

WatchGuard® Firebox® X Edge User Guide

**Firebox X Edge - Firmware Version 7.5
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: 7.5
Part Number: 1776-0000
Guide Version: 7.5

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>	5	
Domain Name Service (DNS)	6	
Services	6	
Ports	6	
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	
<i>Static addresses, DHCP, and PPPoE</i>	13	

<i>Finding your TCP/IP properties</i>	14
<i>Finding PPPoE settings</i>	17
Disabling the HTTP Proxy Setting	17
Connecting the Firebox X Edge	19
<i>Connecting the Edge to more than seven devices</i>	20
Setting Your Computer to Connect to the Edge	22
<i>If your computer gets its address from DHCP</i>	22
<i>If your computer has a static IP address</i>	23
Using the Quick Setup Wizard	24
Registering and Activating LiveSecurity Service	26
CHAPTER 3 Navigating the Firebox X Edge Configuration Pages	29
.....	29
Navigating the Configuration Pages	30
<i>Using the navigation bar</i>	31
Configuration Overview	32
<i>Firebox System Status Page</i>	32
<i>Network Page</i>	33
<i>Administration Page</i>	34
<i>Firewall Page</i>	35
<i>Logging Page</i>	37
<i>WebBlocker Page</i>	38
<i>VPN Page</i>	38
<i>Wizards Page</i>	39
CHAPTER 4 Configuration and Management Basics	41
Factory Default Settings	41
<i>Resetting the Firebox to the factory-default settings</i>	42
Restarting the Firebox	43
<i>Local restart</i>	43
<i>Remote reboot</i>	44
Selecting HTTP or HTTPS for Management	44
Changing the HTTP Server Port	45
Setting up WatchGuard System Manager Access	46
<i>Enable remote management with WSM v8.2 or higher</i>	46
<i>Enable remote management with WSM v8.0 or v8.1</i>	48
<i>Enable remote management with WSM v7.3 or earlier</i>	50
Updating the Firebox X Edge Software	52
<i>Method 1 - Installing software automatically</i>	52
<i>Method 2 - Installing software manually</i>	53
Activating Upgrade Options	54

Enabling the Model Upgrade Option	56
Viewing the Configuration File	57
CHAPTER 5 Changing Your Network Settings	59
Using the Network Setup Wizard	59
Configuring the External Network	60
<i>If your ISP uses DHCP</i>	<i>61</i>
<i>If your ISP uses static IP addresses</i>	<i>62</i>
<i>If your ISP uses PPPoE</i>	<i>63</i>
Configuring the Trusted Network	66
<i>Changing the IP address of the trusted network</i>	<i>67</i>
<i>Using DHCP on the trusted network</i>	<i>68</i>
<i>Setting trusted network DHCP address reservations</i>	<i>69</i>
<i>Configuring the trusted network for DHCP relay</i>	<i>70</i>
<i>Using static IP addresses for trusted computers</i>	<i>71</i>
<i>Adding computers to the trusted network</i>	<i>71</i>
Configuring the Optional Network	72
<i>Enabling the optional network</i>	<i>73</i>
<i>Changing the IP address of the optional network</i>	<i>73</i>
<i>Using DHCP on the optional network</i>	<i>74</i>
<i>Setting optional network DHCP address reservations</i>	<i>75</i>
<i>Configuring the optional network for DHCP relay</i>	<i>76</i>
<i>Using static IP addresses for optional computers</i>	<i>77</i>
<i>Adding computers to the optional network</i>	<i>77</i>
Making Static Routes	78
Viewing Network Statistics	80
Registering with the Dynamic DNS Service	81
Enabling the WAN Failover Option	83
<i>Using the WAN Failover Setup Wizard</i>	<i>84</i>
<i>Using the Network page</i>	<i>85</i>
<i>If you are using a broadband connection for failover</i>	<i>85</i>
<i>If you are using an external modem for failover</i>	<i>87</i>
<i>Dial-up DNS settings</i>	<i>88</i>
<i>Dial-up settings</i>	<i>88</i>
CHAPTER 6 Firebox X Edge Wireless Setup	89
Connecting to the Firebox X Edge Wireless	90
Using the Wireless Network Wizard	90
Configuring Basic Wireless Settings	91
<i>Selecting the wireless network assignment</i>	<i>91</i>
<i>Setting the SSID</i>	<i>92</i>

Setting the operating region and channel	93
Controlling SSID broadcasts	93
Logging authentication events	93
Setting the wireless mode	93
Setting the fragmentation threshold	94
Configuring Wireless Security Settings	94
Setting the wireless authentication method	96
Configuring encryption	96
Configuring wireless clients to use MUVPN	97
Restricting Wireless Access by MAC Address	97
Configuring Wireless Guest Services	99
Enabling guest services	99
Setting password protection	100
Setting network access rules for guests	100
Connecting to the Firebox as a wireless guest	101
Configuring the Wireless Card on Your Computer	101
CHAPTER 7 Configuring Firewall Settings	103
About Services	103
Incoming and outgoing traffic	104
Traffic through VPN tunnels	104
About This Chapter	104
Configuring Incoming Services	105
Configuring common services for incoming traffic	106
About custom services for incoming traffic	107
Adding a custom service using the wizard	107
Adding a custom incoming service manually	108
Filtering incoming traffic for services	110
Filtering outgoing traffic for services	110
Configuring Outgoing Services	111
Configuring common services for outgoing traffic	112
About custom services for outgoing traffic	113
Adding a custom service using the wizard	113
Adding a custom outgoing service manually	114
Filtering incoming traffic for services	116
Filtering outgoing traffic for services	116
Services for the Optional Network	116
Controlling traffic from the trusted to optional network	117
Disabling traffic filters	118
Blocking External Sites	119

Configuring Firewall Options	120
<i>Responding to ping requests</i>	120
<i>Denying FTP access to the Firebox X Edge</i>	121
<i>SOCKS implementation for the Firebox X Edge</i>	121
<i>Logging all allowed outgoing traffic</i>	123
<i>Changing the MAC address of the external interface</i>	123
CHAPTER 8 Configuring Logging and System Time	125
Viewing Log Messages	125
Log to a WatchGuard Log Server	126
Logging to a Syslog Host	128
Setting the System Time	129
CHAPTER 9 Managing Users and Groups	133
Seeing Current Sessions and Users	133
<i>Firebox Users Settings</i>	134
<i>Active Sessions</i>	134
<i>Stopping a session</i>	135
<i>Local User Accounts</i>	136
About User Licenses	137
About User Authentication	137
<i>Setting authentication options for all users</i>	138
<i>Configuring MUVPN client settings</i>	140
<i>Authenticating to the Edge</i>	141
Using Local Firebox Authentication	142
<i>Creating a read-only administrative account</i>	144
<i>Setting a WebBlocker profile for a user</i>	145
<i>Enabling MUVPN for a user</i>	145
<i>The Administrator account</i>	145
<i>Changing a user account name or password</i>	146
Using LDAP/Active Directory Authentication	146
<i>Configuring the LDAP/Active Directory authentication service</i>	147
<i>Using the LDAP authentication test feature</i>	149
<i>Configuring groups for LDAP authentication</i>	150
<i>Adding a group</i>	150
<i>Setting a WebBlocker profile for a user</i>	152
<i>LDAP Authentication and MUVPN</i>	152
Allowing Internal Hosts to Bypass User Authentication	152
CHAPTER 10 Configuring WebBlocker	155
How WebBlocker Works	155
Configuring Global WebBlocker Settings	155

Creating WebBlocker Profiles	159
WebBlocker Categories	161
Allowing Certain Sites to Bypass WebBlocker	171
Blocking Additional Web Sites	172
Bypassing WebBlocker	173
CHAPTER 11 Configuring Virtual Private Networks	175
About This Chapter	175
What You Need to Create a VPN	176
Managed VPN	177
Manual VPN: Setting Up Manual VPN Tunnels	178
<i>What you need for Manual VPN</i>	178
<i>Phase 1 settings</i>	181
<i>Phase 2 settings</i>	184
VPN Keep Alive	186
Viewing VPN Statistics	187
Frequently Asked Questions	187
CHAPTER 12 Configuring the MUVPN Client	191
About This Chapter	192
Enabling MUVPN for Edge Users	193
<i>Configuring MUVPN client settings</i>	193
<i>Enabling MUVPN access for a Firebox user account</i>	194
<i>Configuring the Firebox for MUVPN clients using a Pocket PC</i>	196
Distributing the Software and the .wgx File	196
Preparing Remote Computers for MUVPN	197
<i>WINS and DNS servers</i>	198
<i>Windows NT setup</i>	198
<i>Windows 2000 setup</i>	200
<i>Windows XP setup</i>	202
Installing and Configuring the MUVPN Client	204
<i>Installing the MUVPN client</i>	204
<i>Uninstalling the MUVPN client</i>	206
Connecting and Disconnecting the MUVPN Client	207
<i>Connecting the MUVPN client</i>	207
<i>The MUVPN client icon</i>	207
<i>Allowing the MUVPN client through a personal firewall</i>	208
<i>Disconnecting the MUVPN client</i>	209
Monitoring the MUVPN Client Connection	209
<i>Using Log Viewer</i>	210

<i>Using Connection Monitor</i>	210
The ZoneAlarm Personal Firewall	211
<i>Allowing traffic through ZoneAlarm</i>	211
<i>Shutting down ZoneAlarm</i>	212
<i>Uninstalling ZoneAlarm</i>	212
Using MUVPN on the Edge Wireless Network	213
Tips for Configuring the Pocket PC	214
Troubleshooting Tips	216
APPENDIX A Firebox X Edge Hardware	219
Package Contents and Specifications	219
Hardware Description	221
<i>Front panel</i>	221
<i>Rear view</i>	223
<i>Side panels</i>	223
About IEEE 802.11g/b Wireless	224
<i>Noise level</i>	224
<i>Signal strength (Watts)</i>	225
<i>Channel bandwidth</i>	226
APPENDIX B Legal Notifications	229
Copyright, Trademark, and Patent Information	229
Certifications and Notices	233
Declaration of Conformity	236
Limited Hardware Warranty	237

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 a large 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. A hacker can use your computer as a platform to attack other computers or networks or use your account information to send e-mail spam or attacks. Your account 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 with a serial cable, or many computers around the world connected through the Internet. Computers on the same network can do work together and share data.

A LAN (Local Area Network) is a connected group of computers that use the same method of communication to share data.

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

Clients and servers

Clients and servers are components of a network. A server is a computer that makes its resources available to the network. Some of these resources are documents, printers, and programs. A client is a computer that uses the resources made available by the server.

Connecting to the Internet

ISPs (Internet service providers) are companies that give access to the Internet through network connections. Bandwidth is the rate at which a network connection can send data: for example, 3 megabits per second (Mbps).

A high-speed Internet connection, such as a cable modem or a DSL (Digital Subscriber Line), is known as a broadband connection.

Broadband connections are much faster than dial-up connections: the bandwidth of a dial-up connection is less than .1 Mbps, while a cable modem can be 5 Mbps or more.

Typical speeds for cable modems are usually lower than the maximum speeds, because each person in a neighborhood is a member of a LAN. Each computer in that LAN uses some of the bandwidth. Because of this “shared-medium” system, cable modem connections can become slow when more users are on the network.

DSL connections supply constant bandwidth, but they are usually slower than cable modem connections. Also, the bandwidth is only constant between your home or office and the DSL central office. The DSL central office cannot supply a constant connection to a Web site or network.

Protocols

A protocol is a group of rules that allow computers to connect across a network. Protocols are the “grammar” that computers use to speak to each other.

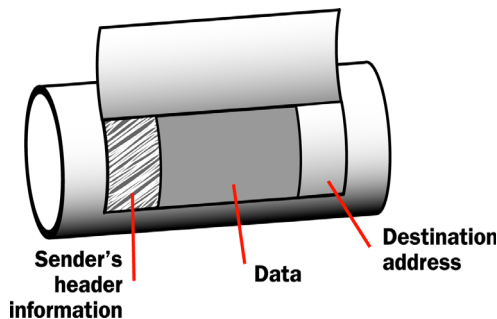
The standard protocol when you connect to the Internet is the IP (Internet Protocol). This protocol is the usual language of computers on the Internet.

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 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 Firebox® X Edge. For more information on TCP/IP, see “Finding your TCP/IP properties” on page 15.

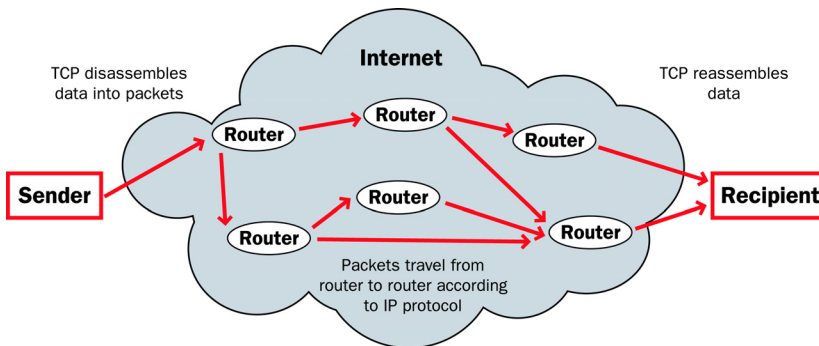
How Information Travels on the Internet

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 connection can use different routes through the Internet. When they all get to their destination, they are assembled back into a 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 disassembles the data and assembles it again. IP adds information to the packets, such as the sender, the recipient, and any special instructions.



Packets traveling on the Internet

IP Addresses

To send mail to a person, you must first know their physical address. For a computer 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. Only one device can use an IP address at a time.

An IP address is a group of four numbers divided by decimal points. Some examples of IP addresses are:

- 192.168.0.11
- 10.1.20.18
- 208.15.15.15

Network addressing

ISPs (Internet service providers) assign an IP address to each device on their network. The IP address can be static or dynamic. Each ISP has a small number of IP addresses.

Static IP addresses are permanently assigned to a device. These addresses do not change automatically, and are frequently used for servers.

Dynamic IP addresses change with time. If a dynamic address is not in use, it can be automatically assigned to a different device.

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

About DHCP

Many ISPs assign dynamic IP addresses through DHCP (Dynamic Host Configuration Protocol). 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 DNS (Domain Name Service). Each Web site has a domain name (such as “mysite.com”) that is equal to an IP address. When you type a domain name to show a Web site, your computer gets the IP address from a DNS server.

A URL (Uniform Resource Locator) includes a domain name and a protocol. 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 SSH (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

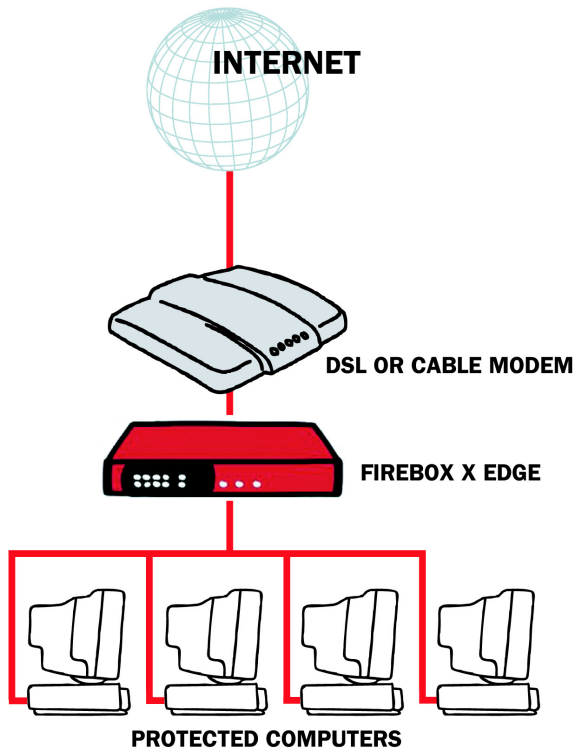
Usually, a port is a connection point where you use a socket and a plug to connect two devices. Computers also have ports that are not physical locations. These ports are where programs transmit data.

Some protocols, such as HTTP, have ports with assigned numbers. For example, most computers transmit e-mail on port 25 because the SMTP protocol is assigned to port 25. Other programs are assigned port numbers dynamically for each connection. The IANA (Internet Assigned Numbers Authority) keeps a list of well known ports. You can see this list at www.iana.org/assignments/port-numbers.

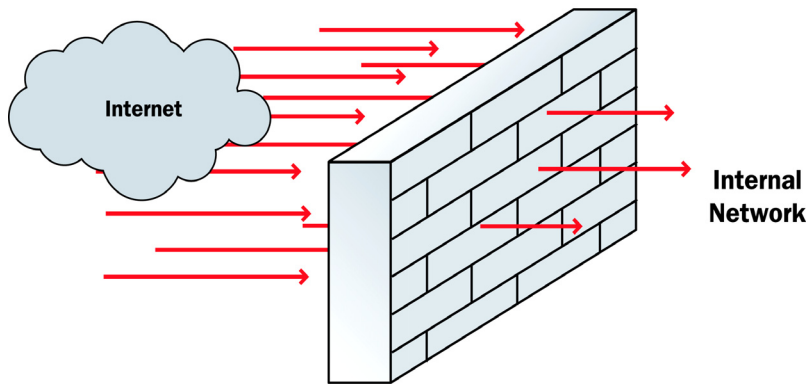
Most services are given a port number in the range from 0 to 1024, but possible port numbers range from 0 to 65535.

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 computers from the Internet.



Firewalls use access policies to identify different types of information. They can also control which services or ports the protected computers can use on the Internet (outbound 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 7, “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:

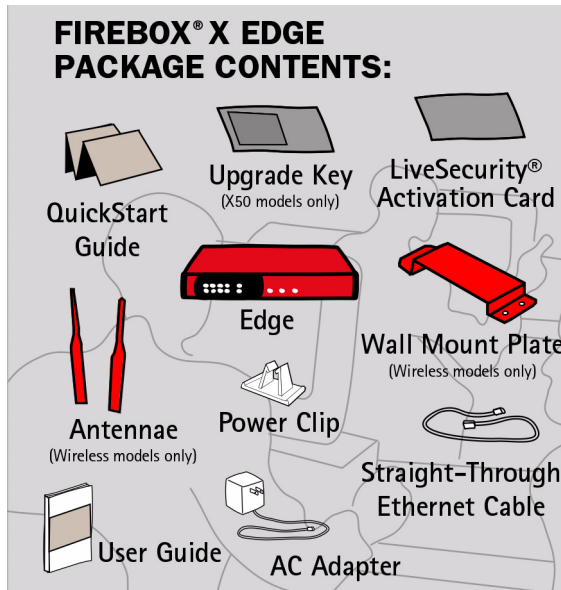
- Identify and record the TCP/IP properties for your Internet connection.
- Disable the HTTP proxy properties of your Web browser.
- Connect the Firebox X Edge to your network.
- Connect your computer to the Edge.
- Use the Quick Setup Wizard to configure the Edge.
- Activate the LiveSecurity® Service.

