shared key to perform the authentication and generate the initial data encryption keys. Then, it dynamically varies the encryption key. For a full explanation of WPA, see <a href="#">“WPA Wireless Security” on page E-8</a>.</p> <p><b>Note:</b> 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.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>WPA</b>                                                | <p>User authentication is implemented using RADIUS servers. For a full explanation of WPA, see <a href="#">“WPA Wireless Security” on page E-8</a>.</p> <p>Fill in the following:</p> <ul style="list-style-type: none"><li>• Primary Radius Server Name/IP Address<br/>This field is required. Enter the name or IP address of the Radius Server on your LAN.</li><li>• Secondary Radius Server Name/IP Address<br/>This field is optional. Enter the name or IP address of the Secondary Radius Server on your LAN.</li><li>• Radius Port<br/>Enter the port number used for connections to the Radius Server.</li><li>• Radius Shared Key<br/>Enter the desired value for the Radius shared key. This key enables the FWG114P to log in to the Radius server and must match the value used on the Radius server.</li></ul> <p><b>Radius Accounting Option</b></p> <p>The Radius Accounting option can be enabled so that you can track various information like who connected to the network, when they connected, how long they were connected, how much network traffic they generated, and so on.</p> |

## Default Factory Settings

The FWG114P 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 Rear Panel” on page 2-8](#). After you install the FWG114P 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                                                      | <b>NETGEAR</b>                         |
| RF Channel                                                | <b>11 until the region is selected</b> |
| Access Point                                              | <b>Enabled</b>                         |
| SSID broadcast                                            | <b>Enabled</b>                         |
| Wireless Card Access List for<br>Access Point Connections | <b>All wireless stations allowed</b>   |
| WEP Security                                              | <b>Disabled</b>                        |
| Authentication Type                                       | <b>Open System</b>                     |

## 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.

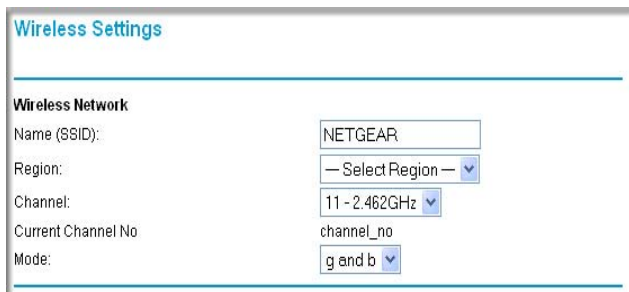
- **SSID:** The Service Set Identification (SSID) identifies the wireless local area network. **Wireless** is the default FWG114P SSID. However, you may customize it by using up to 32 alphanumeric characters. Write your customized SSID on the line below.  
**Note:** The SSID in the wireless firewall/print 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.
- **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 (Pre-Shared Key)**  
Record the WPA-PSK key:  
Key: \_\_\_\_\_
- **WPA RADIUS Settings**  
For WPA, 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. 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.



**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. If they do not match, you will not get a wireless connection to the FWG114P.

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.”

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



**Note:** If you are configuring the FWG114P 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's new settings.

- 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. 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:

- Log in at the default LAN address of <http://192.168.0.1> with the default user name of **admin** and default password of **password**.
- Click **Wireless** in the main menu of the FWG114P. From the Wireless Settings menu, click **Setup Access List**.
- Click the **Turn Access Control On** checkbox to enable MAC filtering.
- Click **Add** to open the Wireless Card Access Setup menu. You can select a device from the list of available wireless cards the FWG114P has discovered in your area, or you can manually enter the MAC address and Device Name (usually the NetBIOS name).
- Click **Add** to add this device to your MAC access control list.



**Note:** When configuring the FWG114P 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.

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.
3. Click the **WEP** radio button. 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.
  - Automatic - Enter a word or group of printable characters in the Passphrase box. This phrase is case sensitive. Click Generate. The four keys will be automatically generated.
  - Manual - 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 the default.

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.

