

WatchGuard® Firebox® X Edge User Guide

**Firebox X Edge - Firmware Version 7.2
All Firebox X Edge Standard and Wireless Models**



Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Copyright, Trademark, and Patent Information

Copyright© 1998 - 2005 WatchGuard Technologies, Inc. All rights reserved.

Complete copyright, trademark, patent, and licensing information can be found in an appendix at the end of this book. You can also find it online at:

<http://www.watchguard.com/help/documentation/>

All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This product is for indoor use only.

WatchGuard Firebox Software End-User License Agreement

IMPORTANT - READ CAREFULLY BEFORE ACCESSING WATCHGUARD SOFTWARE:

This Firebox Software End-User License Agreement ("AGREEMENT") is a legal agreement between you (either an individual or a single entity) and WatchGuard Technologies, Inc. ("WATCHGUARD") for the WATCHGUARD Firebox software product, which includes computer software components (whether installed separately on a computer workstation or on the WATCHGUARD hardware product or included on the WATCHGUARD hardware product) and may include associated media, printed materials, and on-line or electronic documentation, and any updates or modifications thereto, including those received through the WatchGuard LiveSecurity Service (or its equivalent), (the "SOFTWARE PRODUCT"). WATCHGUARD is willing to license the SOFTWARE PRODUCT to you only on the condition that you accept all of the terms contained in this Agreement. Please read this Agreement carefully. By installing or using the SOFTWARE PRODUCT you agree to be bound by the terms of this Agreement. If you do not agree to the terms of this AGREEMENT, WATCHGUARD will not license the SOFTWARE PRODUCT to you, and you will not have any rights in the SOFTWARE PRODUCT. In that case, promptly return the SOFTWARE PRODUCT, along with proof of payment, to the authorized dealer from whom you obtained the SOFTWARE PRODUCT for a full refund of the price you paid. The WATCHGUARD hardware product is subject to a separate agreement and limited hardware warranty included with the WATCHGUARD hardware product packaging and/or in the associated user documentation.

1. Ownership and License. The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. This is a license agreement and NOT an agreement for sale. All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and applets incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by WATCHGUARD or its licensors. Your rights to use the SOFTWARE PRODUCT are as specified in this AGREEMENT, and WATCHGUARD retains all rights not expressly granted to you in this

AGREEMENT. Nothing in this AGREEMENT constitutes a waiver of our rights under U.S. copyright law or any other law or treaty.

2. Permitted Uses. You are granted the following rights to the SOFTWARE PRODUCT:

(A) You may install and use the SOFTWARE PRODUCT on any single WATCHGUARD hardware product at any single location and may install and use the SOFTWARE PRODUCT on multiple workstation computers.

(B) To use the SOFTWARE PRODUCT on more than one WATCHGUARD hardware product at once, you must purchase an additional copy of the SOFTWARE PRODUCT for each additional WATCHGUARD hardware product which you want to use it. To the extent that you install copies of the SOFTWARE PRODUCT on additional WATCHGUARD hardware products in accordance with the prior sentence without installing the additional copies of the SOFTWARE PRODUCT included with such WATCHGUARD hardware products, you agree that use of any software provided with or included on the additional WATCHGUARD hardware products that does not require installation will be subject to the terms and conditions of this AGREEMENT. You must also maintain a current subscription to the WatchGuard LiveSecurity Service (or its equivalent) for each additional WATCHGUARD hardware product on which you will use a copy of an updated or modified version of the SOFTWARE PRODUCT received through the WatchGuard LiveSecurity Service (or its equivalent).

(C) In addition to the copies described in Section 2(A), you may make a single copy of the SOFTWARE PRODUCT for backup or archival purposes only.

3. Prohibited Uses. You may not, without express written permission from WATCHGUARD:

(A) Use, copy, modify, merge or transfer copies of the SOFTWARE PRODUCT or printed materials except as provided in this AGREEMENT;

(B) Use any backup or archival copy of the SOFTWARE PRODUCT (or allow someone else to use such a copy) for any purpose other than to replace the original copy in the event it is destroyed or becomes defective;

(C) Sublicense, lend, lease or rent the SOFTWARE PRODUCT;

(D) Transfer this license to another party unless

(i) the transfer is permanent,

(ii) the third party recipient agrees to the terms of this AGREEMENT, and

(iii) you do not retain any copies of the SOFTWARE PRODUCT; or

(E) Reverse engineer, disassemble or decompile the SOFTWARE PRODUCT.

4. Limited Warranty. WATCHGUARD makes the following limited warranties for a period of ninety (90) days from the date you obtained the SOFTWARE PRODUCT from WATCHGUARD or an authorized dealer:

(A) Media. The disks and documentation will be free from defects in materials and workmanship under normal use. If the disks or documentation fail to conform to this warranty, you may, as your sole and exclusive remedy, obtain a replacement free of charge if you return the defective disk or documentation to WATCHGUARD with a dated proof of purchase.

(B) SOFTWARE PRODUCT. The SOFTWARE PRODUCT will materially conform to the documentation that accompanies it. If the SOFTWARE PRODUCT fails to operate in accordance with this warranty, you may, as your sole and exclusive remedy, return all of the SOFTWARE PRODUCT and the documentation to the authorized dealer from whom you obtained it, along with a dated proof of purchase, specifying the problems, and they will provide you with a new version of the SOFTWARE PRODUCT or a full refund, at their election.

Disclaimer and Release. THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 4, 4(A) AND 4(B) ABOVE ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD AND ITS LICENSORS AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD AND ITS LICENSORS, EXPRESS OR IMPLIED, ARISING BY LAW OR

OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN THE SOFTWARE PRODUCT (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY WARRANTY OF NONINFRINGEMENT, ANY WARRANTY THAT THE SOFTWARE PRODUCT WILL MEET YOUR REQUIREMENTS, ANY WARRANTY OF UNINTERRUPTED OR ERROR-FREE OPERATION, ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD AND ITS LICENSORS AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY, THE SOFTWARE PRODUCT).

Limitation of Liability. WATCHGUARD'S LIABILITY (WHETHER IN CONTRACT, TORT, OR OTHERWISE; AND NOTWITHSTANDING ANY FAULT, NEGLIGENCE, STRICT LIABILITY OR PRODUCT LIABILITY) WITH REGARD TO THE SOFTWARE PRODUCT WILL IN NO EVENT EXCEED THE PURCHASE PRICE PAID BY YOU FOR SUCH PRODUCT. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY. IN NO EVENT WILL WATCHGUARD BE LIABLE TO YOU OR ANY THIRD PARTY, WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT), FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT, EVEN IF WATCHGUARD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY.

5. United States Government Restricted Rights. The SOFTWARE PRODUCT is provided with Restricted Rights. Use, duplication or disclosure by the U.S. Government or any agency or instrumentality thereof is subject to restrictions as set forth in subdivision (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, or in subdivision (c)(1) and (2) of the Commercial Computer Software -- Restricted Rights Clause at 48 C.F.R. 52.227-19, as applicable. Manufacturer is WatchGuard Technologies, Inc., 505 5th Ave. South, Suite 500, Seattle, WA 98104.

6. Export Controls. You agree not to directly or indirectly transfer the SOFTWARE PRODUCT or documentation to any country to which such transfer would be prohibited by the U.S. Export Administration Act and the regulations issued thereunder.

7. Termination. This license and your right to use the SOFTWARE PRODUCT will automatically terminate if you fail to comply with any provisions of this AGREEMENT, destroy all copies of the SOFTWARE PRODUCT in your possession, or voluntarily return the SOFTWARE PRODUCT to WATCHGUARD. Upon termination you will destroy all copies of the SOFTWARE PRODUCT and documentation remaining in your control or possession.

8. Miscellaneous Provisions. This AGREEMENT will be governed by and construed in accordance with the substantive laws of Washington excluding the 1980 United National Convention on Contracts for the International Sale of Goods, as amended. This is the entire AGREEMENT between us relating to the SOFTWARE PRODUCT, and supersedes any prior purchase order, communications, advertising or representations concerning the SOFTWARE PRODUCT AND BY USING THE SOFTWARE PRODUCT YOU AGREE TO THESE TERMS. IF THE SOFTWARE PRODUCT IS BEING USED BY AN ENTITY, THE INDIVIDUAL INDICATING AGREEMENT TO THESE TERMS REPRESENTS AND WARRANTS THAT (A) SUCH INDIVIDUAL IS DULY AUTHORIZED TO ACCEPT THIS AGREEMENT ON BEHALF OF THE ENTITY AND TO BIND THE ENTITY TO THE TERMS OF THIS AGREEMENT; (B) THE ENTITY HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THIS AGREEMENT AND PERFORM ITS OBLIGATIONS UNDER THIS AGREEMENT AD// (C) THIS AGREEMENT AND THE PERFORMANCE OF THE ENTITY'S OBLIGATIONS UNDER THIS AGREEMENT DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE ENTITY IS A PARTY. No change or modification of this AGREEMENT will be valid unless it is in writing and is signed by WATCHGUARD.

Version: 040226

Firmware Version: 7.2
Part Number: 1776-0000
Guide Version: 7.2

Abbreviations Used in this Guide

3DES	Triple Data Encryption Standard
BOVPN	Branch Office Virtual Private Network
DES	Data Encryption Standard
DNS	Domain Name Service
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
IP	Internet Protocol
IPSec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
MAC	Media Access Control
MUVPN	Mobile User Virtual Private Network
NAT	Network Address Translation
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
TCP	Transfer Control Protocol
UDP	User Datagram Protocol
URL	Universal Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network
WSEP	WatchGuard Security Event Processor

ADDRESS:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

SUPPORT:

www.watchguard.com/support
support@watchguard.com
U.S. and Canada +877.232.3531
All Other Countries +1.206.613.0456

SALES:

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.521.8340

ABOUT WATCHGUARD

WatchGuard network security solutions provide small- to mid-sized enterprises worldwide with effective, affordable security. Our Firebox line of extendable, integrated security appliances is designed to be fully upgradeable as an organization grows, and to deliver the industry's best combination of security, performance, intuitive interface, and value. WatchGuard Intelligent Layered Security architecture protects against emerging threats effectively and efficiently, and provides the flexibility to integrate additional security functionality and services offered through WatchGuard. Every WatchGuard product comes with an initial LiveSecurity Service subscription to help customers stay on top of security with vulnerability alerts, software updates, expert security instruction, and superior customer care.

FOR MORE INFORMATION: Please visit us at www.watchguard.com or contact your reseller for more information.

Contents

CHAPTER 1	Introduction to Network Security	1
Network Security	1
About Networks	2
<i>Clients and servers</i>	2
Connecting to the Internet	2
Protocols	3
How Information Travels on the Internet	4
IP Addresses	5
<i>Network addressing</i>	5
<i>About DHCP</i>	5
<i>About PPPoE</i>	6
Domain Name Service (DNS)	6
Services	6
Ports	7
Firewalls	8
Firebox® X Edge and Your Network	9
CHAPTER 2	Installing the Firebox X Edge	11
Package Contents	11
Installation Requirements	12
Identifying Your Network Settings	13
<i>About network addressing</i>	13

Static addresses, DHCP, and PPPoE	13
Finding your TCP/IP properties	14
Finding PPPoE settings	17
Disabling the HTTP Proxy Setting	17
Connecting the Firebox X Edge	19
Connecting the Edge to more than seven devices	20
Setting Your Computer to Connect to the Edge	22
If your computer gets its address from DHCP	22
If your computer has a static IP address	23
Running the Quick Setup Wizard	24
Registering and Activating LiveSecurity Service	25
CHAPTER 3 Configuration and Management Basics	27
Navigating the Configuration Pages	28
Using the navigation bar	29
Configuration Overview	30
Firebox System Status Page	30
Network Page	31
Firebox Users Page	33
Administration Page	34
Firewall Page	35
Logging Page	36
WebBlocker Page	37
VPN Page	38
Wizards Page	39
Updating Firebox X Edge Software	39
Factory Default Settings	40
Resetting the Firebox to the factory default settings	41
Restarting the Firebox	42
Local restart	42
Remote restart	43
CHAPTER 4 Changing Your Network Settings	45
Using the Network Setup Wizard	45
Configuring the External Network	46
If your ISP uses DHCP	47
If your ISP uses static IP addresses	48
If your ISP uses PPPoE	49
Configuring the Trusted Network	53
Changing the IP address of the trusted network	53
Using DHCP on the trusted network	54

Setting trusted network DHCP address reservations	55
Configuring the trusted network for DHCP relay	56
Using static IP addresses for trusted computers	57
Adding computers to the trusted network	57
Configuring the Optional Network	58
Enabling the optional network	59
Changing the IP address of the optional network	59
Using DHCP on the optional network	60
Setting optional network DHCP address reservations	60
Configuring the optional network for DHCP relay	61
Using static IP addresses for optional computers	62
Adding computers to the optional network	62
Making Static Routes	63
Viewing Network Statistics	65
Registering with the Dynamic DNS Service	66
Enabling the WAN Failover Option	68
Using the WAN Failover Setup Wizard	69
Using the Network page	70
If you are using a broadband connection for failover	71
If you are using an external modem for failover	72
DNS settings	73
Dialup settings	74
CHAPTER 5 Firebox X Edge Wireless Setup	75
How Wireless Networking Works	76
Connecting to the Firebox X Edge Wireless	76
Configuring the Wireless Card on Your Computer	76
Using the Wireless Network Wizard	77
Wireless Security Options	77
Setting up the Wireless Access Point	79
Configuring basic settings	79
Security Settings	81
Configuring encryption	82
Configuring wireless clients to use MUVPN	83
Configuring advanced settings	84
CHAPTER 6 Configuring Firewall Settings	87
About Services	87
Incoming and outgoing traffic	88
Traffic through VPN tunnels	88
About This Chapter	88

Configuring Incoming Services	89
<i>Configuring common services for incoming traffic</i>	90
<i>About custom services for incoming traffic</i>	91
<i>Adding a custom service using the wizard</i>	91
<i>Adding a custom incoming service manually</i>	92
<i>Filtering traffic for incoming services</i>	94
Configuring Outgoing Services	95
<i>Configuring common services for outgoing traffic</i>	96
<i>About custom services for outgoing traffic</i>	97
<i>Adding a custom service using the wizard</i>	97
<i>Adding a custom outgoing service manually</i>	98
<i>Filtering a service for outgoing traffic</i>	100
Services for the Optional Network	101
<i>Controlling traffic from the trusted to optional network</i>	102
<i>Disabling traffic filters</i>	103
Blocking External Sites	104
Configuring Firewall Options	105
<i>Responding to ping requests</i>	105
<i>Denying FTP access to the trusted network interface</i>	106
<i>SOCKS implementation for the Firebox X Edge</i>	106
<i>Logging all allowed outgoing traffic</i>	108
<i>Changing the MAC address of the external interface</i>	108
CHAPTER 7 Configuring Logging and System Time	111
Viewing Log Messages	111
Log to a WatchGuard Log Server	112
Logging to a Syslog Host	113
Setting the System Time	115
CHAPTER 8 Configuring WebBlocker	117
How WebBlocker Works	117
Configuring Global WebBlocker Settings	118
Creating WebBlocker Profiles	121
WebBlocker Categories	122
Allowing Certain Sites to Bypass WebBlocker	125
Blocking Additional Web Sites	126
Allowing Internal Hosts to Bypass WebBlocker	127
CHAPTER 9 Configuring Virtual Private Networks	129
About This Chapter	129
What You Need to Create a VPN	130

Managed VPN: With a Firebox III or Firebox X and WatchGuard System Manager 8.0	131
<i>Setting up a Firebox X Edge for managed VPN</i>	132
Managed VPN: With a Firebox III or Firebox X and WatchGuard System Manager 7.3	135
<i>Getting information about the DVCP Server</i>	136
<i>Setting up the Edge for Basic DVCP</i>	137
<i>Setting up the Edge for VPN Manager</i>	137
Manual VPN: Setting Up Manual VPN Tunnels	140
<i>What you need for Manual VPN</i>	140
<i>Phase 1 settings</i>	143
<i>Phase 2 settings</i>	147
VPN Keep Alive	148
Viewing VPN Statistics	149
Frequently Asked Questions	149
CHAPTER 10 Configuring the MUVPN Client	153
About This Chapter	154
Enabling MUVPN for Edge Users	155
<i>Configuring MUVPN client settings</i>	155
<i>Enabling MUVPN access for a Firebox user account</i>	156
<i>Configuring the Firebox for MUVPN clients using a Pocket PC</i>	158
Distributing the Software and the .wgx File	158
Preparing Remote Computers for MUVPN	159
<i>WINS and DNS servers</i>	160
<i>Windows NT setup</i>	160
<i>Windows 2000 setup</i>	162
<i>Windows XP setup</i>	164
Installing and Configuring the MUVPN Client	167
<i>Installing the MUVPN client</i>	167
<i>Uninstalling the MUVPN client</i>	168
Connecting and Disconnecting the MUVPN Client	169
<i>Connecting the MUVPN client</i>	169
<i>The MUVPN client icon</i>	169
<i>Allowing the MUVPN client through a personal firewall</i>	171
<i>Disconnecting the MUVPN client</i>	171
Monitoring the MUVPN Client Connection	172
<i>Using Log Viewer</i>	172
<i>Using Connection Monitor</i>	172
The ZoneAlarm Personal Firewall	173

<i>Allowing traffic through ZoneAlarm</i>	174
<i>Shutting down ZoneAlarm</i>	175
<i>Uninstalling ZoneAlarm</i>	175
Using MUVPN on the Edge Wireless Network	176
Tips for Configuring the Pocket PC	177
Troubleshooting Tips	179
CHAPTER 11 Managing the Firebox and User Accounts	183
Seeing Current Sessions and Users	183
<i>Firebox Users Settings</i>	184
<i>Active Sessions</i>	184
<i>Local User Accounts</i>	185
About User Authentication	187
<i>Authenticating to the Edge</i>	187
<i>Changing authentication options for all users</i>	188
<i>Configuring MUVPN client settings</i>	190
Adding or Editing a User Account	190
<i>Creating a read-only administrative account</i>	193
<i>Setting a WebBlocker profile for a user</i>	193
<i>Enabling MUVPN for a user</i>	193
<i>The Administrator account</i>	193
<i>Stopping a session</i>	194
<i>Changing a user account name or password</i>	195
About Seat Licenses	196
Selecting HTTP or HTTPS for Management	197
Changing the HTTP Server Port	198
Setting up WatchGuard System Manager Access	198
Updating the Firmware	199
<i>Method 1</i>	200
<i>Method 2</i>	200
Activating Upgrade Options	201
Enabling the Model Upgrade Option	203
Configuring Additional Options	204
Viewing the Configuration File	204
APPENDIX A Firebox X Edge Hardware	207
Package Contents and Specifications	207
Hardware Description	209
<i>Front panel</i>	209
<i>Rear view</i>	211

<i>Side panels</i>	211
About IEEE 802.11g/b Wireless	212
<i>Noise level</i>	212
<i>Signal strength (Watts)</i>	213
<i>Channel bandwidth</i>	214
APPENDIX B Legal Notifications	217
Copyright, Trademark, and Patent Information	217
Certifications and Notices	220
Declaration of Conformity	223
Limited Hardware Warranty	224

Introduction to Network Security

Thank you for your purchase of the WatchGuard® Firebox® X Edge. This security device helps protect your computer network from threat and attack.

This chapter gives you basic information about networks and network security. This information can help you when you configure the Edge. If you are experienced with computer networks, we recommend that you go to the subsequent chapter.

Network Security

While the Internet gives you access to an enormous quantity of information and business opportunity, it also opens your network to attackers. A good network security policy helps you find and prevent attacks to your computer or network.

Many people think that their computer holds no important information. They do not think that their computer is a target for a hacker. This is not correct. Your computer is valuable to a hacker, because an attacker can use it as a platform to attack other computers or networks or use your account information to send e-mail spam or attacks. Your identity information is also vulnerable and valuable to hackers.

About Networks

A *network* is a group of computers and other devices that are connected to each other. It can be two computers that you connect by a serial cable or many computers connected by data communication links located around the world.

A *Local Area Network* (LAN) is a group of computers connected to make a common work environment. This makes it easy to share applications and data, and is important when a group of people must do work together on one project.

A *Wide Area Network* (WAN) is a group of computers that can be far apart in different locations.

Clients and servers

The computer industry uses the words client and server for computers that are components of a network. A *server* is a computer that makes its resources available to the network and obeys the commands of a client. Examples of server shared resources are files (a file server), printers (a print server), and processing power (an application server). A *client* is a computer that uses the resources made available by the server.

Connecting to the Internet

You have some options when you connect to the Internet. High-speed Internet connections, including cable modem and Digital Subscriber Line (DSL), are *broadband connections*. *Bandwidth* is the relative speed of an Internet connection, for example 1 Megabit per second (Mbps).

You can use a cable modem to connect to the Internet through the cable TV network. The cable modem usually has an Ethernet LAN connection to the computer, and its speed can be more than 5 Mbps.

Typical speeds are usually lower than the maximum because cable providers turn full neighborhoods into LANs that use the same bandwidth. Because of this “shared-medium” topology, cable modem users could have slower network access during times of peak demand and can be more vulnerable to some attacks than users with other types of connectivity.

Digital Subscriber Line (DSL) Internet connectivity, unlike cable modem-based service, gives the user dedicated bandwidth. However, the maximum bandwidth available to DSL users is usually lower than the maximum cable modem rate because of differences in their respective network technologies. Also, the “dedicated bandwidth” is dedicated only between your home or office and the DSL provider’s central office. The provider gives no guarantee of bandwidth across the Internet.

Internet Service Providers (ISP) are companies that give access to the Internet.

Protocols

In computer network discussions, you frequently hear the term protocol. A *protocol* is a specification that makes computers able to connect across a network. Protocols define the “grammar” that computers use to speak to each other.

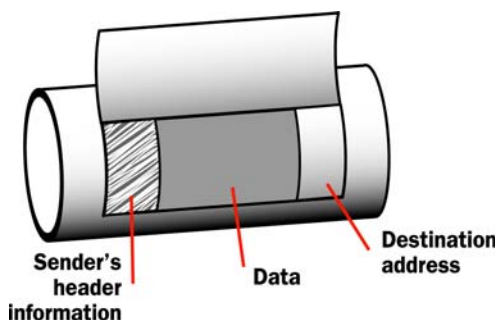
The standard protocol when you connect to the Internet is the Internet Protocol (IP). This protocol is the usual language of computers on the Internet.

A protocol also tells how data is sent through a network. The most frequently used protocols are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). Other IP protocols are less frequently used.

TCP/IP is the basic protocol used by computers that connect to the Internet. You must know some settings of TCP/IP when you set up your Firefox® X Edge. For more information on TCP/IP, see “Finding your TCP/IP properties” on page 15.

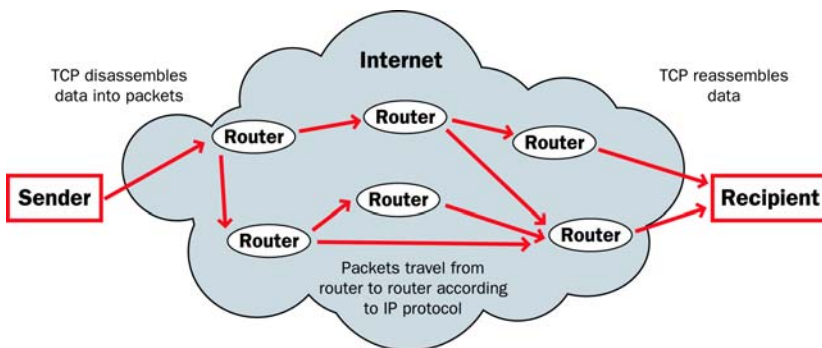
How Information Travels on the Internet

The data that you send through the Internet is cut into units, or packets. Each packet includes the Internet address of the destination. The packets that make up a file can use different routes through the Internet. When they all get to their destination, they are assembled back into the original file. To make sure that the packets get to the destination, address information is added to the packets.



Data packet

The TCP and IP protocols are used to send and receive these packets. TCP takes the data apart and assembles it again. IP adds information to the packets that includes the destination and the handling requirements.



Packets traveling on the Internet

IP Addresses

To send mail to a person, you must first know the person's street address. When a computer connects to the Internet to send data to a different computer, it must first know the address of that computer. A computer address is known as an *IP address*.

Each computer on the Internet has a unique IP address. An IP address has four sets of numbers which are divided by decimal points. Examples of IP addresses are:

- 192.168.0.11
- 10.1.20.18
- 208.15.15.15

A firewall device such as the Firebox® X Edge is also a computer and thus has an IP address.

Network addressing

Your ISP assigns IP addresses, which are a requirement to connect to the Internet. IP addresses can be dynamic or static.

Static IP addresses occur when an ISP permanently assigns one or more IP addresses for a user. This addresses does not change with time. Because ISPs have a limited number of addresses allocated to them, they must make efficient use of their addresses.

Dynamic IP addresses allow the ISP to use their address space more efficiently. Using dynamic IP addresses, the IP addresses of individual user computers can change with time. If a dynamic address is not in use (the user is not connected to the network), it can be automatically assigned to a different computer.

Your ISP can tell you how their system assigns IP addresses.

About DHCP

Many ISPs assign dynamic IP addresses through (Dynamic Host Configuration Protocol (DHCP). When a computer connects to the network, a DHCP server at the ISP assigns that computer an IP address. It is not necessary to assign IP addresses manually when you use DHCP.

About PPPoE

Some ISPs assign their IP addresses through Point-to-Point Protocol over Ethernet (PPPoE). PPPoE expands a standard dial-up connection to add some of the features of Ethernet and PPP. This system allows the ISP to use the billing, authentication, and security systems of their dial-up infrastructure with DSL modem and cable modem products.

Domain Name Service (DNS)

If you do not know the address of a person, you can frequently find it in the telephone directory. On the Internet, the equivalent to a telephone directory is the Domain Name Service (DNS). You use DNS all the time, but you may not know it. When you use a “.com” address such as www.mysite.com, www.mysite.com is the domain name of the Web site. A special computer on your corporate network or at your ISP does DNS resolution to find the IP address which goes with the domain name. When you type the .com address into your Internet browser, your computer gets the real IP address from the DNS server.

A URL (Uniform Resource Locator) identifies each IP address on the Internet. An example of a URL is:

<http://www.watchguard.com/>

Services

A *service* opens access from your network to a computer that is external to your network. You use services to send e-mail or move files from one computer to a different computer through the network. These services use protocols. Frequently used Internet services are:

- World Wide Web access uses Hypertext Transfer Protocol (HTTP)
- E-mail uses Simple Mail Transfer Protocol (SMTP)
- File transfer uses File Transfer Protocol (FTP)
- Changing a domain name to an Internet address uses Domain Name Service (DNS)
- Remote terminal access uses Telnet or Secure Shell

Some services are necessary, but each service you add to your security policy can also add a security risk. To send and receive data, you must “open a door” in your computer, which puts your network at risk. Attackers can use open access of a service to try to get into a network. We recommend that you only add services that are necessary for your business.

Ports

Usually, a port is a connection point where you use a socket and a plug to connect two devices. Computers also have ports that are not physical locations. These ports are “logical connection places” for programs or applications on a computer in a network. Some applications, such as HTTP, have ports with assigned numbers. These are “well-known ports.” Other application processes are assigned port numbers dynamically for each connection.

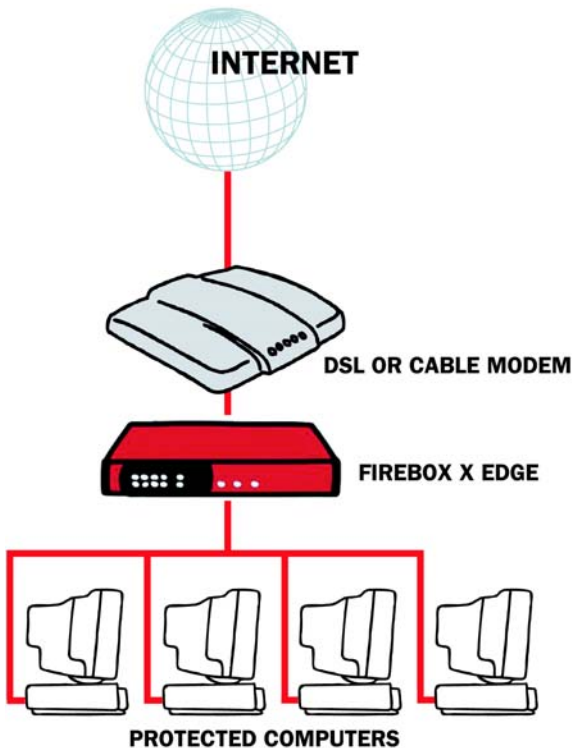
Each Internet service that uses TCP uses a unique port number.

When a client starts a connection to a server, it connects to, for example, port 25 on the remote computer. Port 25 is given to the SMTP protocol, which is the service that supplies electronic mail.

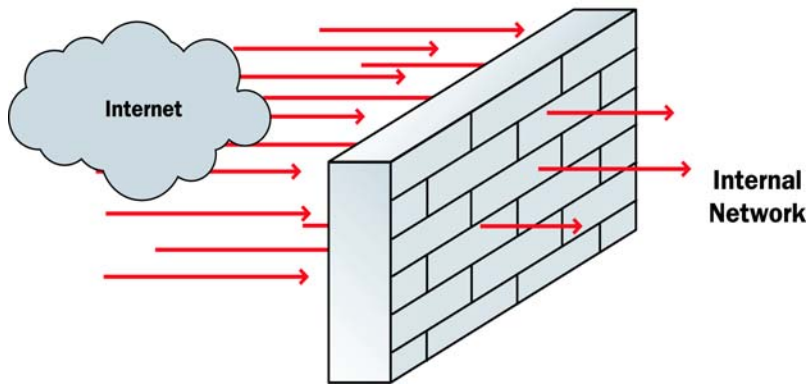
Most services are given a port number in the range from 0 to 1024, but possible port numbers range from 0 to 65535.

Firewalls

A firewall divides your internal network from the Internet to decrease risk from an external attack. We refer to the computers and networks on the Internet as the external network. The computers on the internal side of the firewall are protected. We refer to these as trusted computers. The figure below shows how a firewall divides the trusted network from the Internet.



Firewalls let users create access policies for the Internet traffic that goes to the computers they protect. They can also control which services or ports the protected computers can use on the Internet (out-bound access). Many firewalls have sample security policies and users can select the policy that is best for them. With others –such as the Firebox® X Edge– the user can customize these policies.



Firewalls can be in the form of hardware or software. They can prevent unauthorized Internet users from accessing private networks connected to the Internet. All messages that enter or go out of the trusted or protected networks go through the firewall, which examines each message and denies those that do not match the security criteria.

Firebox® X Edge and Your Network

The Firebox® X Edge controls all traffic between the external network and the trusted network. The Edge also includes an optional network. Use the optional network for computers with “mixed trust.” For example, customers frequently use the optional network for their remote users or for public servers such as a Web server or e-mail server. Your firewall can stop all suspicious traffic from the external network to your trusted and optional networks. The rules and policies that identify the suspicious traffic appear in Chapter 6, “Configuring Firewall Settings.”

The Firebox X Edge is a firewall for small and remote offices. Customers who purchase an Edge frequently do not know much about computer networks or network security. There are wizards and many self-help tools for these customers. Advanced customers can use integration features to connect an Edge to a larger wide area net-

work. The Edge connects to a cable modem, DSL modem, or ISDN router.

The Web-based user interface of the Firebox X Edge lets you manage your network safely. You can manage your Edge from different locations and at different times. It gives you more time and resources to use on other components of your business.

Installing the Firebox X Edge

To install the WatchGuard® Firebox® X Edge in your network, you must complete these steps:

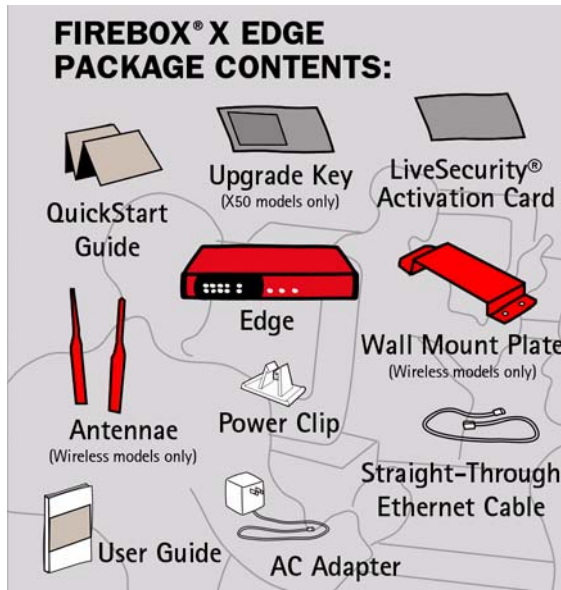
- Identify and record the TCP/IP properties for your Internet connection.
- Disable the HTTP proxy properties of your Web browser.
- Connect the Firebox X Edge to your network.
- Connect your computer to the Edge.
- Use the Quick Setup Wizard to configure the Edge.
- Activate the LiveSecurity® Service.

Package Contents

Make sure that the package for your Firebox® X Edge includes these items:

- The Firebox X Edge *QuickStart Guide*
- A LiveSecurity® Service activation card
- A Hardware Warranty Card
- An AC power adapter (12 V)

- A power cable clip
Use this clip to attach the cable to the side of the Edge. It decreases the tension on the power cable.
- One straight-through Ethernet cable
- A wall mount plate (Wireless models only)
- Two antennae (Wireless models only)



Installation Requirements

The Firebox® X Edge installation requirements are:

- A computer with a 10/100BaseT Ethernet network interface card to configure the Firebox.
- A Web browser. You can use Netscape 7.0 (or later), Internet Explorer 6.0 (or later), or an equivalent browser.
- The serial number of the Firebox X Edge.
You can find the serial number on the bottom of the Firebox. You use the serial number to register the Edge.

- An Internet connection.
The external network connection can be a cable or DSL modem with a 10/100BaseT port, an ISDN router, or a direct LAN connection. If you have problems with your Internet connection, call your Internet Service Provider (ISP) to solve the problem before you install the Firebox X Edge.

Identifying Your Network Settings

You use an Internet Service Provider (ISP) to connect to the Internet. An ISP assigns your computer or firewall an Internet Protocol (IP) address. The IP address can be static or dynamic, and this address lets you connect to Web sites on the Internet.

About network addressing

You must ask your ISP or corporate network administrator how your computer gets its external IP address. Use the same method to connect to the Internet with the Edge that you use with your computer. If you connect your computer directly to the Internet with a broadband connection and you put the Firebox® X Edge between your computer and the Internet, you can use the network configuration from your computer to configure the Edge external interface. You can use a static IP address, DHCP, or PPPoE to configure the external interface.

You must also configure your computer to connect with a Web browser to configure and manage the Edge. Your computer must have an IP address in a range that is the same as the Edge. In the factory default configuration, the Edge assigns your computer an IP address with DHCP. You can set your computer to use DHCP and you can then connect to the Edge to manage it. You can also give your computer a static IP address that is in the range of the trusted network on the Edge. For information on setting your computer to connect to the Edge, see “Setting Your Computer to Connect to the Edge” on page 22.

Static addresses, DHCP, and PPPoE

Your ISP gives you an IP address using one of these methods:

- Static: A *static IP address* is an IP address that always stays the same. If you have a Web server, FTP server, or other Internet resource that must have an address that cannot change, you can get a static IP address from your ISP. A static IP address can cost more money than a dynamic IP address.

- **DHCP:** A *dynamic IP address* is an IP address that an ISP lets you use (lease). With DHCP, your computer does not always use the same IP address. When you close an Internet connection that uses a dynamic IP address, the dynamic address is made available again. Then the ISP can assign that IP address to a different customer. ISPs use Dynamic Host Configuration Protocol (DHCP) to assign you a dynamic IP address. Each time you connect to the ISP, a DHCP server assigns you an IP address. It could be the same IP address you had before, or it could be a new IP address.
- **PPPoE:** ISPs can also use Point-to-Point Protocol over Ethernet (PPPoE) to assign you an IP address. A user name and password are necessary for PPPoE. Usually, a PPPoE address is dynamic.

The ISP also assigns a subnet mask (also known as the netmask) to a computer. A *subnet mask* divides a larger network into smaller networks. A subnet mask is a string of bits that “mask” one section of an IP address to show how many IP addresses can be on the smaller network.

Read your DSL or cable modem instructions or speak to your ISP to learn if you have a dynamic IP address or a static IP address.

Finding your TCP/IP properties

Transmission Control Protocol/Internet Protocol (TCP/IP) is the primary protocol computers use to connect to the Internet. To use TCP/IP, your computer must have an IP address and information about the computer network of your ISP. You must have this information to install your Firebox X Edge.

NOTE

If your ISP assigns your computer an IP address that starts with 10 or 192.168 or 172.16 to 172.31, then your ISP uses Network Address Translation (NAT). We recommend that you get a public IP address for your Edge external IP address. If you use a private IP address, you can have problems with some features, including VPN.

Your TCP/IP Properties Table

TCP/IP Property		Value
IP Address		. . .
Subnet Mask		. . .
Default Gateway		. . .
DHCP Enabled		Yes No
DNS Server(s)	Primary	. . .
	Secondary	. . .

To find your TCP/IP properties, use the instructions for your computer operating system.