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 ISP (Internet Service Provider) to correct the problem before you install the Firebox X Edge.

Identifying Your Network Settings

You use an ISP (Internet Service Provider) to connect to the Internet. An ISP assigns your computer or firewall an IP (Internet Protocol) 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, you can put the Firebox® X Edge between your computer and the Internet and 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 Edge 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 temporarily. ISPs use DHCP (Dynamic Host Configuration Protocol) to assign you a dynamic IP address. With DHCP, your computer does not always use the same 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. When you close an Internet connection that uses a dynamic IP address, the ISP can assign that IP address to a different customer.
- **PPPoE:** An ISP can also use PPPoE (Point-to-Point Protocol over Ethernet) to assign you an IP address. Usually, a PPPoE address is dynamic. You must have a user name and a password to use PPPoE.

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

TCP/IP (Transmission Control Protocol/Internet Protocol) 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, 192.168, or 172.16 to 172.31, then your ISP uses NAT (Network Address Translation) and your IP address is private. 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**.
The Command Prompt window appears.
- 2 At the command 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**.
The Command Prompt window appears.
- 2 At the command 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**.
The Run window appears.
- 2 Type `winipcfg` and then press **Enter**.
The IP Configuration window appears.
- 3 Select the **Ethernet Adapter** from the drop-down list.
- 4 Click **More Info** for additional settings.
- 5 Record the values in Your TCP/IP Properties Table on page 15.
- 6 Close the window.

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 X

- 1 Click the **Apple** menu > **System Preferences**.
The System Preferences window appears.
- 2 Click the **Network** icon.
The Network preference pane appears.
- 3 From the **Show** drop-down list, select the network adapter you use to connect to the Internet.
- 4 Record the values in Your TCP/IP Properties Table on page 15.
- 5 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 Firefox, Mozilla, 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 Firefox or Netscape

- 1 Open the browser software.
- 2 If you are using Firefox, click **Tools > Options**. If you are using Netscape, click **Edit > Preferences**.
The Options window appears.
- 3 Click the **General** icon.
The General preference window appears.
- 4 Click the **Connection Settings** button.
The Connection Settings dialog box appears.
- 5 Make sure the **Direct Connection to the Internet** option is selected.
- 6 Click **OK** two times.

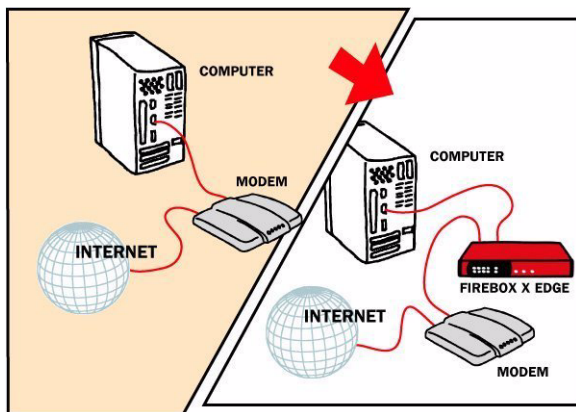
Disable the HTTP proxy in Mozilla

- 1 Open the browser software.
- 2 Click **Edit > Preferences**.
The Preferences window appears.
- 3 Click the arrow adjacent to the **Advanced** label and select **Proxies**.
The Proxies preference window appears.
- 4 Make sure the **Direct Connection to the Internet** option is selected.
- 5 Click **OK**.

Disable the HTTP proxy in Internet Explorer

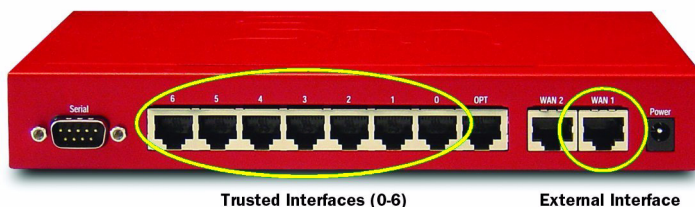
- 1 Open Internet Explorer.
- 2 Click **Tools > Internet Options**.
The Internet Options window appears.
- 3 Click the **Connections** tab.
- 4 Click the **LAN Settings** button.
The Local Area Network (LAN) Settings window appears.
- 5 Clear the check box labeled **Use a proxy server for your LAN**.
- 6 Click **OK** twice.

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 (labeled 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/AdvancedFaq/edge_seatlicense.asp

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

<http://www.watchguard.com/products/purchaseoptions.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 comes 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.
The Local Area Connection Status window appears.
- 4 Click the **Properties** button.
The Local Area Connection Properties window appears.
- 5 Double-click the **Internet Protocol (TCP/IP)** list item.
The Internet Protocol (TCP/IP) Properties dialog box appears.
- 6 Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** options.
- 7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** dialog box.
- 8 Click **OK** to close the **Local Area Network Connection Properties** dialog box. Close the **Local Area Connection Status**, **Network Connections**, and **Control Panel** windows.
Your computer is ready to connect to the Firebox X Edge.
- 9 When the Edge is ready, start your Internet browser.
- 10 Type `https://192.168.111.1/` into the URL entry field of your browser and press **Enter**. If you are asked to accept a security certificate, click **OK**.
The Quick Setup Wizard starts.
- 11 Run the Quick Setup Wizard, as shown in “Using 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.
The Local Area Connection Status window appears.
- 4 Click the **Properties** button.
The Local Area Connection Properties window appears.
- 5 Double-click the **Internet Protocol (TCP/IP)** list item.
The Internet Protocol (TCP/IP) Properties dialog box appears.
- 6 Select the **Use the following IP address** option.
- 7 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.
- 8 In the **Subnet Mask** field, type 255.255.255.0.
- 9 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.
- 10 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** dialog box.
- 11 Click **OK** to close the **Local Area Network Connection Properties** dialog box. Close the **Local Area Connection Status**, **Network Connections** and **Control Panel** windows.
Your computer is ready to connect to the Firebox X Edge.
- 12 When the Edge is ready, start your Internet browser.
- 13 Type `https://192.168.111.1/` into the URL entry field of your browser and press **Enter**. If you are asked to accept a security certificate, click **OK**.
The Quick Setup Wizard starts.
- 14 Use the Quick Setup Wizard, as shown in the subsequent section.

Using 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. If your browser blocks pop-up windows, you must disable that function to complete the Quick Setup Wizard. 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 setting cannot be changed after it is set.

Set the Time Zone

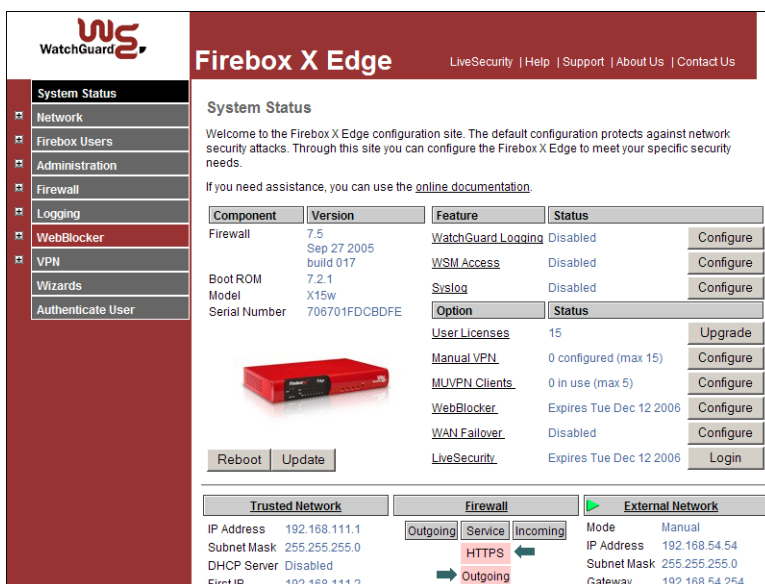
Use this screen to set the time zone the Firebox X Edge is operating in.

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. If you changed the IP address of the trusted interface, you must restart your computer before you connect to the Firebox X Edge.

The System Status page

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 default configuration protects against network security attacks. Through this site you can configure the Firebox X Edge to meet your specific security needs.

If you need assistance, you can use the [online documentation](#).

Component	Version	Feature	Status	
Firewall	7.5 Sep 27 2005 build 017	WatchGuard Logging	Disabled	Configure
		WSM Access	Disabled	Configure
Boot ROM	7.2.1	Syslog	Disabled	Configure
Model	X15w			
Serial Number	706701FDCBDFE			

Option	Status	
User Licenses	15	Upgrade
Manual VPN	0 configured (max 15)	Configure
MUVPN Clients	0 in use (max 5)	Configure
WebBlocker	Expires Tue Dec 12 2006	Configure
WAN Failover	Disabled	Configure
LiveSecurity	Expires Tue Dec 12 2006	Login

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

Trusted Network		Firewall		External Network	
IP Address	192.168.111.1	Outgoing	Service	Mode	Manual
Subnet Mask	255.255.255.0		HTTPS	IP Address	192.168.54.54
DHCP Server	Disabled		Outgoing	Subnet Mask	255.255.255.0
First IP	192.168.111.2			Gateway	192.168.54.254

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 to set up upgrades that you purchase. To install an upgrade, log in to the LiveSecurity service and type your upgrade key. You then receive a feature key to activate the feature on your Firebox X Edge.

To register, find the serial number of your Firebox X Edge. The Edge serial number is printed on the bottom of the device. Record your serial number in the table below and complete the following steps:

- 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 Service User Profile

User name:	
Password:	
Serial Number:	

- 4 If a model upgrade key is included with your model, activate it at:

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

- 5 Select your product and follow the instructions for product activation. At this time you can configure your Edge.

Navigating the Firebox X Edge Configuration Pages

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 Chapter 2, "Installing the Firebox X Edge". Also, to configure the Firebox X Edge, your network administrator must configure your user account to see and change the configuration pages. See Chapter 9 "Managing Users and Groups" 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.

WatchGuard

Firebox X Edge

LiveSecurity | Help | Support | About Us | Contact Us

System Status

Welcome to the Firebox X Edge configuration site. The default configuration protects against network security attacks. Through this site you can configure the Firebox X Edge to meet your specific security needs.

If you need assistance, you can use the [online documentation](#).

Component	Version	Feature	Status	
Firewall	7.5	WatchGuard Logging	Disabled	Configure
	Sep 27 2005	WSM Access	Disabled	Configure
	build 017	Sislog	Disabled	Configure
Boot ROM	7.2.1			
Model	X15w			
Serial Number	706701FDCBDFE			

Option	Status	
User Licenses	15	Upgrade
Manual VPN	0 configured (max 15)	Configure
MUVPN Clients	0 in use (max 5)	Configure
WebBlocker	Expires Tue Dec 12 2006	Configure
WAN Failover	Disabled	Configure
LiveSecurity	Expires Tue Dec 12 2006	Login

Reboot Update

Trusted Network		Firewall		External Network	
IP Address	192.168.111.1	Outgoing	Service	Mode	Manual
Subnet Mask	255.255.255.0		HTTPS	IP Address	192.168.54.54
DHCP Server	Disabled		Outgoing	Subnet Mask	255.255.255.0
First IP	192.168.111.2			Gateway	192.168.54.254

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`.”

This opens your Firebox system configuration pages. You can change the IP address of the trusted network from 192.168.111.1 to a different IP address if necessary. For more information, see “Configuring the Trusted Network” on page 66.

For example, if you use Internet Explorer as your primary browser:

- 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 of 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 and 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 is the primary configuration page of the Firebox X Edge. The center panel of the page shows information about the current settings. It also contains the buttons you use to change these settings. You can see details about each property in later chapters.

The 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 5, “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

Domain

MAC Address

00907F-178892

Trusted Network

IP Address

192.168.111.1

Configure

Subnet Mask

255.255.255.0

MAC Address

00907F-178890

DHCP Server

Disabled

0 addresses in use (251 max)

First address: 192.168.111.2

IP Address

Name

Timeout

HW Address

Optional Network

IP Address

192.168.113.1

Configure

Subnet Mask

255.255.255.0

The **Network** menu contains links to these pages:

- **External:** Configure the Edge external network interface, or how the Edge connects to the Internet and other networks.
- **Trusted:** Configure the Edge trusted network interface, or how the Edge gives IP addresses to trusted devices.
- **Optional:** Configure the Edge optional network interface, or how the Edge gives IP addresses to other devices.
- **WAN Failover:** Configure a redundant network connection for the external interface.
- **Dynamic DNS:** Register the external IP address of the Edge when using a dynamic DNS (Domain Name Server) service.
- **Routes:** Create a static route to a computer on the trusted or optional networks from the external interface.
- **Network Statistics:** Show 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 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 9 “Managing Users and Groups.”

The **Firebox Users** menu contains links to these 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 the user can send and receive.
- **New Group:** Use this page to add a user group.
- **Trusted Hosts:** Use this page to add the IP addresses of users who are exempt from the configured authentication and WebBlocker rules.

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 4, “Configuration and Management Basics.”

Administration

Administrative Options

System Security	HTTPS mode	Configure
-----------------	------------	-----------

WSM Access	Disabled	Configure
------------	----------	-----------

Upgrades
 Upgrade

Installed Options:

User Licenses	Unrestricted
Remote Gateways	Installed
MUVPN Clients	Installed - license count 50
WebBlocker	Installed
WAN Failover	Installed

View Configuration File

The **Administration** menu contains links to these pages:

- **System Security:** Use the System Security page to select HTTP or HTTPS for administrative access.
- **WSM Access:** Use the WSM Access page to enable remote management of the Edge through the WatchGuard Management Server.
- **Update:** Update the Edge firmware.
- **Upgrade:** Activate your Edge upgrade options.
- **View Configuration:** Shows the Edge configuration file as text.

Firewall Page

The Firewall page shows incoming and outgoing services, blocked sites, and other firewall settings. This page also has buttons to change these settings. For more information, see Chapter 7, “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** menu contains links to these 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 to the optional network.
- Blocked Sites: Prevent access to specified network addresses on the external interface.
- Firewall Options: Customize your security policy.

Logging Page

The Logging page shows the current event log, the status of the Log Server 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 8, “Configuring Logging and System Time.”

Logging
Refresh

Logging Options

WatchGuard Logging Disabled WatchGuard Log Server None Configure

Syslog Logging Disabled Syslog Host 0.0.0.0 Configure

System Time Configure

Time Source NTP Server ntp3.cs.wisc.edu
ntp1.cs.wisc.edu

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

DST Enabled

Current Time 2005-09-06-17:22:08

Sync Time With Browser Now

Event Log

Time	Category	Message
2005-09-06-17:22:03	IP	allowed from 192.168.54.150 port 1038 to 192.168.54.54 port 443 TCP SYN (HTTPS)
2005-09-06-17:15:50	IP	allowed from 192.168.54.150 port 4995 to 192.168.54.54 port 443 TCP SYN (HTTPS)
2005-09-06-17:15:48	MONITOR	Administrator access allowed from 192.168.54.150

The **Logging** menu contains links to these pages:

- WatchGuard Logging: 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 10, “Configuring WebBlocker.”

WebBlocker

WebBlocker Settings

Status	Enabled	Configure
Inactivity Time-out (minutes):	15	
Site access when WebBlocker server is unavailable:	Denied	
Site access when WebBlocker license expires:	Denied	
Custom message for blocked user field:	Not defined	

WebBlocker Profiles

Profiles and assigned users:

[Default]

admin

Recent-hire

SeniorManagement

Configure

Allowed Sites

There are no allowed sites.

Configure

Denied Sites

There are no denied sites.

Configure

The **WebBlocker** menu contains links to these pages:

- Settings: Configure the WebBlocker settings for all users.
- Profiles: Create sets of restrictions and apply them to groups of 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.

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. You can add the Firebox® X Edge to a Watchguard System Manager VPN network with the WSM Access page in Administration. For more information, see Chapter 11, “Configuring Virtual Private Networks.”

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** menu contains links to these pages:

- 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. Each wizard launches a new window to help you configure the Edge settings.

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.	
Set up services to allow traffic for WSM management of other Fireboxes.	

If a wizard is not available, it is not shown on the Wizards page.
Some of the wizards are:

- **Service Configuration Wizard**
Create a rule to filter network traffic between interfaces. For more information, see "About custom services for incoming traffic" on page 107.
- **Network Interface Wizard**
Configure the Edge interfaces. For more information, see "Using the Network Setup Wizard" on page 59.
- **Wireless Network Wizard (Wireless models only)**
Set up the wireless interface. For more information, see Chapter 6, "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 83.

Configuration and Management Basics

After your Firebox® X Edge is installed on your network and operating with a basic configuration file, you can start to add custom configuration settings to meet the needs of your organization. This chapter shows you how to do some basic management and maintenance tasks.

These basic configuration tasks include:

- Reset the Firebox X Edge to factory-default settings
- Restart the Firebox X Edge
- Set HTTP management preferences
- Enable remote management on the Firebox X Edge
- Update the firmware
- Activate upgrade options

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.
- The 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 you complete the Quick Setup Wizard, you must use the user name and password that you selected to see the configuration pages.
- The Firebox X Edge is set up with a local log file and for local management only.

WebBlocker

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

Upgrade Options

- Upgrade options are always available. You must type the license keys into the configuration page to activate upgrade options the first time. If you reset the Firebox X Edge to its factory-default settings, you do not have to type the license keys again.

Resetting the Firebox to the factory-default settings

If you cannot correct a configuration problem and must “start over,” you can go back to the factory-default settings. For example, if you do not know the administrator account passphrase or a power interruption damages the Firebox X Edge firmware, you can reset the Firebox to the factory-default settings.

Use 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. If you do not start the Edge one more time, when you try to connect to the Edge you will see a web page with "Your WatchGuard Firebox X Edge is running from a backup copy of firmware." You could also see this message if the reset button is stuck in the depressed position. Check the reset button, restart the Edge and try again.

- 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 connected to the Firebox external interface.

The Firebox restart cycle can be 40 seconds or less. During the restart cycle, the mode indicator on the front of the Firebox turns off and then turns on again.