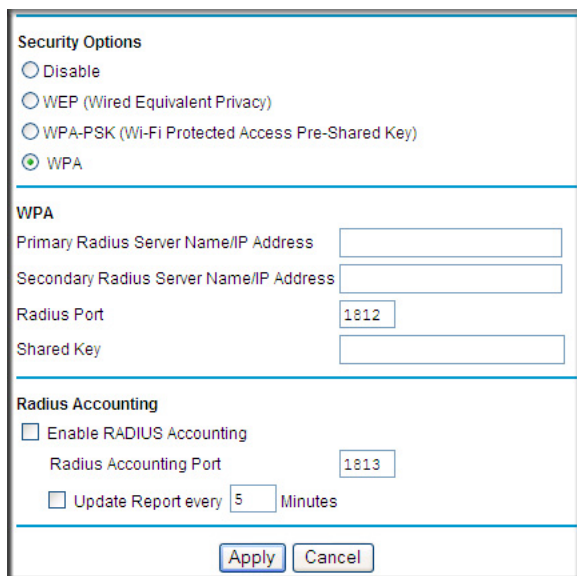
5. Click **Apply** to save your settings.

## How to Configure WPA

**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, 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 Setup section of the main menu of the FWG114P.



The screenshot shows a web-based configuration interface for the FWG114P. It is titled "Security Options" and contains three radio buttons: "Disable", "WEP (Wired Equivalent Privacy)", and "WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)". The "WPA" radio button is selected. Below this, there is a section for "WPA" configuration with four input fields: "Primary Radius Server Name/IP Address", "Secondary Radius Server Name/IP Address", "Radius Port" (with the value "1812" entered), and "Shared Key". Below the WPA section is a section for "Radius Accounting" with two checkboxes: "Enable RADIUS Accounting" and "Update Report every". The "Update Report every" checkbox is checked, and its value is "5" minutes. The "Radius Accounting Port" field has the value "1813" entered. At the bottom of the form are "Apply" and "Cancel" buttons.

**Figure 4-4: Wireless Settings menu**

3. Choose the **WPA** radio button. The WPA menu will open.
4. Enter the Radius settings.
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 Setup section of the main menu of the FWG114P.
3. Choose the **WPA-PSK** radio button. The WPA-PSK menu will open.
4. Enter the pre-shared key in the Passphrase field.
5. Enter the Key Lifetime. This setting determines how often the encryption key is changed. Shorter periods provide greater security, but adversely affect performance.
6. 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. The FWG114P serial port lets you share the broadband connection of another FWG114P, 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 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 3-14](#).

The FWG114P 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 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 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 wireless firewall/print servers to:
  - Share resources on the two LANs.
  - Let users on one FWG114P share the Internet connection of the other FWG114P.
  - Let users on one FWG114P connect to the Internet through the second FWG114P in case the broadband connection of the first FWG114P 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

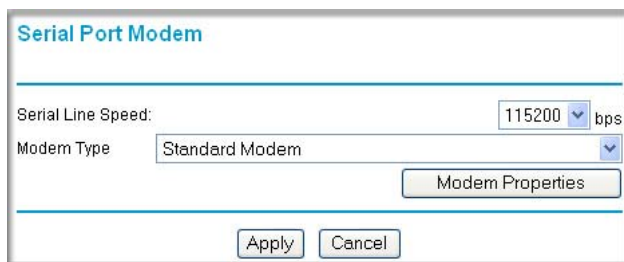
Configuring a serial port modem requires these elements:

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.



**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 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 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

