

WatchGuard

Firebox X Edge e-Series

User Guide

Firebox X Edge e-Series version 10
All Firebox X Edge e-Series 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.

Guide revision: 04/7/2008

Copyright, Trademark, and Patent Information

Copyright © 1998 - 2008 WatchGuard Technologies, Inc. All rights reserved. All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Complete copyright, trademark, patent, and licensing information can be found in the Reference Guide, available online: <http://www.watchguard.com/help/documentation/>



This product is for indoor use only.

Abbreviations Used in this Guide

3DES	Triple Data Encryption Standard	IPSec	Internet Protocol Security	SSL	Secure Sockets Layer
BOVPN	Branch Office Virtual Private Network	ISP	Internet Service Provider	TCP	Transfer Control Protocol
DES	Data Encryption Standard	MAC	Media Access Control	UDP	User Datagram Protocol
DNS	Domain Name Service	NAT	Network Address Translation	URL	Uniform Resource Locator
DHCP	Dynamic Host Configuration Protocol	PPP	Point-to-Point Protocol	VPN	Virtual Private Network
DSL	Digital Subscriber Line	PPTP	Point-to-Point Tunneling Protocol	WAN	Wide Area Network
IP	Internet Protocol	PPPoE	Point-to-Point Protocol over Ethernet	WSM	WatchGuard System Manager

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. Our Firebox X family of unified threat management (UTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. All products are backed by LiveSecurity® Service, a ground-breaking support and maintenance program. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. For more information, please call 206.613.6600 or visit www.watchguard.com.

ADDRESS

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

SUPPORT

www.watchguard.com/support
U.S. and Canada +877.232.3531
All Other Countries +1.206.521.3575

SALES

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.613.0895

Table of Contents

Chapter 1	Introduction to Network Security	1
	About networks and network security	1
	About Internet Connections	1
	About protocols.....	2
	How Information Travels on the Internet.....	2
	About IP addresses.....	3
	Private addresses and gateways.....	3
	About subnet masks	3
	About slash notation	3
	About entering IP addresses.....	4
	Static and dynamic IP addresses	4
	About DHCP	4
	About PPPoE.....	4
	About Domain Name Service (DNS)	5
	About services and policies	5
	About ports.....	6
	About Firewalls.....	7
	The Firebox X Edge and your Network	8
Chapter 2	Installation	9
	Before you begin.....	9
	Verify basic requirements	9
	Identify your network settings	10
	Find your TCP/IP Properties	11
	Find PPPoE settings.....	12
	Disable the HTTP proxy	13
	Disable the HTTP proxy in Internet Explorer 6.x or 7.x	13
	Disable the HTTP proxy in Firefox 2.x	14
	Disable the HTTP proxy in Safari 2.0.....	14
	Disable pop-up blocking.....	14
	Disable the pop-up blocker in Internet Explorer 6.x or 7.x	14
	Disable the pop-up blocker in Firefox 2.x	14
	Disable the pop-up blocker in Safari 2.0.....	14
	Add computers to the trusted network.....	16
	Connect the Edge to more than four devices.....	16

Set your computer to connect to the Edge.....	17
Use DHCP	17
Use a static IP address	18
Chapter 3 Configuration Pages Overview	21
About Edge Configuration Pages	21
Connect to the Firebox X Edge.....	21
Navigating the Firebox X Edge User Interface	23
System Status page.....	23
Network page.....	24
Firebox Users page	25
Administration page.....	26
Firewall page	27
Logging page	28
WebBlocker page	29
spamBlocker page	30
Gateway AV/IPS page.....	31
VPN page.....	32
Wizards page	32
ARP table.....	33
Authentications	34
Connections.....	34
Proxy filter connections	34
Packet filter connections.....	34
Components list	35
DHCP leases	35
Dynamic DNS.....	36
Hostile sites	36
Interfaces.....	36
License	37
LiveSecurity.....	37
Memory	37
Processes.....	37
Protocols	38
Routes	38
Security Services.....	39
Syslog	39
Traffic Control.....	39
Wireless statistics	40
Chapter 4 Configuration and Management Basics	41
About basic configuration and management tasks.....	41
About the Edge backup configuration file	41
Before You Begin.....	42
See the Configuration File	42
Create a backup configuration file	43
Restore your Edge configuration	43
Before You Begin.....	43
Restore your configuration from a backup file	43
Reconnect the Firebox X Edge to a management server.....	44
Related questions	45
About feature keys	47
When you purchase a new feature	47
Get a current feature key.....	47

Get a feature key	48
Restart the Firebox locally.....	49
Using the web browser.....	49
Disconnecting the power supply.....	49
To set the system time	51
SNMP polls.....	53
Enable SNMP Polling.....	53
About MIBs.....	53
About selecting HTTP or HTTPS for management.....	54
Use HTTP instead of HTTPS	54
Change the HTTP server port.....	55
About WatchGuard System Manager access.....	55
Rename the Firebox X Edge e-series in WSM	55
Enable centralized management with WSM	56
Enable remote management with WFS v7.3 or earlier.....	57
Allow traffic from a management server.....	58
About managing the Edge from a remote location.....	58
About updating the Firebox X Edge software	60
Method 1: Install software automatically.....	60
Method 2: Install software manually.....	60
About upgrade options.....	61
Available upgrade options	61
Add a feature to your Firebox X Edge	61
Upgrade your Firebox X Edge model	62
Chapter 5 Network Settings	63
About network interface setup.....	63
If your ISP uses DHCP.....	65
Advanced PPPoE settings	68
Configure your external interface as a wireless interface	69
About advanced external network settings.....	70
Change the MAC address of the external interface.....	70
About configuring the trusted network.....	71
About changing the IP address of the trusted network	72
Change the IP address of the trusted network.....	72
Set trusted network DHCP address reservations.....	74
Make the Firebox a DHCP relay agent for the trusted interface	75
Use static IP addresses for trusted computers	76
Allow wireless connections to the trusted interface.....	76
About restricting access to an interface by MAC address.....	76
Restrict access to the trusted interface by MAC address.....	77
Find the MAC address of a computer	78
Enable the optional network	80
Set optional network DHCP address reservations	82
About DHCP relay agents	82
Make the Firebox a DHCP relay agent for the optional interface	83
Use static IP addresses for optional computers	83
Add computers to the optional network	83
Allow wireless connections to the optional interface	83
About restricting access to an interface by MAC address.....	84
Restrict access to the optional interface by MAC address	84
About static routes.....	84
Add a static route.....	85

About the Dynamic DNS service	86
Create a DynDNS account.....	86
Set up the Firebox X Edge for Dynamic DNS	86
Configure the Firebox to use BIDS	87
About using multiple external interfaces	88
Multiple WAN configuration options.....	88
WAN Failover	88
Multi-WAN load balancing	88
About multiple external interfaces and DNS	89
Configure a second external interface for a broadband connection.....	89
Configure the Edge to use round-robin load balancing.....	91
Configure WAN failover	92
Enable WAN failover with the Setup Wizard	92
Configure the Edge for serial modem failover	93
About virtual local area networks (VLANs)	96
Add a VLAN tag to the External Interface.....	96
Add a VLAN tag to the Trusted or Optional Interface.....	97
Chapter 6 Wireless Setup	99
About wireless setup.....	99
Before you begin.....	99
About wireless configuration settings.....	100
Change the SSID	100
Enable/disable SSID broadcasts	100
Log authentication events.....	101
Change the fragmentation threshold	101
About the frame size.....	101
Change the RTS threshold	101
About wireless security settings.....	102
Set the wireless authentication method	102
Set the encryption level.....	102
WPA and WPA2 PSK authentication.....	103
About wireless connections to the trusted interface	103
Allow wireless connections to the trusted interface.....	104
Allow wireless connections to the optional interface	105
Enable a wireless guest network manually	106
About wireless radio settings	108
Set the operating region and channel	108
Set the wireless mode of operation	108
Configure the wireless card on your computer	109
Chapter 7 Firewall Policies	111
About policies	111
Packet filter and proxy policies	111
Common Proxy Policies	113
Common Packet Filter Policies.....	113
Policy rules.....	114
Incoming and outgoing traffic.....	114
Editing common packet filter policies	117
Set access control options (incoming)	117
Set access control options (outgoing).....	118
Add a custom policy using a wizard	119
Add a custom packet filter policy manually	120
Filter incoming traffic for a custom policy	120