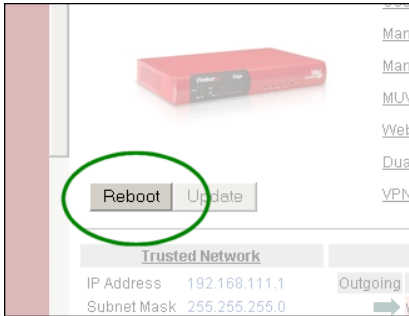
Local restart

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 then the IP address of the Edge trusted network interface.
The default URL is: `https://192.168.111.1`

- 2 Click **Reboot**.



Disconnecting the power supply

Disconnect the Firebox power supply. Wait for a minimum of 10 seconds, and then connect the power supply.

Remote reboot

You must configure the remote Firebox X Edge to allow incoming HTTPS traffic to the Edge trusted interface IP address if the computer is not on the trusted interface. For more information on how to configure the Firebox to receive incoming traffic, see “Configuring Incoming Services” on page 105. After HTTPS traffic is allowed, you can remotely manage your Firebox X Edge using your browser. To do a remote reboot:

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

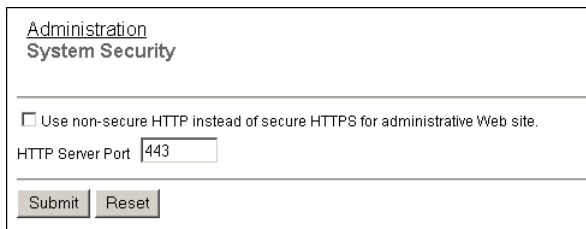
Selecting HTTP or HTTPS for Management

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. When HTTPS is used, the Web server and your browser encrypt and decrypt the information you transmit. 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 use HTTP. Using HTTP is less secure. When you use HTTP, all configuration changes are sent to the Edge from your computer in unencrypted text. We recommend that you use HTTPS to configure your Firebox X Edge.

Follow these instructions to use 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.



- 3 Select the **Use non-secure HTTP instead of secure HTTPS for administrative Web site** check box.
You will see a warning to make sure you change the HTTP server port to its default port of 80. To connect to the Firebox X Edge, you must use the same port in your browser as the HTTP server port on the Edge.
- 4 Click **Submit**.

If you select this check box, you must type `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 this FAQ:

https://www.watchguard.com/support/advancedfaqs/edge_https_serverport.asp

Setting up WatchGuard System Manager Access

Use the WatchGuard® System Manager (WSM) Access page to enable remote management by WatchGuard System Manager.

- With WatchGuard System Manager v7.3 or earlier, you can use VPN Manager to create managed VPN tunnels between a Firebox® X Edge and another WatchGuard Firebox.
- With WatchGuard System Manager 8.0 and above, you can create managed VPN tunnels between a Firebox X Edge and another WatchGuard Firebox using the WatchGuard Management Server.
- With WatchGuard System Manager 8.2 and above, you can do centralized management for Firebox X Edge devices and manage Edge policies, updates, and VPNs from one location.

Enable remote management with WSM v8.2 or higher

Follow these instructions to configure remote access from WatchGuard System Manager v8.2 or higher. These versions of WatchGuard System Manager support centralized management of Firebox X Edge devices.

- 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 **Administration > WSM Access**. The WatchGuard System Manager Access page appears.

Administration
WatchGuard Management Access

☐ Enable remote management

Management Type WatchGuard System Manager

☐ Use Centralized Management

☐ VPN Manager 7.2 or below

Status Passphrase

Confirm Status Passphrase

Configuration Passphrase

Confirm Configuration Passphrase

Management Server Address

Client Name

Shared Key

- Select the **Enable remote management** check box.
- From the **Management Type** drop-down list, select WatchGuard Management System.
- To put the Firebox X Edge into the control of WatchGuard System Manager centralized Edge management, click the **Use Centralized Management** check box.
When the Firebox X Edge is under centralized management, access to the Firebox X Edge configuration pages is set to read-only. The only exception is access to the WSM Access configuration page. If you disable the remote management feature, you get read-write access to the Firebox X Edge configuration again.
Do not select the Use Centralized Management check box if you are using WatchGuard System Manager only to manage VPN tunnels.
- Type a status passphrase for your Firebox X Edge and then type it again to confirm in the correct fields.
- 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 or the connection will fail.

- 8 In the **Management Server Address** text box, type the IP address of the Management Server if it has a public IP address. If the Management Server has a private IP address, type the public IP address of the Firebox protecting the Management Server.
The Firebox protecting the Management Server automatically monitors all ports used by the Management Server and will forward any connection on these ports to the configured Management Server. No special configuration is necessary for this to occur.
- 9 Type the **Client Name** to give your Firebox X Edge.
This is the name used to identify the Edge in the Management Server.
- 10 Type the **Shared Key**.
The shared key is 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**.

Enable remote management with WSM v8.0 or v8.1

Follow these instructions to configure remote access from WatchGuard System Manager v8.0 or 8.1. These versions of WatchGuard System Manager allow the management of VPN tunnels but do not support centralized management.

- 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 **Administration > WSM Access**. The WatchGuard System Manager Access page appears.

The screenshot shows the 'Administration' section of the WatchGuard System Manager Access page. At the top, there is a link for 'Administration' and the title 'WatchGuard Management Access'. Below this, there is a checkbox for 'Enable remote management'. Underneath, the 'Management Type' is set to 'WatchGuard System Manager' in a dropdown menu. There are two checkboxes: 'Use Centralized Management' (which is unchecked) and 'VPN Manager 7.2 or below' (which is checked). Below these are four password fields: 'Status Passphrase' (with a strength indicator), 'Confirm Status Passphrase', 'Configuration Passphrase' (with a strength indicator), and 'Confirm Configuration Passphrase'. At the bottom, there are three text input fields: 'Management Server Address', 'Client Name', and 'Shared Key'. At the very bottom, there are 'Submit' and 'Reset' buttons.

- Select the **Enable remote management** check box.
- From the **Management Type** drop-down list, select WatchGuard Management System.
- Make sure the **Use Centralized Management** check box is cleared.
WatchGuard System Manager v8.0 and 8.1 do not support centralized Edge management.
- Type a status passphrase for your Firebox X Edge and then type it again to confirm in the correct fields.
- 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 or the connection will fail.

- In the **Management Server Address** text box, type the IP address of the Management Server if it has a public IP address. If the Management Server has a private IP address, type the

public IP address of the Firebox protecting the Management Server.

The Firebox protecting the Management Server automatically monitors all ports used by the Management Server and will forward any connection on these ports to the configured Management Server. No special configuration is necessary for this to occur.

- 9 Type the **Client Name** to give your Firebox X Edge.
This is the name used to identify the Edge in the Management Server.
- 10 Type the **Shared Key**.
The shared key is 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**.

Enable remote management with WSM v7.3 or earlier

Follow these instructions to configure remote access from WatchGuard System Manager v7.3 or earlier. These versions of WatchGuard System Manager include VPN Manager and use the Firebox as a DVCP 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`

- From the navigation bar, select **Administration > WSM Access**.

The WatchGuard System Manager Access page appears.

Administration
WatchGuard Management Access

☒ Enable remote management

Management Type **VPN Manager**

☐ Use Centralized Management

☐ VPN Manager 7.2 or below

VPN Manager Access

☐ Enable VPN Manager Access

Status Passphrase

Confirm Status Passphrase

Configuration Passphrase

Confirm Configuration Passphrase

Managed VPN

☐ Enable Managed VPN

DVCP Server Address

Client Name

Shared Key

Submit **Reset**

- Select the **Enable remote management** check box.
- From the **Management Type** drop-down list, select **VPN Manager**.
- If you use VPN Manager 7.2 or below, click the **VPN Manager 7.2** or below check box.
- Click the **Enable VPN Manager Access** check box to allow VPN Manager to connect to the Firebox X Edge. Type and confirm the status and configuration passphrase for the Firebox X Edge.

NOTE

These passphrases must match the passphrases you use when you add the device to VPN Manager or the connection will fail.

- Click the **Enable Managed VPN** check box to configure the Firebox X Edge as a client to a WatchGuard DVCP server.

- 8 In the **DVCP Server Address** text box, type the IP address of the DVCP server.
- 9 Type the **Client Name** to give your Firebox X Edge.
This is the name used to identify the Edge in VPN Manager.
- 10 Type the **Shared Key**.
The shared key is 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.
- 11 Click **Submit**.

Updating the 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. To load any firmware on the Firebox X Edge, you must have a current LiveSecurity subscription. See the WatchGuard web site regularly for Firebox® X Edge updates: <https://www.watchguard.com/archive/softwarecenter.asp> (select Firebox X Edge)

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 - Installing software automatically

The first method uses an executable file and is the preferred method to install 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 Windows computer 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

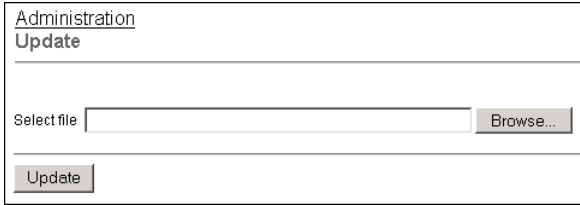
Because the Installer uses FTP to transfer files, make sure your Firebox X Edge is not configured to deny FTP access, as described in "Denying FTP access to the Firebox X Edge" on page 121.

Method 2 - Installing software manually

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 with an archiving utility such as WinZip (for Windows computers), StuffIt (for Macintosh), or the zip program (for Linux).
- 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 that contains 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.
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.



Administration Update
Select file <input type="text"/> <input data-bbox="709 332 803 360" type="button" value="Browse..."/>
<input data-bbox="244 389 325 417" type="button" value="Update"/>

Activating Upgrade Options

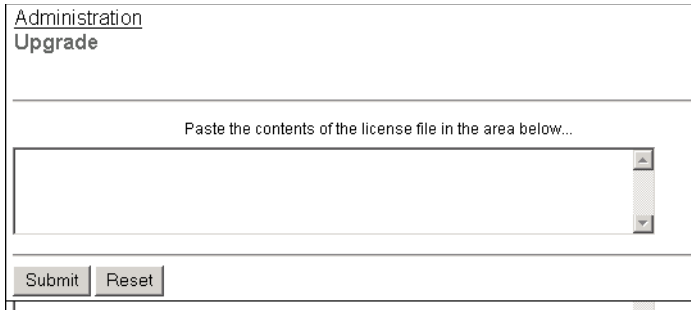
All Firebox® X Edge devices include the software for all upgrade options. These options are activated when you install a license key on the Firebox. To get a license key, purchase and activate an upgrade option at the LiveSecurity service Web site or from a WatchGuard-authorized reseller. See “Registering and Activating LiveSecurity Service” on page 26 for more information.

After you have purchased an upgrade option, you are given a license key. You use the license key to get the feature key for the upgrade. Use these steps to activate your license key and get your feature key:

- 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.



The screenshot shows a web interface for the 'Upgrade' page. At the top, there is a navigation bar with 'Administration' and 'Upgrade' links. Below the navigation bar, there is a large text area with the instruction 'Paste the contents of the license file in the area below...'. This text area is empty and has a vertical scrollbar on the right side. At the bottom of the page, there are two buttons: 'Submit' and 'Reset'.

- 8 Paste the feature key in the correct 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 10, “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 83.

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.

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**.

The configuration file is shown.

```
Administration
View Configuration File

-----

FDATE: Sep 12 2005
FTIME: 10:18:33
FVER: 7.5
admin.description: Administrator
admin.external_access: 1
admin.full_name:
admin.idle_timeout: 0
admin.ipsec_access: 1
admin.max_access: 0
admin.muvpn_access: 0
admin.trusted_access: 1
admin.webblocker_profile: [Default]
admin.wireless_access: none
auth.ldap.domain: qa2
auth.ldap.enable: 0
auth.ldap.group_attr: isMemberOf
```


Changing Your Network Settings

A primary component of the 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 61.

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 63.

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 62.

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 66.

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 ISP (Internet Service Provider) uses to give you an IP address for your Firebox. There are three methods ISPs use to assign IP addresses:

- **DHCP** - Network administrators use DHCP (Dynamic Host Configuration Protocol) 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 PPPoE (Point to Point Protocol over Ethernet) 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

Link Speed

Automatic

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

Link Speed

Automatic

- 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 5.

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

- 3 Type your 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 number of minutes before the Edge disconnects inactive connections.
We recommend a value of 20.

- 5 Select **Automatic** from the **Link Speed** drop-down list to have the Edge select the best network speed, or select a static link speed that you know is compatible with your equipment. We recommend that you set the link speed to Automatic unless you know this setting is incompatible with your equipment.

Advanced PPPoE Settings

The Quick Setup Wizard allows you to set up basic PPPoE settings. If necessary, 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 must 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 the PPPoE connection is considered 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 most cases, the default setting of three is the best.

Reconnect lost PPPoE link

This setting controls 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 to troubleshoot 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 built-in 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. The factory-default settings of a Firebox DHCP server automatically give 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 settings use the same DNS server information on the internal and external interfaces.

If necessary, you can disable the Firebox DHCP server. Or, you can use the Firebox as 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 at one time 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 IP 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 (Virtual Private Network) 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 176.

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.

Network
Trusted Network Configuration

IP Address

Subnet Mask

☐ Enable DHCP Server on Trusted Network

First address for DHCP server

Last address for DHCP server [DHCP Reservations...](#)

WINS Server Address

DNS Server Address

Secondary DNS Server Address

DNS Domain Suffix

☐ Enable DHCP Relay

DHCP relay server

[Submit](#) [Reset](#)

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. By default, a 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 and last available IP addresses for the trusted network. Do not include the IP address of the Firebox X Edge.
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 If you have a WINS or DNS server, type the **WINS Server Address**, **DNS Server Primary Address**, **DNS Server Secondary Address**, and **DNS Domain Suffix** in the correct text boxes.
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.

- 2 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 table has one row with the values '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 form are 'Submit' and 'Reset' buttons.

IP Address	MAC Address
192.168.111.24	000BDBA3B091

Remove

IP Address MAC Address

Add

Submit Reset

- 3 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.
- 4 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**.
- 5 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 the DHCP relay function 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 and click **Submit**.

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 as 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. By default, a Firebox® does not allow traffic from the optional network to get to the trusted network. The factory-default settings do 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 116 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 for the System Status page from the optional network 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

Link Speed

Changing the IP address of the optional network

If necessary, you can change the optional network address. By default, the optional interface IP address is 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.

The screenshot shows the 'Optional Network Configuration' page. At the top, there's a 'Network' link and the title 'Optional Network Configuration'. Below this, there's a section for 'Enable Optional Network' with a checked checkbox. Underneath, there are text boxes for 'IP Address' (containing '192.168.112.1') and 'Subnet Mask' (containing '255.255.255.0'). Below that is a section for 'Enable DHCP Server on Optional Network' with an unchecked checkbox. Underneath, there are text boxes for 'First address for DHCP server' (containing '192.168.112.2') and 'Last address for DHCP server' (containing '192.168.112.252'). There is a button labeled 'DHCP Reservations...'. Below that are text boxes for 'WINS Server Address', 'DNS Server Address', 'Secondary DNS Server Address', and 'DNS Domain Suffix'. There is another section for 'Enable DHCP Relay on Optional Network' with an unchecked checkbox. Underneath, there is a text box for 'DHCP relay server' and a dropdown menu for 'Link Speed' (set to 'Automatic'). At the bottom, there are 'Submit' and 'Reset' buttons.

- 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.
- 5 Click **Submit**.

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. By default, a 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 the last available 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 If you have a WINS or DNS server, type the **WINS Server Address**, **DNS Server Primary Address**, **DNS Server Secondary Address**, and **DNS Domain Suffix** in the related fields.
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.

The screenshot shows the 'DHCP Address Reservations' page. At the top, there is a breadcrumb trail: 'Network > Optional Network' followed by the page title 'DHCP Address Reservations'. Below this, network configuration details are listed: 'Optional Network IP Address' is 192.168.112.1, 'Optional Network Subnet Mask' is 255.255.255.0, and 'DHCP Address Pool' is 192.168.112.2-192.168.112.252. The main section is titled 'DHCP Address Reservations' and contains a table with two columns: 'IP Address' and 'MAC Address'. The table is currently empty. 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.

- 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 and transmit the reply to the computers on the 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 activate.

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 the DHCP relay function 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 devices with a static IP address. For example, this is necessary for a Web server or network printer. Static IP addresses must be on the same network as the Edge optional interface. Computers with static IP addresses on the optional network must use the optional interface IP address of the Edge as the default gateway or router.

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

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 optional interface 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 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

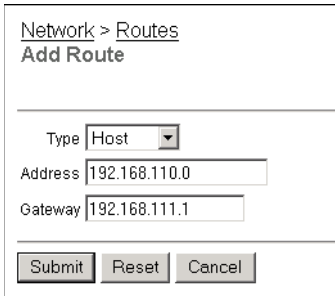
You can configure the Firebox® to send traffic to networks that are behind routers on your trusted network when you add static routes to these networks. Use the Routes page to make a static route:

- 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

3 Click **Add**.

The Add Route page appears.



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 CIDR, or Classless Inter Domain Routing, 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://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 FAQs:

What is Dynamic DNS?

http://watchguard.com/support/AdvancedFaqs/sogen_main.asp

How do I set up Dynamic DNS?

http://watchguard.com/support/AdvancedFaqs/sogen_setupdyndns.asp

You must 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 site:

<http://www.dyndns.org>

This site also has information about how Dynamic DNS operates.

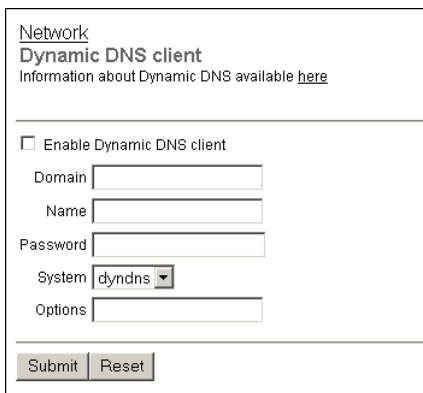
For more information, see the Technical Support FAQ “How do I set up Dynamic DNS?”

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

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 starts up. The Firebox connects to the IP address it finds for members.dyndns.org to register the current Firebox external interface 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 ping 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 feature, 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 must 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.

Failover Settings

☐ Enable failover using the **Modem (serial port)** 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:

- 2 Select the **Enable failover using the Ethernet (WAN2)/Modem (serial port) interface** check box.
- 3 From the drop-down list, select the interface for the feature: **Ethernet (WAN2)** or **Modem (serial port)**.
- 4 Type the IP addresses of the hosts to ping for the 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 **No Reply Limit** field.
- 7 Type the number of successful pings that must be made before the Edge uses the WAN1 interface again in the **Ping replies needed for fallback** field.