Microsoft Windows 2000, Windows 2003 and Windows XP

- 1 Click **Start > Programs > Accessories > Command Prompt.**
- 2 At the MS-DOS prompt, type `ipconfig /all` and then press **Enter.**
- 3 Record the values in Your TCP/IP Properties Table on page 15.
- 4 Close the window.

Microsoft Windows NT

- 1 Click **Start > Programs > Command Prompt.**
- 2 At the MS-DOS prompt, type `ipconfig /all` and then press **Enter.**
- 3 Record the values in Your TCP/IP Properties Table on page 15.
- 4 Close the window.

Microsoft Windows 98 or ME

- 1 Click **Start > Run.**
- 2 At the MS-DOS prompt, type `winipcfg` and then press **Enter.**
- 3 Click **OK.**
- 4 Select the **Ethernet Adapter.**
- 5 Record the values in Your TCP/IP Properties Table on page 15.
- 6 Click **Cancel.**

Macintosh OS 9

- 1 Click the **Apple menu > Control Panels > TCP/IP.**
- 2 Record the values in Your TCP/IP Properties Table on page 15.
- 3 Close the window.

Macintosh OS 10

- 1 Click the **Apple** menu > **System Preferences** > **Network** > **TCP/IP**.
- 2 Record the values in Your TCP/IP Properties Table on page 15.
- 3 Close the window.

Other operating systems (Unix, Linux)

- 1 Read your operating system guide to find the TCP/IP settings.
- 2 Record the values in Your TCP/IP Properties Table on page 15.
- 3 Exit the TCP/IP configuration screen.

Finding PPPoE settings

Many ISPs use Point to Point Protocol over Ethernet (PPPoE) because it is easy to integrate with a dial-up infrastructure. If your ISP uses PPPoE to assign IP addresses, you must get more information.

PPPoE Address Settings

PPPoE Setting	Value
Login Name	
Domain	
Password	

Disabling the HTTP Proxy Setting

Many Web browsers are configured to use an HTTP proxy server. A proxy server is a computer that your browser connects to help speed up the download of Web pages. To manage the Firebox® X Edge, your computer must connect to the Edge configuration pages directly without a proxy. To do this, you must temporarily disable the HTTP proxy setting in your browser.

You can use these instructions to disable the HTTP proxy in Netscape or Internet Explorer. If you are using a different browser, use the browser Help system to find the necessary information. Many browsers automatically disable the HTTP proxy feature.

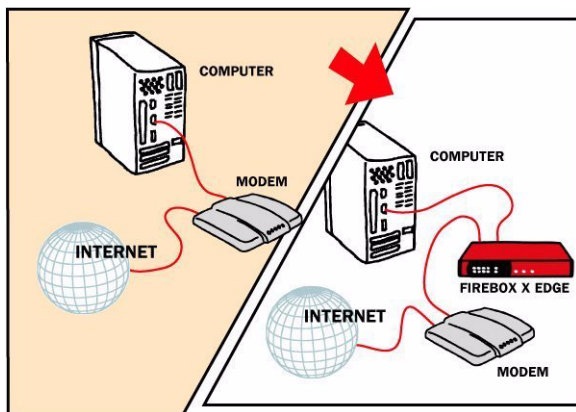
Disable the HTTP proxy in Netscape or Mozilla

- 1 Open the browser software.
- 2 Click **Edit > Preferences**.
The Preferences window appears.
- 3 A list of options appears. Click the arrow symbol adjacent to **Advanced** to expand the list.
- 4 Click **Proxies**.
- 5 Make sure the **Direct Connection to the Internet** option is selected.
- 6 Click **OK**.

Disable the HTTP proxy in Internet Explorer

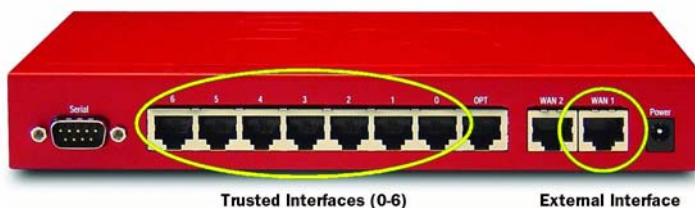
- 1 Open Internet Explorer.
- 2 Click **Tools > Internet Options**.
The Internet Options window appears.
- 3 Click the **Advanced** tab.
- 4 Scroll down the page to **HTTP 1.1 Settings**.
- 5 Clear all of the check boxes.
- 6 Click **OK**.

Connecting the Firebox X Edge



Use this procedure to connect your Firebox® X Edge Ethernet and power cables:

- 1 Shut down your computer.
- 2 If you use a DSL or cable modem to connect to the Internet, disconnect its power supply.
- 3 Find the Ethernet cable between the modem and your computer. Disconnect this cable from your computer and connect it to the Edge external interface (WAN 1).



- 4 Find the Ethernet cable supplied with your Edge. Connect this cable to a trusted interface (0-6) on the Edge. Connect the other end of this cable to the Ethernet interface of your computer.
- 5 If you use a DSL or cable modem, connect its power supply.

- 6 Find the AC adapter supplied with your Edge. Connect the AC adapter to the Edge and to a power source.
The Edge power indicator light comes on and the WAN indicator lights flash and then come on.

NOTE

Only use the AC adapter for the Firebox X Edge.

Connecting the Edge to more than seven devices

Although the Firebox® X Edge has only seven numbered Ethernet ports (labeled 0-6), you can connect more than seven devices. Use one or more network hubs to make more connections.

The maximum number of devices that can connect to the Internet at the same time is set by model. For example, if a Firebox X Edge model has a 12-session license, there can be more than 12 devices on the trusted network. But, the Edge allows only 12 Internet connections at the same time.

The Edge uses a session when a trusted or optional computer makes a connection to the external interface. That same computer can then have more than one connection through the Firebox without adding another session. Sessions are based on the number of computers with active connections through the Firebox external interface. The Edge releases the session when any of these things happen:

- If Firebox user authentication is necessary for external network connections, the Edge releases the session after the idle time-out limit set for that account.
- If Firebox user authentication is necessary for external network connections, the Edge releases the session after the maximum time-out limit set for that account.
- If Firebox user authentication is necessary for external network connections, the Edge releases the session when the Firebox user manually stops the session. To stop the session, the user closes the **Login Status** box and all other browser windows.
- If the Edge administrator uses the Firebox Users page to stop a session, the Edge releases that session.
- If the Automatic Session Termination time limit for all sessions is reached, the Edge releases all sessions at one time.
- If the Edge restarts, all sessions are released.

For more information, see the FAQ:

www.watchguard.com/support/AdvancedFaqs/edge_seatlicense.asp

License upgrades are available from your reseller or from the WatchGuard Web site:

<http://www.watchguard.com/sales/buyonline.asp>

To connect more than seven devices to the Edge, you must have:

- An Ethernet 10/100Base TX hub or switch
- A straight-through Ethernet cable, with RJ-45 connectors, for each computer
- A straight-through Ethernet cable to connect each hub to the Firebox X Edge.

To connect more than seven devices to the Firebox X Edge:

- 1 Shut down your computer.
- 2 If you use a DSL or cable modem to connect to the Internet, disconnect its power supply.
- 3 Disconnect the Ethernet cable that runs from your DSL modem, cable modem, or other Internet connection to your computer. Connect the Ethernet cable to the WAN port on the Firebox X Edge.
The Firebox X Edge is connected directly to the modem or other Internet connection.
- 4 Connect one end of the straight-through Ethernet cable supplied with your Firebox X Edge to one of the seven Ethernet ports on the Edge. Connect the other end to the uplink port of the Ethernet hub or switch.
The Firebox X Edge is connected to the Internet and your Ethernet hub or switch.
- 5 Connect an Ethernet cable between each computer and one of the uplink ports on the Ethernet hub, and make sure the link lights are lit on the devices when they are turned on.
- 6 If you connect to the Internet through a DSL modem or cable modem, connect the power supply to this device. The indicator lights flash and then stop.
- 7 Attach the AC adapter to the Firebox X Edge. Connect the AC adapter to a power supply.

Setting Your Computer to Connect to the Edge

Before you can use the Quick Setup Wizard, configure your computer network interface card to connect to the Firebox® X Edge and see the configuration pages. You can give your computer a static IP address, or get an IP address from the Edge using DHCP.

If your computer gets its address from DHCP

This procedure configures a computer with the Windows XP operating system to use DHCP. If your computer does not use Windows XP, read the operating system help for instructions on how to set your computer to use DHCP.

- 1 Click **Start > Control Panel**.
The Control Panel window appears.
- 2 Double-click the **Network Connections** icon.
- 3 Double-click the **Local Area Connection** icon.
- 4 Double-click the **Internet Protocol (TCP/IP)** list item.
The Internet Protocol (TCP/IP) Properties dialog box appears.
- 5 Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** options.
- 6 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** dialog box.
- 7 Click **OK** to close the **Local Area Network Connection Properties** dialog box. Close the **Network Connections** and **Control Panel** windows.
Your computer is ready to connect to the Firebox X Edge.
- 8 When the Edge is ready, start your computer and start your Internet browser.
- 9 Type `https://192.168.111.1/` into the URL entry field of your browser and press **Enter**.
The Quick Setup Wizard starts.
- 10 Run the Quick Setup Wizard, as shown in “Running the Quick Setup Wizard” on page 24.

If your computer has a static IP address

This procedure configures a computer with the Windows XP operating system to use a static IP address. If your computer does not use Windows XP, read the operating system help for instructions on how to set your computer to use a static IP address. You must use an IP address on the same network as the Firebox X Edge trusted interface.

- 1 Click **Start > Control Panel**.
The Control Panel window appears.
- 2 Double-click the **Network Connections** icon.
- 3 Double-click the **Local Area Connection** icon.
- 4 Double-click the **Internet Protocol (TCP/IP)** list item.
The Internet Protocol (TCP/IP) Properties dialog box appears.
- 5 Select the **Use the following IP address** option.
- 6 In the **IP address** field, type an IP address on the same network as the Edge trusted interface. We recommend 192.168.111.2.
The default trusted interface network is 192.168.111.0/24. The last number can be between 2 and 254.
- 7 In the **Subnet Mask** field, type 255 . 255 . 255 . 0.
- 8 In the **Default Gateway** field, type the IP address of the Edge trusted interface.
The default Edge trusted interface address is 192.168.111.1.
- 9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** dialog box.
- 10 Click **OK** to close the **Local Area Network Connection Properties** dialog box. Close the **Network Connections** and **Control Panel** windows.
Your computer is ready to connect to the Firebox X Edge.
- 11 When the Edge is ready, start your computer and start your Internet browser.
- 12 Type <https://192.168.111.1/> into the URL entry field of your browser and press **Enter**.
The Quick Setup Wizard starts.
- 13 Use the Quick Setup Wizard, as shown in the subsequent section.

Running the Quick Setup Wizard

After you start your computer and type **https://192.168.111.1** into the URL entry field of your Internet browser, the Quick Setup Wizard starts. You must use the wizard to configure the Ethernet interfaces. You can change the configuration of the interfaces after you use the wizard.

The Quick Setup Wizard includes this set of dialog boxes. You will not see all of these dialog boxes because some only appear based on the configuration method you select:

Welcome

The first screen tells you about the wizard.

Configure the External Interface of your Firebox

This screen sets the method your ISP uses to assign your IP address.

Configure the External Interface for DHCP

On this screen, type in your DHCP identification as supplied by your ISP.

Configure the External Interface for PPPoE

On this screen, type in your PPPoE information as supplied by your ISP.

Configure the External Interface with a static IP address

On this screen, type in your static IP address information as supplied by your ISP.

Configure the Trusted Interface of the Firebox

On this screen, type the IP address of the trusted interface.

Set the User Name and Passphrase

Use this screen to set the user name and passphrase for the administrator account for the Edge.

Set the Wireless Region

(For wireless models only.) Type the country or region in which the Firebox X Edge Wireless is being used. This cannot be changed after it is set.

Set the Time Zone

Use this screen to set the time zone the Firebox X Edge is operating in.

The Quick Setup Wizard is complete

The Quick Setup Wizard supplies a link to the WatchGuard web site to register your product. After you complete the wizard, the Firebox X Edge restarts. The system Status page appears on the screen. You can configure more features of your Edge at this time.


WatchGuard **Firebox X Edge** [LiveSecurity](#) | [Help](#) | [Support](#) | [About Us](#) | [Contact Us](#)

System Status

Welcome to the Firebox X Edge configuration site. The standard configuration provides basic protection against network security attacks. Through this site you can customize the Firebox X Edge to meet your specific security needs.

If you need assistance, review the [Help pages](#) for information about this release or review the [Online Documentation](#).

Component	Version	Feature	Status	
Firewall	7.1.0 Oct 11 2004 build 8	WSEP Logging	Enabled	Configure
		VPN Manager Access	Enabled	Configure
Boot ROM	7.1	Syslog	Disabled	Configure
Model	X15			
Serial Number	0067000171c1e			



[Reboot](#) [Update](#)

Option	Status	
User Licenses	15	Upgrade
Managed VPN	Disabled	Configure
Manual VPN	1 configured (max 15)	Configure
MUVPN Clients	0 in use (max 15)	Configure
WebBlocker	Enabled	Configure
WAN Failover	Enabled	Configure

Trusted Network		Firewall		External Network	
IP Address	192.168.111.1	Outgoing	Service	Incoming	Mode
Subnet Mask	255.255.255.0		HTTPS		Manual
DHCP Server	Disabled		Outgoing		IP Address
First IP	192.168.111.2		myservice		192.168.54.54
MAC	00907F-160F42		FTP		Subnet Mask
					255.255.255.0
					Gateway
					192.168.54.254
					MAC
					00907F-160F44

Registering and Activating LiveSecurity Service

After you install the Firebox® X Edge, you can register the Edge and activate your LiveSecurity service subscription. The LiveSecurity service gives you threat alert notifications, security advice, virus protection information, software updates, technical support by Web or telephone, and access to online help resources and the WatchGuard user forum.

You must have a subscription to the LiveSecurity service before you can get license keys for upgrades that you purchase. To install an upgrade, you must log in to LiveSecurity service and type your upgrade key. You then get a feature key to activate the features on your Firebox X Edge.

You must have the serial number of your Firebox X Edge to register. The Edge serial number is on the bottom of the device. Record the serial number in the table below:

- 1 Register your Firebox X Edge with the LiveSecurity Service at the WatchGuard Web site:

<http://www.watchguard.com/activate>

NOTE

To activate the LiveSecurity Service, your browser must have JavaScript enabled.

- 2 If you are registered at the WatchGuard Web site, type your user name and password. If you are not registered, you must create a user profile. To do this, follow the instructions on the Web site.
- 3 Record your LiveSecurity Service user profile information in the table below. Keep this information confidential.

WatchGuard LiveSecurity User Profile

User name:	
Password:	
Serial Number:	

- 4 If a model upgrade key is included with your model, activate it by going to:
<http://www.watchguard.com/upgrade>
- 5 Select your product and use the instructions for product activation. At this time you can configure your Edge.

Configuration and Management Basics

When you configure a WatchGuard® Firebox® X Edge, you create firewall rules to apply the security rules of your company. Before you create these rules you must install your Firebox. To create a basic configuration, use your Web browser to connect to the Web pages on the Firebox X Edge.

You can also use the Edge configuration pages to create an account, look at network statistics, and see the current configuration of the Edge.

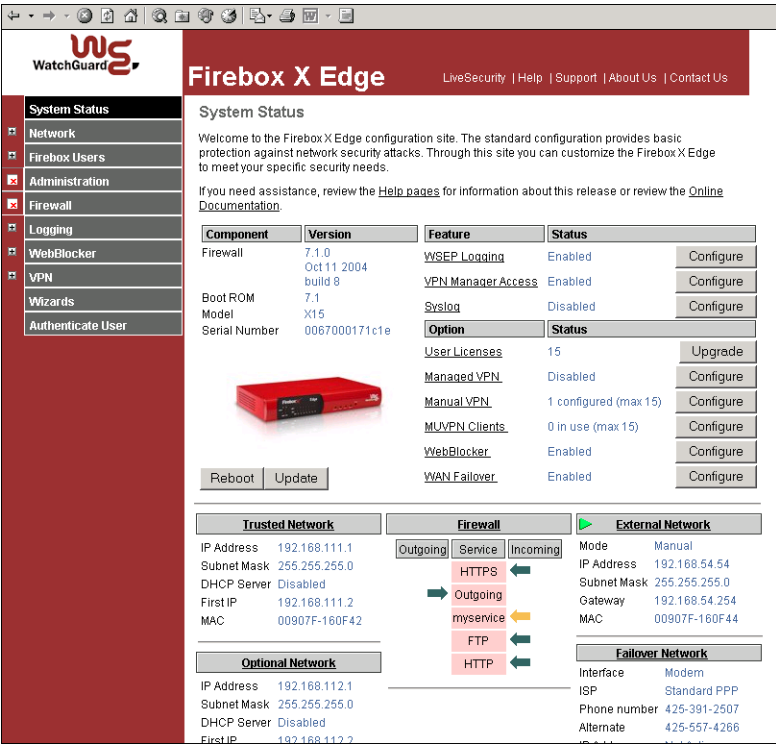
Read this chapter to find basic information about the Firebox X Edge configuration pages. There are sections in subsequent chapters that have more advanced procedures. This chapter contains links to subsequent sections.

NOTE

You can see the configuration pages only if you used the Quick Setup Wizard, as shown in the "Installing the Firebox X Edge" chapter. Also, to configure the Firebox X Edge, your network administrator must configure your user account to see and change the configuration pages. See Chapter 11, "Managing the Firebox X Edge and User Accounts," for more information on user accounts.

Navigating the Configuration Pages

You use the configuration pages for all procedures to configure the Firebox® X Edge. The System Status page, the primary navigation page, appears below.



In this User Guide, most procedures start with this step:

“To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface. The default URL is: **https://192.168.111.1**.”

The function of the step is to open your Firebox system configuration pages. You can change the IP address of the trusted network from **https://192.168.111.1** to a different IP address if necessary. For more information, see “Configuring the Trusted Network” on page 53.

For example, if you use Internet Explorer to configure your Firebox:

- 1 Start Internet Explorer.
- 2 Click **File > Open**, type **https://192.168.111.1** in the text box adjacent to the word **Open**, and then click **OK**.

You can also type the URL directly into the address bar and press the Enter key.

NOTE

If necessary, you can connect to the Web server on the Firebox X Edge in HTTP mode instead of HTTPS mode. HTTP mode is less secure, because any configuration changes you make are sent to the Firebox in unencrypted text.

Using the navigation bar

On the left side of the System Status page is the navigation bar you use to get to other Firebox X Edge configuration pages.



To see the primary page for each feature, click the menu item on the navigation bar. For example, to see how logging is configured for your Firebox and to see the current event log, click **Logging**.

Each menu item contains submenus that you use to configure the properties in that feature. To see these submenus, click the plus sign (+) to the left of the menu item. For example, if you click the plus sign adjacent to **WebBlocker**, these submenu items appear: **Settings**, **Profiles**, **Allowed Sites**, **Denied Sites**, and **Trusted Hosts**.

This user guide uses an arrow (>) symbol to show menu items that you expand or click. The menu names are in **bold**. For example, the command to open the Denied Sites page appears in the text as **WebBlocker > Denied Sites**.

Configuration Overview

You use the Firebox® X Edge system configuration pages to set up your Edge to protect your network. This section gives an introduction to each category of pages and tells you which chapters in this User Guide contain detailed information about each feature.

Firebox System Status Page

The System Status page, which appears on page 28, is the primary configuration page of the Firebox X Edge. The center panel of the page shows information about the current properties. It also contains the buttons you use to change these properties. You can see details about each property in later chapters.

Basic information on this page includes:

- Firebox components and their current versions
- The serial number of the device
- The status of key Firebox X Edge features
- The status of upgrade options
- Network configuration information
- Which external network (external or failover) is active. A green triangle appears adjacent to the active network.
- Firewall configuration information
- A button to restart the Firebox

Network Page

The Network page shows the configuration of each network interface. It also shows any configured routes and has buttons you can use to change configurations and to see network statistics. For more information, see Chapter 4, “Changing Your Network Settings.”

Network		
External Network [Active]		
Configuration Method	Manual Configuration	Configure
IP Address	192.168.54.54	
Subnet Mask	255.255.255.0	
Gateway	192.168.54.254	
Primary DNS Server	192.168.130.131	
Secondary DNS Server	192.168.130.245	
Domain	wgti.net	
MAC	00907F-160F44	
Trusted Network		
IP Address	192.168.111.1	Configure
Subnet Mask	255.255.255.0	
MAC	00907F-160F42	
DHCP Server	Disabled	
	5 addresses in use (251 max)	
	First address: 192.168.111.2	
Optional Network		
IP Address	192.168.112.1	Configure
Subnet Mask	255.255.255.0	
MAC	00907F-160F41	
DHCP Server	Disabled	
	0 addresses in use (251 max)	
	First address: 192.168.112.2	
Failover Network [Not Active]		
Interface	Modem	Configure

The Network page contains these links to other configuration pages:

- **External:** Use this page to configure the Edge external network interface.
- **Trusted:** Use this page to configure the Edge trusted network interface. Select the method the Edge uses to give IP addresses to computers on the trusted network.

- **Optional:** Use this page to configure the Edge optional network interface. Select the method the Edge uses to give IP addresses to computers on the optional network.
- **WAN Failover:** Configure a redundant network connection for the external interface.
- **Dynamic DNS:** Register the external IP address of the Edge with a dynamic Domain Name Server (DNS) service.
- **Routes:** Make a static route to a computer on the trusted or optional networks.
- **Network Statistics:** Shows information on network performance.
- **(For Wireless models only) Wireless (802.11g):** Set up and configure the wireless network.

Firebox Users Page

The Firebox Users page shows statistics on the active sessions and local user accounts. It also has buttons to close current sessions and to add, edit, and delete user accounts.

This page also shows the MUVPN client configuration files that you can download. For more information, see Chapter 11, “Managing the Firebox X Edge and User Accounts.”

Firebox Users

Firebox User Settings

Firebox User accounts are **enabled**

Configure

Restrict External Network access: **Enabled**
Restrict VPN tunnel access: **Enabled**
Enforce session idle time-out: **Disabled**
Enforce maximum access time: **Enabled**
Reset idle on Firebox X Edge access: **Disabled**
Time-out setting (hours): **1**
Elapsed time (hours:minutes): **0:00**
Time remaining (hours:minutes): **1:00**

Active Sessions

Active session total is 0. Count of sessions occupying user licenses is 0 (maximum is 15).
The following sessions are currently active on this Firebox.

User	Host	On-line Time	Idle Timeout	License	Close
<div>Close All</div>					

Local User Accounts

The following local user accounts have been defined for this Firebox.

Add...

Name	Internet Access	Admin Level	WebBlocker	MUVPN	VPN	Edit	Delete
admin	Allow	Full	No WebBlocker	Enabled	Allow		
cfgview	Allow	Read Only	No WebBlocker	Enabled	Allow		
muvpn	Allow	None	No WebBlocker	Enabled	Allow		
user	Allow	None	restricted	Enabled	Allow		

Secure MUVPN Client Configuration Files

External MUVPN access count: **0** (maximum 15)
The following secure (encrypted) MUVPN client configuration (.wgp) files are available for download. Once downloaded, these files can be used to configure your MUVPN client software in a manner that is consistent with the currently defined MUVPN settings on the X15.

Account Name	MUVPN Client Configuration Files
admin	admin.wgp
muvpn	muvpn.wgp
user	user.wgp
cfgview	cfgview.wgp

The Firebox Users page contains these links to other configuration pages:

- **Settings:** Use this page to set the properties that apply to all Edge users.
- **New User:** From here you can make one or more user profiles and set the network traffic types they can send and receive.

Administration Page

The Administration page shows if the Firebox uses HTTP or HTTPS for its configuration pages, if the Edge is configured as a managed Firebox client, and which upgrades are enabled. It has buttons to change configurations, add upgrades, and see the configuration file. For more information, see Chapter 11, “Managing the Firebox X Edge and User Accounts.”

The screenshot shows the 'Administration' page with the following sections:

- Administrative Options**
 - System Security:** HTTPS mode (with a 'Configure' button)
 - VPN Manager Access:** Disabled (with a 'Configure' button)
- Upgrades:** (with an 'Upgrade' button)
- Installed Options:**
 - User Licenses: 15
 - Remote Gateways: Installed
 - MUVPN Clients: Installed - license count 15
 - WebBlocker: Installed
 - WAN Failover: Installed
- View Configuration File:** (button)

The Administration page contains these pages:

- **System Security:** Use this page to select HTTP or HTTPS for configuration pages. You can also select the HTTP server port.
- **VPN Manager Access:** Let a remote network administrator configure your Firebox X Edge as a managed Firebox Client using WatchGuard System Manager software and WatchGuard Management Server (formerly known as a DVCP Server).
- **Update:** Update the Edge firmware.
- **Upgrade:** Activate your Edge upgrade options.

- View Configuration: Shows the Edge configuration file in a text format.

Firewall Page

The Firewall page shows the incoming and outgoing services, blocked sites, and other firewall settings. This page also has buttons to change these settings. For more information, see Chapter 6, “Configuring Firewall Settings.”

Firewall

Trusted Network Optional Network	Firewall	External Network
Outgoing	Service	Incoming
Disabled	HTTPS	Allowed
Allowed	Outgoing	
Disabled	myservice	Denied
Disabled	FTP	Allowed
Disabled	HTTP	Allowed

Configure

Configure

Trusted Network	Firewall	Optional Network
Outgoing	Service	
Allowed	Outgoing	

Configure

Blocked Sites

No blocked sites are defined.

Configure

Firewall Options

PING requests from External Network	Respond	Configure
PING requests from Trusted Network	Respond	
FTP access from Trusted Network	Allowed	
SOCKS proxy	Enabled	
Log All Allowed Outbound Access	Disabled	
Override MAC address on External	Disabled	
Override MAC address on Failover	Disabled	

The Firewall page contains these links to other configuration pages:

- Incoming: Make one or more security services for incoming traffic to the trusted or optional networks.

- **Outgoing:** Make one or more security services for outgoing traffic to the external network.
- **Optional:** Make one or more security services for outgoing traffic from the trusted network to the optional network.
- **Blocked Sites:** Prevent access to specified network addresses on the external interface.
- **Firewall Options:** Set the options that customize your security policy.

Logging Page

The Logging page shows the current event log, the status of the Log Server (also known as the WSEP) and Syslog logging, and the system time. It also has buttons to change these properties and to set your system time to the same value as your local computer. For more information, see Chapter 7, “Configuring Logging and System Time.”

Logging

Refresh

Logging Options

WSEP Logging

Enabled

WSEP Log Host

192.168.52.170

Configure

Syslog Logging

Disabled

Syslog Host

0.0.0.0

Configure

System Time

Configure

Time Source

WSEP Log Host

192.168.52.170

Time Zone

(GMT-08:00) Pacific Time (US & Canada); Tijuana

DST

Disabled

Current Time

2004-10-16-21:43:15

Sync Time With Browser Now

Event Log

Time	Category	Message
2004-10-16-21:43:15	MONITOR	Administrator access allowed from 10.168.3.90
2004-10-16-21:43:12	IP	allowed from 10.168.3.90 port 3243 to 192.168.54.54 port 443 TCP SYN (HTTPS)
2004-10-16-21:43:11	MONITOR	Remote logging connection open to 192.168.52.170

The Logging page contains these links to other configuration pages:

- WSEP Log: Configure the WatchGuard Log Server to accept the log messages from your Edge.
- Syslog Log: Configure the Edge to send log messages to a Syslog host.
- System Time: Set the time zone and if your Edge uses daylight saving time.

WebBlocker Page

The WebBlocker page shows the WebBlocker settings, profiles, allowed sites, denied sites, and trusted hosts. It also has buttons to change the current settings. For more information, see Chapter 8, “Configuring WebBlocker.”

WebBlocker

WebBlocker Settings

Status

Enabled

Configure

Inactivity Time-out (minutes)

5


Authentication for Web Access


Not Required

WebBlocker Profiles

Profiles and assigned users:

Configure

 [restricted](#)

 [user](#)

Allowed Sites

Allowed Sites

1.2.3.4

Configure

Denied Sites

No denied sites are defined.

Configure

Trusted Hosts

No trusted hosts are defined.

Configure

The WebBlocker page contains these links to other configuration pages:

- Settings: Configure the WebBlocker settings for all users.
- Profiles: Create one or more sets of restrictions to apply to Edge users.

- **Allowed Sites:** Make a list of Web sites that you can browse to when WebBlocker properties block the Web site.
- **Denied Sites:** Make a list of Web sites that you cannot browse to when WebBlocker settings allow the Web site.
- **Trusted Hosts:** Make a list of computers on the trusted or optional networks that can bypass WebBlocker.

VPN Page

The VPN page shows information on managed VPN tunnels, manual VPN gateways, echo hosts, and buttons to change the configuration of VPN tunnels. It also has a button for you to see statistics on active tunnels. For more information, see Chapter 9, “Configuring Virtual Private Networks.”

The screenshot shows the 'VPN' configuration page. It is divided into three main sections: 'Managed VPN Gateways', 'Manual VPN Gateways', and 'VPN Keep Alive'. Each section has a 'Configure' button. The 'Managed VPN Gateways' section shows 'Configuration Mode' as 'Disabled' and 'Status' as 'Tunnel is not configured'. The 'Manual VPN Gateways' section shows 'Remote Gateways' as '1 configured (max 15)' and a 'Regenerate IPSec Keys' button. The 'VPN Keep Alive' section shows 'Echo Hosts' as '192.168.53.154'. At the bottom, there is a 'View VPN Statistics' button.

VPN	
Managed VPN Gateways	
Configuration Mode	Disabled Configure
Status	Tunnel is not configured
Manual VPN Gateways	
Remote Gateways	1 configured (max 15) Configure
Regenerate IPSec Keys	
VPN Keep Alive	
Echo Hosts	192.168.53.154 Configure
View VPN Statistics	

The VPN page contains these links to other configuration pages:




- **Managed VPNs:** Add the Firebox X Edge to a WatchGuard System Manager VPN network.
- **Manual VPNs:** Make a VPN tunnel to an IPSec compliant device such as a second Firebox X Edge.
- **VPN Keep Alive:** Keep a VPN tunnel open when no regular network traffic goes through it.
- **VPN Statistics:** Show important data you can use to monitor your VPN traffic and to troubleshoot a problem with the VPN configuration.

Wizards Page

The Wizards page shows the wizards you can use to help you set up Firebox X Edge features:

- Service Configuration Wizard
Create a rule to filter network traffic between interfaces. For more information, see “About custom services for incoming traffic” on page 91.
- Network Interface Wizard
Configure the Edge interfaces. For more information, see “Using the Network Setup Wizard” on page 45.
- Wireless Network Wizard (Wireless models only)
Set up the wireless interface. For more information, see Chapter 5, “Setting up the Firebox X Edge Wireless.”
- WAN Failover Setup Wizard
Set up the failover network. For more information, see “Enabling the WAN Failover Option” on page 68.

Wizards

What do you want to do?	Go!
Define a custom service for filtering network traffic between the External network and the Trusted and Optional networks.	
Setup the primary network interfaces of the Firebox X Edge.	
Configure the automatic WAN failover capability of your Firebox Edge.	

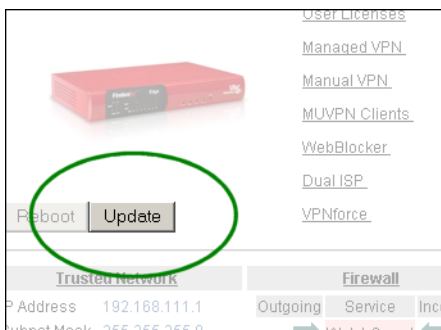
Updating Firebox X Edge Software

One advantage of your LiveSecurity® Service is ongoing software updates. As new threats appear and WatchGuard adds product enhancements, you receive alerts to let you know about new versions of your Firebox® X Edge software.

When you receive the alert, WatchGuard gives you instructions about how to download the software to your computer. After this

download completes, use the procedure below to update your Firebox software:

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 2 At the bottom of the System Status page, click **Update**.



- 3 Type the name of the file that contains the new Firebox X Edge software in the **Select text** box or click **Browse** to find the file on your local computer.
- 4 Click **Update**.

The Firebox makes sure the software package is a legitimate software upgrade. It then copies the new software to the system. This can take 15 to 45 seconds. When the update is complete, click the Reboot button that appears on the Update page. After the Firebox restarts, the System Status page appears and shows the new version number.

Factory Default Settings

The term “factory default settings” refers to the configuration on the Firebox® X Edge when you first receive it—before you make changes to the configuration file. The default network and configuration properties for the Firebox X Edge are as follows:

Trusted network

- The default IP address for the trusted network is 192.168.111.1. The subnet mask for the trusted network is 255.255.255.0.
- The Firebox X Edge is configured to give IP addresses to computers on the trusted network through DHCP. You can also

give static addresses to computers in the trusted network with IP addresses in the 192.168.111.2–192.168.111.254 range.

External network

- The external network properties use DHCP.

Optional network

- The optional network is disabled.

Firewall settings

- All incoming services are denied.
- An outgoing service allows all outgoing traffic.
- Ping requests received on the external network are denied.

System Security

- The Edge administrator account is set to the default user name of “admin” and the default passphrase of “admin”. When you connect to the Edge, the Quick Setup Wizard includes a dialog box for you to set the administrator account user name and passphrase. After doing that, you must use this user name and password to see the configuration pages.
- Remote Management is disabled.
- VPN Manager Access is disabled.
- Remote logging is not configured.

WebBlocker

- The WebBlocker feature is disabled and no properties are configured.

Upgrade Options

- The upgrade options are disabled until you type the license keys into the configuration page.

Resetting the Firebox to the factory default settings

You can reset the Firebox to the factory default settings. For example, if you cannot correct a configuration problem and must “start over.” Sometimes, you have no choice. For example, if you do not know the administrator account passphrase or a power interruption damages the Firebox X Edge firmware, you must set the Firebox to the factory default settings.

You must have a copy of the most recent Firebox X Edge software on your local computer before you use this procedure.

Follow these steps to set the Firebox to the factory default settings:

- 1 Disconnect the power supply.
- 2 Hold down the **Reset** button, on the front of the Firebox.
- 3 Connect the power supply while you continue to hold down the **Reset** button.
- 4 Continue to hold down the button until the yellow Attn light comes on and stays on. This shows you that the Edge has been successfully reset.

NOTE

Do not try to connect to the Edge at this time. Start the Edge one more time, as the subsequent steps show.

- 5 Disconnect the power supply.
- 6 Connect the power supply again.
The Power Indicator is on and your Edge is reset.

Restarting the Firebox

You can restart the Firebox® X Edge from a computer on the trusted network. You can also restart the Firebox from a computer on the Internet connecting to the Firebox external interface.

The Firebox restart cycle is up to 40 seconds. During the restart cycle, the mode light on the front of the Firebox turns off and then turns on again.

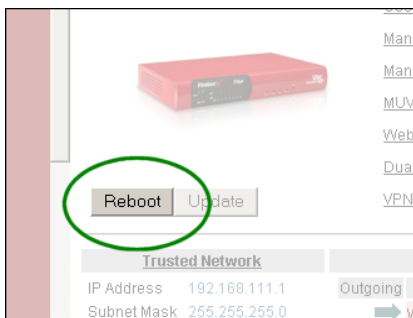
Local restart

You can locally restart the Firebox X Edge with two methods: use the Web browser or disconnect the power supply.

Using the Web browser

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`

- 2 Click **Reboot**.



Disconnecting the power supply

Disconnect the Firebox power supply. After a minimum of 10 seconds, connect the power supply.

Remote restart

You must configure the remote Firebox X Edge to send incoming HTTPS traffic to the Edge trusted interface IP address to use the method below to restart it. For more information on how to configure the Firebox to receive incoming traffic, see “Configuring Incoming Services” on page 89. After you send HTTPS traffic to the Edge trusted interface IP address:

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 2 Click **Reboot**.

Changing Your Network Settings

A primary component of WatchGuard® Firebox® X Edge setup is the configuration of the network interface IP addresses. At a minimum, you must configure the external network and the trusted network to let traffic flow through the Edge. You do this when you use the Quick Setup Wizard after you install the Edge. You can use the procedures in this chapter to change this configuration after you run the Quick Setup Wizard.

You can also set up the optional interface. Many customers use the optional network for public servers. An example of a public server is a Web server.

Using the Network Setup Wizard

The easiest method to change the network IP addresses of the Firebox® X Edge is with the Network Setup Wizard.

- 1 To connect to the System Status page, type **https://** in the browser address bar, followed by the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 2 From the navigation bar, select **Wizards**.
- 3 Adjacent to **Setup the primary network interfaces of the Firebox X Edge**, click **Go**.

4 Follow the instructions on the screens.

The Network Setup Wizard has these steps:

Welcome

The first screen describes the purpose of the wizard.

Configure the external interface of your Firebox

This screen asks the method your ISP uses to set your IP address.

For more information, see the subsequent section in this guide, “Configuring the External Network.”

Configure the external interface for DHCP

If your ISP uses DHCP, type the DHCP information that your ISP gave you. For more information, see “If your ISP uses DHCP” on page 47.

Configure the external interface for PPPoE

If your ISP uses PPPoE, type the PPPoE information that your ISP gave you. For more information, see “If your ISP uses PPPoE” on page 49.

Configure the external interface with a static IP address

If your ISP uses static IP addresses, type the static IP address information your ISP gave you. For more information, see “If your ISP uses static IP addresses” on page 48.