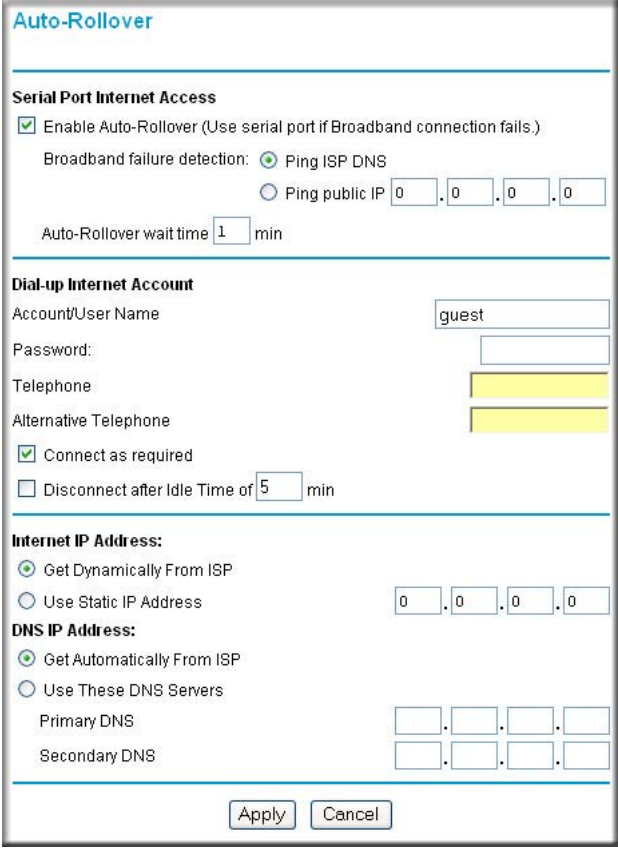
Auto-Rollover requires these elements:

1. A broadband connection to the FWG114P.
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.

### 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.



The screenshot shows the 'Auto-Rollover' configuration window. It is divided into three main sections: 'Serial Port Internet Access', 'Dial-up Internet Account', and 'Internet IP Address:'.  
1. 'Serial Port Internet Access': Contains a checked checkbox 'Enable Auto-Rollover (Use serial port if Broadband connection fails.)'. Below it, 'Broadband failure detection:' has 'Ping ISP DNS' selected with a radio button, and 'Ping public IP' is unselected. The 'Auto-Rollover wait time' is set to '1' min.  
2. 'Dial-up Internet Account': Includes fields for 'Account/User Name' (filled with 'guest'), 'Password', 'Telephone', and 'Alternative Telephone'. Below these are checkboxes for 'Connect as required' (checked) and 'Disconnect after Idle Time of' (set to '5' min).  
3. 'Internet IP Address:': Has 'Get Dynamically From ISP' selected with a radio button, and 'Use Static IP Address' is unselected. Below this is the 'DNS IP Address:' section with 'Get Automatically From ISP' selected and 'Use These DNS Servers' unselected. Fields for 'Primary DNS' and 'Secondary DNS' are present but empty.  
At the bottom are 'Apply' and 'Cancel' buttons.

**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 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

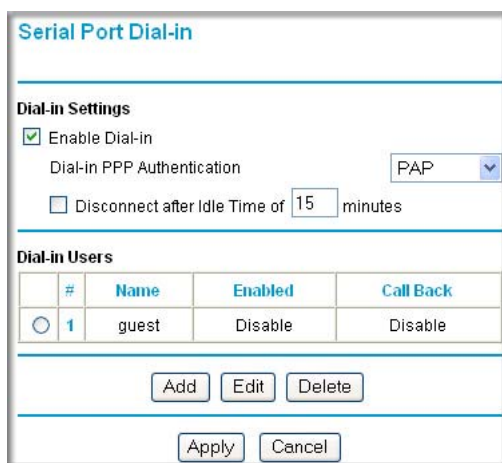
Dial-in requires these elements:

1. A broadband connection to the FWG114P.
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.

## 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**.



The screenshot shows the 'Serial Port Dial-in' configuration window. It has a title bar 'Serial Port Dial-in'. Below the title bar is a section 'Dial-in Settings' containing a checked checkbox 'Enable Dial-in', a dropdown menu for 'Dial-in PPP Authentication' set to 'PAP', and an unchecked checkbox 'Disconnect after Idle Time of' followed by a text box '15' and the word 'minutes'. Below this is a section 'Dial-in Users' containing a table with columns '#', 'Name', 'Enabled', and 'Call Back'. The table has one row with '#1', 'guest', 'Disable', and 'Disable'. Below the table are three buttons: 'Add', 'Edit', and 'Delete'. At the bottom are two buttons: 'Apply' and 'Cancel'.

| # | 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 wireless firewall/print servers.