If you are using a broadband connection for failover

If you selected to enable failover with an Ethernet connection on WAN2, select your configuration mode from the drop-down list:

- 1 If your IP address is assigned automatically, select **DHCP Client**.
- 2 If you have a static IP address, select **Manual Configuration**.
- 3 If your IP address is assigned using PPPoE, select **PPPoE Client**.

If you selected DHCP Client

The screenshot shows the 'Ethernet (WAN2) Configuration' window. The 'Configuration Mode' dropdown is set to 'DHCP Client'. Below it, several fields are listed with the status 'Not Active' in blue text: 'IP Address', 'Subnet Mask', 'Default Gateway', 'Primary DNS server', 'Secondary DNS server', and 'DNS Domain Suffix'. The 'DHCP Identifier' field is empty, followed by the text '[optional]'. The 'Link Speed' dropdown is set to 'Automatic'.

- 1 If you must identify your computer when you request an IP address, type the name in the **Optional DHCP Identifier** field. If necessary, adjust the link speed from the drop-down list.
- 2 Click **Submit**.

If you selected Manual Configuration

The screenshot shows the 'Ethernet (WAN2) Configuration' window. The 'Configuration Mode' dropdown is set to 'Manual Configuration'. Below it, several text input fields are shown, each containing '0.0.0.0': 'IP Address', 'Subnet Mask', and 'Default Gateway'. Below these are three more empty text input fields: 'Primary DNS server', 'Secondary DNS server' (with '[optional]' to its right), and 'DNS Domain suffix'. The 'Link Speed' dropdown is set to 'Automatic'.

- 1 Type the IP address, subnet mask, default gateway, primary DNS, secondary DNS, and DNS domain suffix into the related fields. If necessary, select the appropriate link speed from the drop-down list.
If you completed the table on page 15, type the information from the table. If you do not have this information, speak with your ISP or corporate network administrator.
- 2 Click **Submit**.

If you selected PPPoE

See “If your ISP uses PPPoE” on page 63 for information on PPPoE settings. Configure the WAN2 interface using that 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

Use these steps to set up your external modem for failover:

- 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 and your account name in the relevant fields. If you have an alternate telephone number, you can enter that below the telephone number.
- 4 If you log in to your account with a domain name (such as msn.com), enter it in **Account Domain**.
- 5 Type the account password.
- 6 Select the **Enable modem and PPP debug trace** check box to create a log of the problem. Do not enable this check box unless you have problems with your connection.
- 7 Click **Submit**, or select a different tab to change more settings.

Modem (serial port) Configuration

Account

DNS

Dial Up

Dial Up Account Settings

Internet Service Provider

MSN

Telephone number

425-391-2506

Alternate telephone number

425-557-4266

[optional]

Account name

MyAccount

Account domain

wgrd

[optional]

Account password

☐ Enable modem and PPP debug trace

Dial-up DNS settings

If your dial-up ISP does not give DNS server IP addresses, or if 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. If you have a secondary DNS server, type type its IP address in the **Secondary DNS server** field.
- 3 Click **Submit**, or select a different tab to change more settings.

Modem (serial port) Configuration

Account
DNS
Dial Up

DNS Settings

☐ Manually configure DNS server IP addresses

Primary DNS server

Secondary DNS server [optional]

Dial-up settings

- 1 In the **Dial up time-out** field, enter 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.
- 5 Click **Submit**, or select a different tab to change more settings.

Modem (serial port) Configuration

Account
DNS
Dial Up

Dialing Options

Dial up time-out (minutes)

Redial attempts

Inactivity Timeout (minutes)

Speaker volume

Firebox X Edge Wireless Setup

Wireless networks use RF (radio frequency) signals to send and receive traffic from computers. The Firebox® X Edge Wireless protects the computers that are connected to your network and it protects your network wireless connections. The Firebox® X Edge Wireless obeys the 802.11b and 802.11g guidelines set by the Institute of Electrical and Electronics Engineers (IEEE). This chapter examines how to install the Firebox X Edge Wireless and set up the wireless network.

By default, the wireless features of your Firebox are disabled for more security. You must enable the wireless feature after you complete the Firebox X Edge Wireless Quick Setup wizard.

To install the Firebox X Edge Wireless:

- Identify and record your TCP/IP settings
- Disable the HTTP Proxy settings of your Web browser
- Activate DHCP on your computer
- Make a physical Ethernet connection between the Firebox X Edge Wireless and your network. You must connect to the Edge with a wired connection to configure its wireless properties.
- 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. This is an FCC requirement for low power transmitters.

- Put the Firebox X Edge Wireless in a location away from other antennae or transmitters to decrease interference.

To set up the wireless network:

- Select and configure the Firebox X Edge trusted or optional networks
- Configure the Wireless Access Point (WAP)
- Configure the wireless adapter on your computer

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 uses switch functionality to connect other computers.

To set up a wireless network, connect a computer with a Web browser to the Firebox X Edge Wireless with an Ethernet cable.

Use this computer to configure the wireless network.

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

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 task: **Configure the wireless network interface of the Firebox X Edge**.

Configuring Basic Wireless Settings

If you do not use the Wireless Network Wizard, or if you want to change wireless settings manually, you can use the Firebox X Edge Wireless 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 **Network > Wireless (802.11g)**.

[Network](#)
Wireless Configuration

Settings | Security | Allowed Addresses | Guest Services

Network assignment: None (Disable Wireless)

Network name (SSID):

Operating Region: Americas

Channel: Auto

The Firebox X Edge Wireless is intended for indoor use only.

☒ Broadcast SSID and respond to SSID queries

☒ Log Authentication Events

Wireless mode: 802.11g and 802.11b

Fragmentation Threshold: 2346 (256-2346 bytes)

Submit Reset

The Wireless Configuration page appears, with the Settings tab active.

NOTE

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

Selecting the wireless network assignment

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

None (disable wireless)

In this mode, the wireless feature is disabled.

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. If this option is selected, the wireless client can send any type of traffic to the other computers on the trusted network. This includes Windows Networking NetBIOS broadcasts, which are useful for users who browse with Windows Network Neighborhood.

Bridge to Optional

In this mode, the wireless client is a component of the optional network. You must use the Bridge to Optional mode if you enable guest services on the Firebox X Edge Wireless. If you use this option, you must first activate the optional network. The optional network 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. If this option is selected, the wireless client can send any type of traffic to the other computers on the optional network. This includes Windows Networking NetBIOS broadcasts.

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 they are optional or trusted network clients, a wireless client can be a part of any Branch Office VPN tunnels in which the local network component of the Phase 2 settings include optional or trusted network IP addresses. To control access to the VPN, you can force Firebox users to authenticate.

Setting the SSID

The SSID (Service Set Identifier) is the unique name of your wireless network. To use the wireless network from a client computer, the

wireless network card in your computer must have the same SSID as the Firebox X Edge Wireless.

To change the SSID of the Firebox X Edge Wireless, type a new name in the **SSID** field to uniquely identify your wireless network.

Setting the operating region and channel

There are eight options for operating region: Americas, Asia, Australia, EMEA, France, Israel, Japan and the People's Republic of China. This parameter is configured when you use the Quick Setup Wizard and cannot be changed after it is set.

The set of channels available for each operating region are in the **Channel** drop-down list. With the channel set to **Auto**, the Firebox X Edge automatically selects the channel with the strongest signal available in its physical location.

Controlling SSID broadcasts

Computers with wireless network cards 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 these requests, select the **Broadcast SSID and respond to SSID queries** check box. For security, turn this option on only when you are configuring computers on your network to connect to the Edge. Disable this option after all your clients are configured. If you use the wireless guest services feature, it can be necessary to allow SSID broadcasts in standard operation.

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 these events in the log file, select the **Log Authentication Events** check box.

Setting the wireless mode

Most wireless cards can operate only in 802.11b (up to 11 MB/second) or 802.11g (54 MB/second) 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:

802.11g only

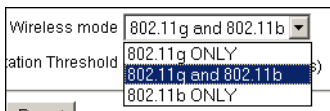
This is the default mode. This allows you to deny access to 802.11b clients so that you can keep the Edge operating in the faster 802.11g mode.

802.11g and 802.11b

This mode allows the Firebox X Edge Wireless to connect with devices that use 802.11b or 802.11g.

802.11b only

This mode allows the Firebox X Edge Wireless to connect to devices using only 802.11b.



NOTE

The Firebox X Edge only operates in 802.11g mode if all the wireless cards connected to the Edge are using 802.11g. If any 802.11b clients connect to the Edge, all connections automatically drop to 802.11b mode.

Setting the fragmentation threshold

The Edge Wireless allows you to set the maximum frame size it can send without fragmenting the frame. This is called the fragmentation threshold. This setting is rarely changed. It is set at the default maximum frame size of 2346, which means that it will never fragment any frames that it sends to wireless clients. This is best for most environments.

To change the fragmentation threshold, type a value in the **Fragmentation Threshold** field. The possible values are 256 through 2346. For more information on the fragmentation threshold parameter, see this FAQ:

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

Configuring Wireless Security Settings

The Firebox® X Edge uses two security protocol standards to protect your wireless network. They are WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access). WEP and WPA encrypt the transmis-

sions on the wireless LAN between the computers and the access points. WPA and WEP can also prevent unauthorized access to the wireless access point.

WEP and WPA each use pre-shared keys, but WPA can use an algorithm to change the encryption key at regular intervals. This keeps the data sent on a wireless connection more secure. If you use the Windows XP operating system with Service Pack 2 or higher, you can use WPA-PSK (WPA with pre-shared keys) with no additional driver installation. If you use an earlier version of Windows or a different operating system, it can be necessary to install other drivers to use WPA-PSK. If you cannot use WPA-PSK, WatchGuard recommends that you use Shared Key authentication with WEP encryption or MUVPN without WPA or WEP.

To protect privacy, you can use these features together with other LAN security mechanisms such as password protection, VPN tunnels, and user authentication.

- 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 (802.11g)** and click the **Security** tab.

[Network](#)
Wireless Configuration

Settings	Security	Allowed Addresses	Guest Services
----------	----------	-------------------	----------------

Authentication WPA-PSK
Encryption Auto
Passphrase

☐ Require encrypted MUVPN connections for wireless clients

Setting the wireless authentication method

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. 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, other methods are more secure.

Shared Key

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

WPA-PSK

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

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 and shared key authentication

Encryption options for open system and shared key authentication are WEP 64 bit hexadecimal, WEP 40 bit ASCII, WEP 128 bit hexadecimal, and WEP 128 bit ASCII. If you select open system authentication, you can also select no encryption.

- 1 If you use WEP encryption, type hexadecimal or ASCII characters in the **Key** text boxes. Not all wireless adapter drivers support ASCII characters.

You can have a maximum of four keys.

- 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 (0-f) characters.
- 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.

WPA-PSK authentication

The encryption options for WPA-PSK authentication are TKIP, AES, and Auto. WPA-PSK only operates correctly if you are using Windows XP Service Pack 2 or higher or have installed a driver for your operating system that supports PSK.

We recommend that you set the WPA-PSK encryption option to **Auto** to have the Firebox accept TKIP and AES settings.

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** and click the **Security** tab.

- 3 Select the check box **Require encrypted MUVPN connections for wireless clients**.

If you use WEP/WPA encryption and use encrypted MUVPN at the same time, network speeds will decrease.

- 4 Click **Submit**.

Restricting Wireless Access by MAC Address

You can control access to the Firebox®X Edge Wireless by computer hardware (MAC) address. If this feature is enabled, and the MAC address of a computer that tries to connect to the Firebox X Edge Wireless is not included in this configuration, the connection fails.

When you restrict wireless access by MAC address, it is possible that a hacker can get access to the wireless network by spoofing an allowed MAC address. Use authentication and encryption together

with MAC address restrictions to keep your wireless network connections secure.

- 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 (802.11g)** and click the **Allowed Addresses** tab.

The screenshot shows the 'Wireless Configuration' page with the 'Allowed Addresses' tab selected. The 'Restrict Access by Hardware Address' checkbox is checked. Below it, a list of 'Allowed Hardware Addresses' is displayed in a scrollable box, containing the following MAC addresses: 0004235013F2, 000BDBD9ABEA, 00042399AB46, 0004235012B5, 000423501162, 000E35D85A3D, 000E35D81731, 000e35d82e34, 000423a2b017, and 000423a2ade0. To the right of the list is a 'Remove' button. Below the list is a 'MAC Address' input field and an 'Add' button. At the bottom of the page are 'Submit' and 'Reset' buttons.

- 3 Select the **Restrict Access by Hardware Address** check box.
- 4 Click **Edit**.
- 5 Type the MAC address of the computer that is allowed to connect to the Firebox X Edge Wireless in the correct field.
See "Finding your TCP/IP properties" on page 14 for more information.
Look for the physical address of the wireless adapter.
- 6 Click **Add**.
Repeat steps 3–4 for each computer that can connect to the Edge.
- 7 Click **Submit**.

Configuring Wireless Guest Services

The Firebox® X Edge Wireless includes a default local user account called “guest”. A guest is a wireless user that is not usually connected to the wireless network. A guest could be a business associate visiting your organization and given temporary access to the Internet, or possibly to your trusted network. You can also use guest services if you use your Firebox X Edge to host wireless users other than the users the Firebox X Edge is protecting with its firewall.

WARNING

Both guests and regular Firebox users can get access to the Firebox X Edge through the wireless interface. Guest users can connect to all regular Firebox user computers on the wireless network and Firebox users can connect to all guest user computers. If you host wireless access for people outside your organization and keep other security settings low, the confidentiality of your data is at risk.

When guest services are enabled:

- The **Network Assignment** must be set to **Bridge to Optional Network** on the Wireless Configuration page.
- You must disable MAC address filters, or add the MAC address of each guest to the Allowed Hardware Addresses list.
- The guest user account is enabled. You can make users authenticate with a password, or without a password.

Enabling guest services

- 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 (802.11g)** and click the **Guest Services** tab.

The screenshot shows the 'Wireless Configuration' page with the 'Guest Services' tab selected. The page has a navigation bar with tabs: Settings, Security, Allowed Addresses, and Guest Services. The main content area contains the following options:

- ☐ Enable guest services.
 - ☐ Guest account is **not** password protected.
 - ☒ Guest account is password protected.
 - Password:
 - Confirm password:
- ☒ Guests can access the External Network.
- ☐ Guests can access the Trusted Network.
- ☐ Guests can access VPN.
- WebBlocker Profile:

At the bottom, there are two buttons: 'Submit' and 'Reset'.

- 3 Select the **Enable guest services** check box to turn on the guest service feature.

When you enable this feature, you also enable the default local user account "guest". Any user who gets access to the Firebox as a guest user must use the local user account named "guest". You cannot change the default name of the guest account.

Setting password protection

When a guest user connects to the wireless network using the Firebox X Edge Wireless as the wireless access point, you can make the user type a password, or disable password protection. If you disable password protection, the user does not have to type a password when they connect to the network.

Setting network access rules for guests

You can set the level of network access a guest user has on the Wireless Guest Services configuration page.

Guests can access the External Network

When this check box is selected, all wireless guests can use the Firebox X Edge as their access point to use resources on the

external network. This option is selected by default so that all guest users have access to the Internet.

Guests can access the Trusted Network

Select this check box to allow guest users to use resources on the trusted network protected by the Firebox X Edge.

Guests can access VPN

Select this check box to allow guest users to access VPN tunnels through the Firebox X Edge.

WebBlocker Profile

If you use WebBlocker, the options in this drop-down list control the types of web sites guest users can get access to through the Firebox X Edge. You can apply any existing WebBlocker profile to guest users. If this option is set to **No WebBlocker**, all guest users have full access to all web sites.

Connecting to the Firebox as a wireless guest

To log on as a wireless guest user, a user must open their Web browser and do one of these procedures:

- Type `https://` in their browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
- Try to get access to any HTTP Web site on the Internet. The Firebox X Edge will automatically redirect the user to the login Web page.
The Firebox will not automatically redirect a user who tries to get access to an HTTPS Web site.

The user must type “guest” as the user name. If password protection is not required, the user does not have to type a password in the password text box. They can keep the text box blank and click **OK**.

Configuring the Wireless Card on Your Computer

These instructions are for the Windows XP with Service Pack 2 operating system. To see the installation instructions for other operating systems, go to:

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

To set up a wireless connection using Windows XP SP2:

- 1 Click **Start > Settings > Control Panel > Network Connections**.
The Network Connections dialog box appears.
- 2 Right-click **Wireless Network Connection** and select **Properties**.
The Wireless Network Connection dialog box appears.
- 3 Select the **Wireless Networks** tab.
- 4 Below **Preferred Networks**, click **Add**.
The Wireless Network Properties dialog box appears.
- 5 Type the SSID in the **Network Name (SSID)** text box.
- 6 Select the network authentication and data encryption methods from the drop-down lists.
If necessary, clear the check box labeled **The key is provided for me automatically** and type the network key two times.
- 7 Click **OK** to close the **Wireless Network Properties** dialog box.
- 8 Click the **View Wireless Networks** button.
All available wireless connections appear in the Available Networks text box.
- 9 Select the SSID of the wireless network and click **Connect**.
If the network uses encryption, type the network key twice in the Wireless Network Connection dialog box and click **Connect** again.
- 10 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.

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 a Mobile User VPN tunnel from remote users, or when you create a Branch Office VPN tunnel to other offices, the Firebox X Edge automatically allows all traffic through that VPN tunnel. No other configuration is necessary after the VPN tunnel is set up.

About This Chapter

The section “Configuring Outgoing Services” on page 111 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 116 shows you how to control traffic between the trusted and optional networks. 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 MAC address of the Firebox hardware

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

The incoming services in this section have no effect on traffic between the trusted and optional networks. These services also have no effect on traffic between computers on the trusted network or between computers on the optional network.

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 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 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**.
By default, the Firebox does not allow incoming traffic to your network.

- 4 If you allow 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 steps 1–5 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. Traffic from that service goes to the service host.

To limit which the external sources can use the ports and protocols of the service you are adding, 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 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 filter.

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**.
The Filter Incoming Traffic page appears.
- 3 Scroll to the bottom of the page.

Custom Services

Filter	Service	Service Host	
Deny	 myservice	0.0.0.0	<div>EditDelete</div>

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 Settings** drop-down list, select **TCP Port**, **UDP Port**, or **Protocol**.
- 7 In the text box adjacent to the **Port/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 its number. IP protocols numbers include: 47 for GRE (Generic Routing Encapsulation) and 50 for ESP (Encapsulated Security Payload). Most settings are done with TCP or UDP ports.