Filter outgoing traffic for a custom policy	121
Control traffic from the trusted to optional network.....	122
Disable traffic filters between trusted and optional networks.....	123
About policy precedence.....	123
Chapter 8 Proxy Settings	125
About proxy policies.....	125
Enable a common proxy policy	126
Add or Edit a Proxy Policy	126
Set access control options	127
Use a policy to manage manual VPN network traffic	127
About the HTTP proxy.....	128
HTTP proxy: Proxy Limits.....	128
HTTP requests: General settings.....	129
HTTP responses: General settings.....	129
Configure the HTTP proxy policy deny message.....	130
Define exceptions	131
To add an HTTP proxy exception:	131
HTTP responses: Content types	131
HTTP requests: URL paths	132
Block unsafe URL path patterns.....	132
HTTP responses: Cookies.....	132
Block cookies from a site	132
About the FTP proxy.....	133
Edit the FTP proxy	133
Set access control options	133
FTP proxy: Proxy limits	134
About the POP3 proxy	135
Edit the POP3 proxy	135
Set access control options	136
POP3 proxy: Proxy limits.....	136
POP3 proxy: Content types	138
POP3 proxy: Allow only safe content types.....	138
About the SMTP proxy	139
Set access control options	140
SMTP Proxy: Filter email by address pattern.....	142
SMTP proxy: Email content.....	143
Allow only safe content types	143
Add or remove a content type.....	143
Add or remove file name patterns.....	143
Deny unsafe file name patterns.....	144
About the HTTPS proxy	144
About the Outgoing Proxy	147
Settings tab	147
Content tab	147
About additional security subscriptions for proxies	147
Chapter 9 Default Threat Protection	149
About intrusion prevention	149
About blocked sites	150
Permanently blocked sites.....	150
Auto-blocked sites/Temporary Blocked Sites list.....	150
Block a site permanently	151
Block sites temporarily	152

About blocked ports.....	153
Default blocked ports.....	153
Block a port	154
Drop DoS flood attacks	155
Distributed denial-of-service prevention.....	156
Configure firewall options.....	157
Chapter 10 Traffic Management	159
About Traffic Management.....	159
About network traffic	159
Causes for slow network traffic.....	159
Traffic Categories	160
Interactive traffic	160
High priority	160
Medium priority.....	160
Low priority	160
Traffic Marking	161
About Traffic Control Options.....	162
Enable Traffic Control.....	163
Related Questions.....	164
Types of NAT	165
NAT behavior	165
Secondary IP addresses	165
About dynamic NAT.....	166
About static NAT	166
About 1-to-1 NAT.....	166
About 1-to-1 NAT and VPNs.....	167
Enable 1-to-1-NAT	167
Three steps are necessary to enable 1-to-1 NAT:	167
Add a secondary external IP address for 1-to1 NAT mapping.....	168
Add or edit a policy for 1-to-1 NAT	168
Enable secondary addresses	168
Add or edit a policy for 1-to-1 NAT	168
Chapter 11 Logging	169
About logging and log files	169
Log Servers	169
Event Log and System Status Syslog	170
Logging and notification in applications and servers	170
About log messages.....	170
See the event log file	170
To see the event log file.....	170
Send your event logs to the Log Server.....	171
Send logs to a Syslog host	173
Chapter 12 Certificates	175
About certificates.....	175
Certificate authorities and signing requests	175
About certificates and the Firebox X Edge	175
Create a certificate.....	176
Use OpenSSL to generate a CSR	176

Use Microsoft CA to create a certificate	176
Send the certificate request	176
Issue the certificate.....	177
Download the certificate.....	177
About using certificates on the Firebox X Edge	177
Import a certificate	177
Use a local certificate	177
Remove a certificate.....	178
Examine the properties of a certificate	178
Related questions	178
Can I sign my own certificates?.....	178
I have a certificate or CSR that is not in the format I need. What do I do?.....	178
What is the maximum number of certificates I can import on the Firebox X Edge?	178
If I make a backup of my Firebox X Edge configuration, are my certificates saved?	178
Chapter 13 User and Group Management	179
About user licenses	179
When a user license is used.....	179
Managing user sessions.....	180
How users authenticate.....	181
Set authentication options for all users	182
Configure an individual user account	183
Require users to authenticate to the Edge	184
Authenticate a session without administrative access	185
Create a read-only administrative account	185
Use the built-in administrator account	186
Set a WebBlocker profile for a user.....	186
Change a user account name or password	187
About using third-party authentication servers	188
Configure the LDAP/Active Directory authentication service	189
Use the LDAP authentication test feature	190
Configure groups for LDAP authentication.....	190
Add a group for LDAP authentication.....	191
Set a WebBlocker profile for an LDAP group	192
LDAP authentication and Mobile VPN with IPSec.....	192
About Single Sign-On (SSO)	192
Before You Begin.....	193
Install the WatchGuard Single Sign-On (SSO) agent.....	194
Download the SSO agent software	194
Install the SSO agent service	195
See active sessions and users	197
Firebox user settings.....	197
Active sessions	197
Local User account	198
Editing a user account.....	199
Deleting a user account	199
Allow internal devices to bypass user authentication	199
Chapter 14 WebBlocker	201
About WebBlocker	201
Download the server software	204
Install Quarantine Server and WebBlocker Server	204
About WebBlocker profiles	204
See whether a site is categorized.....	207

Add, remove, or change a category	208
Add an allowed site	209
Add a denied site	210
Allow internal hosts to bypass WebBlocker	211
Chapter 15 spamBlocker	213
About spamBlocker	213
spamBlocker requirements	213
About Virus Outbreak Detection (VOD)	214
spamBlocker actions, tags, and categories	214
spamBlocker tags	214
Enable spamBlocker	215
Configure spamBlocker	215
Set POP3 email actions	217
Set SMTP email actions	217
About spamBlocker exceptions	218
Create exceptions	218
Change the order of exceptions	218
About using spamBlocker with multiple proxies	219
Create rules for your email reader	219
Send spam or bulk email to special folders in Outlook	219
Send a report about false positives or false negatives	220
Use RefID record instead of message text	221
Find the category a message is assigned to	221
Add Trusted Email Forwarders	222
Chapter 16 Quarantine Server	223
About the Quarantine Server	223
Install the Quarantine Server and WebBlocker Server	224
Download the server software	224
Install Quarantine Server and WebBlocker Server	224
Install server components	225
Run the Setup Wizard	225
Define the server location	225
Set general server parameters	226
Change expiration settings and user domains	227
Change notification settings	228
Enable or disable logging	230
Add or prioritize Log Servers	230
Send messages to the Windows Event Viewer	230
Send messages to a file	230
Open the messages dialog box	233
Save messages or send to a user's inbox	234
Delete messages manually	234
Delete messages automatically	234
Open the messages dialog box	235
Add users	237
Remove users	237
Change the notification option for a user	237
Get statistics on Quarantine Server activity	238
See statistics from specific dates	238
See specific types of messages	238
Group statistics by month, week, or day	238
Export and print statistics	238

Chapter 17 Gateway AntiVirus and Intrusion Prevention Service	239
About Gateway AntiVirus and Intrusion Prevention	239
About Gateway AntiVirus settings.....	240
POP3 proxy deny messages and Gateway AV/IPS	240
About Intrusion Prevention Service settings	242
Chapter 18 Branch Office Virtual Private Networks	245
Process required to create a tunnel.....	245
About VPN Failover	246
About managed VPNs.....	247
Set up manual VPN tunnels	247
What you need for Manual VPN.....	247
Sample VPN address information table	248
Create Manual VPN tunnels on your Edge.....	249
Phase 1 settings.....	250
See VPN statistics	255
Why do I need a static external address?	256
How do I get a static external IP address?.....	256
How do I troubleshoot the connection?.....	256
Why is ping not working?	256
How do I set up more than the number of allowed VPN tunnels on my Edge?.....	256
Chapter 19 About Mobile VPN with PPTP	257
Enable PPTP on the Edge	258
Configure DNS and WINS settings	259
Prepare the client computers.....	261
Create and connect a PPTP Mobile VPN for Windows Vista.....	261
Create a PPTP connection	261
Establish the PPTP connection.....	261
Create and connect a PPTP Mobile VPN for Windows XP	262
Create the PPTP Mobile VPN	262
Connect with the PPTP Mobile VPN	262
Create the PPTP Mobile VPN	263
Connect with the PPTP Mobile VPN	263
Default-route VPN.....	264
Split tunnel VPN.....	264
Default-route VPN setup for Mobile VPN with PPTP	264
Split tunnel VPN setup for Mobile VPN with PPTP	264
Chapter 20 About Mobile VPN with IPSec	265
Client requirements	265
Enable Mobile VPN for a Firebox user account.....	266
Enable Mobile VPN for a group.....	267
About Mobile VPN Client configuration files.....	268
Configure global Mobile VPN with IPSec client settings	268
WINS/DNS Settings for Mobile VPN with IPSec.....	269
Get the user's .wgx file	269
Client Requirements	271
Import the end-user profile.....	271
Select a certificate and enter the PIN.....	272
Uninstall the Mobile VPN client.....	272
Connect and disconnect the Mobile VPN client	273
Disconnect the Mobile VPN client	273
Control connection behavior.....	274