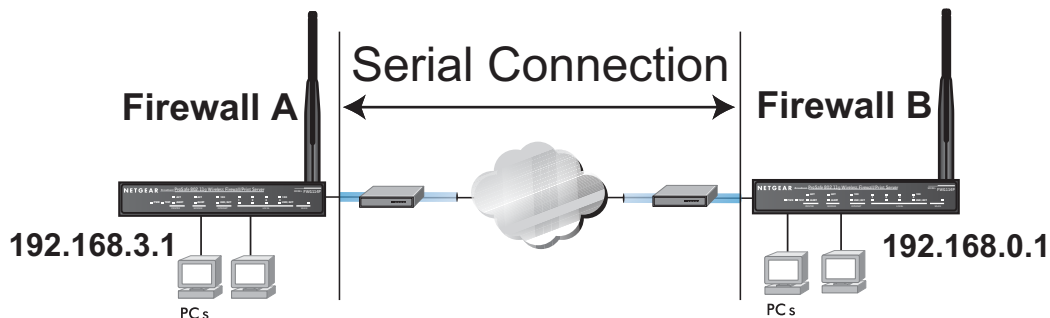


Figure 5-4: LAN-to-LAN network configuration

### Basic Requirements for LAN-to-LAN Connections

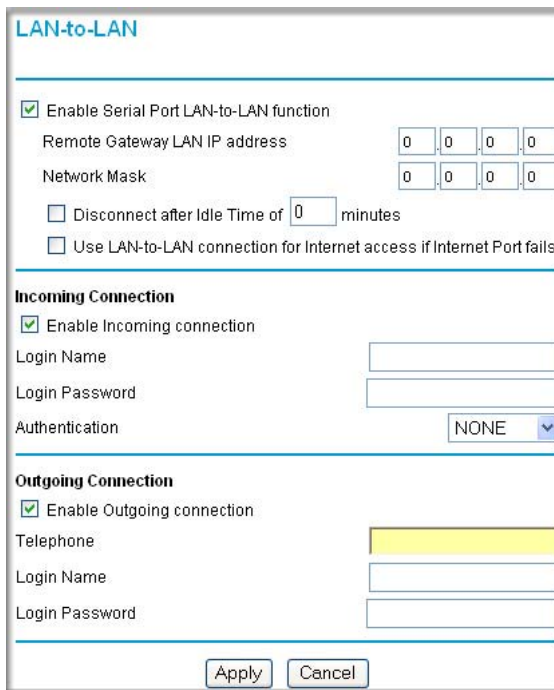
Serial port LAN-to-LAN configurations require these elements:

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 for LAN-to-LAN auto-rollover Internet access.
4. The LAN-to-LAN settings configured and applied to the two FWG114P 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.



The image shows a web-based configuration interface titled "LAN-to-LAN". It is divided into three main sections: "Enable Serial Port LAN-to-LAN function", "Incoming Connection", and "Outgoing Connection".

**Enable Serial Port LAN-to-LAN function:** This section has a checked checkbox. Below it are two rows of IP address input fields. The first row is for the "Remote Gateway LAN IP address" with all four digits set to "0". The second row is for the "Network Mask" with all four digits set to "0". There are two unchecked checkboxes: "Disconnect after Idle Time of 0 minutes" and "Use LAN-to-LAN connection for Internet access if Internet Port fails".

**Incoming Connection:** This section has a checked checkbox. Below it are three input fields: "Login Name", "Login Password", and "Authentication" (a dropdown menu currently showing "NONE").

**Outgoing Connection:** This section has a checked checkbox. Below it are three input fields: "Telephone" (highlighted in yellow), "Login Name", and "Login Password".

At the bottom of the form are two buttons: "Apply" and "Cancel".

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

3. Configure the LAN-to-LAN settings.

**Note:** The LAN subnet address of each FWG114P 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 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 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 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

Add Keyword

Block sites containing these keywords or domain names:

Delete Keyword Clear List

Trusted IP Address

Apply Cancel

**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.