Configure the trusted interface of the Firebox

On this screen, type the IP address of the trusted interface. For more information, see “Configuring the Trusted Network” on page 53.

The Network Setup Wizard is complete

Configuring the External Network

You must configure your Firebox® X Edge external network manually if you do not use the Network Setup Wizard.

When you configure the external network, set the method your Internet Service Provider (ISP) uses to give you an IP address for your Firebox. There are three methods ISPs use to assign IP addresses:

- **DHCP** - Network administrators use the Dynamic Host Configuration Protocol (DHCP) to give IP addresses to computers on their network automatically. With DHCP, your

Firebox receives an external IP address each time it connects to the ISP network. It can be the same IP address each time, or it can be a different IP address.

- **Static IP address** - Network administrators use static IP addresses to manually give an IP address to each computer on their network. A static IP address can be more expensive than a dynamic IP address because static IP addresses make it easier to set up servers. Static IP addresses are also known as manual addresses.
- **PPPoE** - Many ISPs use Point to Point Protocol over Ethernet (PPPoE) to give IP addresses to each computer on their network.

To configure your Firebox® X Edge, you must know how it gets the IP address for the external interface. If you do not know the method, get the information from your ISP or corporate network administrator.

If your ISP uses DHCP

The default configuration sets the Firebox X Edge to get its external address information through DHCP. If your ISP uses DHCP, your Edge gets a new external IP address when it starts and connects to the ISP network.

For more information about DHCP, see “About DHCP” on page 5.

To manually set your Firebox to use DHCP on the external interface:

- 1 To connect to the System Status page, type **https://** in the browser address bar, followed by the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 2 From the navigation bar, select **Network > External**.
The External Network Configuration page appears.
- 3 From the Configuration Mode drop-down list, select **DHCP Client**.
- 4 If your ISP makes you identify your computer to give you an IP address, type this name in the **Optional DHCP Identifier** field.
- 5 Click **Submit**.

Network
External Network Configuration

Configuration Mode

DHCP Client

IP Address

192.168.54.54

Subnet Mask

255.255.255.0

Default Gateway

192.168.54.254

Primary DNS

192.168.130.131

Secondary DNS

192.168.130.245

DNS Domain Suffix

wgtl.net

Optional DHCP Identifier

Submit

Reset

If your ISP uses static IP addresses

If your ISP uses static IP addresses, you must enter the address information into your Edge before it can send traffic through the external interface.

To set your Edge to use a static IP address for the external interface:

- 1 Use your browser to connect to the System Status page. From the navigation bar, select **Network > External**. The External Network Configuration page appears.

- 2 From the **Configuration Mode** drop-down list, select **Manual Configuration**.

Network
External Network Configuration

Configuration Mode **Manual Configuration**

IP Address 192.168.54.54

Subnet Mask 255.255.255.0

Default Gateway 192.168.54.254

Primary DNS 192.168.130.131

Secondary DNS 192.168.130.245

DNS Domain Suffix mydomain.net

Submit **Reset**

- 3 Type the IP address, subnet mask, default gateway, primary DNS, secondary DNS, and DNS domain suffix into the related fields. Get this information from your ISP or corporate network administrator.
If you completed the table on page 15, type the information from the table.
- 4 Click **Submit**.

If your ISP uses PPPoE

If your ISP uses PPPoE, you must enter the PPPoE information into your Firebox before it can send traffic through the external interface. For more information in PPPoE, see “About PPPoE” on page 6. To set your Firebox to use PPPoE on the external interface:

- 1 Use your browser to connect to the System Status page. From the navigation bar, select **Network > External**.
The External Network Configuration page appears.

- 2 From the Configuration Mode drop-down list, select **PPPoE Client**.

The screenshot shows the 'Network' tab with the 'External Network Configuration' section. The 'Configuration Mode' is set to 'PPPoE Client'. Below this are fields for 'Name', 'Domain', and 'Password'. The 'Inactivity Timeout' is set to '0 (minutes)' and 'Link Speed' is set to 'Automatic'. The 'Advanced Settings' section includes 'Service Name', 'Access Concentrator Name', a checkbox for 'Use Host-Uniq tag in PPPoE discovery packets.', 'Static IP Address', 'Authentication retries' set to 'None', a checked checkbox for 'Use LCP echo requests to detect lost PPPoE link.', 'LCP echo interval' set to '30 seconds', 'LCP echo retries' set to '3', 'Reconnect lost PPPoE link' set to 'on outgoing packet', and a checkbox for 'Enable PPPoE debug trace.' At the bottom are 'Submit' and 'Reset' buttons.

Network
External Network Configuration

Configuration Mode: **PPPoE Client**

Name:

Domain:

Password:

Inactivity Timeout: (minutes)

Link Speed: **Automatic**

Advanced Settings

Service Name:

Access Concentrator Name:

☐ Use Host-Uniq tag in PPPoE discovery packets.

Static IP Address:

Authentication retries: **None**

☒ Use LCP echo requests to detect lost PPPoE link.

LCP echo interval: **30 seconds**

LCP echo retries: **3**

Reconnect lost PPPoE link: **on outgoing packet**

☐ Enable PPPoE debug trace.

Submit **Reset**

- 3 Type the name and password in the related fields. Get this information from your ISP. If your ISP gives you a domain name, type it into the **Domain** field.
Most ISPs using PPPoE make you use the domain name and your user name. Do not include the domain name with your user name like this: *myname@ispdomain.net*. If you have a PPPoE name with this format, type the myname section in the Name field. Type the ispdomain section in the Domain field. Do not type the @ symbol. Some ISPs do not use the domain.
- 4 In the **Inactivity Time-out** field, type the time before the Edge disconnects inactive connections.
We recommend a value of 20.

- 5 Select the **Link Speed** to set automatically, or select to assign the link speed statically at 10 Mbps Half Duplex, 10 Mbps Full Duplex, 100 Mbps Half Duplex, or 100 Mbps Full Duplex. WatchGuard recommends that you configure the link speed to Auto, unless you know this setting is not compatible with the equipment supplied by your ISP.

Advanced PPPoE Settings

In the Quick Setup Wizard you configure the basic PPPoE settings. If necessary for your configuration, you can also configure more advanced parameters:

Service Name

Use this field to add a service name. The Edge only starts with access concentrators that support the specified service. This option is not usually used. Use it only if there is more than one access concentrator or you know that you must use a specified service name.

Access Concentrator Name

Use this field to identify a PPPoE server, known as an access concentrator. The Edge only starts a session with the access concentrator you identify in this field. This option is not usually used. Use it only if you know there is more than one access concentrator. If you enter a Service Name and Access Concentrator Name, you must use the same value for the Edge to negotiate a PPPoE session.

Use Host-Uniq tag in PPPoE discovery packets

Select this option if there is more than one installation of the same PPPoE client on the network. This can prevent interference between the discovery packets of each client. This is not a supported Edge feature; WatchGuard includes this option to make the Edge compatible with ISPs which have this requirement.

Authentication retries

This field controls the number of times the Edge tries to send PAP authentication information to the PPPoE server. The default value of None is sufficient for most installations. You enter a high value to make the Edge compatible with some ISPs.

Use LCP echo request to detect lost PPPoE link

When you enable this check box, the Edge sends an LCP echo request at regular intervals to the ISP to make sure that the PPPoE connection is active. If you do not use this option, the Edge must get a PPPoE or PPP session termination request from the ISP to identify a broken connection.

LCP echo interval

When you enable LCP echoes, this value sets the interval between LCP echo requests sent by the Edge to the ISP. The more frequently the LCP echo requests are sent, the faster the Edge can identify a broken link. A shorter interval uses more bandwidth on the external interface, but even the shortest interval does not significantly decrease performance.

LCP echo retries

When you enable LCP echoes, this value sets the number of times the Edge tries to get a response to an LCP echo request before it thinks the PPPoE connection is inactive. If an ISP does not send a reply to three LCP requests, there is a low probability that it will reply to subsequent LCP echo requests. In more cases, the default setting of three is the best.

Reconnect lost PPPoE link

This setting shows how and when the Edge tries to restart a PPPoE connection after it is broken. The default value is **on outgoing packet**. With this option, the Edge tries to connect when a computer on the trusted or optional networks sends traffic to the external network. If you set the Edge to connect **immediately**, the Edge tries to connect when it finds that the PPPoE connection is broken.

Enable PPPoE debug trace

WatchGuard Technical Support uses this check box when you are troubleshooting PPPoE problems. With this option on, the Edge makes a file that you can send to Technical Support. Use this option only when Technical Support tells you because it decreases Edge performance.

Click **Submit** when you have completed the configuration of the Advanced PPPoE settings.

Configuring the Trusted Network

You must configure your trusted network manually if you do not use the Network Setup Wizard.

You can use static IP addresses or DHCP for the computers on your trusted network. The Firebox® X Edge has a DHCP server to give IP addresses to computers on your trusted and optional networks. You can also change the IP address of the trusted network.

With a factory default Firebox, its DHCP server automatically gives IP addresses to computers on the trusted network. The trusted network starts with IP address 192.168.111.1. It is a “class C” network with a subnet mask of 255.255.255.0. The Firebox can give an IP address from 192.168.111.2 to 192.168.111.254. The factory default configuration uses the same DNS server IP addresses and domain name as it uses for the external interface. For more information, see “IP Addresses” on page 5.

If necessary, you can disable the Firebox DHCP server. The Firebox can also be a DHCP Relay Agent and send DHCP requests to a DHCP server on a different network using a VPN tunnel. You can also use static IP addresses for the computers on your trusted network.

Any changes to the trusted network configuration page require that you click **Submit** and then restart the Firebox before the new configuration starts. You can make many changes and then restart just one time when you are done.

Changing the IP address of the trusted network

If necessary, you can change the trusted network address. For example, if you connect two or more Firebox devices in a virtual private network, each Firebox must use a different trusted network address. If the two sides of the VPN use the same trusted network IP addresses, one side must change the trusted network IP address range so that it is different from the other side. For more information, see “What You Need to Create a VPN” on page 130.

NOTE

If you change the IP address of the Edge's trusted interface, you must use the new IP address in your browser address bar to connect to the Edge's Web management interface.

For example, you change the Edge trusted interface IP address from the default 192.168.111.1 to 10.0.0.1, then you click Submit.

Then, you must use `https://10.0.0.1` in your browser address bar to connect to the Edge's System Status page. Also, your computer's IP address must be changed to be in the new trusted interface IP subnet range.

To change the IP address of the trusted network:

- 1 To connect to the System Status page, type **https://** in the browser address bar, followed by the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 2 From the navigation bar, select **Network > Trusted**.
The Trusted Network Configuration page appears.
- 3 Type the new IP address of the Firebox X Edge's trusted interface in the **IP Address** text field.
- 4 If necessary, type the new subnet mask.
Most networks use 255.255.255.0 which includes 254 addresses.

The screenshot shows the 'Trusted Network Configuration' page. It has a title bar with 'Network' and 'Trusted Network Configuration'. Below the title bar, there are several configuration fields: 'IP Address' (192.168.111.1), 'Subnet Mask' (255.255.255.0), a checkbox for 'Enable DHCP Server on Trusted Network', 'First address for DHCP server' (192.168.111.2), 'Last address for DHCP server' (192.168.111.252) with a 'DHCP Reservations...' button, 'WINS Server Address', 'DNS Server Address', 'Secondary DNS Server Address', 'DNS Domain Suffix', a checkbox for 'Enable DHCP Relay', and 'DHCP relay server'. At the bottom, there are 'Submit' and 'Reset' buttons.

Using DHCP on the trusted network

The DHCP Server option sets the Firebox X Edge to give IP addresses to the computers on the trusted network. When the Firebox receives a DHCP request from a computer on the trusted network, it gives

the computer an IP address. A factory default Firebox has the DHCP Server option for the trusted interface enabled.

To use DHCP on the trusted network:

- 1 Use your browser to connect to the System Status page. From the navigation bar, select **Network > Trusted**.
The Trusted Network Configuration page appears.
- 2 Select the **Enable DHCP Server on the Trusted Network** check box.
- 3 Type the first available IP address for the trusted network. Type the last IP address.
The IP addresses must be on the same network as the trusted IP address. For example, if your trusted IP address is 192.168.200.1, the IP addresses can be from 192.168.200.2 to 192.168.200.254.
- 4 Type the **WINS Server Address**, **DNS Server Primary Address**, **DNS Server Secondary Address**, and **DNS Domain Suffix** in the correct text boxes.
Use these fields if you have a WINS or DNS server. If you do not enter a value, the Firebox uses the same values as those used for the external network.
- 5 Click **Submit**.

Setting trusted network DHCP address reservations

You can manually give the same IP address to a specified computer on your trusted network each time that computer makes a request for a DHCP IP address. The Firebox identifies the computer by its MAC address.

- 1 Use your browser to connect to the System Status page. From the navigation bar, select **Network > Trusted**.
The Trusted Network Configuration page appears.

- Click the **DHCP Reservations** button.
The DHCP Address Reservations page appears.

The screenshot shows the 'DHCP Address Reservations' page. At the top, there is a breadcrumb trail: 'Network > Trusted Network' followed by the page title 'DHCP Address Reservations'. Below this, network configuration details are listed: 'Trusted Network IP Address' is 192.168.111.1, 'Trusted Network Subnet Mask' is 255.255.255.0, and 'DHCP Address Pool' is 192.168.111.2-192.168.111.252. The main section is titled 'DHCP Address Reservations' and contains a table with two columns: 'IP Address' and 'MAC Address'. The first row shows '192.168.111.24' and '000BDBA3B091'. To the right of the table is a 'Remove' button. Below the table are two input fields labeled 'IP Address' and 'MAC Address', followed by an 'Add' button. At the bottom of the page are 'Submit' and 'Reset' buttons.

IP Address	MAC Address
192.168.111.24	000BDBA3B091

Remove

IP Address MAC Address

Add

Submit Reset

- Type a static IP address in the **IP Address** field. The IP address must be on the trusted network.
For example, if the trusted network starts with 192.168.111.1, you can enter any address from 192.168.111.2 to 192.168.111.254.
- Type the MAC address of the computer on the trusted network in the **MAC Address** field. You must enter the MAC address as 12 hexadecimal digits with no space, dash, or semicolon characters. Click **Add**.
- Click **Submit**.

Configuring the trusted network for DHCP relay

One method to get IP addresses for the computers on the Firebox trusted network is to use a DHCP server on a different network. The Firebox can send a DHCP request to a DHCP server at a different location through a VPN tunnel. It gives the reply to the computers on the Firebox trusted network. This option lets computers in more than one office use the same network address range. In this procedure the Firebox is a DHCP Relay Agent. You must set up a VPN between the Firebox and the DHCP server for this feature to operate correctly.

To configure the Firebox as a DHCP Relay Agent for the trusted interface:

- 1 Use your browser to connect to the System Status page. From the navigation bar, select **Network > Trusted**. The Trusted Network Configuration page appears.
- 2 Select the **Enable DHCP Relay** check box.
- 3 Type the IP address of the DHCP server in the related field.
- 4 Click **Submit**. You must restart the Firebox for new configuration to start.

NOTE

If the Firebox cannot connect to the DHCP server in 30 seconds, it uses its own DHCP server to give IP addresses to computers on the trusted network. You must enable the DHCP Server on the trusted network for DHCP relay to operate.

Using static IP addresses for trusted computers

You can use static IP addresses for some or all of the computers on your trusted network. If you disable the Edge DHCP server and you do not have a DHCP server on your network, you must manually configure the IP address and subnet mask of each computer. For example, this is necessary when a client-server software application must use a static IP address for the server. Static IP addresses must be on the same network as the Firebox trusted interface. Computers on the trusted network with static IP addresses must use the Firebox's trusted interface IP address for the default gateway.

To disable the Firebox DHCP server, clear the **Enable DHCP Server on the Trusted Network** check box on the Trusted Network Configuration page.

NOTE

Computers on the trusted network must use the Firebox's trusted interface IP address as the default gateway. If a computer does not use the Firebox for the default gateway, it usually cannot get to the external network or the Internet.

Adding computers to the trusted network

You can connect as many as seven computers to the trusted interface of the Firebox X Edge if you connect each computer to one of the Edge's Ethernet ports 0 through 6. You can use 10/100 BaseT

Ethernet hubs or switches with RJ-45 connectors to connect more than seven computers. It is not necessary for the computers on the trusted network to use the same operating system.

To add more than seven computers to the trusted network:

- 1 Make sure that each computer has a functional Ethernet card.
- 2 Connect each computer to the network. Use the procedure “Connecting the Edge to more than seven devices” on page 20.

Configuring the Optional Network

The optional network is an isolated network for less secure public resources. A factory default Firebox does not allow traffic from the optional network to get to the trusted network. A factory default Firebox does allow traffic that starts from the trusted network to get to the optional network, but you can restrict that traffic. See “Services for the Optional Network” on page 101 to see how to do this. Because traffic that is started from the optional network is usually not allowed to the trusted network, you can use the optional network for servers that other computers can connect to from the Internet, such as a Web, e-mail, or FTP server. We recommend you isolate your private network from these servers because the public can connect to them. If a server on the optional network is attacked from the Internet, the attacker cannot get to the computers on the trusted network. The trusted network is the most secure location for your private network.

If your computer is on the optional network, you can connect to the Edge’s system configuration pages using the optional interface IP address. The default URL is <https://192.168.112.1>.

You can use the Firebox X Edge DHCP server or you can use static IP addresses for computers on the optional network. You can also change the IP address range of the optional network.

If you make any changes to the optional network configuration page, you must click **Submit** and then restart the Firebox before the new configuration starts. You can make many changes, and then restart just once when you are done.

Enabling the optional network

- 1 To connect to the System Status page, type **https://** in the browser address bar, followed by the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 2 From the navigation bar, select **Network > Optional**.
The Optional Network Configuration page appears.
- 3 Select the **Enable Optional Network** check box.

Network
Optional Network Configuration

☒ Enable Optional Network

IP Address

Subnet Mask

☒ Enable DHCP Server on Optional Network

First address for DHCP server

Last address for DHCP server

WINS Server Address

DNS Server Address

Secondary DNS Server Address

DNS Domain Suffix

☐ Enable DHCP Relay on Optional Network

DHCP relay server

Changing the IP address of the optional network

If necessary, you can change the optional network address. A factory default Firebox has the optional interface IP address set to 192.168.112.1, so the trusted network and the optional networks are on two different subnets.

To change the IP address of the optional network:

- 1 To connect to the System Status page, type **https://** in the browser address bar, followed by the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`

- 2 From the navigation bar, select **Network > Optional**.
The Optional Network Configuration page appears.
- 3 Type the first address of the new network address range in the **IP Address** text field.
- 4 If necessary, type the new subnet mask.
Most networks use 255.255.255.0 which includes 254 addresses.

Using DHCP on the optional network

The DHCP Server option sets the Firebox X Edge to give IP addresses to the computers on the optional network. When the Firebox receives a DHCP request from a computer on the optional network, it gives the computer an IP address. A factory default Firebox has the DHCP Server option for the optional interface turned off.

To use DHCP on the optional network:

- 1 Use your browser to connect to the System Status page. From the navigation bar, select **Network > Optional**.
The Optional Network Configuration page appears.
- 2 Select the **Enable DHCP Server on the Optional Network** check box.
- 3 Type the first available IP address for the optional network. Type last IP address.
The IP addresses must be on the same network as the optional IP address. For example, if your optional IP address is 192.168.112.1, the IP addresses can be from 192.168.112.2 to 192.168.112.254.
- 4 Type the **WINS Server Address**, **DNS Server Primary Address**, **DNS Server Secondary Address**, and **DNS Domain Suffix** in the related fields.
Use these fields if you have a WINS or DNS server. If you do not enter a value, the Firebox uses the same values as those used for the external network.
- 5 Click **Submit**.

Setting optional network DHCP address reservations

You can manually assign an IP address to a specified computer on your optional network. The Firebox identifies the computer by its MAC address.

- 1 Use your browser to connect to the System Status page. From the navigation bar, select **Network > Optional**.
The Optional Network Configuration page appears.

- 2 Click the **DHCP Reservations** button.
The DHCP Address Reservations page appears.

Network > [Optional Network](#)
DHCP Address Reservations

Optional Network IP Address 192.168.112.1
 Optional Network Subnet Mask 255.255.255.0
 DHCP Address Pool 192.168.112.2-192.168.112.252

DHCP Address Reservations

IP Address	MAC Address	
<input type="text"/>	<input type="text"/>	<input type="button" value="Remove"/>

IP Address MAC Address

- 3 Type a static IP address in the **IP Address** field. The IP address must be on the optional network.
For example, if the optional network starts with 192.168.112.1, you can enter 192.168.112.2 to 192.168.112.251.
- 4 Type the MAC address of the computer on the optional network in the **MAC Address** field. You must enter the MAC address as 12 hexadecimal digits with no space, dash, or semicolon characters. Click **Add**.
- 5 Click **Submit**.

Configuring the optional network for DHCP relay

One method to get IP addresses for the computers on the Firebox optional network is to use a DHCP server on a different network. The Firebox can send a DHCP request to a DHCP server at a different location. It gives the reply to the computers on the Firebox optional network. This option lets computers in more than one office use the same network address range. In this procedure, the Firebox is a DHCP Relay Agent.

To configure the Firebox as a DHCP Relay Agent for the optional interface:

- 1 Use your browser to connect to the System Status page. From the navigation bar, select **Network > Optional**. The Optional Network Configuration page appears.
- 2 Select the **Enable DHCP Relay on Optional Network** check box.
- 3 Type the IP address of the DHCP server in the related field.
- 4 Click **Submit**. You must restart the Edge for the new configuration to start.

NOTE

If the Firebox cannot connect to the DHCP server in 30 seconds, it uses its DHCP server to give IP addresses to computers on the optional network. You must enable the DHCP server on the optional network for DHCP relay to operate.

Using static IP addresses for optional computers

You can use static IP addresses for some or all of the computers on your optional network. If you disable the DHCP server and you do not have a DHCP server on your optional network, you must manually configure the IP address and subnet mask of each computer. You can also configure specified computers with a static IP address. For example, this is necessary when a client-server software application must use a static IP address for the server. Static IP addresses must be on the same network as the Edge optional interface. Computers on the optional network with static IP addresses must use the Firebox's optional interface IP address for the default gateway.

To disable the Firebox DHCP server, clear the **Enable DHCP Server on the Optional Network** check box on the Optional Network Configuration page.

NOTE

Computers on the optional network must use the Firebox's optional interface IP address as the default gateway. If a computer does not use the Firebox for the default gateway, it usually cannot get to the external network or the Internet.

Adding computers to the optional network

You can directly connect only one computer to the Firebox X Edge because there is only one optional Ethernet port. To connect more

than one computer to the optional interface, use a 10/100 BaseT Ethernet hub or switch with RJ-45 connectors. It is not necessary for the computers on the optional network to use the same operating system.

To add more than one computer to the optional network:

- 1 Make sure that each computer has a functional Ethernet card.
- 2 Set each computer to use DHCP. For more information, see “Setting Your Computer to Connect to the Edge” on page 22.
- 3 Connect each computer to the network. Use the procedure “Connecting the Edge to more than seven devices” on page 20.
- 4 Restart each computer.

Making Static Routes

You can configure the Firebox to send traffic to networks that are behind routers on your trusted network by adding static routes to these networks. Use the Routes page to make a static route:

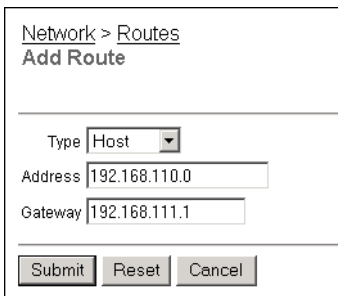
- 1 To connect to the System Status page, type **https://** in the browser address bar, followed by the IP address of the Edge trusted interface.
The default URL is: https://192.168.111.1
- 2 From the navigation bar, select **Network > Routes**.
The Routes page appears.

Address	Gateway
Host 192.168.110.0	192.168.111.1

Add...
Remove

3 Click **Add**.

The Add Route page appears.



Network > Routes
Add Route

Type

Address

Gateway

4 From the **Type** drop-down list, select **Host** or **Network**.

This box tells if the destination for the static route is one computer or a network of computers.

NOTE

A host is one computer. A network is more than one computer using a range of IP addresses.

You must type network addresses in "slash" notation (also known as Classless Inter Domain Routing or CIDR notation). Do not type a slash for a host IP address. For more information on how to enter IP addresses in slash notation, refer to this FAQ: http://www.watchguard.com/support/advancedfaqs/general_slash.asp

5 Type the destination IP address and the gateway in the related fields.

The gateway is the local interface IP address of the router. The gateway IP address must be in the Firebox's trusted, optional, or external network range.

6 Click **Submit**.

To remove a static route, click the IP address and click **Remove**.

Viewing Network Statistics

The Firebox® X Edge Network Statistics page shows information about performance. Network administrators frequently use this page to troubleshoot a problem with the Firebox or network.

- 1 To connect to the System Status page, type **https://** in the browser address bar, followed by the IP address of the Edge trusted interface.
The default URL is: https://192.168.111.1
- 2 From the navigation bar, select **Network > Network Statistics**.
The Network Statistics page appears.

Network Statistics	
IP	
IP:	Up for 42 minutes 44 seconds Network Buffers Allocated/Total (-4913/100) Memory Total/Largest Block (21062352/20739312) Sockets Allocated/Total (7/80) NAT Ports Avail (7000) RAM Disk Available (514048 bytes 96%) Flash Disk Available (129578 bytes 98%) Tx: packets (841) Rx: packets (1055) hdr Err (309) delivered (746)
External Network	
eth0:	Link encap:Ethernet HWaddr 00:90:7f:0f:dd:dd inet addr:192.168.54.54 RX packets:904 errors:0 bcast:4096 disc:0 unk:0 TX packets:887 errors:0 bcast:0
Trusted Network	
eth1:	Link encap:Ethernet HWaddr 00:90:7f:0f:ff:ff inet addr:192.168.111.1 RX packets:0 errors:0 bcast:0 disc:0 unk:0 TX packets:0 errors:0 bcast:0

This page includes this information:

- Miscellaneous system status counters
- IP protocol stack counters
- Network interface counters, in this order:
 - External interface
 - Trusted interface
 - Optional interface
 - Failover interface
- Routing table for the Firebox

Registering with the Dynamic DNS Service

You can register the external IP address of the Firebox X Edge with the dynamic Domain Name Server (DNS) service DynDNS.org. A dynamic DNS service makes sure that the IP address attached to your domain name changes when your ISP gives your Firebox X Edge a new IP address. For more information, refer to these WatchGuard FAQs:

What is Dynamic DNS?

How do I set up Dynamic DNS?

https://www.watchguard.com/support/AdvancedFaqs/sogen_main.asp

After you click this link, log into your LiveSecurity Service account to see the FAQ.

NOTE

WatchGuard is not affiliated with DynDNS.org.

Create a DynDNS.org account.

To set up your account, go to this Web page:

<http://www.dyndns.org>

This page also has information about how Dynamic DNS operates.

For more information, see the Technical Support FAQ “How do I set up Dynamic DNS?”

Set up the Firebox for Dynamic DNS

- 1 To connect to the System Status page, type **https://** in the browser address bar, followed by the IP address of the Edge trusted interface.

The default URL is: <https://192.168.111.1>

- 2 From the navigation bar, select **Network > Dynamic DNS**.
The Dynamic DNS client page appears.

Network

Dynamic DNS client

Information about Dynamic DNS available [here](#)

☐ Enable Dynamic DNS client

Domain

Name

Password

System dyndns

Options

- 3 Select the **Enable Dynamic DNS client** check box.
- 4 Type the **Domain**, **Name**, and **Password** in the related fields.
- 5 In the **System** drop-down list, select the system to use for this update.
The option dyndns sends updates for a Dynamic DNS host name. The option statdns sends updates for a Static DNS host name. The option custom sends updates for a Custom DNS host name. For an explanation of each option, see: <http://www.dyndns.org/services/>
- 6 In the **Options** field, you can type these options:
mx=mailexchanger
backmx=YES|NO
wildcard=ON|OFF|NOCHG
offline=YES|NO
See this site for more information:
<http://www.dyndns.org/developers/specs/syntax.html>
- 7 Click **Submit**.

NOTE

The Firebox gets the IP address of members.dyndns.org when it connects to a time server. The Firebox connects to a time server when it starts up.

The Firebox connects to the IP address it finds for members.dyndns.org to register the current Firebox external IP address with the DynDNS service.

The Firebox does not operate with other Dynamic DNS services, only DynDNS.org.

Enabling the WAN Failover Option

The WAN Failover option supplies redundant support for the external interface. With this option, the Firebox® X Edge starts a connection through the WAN2 port when the primary external interface (WAN1) cannot send traffic. Companies use this option if they must have a constant Internet connection. You must have a second Internet connection to use this option. You can have a second broadband connection, or use an external modem connected to the Edge to supply a failover Internet connection.

It is not necessary to configure new services to use this option. The failover interface uses the same services and network properties as the external interface.

The Firebox uses two procedures to see if the external interface is functional:

- The status of the link between the external interface and the device it is connected to (usually a router).
- A ping command to a specified location

The Firebox sends a pings to the default gateway or a computer specified by the administrator. If there is no reply, the Firebox changes to the secondary external network interface (WAN2).

When you enable the WAN Failover, the Firebox does the following:

- If the WAN1 interface connection stops, the Firebox starts to use the WAN2 interface.
- If the WAN2 interface connection stops, the Firebox starts to use the WAN1 interface.

- If the WAN1 interface and the WAN2 interface stop, the Firebox tries the two interfaces until it makes a connection.

When the WAN2 interface is in use, the Edge will monitor the primary (WAN1) interface. When the WAN1 interface becomes available, the Edge will automatically go back to using the WAN1 interface.

To configure the WAN failover network:

- 1 Connect one end of a straight-through Ethernet cable to the WAN2 interface. Connect the other end to the source of the secondary external network connection. This connection can be a cable modem or a hub.
- 2 To connect to the System Status page, type **https://** in the browser address bar, followed by the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 3 Configure the failover network with the WAN Failover Setup Wizard or with the Network page of the configuration pages, as described in the subsequent two sections.

Using the WAN Failover Setup Wizard

- 1 From the navigation bar, select **Wizards**.
- 2 Adjacent to **Configure the automatic WAN failover capability of your Firebox Edge**, click **Go**.
- 3 Follow the instructions on the screens.

The WAN Failover Setup Wizard includes these steps:

Welcome

The first screen tells you about the wizard.

Select the secondary interface

Use this screen to set the secondary interface your Edge uses: broadband or modem.

Configure the broadband interface

If you use a broadband interface, select the method your ISP uses to get your IP address.

Configure the modem interface

If you use a modem interface, select your ISP and type the necessary settings to connect to your ISP.

Identify the computers to connect

Type the IP addresses of computers to which the Edge can connect.

The WAN Failover Setup Wizard is complete

You can restart your Edge to activate the WAN Failover feature.

Using the Network page

- 1 From the navigation bar, select **Network > WAN Failover**.
The WAN Failover page appears.

The screenshot shows the 'Network' section with 'WAN Failover' selected. It contains two main configuration areas: 'Failover Settings' and 'Ethernet (WAN2) Configuration'.

Failover Settings

- ☐ Enable failover using the **Ethernet (WAN2)** interface
- Host to ping on the External Network:
- Host to ping on the Failover Network:
- Ping interval: (seconds)
- Reply timeout: (seconds)
- No reply limit:
- Ping replies needed for fallback:

Ethernet (WAN2) Configuration

- Configuration Mode: **PPPoE Client**
- Name:
- Domain: [optional]
- Password:
- Inactivity Timeout: (minutes)
- Link Speed: **Automatic**

- 2 From the drop-down list, select the interface for the feature:
Ethernet (WAN2) or Modem (serial port).
- 3 Select the **Enable failover using the Ethernet (WAN2)/Modem (serial port) interface** check box.
- 4 Type the IP addresses of the hosts to ping for WAN1 (external) and WAN2 (failover) interfaces in the correct fields.
- 5 Type the number of seconds between pings and the number of seconds to wait for a reply in the correct fields.

- 6 Type the maximum number of pings before time-out in the related field.

Network
WAN Failover

Failover Settings

☒ Enable failover using the **Ethernet (WAN2)** interface

Host to ping on the External Network

Host to ping on the Failover Network

Ping interval (seconds)

Reply timeout (seconds)

No reply limit

If you are using a broadband connection for failover

If you selected to enable failover with a broadband connection on WAN2, select your configuration mode from the drop-down list.

If you selected DHCP Client

If your ISP makes you identify your computer to give you an IP address, type this name in the **Optional DHCP Identifier** field.

Ethernet (WAN2) Configuration

Configuration Mode **DHCP Client**

IP Address **Not Active**

Subnet Mask **Not Active**

Default Gateway **Not Active**

Primary DNS server **Not Active**

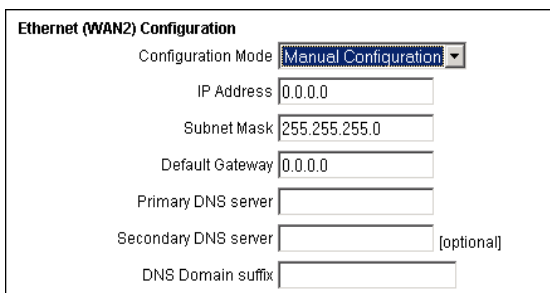
Secondary DNS server **Not Active**

DNS Domain Suffix **Not Active**

DHCP Identifier [optional]

If you selected Manual Configuration

- 1 Type the IP address, subnet mask, default gateway, primary DNS, secondary DNS, and DNS domain suffix into the related fields. Get this information from your ISP or corporate network administrator.
If you completed the table on page 15, type the information from the table.
- 2 Click **Submit**.



The screenshot shows the 'Ethernet (WAN2) Configuration' window. At the top, 'Configuration Mode' is set to 'Manual Configuration' in a dropdown menu. Below this are several input fields: 'IP Address' with the value '0.0.0.0', 'Subnet Mask' with '255.255.255.0', 'Default Gateway' with '0.0.0.0', 'Primary DNS server' (empty), 'Secondary DNS server' (empty) with a '[optional]' label, and 'DNS Domain suffix' (empty).

If you selected PPPoE

See “If your ISP uses PPPoE” on page 49 for information on PPPoE settings and configure WAN2 with this information.

If you are using an external modem for failover

If failover occurs, the Edge can find a remote secondary host for sending traffic with a modem. We support these modems:

- Hayes 56K V.90 serial fax modem
- Zoom FaxModem 56K model 2949
- U.S. Robotics 5686 external modem
- Creative Modem Blaster V.92 serial modem
- MultiTech 56K Data/Fax Modem International

- 1 From the drop-down list on the WAN Failover page, select **Modem (serial port)**.
- 2 Below **Dial Up Account Settings**, use the drop-down list to select your ISP. We support these ISPs: Standard PPP, AT&T Worldnet, CompuServe 4.0, EarthLink, and MSN.
- 3 Type the telephone number of your ISP. You can also type an alternate telephone number.
- 4 Type the account name used by your ISP for your modem.
- 5 (Optional) If you log in to your account with a domain name (such as msn.com), enter it in **Account Domain**.
- 6 Type the account password.

- 7 To enable modem and PPP debug trace, select the related check box.

Modem (serial port) Configuration

Account DNS Dial Up

Dial Up Account Settings

Internet Service Provider MSN

Telephone number 330-0040

Alternate telephone number [optional]

Account name msn/watchguardqa

Account domain [optional]

Account password

☐ Enable modem and PPP debug trace

Submit Reset

DNS settings

If your dialup ISP does not give DNS server IP addresses, or if your ISP gives you a DNS server IP address and you must use a different DNS server, you can manually enter the IP addresses for your DNS server:

- 1 Select the **Manually configure DNS server IP addresses** check box.
- 2 In the **Primary DNS Server** text box, type the IP address of the primary DNS server.
- 3 (Optional) In the **Secondary DNS Server** text box, type the IP address of the secondary DNS server.

Modem (serial port) Configuration

Account

DNS

Dial Up

DNS Settings

☐ Manually configure DNS server IP addresses

Primary DNS server

Secondary DNS server [optional]

Submit

Reset

Dialup settings

- 1 In the **Dial up time-out** field, type the number of seconds before time-out if your modem does not connect.
- 2 In the **Redial attempts** field, enter the number of times the Edge will try to redial if your modem does not connect.
- 3 In the **Inactivity time-out** field, enter the number of seconds before time-out if no traffic goes through the modem.
- 4 In the **Speaker volume** field, set your modem speaker volume to off, low, medium, or high.

Modem (serial port) Configuration

Account

DNS

Dial Up

Dialing Options

Dial up time-out (minutes)

Redial attempts

Inactivity Timeout (minutes)

Speaker volume

Submit

Reset

Firebox X Edge Wireless Setup

The Firebox® X Edge Wireless protects the computers that are connected to your network and it protects your network wireless connections. This chapter examines how to install the Firebox X Edge Wireless and set up the wireless network.

To make sure that your network is secure, WatchGuard disables the wireless feature of the Firebox X Edge Wireless until you activate wireless traffic.