Mobile User VPN client icon	275
See Mobile VPN log messages	275
Secure your computer with the Mobile VPN firewall.....	275
Enable the link firewall	275
About the desktop firewall.....	276
Create firewall rules.....	278
General tab	279
Applications tab	282
Chapter 21 About Mobile VPN with SSL	283
Before You Begin.....	283
Steps required to set up your tunnels	283
Options for Mobile VPN with SSL tunnels.....	283
Client requirements	284
Enable Mobile VPN with SSL for a Firebox user	284
Enable Mobile VPN with SSL for a group	285
SSL VPN General Tab.....	287
SSL VPN Advanced tab	288
Download the client software.....	289
Install the Mobile VPN with SSL client software (Windows Vista and Windows XP)	290
Connect to the Firebox with the Mobile VPN with SSL client (Windows Vista and Windows XP).....	291
Connect to the Firebox with the Mobile VPN with SSL client (Mac OS X)	291
Mobile VPN with SSL client controls	292
Uninstall the Mobile VPN with SSL client	292
Mobile VPN with SSL client for Windows Vista and Windows XP	292
Mobile VPN with SSL client for Mac OS X	292

1

Introduction to Network Security

About networks and network security

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 work together and share data.

Although 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.

Attacks are costly. Computers may need to be repaired or replaced. Employee time and resources are used to fix problems created by attacks. Valuable information can be taken from the 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 email spam or attacks. Your personal information and account information is also vulnerable and valuable to hackers.

About Internet Connections

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 computer 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 guarantee a constant connection bandwidth to a web site or network.

About protocols

A *protocol* is a group of rules that allow computers to connect across a network. Protocols are the grammar of the language that computers use when they speak to each other across a network.

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.

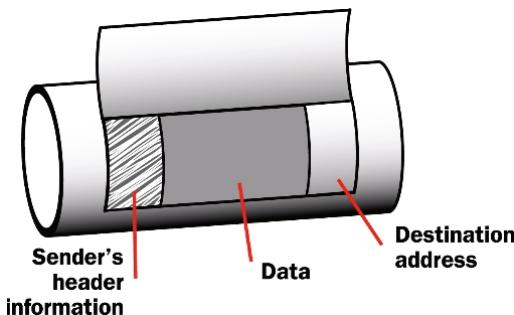
A protocol also tells how data is sent through a network. The most frequently used protocols are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

TCP/IP is the basic protocol used by computers that connect to the Internet.

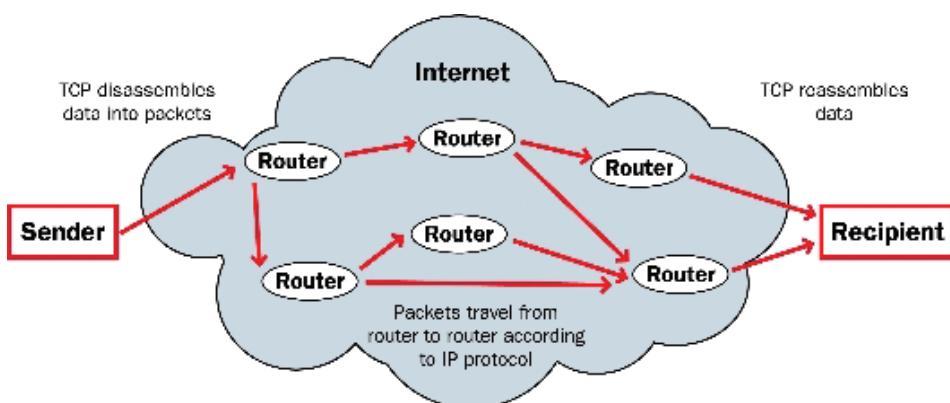
You must know some settings of TCP/IP when you set up your Firebox X Edge. For more information on TCP/IP, see [Find your TCP/IP Properties](#).

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 the original order. To make sure that the packets get to the destination, address information is added to the packets.



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.



About IP addresses

To send ordinary mail to a person, you must know his or her street address. For one computer on the Internet to send data to a different computer, it must know the address of that computer. A computer address is known as an *Internet Protocol (IP) address*. All devices on the Internet have unique IP addresses, which enable other devices on the Internet to find and interact with them.

An IP address consists of four octets (8-bit binary sequences) expressed in decimal format and separated by periods. Each number between the periods must be within the range of 0 and 255. Some examples of IP addresses are:

- 206.253.208.100
- 4.2.2.2
- 10.0.4.1

Private addresses and gateways

Many companies create private networks that have their own address space. The addresses 10.x.x.x and 192.168.x.x are set aside for private IP addresses. Computers on the Internet cannot use these addresses. If your computer is on a private network, you connect to the Internet through a *gateway* device that has a public IP address.

Usually, the *default gateway* is the router that is between your network and the Internet. After you install the Firebox on your network, it becomes the default gateway for all computers connected to its trusted or optional interfaces.

About subnet masks

Because of security and performance considerations, networks are often divided into smaller portions called subnets. All devices in a subnet have similar IP addresses. For example, all devices that have IP addresses whose first three octets are 50.50.50 would belong to the same subnet.

A network IP address's subnet mask, or netmask, is a string of bits that mask sections of the IP address to show how many addresses are available and how many are already in use. For example, a large network subnet mask might look like this: 255.255.0.0. Each zero shows that a range of IP addresses from 1 to 255 is available. Each decimal place of 255 represents an IP address range that is already in use. In a network with a subnet mask of 255.255.0.0, there are 65,025 IP addresses available. A smaller network subnet mask is 255.255.255.0. Only 254 IP addresses are available.

About slash notation

The Firebox uses *slash notation* for many purposes, including policy configuration. Slash notation is a compact way to show the subnet mask for a network. To write slash notation for a subnet mask:

1. First, find the binary representation of the subnet mask.
For example, the binary representation of 255.255.255.0 is
11111111.11111111.11111111.00000000.
2. Count each 1 in the subnet mask.
This example has twenty-four (24) of the numeral 1.
3. Add the number from step two to the IP address, separated by a forward slash (/).

The IP address 192.168.42.23/24 is equivalent to an IP address of 192.168.42.23 with a netmask of 255.255.255.0.

This table shows common network masks and their equivalents in slash notation.

Network mask	Slash equivalent
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30

About entering IP addresses

When you type IP addresses in the Quick Setup Wizard or dialog boxes in Firebox management software, type the digits and periods in the correct sequence. Do not use the TAB key, arrow key, spacebar, or mouse to put your cursor after the periods.

For example, if you type the IP address 172.16.1.10, do not type a space after you type 16. Do not try to put your cursor after the subsequent period to type 1. Type a period directly after 16, and then type 1.10. Press the slash (/) key to move to the netmask.

Static and dynamic IP addresses

ISPs (Internet service providers) assign an IP address to each device on their network. The IP address can be *static* or *dynamic*.

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 is usually more expensive than a dynamic IP address, and some ISPs do not supply static IP addresses. You must configure a static IP address manually.

A dynamic IP address is an IP address that an ISP lets you use temporarily. If a dynamic address is not in use, it can be automatically assigned to a different device. Dynamic IP addresses are assigned using either DHCP or PPPoE.

About DHCP

Dynamic Host Configuration Protocol (DHCP) is an Internet protocol that computers on a network use to get IP addresses and other information such as the default gateway. When you connect to the Internet, a computer configured as a DHCP server at the ISP automatically assigns you an IP address. It could be the same IP address you had before, or it could be a new one. When you close an Internet connection that uses a dynamic IP address, the ISP can assign that IP address to a different customer.

You can configure the Firebox as a DHCP server for networks behind the Firebox. You assign a range of addresses that the DHCP server can choose from.

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 network protocol allows the ISP to use the billing, authentication, and security systems of their dial-up infrastructure with DSL modem and cable modem products.

About 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 System). This is a network system of servers that translates numeric IP addresses into readable Internet addresses, and vice versa. DNS takes the “friendly” domain name you type when you want to see a particular web site, such as www.example.com, and finds the equivalent IP address, such as 50.50.50.1. Network devices need the actual IP address to find the web site, but domain names are much easier for users to type and remember than IP addresses.

A *DNS server* is a server that performs this translation.

About services and policies

You use a *service* to send different types of data (such as email, files, or commands) from one computer to another across a network or to a different network. These services use protocols. Frequently used Internet services are:

- World Wide Web access uses Hypertext Transfer Protocol (HTTP)
- Email uses Simple Mail Transfer Protocol (SMTP) or Post Office Protocol (POP3)
- File transfer uses File Transfer Protocol (FTP)
- Resolving a domain name to an Internet address uses Domain Name Service (DNS)
- Remote terminal access uses Telnet or SSH (Secure Shell)

When you allow or deny a service, you must add a *policy* to your Firebox configuration. Each policy you add 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. We recommend that you add only the policies that are necessary for your business.