- 8 Click **Add**.
Repeat steps 6–8 until you have a list of all the ports and protocols that this service uses. You can add more than one port and more than one protocol to a custom service. More ports and protocols make the network less secure. Add only the ports and protocols that are necessary.

Filtering incoming traffic for services

These steps restrict incoming traffic for a service to specified computers behind the firewall. Refer to the subsequent section 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**, type the IP address of the service host. This is the computer that receives the traffic.
To allow incoming traffic from the external network without restrictions, skip to step 7.
- 3 To limit incoming traffic from the external network to the service host, use the drop-down list to select **Host IP Address**, **Network IP Address**, or **Host Range**.
- 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 external network that can send traffic to the service host. Type Network IP addresses in "slash" notation (also known as CIDR or Classless Inter-Domain Routing notation). For more information on entering IP addresses in slash notation, see this FAQ: http://www.watchguard.com/support/advancedfaqs/general_slash.asp
- 5 Click **Add**. The **From** box shows the host range, host IP address, or network IP address that you typed.
Repeat steps 3–5 until all of the address information for this custom service is set. The From box can have more than one entry.
- 6 If this service is only for incoming traffic, keep the outgoing filter set to **No Rule**.
To limit which computers can send information using this service, go to the subsequent section, "Filtering outgoing traffic for services."
- 7 Click **Submit**.

Filtering outgoing traffic for services

These steps restrict outgoing traffic through the Firebox. Refer to the previous section for information on filtering incoming traffic.

- 1 From the **Outgoing Filter** drop-down list, select **Allow** or **Deny**.
To allow all outgoing traffic from the trusted or optional network to the external network using this service, skip to step 9.
- 2 To limit which computers on the trusted or optional network 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**.
To only limit which computers receive information, skip to step 5.

- 3 In the adjacent 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.
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 Click **Add**. The **From** box shows the IP addresses you added.
Repeat steps 2–4 until all of the address information for this custom service is set. The From box can have more than one entry.
- 5 To limit which computers on the external network can receive network traffic with this service, use the drop-down list below the **To** box to select **Host IP Address**, **Network IP Address**, or **Host Range**.
- 6 In the adjacent 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.
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.
- 7 Click **Add**. The **To** box shows the IP addresses you added.
Repeat steps 5–7 until all of the address information for this custom service is set. The To box can have more than one entry.
- 8 If this service is only for outgoing traffic, keep the Incoming Filter set to **No Rule**.
To limit which computers can receive information using this service, go to the previous section, "Filtering incoming traffic for services."
- 9 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.

By default, the Firebox® X Edge allows all traffic that starts in the trusted or optional networks to go to the external network. To deny outgoing connections, you must make rules for those connections.

NOTE

The outgoing services in this section have no effect on traffic between the trusted and optional networks. These services also have no effect on traffic between computers on the trusted network or between computers on the optional 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`
- 2 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

By default, the Firebox allows all traffic to go out to the external network. This is because the common service called Outgoing is set to **Allow**. When the Outgoing common service is set to **Deny**, all outgoing traffic is blocked. When the Outgoing common service is set to **No Rule**, traffic that is not specially permitted is blocked.

The Outgoing common service and other common services are found on the **Firewall > Outgoing** page.

- To allow all traffic from the trusted and optional networks to get to the external network, you must set the Outgoing common service to **Allow**.
- To allow only specified traffic from the trusted and optional network to get to the external network, you must:
 - Set the Outgoing common service to **No Rule**.
 - Select other common services and set them to **Allow**.

NOTE

To limit traffic sent from the trusted or optional networks not specified in a common service, you must create 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 Adjacent to **Define a custom service**, click **Go**.
- 3 Follow the instructions in the wizard.

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

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.

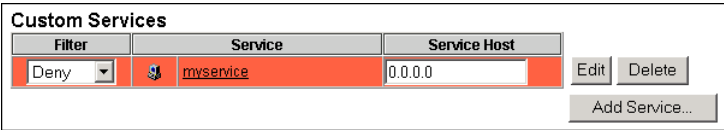
Restrict to local computers

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 > Outgoing**.
- 3 Scroll to the bottom of the page.



- 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, select **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 its number. IP protocols numbers include: 47 for GRE (Generic Routing Encapsulation) and 50 for ESP (Encapsulated Security Payload). Most settings are done with TCP or UDP ports.

- 8 Click **Add**.
Repeat steps 6–8 until you have a list of all the ports and protocols that this service uses. You can add more than one port and more than one protocol to a custom service. More ports and protocols can make the network less secure. Add only the ports and protocols that are necessary.

Filtering incoming traffic for services

To limit the computers that can send incoming traffic from the external network using the service, see “Filtering incoming traffic for services” on page 110.

Filtering outgoing traffic for services

To limit what computers can send traffic from the internal network using the service, and what computers on the external network can receive that traffic, see “Filtering outgoing traffic for services” on page 110.

Services for the Optional Network

By default, the Firebox® X Edge allows all traffic that starts in the trusted network and tries to go to the optional network, and 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.
- 3 To allow all traffic from the trusted network, select **Allow** for the Outgoing service from the **Filter** drop-down list.
- 4 To deny all traffic from the trusted network, select **Deny** for the Outgoing service from the **Filter** drop-down list.
- 5 To deny some traffic, but allow all other traffic from the trusted network to the optional network, set the Outgoing service to **Deny** from the **Filter** drop-down list. Then, for each service that is permitted, select **Allow** from the **Filter** drop-down list.
- 6 Click **Submit**.

Disabling traffic filters

To allow network traffic from the optional network to the trusted network, you must 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

Submit

Reset

Blocking External Sites

A blocked site is an external IP address that is always blocked from connecting to computers behind the Edge. 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 and stop further attacks from that address range. Use the IP address of the attacker or a range of hostile IP addresses to create a Blocked Site.

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, a table titled 'Blocked Sites' contains one entry with the IP address '10.1.2.1'. To the right of this entry is a 'Remove' button. Below the table, there's a form to add a new entry. It includes a dropdown menu labeled 'Host IP Address' with a 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.
Repeat steps 2–4 to add many IP addresses at one time.
- 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 the Edge from the Trusted Network.

☐ 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 ping requests. This option overrides all other Firebox settings.

- 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 Firebox X Edge

You can configure the Firebox X Edge to not allow any FTP connections from the trusted network. This option overrides all other Firebox settings.

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

NOTE

You must clear the **Do not allow FTP access to the Edge from the Trusted Network** check box when you apply an update to the Edge firmware with the automatic installer. If you do not clear this check box, the Software Update Installer cannot move firmware files to the Firebox X Edge.

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 external interface. 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 do not see the option for the Failover Network if you do not have the WAN Failover option installed.

- 2 In the **External network override MAC 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**.

If the changes are successful, you must restart the Firebox.

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. To keep the information permanently, you must configure an external syslog or Log Server.

Viewing Log Messages

The Firebox® X Edge keeps a maximum of 300 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.

Use this procedure 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 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 a primary Log Server to collect the log messages from your Firebox X Edge. You can also configure a backup Log Server. If the Firebox X Edge cannot connect to the primary Log Server, it tries to connect to the backup Log Server. It sends log messages to the backup Log Server until the primary Log Server becomes available. When the Firebox X Edge can resume its connection to the primary Log Server, it automatically starts to send log messages to the primary Log Server again. For instructions on how to configure the Log Server to accept the log messages, see the

WatchGuard System Manager User Guide. 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** > **WatchGuard Logging**.
The WatchGuard Logging page appears.

Logging
WatchGuard Logging

☒ Enable WatchGuard Logging

Device Name

Primary Log Host

Log Host IP Address

Log Encryption Key

Confirm Key

Backup Log Host

Log Host IP Address

Log Encryption Key

Confirm Key

- 3 Select the **Enable WatchGuard Logging** check box.
- 4 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. The Device Name appears in the Log Viewer. If this field is clear, the Firebox X Edge is identified in the log by the IP address of the Firebox external interface.
- 5 Below Primary Log Host, type the IP address of the primary Log Server in the **Log Host IP Address** field.
- 6 Type a passphrase in the **Log Encryption Key** field and confirm the passphrase in the **Confirm Key** field.
The same passphrase must also be used when the Log Server is configured to receive log messages from this Firebox X Edge.

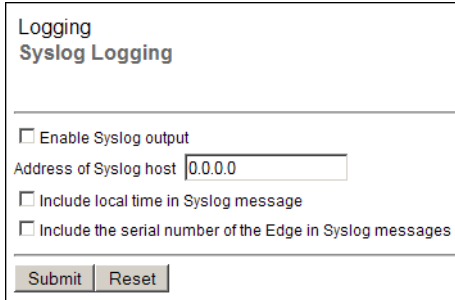
- 7 If you have a backup Log Server available, type its IP address and Log Encryption Key.
If the Firebox X Edge cannot connect to the primary Log Server, it will send log messages to the backup Log Server until the primary Log Server becomes available again.
- 8 Click **Submit**.

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.

Follow these instructions to 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 the serial number of the Edge 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 To include the local time in the syslog messages, select the **Include local time in syslog message** check box.

- 6 To include the Firebox X Edge serial number in the syslog messages, select the **Include serial number in syslog messages** check box.

This setting is 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. You can change the NTP server that the Edge uses, or you can set the system time manually.

To 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`

- From the navigation bar, click **Logging > System Time**.
The System Time page appears.

Logging

System Time

Time Zone

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

☒ Adjust for daylight savings time

Time Source
☒ Use NTP to periodically automatically set system time.

NTP Servers

ntp3.cs.wisc.edu
ntp1.cs.wisc.edu
ntp-0.cso.uiuc.edu
ntp-1.cso.uiuc.edu
ntp-2.cso.uiuc.edu

Remove

Add New Server

Add

If you do not select an NTP server, default servers are automatically selected when you click submit.

☐ Set date and time manually

using input fields

Date

September

2004

Sun	Mon	Tue	Wed	Thu	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

Time

6 : 12 : 00 PM

Submit

Reset

- Select the time zone from the drop-down list.
If your area uses daylight savings time, select the **Adjust for daylight savings time** check box.
- To set the system time automatically, select the **Use NTP to periodically automatically set system time** option. To set the time manually, select the **Set date and time manually** option.
If you set the system time manually, skip to step 6.
- If you set the system time automatically, the Edge gets the current time from the selected server in the NTP Servers list. If a server is not available, the Edge uses the subsequent server.

- To add a time server, type the server name in the **Add New Server** field and click **Add**.
 - To remove a time server, select the server from the NTP Servers list and click **Remove**.
 - Click a server to select it as the default time server.
- To save your changes, skip to step 8.
- 6 If you set the system time manually, you must set the date and time separately.
 - Select the month from the first drop-down list.
 - Select the year from the second drop-down list.
 - Click the button with the number that is today's date.
 - 7 To the right of the date, set the time.
 - Type the hours in the first field.
 - Type the minutes in the second field.
 - Type the seconds in the third field.
 - Select **AM** or **PM** from the drop-down list.
 - 8 Click **Submit**.

Managing Users and Groups

The Firebox® X Edge includes tools you can use to manage your network and your users. You can create users and manage access to the Internet or to your VPN tunnels with user authentication. Or, you can allow free access to the Internet and VPN tunnels to all users. In this chapter, you learn to do these tasks:

- Examine current users and properties
- Configure local Firebox authentication
- Configure the Firebox to use LDAP or Active Directory authentication
- Allow internal hosts to bypass user authentication

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. 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.

NOTE

Only sessions from computers on the Edge's trusted or optional network to computers on the external network use a user license. For

more information on user licenses, see “About User Licenses” on page 137.

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.

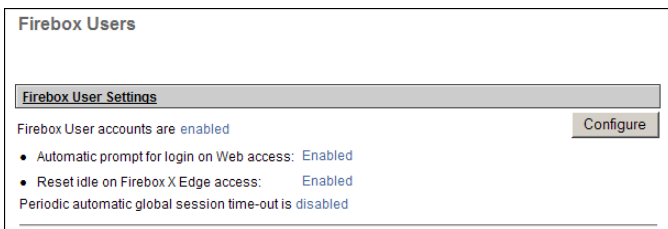
The default URL is: `https://192.168.111.1`.

- 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. To get access to the configuration page for these settings, click the **Configure** button to open the Settings page. For more information, see “Using Local Firebox Authentication” on page 142 and “Configuring MUVPN client settings” on page 140.



Active Sessions

If local user accounts are enabled, the **Active Sessions** section of the Firebox Users page shows information for all current sessions, including:

- The name of the user who started the session
- The total time since the session started
- The time between the last packet and the session expiration is known as the idle time. If the idle time is set 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

If local user accounts are not enabled, each active session shows the IP address of the hosts that have started sessions.

Stopping a session

The Edge monitors and records the properties of each user session.

If the Automatic Session Termination time limit for all sessions is reached, or if the Edge restarts, all sessions are stopped at the same time. The Edge administrator can also use the Firebox Users page to stop a session.

To stop 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 stop all sessions, click the **Close All** button.

If Firebox user authentication is enabled for external network connections, a session stops when one of these events occurs:

- The idle time-out limit set for that account is reached.
- The maximum time limit set for that account is reached.
- The Firebox user manually stops the session.


To stop the session, the user clicks the **Logout** button on the Login Status dialog box and closes all open browser windows.

You can increase the number of sessions available with a license upgrade. For more information, see the FAQ:

https://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/products/purchaseoptions.asp>



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

If a session used a user license and the session closes, the user license is available for a different user. For more information on user licenses, see “About User Licenses” on page 137.

Local User Accounts

Below **Local User Accounts**, you can see information on the users you configured to use this Edge:

- **Name:** The name given to the user. The Admin user is part of the default configuration and cannot be deleted.
- **Admin Level:** You can set the user permissions to Full, None, or Read-only. For more information, see “Using Local Firebox Authentication,” on page 142.
- **Options:** You can configure a user to use WebBlocker or MUVPN.

Local User Accounts					
					Add...
Name	Admin Level	WebBlocker	MUVPN	Edit	Delete
admin	Full	No WebBlocker	Disabled		

If local user accounts are enabled, you also see information about Internet and VPN access rights .

Editing a user account

To edit a user account, click the **Edit** icon. For descriptions of the fields you can configure, see “Using Local Firebox Authentication,” on page 142.

Deleting a user account

To remove a user account, click the **X** adjacent to the account name. A dialog box appears. Click **Yes** to remove the account.

About User Licenses

The Firebox® X Edge comes with a set number of available user licenses. The number of user licenses puts a limit on how many users can access the Internet at one time. The total number of available user licenses is set by the Edge model you have and any upgrade licenses you apply.

The Firebox Users page shows the maximum number of user licenses available and how many are in use at a given time.

You use a user license when you send traffic from the trusted or optional network to the external network.

You do not use a user license when you make connections between computers on the trusted network or through a VPN tunnel. You also do not use a user license when you make connections from the trusted network to the optional network.

If you make users authenticate before they connect to the external network, you can make sure that no user licenses are used by unauthorized computers. If authentication is required, and a user or computer tries to connect to the external network without authenticating, the Edge does not allow the connection.

About User Authentication

The Firebox® X Edge uses advanced authentication options to increase network security. You can configure the Firebox X Edge as a local authentication server. You can also configure the Firebox to use an existing Active Directory or LDAP authentication server. When you use LDAP authentication, account privileges for users that authenticate to the Active Directory/LDAP server are based on group membership.

User authentication gives options to prevent connections to some resources and to help decrease the number of user 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.

Setting authentication options for all users

Some authentication options apply to all users. To set or 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).
☒ Automatically prompt for login on Web access.
☒ Reset idle timer on Firebox X Edge embedded Web site access.
☐ Enable automatic session termination every

LDAP Authentication Service

You can use LDAP authentication to have Firebox X Edge users log in using your Active Directory domain or other LDAP defined user accounts.

☒ Enable LDAP authentication.
 Domain Name
 LDAP server type
 LDAP Server Address
 LDAP Server Port
 LDAP Timeout
 Search Base

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 (Enable local user accounts):**
 When you select this check box, all users must authenticate to the Firebox X Edge before they can access the external network. If you do not select this check box, there is no user-based control for access to the Internet or VPN tunnels.
- Automatically prompt for login on Web access:** When this option is selected, the authentication dialog box launches any time a user who has not yet authenticated tries to get access to the Internet.
- 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 overrides all other authentication options. It lets you clear the list of sessions in use and make all user licenses 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 accidental changes. 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."

Authenticating to the Edge

When you authenticate with the Edge, it automatically identifies your Administrative Access level. If you select the **Automatically prompt for login on Web access** option from **Firebox Users > Settings**, users will see the login dialog box when they open their web browser. If you select this option or not, you can always open the authentication login dialog box with this procedure:

- 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 that support Java script, 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 continue.

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 with 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. This dialog box is known as the Login Status dialog box.

If you are using local authentication, you must type your name as it appears in the Firebox user list. If you use Active Directory or another LDAP server for authentication through the Firebox X Edge, you must include the domain name. For example, if the administra-

tor authenticates using the local Firebox user list, the administrator types `admin`. If the admin user authenticates with an LDAP authentication server through the Firebox X Edge, the administrator must type `MyCompany\admin`.

When you authenticate with the Edge and make an Internet connection, your user name appears in the **Active Sessions** section of the Firebox Users page.

Using Local Firebox Authentication

When you create a local 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

- 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 authentication.
- 6 In the **Description** field, type a description for the user. This is for your information only. A user does not use this description during authentication.
- 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 144.

- 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 (0) minutes, there is no session time-out and the user can stay connected for any length of time.
- 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 (0) 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 see 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.
- Launch configuration wizards from the Wizard page.

If you try to do these things, you get a message that tells 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 159.

Enabling MUVPN for a user

To enable MUVPN for a new user, see "Connecting and Disconnecting the MUVPN Client" on page 207.

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, "Using Local Firebox Authentication" on page 142.

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 settings. For more information, see "Resetting the Firebox to the factory-default settings" on page 42.

We recommend that you change the administrator passphrase at regular intervals. Use a passphrase of at least eight letters, numbers, and symbols. Do not use a word from an English or other dictionary. Use one or more symbols, a number, and a mixture of upper case and lower case letters for increased security.