To install the Firebox X Edge Wireless:

- Identify and record your TCP/IP settings
- Disable the HTTP Proxy parameters of your Web browser
- Activate DHCP on your computer
- Make the physical connections between the Firebox X Edge Wireless and your network using a 10bt or 100bt ethernet connection. You must connect to the Edge with a network connection to configure it to be used as a wireless device.
- Attach the two antennae to the Firebox X Edge Wireless
- Install the Firebox X Edge Wireless in a location more than 20 centimeters from all persons. Put the Firebox X Edge Wireless in a location away from other antennae or transmitters

To set up the wireless network:

- Configure the wireless network

- Configure the Wireless Access Point (WAP)
- Configure the wireless card on your computer

How Wireless Networking Works

Wireless networks use radio signals to send and receive traffic from computers and the Firebox X Edge Wireless. The Firebox® X Edge Wireless obeys the 802.11b and 802.11g guidelines set by the Institute of Electrical and Electronics Engineers (IEEE). You must protect your wireless network from unauthorized access because the wireless signal can go out of your physical location. If you do not protect your network, unauthorized users use your wireless signal to attack your network or use your Internet connection. You increase the security of your corporate network when you make users authenticate as MUVPN clients. A VPN creates a secure IPSec tunnel from the wireless computer to the Firebox X Edge Wireless.

Connecting to the Firebox X Edge Wireless

The Firebox X Edge Wireless can protect one computer, or all the computers that connect to your network. The Firebox X Edge Wireless also operates as a hub to connect other computers.

To set up a wireless network, you connect a computer with a Web browser to the Firebox X Edge Wireless with an Ethernet cable. You use this computer that is connected through the Ethernet cable to configure the wireless network.

See “Connecting the Edge to more than seven devices,” on page 20 for information about connecting computers, printers, scanners, or other devices that connect directly to the Firebox X Edge Wireless.

Configuring the Wireless Card on Your Computer

These instructions are for the Windows XP operating system. To see the installation instructions for other operating systems, go to:
<http://www.watchguard.com/support/sohoresources/>

- 1 Click **Start > Settings > Control Panel > Network Connections**.

The Network Connections dialog box appears.

- 2 Double-click **Wireless Network Connection**.
The Wireless Network Connection dialog box appears.
- 3 Click the **Wireless Networks** tab.
- 4 In the **Preferred networks** section, click **Add**.
The Wireless Network Properties dialog box appears.
- 5 Type the SSID in the **Network Name (SSID)** text box.
- 6 Click **OK** to close the **Wireless Network Properties** dialog box.
- 7 Click **Refresh**.
All available wireless connections appear in the Available Networks text box. Select the SSID of the computer to configure.
- 8 Click **OK** to enable the wireless connection.
The wireless network connection shows that your wireless network is active.
- 9 Configure the wireless computer to use DHCP. For more information about how to configure DHCP, see “Setting Your Computer to Connect to the Edge” on page 22.

The Firebox® X Edge Wireless is configured to protect the wired and wireless computers that are attached to it from security risks.

Using the Wireless Network Wizard

The Wireless Network Wizard is a tool that you use to automatically configure your Firebox® X Edge wireless network. To start the wizard, select **Wizards** from the navigation bar and click **Go** adjacent to the Wireless Network Wizard.

Wireless Security Options

The Firebox® X Edge has many options you can use when protecting your wireless network.

Two of the most important options are:

- The type of authentication to use
- The type of encryption to use

The Firebox X Edge uses two security protocol standards to protect your wireless network. They are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). These two protocols support the IEEE standards 802.11g and 802.11b. WPA and WEP give a Wireless Local

Area Network (WLAN) a level of security and privacy that compares well to a wired Local Area Network (LAN).

A wired LAN is usually protected by features that include login passphrases, which operate only in a controlled physical area. Because the walls of a building do not stop wireless transmissions, this feature does not help protect a wireless network. WPA and WEP encrypt the transmissions on the WLAN to supply physical security for the wireless connections between the computers and the access points. Also, you must use other LAN security mechanisms including password protection, VPN tunnels, and authentication to protect privacy.

Setting up the Wireless Access Point

To make sure that your network is secure, WatchGuard disables the wireless feature of the Firebox® X Edge Wireless until you activate wireless traffic. You can activate the wireless feature when you configure the security of the wireless connections.

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.

The default URL is: `https://192.168.111.1`

- 1 From the navigation bar, select **Network > Wireless (802.11g)**.

The screenshot shows the 'Network Wireless Configuration' page. It is divided into three sections: Basic Settings, Security Settings, and Advanced Settings. In Basic Settings, 'Network assignment' is set to 'Bridge to Trusted Network', 'Network name (SSID)' is 'tribbles', 'Operating Region' is 'Americas', and 'Channel' is 'Auto'. In Security Settings, 'Authentication' is 'WPA-PSK', 'Encryption' is 'TKIP', and 'Passphrase' is 'tribbles'. There is an unchecked checkbox for 'Require encrypted MUVPN connections for wireless clients'. In Advanced Settings, 'Broadcast SSID and respond to SSID queries' is checked, 'Restrict Access by Hardware Address' is checked with an 'Edit...' button, 'Log Authentication Events' is checked, 'Wireless mode' is '802.11g and 802.11b', and 'Fragmentation Threshold' is '2346' (256-2346 bytes). At the bottom are 'Submit' and 'Reset' buttons.

The Wireless Network Configuration page appears.

Configuring basic settings

The SSID (Service Set Identifier) is the sequence of characters that gives your Wireless network a unique name. You must configure the wireless network card in your computer to have the same SSID so your computer can send traffic to the Firebox X Edge Wireless.

NOTE

When you complete the wireless configuration, restart your Firebox X Edge Wireless.

The **Network Assignment** drop-down list gives you three alternatives:

- None (disable wireless)
 - Bridge to trusted network
 - Bridge to optional network
- Select the option that matches your needs.

Bridge to Trusted

In this mode, the wireless client is a part of the trusted network. If the wireless client sets the IP address of its wireless network card with a static IP address, the IP address must be in the trusted IP address range of the Edge. If the wireless network card is set to DHCP, the DHCP server on the Edge's trusted network must be active and configured. The wireless client can send any type of traffic to the other computers on the trusted network if this option is set to Bridge to Trusted. This includes Windows Networking NetBIOS broadcasts.

Bridge to Optional

In this mode, the wireless client is a component of the optional network. If you use this option, you must first activate the optional network. It is not enabled by default. If the wireless client has its wireless network card set with a static IP address, the IP address must be in the optional IP address range of the Edge. If the wireless network card is set to DHCP, the DHCP server on the Edge's optional network must be active and configured. The wireless client can send any type of traffic to the other computers on the optional network if this option is set to Bridge to Optional. This includes Windows Networking NetBIOS broadcasts.

Disabled

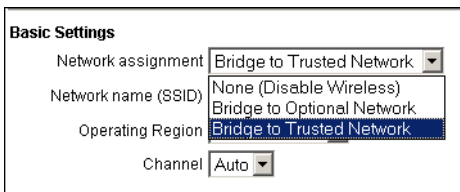
In this mode the radio inside the Firebox X Edge is turned off.

Because the wireless client is a part of the optional network or trusted network, it is important to think about the networking

requirements of wireless clients. The firewall properties control the traffic between these two networks

NOTE

Because any wireless clients are a component of the optional or the trusted networks, wireless clients can be a part of any Branch Office VPN tunnels you have when the local network component of the Phase 2 settings include optional or trusted network IP addresses. To control access to the VPN, you can make Firebox users authenticate.



The screenshot shows a window titled "Basic Settings" with four configuration fields:

- Network assignment:** A dropdown menu with "Bridge to Trusted Network" selected.
- Network name (SSID):** A dropdown menu with "None (Disable Wireless)" selected.
- Operating Region:** A dropdown menu with "Bridge to Trusted Network" selected.
- Channel:** A dropdown menu with "Auto" selected.

To change the SSID of the Firebox X Edge Wireless:

- Type a new identification number in the **SSID** field.

To change the channel:

- Select a value from the **Channel** drop-down list.
There are eight options for operating region: Americas, Asia, Australia, EMEA, France, Israel, Japan and People's Republic of China. This parameter is configured when you use the Quick Setup Wizard. This setting applies to the certification requirements of your region and cannot be changed after it is set.

Security Settings

Select the authentication method to use for your wireless network connection. The options are **Open System**, **Shared Key**, and **WPA-PSK**.

Open System

Open System authentication allows any user to authenticate with the access point, if they know the correct encryption key or if they do not. This method can be used with no encryption, or with WEP encryption. Although Open System authentication is


the default authentication method for some versions of Microsoft windows, it is not recommended.

Shared Key

In Shared Key authentication, only those wireless clients that have the shared key can authentication. This is more secure than Open System authentication. Shared Key authentication can only be used with WEP encryption.

WPA-PSK

Although WPA supports more than one authentication method, PSK (pre-shared key) is the only WPA authentication method the Firebox X Edge supports at this time.



The screenshot shows a 'Security Settings' window with the following fields and options:

- Authentication:** A dropdown menu currently set to 'WPA-PSK'.
- Encryption:** A dropdown menu currently set to 'TKIP'.
- Passphrase:** A text input field containing the word 'tribbles'.
- Require encrypted MUVPN connections for wireless clients:** An unchecked checkbox.

Configuring encryption

From the **Encryption** drop-down list, select the level of encryption for your wireless connections. The options change when you use different authentication mechanisms.

Open system authentication

Encryption options for open system authentication are WEP 64 bit hexadecimal, WEP 40 bit ASCII, WEP 128 bit hexadecimal, WEP 128 bit ASCII, and the option to disable encryption.

- 1 If you use WEP encryption, type hexadecimal or ASCII characters in the **Key** text boxes. Not all versions of Windows support ASCII characters.
You can have a maximum of four keys that the wireless network uses for connections.
 - A WEP 64-bit hexadecimal key must have 10 hexadecimal (0-F) characters.
 - A WEP 40-bit ASCII key must have 5 characters.
 - A WEP 128-bit hexadecimal key must have 26 hexadecimal characters (0-F).
 - A WEP 128-bit ASCII key must have 13 characters.

- 2 If you typed more than one key, click the key to use as the default key from the **Key Index** drop-down list.
The Firebox X Edge can use only one key at a time. If you select a key other than the first key in the list, you must also set your wireless client to use the same key number.

Shared key authentication

Encryption options for shared key authentication are WEP 64 bit hexadecimal, WEP 40 bit ASCII, WEP 128 bit hexadecimal, and WEP 128 bit ASCII.

- 1 If you use WEP encryption, type hexadecimal or ASCII characters in the **Key** text boxes.
You can have a maximum of four keys that the wireless network uses for connections.
 - A WEP 64-bit hexadecimal key must have 10 hexadecimal (0-F) characters.
 - A WEP 40-bit ASCII key must have 5 characters.
 - A WEP 128-bit hexadecimal key must have 26 hexadecimal characters (0-F).
 - A WEP 128-bit ASCII key must have 13 characters.
- 2 If you typed more than one key, click the key you want to use as the default key from the **Key Index** drop-down list.

WPA-PSK authentication

The encryption options for WPA-PSK authentication are TKIP and AES. WPA-PSK only operates correctly if you are using Windows XP Service Pack 2 or higher.

Click **Auto** to select the encryption algorithm.

Configuring wireless clients to use MUVPN

To make wireless computers authenticate as MUVPN clients:

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`.
- 2 From the navigation bar, select **Network > Wireless**.
- 3 Select the check box **Require encrypted MUVPN connections for wireless clients**.
- 4 Click **Submit**.

Configuring advanced settings

You can configure how the Firebox X Edge Wireless transmits data to your wireless computer.

Wireless computers send requests to see if there are wireless access points to which they can connect. To configure the Firebox X Edge Wireless to send and answer to these requests, select the **Broadcast SSID and respond to SSID queries** check box. For security, turn this option on only when you are configuring your network to connect to the Firebox X Edge. Then, disable this option after all your clients have been configured.

To control access to the Firebox X Edge Wireless by computer hardware (MAC) address:

- 1 Select the **Restrict Access by Hardware Address** check box.
- 2 Click **Edit**.
- 3 Type the MAC addresses of the computers that are allowed to connect to the Firebox X Edge Wireless in the correct field.
To find the MAC address of your wireless card, open a command prompt on your computer and type "ipconfig /all".
- 4 Click **Add** and then **Submit**.

Logging authentication events

An authentication event occurs when a wireless computer tries to connect to the Firebox X Edge Wireless. To have the Firebox X Edge Wireless record authentication events in the log file, select the **Log Authentication Events** check box.

To change the fragmentation threshold, type a value in the **Fragmentation Threshold** field. The values are 256 through 2346.

Configuring the wireless mode

Most wireless cards can operate only in 802.11b (11 MB/second) or 802.11g (54 MB/second) mode. The Firebox X Edge only operates in 802.11g mode if all the wireless cards connected to the Edge are using 802.11g mode. If any 802.11b clients connect to the Edge, all clients drop down to the 802.11b mode. To set the operating mode for the Firebox X Edge, select an option from the **Wireless Mode** drop-down list. There are three wireless modes from which to select:

802.11g only

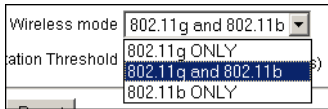
This is the default mode, which allows you to deny access to 802.11b clients so that you can keep the Edge operating in the faster 802.11g mode.

802.11g and 802.11b

This mode allows Firebox X Edge Wireless to connect with wireless devices using the two wireless protocols

802.11b only

This mode allows the Firebox X Edge Wireless to connect to devices using only this wireless protocol.



NOTE

Using 802.11b and 802.11g allows access to all clients with these protocols activated. When 802.11b clients connect to the Firebox X Edge Wireless, then all clients connect at the 802.11b speed of 11Mb.

For more information on the fragmentation threshold parameter, see this FAQ:

www.watchguard.com/support/advancedfaqs/edge_fragthreshold.asp

Configuring Firewall Settings

The Firebox® X Edge uses services and other firewall options to control the traffic between the trusted, optional, and external networks. The configuration of allowed services and firewall options set the level of security the Firebox applies to your network.

About Services

A Firebox® service is one or more rules that together monitor and control traffic. These rules set the firewall actions for a service:

- **Allow** lets data or a connection through the Firebox.
- **Deny** stops data or a connection from going through the Firebox, and sends a response to the source.
- **No Rule** sets a rule to off, as if the rule was not defined. This option is available to allow you to manage only the incoming or only the outgoing properties of a service.

For example, to operate a Web server behind the Firebox X Edge, configure the HTTP service to let incoming traffic flow to the IP address of the Web server (the internal computer that receives the requests for Web pages).

Incoming and outgoing traffic

Traffic that does not start in your trusted or optional network is incoming traffic. Traffic that starts in your trusted or optional network and goes to the external network is outgoing traffic. In the default configuration, the Firebox stops all traffic from getting to your trusted network.

The default configuration of the Firebox X Edge allows this traffic:

- From the trusted network to the external network
- From the trusted network to the optional network
- From the optional network to the external network

The default configuration of the Firebox denies this traffic:

- From the external network to the trusted network
- From the optional network to the trusted network
- From the external network to the optional network

Traffic through VPN tunnels

When you create Mobile User VPN tunnels from remote users, or when you create Branch Office VPN tunnels to other offices, the Firebox X Edge allows all traffic through the VPN tunnel. No other configuration is necessary after the VPN tunnel is set up. Do not configure services as shown in this chapter to allow or deny traffic across a VPN tunnel. All traffic is allowed between the IPSec VPN peer networks.

About This Chapter

“Configuring Incoming Services” shows you how to control traffic from the external network to the trusted and optional networks.

The section “Configuring Outgoing Services” on page 95 shows you how to control traffic to the external network from the trusted and optional networks.

The section “Services for the Optional Network” on page 101 shows how you can control traffic between the trusted and optional networks. This is traffic that goes from the trusted network to the optional network, or traffic that goes from the optional network to

the trusted network. This section also has examples of how to use the optional network.

Other sections show how to use the Blocked Sites feature and other firewall options:

- Responding to pings
- Creating log messages for all outgoing traffic
- FTP access to the Firebox
- SOCKS
- Changing the Firebox's hardware MAC address

Configuring Incoming Services

You can control the traffic that goes to the trusted or optional networks from the external network using incoming services. Usually, the Internet is the external network.

The Firebox® X Edge supplies a list of frequently used services you can use to easily allow the most used traffic categories into your trusted or optional network. You can also create custom services if you must allow traffic that is not in the list of frequently used services.

You must be careful when you allow incoming services. When you allow an incoming service, you open the protected networks behind the Edge to more traffic, which increases risk. Make sure that you compare the value of added access to the security risk.

NOTE

You can set the incoming services in this section to allow traffic that starts on the external network to flow to a computer on the trusted network or to a computer on the optional network. These services do not affect traffic between the trusted and optional networks.

Configuring common services for incoming traffic

The Firebox X Edge includes standard services known as common services that you can use to control traffic through the Firebox. You can use the procedure below to configure the properties of a common service.

For more information on the common services, refer to the list at the end of this FAQ:

www.watchguard.com/support/Tutorials/stepsoho_blockoutservice.asp

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 2 From the navigation bar, select **Firewall > Incoming**.
The Filter Incoming Traffic page appears.

Firewall

Filter Incoming Traffic

Warning:

- Firebox X Edge FTP service is exposed to the External Network by service: "FTP"
- Firebox X Edge HTTP service is exposed to the External Network by service: "HTTPS"

Common Services

Filter	Service	Service Host
No Rule	DNS	0.0.0.0
Allow	FTP	192.168.161.1
No Rule	HTTP	0.0.0.0
Allow	HTTPS	192.168.161.1
No Rule	ILS	0.0.0.0
No Rule	IPSec	0.0.0.0
No Rule	NetMeeting	0.0.0.0
No Rule	NNTP	0.0.0.0
No Rule	Ping	0.0.0.0
No Rule	POP3	0.0.0.0

- 3 Find the name of the common service to allow into your trusted or optional network from the external network. From the **Filter**

drop-down list adjacent to the service name, select **Allow** or **Deny**.

In its default configuration, the Firebox does not allow incoming traffic to your network. Because of this, you can keep a service's filter rule set to No Rule and the traffic is denied.

- 4 If you use **Allow** for a service, enter the IP address of the service host.

The service host is the computer on the trusted or optional network that receives the traffic.

- 5 Click **Submit**.

- 6 Repeat to allow or deny more common services.

NOTE

If you set a common service to Allow, the Edge allows traffic that uses that service from any source on the external network. The Firebox only allows traffic to go to the service host.

To put a limit on the external sources that can use the ports and protocols of the service you are adding, you must create a custom service.

About custom services for incoming traffic

A custom service for incoming traffic is necessary if:

- Incoming traffic does not use the same ports or protocols used by one of the common services.
- You restrict the IP addresses on the external network that can use a service to connect to a computer behind the Firebox X Edge.

You can add a custom service using one or more of these:

- TCP ports
- UDP ports
- An IP protocol that is not TCP or UDP. You identify an IP protocol that is not TCP or UDP with the IP protocol number.

Adding a custom service using the wizard

- 1 From the navigation bar, click **Wizards**.
- 2 Adjacent to **Define a custom service...** click **Go**.
- 3 Use the instructions in the wizard to add a custom service.

The Traffic Filter Wizard includes these steps:

Welcome

The first screen tells you about the wizard and the information you must have to complete the wizard.

Service Name

On this screen, type a name to identify the service.

Protocols and Ports

Set the protocol and ports to assign to this traffic rule.

Traffic Direction

Identify if this is an incoming or outgoing service.

Service action

Configures the Firebox to allow or deny this type of service traffic through the firewall.

Restrict to remote computers

To put a limit on the scope of the service, add the IP addresses of the computers or networks outside the firewall to which this service applies.


Restrict to local computers

To put a limit on the scope of the service, add the IP addresses of the computers or networks inside the firewall to which this service applies.

Adding a custom incoming service manually

You can add a custom service without using the wizard.

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 2 From the navigation bar, select **Firewall > Incoming**.
- 3 Scroll to the bottom of the page.

Custom Services				
Filter	Service	Service Host		
Deny	 myservice	0.0.0.0	Edit	Delete
Add Service...				

- 4 Below **Custom Services**, click **Add Service**.
The Custom Service page appears.

Firewall
Custom Service

Service Name

Protocol Settings

Protocol	Port
udp	234-3456

To

Incoming Filter

Service Host

From

Outgoing Filter

- 5 In the **Service Name** text box, type the name for your service.
- 6 From the **Protocol** drop-down list, click **TCP Port**, **UDP Port**, or **Protocol**.
- 7 In the text box adjacent to the **Protocol** drop-down list, type a port number or protocol number. To use a range of ports, type a port number in the second text box.

NOTE

An IP protocol number is not the same as a TCP or UDP port number. TCP is IP protocol number 6 and UDP is IP protocol number 17. If you use an IP protocol that is not TCP or UDP, you must enter the IP protocol number. IP protocols include: IP protocol number 47 for Generic Routing Encapsulation (GRE) or IP protocol number 50 for Encapsulated Security Payload (ESP). IP protocols that are not TCP or UDP are unusual.

8 Click **Add**.

Repeat the last three steps until you have a list of all the ports and protocols that this service uses.

You can have more than one port and more than one protocol in a custom service.

More ports and protocols make the service more dangerous. Restrict the service to only the ports and protocols that are necessary.

Filtering traffic for incoming services

These steps restrict incoming traffic for a service to specified computers behind the firewall. Refer to “About custom services for outgoing traffic” on page 97 for information on controlling outgoing traffic.

1 From the **Incoming Filter** drop-down list, select **Allow** or **Deny**.

2 If you set the Incoming Filter to **Allow**, you must type in the IP address of the service host. This is the computer that receives the traffic.

3 To allow external computers to send incoming traffic to the service host using this service, skip the subsequent instructions and click **Submit** at the bottom of the page.

4 To put a limit on the number of computers that can send traffic to the service host using this service, use the drop-down list to select **Host IP Address**, **Network IP Address**, or **Host Range**.

Type Network IP addresses in “slash” notation (also known as Classless Inter Domain Routing or CIDR notation). For more information on entering IP addresses in slash notation, see this FAQ: http://www.watchguard.com/support/advancedfaqs/general_slash.asp.

5 In the address text boxes, type the host or network IP address, or type the range of IP addresses that identify the computers on the external network that can use this service to send traffic to the service host.

6 Click **Add**. The **From** box shows the host or network IP address you typed.

Repeat the last three steps until all of the address information for this custom service is set. The From box can have more than one entry.

7 If this service is only for incoming traffic, keep the outgoing filter set to **No Rule**. If this service is for outgoing traffic, see the next section, “Configuring Outgoing Services.”

8 Click **Submit**.

Configuring Outgoing Services

You control traffic that starts in the trusted or optional network and goes to the external network using outgoing services. Usually, the Internet is the external network.

In its default configuration, the Firebox® X Edge allows traffic that starts in the trusted or optional network to go to the external network.

Many companies and organizations allow internal computers to use all ports and protocols. To deny all outgoing connections, use this section to make rules for those connections.

NOTE

The outgoing services in this section can be set to allow traffic that starts in the trusted and optional networks to flow to the external network. These services do not affect traffic between the trusted and optional networks. These services also do not affect traffic from computers on the trusted network to other computers on the trusted network.

To see the outgoing traffic rules:

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`

- From the navigation bar, select **Firewall > Outgoing**.
The Filter Outgoing Traffic page appears.

Firewall

Filter Outgoing Traffic

Common Services

Filter	Service
No Rule	DNS
No Rule	FTP
No Rule	HTTP
No Rule	HTTPS
No Rule	ILS
No Rule	IPSec
No Rule	NetMeeting
No Rule	NNTP
No Rule	Ping
No Rule	POP3
No Rule	PPTP
No Rule	SMB
No Rule	SMTP
No Rule	SNMP

Configuring common services for outgoing traffic

In its default configuration, the Firebox allows all traffic to go out to the external network. This is because the common service called Outgoing is set to **Allow**. (The Outgoing service is not found on the **Firewall > Incoming** page.)

You can set the Outgoing service filter to **No Rule**. When you set the Outgoing service to **No Rule**, no traffic can get to the external network unless a different service on the **Firewall > Outgoing** page is set to **Allow**.

You can set other common services to **Allow**. Then you can allow only specified traffic from the trusted and optional networks to get to the external network.

- To allow all traffic from the trusted and optional networks to get to the external network, keep the Outgoing service set to **Allow**.

- To allow only specified traffic from the trusted and optional network to get to the external network:
 - Set the common service Outgoing to **No Rule**.
 - Select the common services to allow outgoing and set these services to **Allow**.

NOTE

If you set a common service on the Filter Outgoing Traffic page to Allow, the Firebox allows traffic that uses that service to get to the external network from computers on the trusted or optional network.

To put limits on the computers on the trusted and optional network that send traffic through the ports and protocols a service uses, you must use a custom service.

About custom services for outgoing traffic

A custom service for outgoing traffic is necessary if:

- You must allow outgoing traffic for a service that is not on the common service list.
- You must restrict the IP addresses on the trusted or optional network that can use a service.

You can add a custom service using one or more of these:

- TCP ports.
- UDP ports.
- An IP protocol that is not TCP or UDP. You identify an IP protocol that is not TCP or UDP with the IP protocol number.

Adding a custom service using the wizard

- 1 From the navigation bar, click **Wizards**.
- 2 Next to **Define a custom service...** click **Go**.
- 3 Obey the on-screen instructions.

The Traffic Filter Wizard includes these steps:

Welcome

The first screen tells you about the wizard and the information you must have to complete the wizard.

Service Name

On this screen, type a name to identify the service.

Protocols and Ports

Set the protocol and ports to assign to this traffic rule.

Traffic Direction

Identify if this is an incoming or outgoing service.

Service action

Configures the Firebox to allow or deny this type of service traffic through the firewall.

Restrict to remote computers

To put a limit on the scope of the service, add the IP addresses of the computers or networks outside the firewall to which this service applies.


Restrict to local computers

To put a limit on the scope of the service, add the IP addresses of the computers or networks inside the firewall to which this service applies.

Adding a custom outgoing service manually

You can add a custom service without using the wizard:

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 2 From the navigation bar, select **Firewall > Incoming**.
- 3 Scroll to the bottom of the page.

Custom Services		
Filter	Service	Service Host
Deny	 myservice	0.0.0.0

- 4 Below **Custom Services**, click **Add Service**.
The Custom Service page appears.

Firewall
Custom Service

Service Name

Protocol Settings

Protocol	Port
udp	234-3456

To

Incoming Filter

Service Host

From

Outgoing Filter

- 5 In the **Service Name** text box, type the name for your service.
- 6 From the **Protocol** drop-down list, click **TCP Port**, **UDP Port**, or **Protocol**.
- 7 In the text box next to the **Protocol** drop-down list, type a port number or protocol number. To use a range of ports, type a port number in the second text box.

NOTE

An IP protocol number is not the same as a TCP or UDP port number. TCP is IP protocol number 6 and UDP is IP protocol number 17. If you use an IP protocol that is not TCP or UDP, you must enter the IP protocol number. IP protocols you might use include: IP protocol number 47 for Generic Routing Encapsulation (GRE) or IP protocol number 50 for Encapsulated Security Payload (ESP). IP protocols that are not TCP or UCP are unusual.

- 8 Click **Add**.

- 9 Repeat the last three steps until you have a list of all the ports and protocols that this service uses.

You can have more than one port and more than one protocol in a custom service.

More ports and protocols make the service more dangerous. Limit the service to only the ports and protocols that are necessary.

Filtering a service for outgoing traffic

These steps restrict outgoing traffic through the Firebox. Refer to “Filtering traffic for incoming services” on page 94 for information on filtering incoming traffic.

- 1 From the **Outgoing Filter** drop-down list, select **Allow** or **Deny**.
- 2 To allow any computers on the trusted or optional network to send traffic to any location on the external network using this service, skip the subsequent instructions and click **Submit** at the bottom of the page.
- 3 To put a limit on the computers on the trusted or optional network that can send traffic to the external network using this service, use the drop-down list below the **From** box to select **Host IP Address, Network IP Address, or Host Range**.
Network IP addresses must be entered in “slash” notation (also known as Classless Inter Domain Routing or CIDR notation). For more information on entering IP addresses in slash notation, see this FAQ: http://www.watchguard.com/support/advancedfaqs/general_slash.asp.
- 4 In the address text boxes, type the host or network IP address, or type the range of IP addresses that identify the computers on the trusted or optional network that can use this service to send traffic to the external network.
- 5 Click **Add**. The **From** box shows the IP addresses you added.
Repeat the last three steps until all of the From address information for this custom service is set. The From box can have more than one entry.
- 6 To put a limit on the computers on the external network that can be connected to using this service, use the drop-down list below the **To** box to select **Host IP Address, Network IP Address, or Host Range**.
- 7 In the address text boxes, type the host or network IP address, or type the range of IP addresses that identify the computers on the external network that internal computers can connect to using this service.

- 8 Click **Add**. The **To** box shows the IP addresses you added.
Repeat the last three steps until all of the address information for this custom service is set. The **To** box can have more than one entry.
- 9 If this service is only for outgoing traffic, keep the Incoming Filter set to **No Rule**. If this service is for incoming traffic, see the section “Configuring Incoming Services” on page 89.
- 10 Click **Submit**.

Services for the Optional Network

The default configuration of the Firebox® X Edge allows all traffic that starts in the trusted network to go to the optional network.

The default configuration of the Firebox denies all traffic that starts in the optional network and tries to go to the trusted network.

Here are some examples of how you can use the optional network:

- You can use the optional network for servers that the external network can get to. This helps to protect the trusted network, because no traffic is allowed to the trusted network from the optional network when the Firebox is in default configuration. When computers are accessible from the external network, they are more vulnerable to attack. If your public Web or FTP server on the optional network is hacked or compromised, the attacker cannot get to your trusted network.
- You can use the optional network to secure a wireless network. Wireless networks are usually less secure than wired networks. If you have a Wireless Access Point you can increase the security of your trusted network by keeping the Wireless Access Point on the optional network.
- You can use the optional network to have a different network IP address range that is allowed to communicate with the trusted network. See the section “Disabling Traffic Filters,” below.

Controlling traffic from the trusted to optional network

You can restrict the traffic that starts in the trusted network and goes to the optional network:

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 2 From the navigation bar, click **Firewall > Optional**.
The Filter Outgoing Traffic to Optional Network page appears.
Use the instructions below to allow all traffic, to deny some traffic but allow all other traffic, or to allow only some traffic:
- 3 To allow any traffic to go from the trusted network to the optional network, keep the Outgoing service set to **Allow**.
- 4 From the **Filter** drop-down list, select **Allow** for the Outgoing service.
- 5 To deny some traffic from the trusted network when it tries to go to the optional network, but allow all other traffic from the trusted network to the optional network, select **Deny** for that traffic's service and keep the Outgoing service set to **Allow**.
- 6 To allow some traffic from the trusted network to the optional network, set the Outgoing service to **No Rule** and set the services to **Allow**.
- 7 Click **Submit**.

Disabling traffic filters

To allow traffic to flow from the optional network to the trusted network, you allow all traffic between the trusted and optional networks.

Select the **Disable traffic filters** check box to allow all incoming and outgoing traffic between the trusted and optional interfaces.








NOTE

When you select the Disable traffic filters check box, the trusted network is not protected from the optional network. All traffic can flow between optional and trusted network.

Firewall
Filter Outgoing Traffic to Optional Network

☐ Disable traffic filters

*Disabling traffic filters will **allow all traffic** in both directions between the Trusted Network and the Optional Network.*

Filter	Service	
No Rule ▾		DNS
No Rule ▾		FTP
No Rule ▾		HTTP
No Rule ▾		HTTPS
No Rule ▾		POP3
No Rule ▾		SMTP
Allow ▾		Outgoing

Blocking External Sites

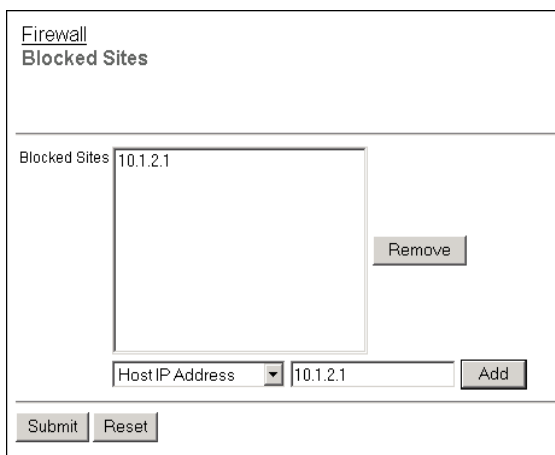
The Blocked Sites feature helps prevent traffic from hostile sites from getting through the Firebox. When you identify a hacker, you can stop all connections that hacker tries to make. When hackers try to connect to your network, the Firebox® X Edge records data about the hacker. You can examine the data to identify attacks.

A blocked site is an external IP address that is blocked from connecting to computers behind the Edge regardless of configured services.

To add a location to the Blocked Sites list:

- 1 From the navigation bar, click **Firewall > Blocked Sites**.

The Blocked Sites page appears.



The screenshot shows the 'Firewall Blocked Sites' configuration page. At the top, there's a header with 'Firewall' and 'Blocked Sites'. Below this is a section titled 'Blocked Sites' containing a list box with the IP address '10.1.2.1'. To the right of the list box is a 'Remove' button. Below the list box is a form with a dropdown menu labeled 'Host IP Address' (currently showing a small downward arrow), a text input field containing '10.1.2.1', and an 'Add' button. At the bottom of the form are 'Submit' and 'Reset' buttons.

- 2 From the drop-down list, click **Host IP Address, Network IP Address, or Host Range**.
- 3 In the text box, type a host IP address, a network IP address, or a range of host IP addresses.
- 4 Click **Add**.
The IP address information appears in the Blocked Sites list.
- 5 Click **Submit**.

Configuring Firewall Options

You can use the Firewall Options page to configure rules that increase your network security with methods other than service rules.

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.

The default URL is: `https://192.168.111.1`

- 2 From the navigation bar, click **Firewall > Options**.

The Firewall Options page appears.

Firewall
Firewall Options

☐ Do not respond to PING requests received on External Network.

☐ Do not respond to PING requests received on Trusted Network.

☐ Do not allow FTP access to Trusted Network interface.

☐ Disable SOCKS proxy.

☐ Log All Allowed Outbound Access.

☐ Enable override MAC address for the External Network.

External Network override MAC address

☐ Enable override MAC address for the Failover Network.

Failover Network override MAC address

Responding to ping requests

You can configure the Firebox X Edge to deny pings. This setting has higher precedence than any configured service.

- 1 Select the **Do not respond to PING requests received on External Network** check box or the **Do not respond to PING requests received on Trusted Network** check box.
- 2 Click **Submit**.

Denying FTP access to the trusted network interface

You can configure the Firebox X Edge to stop FTP traffic from the trusted interface or external interface. This setting has higher precedence than any configured service.

- 1 Select the **Do not allow FTP access to Trusted Network** check box.
- 2 Click **Submit**.

NOTE

You must clear the Do not allow FTP access to Trusted Network check box when you apply an update to the Edge firmware with the automatic installer. If you do not clear this option, the Software Update Installer cannot move firmware files to the Firebox X Edge. For information on updates for Edge firmware, see "Updating the Firmware" on page 199.

SOCKS implementation for the Firebox X Edge

The Firebox X Edge can operate as a SOCKS network proxy server. Software that uses more than one socket connection and uses the SOCKS version 5 protocol can send traffic through the Edge. SOCKS gives you secure, two-way communication between a computer on the external network and a computer on the trusted network. To use a SOCKS-compatible program, configure the program with the necessary information about the Firebox X Edge.

The Firebox X Edge uses SOCKS version 5. Firebox X Edge users do not authenticate before using the Edge configuration pages.

Your Firebox X Edge does not connect with software that finds only DNS (domain name server) names. Configure the SOCKS-compatible software to connect to IP addresses and not connect to domain names.

Software that uses SOCKS and can operate with Firebox X Edge includes ICQ, IRC, and AOL Messenger.

NOTE

If software that uses SOCKS operates on a computer put on the trusted network, then all users on the trusted network can use the SOCKS proxy. To stop this risk, disable the SOCKS proxy on your Firebox X Edge.

Configuring your SOCKS application

Configure the software using SOCKS on trusted network computers to connect to a computer on the external network. When you configure the software, use the recommended properties from that software documentation.

NOTE

The Firebox X Edge uses port 1080 to speak to computers with software using SOCKS. Make sure that port 1080 is open and not used by other software on the computer.

- 1 If you can identify a version, select SOCKS version 5.
- 2 Select port 1080.
- 3 Set the SOCKS proxy to the URL (uniform resource locator) or IP address of the Firebox X Edge. The default IP address is:
192.168.111.1.

Disabling SOCKS on the Edge

When the software using SOCKS stops, port 1080 stays open. To stop this security risk, close the port.

- 1 On the Firewall Options page, select the **Disable SOCKS proxy** check box.
The SOCKS Proxy is disabled.
- 2 Click **Submit**.

To use the SOCKS-compatible application:

- 1 Clear the **Disable SOCKS proxy** check box.
The SOCKS proxy is enabled.
- 2 Click **Submit**.

Logging all allowed outgoing traffic

If you use the standard property settings, the Firebox X Edge records only unusual events. When traffic is denied, the Edge records the information in the log file. You can configure the Edge to record information about all the outgoing traffic in the log file.

NOTE

Recording all outgoing traffic creates a large number of log records. We recommend that you record all the outgoing traffic only as a problem-solving tool, unless you send log messages to a remote Log Server.

To record all outgoing traffic:

- 1 Select the **Log All Allowed Outbound Access** check box.
- 2 Click **Submit**.