As an example of how a policy might be used, suppose the network administrator of a company wants to activate a Windows terminal services connection to the company’s public web server on the optional interface of the Firebox. He or she routinely administers the web server with a Remote Desktop connection. At the same time, he or she wants to make sure that no other network users can use the Remote Desktop Protocol terminal services through the Firebox. The network administrator would add a policy that allows RDP connections only from the IP address of his or her own desktop computer to the IP address of the public web server.

When you configure your Firebox with the Quick Setup Wizard, the wizard adds only limited outgoing connectivity. If you have more software applications and network traffic for the Firebox to examine, you must:

- Configure the policies on the Edge to let necessary traffic through
- Set the approved hosts and properties for each policy
- Balance the requirement to protect your network against the requirements of your users to get access to external resources

About ports

Although computers have hardware ports you use as connection points, ports are also numbers used to map traffic to a particular process on a computer. These ports, also called *TCP and UDP ports*, are where programs transmit data. If an IP address is like a street address, a port number is like an apartment unit number or building number within that street address. When a computer sends traffic over the Internet to a server or another computer, it uses an IP address to identify the server or remote computer, and a port number to identify the process on the server or computer that receives the data.

For example, suppose you want to see a particular web page. Your web browser attempts to connect to port 80 (the port used for HTTP traffic) on the IP address of the web server. When it makes the connection, your web browser sends the request for the web page and gets it from the web server. Both computers then end the connection.

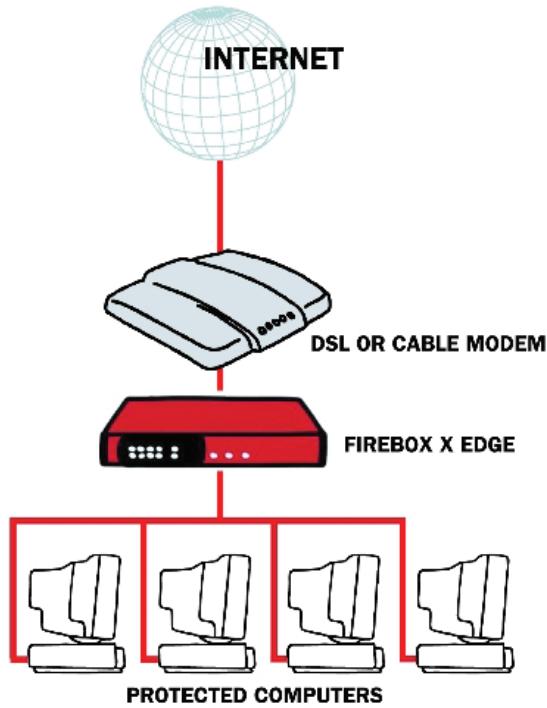
Many ports are used for only one type of traffic, such as port 25 for SMTP (Simple Mail Transfer Protocol). Some protocols, such as SMTP, have ports with assigned numbers. Other programs are assigned port numbers dynamically for each connection. The IANA (Internet Assigned Numbers Authority) keeps a list of well-known ports. You can see this list at:

<http://www.iana.org/assignments/port-numbers>.

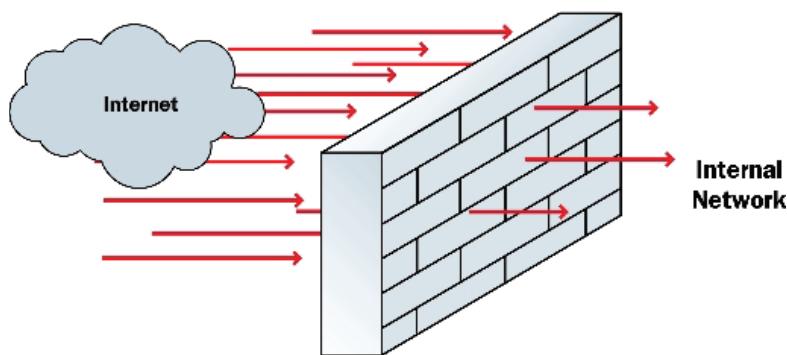
For information on ports used by WatchGuard products and Microsoft products, see the *Reference Guide*. Most policies you add to your Firebox configuration are given a port number in the range from 0 to 1024, but possible port numbers range from 0 to 65535.

About Firewalls

A firewall separates your trusted computers on the internal network from the external network, or the Internet, to decrease risk of an external attack. The figure below shows how a firewall divides the trusted computers from the Internet.



Firewalls use access policies to identify and filter different types of information. They can also control which policies 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, including the Firebox, the user can customize these policies.



Firewalls can be in the form of hardware or software. A firewall protects private networks from unauthorized users on the Internet. All traffic that enters the trusted or protected networks must go through the firewall. The firewall examines each message and denies those that do not match the security criteria or policies.

In some closed, or default-deny firewalls, all network connections are denied unless there is a specific rule to allow the connection. To deploy this type of firewall, you must have detailed information about the network applications required to meet your organization's needs. Other firewalls allow all network connections that have not been explicitly denied. This type of open firewall is easier to deploy, but it is not as secure.

The 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 interface that is separate from the trusted 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 email server. Your firewall can stop all suspicious traffic from the external network to your trusted and optional networks.

The Firebox X Edge e-Series is a firewall for small and remote offices. Some customers who purchase an Edge do not know much about computer networks or network security. The Edge provides wizards and many self-help tools for these customers. Advanced customers can use Edge Pro appliance software's advanced integration features and multiple WAN support to connect an Edge to a larger wide area network. 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. This gives you more time and resources to use on other components of your business.

2 Installation

Before you begin

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

- Verify [basic requirements](#).
- Check the [package contents](#).
- Identify and record the [TCP/IP properties](#) for your Internet connection.
- [Register your Firebox](#) on the WatchGuard LiveSecurity website.
- [Disable the HTTP proxy](#) and [disable the pop-up blocker](#) settings in your web browser.
- [Connect the Edge](#) to your network.
- [Connect your computer](#) to the Edge.
- Use the [Quick Setup Wizard](#) to configure the Edge.

Verify basic requirements

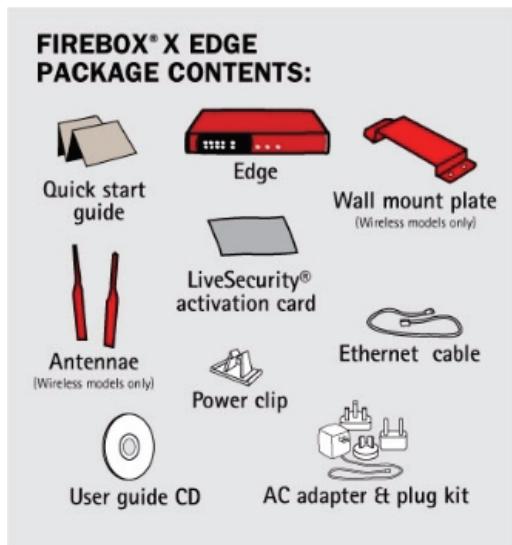
To install the Firebox X Edge e-Series, you must have:

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

Check package contents

Make sure that the package for your Firebox X Edge e-Series includes these items:

- *Firebox X Edge e-Series User Guide* on CD-ROM
- *Firebox X Edge e-Series Quick Start Guide*
- LiveSecurity Service activation card
- Hardware warranty card
- AC power adapter (12 V/1.2A) with international plug kit
- Power cable clip
Use this clip to attach the cable to the side of the Edge. This decreases the tension on the power cable.
- One green straight-through Ethernet cable
- Wall mount plate (wireless models only)
- Two antennae (wireless models only)



Identify your network settings

To configure your Firebox X Edge, you must know some information about your network. Use this section to learn how to identify your network settings. For an overview of network basics, see [About networks and network security](#).

Network Addressing Requirements

Speak with your ISP or corporate network administrator to learn how your computer receives its IP address. Use the same method to connect to the Internet with the Firebox X Edge that you use with your computer. If you connect your computer directly to the Internet with a broadband connection, you can put the 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. For more information about network addressing, see [About configuring external interfaces](#).

Your computer must have a web browser. You use the web browser to configure and manage the Firebox X Edge. Your computer must have an IP address on the same network as the Edge.

In the factory default configuration, the Firebox X Edge assigns your computer an IP address with DHCP (Dynamic Host Configuration Protocol). You can set your computer to use DHCP and then you can connect to the Edge to manage it. You can also give your computer a static IP address that is on the same network as the trusted IP address of the Edge. For more information, see [Set your computer to connect to the Edge](#).