Changing a user account name or password

You can change an account name or account password. 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 'Firebox Users' and 'Edit User: cfgview'. Below this are three tabs: 'Settings', 'WebBlocker', and 'MUVPN', with 'Settings' being the active tab. The main form contains the following fields and controls:

- Account Name:** 'cfgview' (text label)
- Full name:** 'Able to view Config' (text input)
- Description:** 'Read not write' (text input)
- Change Identification:** A button highlighted with a green circle.
- Administrative Access:** A dropdown menu currently showing 'Read Only'.
- Session maximum time-out:** '0' (text input) followed by '(minutes)'.
- Session idle time-out:** '0' (text input) followed by '(minutes)'.
- Allow access to the External Network:** A checked checkbox.
- Allow access to VPN:** A checked checkbox.
- Submit** and **Reset** buttons at the bottom.

Using LDAP/Active Directory Authentication

If you use LDAP authentication, you do not have to keep a separate user database on the Firebox®. You can configure the Firebox to for-

ward user authentication requests to a generic LDAP or Active Directory server. You can use LDAP authentication and local Firebox authentication at the same time.

With LDAP authentication, user privileges are controlled on a group basis. You can add the names of your existing LDAP or Active Directory user groups to the Firebox configuration and assign privileges and a WebBlocker profile. When users authenticate to the Firebox, they prepend their LDAP domain name to their user name in the authentication dialog box (domain\user name). If you use an Active Directory authentication server, users can also authenticate using their fully qualified domain name (username@mycompany.com).

Configuring the LDAP/Active Directory authentication service

When you enable LDAP authentication, you define one authentication server and its properties. To enable LDAP authentication:

- 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 **Firebox Users > Settings**.
The Firebox Users Settings page appears.

The screenshot shows the 'Firebox Users Settings' page. At the top, there's a breadcrumb 'Firebox Users > Settings'. Below it, the 'Firebox User Access Restriction Enforcement and Options' section contains several checkboxes: 'Require user authentication (enable local user accounts)' (unchecked), 'Automatically prompt for login on Web access' (checked), 'Reset idle timer on Firebox X Edge embedded Web site access' (checked), and 'Enable automatic session termination every' (unchecked, with a dropdown set to 'hour'). The 'LDAP Authentication Service' section is highlighted with a green rounded rectangle. It includes the text 'You can use LDAP authentication to have Firebox X Edge users log in using your Active Directory domain or other LDAP defined user accounts.' and a checkbox 'Enable LDAP authentication.' which is checked. Below this are input fields for 'Domain Name', 'LDAP server type' (dropdown set to 'Active Directory'), 'LDAP Server Address', 'LDAP Server Port' (set to '389'), 'LDAP Timeout' (dropdown set to '10 seconds'), and 'Search Base'. A 'Test LDAP Account...' button is at the bottom of this section. The 'Firebox User Common MUVPN Client Settings' section follows, with the text 'The following settings apply to all MUVPN clients.' and a checkbox 'Make the MUVPN client security policy read-only.' (unchecked). Below this are 'Virtual Adapter' (dropdown set to 'Disabled'), 'DNS Server Address' (optional), and 'WINS Server Address' (optional). At the very bottom are 'Submit' and 'Reset' buttons.

- Select the **Enable LDAP authentication** check box.
If user authentication is not enabled in the top section of this configuration page, the LDAP Authentication Service section is not active.
- In the **Domain Name** text box, type the name of the LDAP domain. Do not include the top-level domain.
The domain (or host) name is the part of your company's URL that ends with .com, .net, .org, .biz, .gov, or .edu. For example, if your company URL is mycompany.com, type mycompany in the Domain Name text box.
- From the **LDAP server type** drop-down list, select the type of LDAP implementation you use in your organization: **Active Directory** or **Generic LDAP**.

- 6 In **LDAP Server Address** text box, type the IP address of the LDAP server the Firebox X Edge will use for authentication requests.
The LDAP server can be located on any Firebox interface or available through a VPN tunnel.
- 7 In the **LDAP Server Port** text box, type the port number the Firebox X Edge will use for connections to the LDAP server.
The default LDAP server port number is 389. You do not usually have to change this number.
- 8 Use the **LDAP time-out** drop-down list, select the number of seconds to use as a time-out for any LDAP operation.
- 9 In the **Search Base** text box, type the base in the LDAP directory to start the search for user account entries. This must be a legitimate LDAP DN (Distinguished Name).
A Distinguished Name is a name that uniquely identifies an entry in an LDAP directory. A DN includes as many qualifiers as it must to find an entry in the directory. For example, a DN can look like this:
OU=user accounts,DC=mycompany,DC=com
- 10 If you select Generic LDAP as the LDAP server type, you must enter a **Login Attribute Name** and **Group Attribute Name** in the appropriate text boxes. These text boxes do not appear if you select Active Directory as the LDAP server type.
The **Login Attribute Name** is the name of the login name attribute of user entries in the LDAP directory.
The **Group Attribute Name** is the name of the group membership attribute of user entries in the LDAP directory.
- 11 Click **Submit**.

Using the LDAP authentication test feature

After the Firebox X Edge is configured to use LDAP authentication, you can use the LDAP authentication test feature to make sure the Firebox can connect to the LDAP server. You can use the test for a specified user account to make sure that the Firebox can successfully send and receive authentication requests for that user.

To use the test feature, click **LDAP Authentication Test** and type the name and password of an LDAP user account. The user name must be typed in the domain\user name format, such as mycompany\admin.

The results of the authentication attempt are shown on the screen. If the authentication is successful, the User Permissions section shows the access rights for this user account.

Configuring groups for LDAP authentication

Account privileges for users that authenticate to an LDAP server are set based on group membership. The group that the user is in sets all privileges for that user except MUVPN. MUVPN privileges must be set at the user level.

The name you give to a group on the Firebox X Edge must match the name of the group assigned to user entries in the LDAP directory. On the Edge, there is a built-in default group. The settings of the default group apply to any LDAP user that does not belong to any group configured on the Edge. You can change the properties of the default group, but you cannot delete the default group.

If a user belongs to more than one group, the privileges for that user are set to the least restrictive settings of all groups to which the user belongs. In WebBlocker, the least restrictive profile is the profile with the lowest number of blocked categories. For a more general example, a group “admins” allows administrative access, but the group “powerusers” gives read-only access, and the group “everyone” gives no administrative access. A user that belongs to all three groups gets administrative access because it is the least restrictive setting of the three.

Adding a group

- 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 > New Group**.

The Firebox Users New Group page appears.

- 3 In the **Account Name** text box, type the name of the new group. This name must match the name of a group in the LDAP directory.
This name must contain only letters, numbers, and the underscore (_) or dash (-) characters. Spaces are not permitted.
- 4 In the **Description** text box, you can enter a description of the group. This field is optional.
- 5 From the **Administrative Access** drop-down list, select the level of Firebox X Edge administrative access to assign to the group. You can select:
 - None** - The members of the group have no access to Firebox X Edge administration functions.
 - Read-only** - The members of this group can see, but not change, Firebox X Edge configuration and status.
 - Full** - The members of this group have full Firebox X Edge administrative privileges.
- 6 Use the **Session maximum time-out** text box to set the number of minutes a user session started by a member of this group is allowed to stay active. When this limit occurs, the Firebox will close the session.
- 7 Use the **Session idle time-out** text box to set the number of minutes a user session started by a member of this group can stay idle before it is automatically closed by the Firebox.

- 8 Select the **Allow access to the External Network** check box to allow the members of this group to access the external network through the Firebox X Edge.
- 9 Select the **Allow access to VPN** check box to allow the members of this group to access VPN tunnels using the Firebox X Edge.
- 10 Click **Submit**.

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 control access to external Web sites. To apply a WebBlocker profile to the group, 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. If no profile is assigned, the users in this group have full access to all web sites. For more information on WebBlocker profiles, see "Creating WebBlocker Profiles" on page 159.

LDAP Authentication and MUVPN

Because MUVPN settings cannot be assigned at the group level, you must create a local Firebox user account for the user and add MUVPN settings for the user on the MUVPN. See "Using Local Firebox Authentication" on page 142 for more information.

Allowing Internal Hosts to Bypass User Authentication

You can make a list of internal hosts that bypass user authentication settings. If a host is on this list, a user at that host does not have to

authenticate to get access to the Internet. No WebBlocker rules apply to Web traffic originating from hosts on this list.

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

Firebox Users
Trusted Hosts

Trusted Hosts

Remove

Host IP Address 0.0.0.0 Add

Submit Reset

- 2 In the **Host IP Address** text box, type the IP address of the computer on your trusted or optional network to allow to browse the Internet without authentication restrictions.
- 3 Click **Add**.
Repeat step 2 for other trusted computers.
- 4 Click **Submit**.
To remove a computer from the list, select the address and click **Remove**.

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 offensive web sites.

NOTE

You must purchase the WebBlocker upgrade to use this feature.

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 examines the WebBlocker database. If the web site is not in the database or is not blocked, the page opens. If the web site is in the WebBlocker database and is blocked, a notification appears and the web site is not displayed.

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 time-out
- Set a rule for the Firebox action if the Firebox X Edge cannot connect to the WebBlocker server
- Set a rule for the Firebox action if the WebBlocker license expires
- 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)

When the WebBlocker server is unavailable, access to all sites is denied

When the WebBlocker license expires, access to all sites is denied

Message for blocked user field:

- 3 Select the **Enable WebBlocker** check box to turn on the WebBlocker feature.
- 4 Type a password in the **Full Access Password** field.
The full access password gives access to all web sites until the inactivity timeout is reached or until an authenticated user logs out.
- 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. The value can be from 1 to 1440 minutes.

- 7 Use the **When the WebBlocker server is unavailable, access to all sites is** drop-down list to select if the Firebox is to allow or deny all traffic when it cannot connect to the WebBlocker server.

If you allow web traffic when the WebBlocker server is unavailable, each user who sends a web request must wait 45 seconds for the Firebox to try to connect to the WebBlocker server and time-out. After 45 seconds, the Firebox will allow access to the web site. When the Firebox X Edge can connect to the WebBlocker server again, it will automatically start to apply WebBlocker rules again.

- 8 Use the **When the WebBlocker license expires, access to all sites is** drop-down list to select if the Firebox is to allow or deny all web traffic if the WebBlocker subscription expires.

If the WebBlocker subscription is renewed, the Firebox will keep the previous configuration and apply WebBlocker rules again.