Changing the MAC address of the external interface

Some ISPs use a MAC address to identify the computers on their network. Each MAC address gets one static IP address. If your ISP uses this method to identify your computer, then you must change the MAC address of the Firebox X Edge. Use the MAC address of the cable modem, DSL modem, or router that connected directly to the ISP in your original configuration. The MAC address must have these properties:

- The MAC address must use 12 hexadecimal characters. Hexadecimal characters have a value between 0 and 9 or between “a” and “f”.
- The MAC address must operate with:
 - One or more addresses on the external network
 - The MAC address of the trusted network for the Firebox X Edge
 - The MAC address of the optional network for the The Firebox X Edge
- You cannot set the MAC address to 000000000000
- You cannot set the MAC address to ffffffff

To change the MAC address of the external interface:

- 1 Select the **Enable override MAC address for the External Network** check box, or select the **Enable override MAC address for the Failover Network** check box.
You can select the check boxes together.
- 2 In the **External network override AC address** or **Failover network override AC address** text box, type the new MAC address for the Firebox X Edge external or failover network.
- 3 Click **Submit**.

NOTE

If the field marked MAC address for the external network is cleared and the Firebox X Edge is restarted, the Firebox X Edge uses the standard MAC address for the external network.

To decrease problems with MAC addresses, the Firebox X Edge makes sure that the MAC address you assign to the external interface is unique on your network. If the Edge finds a device using the same MAC address, the Firebox changes back to the standard MAC address for the external interface. Then it restarts.

Configuring Logging and System Time

A log file is a list of all the events that occur on the Firebox® X Edge. An event is one activity, such as when the Firebox denies a packet. A log file records and saves information about these events.

An event log message is an important part of a network security policy. A sequence of denied packets can show a pattern of suspicious network activity. Log records can help you identify possible security problems.

NOTE

The Firebox X Edge log is cleared if the power supply is disconnected or the Edge is restarted. The information is not cleared if an external Syslog or Log Server is configured.

Viewing Log Messages

The Firebox® X Edge keeps a maximum of 150 log messages. New information shows at the top of the file. When new information enters a full log file, it erases the log message at the bottom of the file.

Each log message contains this information:

Time

The time of the event that created the log message.

Category

The type of message. For example, if the message came from an IP address or from a configuration file.

Message

The text of the message.

This procedure shows how to see the event log file:

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 2 From the navigation bar, click **Logging**.
The Logging page appears with the Event Log at the bottom of the page.

Event Log		
Time	Category	Message
2004-07-01-02:25:53	MONITOR	Administrator access allowed from 10.168.3.90
2004-07-01-02:25:52	IP	allowed from 10.168.3.90 port 3382 to 192.168.54.54 port 443 TCP SYN (HTTPS)
2004-07-01-02:25:17	MONITOR	Timeout opening connection to log server
2004-07-01-02:25:08	IP	discard from 192.168.54.57 to to 192.168.54.54 ICMP type (3) code (3)(SIP discarded)

Log to a WatchGuard Log Server

The WatchGuard® Log Server (previously known as the WatchGuard System Event Processor or WSEP) is a component of the WatchGuard System Manager. If you have a Firebox® III, Firebox X Core, or Firebox X Peak, configure the Log Server to collect the log messages from your Firebox X Edge. For instructions on how to configure the Log Server to accept the log messages, see the WatchGuard System Manager User Guide. Then use these instructions to send your event logs to the Log Server.

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`

- 2 From the navigation bar, click **Logging > WSEP Logging**.
The WatchGuard Security Event Processor Logging page appears.

The screenshot shows the 'Logging' configuration page for WatchGuard Security Event Processor Logging. At the top, there is a link 'Logging' and the title 'WatchGuard Security Event Processor Logging'. Below this, there is a section with a checked checkbox labeled 'Enable WatchGuard Security Event Processor Logging'. Underneath the checkbox are four input fields: 'Log Host IP Address' with the value '192.168.54.57', 'Log Encryption Key' with masked characters '••••••', 'Confirm Key' with masked characters '••••••', and 'Device Name' with the value 'PT&P'. At the bottom of the form are two buttons: 'Submit' and 'Reset'.

- 3 The **Enable WatchGuard Security Event Processor Logging** check box must contain a check mark. If it does not, click it.
- 4 In the **Log Host IP Address** field, type the IP address of the Log Server.
- 5 Type a passphrase in the **Log Encryption Key** field and confirm the passphrase in the **Confirm Key** field.
- 6 In the **Device Name** field, type a name for the Firebox X Edge.
This name lets the Log Server know which log messages come from which device. If this field is clear, the Firebox X Edge is identified to the Log Server by the IP address of the Firebox external interface.
- 7 Click **Submit**.

NOTE

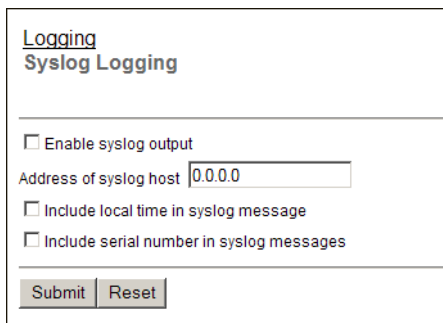
Use the same log encryption key that the Log Server uses.

Logging to a Syslog Host

Syslog is a log interface developed for UNIX but also used by a number of computer systems. This option sends the Firebox® X Edge log messages to a Syslog host. If you use a Syslog host, you can set the Edge to send log messages to that host.

Configure a Syslog host:

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 2 From the navigation bar, click **Logging > Syslog Logging**.
The Syslog Logging page appears.



Logging
Syslog Logging

☐ Enable syslog output

Address of syslog host

☐ Include local time in syslog message

☐ Include serial number in syslog messages

- 3 Select the **Enable Syslog output** check box.
- 4 Adjacent to **Address of Syslog host**, type the IP address of the SysLog host.
- 5 (Optional) Select the **Include local time in syslog message** check box to include the local time in the Syslog messages.
- 6 (Optional) Select the **Include serial number in syslog messages** check box to include the Firebox X Edge serial number in log messages sent to the syslog host.
This can be useful if you have more than one Edge sending syslog messages to the same syslog host.
- 7 Click **Submit**.

NOTE

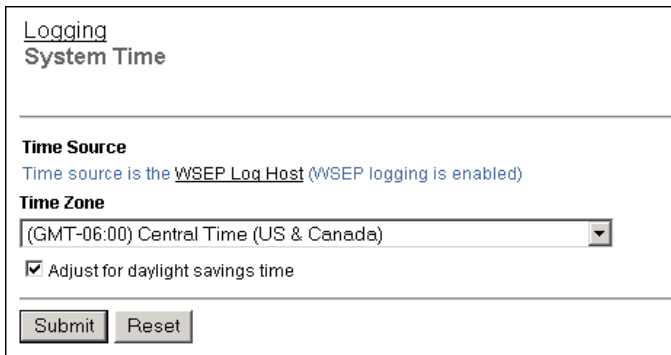
Because Syslog traffic is not encrypted, Syslog messages that are sent through the Internet decrease the security of the trusted network. Use a VPN tunnel to increase the security of Syslog message traffic. If the Syslog messages go through a VPN tunnel, IPSec technology encrypts the data.

Setting the System Time

For each log message, the Firebox® X Edge records the time from its system clock. The Edge uses the NTP protocol to automatically get the correct time.

To manually set the system time:

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 2 From the navigation bar, click **Logging > System Time**.
The System Time page appears.



The screenshot shows the 'System Time' configuration page. At the top, there is a navigation bar with 'Logging' and 'System Time'. Below this, the 'Time Source' section indicates that the time source is the 'WSEP Log Host' and that 'WSEP logging is enabled'. The 'Time Zone' section features a drop-down menu currently set to '(GMT-06:00) Central Time (US & Canada)'. Below the drop-down is a checkbox labeled 'Adjust for daylight savings time', which is checked. At the bottom of the form are two buttons: 'Submit' and 'Reset'.

- 3 Select the time zone from the drop-down list.
- 4 (Optional) Select **Adjust for daylight savings time**.
- 5 Click **Submit**.

Configuring WebBlocker

WebBlocker is an option for the Firebox X Edge that gives you control of the Web sites that are available to your users. Some companies restrict access to some Web sites to increase employee productivity. Other companies restrict access to Web sites that they believe are offensive.

NOTE

You must purchase the WebBlocker upgrade to use this feature. For information on how to activate upgrade options, see "Activating Upgrade Options" on page 201.

How WebBlocker Works

WebBlocker uses a database of Web site addresses controlled by SurfControl®, a Web filter company.

When a user on your network tries to connect to a Web site, the Firebox® X Edge sees if the WebBlocker database contains the Web site. If the Web site is not in the database or not blocked, the page opens. If WebBlocker stops the Web site from appearing, a notification appears.

Configuring Global WebBlocker Settings

The first WebBlocker page in the Firebox® X Edge Web pages is the WebBlocker Settings page. Use this page to:

- Activate WebBlocker
- Set the full access password
- Set the inactivity timeout
- Make sure that your Web users authenticate
- Add a custom message for users to see when WebBlocker denies access to a Web site

To configure WebBlocker:

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 2 From the navigation bar, select **WebBlocker > Settings**.
The WebBlocker Settings page appears.

WebBlocker
Settings

☐ Enable WebBlocker

Full Access Password

Confirm Password

Inactivity Timeout (minutes)

☐ Require Web users to authenticate

Message for blocked user field:

- 3 Select the **Enable WebBlocker** check box.
- 4 Type a password in the **Full Access Password** field.
The full access password gives access to all Web sites until the password expiration or until the browser is closed.
- 5 Type the same password again in the **Confirm Password** field.
- 6 Type a number, in minutes, in the **Inactivity Timeout** field.
The Inactivity Timeout shows the length of time the Full Access Password is active if no Web browsing is done. If a user types the Full Access Password and no HTTP traffic is done from that user's computer for the length of time set in the Inactivity Timeout, WebBlocker rules start again.

- 7 To make users authenticate for WebBlocker, select **Require Web users to authenticate**.

If you use one global WebBlocker setting for all users, it is not necessary to select this option. Use this option if you apply different WebBlocker profiles to different groups of users.

- 8 Add a custom message for users to see when they try to access a Web page that is blocked by WebBlocker. This message will appear with the usual WebBlocker message.

The message cannot contain HTML tags, the less than (<) or greater than (>) symbol, and cannot be more than 1000 characters in length.

For example, you can enter a message "This Web site does not comply with our Internal Use Policy." If a user tries to access a Web site that is blocked by WebBlocker, the user's browser will show:

```
Request for URL http://www.some-denied-
site.com/denied by WebBlocker: blocked for
Full Nudity, Sex Acts, Gross Depictions.
This Web site does not comply with our
Internal Use Policy.
```

- 9 Click **Submit**.

Creating WebBlocker Profiles

A WebBlocker profile is a set of restrictions you apply to groups of users on your network. You can create different profiles, with different groups of restrictions. For example, you can create a profile for new employees, with more restrictions than for other employees. It is not necessary to create WebBlocker profiles if you use one set of WebBlocker rules for all of your users.

After you create profiles, you can apply them when you set up Firebox User accounts. This procedure appears in Chapter 11, “Managing the Firebox X Edge and User Accounts.”

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 2 From the navigation bar, click **WebBlocker > Profiles**.
The Profiles page appears.
- 3 Click **New**.
The New Profile page appears.

WebBlocker
Profiles

Profile TestProfile Delete New

Blocked Categories

<input type="checkbox"/> Alcohol and Tobacco	<input type="checkbox"/> Violence/Profanity
<input checked="" type="checkbox"/> Illegal Gambling	<input type="checkbox"/> Search Engines
<input type="checkbox"/> Militant/Extremist	<input type="checkbox"/> Sports and Leisure
<input type="checkbox"/> Drug Culture	<input type="checkbox"/> Sex Education
<input type="checkbox"/> Satanic/Cult	<input checked="" type="checkbox"/> Sex Acts
<input checked="" type="checkbox"/> Intolerance	<input checked="" type="checkbox"/> Full Nudity
<input type="checkbox"/> Gross Depictions	<input type="checkbox"/> Partial/Artistic Nudity

Submit Reset

- 4 In the **Profile Name** field, type a familiar name.
You use this name to identify the profile during configuration. For example, give the name "90day" to an employee at your company for less than 90 days.
- 5 In **Blocked Categories**, click the groups of Web sites to block.
For more information on categories, see the next section.
- 6 Click **Submit**.

To remove a profile, from the WebBlocker Profiles page, select the profile from the **Profile** drop-down list. Click **Delete**.

WebBlocker Categories

The WebBlocker database contains 14 categories.

A Web site is added to a category when the contents of the Web site meet the correct criteria. Web sites that give opinion or educational material about the subject matter of the category are not included. For example, the drugs/drug culture category denies sites that tell how to use marijuana. They do not deny sites with information about the historical use of marijuana.

The categories:

Alcohol/tobacco

Pictures or text that advocate the sale, consumption, or production of alcoholic beverages and tobacco products.

Illegal Gambling

Pictures or text advocating materials or activities that could be illegal in any or all jurisdictions. Some examples are illegal business schemes, chain letters, copyright infringement, computer hacking, phreaking (using phone lines without permission), and piracy. Also includes text advocating gambling relating to lotteries, casinos, betting, numbers games, online sports, or financial betting, including non-monetary dares.

Militant/extremist

Pictures or text advocating extremely aggressive or combative behavior or advocacy of unlawful political measures. Topic includes groups that advocate violence. It also includes pages about how to make weapons.

Drug Culture

Pictures or text advocating the illegal use of drugs for entertainment. This category includes substances that are used for other than their primary purpose to alter the individual's state of mind. This does not include currently illegal drugs legally prescribed for medicinal purposes (such as drugs used to treat glaucoma or cancer).

Satanic/cult

Pictures or text advocating devil worship, an affinity for evil, wickedness, or the advocacy to join a cult. A cult is a closed society that is headed by an individual, loyalty is demanded, and leaving is forbidden.

Intolerance

Pictures or text advocating prejudice or discrimination against any race, color, national origin, religion, disability or handicap, gender, or sexual orientation. Any picture or text that elevates one group over another. Also includes intolerant jokes or slurs.

Gross Depictions

Pictures or text describing anyone or anything that is either crudely vulgar, grossly deficient in civility or behavior, or shows scatological impropriety. Topic includes depictions of maiming, bloody figures, and indecent depiction of bodily functions.

Violence/profanity

Pictures or text exposing extreme cruelty or profanity. Cruelty is physical or emotional acts against any animal or person that are primarily intended to hurt or inflict pain. This includes obscene words, phrases, and profanity in audio, text, or pictures.

Search Engines

Search engine sites such as Google.

Sports and Leisure

Pictures or text describing sporting events, sports figures or other entertainment activities.

Sex Education

Pictures or text advocating the proper use of contraceptives. Topic includes sites devoted to the explanation and description of condoms, oral contraceptives, intrauterine appliances, and other types of contraceptives. It also includes discussion sites

devoted to conversations with partners about sexually transmitted diseases, pregnancy, and sexual boundaries. Not included in this category are commercial sites selling sexual paraphernalia (topics included under Sexual Acts).

Sexual Acts

Pictures or text exposing anyone or anything involved in explicit sexual acts and/or lewd and lascivious behavior. Topic includes masturbation, copulation, pedophilia, as well as intimacy involving nude or partially nude people in heterosexual, bisexual, lesbian, or homosexual encounters. It also includes phone sex advertisements, dating services, adult personals, and sites devoted to selling pornographic CD-ROMs and videos.

Full Nudity

Pictures exposing any or all portions of human genitalia. Topic does not include sites categorized as Partial/Artistic Nudity containing partial nudity of a wholesome nature. It does not include Web sites for publications such as National Geographic or Smithsonian magazine or sites hosted by museums such as the Guggenheim, the Louvre, or the Museum of Modern Art.

Partial/artistic Nudity

Pictures exposing the female breast or full exposure of either male or female buttocks except when exposing genitalia that is handled in the Full Nudity category. Topic does not include swimsuits, including thongs.

For information on how to see if a Web site is included in the Surf-Control database, and for more information on WebBlocker categories, see

https://www.watchguard.com/support/AdvancedFaq/web_main.asp

- How can I see a list of blocked sites?
- How do different sites map into WebBlocker's 14 categories?

Allowing Certain Sites to Bypass WebBlocker

WebBlocker can deny a Web site that is necessary for your work. You can override WebBlocker using the Allowed Sites feature.

For example, employees in your company frequently use Web sites that contain medical information. Some of these Web sites are forbidden by WebBlocker because they fall into the sex education category. To override WebBlocker, you add the Web site's IP address or its domain name to the Allowed Sites record.

NOTE

This WebBlocker feature is applicable only for Internet Web use. You cannot use WebBlocker to block your users from an internal Web server.

- 1 From the navigation bar, select **WebBlocker > Allowed Sites**. The WebBlocker Allowed Sites page appears.
- 2 From the drop-down list, select a host IP address, network IP address, host range or domain name.

The screenshot shows the 'WebBlocker Allowed Sites' interface. It features a title bar, a list of allowed sites with the entry '64.12.10.124', a 'Remove' button, a 'Host IP Address' dropdown, an input field with '64.12.10.124', an 'Add' button, and 'Submit' and 'Reset' buttons at the bottom.

- 3 Type the host, network IP address or domain name of the Web site to allow. If it is a range of IP addresses, type the start and end point of the range. Click **Add**.

The domain (or host) name is the part of a URL that ends with a high-level domain like .com, .net, .org, .biz, or .edu. To add a domain name, type the URL pattern without the leading "http://". For example, to allow access to the Playboy Web site, select to add a domain name and enter "www.playboy.com".

- 4 Do step 3 again for other Web sites. When you have no more Web sites to add, click **Submit**.

To remove an item from the list, click the address. Click **Remove**.

Blocking Additional Web Sites

You can block some Web sites that WebBlocker allows. For example, you can receive a LiveSecurity® Service alert that tells you that a frequently used Web site is dangerous. Use the Denied Sites feature to add the Web site's IP address or domain name to WebBlocker to make sure your employees do not look at this Web site.

- 1 From the navigation bar, select **WebBlocker > Denied Sites**. The WebBlocker Denied Sites page appears.
- 2 From the drop-down list, select a host IP address, network IP address, host range, or domain name.

WebBlocker
Denied Sites

Denied Sites 64.12.10.127

Remove

Host IP Address 64.12.10.127 Add

Submit Reset

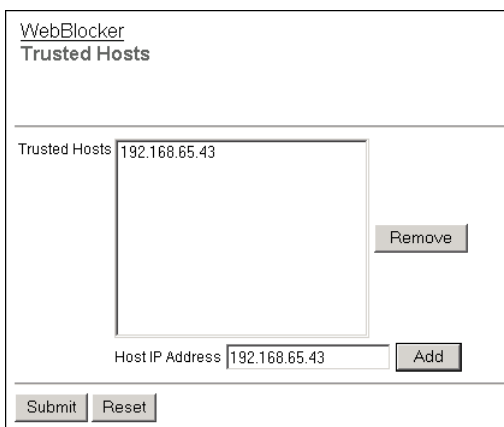
- 3 Type the host, network IP address, or domain name of the denied Web site. If it is a range of IP addresses, type the start and end point of the range. Click **Add**.
The domain (or host) name is the part of a URL that ends with a high-level domain like .com, .net, .org, .biz, or .edu. To block a domain name, type the URL pattern without the leading "http://". For example, to block access to the Playboy Web site, select to add a domain name and enter "www.playboy.com".
- 4 Do step 3 for other denied Web sites. When you have no more Web sites to add, click **Submit**.

To remove an item from the list, select the address. Click **Remove**.

Allowing Internal Hosts to Bypass WebBlocker

You can make a list of internal hosts that bypass WebBlocker settings:

- 1 From the navigation bar, select **WebBlocker > Trusted Hosts**. The WebBlocker Trusted Hosts page appears.



WebBlocker
Trusted Hosts

Trusted Hosts 192.168.65.43

Remove

Host IP Address 192.168.65.43 Add

Submit Reset

- 2 In the text box at the bottom of the page, type the host IP address of the computer on your trusted or optional network to allow to browse the Internet without WebBlocker restrictions. Click **Add**.
- 3 Do step 2 again for other allowed hosts. When you have no more hosts to add, click **Submit**.

To delete an item from the list, select the address. Click **Remove**.

Configuring Virtual Private Networks

You use a virtual private network (VPN) to create secure connections between computers or networks in different locations. The networks and hosts on a VPN tunnel can be corporate headquarters, branch offices, remote users, and telecommuters. When a VPN tunnel is created, the two tunnel endpoints are authenticated. Data in the tunnel is encrypted. Only the sender and the recipient of the message can read it.

About This Chapter

This chapter starts with a section that tells you the basic requirements for your Firebox® X Edge to create a VPN. Start with “What You Need to Create a VPN” on page 130.

The subsequent section tells you how to configure the Edge to be the endpoint of a VPN tunnel created and managed by a WatchGuard® Firebox X Core or Firebox X Peak. This procedure is different for different versions of the WatchGuard System Manager installed on the Firebox X.

Information about how to configure a Manual VPN to another VPN device is also included in this chapter. Use this section to create VPN tunnels to any other IPSec VPN endpoint.

The last part of this chapter includes Frequently Asked Questions and information on how to keep the VPN tunnel operating correctly and see VPN tunnel statistics. These last sections can help you troubleshoot the VPN tunnel.

For more information on VPN tunnels, see the Advanced FAQs:

<https://www.watchguard.com/support/advancedfaqs>

What You Need to Create a VPN

Before you configure your WatchGuard® Firebox® X Edge VPN network, read these VPN requirements:

- You must have two Firebox X Edge devices or one Firebox X Edge and a second device that uses IPSec standards. Examples of these devices are a Firebox III, Firebox X Core, Firebox X Peak, or a Firebox SOHO 6. You must enable the VPN option on the other device if it does not have the option.
- You must have an Internet connection.
- The ISP for each VPN device must let IPSec go across their networks.

Some ISPs do not let you create VPN tunnels on their networks unless you upgrade your Internet service to a level that supports VPN tunnels. Speak with the ISP to make sure they let you use these ports and protocols:

- UDP Port 500 (Internet Key Exchange or IKE)
- UDP Port 4500 (NAT traversal)
- IP Protocol 50 (Encapsulating Security Payload or ESP)
- If the other side of the VPN tunnel has a WatchGuard Firebox III or Firebox X, you can use the Managed VPN option. Managed VPN is easier to configure than Manual VPN. You must get information from the administrator of the Firebox on the other side of the VPN to use this option.
- You must know if the IP address assigned to your Edge's external interface is static or dynamic. To learn about IP addresses, see Chapter 2, "Installing the Firebox X Edge."
- Your Edge model tells you the number of VPN tunnels that you can create on your Edge. You can purchase a model upgrade for

your Edge to make more VPN tunnels, as described in “Enabling the Model Upgrade Option” on page 203.

- If you connect two Microsoft Windows NT networks, they must be in the same Microsoft Windows domain, or they must be trusted domains. This is a Microsoft Networking problem, and not a limit of the Firebox X Edge.
- If you want to use the DNS and WINS servers from the network on the other side of the VPN tunnel, you must know the IP addresses of these servers.

The Edge can give WINS and DNS IP addresses to the computers on its trusted network if those computers get their IP addresses from the Edge using DHCP. If you want to give the computers IP addresses of WINS and DNS servers on the other side of the VPN, you can type those addresses into the DHCP settings in the trusted network setup. For information on how to configure the Edge to give DHCP addresses, see “Using DHCP on the trusted network” on page 54.

- You must know the network address of the private (trusted) networks behind your Firebox X Edge and behind the other VPN device (the networks that will communicate through the VPN tunnel), and their subnet masks.

NOTE

The private IP addresses of the computers behind your Firebox X Edge cannot be the same as the IP addresses of the computers on the other side of the VPN tunnel. If your trusted network uses the same IP addresses as the office to which it will create a VPN tunnel, then your network or the other network must change their IP address arrangement to prevent IP address conflicts.

Managed VPN: With a Firebox III or Firebox X and WatchGuard System Manager 8.0

You can configure a VPN tunnel on the Firebox® X Edge with two procedures: Managed VPN and Manual VPN. This section tells you how to configure your Firebox X Edge for it to be an endpoint in a managed VPN tunnel. For information on creating a Manual VPN, see “Manual VPN: Setting Up Manual VPN Tunnels” on page 140. Dynamic VPN Configuration Protocol (DVCP) is the WatchGuard® protocol that you can use to create IPSec tunnels easily. The WatchGuard Management Server (previously known as the DVCP Server)

uses DVCP to keep the VPN tunnel configuration. You use the name Managed VPN because the Management Server manages the VPN tunnel and sends the VPN configuration to your Edge. This makes the Edge administrator's task easy because you must type only a small quantity of information into the Edge configuration pages. You must have WatchGuard System Manager and a Firebox III, Firebox X Core, or Firebox X Peak to have a Management Server. When your Firebox X Edge gets its VPN configuration from a Management Server, your Edge is a client of the Management Server in a client-server relationship. The Edge gets all of its VPN configuration from the Management Server.

Setting up a Firebox X Edge for managed VPN

You use a different procedure if your Firebox X Edge has a static external IP address than for an Edge with a dynamic external IP address.

Setting up managed VPN on an Edge with dynamic external IP address

If your Firebox X Edge has a dynamic IP address assigned to its external interface, use this procedure to configure it as an endpoint for managed VPN tunnels to a Firebox III or Firebox X and WatchGuard System Manager 8.0:

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`.
- 2 From the navigation bar, select **Administration > VPN Manager Access**
The VPN Manager Access page appears.

Administration
VPN Manager Access

☒ Enable VPN Manager Access

Status Passphrase

Confirm Status Passphrase

Configuration Passphrase

Confirm Configuration Passphrase

☒ Enable interoperability with VPN Manager v7.0, v7.1, and v7.2.

- 3 Select the **Enable VPN Manager Access** check box.
- 4 Type and confirm a status and configuration passphrase to be used to allow the Management Server to make read-only and read-write connections to your Firebox X Edge.
You must give these passphrases to the WatchGuard Management Server administrator. You do not use these passphrases for any other tasks.
- 5 Click the **Submit** button.
- 6 From the navigation bar select **VPN > Managed VPN**.
The Managed VPN page appears.

VPN
Managed VPN

☒ Enable Managed VPN

Configuration Mode

DVCP Server Address

Client Name

Shared Key

- 7 Select the **Enable Managed VPN** check box.
- 8 Type the IP address of the Management Server.
- 9 Type the **Client Name** to give your Firebox X Edge.
This is the name the Edge gives to the Management Server to use to identify the Edge.

10 Type the **Shared Key**.

This is the shared key used to encrypt the connection between the Management Server and the Firebox X Edge. This shared key must be the same on the Edge and the Management Server. You must get the shared key from your VPN administrator.

11 Click **Submit**.

Setting up the Edge for managed VPN on an Edge with static external IP address

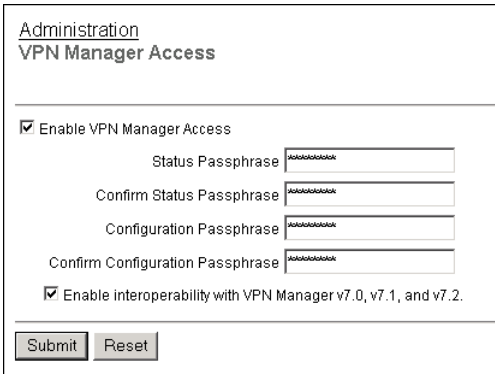
If your Firebox X Edge has a static IP address assigned to its external interface, use this procedure to configure it as an endpoint for managed VPN tunnels to a Firebox III or Firebox X and WatchGuard System Manager 8.0:

- 1 Connect to the Firebox X Edge System Status page. Type **https://** in the browser address bar, and the IP address of the Edge trusted interface.

The default URL is: `https://192.168.111.1`.

- 2 From the navigation bar, select **Administration > VPN Manager Access**

The VPN Manager Access page appears.



The screenshot shows the 'VPN Manager Access' configuration page. At the top, there is a navigation bar with 'Administration' and 'VPN Manager Access'. Below this, there is a section titled 'Enable VPN Manager Access' with a checked checkbox. Underneath, there are four password fields: 'Status Passphrase', 'Confirm Status Passphrase', 'Configuration Passphrase', and 'Confirm Configuration Passphrase'. Each field has a masked input (asterisks). At the bottom, there is another checked checkbox labeled 'Enable interoperability with VPN Manager v7.0, v7.1, and v7.2'. At the very bottom, there are two buttons: 'Submit' and 'Reset'.

- 3 Select the **Enable VPN Manager Access** check box.

- 4 Type and confirm a status and configuration passphrase to be used to allow the Management Server to make read-only and read-write connections to your Firebox X Edge.

You must give these passphrases to the WatchGuard Management Server administrator. You do not use these passphrases for any other tasks.

5 Click Submit.

Managed VPN: With a Firebox III or Firebox X and WatchGuard System Manager 7.3

You can configure a VPN on the Firebox® X Edge with two different methods: Managed VPN and Manual VPN. This section tells you how to use Managed VPN, or DVCP. For information on creating a Manual VPN, see “Manual VPN: Setting Up Manual VPN Tunnels” on page 140.

Dynamic VPN Configuration Protocol (DVCP) is the WatchGuard® protocol that you can use to create IPSec tunnels easily. The DVCP server does the VPN tunnel configuration. You use the name Managed VPN because the DVCP Server manages the VPN and sends the VPN configuration to your Edge. This makes the Edge administrator’s task easy because you must type only a small quantity of information into the Edge configuration pages.

You can use only a Firebox III or Firebox X Core model as a DVCP server. The Firebox X Edge cannot be a DVCP Server. When your Firebox X Edge uses DVCP to get its VPN configuration, your Edge is a client of a DVCP server Firebox in a client-server relationship. The Edge gets all of its VPN configuration from the DVCP Server Firebox.

DVCP servers are of two types:

- **Basic DVCP** – All Firebox III and Firebox X Core models can be a Basic DVCP server. The Firebox X Edge cannot be a Basic DVCP server.
- **VPN Manager** – Firebox III 1000 or above and Firebox X Core model X700 or higher Fireboxes can be VPN Manager DVCP Servers. VPN Manager is an advanced version of Basic DVCP. The Firebox III or Firebox X administrator can manage your Edge from the VPN Manager interface.

For more information, see the FAQ:

https://www.watchguard.com/support/advancedFAQs/basicdvcp_whatIs.asp

Getting information about the DVCP Server

You must get this information from the administrator of the DVCP Server Firebox:

- Find out if the DVCP Server Firebox is a **Basic DVCP Server** or a **VPN Manager DVCP Server**.

Find the procedure below to set up the Edge for Basic DVCP or VPN Manager.

- The DVCP shared key

This is different from the VPN shared key that you use to create a Manual VPN. When the DVCP Client gets its VPN configuration information from the DVCP Server, the DVCP shared key is used to encrypt these connections. The DVCP Server automatically makes the shared key that encrypts actual tunnel data, and sends this key to the Edge when it sends the Edge its VPN configuration.

You do not have to know this information if you have a Firebox X Edge with a public IP address on the external interface that is static, and if the Edge will be a client of a VPN Manager DVCP Server. VPN Manager automatically makes the DVCP shared key and sends it to the Edge.

- Client name

This name is case-sensitive.

You do not have to know this information if you have a static Firebox X Edge that will be a client of a VPN Manager DVCP Server. VPN Manager automatically gets this and sends it to the Edge.

- The external IP address of the DVCP Server

You do not have to know this information if you have a static Firebox X Edge that will be a client of a VPN Manager DVCP Server. VPN Manager can connect to your Firebox X Edge because it knows the Edge's static external IP address.

- The VPN Manager status and configuration passphrases

This information is not used for Basic DVCP.

Setting up the Edge for Basic DVCP

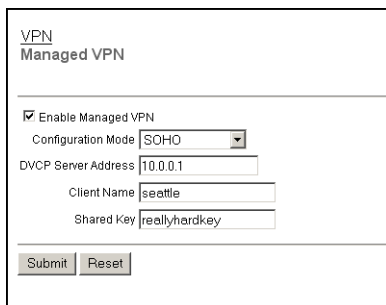
Use this procedure to make a Firebox X Edge a client of a Basic DVCP server. The procedure is the same if your Edge has a static IP address or a dynamic IP address on its external interface:

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.

The default URL is: `https://192.168.111.1`.

- 2 From the navigation bar, select **VPN > Managed VPN**.

The Managed VPN page appears.



VPN
Managed VPN

☒ Enable Managed VPN

Configuration Mode SOHO

DVCP Server Address 10.0.0.1

Client Name seattle

Shared Key reallyhardkey

Submit Reset

- 3 Select the **Enable Managed VPN** check box.

- 4 Type the IP address of the DVCP server.

- 5 Type the **Client Name** to give your Firebox X Edge.

This is the name the Edge gives to the DVCP Server to use to identify the Edge.

- 6 Type the **Shared Key**.

This is the shared key used to encrypt the connection between the DVCP Server and the Firebox X Edge. This shared key must be the same on the Edge and the DVCP Server. You must get the shared key from your VPN administrator.

Setting up the Edge for VPN Manager

You use a different procedure when the Edge has a static IP address than you do when the Edge has a dynamic IP address.

Setting up VPN Manager on an Edge with dynamic external IP address

If the IP address assigned to your Firebox X Edge external interface is dynamic, use this procedure to configure it for VPN Manager:

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.

The default URL is: `https://192.168.111.1`.

- 2 From the navigation bar, select **Administration > VPN Manager Access**

The VPN Manager Access page appears.

Administration
VPN Manager Access

☒ Enable VPN Manager Access

Status Passphrase

Confirm Status Passphrase

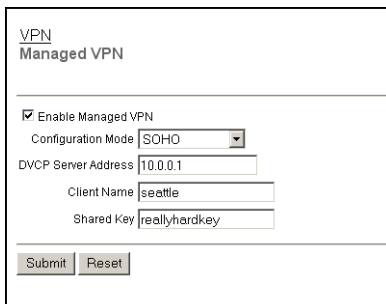
Configuration Passphrase

Confirm Configuration Passphrase

☒ Enable interoperability with VPN Manager v7.0, v7.1, and v7.2.

- 3 Select the **Enable VPN Manager Access** check box.
- 4 Type and confirm a status and configuration passphrase to be used to allow the DVCP Server to make read-only and read-write connections to your Firebox X Edge.
You must give these passphrases to the WatchGuard DVCP Server administrator. You do not use these passphrases for any other tasks.
- 5 If the DVCP Server Firebox uses a version of WatchGuard System Manager older than WSM version 7.3, select the **Enable Interoperability with VPN Manager v7.0, v7.1, and v7.2** check box. If the DVCP Server Firebox uses WatchGuard System Manager 7.3 or later, do not select this check box.
- 6 Click the **Submit** button.

- 7 From the navigation bar select **VPN > Managed VPN**.
The Managed VPN page appears.



VPN
Managed VPN

☒ Enable Managed VPN

Configuration Mode SOHO

DVCP Server Address 10.0.0.1

Client Name seattle

Shared Key reallyhardkey

Submit Reset

- 8 Select the **Enable Managed VPN** check box.
- 9 Type the IP address of the DVCP server.
- 10 Type the client name and the shared key.
- 11 Click **Submit**.

Setting up the Edge for VPN Manager on an Edge with static external IP address

If your Firebox X Edge has a static IP address assigned to its external interface, use this procedure to configure it for VPN Manager:

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`.
- 2 From the navigation bar, select **Administration > VPN Manager Access**
The VPN Manager Access page appears.

Administration
VPN Manager Access

☒ Enable VPN Manager Access

Status Passphrase

Confirm Status Passphrase

Configuration Passphrase

Confirm Configuration Passphrase

☒ Enable interoperability with VPN Manager v7.0, v7.1, and v7.2.

- 3 Select the **Enable VPN Manager Access** check box.
- 4 Type the status passphrase and type it again to confirm it. Type the configuration passphrase and type it again to confirm it.
- 5 If the DVCP Server Firebox uses a version of WatchGuard System Manager older than WSM version 7.3, select the **Enable Interoperability with VPN Manager v7.0, v7.1, and v7.2** check box. If the DVCP Server Firebox uses WatchGuard System Manager 7.3 or later, do not select this check box.
- 6 Click the **Submit** button.

Manual VPN: Setting Up Manual VPN Tunnels

To create a VPN tunnel manually to another Firebox® X Edge or to a Firebox III or Firebox X, or to configure a VPN tunnel to a device that is not a WatchGuard® device, you must use Manual VPN. Use this section to configure Manual VPN on the Firebox X Edge.

What you need for Manual VPN

In addition to the VPN requirements at the start of this chapter, you must have this information for a Manual VPN:

- You must know if the IP address assigned to the other VPN device is static or dynamic. If the other VPN device is dynamic, your Edge must find the other device by domain name. This means that the other device must use Dynamic DNS if its external IP address is dynamic.

- You must know the shared key (passphrase) for the tunnel. The same shared key must be used by the two devices.
- You must know the encryption method used for the tunnel (DES or 3DES). Each VPN device must use the same encryption method.
- You must know the authentication method for each end of the tunnel (MD5 or SHA1). Each VPN device must use the same authentication method.

We recommend that you write down your Firebox X Edge configuration, and the related information for the other device. Use the Sample VPN Address Information table on the subsequent page to record this information.