Find your TCP/IP Properties

To learn about the properties of your network, look at the TCP/IP properties of your computer or any other computer on the network. You must have the following information to install your Firebox X Edge:

- IP address
- Subnet mask
- Default gateway
- Whether your computer has a static or dynamic IP address
- IP addresses of primary and secondary DNS servers



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 Firebox X Edge external IP address. If you use a private IP address, you can have problems with some features, such as virtual private networking.

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

Finding your TCP/IP properties on Microsoft Windows Vista

1. Select **Start > Programs > Accessories > Command Prompt**.
The Command Prompt window appears.
2. At the command prompt, type `ipconfig /all` and press **Enter**.
3. Record the values that you see for the primary network adapter.

Finding your TCP/IP properties on Microsoft Windows 2000, Windows 2003, and Windows XP

1. Select **Start > All Programs > Accessories > Command Prompt**.
The Command Prompt window appears.
2. At the command prompt, type `ipconfig /all` and press **Enter**.
3. Record the values that you see for the primary network adapter.

Finding your TCP/IP properties on Microsoft Windows NT

1. Select **Start > Programs > Command Prompt**.
The Command Prompt window appears.
2. At the command prompt, type `ipconfig /all` and press **Enter**.
3. Record the values that you see for the primary network adapter.

Finding your TCP/IP properties on Macintosh OS 9

1. Select the **Apple** menu > **Control Panels** > **TCP/IP**.
The TCP/IP window appears.
2. Record the values that you see for the primary network adapter.

Finding your TCP/IP properties on Macintosh OS X 10.5

1. Select the **Apple** menu > **System Preferences**, or select the icon from the Dock.
The System Preferences window appears.
2. Click the **Network** icon.
The Network preference pane appears.
3. Select the network adapter you use to connect to the Internet.
4. Record the values that you see for the network adapter.

Finding your TCP/IP properties on other operating systems (Unix, Linux)

1. Read your operating system guide to find the TCP/IP settings.
2. Record the values that you see for the primary network adapter.

Find PPPoE settings

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

- Login name
- Domain (optional)
- Password

Register your Firebox and activate LiveSecurity Service

To enable all of the features on your Firebox X Edge, you must register on the WatchGuard LiveSecurity web site and retrieve your feature key. You have only one user license (seat license) until you apply your feature key. You must also use your feature key to apply any additional upgrades that you purchase. See [About user licenses](#) for more information.

When you register, you also activate your free 90-day 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.

To register your Firebox X Edge:

1. Use your browser to go to <http://www.watchguard.com/activate/>



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

2. If you are a new customer, you must create a user profile.
3. If you are an existing customer, log in with your LiveSecurity Service user name and password.
4. Follow the online instructions to register your Firebox X Edge. You must have the serial number. You can find the serial number on the bottom of the Edge or on the box it is packaged in.
5. When you enter your serial number, you receive a feature key. Copy and save this text to a file on your local drive.
6. We recommend that you also download the latest appliance software for your Edge at this time.
7. If a model upgrade key is included with your model, activate it at <http://www.watchguard.com/upgrade>.

Disable the HTTP proxy

Many web browsers are configured to use an HTTP proxy server to increase the download speed of web pages. To manage or configure the Firebox X Edge e-Series, your browser must connect directly to the Edge. If you use an HTTP proxy server, you must temporarily disable the HTTP proxy setting in your browser. You can reenable the HTTP proxy server setting in your browser after you set up the Edge.

Use these instructions to disable the HTTP proxy in Firefox, Safari, 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 Internet Explorer 6.x or 7.x

1. Open Internet Explorer.
2. Select **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** two times.

Disable the HTTP proxy in Firefox 2.x

1. Open the browser software.
2. Select **Tools > Options**.
The Options window appears.
3. Click the **Advanced** icon.
4. Select the **Network** tab. Click **Settings**.
5. Click the **Connection Settings** button.
The Connection Settings dialog box appears.
6. Make sure the **Direct Connection to the Internet** option is selected.
7. Click **OK** two times.

Disable the HTTP proxy in Safari 2.0

1. Open the browser software.
2. From the application menu, select **Preferences**.
The Safari preferences window appears.
3. Click the **Advanced** icon.
4. Click the **Change Settings** button.
The System Preference window appears.
5. Clear the **Web Proxy (HTTP)** check box.
6. Click **Apply Now**.

Disable pop-up blocking

The Firebox X Edge e-Series uses pop-up windows for many features, including the Quick Setup Wizard. If you block pop-up windows, you must disable this function when you connect to the Edge.

Use these instructions to disable the pop-up blocking option in Firefox, Netscape, Safari, or Internet Explorer. If you are using a different browser, use the browser Help system to find the necessary information.

Disable the pop-up blocker in Internet Explorer 6.x or 7.x

1. Open Internet Explorer.
2. Select **Tools > Pop-Up Blocker > Turn Off Pop-Up Blocker**.

Disable the pop-up blocker in Firefox 2.x

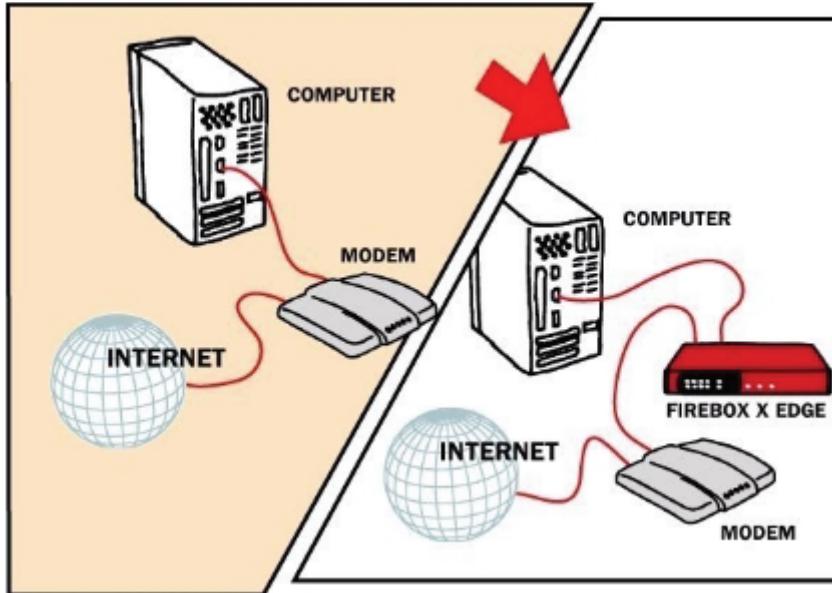
1. Open the browser software.
2. Select **Tools > Options**.
The Options window appears.
3. Click the **Content** icon.
4. Make sure the **Block pop-up windows** option is not selected.
5. Click **OK**.

Disable the pop-up blocker in Safari 2.0

1. Open the browser software.
2. Click **Application**. Make sure that the **Block Pop-Up Windows** menu item is not selected.

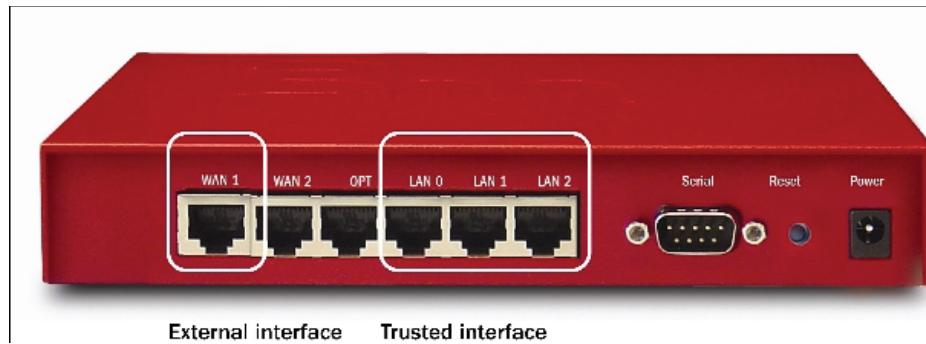
Connect the Firebox X Edge

Many people configure their Firebox X Edge e-Series on one computer before they put it on the network.



Use this procedure to connect a computer to your 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. 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 green Ethernet cable supplied with your Edge. Connect this cable to a trusted interface (LAN0-LAN2) 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, then the WAN indicator lights flash and then come on.



Use only the supplied AC adapter for the Firebox X Edge.

For more information about the location and meaning of the indicator lights on the Firebox X Edge, see the *Firebox X Edge e-Series Hardware Guide*.

Add computers to the trusted network

You can connect as many as three computers to the trusted interface of the Firebox X Edge e-Series if you connect each computer to one of the Edge's Ethernet ports 0 through 2. You can use 10/100 BaseT Ethernet hubs or switches with RJ-45 connectors to connect more than three computers. It is not necessary for the computers on the trusted network to use the same operating system.