- 9 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 (>) symbols, 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  
Adult/Sexually Explicit.  
This web site does not comply with our  
Internal Use Policy.
```

- 10 Click **Submit**.

Creating WebBlocker Profiles

A WebBlocker profile is a set of restrictions you apply to users or 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 Firefox® User accounts. This procedure appears in Chapter 9, “Managing Users and Groups.”

- 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: SeniorManagement Delete New

WebBlocker Categories

<input type="checkbox"/> Adult	<input type="checkbox"/> Shopping
<input checked="" type="checkbox"/> Adult/Sexually Explicit	<input checked="" type="checkbox"/> Advertisements
<input checked="" type="checkbox"/> Drugs, Alcohol & Tobacco	<input checked="" type="checkbox"/> Food & Drink
<input checked="" type="checkbox"/> Gambling	<input checked="" type="checkbox"/> Motor Vehicles
<input checked="" type="checkbox"/> Glamour & Intimate Apparel	<input checked="" type="checkbox"/> Real Estate
<input checked="" type="checkbox"/> Sex Education	<input checked="" type="checkbox"/> Shopping
<input type="checkbox"/> Crime	<input type="checkbox"/> Computers
<input checked="" type="checkbox"/> Criminal Skills	<input checked="" type="checkbox"/> Chat
<input checked="" type="checkbox"/> Hacking	<input checked="" type="checkbox"/> Computing & Internet
<input checked="" type="checkbox"/> Hate Speech	<input checked="" type="checkbox"/> Hosting Sites
<input checked="" type="checkbox"/> Violence	<input checked="" type="checkbox"/> Remote Proxies
<input checked="" type="checkbox"/> Weapons	<input checked="" type="checkbox"/> Web-based Email
<input type="checkbox"/> Entertainment	<input type="checkbox"/> News
<input checked="" type="checkbox"/> Arts & Entertainment	<input checked="" type="checkbox"/> News

4 In the **Profile Name** field, type a familiar name.

Use this name to identify the profile during configuration. For example, give the name "90day" to a group of employees at your company that work for less than 90 days.

5 In **WebBlocker Categories**, select the categories of web sites to block by clicking the check box adjacent to the category name.

For more information on categories, see the next section. If you select the check box adjacent to a category group, it automatically selects all of the categories in that group. If you clear the check box adjacent to a category group, all of the categories in that group will be deselected.

6 Click **Submit**.

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

NOTE

If you do not use user authentication, the default WebBlocker profile is applied to all users. For more information about user authentication, see Chapter 9 "Managing Users and Groups".

WebBlocker Categories

The WebBlocker database contains nine groups of categories with 40 individual 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.

Category	Description of Content
Adult/ Sexually Explicit	<ul style="list-style-type: none">• Sexually oriented or erotic full or partial nudity• Depictions or images of sexual acts, including inanimate objects used in a sexual manner• Erotic stories and textual descriptions of sex acts• Sexually exploitive or sexually violent text or graphic• Bondage, fetishes, genital piercing• Adult products including sex toys, CD-ROMs, and videos• Adult services including videoconferencing, escort services, and strip clubs• Explicit cartoons and animation• Child pornography/pedophilia• Online groups, including newsgroups and forums that are sexually explicit in nature• Naturist sites that feature nudity• Erotic or fetish photography which depicts nudity
Advertise- ments	<ul style="list-style-type: none">• Banner Ad servers• Pop-up advertisements• Adware
Arts & Entertain- ment	<ul style="list-style-type: none">• Television, movies, music, and video programming guides• Comics, jokes, movie, video, or sound clips• Performing arts (theatre, vaudeville, opera, symphonies, etc.)• Online magazines and reviews on the entertainment industry• Dance companies, studios, and training• Broadcasting firms and technologies (satellite, cable, etc.)• Book reviews and promotions, variety magazines, and poetry• Jokes, comics, comic books, comedians, or any site designed to be funny or satirical• Online museums, galleries, artist sites (including sculpture, photography, etc.)• Celebrity fan sites• Horoscopes• Online greeting cards• Amusement/theme parks
Chat	<ul style="list-style-type: none">• Web-based chat• Instant Message servers

Category	Description of Content
Computing and Internet	<ul style="list-style-type: none"> • Reviews, information, computer buyer's guides, computer parts and accessories, and software • Computer/software/Internet companies, industry news, and magazines • Pay-to-surf sites • Downloadable (non-streaming) movie, video, or sound clips • Downloadable mobile phone/PDA software, including themes, graphics, and ringtones • Freeware and shareware sites • Personal storage and backup • Clip art, fonts, and animated GIF pages <p>Note: Does not include update sites for operating systems, anti-virus agents, or other business-critical programs.</p>
Criminal Skills	<ul style="list-style-type: none"> • Advocating, instructing, or giving advice on performing illegal acts • Tips on evading law enforcement • Lock-picking and burglary techniques • Phishing • Phone service theft advice • Plagiarism and cheating, including the sale of research papers
Drugs, Alcohol, & Tobacco	<ul style="list-style-type: none"> • Recipes, instructions, or kits for manufacturing or growing illicit substances, including alcohol, for purposes other than industrial usage • Glamorizing, encouraging, or instructing in the use of or masking the use of alcohol, tobacco, illegal drugs, and other substances that are illegal to minors • Alcohol and tobacco promotional web sites • Information on "legal highs": glue sniffing, misuse of prescription drugs, and abuse of other legal substances • Distributing alcohol, illegal drugs, or tobacco free or for a charge • Displaying, selling, or detailing the use of drug paraphernalia <p>Note: SurfControl does not include sites that discuss medicinal drug use, industrial hemp use, or public debate on the issue of legalizing certain drugs. SurfControl also does not include sites sponsored by a public or private agency that provide educational information on drug use.</p>

Category	Description of Content
Education	<ul style="list-style-type: none"> • Educational institutions, including pre-, elementary, secondary, and high schools; universities • Educational sites: pre-, elementary, secondary, and high schools; universities • Distance education, trade schools, and online courses • Online teacher resources (lesson plans, etc.)
Finance & Investment	<ul style="list-style-type: none"> • Stock quotes, stock tickers, and fund rates • Online stock or equity trading • Online banking and bill-pay services • Investing advice or contacts for trading securities • Money management/investment services or firms • General finances and companies that advise thereof • Accountants, actuaries, banks, mortgages, and general insurance companies
Food & Drink	<ul style="list-style-type: none"> • Recipes, cooking instruction and tips, food products, and wine advisors • Restaurants, cafes, eateries, pubs, and bars • Food/drink magazines and reviews
Gambling	<ul style="list-style-type: none"> • Online gambling or lottery web sites that invite the use of real money • Information or advice for placing wagers, participating in lotteries, gambling real money, or running numbers • Virtual casinos and offshore gambling ventures • Sports picks and betting pools • Virtual sports and fantasy leagues that offer large rewards or request significant wagers <p>Note: Casino/hotel/resort sites that do not feature online gambling or provide gaming tips are categorized under Travel.</p>
Games	<ul style="list-style-type: none"> • Game playing or downloading; game hosting or contest hosting • Tips and advice on games or obtaining cheat codes ("cheatz") • Journals and magazines dedicated to online game playing
Glamour & Intimate Apparel	<ul style="list-style-type: none"> • Lingerie, negligee or swimwear modeling • Model fan pages; fitness models/sports celebrities • Fashion or glamour magazines online • Beauty and cosmetics • Modeling information and agencies

Category	Description of Content
Government & Politics	<ul style="list-style-type: none">• Government services such as taxation, armed forces, customs bureaus, and emergency services• Local government sites• Political debate, canvassing, election information, and results• Local, national, and international political sites• Conspiracy theorist and alternative government views that are not hate-based
Hacking	<ul style="list-style-type: none">• Promotion, instruction, or advice on the questionable or illegal use of equipment and/or software for purpose of hacking passwords, creating viruses, or gaining access to other computers and/or computerized communication systems• Sites that provide instruction or work-arounds for filtering software• Cracked software and information sites; "warez"• Pirated software and multimedia download sites• Computer crime• Sites that provide or promote information gathering or tracking that is unknown to, or without the explicit consent of, an end user or organization• Sites that distribute malicious executables or viruses• 3rd-party monitoring and other unsolicited commercial software

Category	Description of Content
Hate Speech	<ul style="list-style-type: none">• Advocating or inciting degradation of or attacks on specified populations or institutions based on associations such as religion, race, nationality, gender, age, disability, or sexual orientation• Promoting a political or social agenda that is supremacist in nature or exclusionary of others based on their race, religion, nationality, gender, age, disability, or sexual orientation• Holocaust revisionist/denial sites• Coercion or recruitment for membership in a gang* or cult**• Militancy, extremist• Flagrantly insensitive or offensive material, including lack of recognition or respect for opposing opinions or beliefs <p>Note: SurfControl does not include news, historical, or press incidents that may include the above criteria in this category (except in graphic examples).</p> <p>*A gang is defined as: a group whose primary activities are the commission of felonious criminal acts, which has a common name or identifying sign or symbol, and whose members individually or collectively engage in criminal activity in the name of the group.</p> <p>**A cult is defined as: a group whose followers have been deceptively and manipulatively recruited and retained through undue influence such that followers' personalities and behavior are altered. Leadership is all-powerful, ideology is totalistic, the will of the individual is subordinate to the group, and the group is outside society.</p>
Health & Medicine	<ul style="list-style-type: none">• General health such as fitness and well-being• Alternative and complementary therapies, including yoga, chiropractic, and cranio-sacral• Medical information and reference about ailments, conditions, and drugs• Medical procedures, including elective and cosmetic surgery• Hospital, medical insurance• Dentistry, optometry, and other medical-related sites• General psychiatry and mental well-being sites• Promoting self-healing of physical and mental abuses, ailments, and addictions• Psychology, self-help books, and organizations

Category	Description of Content
Hobbies & Recreation	<ul style="list-style-type: none"> • Recreational pastimes such as collecting, gardening, or kit airplanes • Outdoor recreational activities such as hiking, camping, rock climbing • Tips or trends focused on a specific art, craft, or technique • Online publications on a specific pastime or recreational activity • Online clubs, associations or forums dedicated to a hobby • Traditional (board, card, etc.) games and their enthusiasts • Animal/pet related sites, including breed-special sites, training, shows, and humane societies • Beauty and cosmetics
Hosting Sites	<ul style="list-style-type: none"> • Web sites that host business and individual web pages (i.e. GeoCities, earthlink.net, AOL)
Job Search & Career Development	<ul style="list-style-type: none"> • Employment agencies, contractors, job listings, career information • Career searches, career-networking groups
Kids' Sites	<ul style="list-style-type: none"> • Child-centered sites and sites published by children
Lifestyle & Culture	<ul style="list-style-type: none"> • Homelife and family-related topics, including weddings, births, and funerals • Parenting tips and family planning • Gay/lesbian/bisexual (non-pornographic) sites • Foreign cultures, socio-cultural information • Tattoo, piercing parlors (non-explicit)
Motor Vehicles	<ul style="list-style-type: none"> • Car reviews, vehicle purchasing or sales tips, parts catalogs • Auto trading, photos, discussion of vehicles including motorcycles, boats, cars, trucks, and RVs • Journals and magazines on vehicle modification, repair, and customization • Online automotive enthusiast clubs
News	<ul style="list-style-type: none"> • Newspapers online • Headline news sites, newswire services, and personalized news services • Weather sites

Category	Description of Content
Personals & Dating	<ul style="list-style-type: none">• Singles listings, matchmaking and dating services• Advice for dating or relationships; romance tips and suggestions
Photo Searches	<ul style="list-style-type: none">• Sites that provide resources for photo and image searches• Online photo albums/digital photo exchange• Image hosting
Real Estate	<ul style="list-style-type: none">• Home, apartment, and land listings• Rental or relocation services• Tips on buying or selling a home• Real estate agents• Home improvement
Reference	<ul style="list-style-type: none">• Personal, professional, or educational reference• Online dictionaries, maps, and language translation sites• Census, almanacs, and library catalogs• Topic-specific search engines
Religion	<ul style="list-style-type: none">• Churches, synagogues, and other houses of worship• Any faith or religious beliefs, including non-traditional religions such as Wicca and witchcraft
Remote Proxies	<ul style="list-style-type: none">• Remote proxies or anonymous surfing• Web-based translation sites that circumvent filtering• Peer-to-peer sharing
Search Engines	<ul style="list-style-type: none">• General search engines (Yahoo, AltaVista, Google)
Sex Education	<ul style="list-style-type: none">• Pictures or text advocating the proper use of contraceptives, including condom use, the correct way to wear a condom, and how to put a condom in place• Sites related to discussion about the use of birth control pills, IUDs, and other types of contraceptives• Discussion sites on how to talk to your partner about diseases, pregnancy, and respecting boundaries <p>Note: Not included in this category are commercial sites that sell sexual paraphernalia. These sites are filtered through the Adult category.</p>

Category	Description of Content
Shopping	<ul style="list-style-type: none">• Department stores, retail stores, company catalogs, and other sites that allow online consumer shopping• Online auctions• Online downloadable product warehouses; specialty items for sale• Freebies or merchandise giveaways
Sports	<ul style="list-style-type: none">• Team or conference web sites• National, international, college, or professional scores and schedules• Sports-related online magazines or newsletters• Fantasy sports and virtual sports leagues that are free or low-cost
Streaming Media	<ul style="list-style-type: none">• Streaming media files or events (any live or archived audio or video file)• Internet TV and radio• Personal (non-explicit) Webcam sites• Telephony sites that allow user to make calls via the Internet• VoIP services
Travel	<ul style="list-style-type: none">• Airlines and flight booking agencies• Accommodation information• Travel package listings• City guides and tourist information• Car rentals

Category	Description of Content
Violence	<ul style="list-style-type: none"> • Portraying, describing, or advocating physical assault against humans, animals, or institutions • Depictions of torture, mutilation, gore, or horrific death • Advocating, encouraging, or depicting self-endangerment or suicide, including the use of eating disorders or addictions • Instructions, recipes, or kits for making bombs and other harmful or destructive devices • Sites promoting terrorism • Excessively violent sports or games (including video and online games) • Offensive or violent language, including through jokes, comics, or satire • Excessive use of profanity or obscene gesticulation <p>Note: We do not block news, historical, or press incidents that may include the above criteria (except in graphic examples).</p>
Weapons	<ul style="list-style-type: none"> • Online purchasing or ordering information, including lists of prices and dealer locations • Any page or site predominantly containing, or providing links to, content related to the sale of guns, weapons, ammunition, or poisonous substances • Displaying or detailing the use of guns, weapons, ammunition or poisonous substances • Clubs which offer training on machine guns, automatic guns, other assault weapons, and/or sniper training <p>Note: Weapons are defined as something (as a club, knife, or gun) used to injure, defeat, or destroy.</p>
Web-based E-mail	<ul style="list-style-type: none"> • Web-based e-mail accounts • Messaging sites (SMS, etc)
Usenet/ Forums	<ul style="list-style-type: none"> • Opinion or discussion forums • Weblogs (blog) sites

For information on how to see if a web site is included in the Surf-Control database, read the “How can I see a list of blocked sites?” topic in this FAQ:

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

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 only applies to web sites on the Internet. You cannot use WebBlocker to block your users from web sites behind the Firebox®.

- 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 table with one entry, '64.12.10.124', which has a 'Remove' button next to it. Below the table is an 'Add' section with a 'Host IP Address' dropdown menu, a text input field containing '64.12.10.124', and an 'Add' button. At the bottom of the form are 'Submit' and 'Reset' buttons.

- 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.
Repeat step 3 for each additional host, IP address, or domain name that you wish to add to the Allowed Sites list.
The domain (or host) name is the part of a URL that ends with .com, .net, .org, .biz, .gov, or .edu. Domain names may also end in a country code, such as .de (Germany) or .jp (Japan).

To add a domain name, type the URL pattern without the leading "http://". For example, to allow access to the Google web site, select to add a domain name and enter "google.com".

If the site has a subdomain that resolves to a different IP address, you must enter that subdomain to allow it. For example, if "www.site.com" and "site.com" are on different servers, you must add both entries.

- 4 Click **Add**.

The site is added to the Allowed Sites list.

- 5 Click **Submit**.

To remove an item from the Allowed Sites list, select the address and click **Remove**, then click **Submit**.

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 cannot 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 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.

Repeat step 3 for each additional host, IP address, or domain name you wish to add to the Denied Sites list.

The domain (or host) name is the part of a URL that ends with .com, .net, .org, .biz, .gov, or .edu. Domain names may also end in a country code, such as .de (Germany) or .jp (Japan).

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 "playboy.com".

If the site has a subdomain that resolves to a different IP address, you must enter that subdomain to deny it. For example, if "www.site.com" and "site.com" are on different servers, you must add both entries.

- 4 Click **Add**.

The site is added to the Denied Sites list.

- 5 Click **Submit**.

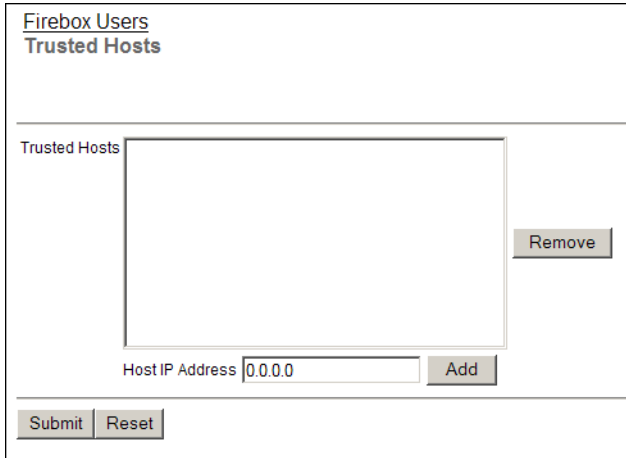
To remove an item from the Denied Sites list, select the address and click **Remove** and then click **Submit**.

Bypassing WebBlocker

You can make a list of internal hosts that bypass WebBlocker. The internal hosts that you put on this list also bypass any user authentication settings. If a user is on this list, that user does not have to authenticate to get access to the Internet. No WebBlocker rules

apply to the users on this list. For more information about user authentication, see Chapter 9, “Managing Users and Groups”.

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



The screenshot shows the 'Firebox Users' configuration page with the 'Trusted Hosts' tab selected. The page features a large empty rectangular box for listing trusted hosts. To the right of this box is a 'Remove' button. Below the box is a 'Host IP Address' text input field containing '0.0.0.0' and an 'Add' button. At the bottom of the page are 'Submit' and 'Reset' buttons.

- 2 In the **Host IP Address** text box, type the IP address of the computer on your trusted or optional network to allow to browse the Internet without authentication restrictions.
- 3 Click **Add**.
Repeat step 2 for other trusted computers.
- 4 Click **Submit**.
To remove a computer from the list, select the address and click **Remove**.

Configuring Virtual Private Networks

A VPN (Virtual Private Network) creates secure connections between computers or networks in different locations. This connection is known as a tunnel. 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 176.

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 Management Server. This procedure is different for different versions of WatchGuard System Manager appliance software installed on the Firebox X. This section also gives procedures for VPN tunnels managed by VPN Manager (available with earlier versions of Watchguard management software).

Information about how to configure a Manual VPN to connect 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, information on how to keep the VPN tunnel operating correctly, and instructions on how to see VPN tunnel statistics. These last sections can help you troubleshoot problems with VPN.

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 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 is not already active.
- 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 is a WatchGuard Firebox X and each Firebox is under WatchGuard System Manager management, 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 56.
- 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 68.

- You must know the network address of the private (trusted) networks behind your Firebox X Edge and of the network behind the other VPN device, 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

You can configure a VPN tunnel on the Firebox® X Edge with two procedures: Managed VPN and Manual VPN. For information on creating a Manual VPN, see "Manual VPN: Setting Up Manual VPN Tunnels" on page 178.

The WatchGuard Management Server (previously known as the DVCP Server) uses DVCP to keep the VPN tunnel configuration. DVCP (Dynamic VPN Configuration Protocol) is the WatchGuard® protocol that you can use to create IPSec tunnels easily. Watchguard uses the name Managed VPN because the Management Server manages the VPN tunnel and sends the VPN configuration to your Edge. An Edge administrator 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.

To configure a Firebox X Edge to allow WatchGuard System Manager access for the creation of VPN tunnels, see “Setting up WatchGuard System Manager Access” on page 46.

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 and the other device must use Dynamic DNS.
- 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 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 expires in kilobytes

Negotiation expires in hours

Diffie-Helman Group

☒ Send IKE Keep Alive Messages

- 4 Type the tunnel name and shared key.
The tunnel name is for your identification only.
The shared key is a passphrase that the devices use to encrypt and decrypt the data on the VPN tunnel. The two devices must use the same passphrase, or 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 the factory-default settings.

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 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 or remote VPN device has a static external IP address, set the local ID type to **IP Address**. Type the external IP address of the Edge or device as the local ID.
- If your Firebox X Edge or remote VPN device has a dynamic external IP address, you must select **Aggressive Mode** and the device must use Dynamic DNS. For more information, see “Registering with the Dynamic DNS Service” on page 81. Set the local ID type to **Domain Name**. Enter the DynDNS domain name of the device as the local 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 never expire, enter zero (0). For example, 24 hours and zero (0) kilobytes means that the phase 1 key is negotiated every 24 hours no matter how much data has passed.
- 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 **Send 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 186.

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 NAT (Network Address Translation) or if your Edge's external interface is connected to a device that does NAT. Watchguard recommends 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 with the NAT device's manufacturer for information on opening these ports and protocols on the NAT device.