Sample VPN Address Information Table

Item	Description	Assign
External IP Address	The IP address that identifies the IPSec-compatible device on the Internet. Site A: 207.168.55.2 Site B: 68.130.44.15	ISP
Local Network Address	An address used to identify a local network. These are the IP addresses of the machines on each side that are allowed to send traffic through the VPN tunnel. We recommend that you use an address from one of the reserved ranges: 10.0.0.0/8—255.0.0.0 172.16.0.0/12—255.240.0.0 192.168.0.0/16—255.255.0.0 The numbers after the slashes indicate the subnet masks. /24 means that the subnet mask for the trusted network is 255.255.255.0. For more information on entering IP addresses in slash notation, see this FAQ: https://www.watchguard.com/support/advancedfaqs/general_slash.asp Site A: 192.168.111.0/24 Site B: 192.168.222.0/24	You
Shared Key	The shared key is a passphrase used by two IPSec-compatible devices to encrypt and decrypt the data that goes through the VPN tunnel. The two devices use the same passphrase. If the devices do not have the same passphrase, they cannot encrypt and decrypt the data correctly. Use a passphrase that contains numbers, symbols, lowercase letters, and uppercase letters for better security. For example, “Gu4c4mo!3” is better than “guacamole”. Site A: OurSharedSecret Site B: OurSharedSecret	You
Encryption Method	DES uses 56-bit encryption. 3DES uses 168-bit encryption. The 3DES encryption method is more secure, but slower. The two devices must use the same encryption method. Site A: 3DES Site B: 3DES	You
Authentication	The two devices must use the same authentication method. Site A: MD5 (or SHA1) Site B: MD5 (or SHA1)	You

To create Manual VPN tunnels on your Firebox X Edge

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`.
- 2 From the navigation bar, select **VPN > Manual VPN**.
The Manual VPN page appears.
- 3 Click **Add**.
The Add Gateway page appears.

VPN > Manual VPN
Add Gateway

Name

Shared Key

Phase 1 Settings

Mode

Remote IP Address

Local ID Type

Remote ID Type

Authentication Algorithm

Encryption Algorithm

Negotiation expiration in kilobytes

Negotiation expiration in hours

Diffie-Hellman Group

☒ Generate IKE Keep Alive Messages

- 4 Type the name and shared key.
The tunnel name is for your identification only. It does not have to be the same as anything on the other device.
The shared key is a passphrase that the devices use to encrypt and decrypt the data on the VPN tunnel. The two devices use the same passphrase. If the devices do not have the same passphrase, they cannot encrypt and decrypt the data correctly.

Phase 1 settings

Internet Key Exchange (IKE) is a protocol used with VPN tunnels to manage keys automatically. IKE negotiates and changes keys. Phase

1 authenticates the two sides and creates a key management security association to protect tunnel data.

The default settings for Phase 1 are the same for all Firebox X devices. Many users keep these settings in their default values.

NOTE

Make sure that the Phase 1 configuration is the same on the two devices.

To change Phase 1 configuration:

- 1 Select the negotiation mode for Phase 1 from the drop-down list.

NOTE

You can use Main Mode only when the two devices have static IP addresses. If any of the devices have external IP addresses that are dynamically assigned, you must use Aggressive Mode.

- 2 Enter the local ID and remote ID. Select the ID types—**IP Address** or **Domain Name**—from the drop-down lists. Make sure this configuration is the same as the configuration on the remote device.

Note that on the other device, the local ID type and remote ID type are reversed.

- If your Firebox X Edge has a static external IP address, set the local ID type to **IP Address**. Type the Edge's external IP address as the local ID.
- If your Firebox X Edge has a dynamic external IP address, you must select **Aggressive Mode** and you must set up Dynamic DNS on the Edge. For information, see "Registering with the Dynamic DNS Service" on page 66. Set the local ID type to **Domain Name**. Enter your Edge's DynDNS domain name as the local ID.
- If the remote VPN device has a static external IP address, set the remote ID type to **IP Address**. Enter the remote gateway's IP address as the remote ID.
- If the remote VPN device has a dynamic external IP address and the remote gateway uses Dynamic DNS, set the remote ID type to remote ID.

NOTE

If your Edge's external interface has a private IP address instead of a public IP address, then your ISP or the Internet access device connected to the Edge's external interface (modem or router) does Network Address Translation (NAT). See the instructions at the end of this section if your Edge's external interface has a private IP address.

- 3 Select the type of authentication from the **Authentication Algorithm** drop-down list.
The options are MD5-HMAC (128-bit authentication) or SHA1-HMAC (160-bit authentication).
- 4 From the **Encryption Algorithm** drop-down list, select the type of encryption.
The options are DES-CBC or 3DES-CBC.
- 5 Type the number of kilobytes and the number of hours until the IKE negotiation expires.
To make the negotiation not expire, enter zero. For example, 24 hours and zero kilobytes means that the phase 1 key is negotiated every 24 hours.
- 6 Select the group number from the **Diffie-Hellman Group** drop-down list. WatchGuard supports group 1 and group 2.
Diffie-Hellman groups securely negotiate secret keys through a public network. Group 2 is more secure than group 1, but uses more processing power and more time.
- 7 Select the **Generate IKE Keep Alive Messages** check box to help find when the tunnel is down.
Select this check box to send short packets across the tunnel at regular intervals. This helps the two devices to see if the tunnel is up. If the Keep Alive packets get no response after three tries, the Firebox X Edge starts the tunnel again.

NOTE

The IKE Keep Alive feature is different from the VPN Keep Alive feature in "VPN Keep Alive," on page 148.

If your Firebox X Edge is behind a device that does Network Address Translation (NAT)

The Firebox X Edge can use NAT-Traversal. This means that you can make VPN tunnels if your ISP does Network Address Translation (NAT) or if your Edge's external interface is connected to a device that does NAT. We recommend that the Edge's external interface

have a public IP address. If that is not possible, use this section for more information.

Devices that do NAT frequently have some basic firewall features built into them. To make a VPN tunnel to your Firebox X Edge when the Edge is behind a device that does NAT, the NAT device must let the traffic through. These ports and protocols must be open on the NAT device:

- UDP port 500 (IKE)
- UDP Port 4500 (NAT Traversal)
- IP Protocol 50 (ESP)

Speak to the NAT device's manufacturer for information on opening these ports and protocols.

If your Edge's external interface has a private IP address, you cannot use IP Address as the local ID type in the Phase 1 settings. Because private IP addresses cannot get through the Internet, the other device cannot find your Edge's private external IP address through the Internet.

- If the NAT device to which the Edge is connected has a dynamic public IP address:
 - You must first set the device to Bridge Mode. In Bridge Mode, the Edge will get the public IP address on its external interface. Refer to the manufacturer of your NAT device for more information.
 - Then, set up Dynamic DNS on the Edge. For information, see "Registering with the Dynamic DNS Service" on page 66. In the Phase 1 settings of the Manual VPN, set the local ID type to **Domain Name**. Enter the DynDNS domain name as the Local ID. The remote device must identify your Edge by domain name and it must use your Edge's DynDNS domain name in its Phase 1 setup.
- If the NAT device to which the Edge is connected has a static public IP address:
 - In the Phase 1 settings of the Manual VPN, set the local ID type drop-down list to **Domain Name**. Enter the public IP address assigned to the NAT device's external interface as the local ID. The remote device must identify your Edge by domain

name, and it must use this same public IP address as the domain name in its Phase 1 setup.

Phase 2 settings

Phase 2 negotiates the data management security association for the tunnel. The tunnel uses this phase to create IPSec tunnels and put data packets together.

You can use the default Phase 2 settings to make configuration easier.

NOTE

Make sure that the Phase 2 configuration is the same on the two devices.

To change the Phase 2 settings:

- 1 Select the authentication method from the **Authentication Algorithm** drop-down list.
- 2 Select the encryption algorithm from the **Encryption Algorithm** drop-down list.
- 3 To use Perfect Forward Secrecy, select the **Enable Perfect Forward Secrecy** check box.
This option makes sure that each new key comes from a new Diffie-Hellman exchange. This option makes the negotiation more secure, but uses more time.
- 4 Type the number of kilobytes and the number of hours until the Phase 2 key expires.
To make the key not expire, enter zero. For example, 24 hours and zero kilobytes means that the Phase 2 key is renegotiated each 24 hours no matter how much data has passed.
- 5 Type the IP address of the local network and the remote networks that will send encrypted traffic across the VPN.
You must enter network addresses in "slash" notation (also known as Classless Inter Domain Routing or CIDR notation). For more information on how to enter IP addresses in slash notation, see this FAQ: http://www.watchguard.com/support/advancedfaqs/general_slash.asp.
- 6 Click **Add**.

7 Click **Submit**.

Phase 2 Settings

Authentication Algorithm
SHA1-HMAC

Encryption Algorithm
3DES-CBC

☐ Enable Perfect Forward Secrecy

Key expiration in kilobytes
8192

Key expiration in hours
24

The Firebox X Edge will create a tunnel for each remote network defined below. In order to interoperate properly, the remote peer must be configured the same way.

Local Network	Remote Network	
		Remove

Local Network
0.0.0.0/0

Remote Network
0.0.0.0/0
Add

Submit
Reset

VPN Keep Alive

To keep the VPN tunnel open when there are no connections through it, you can use the IP address of a computer at the other end of the tunnel as an echo host. The Firebox® X Edge sends a ping each minute to the specified host. Use the IP address of a host that is always up, and that responds to ping messages. You can enter the trusted interface IP address of the Firebox X Edge, or the trusted interface IP address of a Firebox III or Firebox X that is at the other end of the tunnel. You can use more than one IP address so the Firebox X Edge can send a ping to more than one host through different tunnels.

- To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.

The default URL is: <https://192.168.111.1>.

- 2 From the navigation bar, select **VPN > Keep Alive**.
The VPN Keep Alive page appears.

VPN
VPN Keep Alive

Echo Hosts 64.23.103.18 Remove

Host Address 64.23.103.18 Add

Submit Reset

- 3 Type the IP address of an echo host. Click **Add**.
- 4 Click **Submit**.

Viewing VPN Statistics

You can monitor Firebox® X Edge VPN traffic and troubleshoot the VPN configuration with the VPN Statistics page.

To see the VPN Statistics page:

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 2 From the navigation bar, select **VPN > VPN Statistics**.
The VPN Statistics page appears.

Frequently Asked Questions

Why do I need a static external address?

To make a VPN connection, each device must know the IP address of the other device. If the address for a device is dynamic, the IP address can change. If the IP address changes, connections between

the devices cannot be made unless the two devices know how to find each other.

You can use Dynamic DNS. For information, see “Registering with the Dynamic DNS Service” on page 66.

How do I get a static external IP address?

You get the external IP address for your computer or network from your ISP or an administrator. Many ISPs use dynamic IP addresses to make their networks easier to configure and use with many users. Most ISPs can give you a static IP address as an option.

How do I troubleshoot the connection?

If you can send a ping to the trusted interface of the remote Firebox® X Edge and the computers on the remote network, the VPN tunnel is up. The configuration of the network software or the software applications are possible causes of other problems.

Why is ping not working?

If you cannot send a ping the local interface address of the remote Firebox X Edge, follow these steps:

- 1 Ping the external address of the remote Firebox X Edge.
For example, at Site A, ping 68.130.44.15 (Site B). If the ping packet does not come back, make sure the external network settings of Site B are correct. (Site B must be configured to respond to ping requests on that interface.) If the settings are correct, make sure that the computers at Site B have Internet access. If the computers at site B do not have Internet access, speak to a service person at your ISP.
- 2 If you can ping the external address of each Firebox X Edge, try to ping a local address in the remote network.
From Site A, ping 192.168.111.1. If the VPN tunnel is up, the remote Firebox X Edge sends the ping back. If the ping does not come back, make sure the local configuration is correct. Make sure that the local DHCP address ranges for the two networks connected by the VPN tunnel do not use any of the same IP addresses. The two networks connected by the tunnel must not use the same IP addresses.

How do I set up more than the number of allowable VPNs on my Firebox X Edge?

The number of VPN tunnels that you can create on your Firebox X Edge is set by the Edge model you have. You can purchase a model upgrade for your Edge to make more VPN tunnels. You can purchase a Firebox X Edge Model Upgrade from a reseller or from the WatchGuard® Web site:

<http://www.watchguard.com/sales/buyonline.asp>

Is the Firebox X Edge compatible with WatchGuard System Manager?

Yes. The default Firebox X Edge configuration is compatible with WatchGuard System Manager v7.3 and higher. To configure the Edge for use with WSM v7.0, v7.1, and v7.2, browse to the VPN Manager Access page (**Administration > VPN Manager Access**). Select the check box **Enable interoperability with VPN Manager v7.0, v7.1, and v7.2**.

Configuring the MUVPN Client

Mobile User VPN lets remote users connect to your Firebox® X Edge's private network through a secure, encrypted channel. The MUVPN client is a software application that is installed on a remote computer. The client makes a secure connection from the remote computer to your protected network from an unsecured network. The MUVPN client uses Internet Protocol Security (IPSec) to secure the connection.

This example shows how the MUVPN client is used:

- The MUVPN client software is installed on a remote computer.
- The remote user imports a configuration file (.wgx file) to configure the client software.
- The user connects to the Internet with the remote computer. The user starts the MUVPN client by activating the security policy.
- The MUVPN client creates an encrypted tunnel to the Firebox X Edge.
- The Firebox X Edge connects the remote computer to the trusted network. The employee now has secure remote access to the internal network.

The MUVPN client is available in two different packages. One version includes ZoneAlarm®, a personal software-based firewall. ZoneAlarm gives remote computers more security. The other package does not

include ZoneAlarm. The use of ZoneAlarm is optional. Other than ZoneAlarm, the two packages are the same.

This chapter shows how to prepare the Edge and the remote computer for MUVPN. This chapter also includes information about the features of the ZoneAlarm personal firewall.

About This Chapter

You must complete some procedures to make sure that MUVPN operates correctly. Use this chapter to learn about these procedures:

- First, you must enable the Firebox® X Edge user's account for MUVPN and set the options that apply to all MUVPN clients. Read the section "Enabling MUVPN for Edge Users" on page 155 for information on the Firebox user's MUVPN account, and for information on MUVPN options that affect all MUVPN users.
- When the Firebox user's account is configured for MUVPN, the Edge creates a configuration file (.wgx file). You must get this .wgx configuration file from the Edge. You must also download the MUVPN installation program from the WatchGuard support site. Read the section "Distributing the Software and the .wgx File" on page 158 for information about how to get these items and how to give them securely to the remote user.
- The remote user's computer must have the correct networking components for the MUVPN to operate correctly. Read the section "Preparing Remote Computers for MUVPN" on page 159 to be sure that the user's computer is prepared to install and use MUVPN software.
- When the user has the MUVPN installation files and the .wgx configuration file, the user can install the MUVPN software. Read the section "Installing and Configuring the MUVPN Client" on page 167.
- After the sections on how to set up the Edge and the remote client, this chapter has sections on how to use the MUVPN software and how to use the ZoneAlarm personal firewall.
- You can use MUVPN to make the wireless network on the Firebox X Edge Wireless more secure. If you have a Firebox X Edge Wireless, read the section "Using MUVPN on the Edge

Wireless Network” on page 176 for information about how to make the wireless computers use MUVPN on the Edge’s wireless network.

- If you want to use a Pocket PC to make a VPN connection to the Edge, read the section “Tips for Configuring the Pocket PC” on page 177.
- At the end of this chapter is a section with troubleshooting tips.

Enabling MUVPN for Edge Users

Before you configure the MUVPN client, you must configure MUVPN client and user settings on the Firebox® X Edge.

Configuring MUVPN client settings

Some MUVPN client settings apply to all of the Edge’s MUVPN connections. Select **Firebox Users > Settings** to configure these:

- To make the .wgx file read-only so that the user cannot change the security policy, select the **Make the MUVPN client security policy read-only** check box.
- Set how the virtual adapter operates on the client (Disabled, Preferred, or Required). The remote MUVPN computers can use a virtual adapter to get network settings, an IP address, and WINS and DNS address assignments. You can set the virtual adapter rule for your mobile users to:

Disabled

The mobile user does not use a virtual adapter to connect with the MUVPN client. This is the default setting. With the virtual adapter disabled, the MUVPN client is not assigned a WINS or DNS address. Because of this, make sure the computer has correct WINS and DNS addresses configured in the primary network card settings. See the section “Preparing Remote Computers for MUVPN” on page 159 for information on entering WINS and DNS addresses in advanced TCP/IP settings of the network card.

Preferred

If the virtual adapter is in use or it is not available, the mobile user does not use a virtual adapter to connect with the MUVPN client.

If the virtual adapter is available, the remote computer is assigned the WINS and DNS addresses you entered in the **Firebox Users > Settings** area of the Edge configuration pages.

Required

The mobile user must use a virtual adapter to connect with the MUVPN client. If the virtual adapter is not available on the MUVPN client computer, the VPN tunnel cannot connect. The remote computer is assigned WINS and DNS addresses you entered in the **Firebox Users > Settings** area of the Edge configuration pages.

- Type the IP addresses of the DNS and WINS servers for the MUVPN clients.

For information on these settings, see “Configuring MUVPN client settings” on page 190.

Enabling MUVPN access for a Firebox user account

- 1 Add a new Firebox user or edit a Firebox user, as described in “Adding or Editing a User Account” on page 190.
- 2 Click the **MUVPN** tab.
- 3 Select the **Enable MUVPN for this account** check box.
- 4 Type a shared key in the related field.
The .wgx file is encrypted with this shared key. The user enters the shared key when the .wgx file is imported. Do not give the shared key to any user that is not authorized to use this Firebox Users account.
- 5 Type the virtual IP address in the related field.
The virtual IP address must be an address on the Firebox X Edge trusted network that is not used. This address is used by the remote computer to connect to the Firebox X Edge.
- 6 From the **Authentication Algorithm** drop-down list, select the type of authentication.
The options are MD5-HMAC and SHA1-HMAC.
- 7 From the **Encryption Algorithm** drop-down list, select the type of encryption.
The options are DES-CBC and 3DES-CBC.

- 8 Set MUVPN key expiration in kilobytes or hours. The default values are 8192 KB and 24 hours.
- 9 Select **Mobile User** from the **VPN Client Type** drop-down list if the remote user is connecting from a desktop or laptop computer instead of a handheld device such as a Pocket PC.
- 10 Select the **All traffic uses tunnel (0.0.0.0/0 IP Subnet)** check box if the remote client will send all its traffic (including usual Web traffic) through the VPN tunnel to the Firebox X Edge. This can also let the MUVPN client connect with other networks that the Firebox X Edge connects to.
If you do not select this check box, the remote user can connect with the Edge's trusted network only. You must enable this check box for the remote user to be able to connect to:
 - Networks on the other side of a Branch Office VPN tunnel that the Edge has connected.
 - Computers on the Edge's optional network.
 - Networks that are behind a static route on the trusted or optional interface. For information on defining static routes, see "Making Static Routes" on page 63.
- 11 Click **Submit**.

[Firebox Users](#)
 Edit User: **muvpn**

Settings | **WebBlocker** | **MUVPN**

☒ Enable MUVPN for this account.
 Shared Key
 Virtual IP Address
 Authentication Algorithm
 Encryption Algorithm
 Key expiration in kilobytes
 Key expiration in hours
 VPN Client Type
☐ All traffic uses tunnel (0.0.0.0/0 IP Subnet).

Configuring the Firebox for MUVPN clients using a Pocket PC

To create a MUVPN tunnel between the Firebox X Edge and your Pocket PC, you must configure the Firebox User account correctly. Use the previous procedure, but select **Pocket PC** from the **VPN Client Type** drop-down list.

NOTE

WatchGuard does not give a Mobile User VPN software package for the Pocket PC. You must examine the software manufacturer's instructions to configure their software and the Pocket PC. For more information about configuring your Pocket PC as an MUVPN client, see "Tips for Configuring the Pocket PC" on page 177.

Distributing the Software and the .wgx File

You must give the remote user the MUVPN software installer and the end-user profile, or .wgx file.

Get the MUVPN installation files from the WatchGuard® Web site

You must log in to get access to your LiveSecurity® Service at <http://www.watchguard.com/support>

After you log in, go to the Latest Software area and select Firebox® X Edge in the **Choose Product Family** area. There are two different versions of Mobile User VPN software. One version contains the personal firewall ZoneAlarm and the other one does not.

Get the user's .wgx file

The Firebox X Edge has encrypted MUVPN client configuration (.wgx) files available for download.

- To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: <https://192.168.111.1>.
- From the navigation bar, select **Firebox Users** and scroll to the bottom of the page.
- Below **MUVPN Client Configuration Files**, select the .wgx file to download by clicking on the link `username.wgx` where `username` is the Firebox user's name.

- At the prompt, save the .wgx file to your computer.

Secure MUVPN Client Configuration Files	
External MUVPN access count 0 (maximum 15)	
The following secure (encrypted) MUVPN client configuration (.wgx) files are available for download. Once downloaded, these files can be used to configure your MUVPN client software in a manner that is consistent with the currently defined MUVPN settings on the X15.	
Account Name	MUVPN Client Configuration Files
admin	admin.wgx
muvpn	muvpn.wgx
user	user.wgx
cfgview	cfgview.wgx

Give these two files to the remote user

Give the MUVPN software, and the .wgx file to the remote user. You must also give the user the shared key you used when you enabled the Firebox User account to use MUVPN, as described in “Enabling MUVPN for Edge Users” on page 155. The user uses this shared key at the end of the installation process.

NOTE

The shared key is highly sensitive information. For security reasons, we recommend that you do not give the user the shared key in an e-mail. Because e-mail is not secure, an unauthorized user can get the shared key. Give the user the shared key by telling it to the user, or by some other method that does not allow an unauthorized person to get the shared key.

Preparing Remote Computers for MUVPN

Install the MUVPN client only on computers that have these minimum requirements.

- A computer with a Pentium processor (or equivalent)
- Compatible operating systems and minimum RAM:
 - Microsoft Windows NT 4.0 Workstation: 32 MB
 - Microsoft Windows 2000 Professional: 64 MB
 - Microsoft Windows XP: 64 MB

- No other IPSec VPN client software can be on the computer. Remove any other software from the user's computer before you try to install the WatchGuard MUVPN software.
- We recommend that you install the most current service packs for each operating system.
- 10 MB hard disk space
- Native Microsoft TCP/IP communications protocol
- Microsoft Internet Explorer 5.0 or later
- An Internet service provider account
- A dial-up or broadband (DSL or cable modem) connection

WINS and DNS servers

To use Windows file and print sharing on an MUVPN tunnel, the remote computer must connect to the WINS and DNS servers. These servers are on the Firebox® X Edge trusted network. To get to these servers, the servers' IP addresses must be configured on the remote computer or they must be assigned by the Edge when the VPN tunnel connects.

If the MUVPN client uses the virtual adapter, the WINS and DNS server IP addresses are assigned to the remote computer when the VPN tunnel is created.

If the MUVPN client does not use the virtual adapter, the remote computer must have your network's private WINS and DNS server IP addresses listed in the Advanced TCP/IP Properties of the primary Internet connection.

Windows NT setup

Use this section to install the network components for the Windows NT operating system. These components must be installed before you can use the MUVPN client on a Windows NT computer.

Installing Remote Access Services on Windows NT

You must install Remote Access Services (RAS) before you install the Mobile User VPN Adapter. To install RAS, use this procedure:

- 1 Follow the Windows desktop, select **Start > Settings > Control Panel**.
- 2 Double-click the **Network** icon.
The Network window appears.

- 3 Click the **Services** tab and click **Add**.
- 4 Select **Remote Access Services** and click **OK**.
- 5 Type the path to the Windows NT installation files, or put your system installation CD in the computer and click **OK**.
The Remote Access Setup window appears.
- 6 Click **Yes** to add a RAS device, for example, a modem, and then click **Add**.
- 7 Complete the Install New Modem wizard.

NOTE

If there is no modem installed, select the check box marked **Don't detect my modem; I will select it from a list**. Select the standard 28800 modem. If a modem is not available, you can select a serial cable between two computers.

- 8 Select the modem from the Add RAS Device window.
- 9 Click **OK**, click **Continue**, and click **Close**.
- 10 Restart the computer.

Configuring the WINS and DNS settings

The remote computer must be able to contact the WINS servers and the DNS servers. These servers are found on the trusted network that is protected by the Firebox X Edge.

From the Windows desktop:

- 1 Select **Start > Settings > Control Panel**.
- 2 Double-click the **Network** icon.
The Network window appears.
- 3 Click the **Protocols** tab and select the **TCP/IP** protocol.
- 4 Click **Properties**.
The Microsoft TCP/IP Properties window appears.
- 5 Click the **DNS** tab and click **Add**.
- 6 Type the IP address of your DNS server.
To add more DNS servers, repeat steps 5 and 6 for each server.

NOTE

The DNS server on the private network of the Firebox X Edge must be the first server in the list.

- 7 Click the **WINS Address** tab, type the IP address of your WINS server in the applicable field, and then click **OK**.
To add more WINS servers, repeat this step.
- 8 Click **Close** to close the Network window.
The Network Settings Change dialog box appears.
- 9 Click **Yes** to restart the computer.
The computer restarts.

Windows 2000 setup

Use this section to install and configure the network components for the Windows 2000 operating system. These components must be installed before you can use the MUVPN client on a Windows 2000 computer.

From the Windows desktop:

- 1 Select **Start > Settings > Network and Dial-up Connections**.
- 2 Select the dial-up connection you use to get Internet access.
The connection window appears.
- 3 Click **Properties** and click the **Networking** tab.

- 4 Make sure these components are installed and enabled:
 - Internet Protocol (TCP/IP)
 - File and Printer Sharing for Microsoft Networks
 - Client for Microsoft Networks

Installing the Internet Protocol (TCP/IP) network component

From the connection window **Networking** tab:

- 1 Click **Install**.
The Select Network Component Type window appears.
- 2 Double-click the **Protocol** network component.
The Select Network Protocol window appears.
- 3 Select the **Internet Protocol (TCP/IP)** network protocol. Click **OK**.

Installing the File and Printer Sharing for Microsoft Networks

From the connection window **Networking** tab:

- 1 Click **Install**.
The Select Network Component Type window appears.
- 2 Double-click the **Services** network component.
The Select Network Service window appears.
- 3 Select the **File and Printer Sharing for Microsoft Networks** network service and click **OK**.

Installing the Client for Microsoft Networks

From the connection window **Networking** tab:

- 1 Click **Install**.
The Select Network Component Type window appears.
- 2 Double-click the **Client** network component.
The Select Network Protocol window appears.
- 3 Select the **Client for Microsoft Networks** network client and click **OK**.

Configuring the WINS and DNS settings

The remote computer must be able to connect to the WINS and DNS servers. These servers are on the trusted network of the Firebox X Edge.

From the connection window **Networking** tab:

- 1 Select the **Internet Protocol (TCP/IP)** component and click **Properties**.
The Internet Protocol (TCP/IP) Properties window appears.
- 2 Click **Advanced**.
The Advanced TCP/IP Settings window appears.
- 3 Click the **DNS** tab and from the section labeled **DNS server addresses, in order of use**, click **Add**.
The TCP/IP DNS Server window appears.
- 4 Type the IP address of the DNS server and click **Add**.
To add more DNS servers, repeat steps 3 and 4.

NOTE

The DNS server on the private network of the Firebox X Edge must be the first server in the list.

- 5 Select the **Append these DNS suffixes (in order)** check box and click **Add**.
The TCP/IP Domain Suffix window appears.
- 6 Type the domain suffix in the applicable field.
To add additional DNS suffixes, go back to step 5.
- 7 Click the **WINS** tab and then from the section **WINS addresses, in order of use**, click **Add**.
The TCP/IP WINS Server window appears.
- 8 Type the IP address of the WINS server in the applicable field. Click **Add**.
To add more WINS servers, repeat steps 7 and 8.
- 9 Click **OK** to close the Advanced TCP/IP Settings window. Click **OK** to close the Internet Protocol (TCP/IP) Properties window.
- 10 Click **OK**.
- 11 Click **Cancel** to close the connection window.

Windows XP setup

Use this section to install and configure the network components for the Windows XP operating system. You must install these components if you use the MUVPN client on a Windows XP computer.

From the Windows desktop:

- 1 Select **Start > Control Panel**.
The Control Panel window appears.
- 2 Double-click the **Network Connections** icon.

- 3 Double-click the connection you use to get Internet access.
The connection window appears.
- 4 Click **Properties** and then click the **Networking** tab.
- 5 Make sure these components are installed and enabled:
 - Internet Protocol (TCP/IP)
 - File and Printer Sharing for Microsoft Networks
 - Client for Microsoft Networks

Installing the Internet Protocol (TCP/IP) Network Component

From the connection window **Networking** tab:

- 1 Click **Install**.
The Select Network Component Type window appears.
- 2 Double-click the **Protocol** network component.
The Select Network Protocol window appears.
- 3 Select the **Internet Protocol (TCP/IP)** network protocol. Click **OK**.

Installing the File and Printer Sharing for Microsoft Networks

From the connection window **Networking** tab:

- 1 Click **Install**.
The Select Network Component Type window appears.
- 2 Double-click the **Services** network component.
The Select Network Service window appears.
- 3 Select the **File and Printer Sharing for Microsoft Networks** network service. Click **OK**.

Installing the Client for Microsoft Networks

From the connection window **Networking** tab:

- 1 Click **Install**.
The Select Network Component Type window appears.
- 2 Double-click the **Client** network component.
The Select Network Protocol window appears.
- 3 Select the **Client for Microsoft Networks** network client. Click **OK**.

Configuring the WINS and DNS settings

The remote computer must be able to connect to the WINS and DNS servers. These servers are on the trusted network of the Firebox X Edge.

From the connection window **Networking** tab:

- 1 Select the **Internet Protocol (TCP/IP)** component.
- 2 Click **Properties**.
The Internet Protocol (TCP/IP) Properties window appears.
- 3 Click **Advanced**.
The Advanced TCP/IP Settings window appears.
- 4 Click the **DNS** tab and then, from the section labeled **DNS server addresses, in order of use**, click **Add**.
The TCP/IP DNS Server window appears.
- 5 Type the IP address of the DNS server in the related field. Click **Add**.
To add more DNS servers, repeat steps 4 and 5.

NOTE

The DNS server on the private network of the Firebox X Edge must be the first server in the list.

- 6 Select the **Append these DNS suffixes (in order)** check box. Click **Add**.
The TCP/IP Domain Suffix window appears.
- 7 Enter the domain suffix for your network's private domain in the related field.
To add more DNS suffixes, repeat step 6.
- 8 Click the **WINS** tab and in the section **WINS addresses, in order of use**, click **Add**.
The TCP/IP WINS Server window appears.
- 9 Type the IP address of the WINS server in the related field. Click **Add**.
To add more WINS servers, repeat steps 8 and 9.
- 10 Click **OK** to close the Advanced TCP/IP Settings window. Click **OK** to close the Internet Protocol (TCP/IP) Properties window, and then click **OK**.
- 11 Click **Cancel** to close the connection window.

Installing and Configuring the MUVPN Client

NOTE

To install and configure the MUVPN client, you must have local administrator rights on the remote computer.

Installing the MUVPN client

To install the MUVPN client:

- 1 No other IPSec VPN client software can be on the computer. Remove any other IPSec VPN software from the user's computer before installing the WatchGuard® MUVPN software.
- 2 Copy the MUVPN installation file and the .wgx file to the remote computer.
- 3 Double-click the MUVPN installation file to start the InstallShield wizard.
- 4 Click **Next**.
If the InstallShield gives you a message about read-only files, click Yes to continue the installation.
- 5 A welcome message appears. Click **Next**.
The Software License Agreement appears.
- 6 Click **Yes** to accept the license agreement.
The Setup Type window appears.
- 7 Select the type of installation. We recommend that you use the **Typical** installation. Click **Next**.
- 8 On a Windows 2000 computer, the InstallShield looks for the Windows 2000 L2TP component. If the component is installed, the InstallShield does not install it again. Click **OK** to continue.
The Select Components window appears.
- 9 Do not change the default selections. Click **Next**.
The Start Copying Files window appears.
- 10 Click **Next** to install the files.
When the dni_vapmp file is installed, a command prompt window appears. The command prompt can stay for more than one minute. This is usual. After the file is installed, the command window closes and the installation continues.
- 11 After the installation is complete, click **Finish**.

- 12 The InstallShield wizard looks for a user profile. Use the **Browse** button to find and select the folder containing the .wgx file. Click **Next**.
You can click Next at this step if you do not have the .wgx file at this time. You can import the .wgx file later. To import a .wgx file, after the software is installed, double-click the .wgx file and give the shared key.
- 13 Click **OK** to continue the installation.
- 14 The MUVPN client is installed. Make sure the option **Yes, I want to restart my computer now** is selected. Click **Finish**.
The computer restarts.

NOTE

The ZoneAlarm personal firewall could prevent you from connecting to the network after the computer restarts. If this occurs, log on to the computer locally the first time after installation. For more information, see "The ZoneAlarm Personal Firewall" on page 173.

Uninstalling the MUVPN client

Use this procedure to remove the MUVPN client. We recommend that you use the Windows Add/Remove Programs tool.

- 1 Disconnect all existing tunnels and dial-up connections.
- 2 Deactivate the security policy on the client (see "Disconnecting the MUVPN client" on page 171).
- 3 Restart the remote computer.
- 4 From the Windows desktop, select **Start > Settings > Control Panel**.
The Control Panel window appears.
- 5 Double-click the **Add/Remove Programs** icon.
The Add/Remove Programs window appears.
- 6 Select **Mobile User VPN** and click **Change/Remove**.
The InstallShield wizard appears.
- 7 Select **Remove**. Click **Next**.
The Confirm File Deletion dialog box appears.
- 8 Click **OK** to remove all of the components.
When the dni_vapmp file is removed, a command prompt window appears. This is usual. After the file is removed, the command prompt window closes and the procedure continues.
The Uninstall Security Policy dialog box appears.

- 9 Click **Yes** to delete the security policy.
The InstallShield Wizard window appears.
- 10 Select **Yes, I want to restart my computer now**. Click the **Finish** option.
The computer restarts.

NOTE

The ZoneAlarm personal firewall settings are kept in these directories by default".

Windows NT and 2000: c:\winnt\internet logs\

Windows XP: c:\windows\internet logs

To remove these settings, delete the contents of the appropriate directory.

- 11 When the computer restarts, select **Start > Programs**.
- 12 Right-click **Mobile User VPN** and select **Delete** to remove this selection from your **Start** menu.

Connecting and Disconnecting the MUVPN Client

The MUVPN client software makes a secure connection from a remote computer to your protected network on the Internet. To start this connection, you must connect to the Internet and use the MUVPN client to connect to the protected network.

Connecting the MUVPN client

Start your connection to the Internet through a Dial-Up Networking connection, a LAN connection, or a WAN connection.

- 1 If the MUVPN client on the Windows desktop system tray is not active, right-click the icon and select **Activate Security Policy**.
For information about the MUVPN icon, see "The MUVPN client icon" on page 169.
- 2 From the Windows desktop, select **Start > Programs > Mobile User VPN > Connect**.
The WatchGuard Mobile User Connect window appears.
- 3 Click **Yes**.

The MUVPN client icon

The MUVPN icon appears in the Windows desktop system tray. The icon image gives information about the status of the connection.

Deactivated



The MUVPN Security Policy is not active. This icon can appear if the Windows operating system did not start a required MUVPN service. If this occurs, the remote computer must be restarted. If the problem continues, remove and install the MUVPN client again.

Activated



The MUVPN client can make a secure MUVPN tunnel connection.

Activated and Transmitting Unsecured Data



The MUVPN client can make a secure MUVPN tunnel connection. The red bar on the right of the icon tells you that the client is sending data that is not secure.

Activated and Connected



The MUVPN client is connected with one or more secure MUVPN tunnels, but it is not sending data.

Activated, Connected and Transmitting Unsecured Data



The MUVPN client started one or more secure MUVPN tunnel connections. The red bar on the right of the icon tells you that the client is sending data that is not secure.

Activated, Connected, and Transmitting Secured Data



The MUVPN client started one or more secure MUVPN tunnels.
The green bar on the right of the icon tells you that the client is only sending data that is secure.

Activated, Connected, and Transmitting both Secured and Unsecured Data



The MUVPN client started one or more secure MUVPN tunnels.
The green and red bars on the right of the icon tell you that the client is sending data that is secure and data that is not secure.

Allowing the MUVPN client through a personal firewall

To create the MUVPN tunnel, you must allow these programs through the personal firewall:

- MuvpnConnect.exe
- IrelKE.exe

The personal firewall detects when these programs try to get access to the Internet. A New Program alert window appears to request access for the MuvpnConnect.exe program.


From the New Program alert window:

- 1 Select the **Remember this answer the next time I use this program** check box, then click **Yes**.
This option lets the ZoneAlarm personal firewall allow Internet access for this program each time you start a MUVPN connection.
The New Program alert window appears to request access for the IrelKE.exe program.
- 2 Set the **Remember this answer the next time I use this program** check box, then click **Yes**.
This option lets the ZoneAlarm personal firewall allow Internet access for this program each time you start a MUVPN connection.

Disconnecting the MUVPN client

From the Windows desktop system tray:

- 1 Right-click the MUVPN client icon and select **Deactivate Security Policy**.
The MUVPN client icon with a red bar is displayed.
- 2 If the ZoneAlarm personal firewall is active, deactivate it now.
From the Windows desktop system tray:

- 3 Right-click the ZoneAlarm icon shown at right. 
- 4 Select **Shutdown ZoneAlarm**.
The ZoneAlarm window appears.
- 5 Click **Yes**.