To add more than three computers to the trusted network:

1. Make sure that each computer has a functional Ethernet card.
2. Connect each computer to the network. For more information, see [Connect the Edge to more than four devices](#).

Connect the Edge to more than four devices

The Firebox X Edge e-Series has three Ethernet ports (LAN0-LAN2) for the trusted network, and one Ethernet port (OPT) for the optional network. You can connect devices directly to the Edge, or use a hub or switch to connect more than four devices. The number of devices that can connect to the external network is limited by the number of session licenses available. See [About user licenses](#) for more information.

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

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

To connect more 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 WAN1 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 four 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 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.

About user licenses

Your Firebox X Edge firewall is enabled with a set number of user licenses. The total number of available sessions is determined by the Edge model you have, and any upgrade licenses you apply. The number of licenses limits the number of sessions. To control the number of users at any time, close one or more sessions. When you close a session, you make that user license available for another user. There are several procedures to close a session:

- If you require users to authenticate, a Firebox User can manually log out and return his or her license.
- The Edge Administrator can close the session manually. He or she can close the session for an individual user or close all sessions.
- If you require users to authenticate, you can assign a maximum timeout and an idle timeout for each user.
- The Edge administrator can set a global session maximum timeout.
- Reboot the Edge to close all sessions.

You can purchase license upgrades from your reseller, or from the WatchGuard website:
<http://www.watchguard.com/products/purchaseoptions.asp>.

Set your computer to connect to the Edge

Before you can use the Quick Setup Wizard, you must configure your computer to connect to the Firebox X Edge. You can set your network interface card to use a static IP address, or use DHCP to get an IP address automatically.

Use 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. Select **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](#).

Use 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 select an IP address on the same subnet as the trusted network.

1. Select **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. 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. [Run the Quick Setup Wizard](#).

Run the Quick Setup Wizard

The Quick Setup Wizard starts after you type `https://192.168.111.1` into the URL or address field of your Internet browser. If your browser blocks pop-up windows, you must [disable pop-up blocking](#) 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 complete the Quick Setup Wizard.

The Quick Setup Wizard includes this set of dialog boxes. Some dialog boxes appear only if you select certain configuration methods:

Welcome

The first screen tells you about the wizard.

Configure the External Interface of your Firebox

Select the method your ISP uses to assign your IP address.

Configure the External Interface for DHCP

Type your DHCP identification as supplied by your ISP.

Configure the External Interface for PPPoE

Type your PPPoE information as supplied by your ISP.

Configure the External Interface with a static IP address

Type your static IP address information as supplied by your ISP.

Configure the Trusted Interface of the Firebox

Type the IP address of the trusted interface.

Set the User Name and Passphrase

Enter a 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 e-Series Wireless is being used. The country or region 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.

Enter the feature key

(Optional) Paste the feature key text that you copied from the LiveSecurity web site into the empty field.

The Quick Setup Wizard is complete

The Quick Setup Wizard shows a link to the WatchGuard web site to register your product. After you complete the wizard, the Firebox X Edge restarts.



If you change the IP address of the trusted interface, you must change your network settings so that your IP address matches the subnet of the trusted network before you connect to the Firebox X Edge again. If you use DHCP, restart your computer. If you use static addressing, see [Use a static IP address](#).

The System Status page

The System Status page appears on the screen. You can configure more features of your Edge from this page.

Installation

3

Configuration Pages Overview

About Edge Configuration Pages

After you connect the WatchGuard Firebox X Edge e-Series to your network, you must configure the Edge. You can create firewall rules to enforce the security requirements of your company. You can also use the Edge configuration pages to create a user account, look at network statistics, and see the configuration of the Edge.

Read this chapter to find basic information about the Firebox X Edge configuration pages and system monitor pages. Sections in subsequent chapters have more advanced procedures.



You must complete the Quick Setup Wizard before you can see the Firebox X Edge configuration pages. For more information, see [Run the Quick Setup Wizard](#). Also, you must use an account with full administrative access privileges to see and change the configuration pages. For more information, see [About user accounts](#).

Connect to the Firebox X Edge

The System Status page appears when you connect to the Firebox X Edge e-Series. 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 Firebox X Edge trusted interface.

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

This procedure 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 [About changing the IP address of the trusted network](#).

You can also change the Firebox X Edge so that it uses HTTP connections for web management connections instead of HTTPS. HTTP is less secure, because any information you send to the Firebox is unencrypted. We recommend that you always use HTTPS to configure the Firebox X Edge. For more information, see [About selecting HTTP or HTTPS for management](#).

For example:

1. Start your web browser.
2. Select **File > Open**, type `https://192.168.111.1` in the Open text box, and click **OK**. You also can type `https://192.168.111.1` directly into the address or location bar and press **Enter**.
3. When a security certificate notification appears, click **Yes**. You see this warning because the certificate given by the Edge is signed by the WatchGuard certificate authority, which is not a trusted authority on your browser.



This warning will appear each time you use HTTPS to connect to the Firebox X Edge unless you permanently accept the certificate, or generate and import a certificate for the Edge to use. For more information, see [About certificates](#).

4. Enter your user name and password to authenticate.

The System Status page appears.

System Status Uptime: 02:10:24

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	Configure
Firewall	8.6 Jul 18 2007 build 8183	Wireless Guest Network	Disabled	Configure
spamBlocker		WatchGuard Logging	Disabled	Configure
Model	X55e-W	WSM Access	Enabled	Configure
Serial Number	727300019-7529	Syslog	Disabled	Configure

Option	Status	Configure	
User Licenses	Unrestricted	Upgrade	
Manual VPN	0 configured (max 25)	Configure	
MUVPN Clients	0 in use (max 5)	Configure	
WebBlocker	Expires Thu Jan 03 2008	Configure	
spamBlocker	Expires Thu Jan 03 2008	Configure	
GAVIPS	Expires Thu Jan 03 2008	Configure	
VPN	WAN Failover	Disabled	Configure
Wizards	LiveSecurity	Expires Thu Jan 03 2008	Login

Reboot **Update**

Navigating the Firebox X Edge User Interface

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



You must enable JavaScript in your browser to use the navigation bar.

Each menu item contains secondary menus that you use to configure the properties of that feature. To see these secondary menus, click the plus sign (+) to the left of the menu item. For example, if you click the plus sign adjacent to **WebBlocker**, these secondary menu items appear: **Settings**, **Profiles**, **Allowed Sites**, and **Denied Sites**. You can also navigate to the secondary pages directly from the primary pages.

We use an arrow (>) symbol in the documentation 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**.

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. The information on this page includes all general information about your device and configuration. Here you can follow links to network configuration settings, features, and system information.

For more information about using the monitoring categories, see [Monitoring the Firebox X Edge](#).

Network page

The Network page shows the current configuration of the trusted, optional, and external networks. On this page, you can also view WAN failover and any static routes you have configured. Adjacent to each section is a button you can use to change configurations and to see network statistics. For more information, see the topics under [Change the Firebox IP addresses with the Network Setup Wizard](#).

Network		
External Network [Active]		
Configuration Method	Manual Configuration	<input type="button" value="Configure"/>
IP Address	192.168.54.62	
Subnet Mask	255.255.255.0	
Gateway	192.168.54.254	
Primary DNS Server	192.168.130.131	
Secondary DNS Server		
Domain		
MAC Address	00:90:7F:1B:C2:C0	
Trusted Network		
IP Address	192.168.111.1	<input type="button" value="Configure"/>
Subnet Mask	255.255.255.0	
MAC Address	00:90:7F:1B:C2:C1	
DHCP Server	Enabled	
DHCP Lease Duration	0 days 1 hour 0 minutes	
Wireless bridge	Enabled	
Allowed hardware addresses	Disabled	
Optional Network		
IP Address	192.168.112.1	<input type="button" value="Configure"/>
Subnet Mask	255.255.255.0	
MAC Address	00:90:7F:1B:C2:C2	
DHCP Server	Disabled	
DHCP Lease Duration	0 days 1 hour 0 minutes	
Allowed hardware addresses	Disabled	
Wireless Guest Network		
IP Address	192.168.113.1	<input type="button" value="Configure"/>
Subnet Mask	255.255.255.0	
MAC Address	0E:90:7F:1B:C2:C4	
DHCP Server	Disabled	
DHCP Lease Duration	0 days 1 hour 0 minutes	
Allowed hardware addresses	Disabled	

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 [About Mobile VPN client configuration files](#).

Firebox Users

Firebox User Settings

Firebox User accounts are [disabled](#) [Configure](#)

- Automatic prompt for login on Web access: [Disabled](#)
- Reset idle on Firebox X Edge access: [Disabled](#)

Periodic automatic global session time-out is disabled

Active Sessions

Active session count is 1 (maximum is Unrestricted).