If your Edge's external interface has a private IP address, you cannot use an 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 81. 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 and computer resources.
- 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 (0). For example, 24 hours and zero (0) 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 CIDR or Classless Inter Domain Routing 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**.
Repeat step 5 if you must add additional networks.

7 Click **Submit**.

Phase 2 Settings

Authentication Algorithm:

Encryption Algorithm:

☐ Enable Perfect Forward Security

Key expiration in kilobytes:

Key expiration in hours:

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

Local Network:

Remote Network:

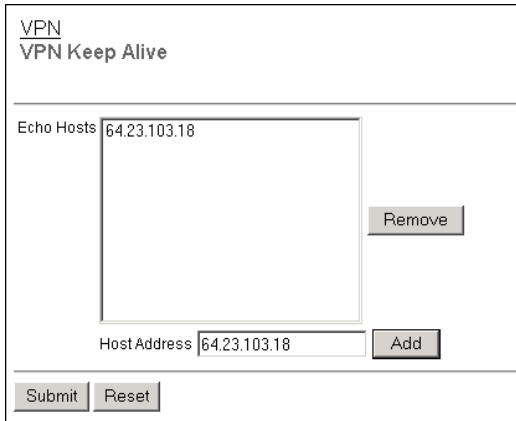
VPN Keep Alive

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 online and can respond to ping messages. You can enter the trusted interface IP address of the Firebox that is at the other end of the tunnel. You can also use more than one IP address so the Firebox X Edge can send a ping to more than one host through different tunnels.

- 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 > 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**.
Repeat step 3 to add additional echo hosts.
- 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 if you cannot get a static external IP address. For more information, see “Registering with the Dynamic DNS Service” on page 81.

How do I get a static external IP address?

You get the external IP address for your computer or network from your ISP or a network 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 the IP address of 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 your ISP or network administrator.
- 2 If you can ping the external address of each Firebox X Edge, try to ping a local address in the remote network.
From a computer at Site A, ping the internal interface IP address of the remote Firebox X Edge. If the VPN tunnel is up, the remote 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 Watch-Guard® Web site:

<http://www.watchguard.com/products/purchaseoptions.asp>

Configuring the MUVPN Client

Mobile User VPN lets remote users connect to your internal 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 through 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 a MUVPN connection. 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 MUVPN on the Firebox® X Edge user's account and set the options that apply to all MUVPN clients. Read the section "Enabling MUVPN for Edge Users" on page 193 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 196 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 MUVPN to operate correctly. Read the section "Preparing Remote Computers for MUVPN" on page 197 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. For more information, read the section "Installing and Configuring the MUVPN Client" on page 204.
- 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 213 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 device to make a VPN connection to the Edge, see “Tips for Configuring the Pocket PC” on page 214.
- 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 set these options:

- To make the .wgx file read-only so that the user cannot change the security policy file by default, 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, the computer must have correct WINS and DNS addresses configured in the primary network card settings. See the section “Preparing Remote Computers for MUVPN” on page 197 for information on entering WINS and DNS addresses in the network card advanced settings.

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 more information on these settings, see “Configuring MUVPN client settings” on page 140.

Enabling MUVPN access for a Firebox user account

- 1 Add a new Firebox user or edit a Firebox user, as described in “Using Local Firebox Authentication” on page 142.
- 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 user 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 and/or hours. The default values are 8192 KB and 24 hours. To remove a size and/or time expiration, set the value to zero (0).
- 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 78.
- 11 Click **Submit**.

[Firebox Users](#)
New User

Settings

WebBlocker

MUVPN

☒ Enable MUVPN for this account.

Shared Key

Virtual IP Address

Authentication Algorithm MD5-HMAC

Encryption Algorithm DES-CBC

Key expires in kilobytes

Key expires in hours

VPN Client Type Mobile User

☐ All traffic uses tunnel (0.0.0.0/0 IP Subnet).

Submit

Reset

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 differently. Follow the previous procedure, but select **Pocket PC** from the **VPN Client Type** drop-down list.

NOTE

WatchGuard does not distribute a MUVPN software package for Pocket PCs. 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 214.

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 the LiveSecurity® Service at <http://www.watchguard.com/support> to download the software. 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 ZoneAlarm® personal firewall 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**.
- 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 193. 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

You can 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 IP addresses of the WINS and DNS servers 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

You must install Remote Access Services (RAS) before you install the Mobile User VPN Adapter. To install RAS, use this procedure:

- 1 From 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 the **Add** button.
- 4 Select **Remote Access Services** and click **OK**.
The Windows NT Setup dialog appears.

- 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, 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**.
You can also add a secondary or backup WINS server IP address.
- 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 and your settings are applied.

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 Right-click the connection you use to get Internet access and select **Properties**.
The connection properties window appears.
- 3 Click the **Networking** tab.
- 4 Make sure these components are installed and enabled:
To enable a component, click the adjacent check box. If a component is not installed, follow the instructions to install it.
 - 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 Below the **Microsoft** manufacturer, select the **Internet Protocol (TCP/IP)** network protocol and 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 Below the **Microsoft** manufacturer, 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)** radio button and click **Add**.
The TCP/IP Domain Suffix window appears.
- 6 Type the domain suffix in the applicable field and click **Add**.
To add more DNS suffixes, repeat steps 5 and 6.
- 7 Click the **WINS** tab. 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** to close the connection properties 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 Right-click the connection you use to get Internet access and select **Properties**.
The connection properties window appears.
- 4 Make sure these components are installed and enabled:
To enable a component, click the adjacent check box. If a component is not installed, follow the instructions to install it.
 - 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 Below the **Microsoft** manufacturer, select the **Internet Protocol (TCP/IP)** network protocol and 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 Below the **Microsoft** manufacturer, 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)** network component.
- 2 Click the **Properties** button.
The Internet Protocol (TCP/IP) Properties window appears.
- 3 Click the **Advanced** button.
The Advanced TCP/IP Settings window appears.
- 4 Click the **DNS** tab.
- 5 From the section labeled **DNS server addresses, in order of use**, click **Add**.
The TCP/IP DNS Server window appears.
- 6 Type the IP address of the DNS server in the related field and 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.

- 7 Select the **Append these DNS suffixes (in order)** radio button.
- 8 Below the radio button, click **Add**.
The TCP/IP Domain Suffix window appears.
- 9 Enter the domain suffix for your network's private domain in the related field and click **Add**.
To add more DNS suffixes, repeat steps 8 and 9.
- 10 Click the **WINS** tab.
- 11 From the section **WINS addresses, in order of use**, click **Add**.
The TCP/IP WINS Server window appears.
- 12 Type the IP address of the WINS server in the related field and click **Add**.
To add more WINS servers, repeat steps 11 and 12.
- 13 Click **OK** to close the Advanced TCP/IP Settings window. Click **OK** to close the Internet Protocol (TCP/IP) Properties window.
- 14 Click **OK** 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 active on the remote computer. Remove any other IPsec VPN software from the user's computer before installing the WatchGuard® MUVPN software.
- 2 Copy the MUVPN installation program 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 shows 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. WatchGuard recommends that you use the **Typical** installation. Click **Next**.
- 8 On a Windows 2000 computer, the InstallShield looks for the Windows 2000 L2TP (Later 2 Tunneling Protocol) 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.
A command prompt window appears during the installation. The command prompt can stay for more than one minute. This is usual. After the file is installed, the command window closes automatically 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 type 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 211.

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 209).
- 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.
A command prompt window appears during the procedure. This is usual. After the file is removed, the command prompt window closes automatically 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** button.
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 207.
- 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 is not connected to 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

- IrrelKE.exe

The ZoneAlarm 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 makes 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 IrrelKE.exe program.
- 2 Set the **Remember this answer the next time I use this program** check box, then click **Yes**.
This option makes 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 shown.
- 2 If the ZoneAlarm personal firewall is active, deactivate it now by following the subsequent instructions.

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**.

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.

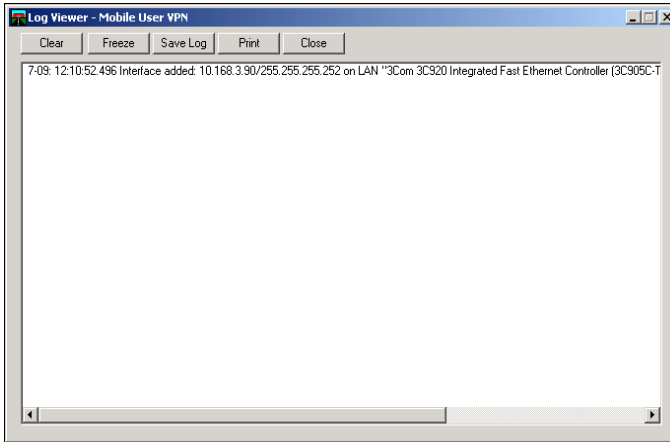
Using Log Viewer

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) information. 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 tells you 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, clear or 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 platform. 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 can 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

You can get more information about the MUVPN client from the WatchGuard® Web site:

<http://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 can not 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. 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**. Type `cmd` and click **OK**. At the command prompt, 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, then restart the MUVPN client.

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.

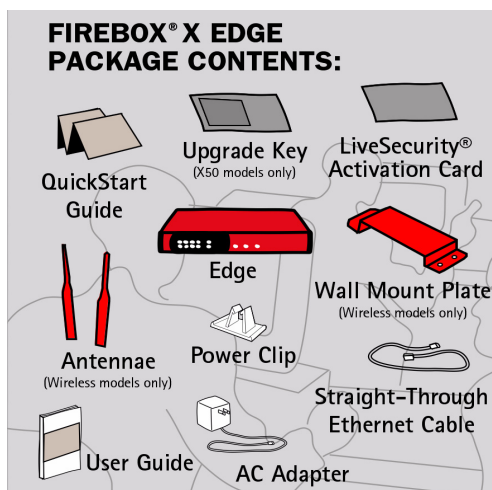


Package Contents and Specifications

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 that the Firebox X Edge is activated as a wireless access point. 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.

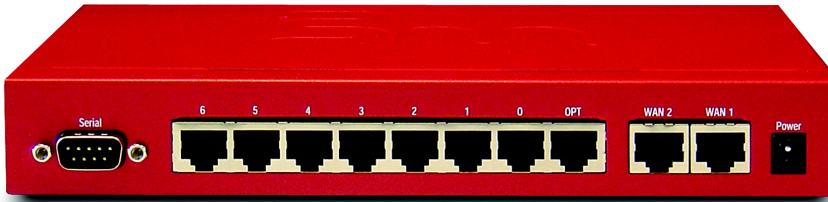
Power

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 41.

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 external networks.

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 (wireless model only)

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: 11 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 that 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 that 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.

Copyright 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved.

The OpenLDAP Public License

Version 2.7, 7 September 2001

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time.

Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS "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 OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE 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 names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

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

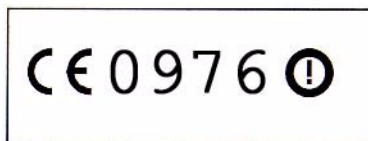
The term “IC:” before the radio certification number only signifies that Industry of Canada technical specifications were met.

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 192
 - distributing 196
 - viewing available 34

A

- Add Gateway page 181
- Add Route page 79
- Administration page
 - described 34
 - subpages of 35
- Administrative Access levels 138
- administrator account 145
- Aggressive Mode 182
- Allow access to the External Network check box 144
- Allow access to VPN check box 144
- Allowed Sites pages 171
- antenna directional gain 225
- authentication. See user authentication

B

- bandwidth, described 2
- Blocked Sites page 119
- broadband connections 2

C

- cables
 - included in package 11, 220
- cabling
 - for 0-6 devices 19
 - for 7+ devices 20
- channel bandwidth 226
- CIDR notation 79, 110, 111, 185
- Classless Inter Domain Routing 79, 110, 111, 185
- Client for Microsoft Networks, installing 201
- configuration file, viewing 57

- configuration pages
 - description 30–40
 - navigating 30
 - opening 30
 - viewing 29
- configuration pages. See also pages
- Connection Monitor, using to monitor MUVPNs 210
- custom incoming services, creating 107, 108, 113
- Custom Service page 108, 114

D

- daylight savings time 130
- default factory settings 41–42
- Denied Sites page 172
- DHCP
 - described 5, 60
 - setting your computer to use 22
 - using on the optional network 74
- DHCP address reservations
 - setting on the optional network 75
 - setting on the trusted network 69
- DHCP Address Reservations page 70, 76
- DHCP relay
 - configuring the optional network 76
 - configuring the trusted network 70
- DHCP server
 - configuring Firebox as 68, 74
- dialog boxes
 - Internet Protocol (TCP/IP) Properties 22, 23
 - Wireless Network Connection 102
- dialup settings, configuring 88
- Diffie-Hellman groups 183
- Digital Subscriber Line (DSL) 2
- DNS service, dynamic 81
- DNS settings, and WAN failover 88
- DNS, described 6
- DVCP, described 178
- Dynamic DNS client page 82
- dynamic DNS service, registering with 81–82
- Dynamic Host Configuration Protocol. See DHCP
- dynamic IP addresses
 - described 14

Dynamic VPN Configuration Protocol, described 178

E

- echo host 187
- Enable DHCP Relay check box 71
- Enable DHCP Server on the Trusted Network check box 69
- Enable Optional Network check box 73
- event, described 125
- external network
 - described 9
 - if ISP uses DHCP 61
 - if ISP uses PPPoE 63
 - if ISP uses static addressing 62
- External Network Configuration page 61, 62, 63

F

- factory default settings
 - described 41
 - resetting to 42
- failover network. See WAN failover
- feature key, described 26
- File and Printer Sharing for Microsoft Networks
 - and Windows XP 203
- File and Printer Sharing for Microsoft Networks, installing 200
- Filter Traffic page 106, 112, 117
- Firebox users
 - creating 142
 - viewing settings for 134
- Firebox Users page 135, 142, 146, 148, 151
 - described 34
 - subpages of 34
- Firebox X Edge
 - administrator account 145
 - and SOCKS 121
 - authenticating to 141
 - back panel 223
 - cabling 19
 - configuring as DHCP server 68
 - described 219
 - front panel 221
 - hardware description 221–223

- hardware specifications 220
- indicator lights 221
- installing 11–27
- package contents 11, 219
- rear panel 223
- rebooting 43–44
- registering 26
- resetting to factory default 42
- serial number 12
- side panel 223
- upgrade options 54
- viewing log messages for 125
- Web pages. See configuration pages
- Firebox X Edge Wireless
 - physically connecting 90
 - setting up 89–??
- Firewall Options page 120
- Firewall page
 - described 35
 - subpages of 36
- firewalls, described 8

H

- hardware description 221–223
- hardware operating specifications 223
- hardware specifications 220
- HTTP proxy settings, disabling 17
- HTTP server port, changing 45
- HTTP/HTTPS, using for Firebox management 44

I

- incoming service, creating custom 107, 108, 113
- indicator lights 221
- 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 11–27
- Internet

- how information travels on 4
- Internet connection, required for Firebox X Edge 13
- Internet Protocol (TCP/IP) Network Component
 - and Windows XP 202
- Internet Protocol (TCP/IP) network component, installing 200
- Internet Protocol (TCP/IP) Properties dialog box 22, 23
- IP addresses
 - described 5
 - giving your computer static 22
 - static 61

L

- lights on front panel 221
- LiveSecurity Service
 - and software updates 52
 - registering with 26
- Local Area Network (LAN)
 - described 2
- Log Authentication Events check box 93
- log messages
 - contents of 125
 - viewing 125
- Log Viewer, using to monitor MUVPNs 210
- logging
 - configuring 125–131
 - described 125
 - to Syslog host 128
 - to WSEP lot host 126
 - viewing status of 37
- Logging page 126
 - described 37
 - subpages of 37

M

- Manual VPN page 181
- Manual VPNs
 - creating 181
 - described 178
- Manually configure DNS server IP addresses check box 88
- model upgrades 56
- modems

- and DNS settings 88
- dialup settings 88
- types supported 87
- using the failover 87
- multipath, described 225
- MUVPN client
 - allowing through firewall 208
 - configuring user settings for 140
 - connecting 207
 - described 191
 - disconnecting 209
 - icon for 207–208
 - installing 204
 - monitoring 209–211
 - preparing remote computers for 197–204
 - troubleshooting 216–218
 - uninstalling 206
- MUVPN Clients upgrade 56
- MUVPNs
 - and .wgx files 196
 - enabling access for users 194
 - monitoring with Connection Monitor 210
 - monitoring with Log Viewer 210
 - system requirements for 197
 - using on wireless networks 213
 - WINS and DNS servers 198

N

- navigation bar 31
- netmask 14
- Network Address Translation (NAT), and the Edge 14, 183
- network addressing, described 13
- network interfaces, configuring 59–85
- Network page
 - described 33
 - subpages of 33–34
- network security, described 1
- Network Setup Wizard 59
- Network Statistics page 80
- network statistics, viewing 80
- networks, types of 2
- New User page 143

noise level 224
numbered ports 223

O

optional network
 assigning static IP addresses on 77
 changing IP address of 73
 configuring 72–78
 configuring additional computers on 77
 described 9, 72
 enabling 73
 setting DHCP address reservations on 75
 using DHCP on 74
 using DHCP relay on 76
Optional Network Configuration page 73, 74, 75, 77
options
 model upgrade 56
 MUVPN Clients 56
 seat license upgrade 56
 WAN failover 56
 WebBlocker 56

P

package contents 11
packets, described 4
pages
 Add Gateway 181
 Add Route 79
 Administration 34
 Allowed Sites 171
 Blocked Sites 119
 Custom Service 108, 114
 Denied Sites 172
 DHCP Address Reservations 70, 76
 Dynamic DNS client 82
 External Network Configuration 61, 62, 63
 Filter Traffic 106, 112, 117
 Firebox Users 34, 135, 142, 146, 148, 151
 Firewall 35
 Firewall Options 120
 Logging 37, 126

- Manual VPN 181
- Network 33
- Network Statistics 80
- New User 143
- Optional Network Configuration 73, 74, 75, 77
- Routes 78
- Settings 138
- Syslog Logging 128
- System Security 45
- System Status 32
- System Time 130
- Trusted Hosts 153, 174
- Trusted Network Configuration 68, 69, 71, 134
- Upgrade 55
- VPN 38
- VPN Keep Alive 187
- VPN Manager Access 46
- VPN Statistics 187
- WAN Failover 85
- WatchGuard Security Event Processor Logging 127
- WebBlocker 38
- WebBlocker Settings 157, 159
- Wireless Network Configuration 91
- passphrases, described 143, 146
- path-loss 225
- Perfect Forward Secrecy 185
- Phase 1 settings 181, 182
- Phase 2 settings 184
- Pocket PCs
 - creating MUVPN tunnels to 196
 - creating tunnels to 196
 - tips for configuring 214
- Point-to-Point Protocol over Ethernet. See PPPoE
- port, changing HTTP server port 45
- ports
 - numbered 223
 - trusted network 223
 - WAN 223
 - WAN1 83
 - WAN2 83
- power cable clip 12, 220
- power input 223
- PPPoE
 - described 5, 14, 61

- entering settings 17
- profiles
 - creating WebBlocker 159–160
- protocols
 - described 3
 - TCP, UDP 3
 - TCP/IP 3

Q

- Quick Setup Wizard
 - and viewing configuration pages 29
 - described 24
 - running 24

R

- read-only administrative account 144
- rebooting 43–44
- Remote Access Services, installing 198
- RESET button 222
- resetting to factory default 42
- Restrict Access by Hardware Address check box 98
- routes
 - configuring static 78
 - viewing 33
- Routes page 78

S

- seat licenses
 - described 133, 137
 - upgrade 56
- seat limitation 20
- serial number, viewing 32
- services
 - creating custom 107–109, ??–111, 113–115
 - creating custom incoming 107, 108, 113
 - described 6, 103
 - viewing current 35
- Session idle time-out field 144
- Session maximum time-out field 144

- sessions
 - closing 135
 - described 133
 - idle timeout 144
 - maximum timeout 144
 - releasing 20
 - viewing current active 134
 - viewing currently active 134
- Settings page 138
- shared secret 180
- signal attenuation 225
- signal strength 225
- SOCKS
 - configuring 122
 - configuring for Edge 121
 - described 121
 - disabling 122
- software updates 52
- SSID (Service Set Identifier) 92
- static IP addresses
 - and VPNs 187
 - described 14
 - obtaining 188
- static routes
 - making 78
 - removing 79
- subnet mask 14
- SurfControl 155
- Syslog host, logging to 128
- Syslog Logging page 128
- Syslog, described 128
- system configuration pages. See configuration pages
- System Security page 45
- System Status page
 - described 32
 - green triangle on 32
 - information show on 32
 - navigation bar 31
- system time
 - setting 129
- System Time page 130

T

- TCP (Transmission Control Protocol) 3
- TCP/IP properties 14
- TCP/IP settings, determining 14–17
- TCP/IP, described 3
- time zone, setting 129
- traffic, logging all outbound 123
- Trusted Hosts page 153, 174
- trusted network
 - assigning static IP addresses on 71
 - changing IP address of 67
 - configuring 66–??
 - configuring additional computers on 71
 - described 8
- Trusted Network Configuration page 68, 69, 71, 134

U

- UDP (User Datagram Protocol) 3
- Uniform Resource Locator (URL) 6
- updating software 40
- upgrade options, activating 54
- upgrade options, viewing status of 32
- Upgrade page 55
- user accounts
 - changing name, password 146
 - configuring MUVPN settings 140
 - configuring MUVPN settings for all 193
 - creating new 142
 - deleting 137
 - editing 136
 - enabling MUVPN access for 194
 - read-only administrative 144
 - setting WebBlocker profile for 145, 152
 - viewing 136
 - viewing current 34
- user authentication
 - changing options for 138
 - described 137
 - process 141
- users. See Firebox users

V

virtual adapter, settings for 140, 193

VPN Keep Alive page 187

VPN Manager

described 46

setting up access to 46–??

VPN Manager Access page 46

VPN page

described 38

subpages of 39

VPN Statistics page 187

VPNs

and static IP addresses 187

described 175

Keep Alive feature 186

special considerations for 176

troubleshooting connections 188

viewing statistics 187

what you need to create 176

W

wall mounting plate 223

WAN Failover

and DNS settings 88

configuring 83

described 56, 83

using broadband connection for 85

using external modem for 87

WAN Failover page 85

WAN Failover Setup Wizard 84

WAN ports 223

WAN1 port 83

WAN2 port 83

WatchGuard Security Event Processor 126

WatchGuard Security Event Processor Logging page 127

Web sites

blocking specific 172

blocking using WebBlocker ??–153, ??–174

bypassing WebBlocker 171

WebBlocker

allowing sites to bypass 171

- categories 161—??
- creating profiles 159—160
- database 155
- defining profile 145, 152
- WebBlocker page
 - described 38
 - subpages of 38—??
- WebBlocker Settings page 157, 159
- Wide Area Network (WAN), described 2
- Windows 2000
 - preparing for MUVPN clients 200
- Windows 98/ME
 - preparing for MUVPN clients 198
- Windows NT
 - preparing for MUVPN clients 198
- Windows XP
 - installing File and Printer Sharing for Microsoft Networks on 203
 - installing Internet Protocol (TCP/IP) Network Component on 202
 - preparing for MUVPN clients 202
- WINS and DNS settings, configuring 199, 201
- wireless card, configuring 101
- wireless communication
 - antenna directional gain 225
 - channel bandwidth 226
 - described 224
 - noise level 224
 - path-loss 225
 - signal attenuation 225
 - signal strength 225
- Wireless Encryption Privacy (WEP) 94
- Wireless Network Configuration page 91
- Wireless Network Connection dialog box 102
- Wireless Network Wizard 90
- wireless networks
 - using MUVPN on 213
- wireless setup 89—??
- wizards
 - NetworkSetup 59
 - Quick Setup 24
 - WAN Failover Setup 84
 - Wireless Network 90
- Wizards page 39
- WSEP 126

Z

ZoneAlarm

- allowing traffic through 211
- described 191, 211
- icon for 209
- shutting down 212
- uninstalling 212