Monitoring the MUVPN Client Connection

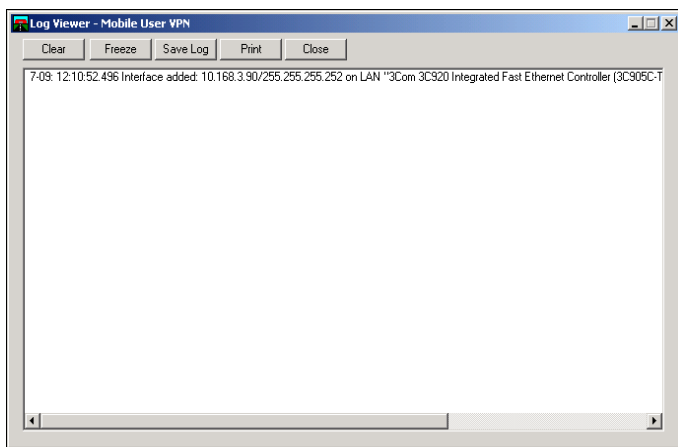
The Log Viewer and the Connection Monitor are installed with the MUVPN client. These tools let you monitor the MUVPN connection and troubleshoot problems.

Using Log Viewer

Use Log Viewer to show the connections log. This log shows the events that occur when the MUVPN tunnel is started.

From the Windows desktop system tray:

- 1 Right-click the **Mobile User VPN** client icon.
- 2 Select **Log Viewer**.
The Log Viewer window appears.



Using Connection Monitor

The Connection Monitor shows statistical and diagnostic information for connections in the security policy. This window shows the security policy settings and the security association (SA) informa-

tion. The monitor records the information that appears in this window during the phase 1 IKE negotiations and the phase 2 IPSec negotiations.

From the Windows desktop system tray:

- 1 Right-click the **Mobile User VPN** client icon.
- 2 Select **Connection Monitor**.

The Connection Monitor window appears.

An icon appears to the left of the connection name:

- SA tells you that the connection only has a phase 1 SA. A phase 1 SA is assigned in these situations:
 - for a connection to a secure gateway tunnel
 - when a phase 2 SA connection has not been made at this time
 - when a phase 2 SA connection cannot be made
- A key tells you that the connection has a phase 2 SA. This connection can also have a phase 1 SA.
- An animated black line below a key tells you that the client is sending or receiving secure IP traffic.
- A single SA icon with more than one key icon above it shows a single phase 1 SA to a gateway that protects more than one phase 2 SAs.

The ZoneAlarm Personal Firewall

ZoneAlarm® Personal firewall protects your computer and network with a simple rule: Block all incoming and outgoing traffic unless you explicitly allow that traffic for trusted programs.

When you use ZoneAlarm, you frequently see New Program alert windows. This alert appears when a software application tries to get Internet or local network access. This alert stops data from your computer without your authorization.

The ZoneAlarm personal firewall includes a tutorial after the MUVPN client is installed. Read the tutorial to learn how to use this software application.

For more information about the features and configuration of ZoneAlarm, use the ZoneAlarm help system. To get access to the help system, select **Start > Programs > Zone Labs > ZoneAlarm Help**.

Allowing traffic through ZoneAlarm

When a software application tries to get access through the ZoneAlarm personal firewall, a New Program alert appears. This alert tells the user the name of the software application. This can cause confusion for users.

To let a program get access to the Internet each time the software application is started, select the **Remember the answer each time I use this program** check box.

Here is a list of some programs that must go through the ZoneAlarm personal firewall when you use their associated software applications.

Programs That Must Be Allowed


MUVPN client	IrelKE.exe MuvpnConnect.exe
MUVPN Connection Monitor	CmonApp.exe
MUVPN Log Viewer	ViewLog.exe

Programs That Can be Allowed

MS Outlook	OUTLOOK.exe
MS Internet Explorer	IEXPLORE.exe
Netscape 6.1	netscp6.exe
Opera Web browser	Opera.exe
Standard Windows network applications	Isass.exe services.exe svchost.exe winlogon.exe

Shutting down ZoneAlarm

From the Windows desktop system tray:

- 1 Right-click the ZoneAlarm icon shown at right. 
- 2 Select **Shutdown ZoneAlarm**.
The ZoneAlarm window appears.
- 3 Click **Yes**.

Uninstalling ZoneAlarm

From the Windows desktop:

- 1 Select **Start > Programs > Zone Labs > Uninstall ZoneAlarm**.
The Confirm Uninstall dialog box appears.
- 2 Click **Yes**.
The ZoneLabs TrueVector service dialog box appears.
- 3 Click **Yes**.
The Select Uninstall Method window appears.
- 4 Make sure **Automatic** is selected and then click **Next**.
- 5 Click **Finish**.

NOTE

The Remove Shared Component window can appear. During the initial installation of ZoneAlarm, some files were installed that can be shared by other programs on the system. Click Yes to All to completely remove all of these files.

- 6 The Install window appears and gives you a prompt to restart the computer. Click **OK** to restart.

Using MUVPN on the Edge Wireless Network

You must protect your wireless network from unauthorized access because the signal can go out of your building. If you do not protect your network, unauthorized users can break into your network or make use of your Internet connection.

Some wireless network cards cannot use the stronger Wi-Fi Protected Access (WPA) encryption and instead use weaker Wired Equivalent Privacy (WEP) to secure the data that goes through the airwaves.

You can increase the security of your wireless network when you make the wireless computer users authenticate as MUVPN clients. This makes the Firebox® X Edge restrict traffic through the firewall unless the wireless computer has connected using an MUVPN tunnel.

To make sure wireless computers authenticate as MUVPN clients:

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`.
- 2 From the navigation bar, select **Network > Wireless**.
- 3 Select the check box **Require encrypted MUVPN connections for wireless clients**.
- 4 Click **Submit**.

Now you must decide which networks the wireless computers can connect with. When the wireless computers must authenticate as MUVPN clients, you can allow the computers to connect to:

Trusted network only

The wireless MUVPN client cannot connect to the Internet, the computers on the optional network, or any other network that the Edge has a connection to.

All networks

This is the usual configuration for wireless MUVPN clients. The wireless MUVPN client can connect to:

- The trusted network
- The optional network
- Networks behind static routes
- Networks on the other side of a Branch Office VPN
- The external network (usually the Internet)

You can configure some Firebox users to connect only to the trusted network, and other Firebox users to connect to all networks:

- 1 To allow a Firebox user to only connect to the trusted network, do not select the check box **All traffic uses tunnel (0.0.0.0/0 IP Subnet)** in the Firebox user's MUVPN setup.
- 2 To allow a Firebox user to connect to all networks through the VPN tunnel, select the check box **All traffic uses tunnel (0.0.0.0/0 IP Subnet)** in the Firebox user's MUVPN setup.

To make wireless computers authenticate as MUVPN clients:

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: **https://192.168.111.1**.
- 2 From the navigation bar, select **Network > Wireless**.
- 3 Select the check box **Require encrypted MUVPN connections for wireless clients**.
- 4 Click **Submit**.

Tips for Configuring the Pocket PC

WatchGuard does not supply a Mobile User VPN software package for the Pocket PC. You must use the software manufacturer's instructions to configure their software and the Pocket PC.

The Firebox® X Edge only allows connections that use IPSec. The Edge does not support PPTP VPN tunnels.

Here are some configuration tips for the Pocket PC.

Phase 1 configuration of the Pocket PC's VPN software

- The Pocket PC's "IPSec Peer Gateway Address" must be the Edge's external IP address if the Pocket PC is connecting from the Internet.
- The IPSec Peer Gateway Address must be the Edge's private IP address if the Pocket PC is connecting from the optional or trusted network.
- The Phase 1 ID type must be "ID_USER_FQDN".
This is also known as the IKE ID by some ISPs. The ID Type can also be known as the "Fully Qualified Username" or "User Name".
- The Phase 1 ID must be the Firebox user's name.
- You must use Aggressive Mode, not Main Mode.
- Extended authentication is not supported on the Firebox X Edge.
- Certificates are not supported on the Edge.
- NAT-Traversal is supported on the Edge.
You could have to disable NAT-Traversal on the Pocket PC because of differences in how this protocol is implemented.
- IKE-Config Mode is supported on the Edge.
Some IPSec software providers call this IKE Mode-Configuration.
- Phase 1 encryption type can be set to DES or 3DES. The Edge uses DES as the default encryption.
- Phase 1 authentication type can be set to SHA1-HMAC or MD5-HMAC. The Edge uses SHA1-HMAC as the default authentication.
- The Diffie-Hellman Group can be set to Group 1 or 2. The Edge uses Group 1 as the default value.
- The Edge accepts most Phase 1 time-out values.

Phase 2 configuration of the VPN

- The encryption algorithm and the authentication algorithm are configured in the Firebox User account settings, on the **MUVPN** tab.
- The IPSec Phase 2 time-outs are configured in the Firebox User account settings, on the **MUVPN** tab.

- The remote user's virtual IP address is configured in the Firebox User account settings, on the **MUVPN** tab. The virtual IP address must be an IP address from the Edge's trusted or optional network that is not being used.
- The Firebox X Edge does not support compression.
- By default, the network that the Edge allows encrypted traffic to is the trusted network.
The default trusted network is 192.168.111.0/24, or 192.168.111.0 with subnet mask 255.255.255.0
- If all traffic from the Pocket PC must flow through the VPN, select the check box **All traffic uses tunnel (0.0.0.0/0 IP Subnet)** in the Firebox user's MUVPN setup.

Troubleshooting Tips

Get more information about the MUVPN client from the WatchGuard Web site:

www.watchguard.com/support

Here are the answers to some frequently asked questions about the MUVPN client:


My computer hangs immediately after installing the MUVPN client.

This can be caused by one of two problems:

- The ZoneAlarm personal firewall software application is stopping usual traffic on the local network.
- The MUVPN client is active and is not able to create VPN tunnels.

When the MUVPN client is not in use, ZoneAlarm and the MUVPN client must be set to be not active.

From the Windows desktop system tray:

- 1 Restart your computer.
- 2 Right-click the MUVPN client icon and select **Deactivate Security Policy**.
The MUVPN client icon with a red bar appears to show that the security policy is not active.
- 3 Right-click the ZoneAlarm icon shown at right. 

- 4 Select **Shutdown ZoneAlarm**.
The ZoneAlarm dialog box appears.
- 5 Click **Yes**.

I must enter my network login information even when I am not connected to the network.

When you start your computer, you must type your Windows network user name, password, and domain. It is very important that you type this information correctly. Windows keeps this information for use by network adapters and network applications. When you connect through the MUVPN client, your computer uses this information to connect to the company network.

I am not asked for my user name and password when I turn my computer on.

The ZoneAlarm personal firewall application can cause this problem. This program is very good at what it does. ZoneAlarm keeps your computer secure from unauthorized incoming and outgoing traffic. It can also prevent your computer from sending its network information. This prevents your computer from sending the login information. Make sure you turn off ZoneAlarm each time you disconnect the MUVPN connection.

Is the MUVPN tunnel working?

The MUVPN client icon appears in the Windows desktop system tray when the software application is started. The MUVPN client shows a key in the icon when the client is connected.

To test the connection, ping a computer on your company network.

- Select **Start > Run** and then type `ping` and the IP address of a computer on your company network.

My mapped drives have a red X through them.

Windows NT and 2000 examine and map network drives automatically when the computer starts. Because you cannot create a remote session with the company network before the computer starts, this procedure fails, which causes a red X to appear on the drive icons. To correct this problem, start a MUVPN tunnel and open the network drive. The red X for that drive disappears.

How do I map a network drive?

Because of a Windows operating system limitation, mapped network drives must be mapped again when you work remotely. To map a network drive again from the Windows desktop:

- 1 Right-click **Network Neighborhood**.
- 2 Select **Map Network Drive**.
The Map Network Drive window appears.
- 3 Use the drop-down list to select a drive letter.
Select a drive from the drop-down list or type a network drive path.
- 4 Click **OK**.

The mapped drive appears in the My Computer window. Even if you select the **Reconnect at Logon** check box, the mapped drive appears when you start your computer only if the computer is directly connected to the network.

I am sometimes prompted for a password when I am browsing the company network.

Because of a Windows networking limitation, remote user VPN products can allow access only to a single network domain. If your company has more than one network connected together, you can only browse your own domain. If you try to connect to other domains, a password prompt appears. Unfortunately, even if you give the correct information, you cannot get access to these other networks.

It takes a very long time to shut down the computer after using the MUVPN client.

If you get access to a mapped network drive during an MUVPN session, the Windows operating system does not shut down until it gets a signal from the network.

I lost the connection to my ISP, and now I cannot use the company network.

If your Internet connection is interrupted, the connection to the MUVPN tunnel could stop. Follow the procedure to close the tunnel. Reconnect to the Internet. Restart the MUVPN client.

Managing the Firebox and User Accounts

The Firebox® X Edge includes tools you can use to manage your network and your users. You can:

- Examine current users and properties
- Configure user profiles and customize user accounts
- Apply upgrades to the Edge and activate new features
- Examine the current configuration file in a text format

Seeing Current Sessions and Users

A session is created when traffic goes from a computer on the trusted or optional network to a computer on the external network. A session is also created when a connection is made from a computer on the trusted or optional network to the Firebox® X Edge. For example, when a user on your trusted network opens a browser to connect to a Web site on the Internet, a session starts on the Firebox X Edge. When a user on the trusted or optional network authenticates to the Edge, a session starts on the Edge.

NOTE

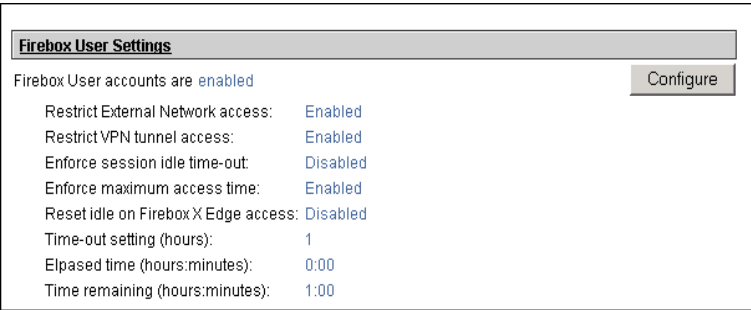
Only sessions from computers on the Edge's trusted or optional network to computers on the external network use a seat license. For more information on seat licenses, see "About Seat Licenses" on page 196.

On the Firebox Users page, you can see information about sessions in the **Active Sessions** section. You can also see information on the users that you configured for this Edge.

- 1 To connect to the System Status page, type **https://** in the browser address bar, with the IP address of the Edge trusted interface.
The default URL is: https://192.168.111.1.
- 2 From the navigation bar, select **Firebox Users**.
The Firebox Users page appears.

Firebox Users Settings

Below **Firebox Users Settings**, you can see the current values for all global user and session settings. Click the **Configure** button to open the Settings page. For more information, see "Changing authentication options for all users" on page 188 and "Configuring MUVPN client settings" on page 190.



Active Sessions

Below **Active Sessions**, the page shows information for all current sessions:

- The name of the user who started the session
- The total length of time of the session

- The time between the last packet and the session expiration is known as the idle time. If you set the idle time for a Firebox user to 0 hours and 0 minutes, the Firebox does not disconnect the session.

Active Sessions

Active session total is 0. Count of sessions occupying user licenses is 0 (maximum is 15).
The following sessions are currently active on this Firebox.

User	Host	On-line Time	Idle Timeout	License	Close
------	------	--------------	--------------	---------	-------

Close All

Stopping a session

To stop an active session, click the **X** for the session. A dialog box appears. Click **Yes** to stop the session. To stop all active sessions, click **Close All**.

Active Sessions

Active session count is 0 (maximum is 5).
The following sessions are currently active on this Firebox.

User	Host	On-line Time	Idle Timer Expiration	Close
admin	10.168.3.90	3 hr: 11 min	0 hr: 0 min	

Close All

- The user can log out manually by clicking the **Logout** button on the **Login Status** dialog box. If the user clicks this button, the **Login Status** dialog box closes, and a warning dialog box appears. The procedure is not complete until the user closes all open browser windows.









When a session closes, the seat license is available for a different user. For more information on seat licenses, see “About Seat Licenses” on page 196.

Local User Accounts

Below **Local User Accounts**, you can see information on the users you configured to use this Edge:







- **Name** -- The administrator account appears first in the list. Other users appear in alphanumeric sequence.

- **Admin Level** -- You can set the user permissions to Full, None, or Read-only. For more information, see “Adding or Editing a User Account,” on page 190.
- **Options** -- You can configure a user to use WebBlocker or MUVPN.

Local User Accounts							
The following local user accounts have been defined for this Firebox.						Add...	
Name	Internet Access	Admin Level	WebBlocker	MUVPN	VPN	Edit	Delete
admin	Allow	Full	No WebBlocker	Enabled	Allow		
cfgview	Allow	Read Only	No WebBlocker	Enabled	Allow		
muvpn	Allow	None	No WebBlocker	Enabled	Allow		
user	Allow	None	restricted	Enabled	Allow		







Editing a user account

To edit a user account, click the **Edit** icon. For descriptions of the fields you can configure, see “Adding or Editing a User Account,” on page 190.

Local User Accounts							
The following local user accounts have been defined for this Firebox.						Add...	
Name	Internet Access	Admin Level	WebBlocker	MUVPN	VPN	Edit	Delete
admin	Allow	Full	None	Disabled	Allow		
testuser	Allow	None	None	Disabled	Allow		
scarlson	Allow	Full	None	Disabled	Allow		

Deleting a user account

To remove a user account, click the **X** for the account. A dialog box appears. Click **Yes** to remove the account.

Local User Accounts							
The following local user accounts have been defined for this Firebox.						Add...	
Name	Internet Access	Admin Level	WebBlocker	MUVPN	VPN	Edit	Delete
admin	Allow	Full	None	Disabled	Allow		
testuser	Allow	None	None	Disabled	Allow		
scarlson	Allow	Full	None	Disabled	Allow		

About User Authentication

The Firebox® X Edge uses advanced authentication options to increase network security. There are options to prevent connections to some resources and to help decrease the number of seat licenses necessary. This section gives information on how a user can authenticate to the Edge, how your users and administrators can close an active session, and which options are available to customize authentication.

Three levels of Administrative Access are available for the Edge:

- **None** -- Use this to connect to resources on the external network. A user who uses this access level cannot see or change the Edge configuration pages.
- **Read-Only** -- Use this to see Edge configuration properties and status. A user who uses this access level cannot change the configuration file.
- **Full** -- Use this to see and to change Edge configuration properties. You can also activate options, disconnect active sessions, restart the Edge, and add or edit user accounts. A user who uses this access level can change the passphrase for all user accounts.

Authenticating to the Edge

When you authenticate to the Edge, it automatically identifies your Administrative Access level. The authentication procedure is the same for all users.

- 1 Open a Web browser.
You can use Netscape Navigator or Microsoft Internet Explorer. It is possible to use the Edge with other Web browsers, but we do not support them.
- 2 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 3 A security dialog box appears. You must accept the warning before you can go on.

NOTE

If your Web browser is configured to block pop-up windows, it is possible that some dialog boxes used by the Edge will not appear.

This includes dialog boxes used by wizards, and the dialog box used to log in to the Edge.

When you authenticate to the Edge, one of two screens appears. A user with Read-Only or Full Administrative Access sees the Firebox X Edge System Status page. A user with Administrative Access set to None sees a dialog box with an authentication status message.

When you authenticate to the Edge, your user name appears in the **Active Sessions** section of the Firebox Users page.

Changing authentication options for all users

Some authentication options apply to all users. To change authentication options:

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 2 From the navigation bar, select **Firebox Users > Settings**.
The Settings page appears.
- 3 Use the definitions below to help you change your parameters.
Click **Submit**.

Firebox Users
Settings

Firebox User Access Restriction Enforcement and Options

☐ Require user authentication (enable local user accounts).

- ☒ Enforce External Network access restrictions.
- ☒ Enforce VPN tunnel access restrictions.
- ☒ Enforce idle time-out.
- ☒ Enforce maximum access time.
- ☒ Reset idle timer on Firebox X Edge embedded Web site access.

☐ Enable automatic session termination every

Firebox User Common MUVPN Client Settings

The following settings apply to all MUVPN clients.

☐ Make the MUVPN client security policy read-only.

Virtual Adapter

DNS Server Address [optional]

WINS Server Address [optional]

- **Require User Authentication** – You must select this check box to use the authentication options.
- **External Network Access Restrictions** – Enable this check box if it is necessary for your users to authenticate before they connect to computers on the external network. The external network is frequently the Internet.
- **VPN Tunnel Access Restrictions** – Enable this check box if it is necessary for your users to authenticate before they can connect to computers on different network through a Branch Office VPN tunnel.
- **Idle Time-Out** – When the user does not send traffic to the external network or to the Edge for the length of the idle time-out, the Edge closes the session.
- **Maximum Access Time** – You can configure the Edge to close a session after a specified interval. Use this option to prevent users from browsing the Internet for long periods of time. When a user authenticates to the Edge, the clock starts on the session. After the specified interval, the user must authenticate again or the Edge closes the session.
- **Reset Idle Timer on Embedded Web Site Access** – If this check box is selected, the Edge does not disconnect a session when an idle time-out occurs if the **Login Status** dialog box is on the desktop. Disable this check box to override the **Login Status** dialog box.

The Login Status box sends traffic to the Edge from the user's computer each two minutes. If you enable this check box, the Edge resets the idle timer to zero each time the Edge receives traffic from the Login Status box.

- **Automatic Session Termination** – This is a global property that applies to all sessions and that overrides all other authentication options. It lets you clear the list of seat licenses in use and make them available again. Enable this check box to disconnect all sessions at the specified time in the drop-down list.

All sessions will be disconnected at the same time. The time limit is the number of hours since the Edge first starts up, not the length of time a session has been active.

Configuring MUVPN client settings

The MUVPN client settings apply to all MUVPN connections to the Edge. To configure MUVPN client settings:

- 1 Use your browser to connect to the System Status page. From the navigation bar, select **Firebox Users > Settings**. The Settings page appears.
- 2 If necessary, use the scroll bar to scroll to the **Firebox User Common MUVPN Client Settings** section.
- 3 You can lock the MUVPN client security policy (.wgx file) to prevent a change to it. Select the **Make the MUVPN client security policy read-only** check box.
- 4 The remote MUVPN computers can use a virtual adapter to get network settings, an IP address, and WINS and DNS address assignments. You can set the virtual adapter rule for your mobile users to:

Disabled

The mobile user does not use a virtual adapter to connect with the MUVPN client. This is the default value.

Preferred

If the virtual adapter is in use or is not available, the mobile user does not use a virtual adapter to connect with the MUVPN client.

Required

The mobile user must use a virtual adapter to connect with the MUVPN client.

- 5 You can also enter a WINS Server address and DNS Server address. Type the server IP addresses in the related field.
For more information on configuring the Mobile User VPN client computer, see Chapter 10, "Configuring the MUVPN Client."

Adding or Editing a User Account

When you create a Firebox user for the Firebox® X Edge, you select the Administrative Access level for that user. You select access control for the external network and the Branch Office VPN tunnel, and

time limits on this access. You can also apply a WebBlocker profile to the user account and configure the user's MUVPN restrictions.

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: https://192.168.111.1.
- 2 From the navigation bar, select **Firebox Users**.
The Firebox Users page appears.
- 3 Below **Local User Accounts**, click **Add**.
The New User page appears. It shows the Settings tab.

Firebox Users
New User

Settings WebBlocker MUVPN

Account Name
Full name
Description
Password
Confirm password
Administrative Access None
Session maximum time-out (minutes)
Session idle time-out (minutes)
☒ Allow access to the External Network
☒ Allow access to VPN

Submit Reset

- 4 In the **Account Name** field, type a name for the account. The user types this name when authenticating.
The account name is case-sensitive.
- 5 In the **Full Name** field, type the first and last name of the user.
This is for your information only. A user does not use this name during authenticating.
- 6 In the **Description** field, type a description for the user.
This is for your information only.

- 7 In the **Password** field, type a password with a minimum of eight characters.
Mix eight letters, numbers, and symbols. Do not use a word you can find in a dictionary. For increased security use a minimum of one special symbol, a number, and a mixture of uppercase and lowercase letters.
- 8 Type the password again in the **Confirm Password** field.
- 9 In the **Administrative Access** drop-down list, set the level to which your user can see and change the Edge configuration properties: None, Read-Only, or Full.

NOTE

If you have Read-Only or Full access, the Edge's configuration pages appear when you authenticate to the Edge. If you have an Administrative access of None, the Login Status dialog box appears when you authenticate to the Edge. If you have Read-Only or Full access, you can click on the Authenticate User link at the bottom of the navigation pane on the left to open the Login Status dialog box.

For more information, see "Creating a read-only administrative account," on page 193.

- 10 In the **Session maximum time-out** field, set the maximum length of time the computer can send traffic to the external network or across a Branch Office VPN tunnel. If this field is set to zero minutes, there is no session time-out and the user can stay connected for any length of time.
You can also apply a global "Maximum session timeout" to all users. The global setting overrides the individual Firebox User setting. For more information, see "Changing authentication options for all users" on page 188.
- 11 In the **Session idle time-out** field, set the length of time the computer can stay authenticated when it is idle (not passing any traffic to the external network or across the Branch Office VPN or to the Firebox X Edge itself). A setting of zero minutes means there is no idle time-out.
- 12 If you want this user to have Internet access, select the **Allow access to the External Network** check box.
- 13 If you want this user to have access to computers on the other side of a Branch Office VPN tunnel, select the **Allow access to VPN** check box.
- 14 Click **Submit**.

Creating a read-only administrative account

You can create a local user account with access to view Firebox configuration pages. When you log in as a read-only administrator, you cannot:

- Click the **Reboot** button on the System Status page.
- Change the configuration mode on the External page.
- Click the **Reset Event Log** and **Sync Time with Browser Now** buttons on the Logging page.
- Click the **Synchronize Now** button on the System Time page.
- Click the **Regenerate IPSec Keys** button on the VPN page.
- Change the configuration mode on the Managed VPN page.
- Click the **Launch Wizard** button from the Wizard page.

If you try to do these things, you get a message tell you that you have read-only access and cannot change the configuration file.

To create a read-only user account, edit the user account. Use the **Administrative Access** drop-down list to select **Read Only**.

Setting a WebBlocker profile for a user

A WebBlocker profile is a unique set of restrictions you can apply to users on your network. To apply a WebBlocker profile to a user's account, click the **WebBlocker** tab and select a profile from the drop-down list. You must first create WebBlocker profiles in the **WebBlocker > Profiles** area of the Edge's configuration pages. For more information on WebBlocker profiles, see "Creating WebBlocker Profiles" on page 121.

Enabling MUVPN for a user

To enable MUVPN for a new user, see "Connecting and Disconnecting the MUVPN Client" on page 169.

The Administrator account

The Firebox X Edge has a built-in administrator account that cannot be deleted. You can change some of the administrator account settings. On the Firebox Users page, click the icon in the **Edit** column of the administrator account.

For descriptions of the fields, see the section, "Adding or Editing a User Account" on page 190.

Make sure you keep the administrator name and password in a safe location. You must have this information to see the configuration pages. If the system administrator name and password are not known, you must reset the Firebox to the factory default configuration. For more information, see “Resetting the Firebox to the factory default settings” on page 41.

We recommend that you change the administrator passphrase monthly. Use a passphrase of eight letters, numbers, and symbols. Do not use an English or foreign word. Use one or more symbols, a number, and a mixture of upper case and lower case letters for increased security.

Stopping a session

The Edge uses a session when it allows a computer on the trusted interface to make a connection to a computer on the external interface. The Edge stops the session when one of these events occurs:

- If Firebox user authentication is necessary for external network connections, the Edge releases the session after the idle time-out limit set for that account.
- If Firebox user authentication is necessary for external network connections, the Edge releases the session after the maximum time limit set for that account.
- If Firebox user authentication is necessary for external network connections, the Edge releases the session when the Firebox user manually stops the session. To stop the session, the user closes the **Login Status** box and all other browser windows.
- If the Edge administrator uses the Firebox Users page to stop a session, the Edge releases that session.
- If the Automatic Session Termination time limit for all sessions is reached, the Edge releases all sessions at one time.
- If the Edge restarts, all sessions are released.

To end a session manually:

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 2 From the navigation bar, select **Firebox Users**.
The Firebox Users page appears.

- 3 Find the session in **Active Sessions** list. Click the **Close** button.
To end all sessions, click the **Close All** button.

For more information, see the FAQ:

[https://www.watchguard.com/support/AdvancedFaqs/
edge_seatlicense.asp](https://www.watchguard.com/support/AdvancedFaqs/edge_seatlicense.asp)

License upgrades are available from your reseller or from the Watch-Guard Web site:

<http://www.watchguard.com/sales/buyonline.asp>

Changing a user account name or password

You can change an account name or account password. You cannot change them both. If you change the account name, you must give the account password.

- 1 To connect to the System Status page, type <https://> in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: <https://192.168.111.1>.
- 2 From the navigation bar, select **Firebox Users**.
The Firebox Users page appears.
- 3 Below **Local User Accounts**, click **Edit** for the account to change the password for.
The Edit User page appears with the Settings tab visible.
- 4 Click **Change Identification**.
- 5 Type the old password and a new password. Confirm the new password.
- 6 Click **Submit**.

The screenshot shows the 'Firebox Users' management interface. At the top, it says 'Edit User: cfgview'. Below this are three tabs: 'Settings' (selected), 'WebBlocker', and 'MUVPN'. The 'Settings' tab contains the following fields and controls:

- Account Name: `cfgview`
- Full name: `Able to view Config`
- Description: `Read not write`
- A button labeled 'Change Identification' is positioned below the description field.
- Administrative Access: A dropdown menu currently showing 'Read Only'.
- Session maximum time-out: `0` (minutes)
- Session idle time-out: `0` (minutes)
- Two checked checkboxes: 'Allow access to the External Network' and 'Allow access to VPN'.
- At the bottom are two buttons: 'Submit' and 'Reset'.

About Seat Licenses

The Firebox® X Edge is enabled with a specified number, or “pool,” of seat licenses. The number of seat licenses puts a limit on how many users can get out to the Internet at one time. The total number of available seat licenses in the pool is set by the Edge model you have and any upgrade licenses you apply.

The Firebox Users page (below **Active Sessions**) shows how many active sessions there are, and how many of those sessions use seat licenses. This page also shows the maximum number of seat licenses allowed.

An active session does not always use a seat license. You only use a seat license when you send traffic from the trusted or optional network to the external network. You do not use a seat license when you make connections between computers on the trusted network. You also do not use a seat license when you make connections through a VPN tunnel. Because you cannot connect to the external network, you create an active session, but do not use a seat license. If you make users authenticate before they connect to the external network, you can make sure that no seat licenses are used by unauthorized computers. If authentication is required, and a user or com-

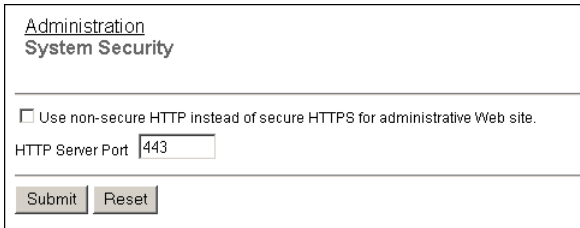
puter tries to connect to the external network without authenticating, the Edge does not allow the connection. A seat license is used only when a user is allowed to connect from the trusted or optional network to the external network.

Selecting HTTP or HTTPS for Management

HTTP (Hypertext Transfer Protocol) is the “language” used to move files (text, graphic images, and multimedia files) on the Internet. HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) is a more secure version of HTTP. It encrypts and decrypts the Web pages sent to your browser and your browser encrypts the information sent with HTTPS. For better security, the Firebox X Edge uses HTTPS by default.

If your browser does not support HTTPS, or to make the Edge HTML configuration pages load faster, you can configure the Edge to use HTTP instead of HTTPS. When you use HTTP, all configuration changes are sent to the Edge from your computer in unencrypted text. Follow these instructions to use less secure HTTP instead of HTTPS:

- 1 Type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`.
- 2 From the navigation bar, select **Administration > System Security**.
The System Security page appears.



Administration
System Security

☐ Use non-secure HTTP instead of secure HTTPS for administrative Web site.

HTTP Server Port

- 3 Select the **Use non-secure HTTP instead of secure HTTPS for administrative Web site** check box.
- 4 Click **Submit**.

If you select this check box, you must use `http://` in the browser's address bar to bring up configuration pages instead of the default `https://`.

Changing the HTTP Server Port

To connect to the Firebox® X Edge to see the configuration pages, or for a user to authenticate to the Edge, the browser's connection must use the same port as the Edge's HTTP server port. Because HTTPS uses TCP port 443 (HTTP uses TCP port 80), the default HTTP server port for the Edge is 443.

To change the port over which you communicate with the Firebox X Edge, type a new value in the **HTTP Server Port** field in the System Security configuration page shown above.

For more information on using HTTP or HTTPS with the Edge and changing the HTTP Server Port, see the FAQ:

https://www.watchguard.com/support/advancedfaqs/edge_httpserverport.asp

Setting up WatchGuard System Manager Access

Use the VPN Manager Access page to allow your Firebox® X Edge to be remotely managed by WatchGuard System Manager. It also enables:

- If you are using WatchGuard System Manager 7.3 or a version released before 7.3, it enables the Edge to be managed by VPN Manager.
- If you are using WatchGuard System Manager 8.0 or later, it enables the Edge as a managed Firebox client of a WatchGuard Management Server.

Follow these instructions to configure WatchGuard System Manager access:

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.

The default URL is: `https://192.168.111.1`

- 2 From the navigation bar, select **Administration >VPN Manager Access**.
The VPN Manager Access page appears.

Administration
VPN Manager Access

☒ Enable VPN Manager Access

Status Passphrase

Confirm Status Passphrase

Configuration Passphrase

Confirm Configuration Passphrase

☒ Enable interoperability with VPN Manager v7.0, v7.1, and v7.2

- 3 Select the **Enable VPN Manager Access** check box.
- 4 Type a status passphrase for your Firebox X Edge and then type it again to confirm in the correct fields.
- 5 Type a configuration passphrase for your Firebox X Edge and then type it again to confirm in the correct fields.

NOTE

These passphrases must match the passphrases you use when you add the device to WatchGuard System Manager, VPN Manager, or the WatchGuard Management Server software or the connection will fail.

- 6 Select the **Enable interoperability with VPN Manager v7.0, v7.1, and v7.2** button if you want to use WatchGuard System Manager 7.0, 7.1, or 7.2 to manage your Edge.
- 7 Click **Submit**.

Updating the Firmware

See the WatchGuard web site regularly for Firebox® X Edge updates:
<https://www.watchguard.com/support/sohoresources>

There are two different methods for installing firmware updates. The first method uses a larger download and applies the firmware

update on the Firebox X Edge automatically when you start it on a Windows computer. The second method uses a smaller download and allows you to apply the firmware updates with the Firebox X Edge configuration pages. If you do not use Windows, install the update with the second procedure.

Method 1

The first method uses an executable file and is the preferred method for installing the Firebox X Edge firmware update from a Windows computer. Download the Software Update Installer to use this method. To use the Software Update Installer:

- 1 Start the installer on a computer operating Windows that is on the trusted network of the Firebox X Edge.
- 2 The installer gives a prompt for an IP address, a user name and password. Type the Firebox X Edge's trusted interface IP address.
The default address is 192.168.111.1
- 3 Type the administrator name and password. Click **OK**.
The installer applies the firmware update to the Firebox X Edge. As part of the update process, the Firebox X Edge restarts one or two times — this is usual.
- 4 When the **Finish** button appears, click it.

NOTE

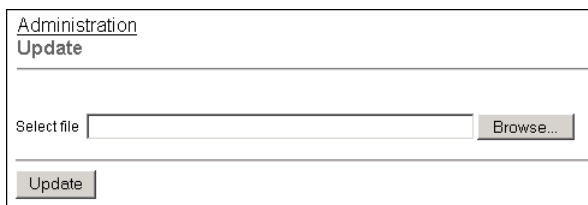
Because the Installer uses FTP to transfer files, make sure your Firebox X Edge is not configured to deny FTP access, as described in "Denying FTP access to the trusted network interface" on page 106.

Method 2

The second method uses the Firebox X Edge configuration pages. This method can be used with Windows or other operating systems.

You must first download the Software Update file, which is a small Zip file.

- 1 Extract the “wgrd” file from the Zip file you downloaded using an archiving utility such as Winzip (for Windows computers), StuffIt (for Macintosh), or Linux archive capabilities.
- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: <https://192.168.111.1>
- 2 From the navigation bar, select **Administration > Update**.
The Update page appears.
- 3 Type the name of the file containing the new Firebox X Edge software in the **Select file** box. Or click **Browse** to find the file on the network.
- 4 Click **Update** and follow the instructions.