User	Host	Close
admin	192.168.111.4	

[Close All](#)

Trusted hosts occupying user licenses: [None](#)

Local User Accounts

[Add...](#)

Name	Admin Level	WebBlocker	MUVPN	PPTP	Edit	Delete
admin	Full	No WebBlocker	Disabled	Disabled	 	
buffster	None	No WebBlocker	Disabled	Enabled	 	

Local Group Accounts

[Add...](#)

Name	Admin Level	WebBlocker	Edit	Delete
Default	None	No WebBlocker	 	

Secure MUVPN Client Configuration Files

External MUVPN access count 0 (maximum 5)

Trusted Hosts

There are no trusted hosts. [Configure](#)

Administration page

The Administration page shows whether the Firebox X Edge uses HTTP or HTTPS for its configuration pages, if the Edge is configured as a managed Firebox client, and which feature upgrades are enabled. It has buttons to change configurations, add upgrades, and see the configuration file. You can also change the name of the Firebox. For more information, see topics under [About basic configuration and management tasks](#).

Administration

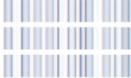
Administrative Options

Device Name

Language

Allow Web browser language preference to override the system language.

System Time

Time Source NTP Server 

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

Current Time 2008-01-03-23:33:57

System Security

WSM Access

Upgrades

Installed Options:

User Licenses	Unrestricted
Remote Gateways	Installed
Mobile VPN with IPSec Clients	Installed - License count 55
WebBlocker	Installed - Expires Wed Dec 31 2008
spamBlocker	Installed - Expires Wed Dec 31 2008
Gateway AV/IPS	Installed - Expires Wed Dec 31 2008
WAN Failover	Installed

Firewall page

The Firewall page shows incoming and outgoing policies and proxies, blocked web sites, and other firewall settings. This page also has buttons to change these settings. For more information, look at the topics below Proxy Settings in the Table of Contents.

Firewall

Trusted Network Optional Network	Firewall	External Network
<u>Outgoing</u>	<u>Policy</u>	<u>Incoming</u>
Disabled	HTTP	Allowed
Disabled	HTTPS	Allowed
Allowed	Outgoing	Disabled
Disabled	FTP	Allowed

[Configure Outgoing](#) [Configure Incoming](#)

Trusted Network	Firewall	Optional Network
<u>Outgoing</u>	<u>Policy</u>	
Allowed	Outgoing	

[Configure Optional](#)

Intrusion Prevention

No blocked sites are defined. [Configure](#)

Log denied traffic from blocked sites: Enabled

Blocked Ports: 0, 1, 111, 513, 514, 2049, 6000, 6001, 6002, 6003, 6004, 6005, 7100, 8000

Auto-block sites that access blocked ports: Disabled

Auto-block source of packets not handled: Disabled

Auto-block duration: 30 minutes

No auto-block exceptions are defined.

Dangerous Activities

Logging page

The Logging page shows the current event log, and the status of the Log Server and syslog logging. For more information, see the topics under Logging in the Table of Contents

Logging			Refresh
Logging Options			
WatchGuard Logging	Disabled	WatchGuard Log Server	Configure
Syslog Logging	Disabled	Syslog Host	0.0.0.0
Configure			
Event Log Filtering			
<input checked="" type="checkbox"/> Status			
<input checked="" type="checkbox"/> Warnings			
<input checked="" type="checkbox"/> Errors			
Submit	Reset		
Event Log			
Time	Category	Message	
Jul 20 12:10:35	fbshd	Remote Management Allowed from 192.168.54.61	
Jul 20 12:10:25	kernel	deny in eth0 78 udp 20 128 192.168.54.144 192.168.54.255 137 137 (broadcast)	
Jul 20 12:10:24	kernel	deny in eth0 78 udp 20 128 192.168.54.144 192.168.54.255 137 137 (broadcast)	

WebBlocker page

The WebBlocker page shows the WebBlocker settings, profiles, allowed sites, and denied sites. For more information, see [About WebBlocker](#).

WebBlocker

WebBlocker Settings

Status	Disabled	Configure
Inactivity Time-out (minutes):	Not Set	
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:	Configure
------------------------------	------------------

 [\[Default\]](#)

Allowed Sites

There are no allowed sites.	Configure
-----------------------------	------------------

Denied Sites

There are no denied sites.	Configure
----------------------------	------------------

spamBlocker page

The spamBlocker page shows spamBlocker status and settings, including actions for suspected spam and the use of trusted email forwarders. For more information, see [About spamBlocker](#).

spamBlocker

spamBlocker Settings

Status for POP3 Proxies	POP3-Proxy	Disabled	Configure
Status for SMTP Proxies	SMTP-Proxy	Disabled	Configure

Actions for suspected spam [POP3](#) [SMTP](#)

Action for spam	Deny
Action for bulk	Deny
Action for suspected spam	Deny

Common Settings [Configure](#)

Trusted Email Forwarders	Disabled
--------------------------	----------

[Learn more about spamBlocker.](#)

Gateway AV/IPS page

The Gateway AV/IPS page shows the Gateway AntiVirus and Intrusion Prevention Service status and settings. It tells you which proxies are enabled for the service, and what version of the signature database you are using. The Gateway AV/IPS menu contains links to change Gateway AV and IPS settings and to update signatures. For more information, see [About Gateway AntiVirus and Intrusion Prevention](#).

Gateway AV/IPS			
Learn more about Gateway AV/IPS.			
Gateway AV Settings			
Status for HTTP proxies	HTTP-Proxy	Disabled	Configure
Status for FTP proxies	FTP-Proxy	Disabled	
Status for POP3 proxies	POP3-Proxy	Disabled	
Status for SMTP proxies	SMTP-Proxy	Disabled	
<hr/>			
Virus is detected (SMTP or POP3 only)			
When an error is encountered		Remove	
Limit Scanning		Disabled	
Signature database version:		Version 45.5348	Configure
Intrusion Prevention Settings			
Status for HTTP proxies	HTTP-Proxy	Disabled	Configure
Status for FTP proxies	FTP-Proxy	Disabled	
Status for POP3 proxies	POP3-Proxy	Disabled	
Status for SMTP proxies	SMTP-Proxy	Disabled	
Signature database version:		Version 10.1.4	Configure

VPN page

The VPN page shows information on managed VPN gateways, manual VPN gateways, echo hosts, and buttons to change the configuration of VPN tunnels. You can add the Firebox X Edge e-Series to a Watchguard System Manager VPN network with the WSM Access page in Administration. For more information, see the topics under [About Branch Office Virtual Private Networks \(BOVPN\)](#).

VPN

Managed VPN Gateways		
Configuration Mode	SOHO	Configure
Manual VPN Gateways		
Remote Gateways	1 configured (max 25)	Configure
Regenerate IPSec Keys		
VPN Keep Alive		
Echo Hosts	10.0.61.254	Configure
VPN Tunnel Status		
Status	Tunnel is active	

Wizards page

The Wizards page shows the wizards you can use to help you set up Firebox X Edge features such as policy configuration, network interface configuration, and WAN failover. Each wizard launches a new window to help you configure the Edge settings.

Wizards

What do you want to do?	Go!
Define a custom policy 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 wireless guest network interface of the Firebox X Edge.	
Configure the automatic WAN failover capability of your Firebox Edge.	
Set up policies to allow traffic for WSM management of other Fireboxes.	

Monitoring the Firebox X Edge

The System Status page is the primary configuration page of the Firebox X Edge. This page appears first when you connect to the Firebox X Edge. The system status page shows:

- Edge components and their current versions
- The serial number of the device
- The status of key 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
- Buttons to restart or update the Edge

When you expand System Status on the navigation bar, you see a list of monitoring categories. With these pages, you can monitor all the components of the Edge and how they work. The Firebox X Edge monitor pages are not set to refresh automatically. If you want a page to refresh automatically, click the **Start Continuous Refresh** or **Restart Continuous Refresh** button at the top of the page. The page refreshes until you click **Pause Continuous Refresh** or you navigate to a new page. You can see a small counter below the button that shows the number of times the page has been refreshed.

IP Address	HW Type	Flags	HW Address	Mask	Device
192.168.54.61	ethernet	valid	00:90:7F:2F:A3:9D	*	external (eth0)
192.168.54.254	ethernet	valid	00:01:30:F3:F1:40	*	external (eth0)

ARP table

This status page shows devices that have responded to an ARP (Address Resolution Protocol) request from the Edge:

IP Address

IP address of the computer that responds to the ARP request.

HW type

Type of Ethernet connection that the IP address uses to connect.

Flags

If the hardware address of the IP resolves, it is marked as **valid**. If it does not, it is marked as **invalid**.