Administration Update	
Select file	<input type="text"/> <input data-bbox="705 841 803 868" type="button" value="Browse..."/>
<input data-bbox="243 898 323 925" type="button" value="Update"/>	

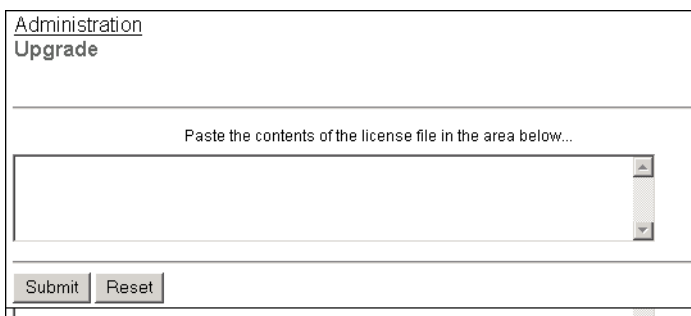
Activating Upgrade Options

All Firebox® X Edge devices include the software for all upgrade options. These options are activated when you install a license key on the Firebox. To get a license key, purchase and activate an upgrade option at the LiveSecurity service Web site or from a WatchGuard-authorized reseller. See “Registering and Activating LiveSecurity Service” on page 25 for more information.

After you have purchased an upgrade option, follow these steps to activate it:

- 1 Go to the upgrade page of the WatchGuard Web site:
<http://www.watchguard.com/upgrade>

- 2 Type your LiveSecurity Service user name and password in the fields provided.
- 3 Click **Log In**.
- 4 Use the instructions on the Web site to activate your license key and to get the feature key.
- 5 Copy the feature key from the LiveSecurity Service Web site.
- 6 To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 7 From the navigation bar, select **Administration > Upgrade**.
The Upgrade page appears.



Administration
Upgrade

Paste the contents of the license file in the area below...

Submit Reset

- 8 Paste the feature key in the applicable field.
- 9 Click **Submit**.

Upgrade options

User licenses

A seat license upgrade allows more connections between the trusted network and the external network. For example, a 5-seat user license upgrade allows five more connections to the external network than the base model with no licenses applied.

MUVPN Clients

The MUVPN Clients upgrade allows remote users to connect to the Firebox X Edge through a secure (IPSec) VPN tunnel. These users have access to trusted network resources.

WebBlocker

The WebBlocker upgrade enables you to control access to Web content. For more information on WebBlocker, see Chapter 8, “Configuring WebBlocker.”

WAN Failover

The WAN failover feature adds redundant support for the external interface. For more information, see “Enabling the WAN Failover Option” on page 68.

Enabling the Model Upgrade Option

A model upgrade gives the Firebox® X Edge the same functions as a higher model. A model upgrade increases speed, capacity, user licenses, sessions, and VPN tunnels. For a brochure that shows the capacities of the different Firebox X Edge models, go to: http://www.watchguard.com/docs/datasheet/edge_ds.asp

You can upgrade an X5 or an X15 to a higher model.

- 1 Go to the upgrade site on the WatchGuard Web site (www.watchguard.com/upgrade) and log into your LiveSecurity Service account.
- 2 In the space provided, type the license key as it appears on your printed certificate or your online store receipt, including hyphens. Click **Continue** and use the instructions.

Configuring Additional Options

Some Firebox® X Edge options are included with your Firebox, but are disabled in the default configuration. To use these features, you must enable and configure them. These options are as follows:

Managed VPN

The managed VPN feature allows you to set up VPN tunnels using a WatchGuard Management Server. For more information, see Chapter 8, “Configuring VPNs.”

Manual VPN

The manual VPN feature allows you to set up VPN tunnels manually. For more information, see Chapter 8, “Configuring VPNs.”

Viewing the Configuration File

You can see the contents of the Firebox® X Edge configuration file in text format from the View Configuration page.

- 1 To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- 2 From the navigation bar, select **Administration > View Configuration File**.

Administration

View Configuration File

```
FDATE: Jun  4 2004
FTIME: 09:19:22
FVER: 7.0.0
admin.external_access: 1
admin.halhash: e80721f9ad6f03b50e89c8a08d082dc3
admin.idle_timeout: 0
admin.ipsec_access: 1
admin.max_access: 0
admin.muvpn_access: 0
admin.name: admin
admin.pass: pass
config.version: 0.1
networking.dhcp_client.enable: 0
networking.dhcpd.enable: 0
networking.dhcpd.firstip: 192.168.111.2
networking.dhcpd.lastip: 192.168.111.252
networking.dhcpd.optional.enable: 0
networking.dhcpd.optional.firstip: 192.168.112.2
networking.dhcpd.optional.lastip: 192.168.112.252
networking.ethernet.00: eth0 192.168.54.54 192.168.54.0 255.255.255.0 192.168.54.254
networking.ethernet.00.linkspeed: 1
networking.ethernet.01: eth1 192.168.111.1 192.168.111.0 255.255.255.0 192.168.111.1
networking.ethernet.02: eth2 192.168.112.1 192.168.112.0 255.255.255.0 192.168.112.1
networking.nameservice.dhcpd.dns.0: 192.168.130.131
networking.nameservice.dhcpd.dns.1: 192.168.130.245
networking.nameservice.dhcpd.domain_suffix: wgt1.net
```


Firebox X Edge Hardware

The WatchGuard® Firebox® X Edge is a firewall for small organizations and branch offices. The WatchGuard Firebox X Edge Wireless can connect to computers with a wireless network interface card.

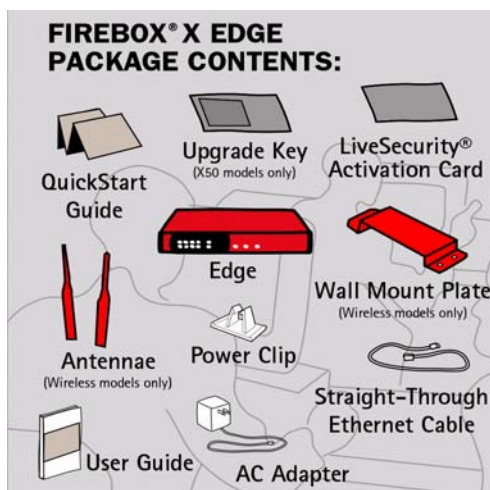


Package Contents and Specifications

The Firebox® X Edge package includes:

- A hardware firewall
- The Firebox X Edge User Guide
- The Firebox X Edge QuickStart Guide

- LiveSecurity® Service activation card
- Hardware Warranty Card
- AC adapter (12 V)
- Power cable clip, to attach to the cable and connect to the side of the Edge. This decreases the tension on the power cable.
- One straight-through cable
- Wall mount plate (wireless models only)
- Two antennae (wireless models only)



Processor	64 bit MIPS
CPU	266 MHz
Memory - Flash	16 MB
Memory - RAM	64 MB
Ethernet interfaces	10 each 10/100
Serial ports	1 DB9
Power supply	12V DC

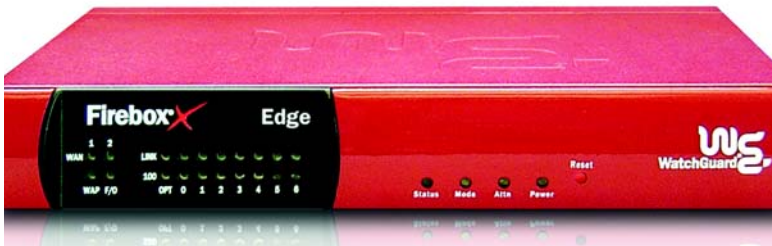
Operating Temperature	0 - 40C
Environment	Indoor use only
Dimensions	Depth = 5 inches Width = 8.75 inches Height = 1.25 inches
Weight	1.9 U.S. pounds

Hardware Description

The Firebox® X Edge has a simple hardware architecture. All indicator lights appear on the front panel while all ports and connectors are on the rear panel of the device.

Front panel

The front panel of the Firebox X Edge has 24 indicator lights to show the link status. The top indicator light in each link pair comes on when a link is made and flashes when traffic goes through the related interface. The bottom indicator light in each pair comes on when the link speed is 100 Mbps. If the bottom indicator light does not come on, the link speed is 10 Mbps.



WAN 1, 2

Shows a physical connection to the external Ethernet interfaces. The indicator light is yellow when traffic goes through the related interface.

WAP

Shows a wireless connection to the Edge. The indicator light is green when traffic goes through the wireless interface on a Firebox X Edge Wireless model.

F/O

Shows a WAN failover. The indicator light is green when there is a WAN failover from WAN1 to WAN2. The indicator light goes off when the external interface connection goes back to WAN1.

Link

The link indicator light shows a physical connection to a trusted Ethernet interface. The trusted interfaces have the numbers 0 through 6. The indicator light comes on when traffic goes through the related interface.

100

When a trusted network interface operates at 100 Mbps, the related 100 indicator light comes on. When it operates at 10 Mbps, the indicator light does not come on.

Status

Shows a management connection to the Edge. The indicator light goes on when you use your browser to connect to the Edge configuration pages. The indicator light goes off a short time after you close your browser.

Mode

Shows the status of the external network connection. The indicator light comes on when the Ethernet cable is correctly connected to the WAN1 interface. The indicator light is green if the Edge can connect to the external network and send traffic. The indicator light flashes if the Edge cannot connect to the external network and send traffic.

Attn

Reserved for future use.

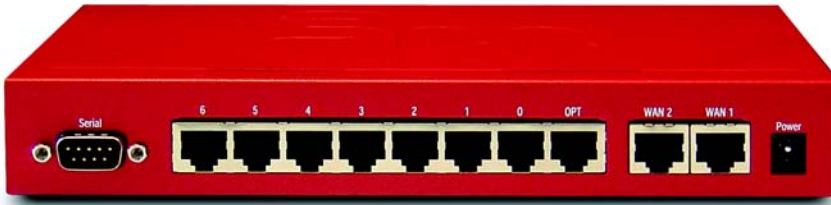
Power

Shows that the Firebox X Edge is on.

RESET button

Use the procedure to reset the Firebox X Edge to “Factory Default Settings” on page 40.

Rear view



Serial port (DB9)

Use the serial port to connect an external modem to the Edge.

Ethernet interfaces 0 through 6

The seven Ethernet interfaces with the marks 0 through 6 are for the trusted network.

OPT interface

This Ethernet interface is for the optional network.

WAN interfaces 1 and 2

The WAN1 and WAN2 interfaces are for the external network.

Power input

We supply a 12-volt AC adapter with your Edge. Connect the AC adapter to the Edge and to a power source. The power supply tip is plus (+) polarity.

Side panels

Computer Lock Slot

There is a slot for a computer lock on the two side panels of the Firebox X Edge.

Antennae (wireless model only)

There are wireless antennae on the two side panels of the Firebox X Edge Wireless models.

Wall mounting plate

The wall mounting plate enables you to put the Firebox X Edge in a good location to increase the range.

About IEEE 802.11g/b Wireless

In general, RF power and signal bandwidth create a maximum limit on the rate that data can be sent on a wireless connection. The equation below calculates the maximum data rate:

$$\text{ChannelCapacity} = \text{ChannelBandwidth} \times \log_2 \left(\frac{1 + \text{SignalStrength}}{\text{NoiseLevel}} \right)$$

This equation shows that the channel capacity (bits/s) is set by:

- Channel bandwidth: 22 Mbits/s for 802.11b and 54 Mbits/s for 802.11g
- Signal strength: 15 dBm transmitted by the Firebox X Edge Wireless
- Noise level: Set by the environmental conditions and the design of the receiver.

The maximum data rate cannot be more than the channel capacity.

Noise level

Channel capacity is decreased by increasing the noise level in the frequency range of the system. The noise level is set by many factors. First, it is affected by background noise caused by the ambient temperature of the atmosphere at the frequency range of the system. Also, the operating temperature of the components of the 802.11 g/b receiver creates noise. The primary cause of interference is transmitters which use the same frequency range:

- Cordless phones
- An 802.11b device set to use adjacent channels. We recommend that you set three channels between each adjacent wireless access points (e.g. 1, 5, and 9 or 2, 6, and 10).
- Microwave ovens
- Sodium-type lighting systems (fusion lamps)
- Arc welders (broadband spark-gap transmitters)
- Blue-Tooth transmitters (A Blue-Tooth transmitter operates at a lower power level than an 802.11b device. To cause interference, the Blue-Tooth transmitter must be very near to an 802.11b receiver.)
- Industrial, scientific, and medical equipment which can also operate in this frequency range.

Signal strength (Watts)

The signal strength is set by these factors:

- Power of the RF signal that is sent and received
- Amount of directional antenna gain at the transmitter and the receiver
- Signal attenuation (path-loss) between the transmitter and receiver

Antenna directional gain

Antenna directional gain is calculated from the degree to which the radiation pattern of an antenna is focused in a specified direction. A highly directional antenna has a higher gain.

The Firebox X Edge Wireless uses 5 dBi antennas. These antennas have a maximum 5 dBi gain pattern perpendicular to the antenna position. The antenna gain of a laptop computer with an embedded wireless antenna can be as low as -10 dBi.

Signal attenuation (path-loss)

This equation finds the signal attenuation (path-loss):

$$\text{Loss} = 20 \times \log_{10} \left(4\pi \times \frac{\text{distance}}{\text{wavelength}} \right)$$

The “distance” is the line-of-sight distance between the transmitter and the receiver.

The “wavelength” is the speed of light divided by the frequency. Higher frequency signals have a shorter wavelength. Shorter wavelength signals have a higher path-loss than signals with a higher wavelength in the same frequency range.

In a usual office environment, the calculated loss is only accurate for approximately 20 feet. For each additional 100 feet, 30 dB must be added. Furniture, walls, windows, and other objects also cause interference.

Fading because of multi-path reflections also causes signal attenuation. Multi-path reflections are the result of an RF signal moving along more than one path from the transmitter to the receiver.

Multi-path occurs when a signal is reflected by surfaces in the area. A signal with a frequency of 2.4 GHz is reflected by many surfaces. When multi-path occurs, some reflected signals cancel each other.

The signal attenuation caused by multi-path reflections is the result of how you adjust the antenna. When the receiver is moved $\frac{1}{2}$ wavelength, the signal strength changes by as much as 30 dB. To adjust for this problem, the Firebox X Edge Wireless uses “antenna receiver diversity.” In this system, the effect of multi-path fading is decreased through the use of two antennas that are spaced other than $\frac{1}{2}$ wavelength apart. The Firebox X Edge Wireless automatically selects the antenna that receives the stronger signal.

Laptop computers usually have one antenna and have signal loss because of antenna position. Because of this, the Firebox X Edge can receive signals from the laptop while the laptop does not receive signals from the Edge.

Channel bandwidth

Channel bandwidth changes when you use different modulations. Devices compliant with the 802.11b standard use the CCK (11 Mbps, 5.5 Mbps), DQPSK (2 Mbps), and DBPSK (1 Mbps) modulation schemes. 802.11g devices use OFDM. The Firebox X Edge automatically selects the modulation procedure that gives the lowest Packet Error Rate (PER). The PER is not allowed to be more than eight per-

cent. When a different modulation scheme is selected, the data rate changes.



Legal Notifications

Copyright, Trademark, and Patent Information

Copyright© 1998 - 2005 WatchGuard Technologies, Inc. All rights reserved.

WatchGuard, the WatchGuard logo, Firebox, LiveSecurity, and any other mark listed as a trademark in the "Terms of Use" portion of the WatchGuard Web site that is used herein are either registered trademarks or trademarks of WatchGuard Technologies, Inc. and/or its subsidiaries in the United States and/or other countries. All other trademarks are the property of their respective owners.

Microsoft®, Internet Explorer®, Windows® 95, Windows® 98, Windows NT®, Windows® 2000 and Windows XP are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States and other countries.

RealNetworks, RealAudio, and RealVideo are either a registered trademark or trademark of RealNetworks, Inc. in the United States and/or other countries.

Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All right reserved.

© 1995-1998 Eric Young (eay@cryptsoft). All rights reserved.

© 1998-2003 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

© 1995-2003 Eric Young (ey@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (ey@cryptsoft.com).

The implementation was written so as to conform with Netscapes' SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (ey@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The mod_ssl package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.

Copyright (c) 1998-2003 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>).

4. The names "mod_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.
5. Products derived from this software may not be called "mod_ssl" nor may "mod_ssl" appear in their names without prior written permission of Ralf S. Engelschall.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Certifications and Notices

FCC Certification

This appliance has been tested and found to comply with limits for a Class A digital appliance, pursuant to Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This appliance may not cause harmful interference.
- This appliance must accept any interference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Notice

The CE symbol on your WatchGuard Technologies equipment indicates that it is in compliance with the Electromagnetic Compatibility (EMC) directive and the Low Voltage Directive (LVD) of the European Union (EU).



Industry Canada

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

CANADA RSS-210

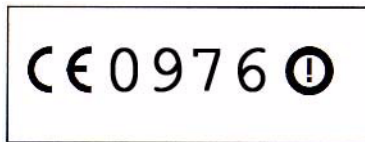
The term “IC:” before the radio certification number only signifies that Industry of Canada technical specifications were met.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

France

NOTE! En France, ce produit ne peut être installé et opéré qu'à l'intérieur, et seulement sur les canaux 10, 11, 12, 13 comme défini par IEEE 802.11g/b. L'utilisation de ce produit à l'extérieur ou sur n'importe quel autre canal est illégal en France.

NOTE! In France, this product may only be installed and operated indoors, and only on channels 10, 11, 12, 13 as defined by IEEE 802.11g/b. Use of the product outdoors, or on any other channel, is illegal in France.



Class A Korean Notice

사용자 안내문(A급 기기)
본 기기는 업무용으로 전자파적합등록을 받은 기기이오니,
만약 잘못 구입하셨을 때에는 구입한 곳에서 비업무용으로
교환 하시기 바랍니다.

VCCI Notice Class A ITE

この装置は、情報処理装置等電波障害自主規制協議会(VCCI)の基準に基づくクラス A 情報技術装置です。この装置を家庭用環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Taiwanese Notices

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

根據交通部 低功率管理辦法 規定：

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Declaration of Conformity

DECLARATION OF CONFORMITY

WatchGuard Technologies, Inc.

505 Fifth Ave. S., Suite 500
Seattle, WA 98104-3892
USA

WatchGuard Technologies Inc. hereby declares that the product(s) listed below conform to the European Union directives and standards identified in this declaration.

Product (s):

Wireless Internet Firewall with VPN, Model MF16S32E9W

EU Directive(s):

Radio & Telecommunications Terminal Equipment (1999/5/EC)

Low Voltage (73/23/EEC)

Electromagnetic Compatibility (89/336/EEC)

Standard(s):

EN60950 3rd Ed. (1999) Safety of ITE

ETSI EN 300 328-02 V1.4.1 (2003-04) EMC and Radio Spectrum Matters

ETSI EN 301 489-17 V1.1.1 (2000-09) EMC and Radio Spectrum Matters

ETSI EN 301 489-01 V1.4.1 (2002-08) EMC and Radio Spectrum Matters

EN50022 (1998), Class A Emissions for ITE

EN50024 (1998) Immunity for ITE

Signature

Full Name Edward Borey

Position Chairman, CEO

Date 30 September 2004

Limited Hardware Warranty

This Limited Hardware Warranty (the "Warranty") applies to the enclosed Firebox hardware product, not including any associated software which is licensed pursuant to a separate end-user license agreement and warranty (the "Product"). BY USING THE PRODUCT, YOU (either an individual or a single entity) AGREE TO THE TERMS HEREOF. If you do not agree to these terms, please return this package, along with proof of purchase, to the authorized dealer from which you purchased it for a full refund. WatchGuard Technologies, Inc. ("WatchGuard") and you agree as set forth below or on the reverse side of this card, as applicable:

1. LIMITED WARRANTY. WatchGuard warrants that upon delivery and for one (1) year thereafter (the "Warranty Period"): (a) the Product will be free from material defects in materials and workmanship, and (b) the Product, when properly installed and used for its intended purpose and in its intended operating environment, will perform substantially in accordance with WatchGuard applicable specifications.

This warranty does not apply to any Product that has been: (i) altered, repaired or modified by any party other than WatchGuard except for the replacement or inclusion of specified components authorized in and performed in strict accordance with documentation provided by WatchGuard; or (ii) damaged or destroyed by accidents, power spikes or similar events or by any intentional, reckless or negligent acts or omissions of any party. You may have additional warranties with respect to the Product from the manufacturers of Product components. However, you agree not to look to WatchGuard for, and hereby release WatchGuard from any liability for, performance of, enforcement of, or damages or other relief on account of, any such warranties or any breach thereof.

2. REMEDIES. If any Product does not comply with the WatchGuard warranties set forth in Section 1 above, WatchGuard will, following receipt of the product you claim is defective and at its option, either (a) repair the Product, or (b) replace the Product; provided, that you will be responsible for returning the Product and for all costs of shipping and handling. Repair or replacement of the Product shall not extend the Warranty Period. Any Product, component, part or other item replaced by WatchGuard becomes the property of WatchGuard. WatchGuard shall not be responsible for return of or damage to any software, firmware, information or data contained in, stored on, or integrated with any returned Products.

3. DISCLAIMER AND RELEASE. THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 1 AND 2 ABOVE ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN THE PRODUCT (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY WARRANTY OF NONINFRINGEMENT, ANY WARRANTY OF UNINTERRUPTED OR ERROR-FREE OPERATION, ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD OR FROM PRODUCT LIABILITY, STRICT LIABILITY OR OTHER THEORY, AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY, THE PRODUCT).

4. LIMITATION AND LIABILITY. WATCHGUARD'S LIABILITY (WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT) OR OTHER THEORY) WITH REGARD TO ANY PRODUCT WILL IN NO EVENT EXCEED THE PURCHASE PRICE PAID BY YOU FOR SUCH PRODUCT. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF ANY AGREED REMEDY. IN NO EVENT WILL WATCHGUARD BE LIABLE TO YOU OR ANY THIRD PARTY (WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT) OR OTHER THEORY) FOR COST OF COVER OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF PROFITS, BUSINESS, OR DATA) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR

THE USE OF OR INABILITY TO USE THE PRODUCT, EVEN IF WATCHGUARD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF ANY AGREED REMEDY.

5. MISCELLANEOUS PROVISIONS. This Warranty will be governed by the laws of the state of Washington, U.S.A., without reference to its choice of law rules. The provisions of the 1980 United Nations Convention on Contracts for the International Sales of Goods, as amended, shall not apply. You agree not to directly or indirectly transfer the Product or associated documentation to any country to which such transfer would be prohibited by the U.S. Export laws and regulations. If any provision of this Warranty is found to be invalid or unenforceable, then the remainder shall have full force and effect and the invalid provision shall be modified or partially enforced to the maximum extent permitted by law to effectuate the purpose of this Warranty. This is the entire agreement between WatchGuard and you relating to the Product, and supersedes any prior purchase order, communications, advertising or representations concerning the Product AND BY USING THE PRODUCT YOU AGREE TO THESE TERMS. IF THE PRODUCT IS BEING USED BY AN ENTITY, THE INDIVIDUAL INDICATING AGREEMENT TO THESE TERMS BY USING THE PRODUCT REPRESENTS AND WARRANTS THAT (A) SUCH INDIVIDUAL IS DULY AUTHORIZED TO ACCEPT THE WARRANTY ON BEHALF OF THE ENTITY AND TO BIND THE ENTITY TO THE TERMS OF THIS WARRANTY; (B) THE ENTITY HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THE WARRANTY AND PERFORM ITS OBLIGATIONS UNDER THE WARRANTY AND; (C) THE WARRANTY AND THE PERFORMANCE OF THE ENTITY'S OBLIGATIONS UNDER THE WARRANTY DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE ENTITY IS A PARTY. No change or modification of the Warranty will be valid unless it is in writing and is signed by WatchGuard.

Symbols

.wgx files
described 154
distributing 158
viewing available 33

A

Add Gateway page 143
Add Route page 64
Administration page
described 34
subpages of 34
Administrative Access levels 187
administrator account 193
Aggressive Mode 144
Allow access to the External Network check box 192
Allow access to VPN check box 192
Allowed Sites pages 125
antenna directional gain 213
authentication. See user authentication

B

bandwidth, described 2
Basic DVCP, setting up Edge for 137
Blocked Sites page 104
Bridge to Optional option 80
Bridge to Trusted option 80
broadband connections 2

C

cable modem 2
cables
included in package 11, 208
cabling
for 0-6 devices 19
for 7+ devices 20
channel bandwidth 214

- CIDR notation 64, 94, 100, 147
- Classless Inter Domain Routing 64, 94, 100, 147
- Client for Microsoft Networks, installing 163
- client, described 2
- configuration file, viewing 204
- configuration pages
 - description 28–39
 - navigating 28
 - opening 28
 - viewing 27
- configuration pages. See also pages
- Connection Monitor, using to monitor MUVPNs 172
- custom incoming services, creating 91, 92, 97
- Custom Service page 92, 98

D

- daylight savings time 115
- default factory settings 40–41
- Denied Sites page 126
- DHCP
 - described 5, 46
 - setting your computer to use 22
 - using on the optional network 60
- DHCP address reservations
 - setting on the optional network 60
 - setting on the trusted network 55
- DHCP Address Reservations page 56, 61
- DHCP relay
 - configuring the optional network 61
 - configuring the trusted network 56
- DHCP server
 - configuring Firebox as 54, 60
- dialog boxes
 - Internet Protocol (TCP/IP) Properties 22, 23
 - Wireless Network Connection 77
- dialup settings, configuring 74
- Diffie-Hellman groups 145
- Digital Subscriber Line (DSL) 2
- DNS service, dynamic 66
- DNS settings, and WAN failover 73
- DNS, described 6
- DSL 3

- DVCP Server, getting information on 136
- DVCP, described 131, 135
- Dynamic DNS client page 67
- dynamic DNS service, registering with 66–67
- Dynamic Host Configuration Protocol. See DHCP
- dynamic IP addresses
 - described 14
- Dynamic VPN Configuration Protocol, described 131, 135

E

- echo host 149
- Enable DHCP Relay check box 57
- Enable DHCP Server on the Trusted Network check box 55
- Enable Optional Network check box 59
- Enable VPN Manager Access check box 133, 134, 138
- event, described 111
- external network
 - described 9
 - if ISP uses DHCP 47
 - if ISP uses PPPoE 49
 - if ISP uses static addressing 48
- External Network Configuration page 47, 48, 49

F

- factory default settings
 - described 40
 - resetting to 41
- failover network. See WAN failover
- feature key, described 26
- File and Printer Sharing for Microsoft Networks
 - and Windows XP 165
- File and Printer Sharing for Microsoft Networks, installing 163
- Filter Traffic page 90, 96, 102
- Firebox users
 - creating 190
 - viewing settings for 184
- Firebox Users page 191, 194, 195
 - described 33
 - subpages of 34
- Firebox X Edge

- administrator account 193
- and SOCKS 106
- authenticating to 187
- back panel 211
- cabling 19
- configuring as DHCP server 54
- described 207
- front panel 209
- hardware description 209–211
- hardware specifications 208
- indicator lights 209
- installing 11–26
- package contents 11, 207
- rear panel 211
- rebooting 42–43
- registering 25
- resetting to factory default 41
- serial number 12
- side panel 211
- updating software 39
- upgrade options 201
- viewing log messages for 111
- Web pages. See configuration pages
- Firebox X Edge Wireless
 - advanced settings 84
 - physically connecting 76
 - setting up 75–85
- Firewall Options page 105
- Firewall page
 - described 35
 - subpages of 35–36
- firewalls, described 8
- firmware, updating 199

H

- hardware description 209–211
- hardware operating specifications 211
- hardware specifications 208
- HTTP proxy settings, disabling 17
- HTTP server port, changing 198
- HTTP/HTTPS, using for Firebox management 197

I

- incoming service, creating custom 91, 92, 97
- indicator lights 209
- installation
 - determining TCP/IP settings 13
 - disabling TCP/IP proxy settings 17
 - setting your computer to connect to Edge 22
 - TCP/IP properties 14
- installation requirements 11, 12
- installing the Firebox X Edge 11–26
- Internet
 - how information travels on 4
 - options for connecting to 2
- Internet connection, required for Firebox X Edge 13
- Internet Protocol (IP) 3
- Internet Protocol (TCP/IP) Network Component
 - and Windows XP 165
- Internet Protocol (TCP/IP) network component, installing 163
- Internet Protocol (TCP/IP) Properties dialog box 22, 23
- IP addresses
 - described 5
 - dynamic 5
 - giving your computer static 22
 - static 47

L

- lights on front panel 209
- LiveSecurity Service
 - and software updates 39
 - registering with 25
- Local Area Network (LAN)
 - described 2
- Log Authentication Events check box 84
- log messages
 - contents of 111
 - viewing 111
- Log Viewer, using to monitor MUVPNs 172
- logging
 - configuring 111–115
 - described 111
 - to Syslog host 113
 - to WSEP lot host 112

- viewing status of 36
- Logging page 112
 - described 36
 - subpages of 36–37

M

- Managed VPN page 133, 137, 139
- Managed VPNs
 - and VPN Manager 137
 - described 131, 135
 - setting Edge for DVCP 137
- Manual VPN page 143
- Manual VPNs
 - creating 143
 - described 140
- Manually configure DNS server IP addresses check box 73
- model upgrades 203
- modems
 - and DNS settings 73
 - dialup settings 74
 - types supported 72
 - using the failover 72
- multipath, described 213
- MUVPN client
 - allowing through firewall 171
 - configuring user settings for 190
 - connecting 169
 - described 153
 - disconnecting 171
 - icon for 169–171
 - installing 167
 - monitoring 172–173
 - preparing remote computers for 159–166
 - troubleshooting 179–181
 - uninstalling 168
- MUVPN Clients upgrade 203
- MUVPNs
 - and .wgx files 158
 - enabling access for users 156
 - monitoring with Connection Monitor 172
 - monitoring with Log Viewer 172
 - system requirements for 159
 - using on wireless networks 176

N

- navigation bar 29
- netmask 14
- Network Address Translation (NAT), and the Edge 14, 145
- network addressing, described 13
- network interfaces, configuring 45–71
- Network page
 - described 31
 - subpages of 31–32
- network security, described 1
- Network Setup Wizard 45
- Network Statistics page 65
- network statistics, viewing 65
- networks, types of 2
- New User page 191
- noise level 212
- numbered ports 211

O

- optional network
 - assigning static IP addresses on 62
 - changing IP address of 59
 - configuring 58–63
 - configuring additional computers on 62
 - described 9, 58
 - enabling 59
 - setting DHCP address reservations on 60
 - using DHCP on 60
 - using DHCP relay on 61
- Optional Network Configuration page 59, 60, 62
- options
 - Managed VPN 204
 - Manual VPN 204
 - model upgrade 203
 - MUVPN Clients 203
 - seat license upgrade 203
 - WAN failover 203
 - WebBlocker 203

P

package contents 11

packets, described 4

pages

- Add Gateway 143

- Add Route 64

- Administration 34

- Allowed Sites 125

- Blocked Sites 104

- Custom Service 92, 98

- Denied Sites 126

- DHCP Address Reservations 56, 61

- Dynamic DNS client 67

- External Network Configuration 47, 48, 49

- Filter Traffic 90, 96, 102

- Firebox Users 33, 191, 194, 195

- Firewall 35

- Firewall Options 105

- Logging 36, 112

- Managed VPN 133, 137, 139

- Manual VPN 143

- Network 31

- Network Statistics 65

- New User 191

- Optional Network Configuration 59, 60, 62

- Routes 63

- Settings 188

- Syslog Logging 114

- System Security 197

- System Status 30

- System Time 115

- Trusted Hosts 127

- Trusted Network Configuration 54, 55, 57, 184

- Upgrade 202

- VPN 38

- VPN Keep Alive 149

- VPN Manager Access 132, 134, 138, 139, 198, 199

- VPN Statistics 149

- WAN Failover 70

- WatchGuard Security Event Processor Logging 113

- WebBlocker 37

- WebBlocker Settings 119, 121

- Wireless Network Configuration 79

- passphrases, described 191, 195
- path-loss 213
- Perfect Forward Secrecy 147
- Phase 1 settings 143, 144
- Phase 2 settings 147
- Pocket PCs
 - creating MUVPN tunnels to 158
 - creating tunnels to 158
 - tips for configuring 177
- Point-to-Point Protocol over Ethernet. See PPPoE
- port, changing HTTP server port 198
- ports
 - numbered 211
 - trusted network 211
 - WAN 211
 - WAN1 68
 - WAN2 68
- power cable clip 12, 208
- power input 211
- PPPoE
 - described 6, 14, 47
 - entering settings 17
- profiles
 - creating WebBlocker 121–122
- protocols
 - described 3
 - IP 3
 - TCP, UDP 3
 - TCP/IP 3

Q

- Quick Setup Wizard
 - and viewing configuration pages 27
 - described 24
 - running 24

R

- read-only administrative account 193
- rebooting 42–43
- Remote Access Services, installing 160
- RESET button 210

- resetting to factory default 41
- Restrict Access by Hardware Address check box 84
- routes
 - configuring static 63
 - viewing 31
- Routes page 63

S

- seat licenses
 - described 184, 196
 - upgrade 203
- seat limitation 20
- serial number, viewing 30
- server, described 2
- services
 - creating custom 91–94, 97–101
 - creating custom incoming 91, 92, 97
 - described 6, 87
 - viewing current 35
- Session idle time-out field 192
- Session maximum time-out field 192
- sessions
 - closing 185
 - described 183
 - idle timeout 192
 - maximum timeout 192
 - releasing 20
 - terminating 194
 - viewing current active 184
 - viewing currently active 184
- Settings page 188
- shared secret 142
- signal attenuation 213
- signal strength 213
- SOCKS
 - configuring 107
 - configuring for Edge 106
 - described 106
 - disabling 107
- software updates 39
- SSID (Service Set Identifier) 79
- static IP addresses

- and VPNs 149
- described 13
- obtaining 150
- static routes
 - making 63
 - removing 64
- subnet mask 14
- SurfControl 117
- Syslog host, logging to 113
- Syslog Logging page 114
- Syslog, described 113
- system configuration pages. See configuration pages
- System Security page 197
- System Status page
 - described 30
 - green triangle on 30
 - information show on 30
 - navigation bar 29
- system time
 - setting 115
- System Time page 115

T

- TCP (Transmission Control Protocol) 3
- TCP/IP properties 14
- TCP/IP settings, determining 14–17
- TCP/IP, described 3
- time zone, setting 115
- traffic, logging all outbound 108
- Trusted Hosts page 127
- trusted network
 - assigning static IP addresses on 57
 - changing IP address of 53
 - configuring 53–??
 - configuring additional computers on 57
 - denying FTP access to 106
 - described 8
- Trusted Network Configuration page 54, 55, 57, 184

U

- UDP (User Datagram Protocol) 3
- Uniform Resource Locator (URL) 6
- updating firmware 199
- updating software 39
- upgrade options, activating 201
- upgrade options, viewing status of 30
- Upgrade page 202
- user accounts
 - changing name, password 195
 - configuring MUVPN settings 190
 - configuring MUVPN settings for all 155
 - creating new 190
 - deleting 186
 - editing 186
 - enabling MUVPN access for 156
 - read-only administrative 193
 - setting WebBlocker profile for 193
 - viewing 185
 - viewing current 33
- user authentication
 - changing options for 188
 - described 187
 - process 187
- users. See Firebox users

V

- virtual adapter, settings for 155, 190
- VPN Keep Alive page 149
- VPN Manager
 - described 198
 - setting up access to 198–199
- VPN Manager Access page 132, 134, 138, 139, 198, 199
- VPN Manager, and Managed VPNs 135, 137
- VPN page
 - described 38
 - subpages of 38
- VPN Statistics page 149
- VPNs
 - and static IP addresses 149
 - described 129

- Keep Alive feature 148
- special considerations for 130
- troubleshooting connections 150
- viewing statistics 149
- what you need to create 130

W

- wall mounting plate 211
- WAN Failover
 - and DNS settings 73
 - configuring 69
 - described 68, 203
 - using broadband connection for 71
 - using external modem for 72
- WAN Failover page 70
- WAN Failover Setup Wizard 69
- WAN ports 211
- WAN1 port 68
- WAN2 port 68
- WatchGuard Security Event Processor 112
- WatchGuard Security Event Processor Logging page 113
- Web sites
 - blocking specific 126
 - blocking using WebBlocker ??–127
 - bypassing WebBlocker 125
- WebBlocker
 - allowing internal hosts to bypass 127
 - allowing sites to bypass 125
 - categories 122–124
 - creating profiles 121–122
 - database 117
 - defining profile 193
- WebBlocker page
 - described 37
 - subpages of 37–38
- WebBlocker Settings page 119, 121
- Wide Area Network (WAN), described 2
- Windows 2000
 - preparing for MUVPN clients 162
- Windows 98/ME
 - preparing for MUVPN clients 160
- Windows NT
 - preparing for MUVPN clients 160

Windows XP

- installing File and Printer Sharing for Microsoft Networks on 165
- installing Internet Protocol (TCP/IP) Network Component on 165
- preparing for MUVPN clients 164

WINS and DNS settings, configuring 161, 163

wireless access point, setting up 79

wireless card, configuring 76

wireless communication

- antenna directional gain 213
- channel bandwidth 214
- described 212
- noise level 212
- path-loss 213
- signal attenuation 213
- signal strength 213

Wireless Encryption Privacy (WEP) 78

Wireless Network Configuration page 79

Wireless Network Connection dialog box 77

Wireless Network Wizard 77

wireless networks

- described 76
- security 78
- security options 77
- using MUVPN on 176

wireless setup 75–85

wizards

- NetworkSetup 45
- Quick Setup 24
- WAN Failover Setup 69
- Wireless Network 77

Wizards page 39

WSEP 112

Z

ZoneAlarm

- allowing traffic through 174
- described 153, 173
- icon for 172
- shutting down 175
- uninstalling 175