*A valid hardware address can briefly show as **invalid** while the Edge waits for a response for the ARP request.*

HW Address

MAC address of the network interface card that is associated with the IP address.

Mask

If a netmask is associated with the entry, it is listed here. If not, an asterisk (*) is shown.

Device

Interface on the Edge where the hardware address for that IP address was found. The Linux kernel name for the interface is shown in parentheses.

Authentications

This status page shows the IP address, user name, start time, idle time, and connection type for every user that is currently authenticated to the Edge.

Connections

This status page shows all TCP/IP connections that go through the Edge. It is divided between proxy filters and packet filters. The packet filter list is sorted by protocol, with TCP protocols at the top of the list, then UDP connections, then other IP protocols. In TCP/UDP protocols, it is sorted by timeout values.

Proxy filter connections

Type

HTTP, HTTPS, FTP, SMTP, POP3, SIP, or H323

Source: Port

IP address of the computer that sent the packet and the port used to send the packet.

Destination: Port

IP address the packet is being sent to, and the port.

Example Actions

- POP3 shows "n/a"
- HTTP shows the type of request, such as GET or POST. It also shows a hyperlink to the destination web page.
- FTP shows the last FTP command the user issued, such as LIST, CWD, or GET

Packet filter connections

Protocol

Protocol that the connections uses.

Dir

Direction of the connection: incoming or outgoing.

Source: Port

Source IP address and port. A green arrow shows the direction of the connection.

Destination: Port

Destination IP address and port.

State

State of the connection. For TCP it is:

- TIME_WAIT - waiting for the TCP socket to close
- CLOSE - closing the socket
- ESTABLISHED - active connection
- SYN_SENT - establishing connection

UDP is a stateless protocol. For UDP, the connection shows as:

- REPLIED - there have been packets sent in both directions
- UNREPLIED - packets have been sent in only one direction

Other protocols are shown as "n/a".

Expires in (secs)

Number of seconds before the connection times out unless traffic is sent on the connection to restart the timer.

Components list

This status page shows the software that is installed on the Edge. Each attribute is shown separately:

- Name
- Version
- Build number
- Build time
- Remove link - The Remove column does not usually show any components. Any components shown on this list are those supplied by an Edge technical support representative given to you for troubleshooting.

DHCP leases

This status page shows the DHCP server and the leases used by the Edge, including DHCP reservations.

Status

If it appears to the DHCP server that the Edge is using the address, the status is **Active**. If it appears to the DHCP server that the Edge is not using the address, the status is **Abandoned**.

IF

Edge interface that the client is connected to.

IP

IP address for the lease.

Times

S = time that the client requested the lease (start time).

E = time that the lease expires (end time).

MAC

MAC address associated with the lease.

Hostname

If a host name is available, it is shown here.

Disk usage

This status page shows the current state of the flash memory on the Edge.

Filesystem

Name of the partition on the flash memory. "None" is a partition that exists only in memory, not on the flash card.

Size

Size of the partition.

Used

Amount of memory that is used in the partition.

Avail

Amount of free space that is in the partition.

% Used

Percentage of used space on the partition.

Mounted on

Where the partition is mounted in the system.

Dynamic DNS

This status page shows the state of the Dynamic DNS configuration.

Last

Last time the DNS was updated.

Next

Next time the DNS will be updated.

Hostile sites

This status page shows the amount of time an IP address is blocked from access through the Firebox when they are added to the Hostile Sites list. This page also shows a list of IP addresses currently on the Hostile Sites list.

Interfaces

This status page shows information on each interface:

Link Encap

Type of interface. Usually it is Ethernet or PPPoE.

HWaddr

MAC address of the interface.

inet addr

IP address of the interface.

Bcast

Broadcast address of the interface.

Mask

Network mask.

Interface status

If interface is active, the word "Up" appears.

MTU
TCP maximum transmission unit.

Metric
Metric of the interface.

RX packets
Statistics of received packets.

TX packets
Statistics of sent packets.

Collisions
The number of collisions.

TXqueuelen
The maximum size of the transmit queue before the Edge starts to drop packets.

RX and TX bytes
Amount of data received and sent on the interface.

License

This status page shows basic information about licenses that are used on the Edge. It also shows the original feature key. You can see this information for each license:

- Name - the name of the license
- Use - the number of users
- Maximum use - maximum number of users allowed by the license
- Reboot - shows if a reboot is necessary after a configuration change for that license
- Expiration - shows when the license expires
- Comment

LiveSecurity

This page shows you the most recent alerts from the WatchGuard LiveSecurity Service. When a new alert is available, you see a note in the upper right corner of the System Status page. Click the alert notice to see the alert. Alerts notifications are sent no more than one time each day.

Memory

This status page shows the state of the linux kernel memory.

Processes

This status page shows all processes that run on the Edge. It also shows the load average for the CPU. Averages are shown in 1-minute, 5-minute, and 15-minute increments.

PID
Process ID, a unique number that shows when the process started.

NAME
Name of the process.

STATE

State of the process:

R — running

S — sleeping

D,Z — inactive

RSS

Total number of kilobytes of physical memory used by the process.

SHARE

Total number of kilobytes of shared memory used by the process.

TIME

Time that the process has used since the last time the Edge was started.

CPU

Percentage of CPU time used by the process since the last time the Edge was rebooted.

PRI

Priority of the process. A lower number has a higher priority for CPU resources.

SCHED

Measure of how the kernel schedules the process.

Protocols

This status page shows the protocol statistics for IP, ICMP, TCP, and UDP.

Routes

This status page shows the Edge routing table.

Interface

Interface associated with the route.

Network

Network that the route has been created for.

Gateway

Gateway that the network uses.

Flg

Flags set for each route.

Met

Metric set for this route in the routing table.

Mask

Network mask for the route.

MTU

TCP Maximum Transmission Unit.

Win

TCP window size for connections on this route.

Ref

Number of references to this route.

Security Services

This status page shows basic reports on the activity of any enabled security subscription: Gateway AntiVirus, the Intrusion Prevention Service, WebBlocker, and spamBlocker. There is a report for each security subscription in which you can see the amount of processed and blocked requests for each service over a time period you specify.

Syslog

This status page shows the most recent entries in the Edge log file. This is different from the log files shown on the Logging page. The Logging page shows a summary of the log message and the Syslog monitor shows all details for the log message. This is useful for troubleshooting network problems. The log messages are color-coded:

- Red - Error
- Yellow - Warning
- Green - Information
- Blue - Debug
- Gray - Other

Traffic Control

This status page shows how traffic control handles packets.

Priority

You can set four levels of priority for Traffic Control:

- Interactive
- High
- Medium
- Low

Rate

Rate set for each priority.

Ceiling

Maximum bandwidth each priority can use.

Data Sent

Number of bytes of data sent.

Packets Sent

Number of packets sent.

Dropped

Number of packets dropped.

Overlimits

Number of packets over the limit for each priority.

VPN statistics

This status page shows VPN statistics such as:

- SA (Security Association)
- Traffic control within VPN tunnels
- Packet counts
- Errors

Wireless statistics

This status page shows statistics about wireless traffic such as:

- Interface statistics
- Keys
- Bit rates
- Frequencies

4

Configuration and Management Basics

About basic configuration and management tasks

After your Firebox X Edge e-Series 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. The topics in this section help you perform these basic management and maintenance tasks.

About the Edge backup configuration file

Sometimes, you must restore the factory-default settings for your Firebox X Edge e-Series. When you do this, all of your configuration changes are lost. If you have complex policy settings or many user accounts, it can take a long time to configure all of your policies and users again.

To decrease this setup time, you can back up your configuration to a local file and restore it later. This procedure does not help you if you forgot or do not know an administration passphrase for your Edge. In this case, you must reset the Edge to factory-default settings and create a new configuration. You can restore your Firebox X Edge configuration when you run the Quick Setup Wizard, or from an Edge management session. You can also use a backup configuration file to copy your configuration to a different Firebox X Edge if you have a second serial number and feature key.

A backup configuration file stores:

- Trusted, optional, and external network settings
- Certificates
- Local user accounts and passwords
- Passwords used with a Management Server
- Proxy and packet filter policies
- WebBlocker, spamBlocker, Gateway AV, and IPS settings

A backup configuration file does not include:

- Your license key or feature keys
- Gateway AV, IPS, or spamBlocker signatures
- The serial number of your Edge
- The MAC address of any network interface on the Edge

Before You Begin

- Do not edit your configuration file manually. Always use a WatchGuard Management Server or the Firebox X Edge web interface to make changes to your configuration.
- User passwords in the backup configuration file are encrypted, but the full file is not encrypted. We recommend that you encrypt your backup configuration file and keep it in a safe location.
- When you restore your previous configuration from a backup configuration file, the administrator user name and password used when the backup file was created are used again. If you do not remember the password set in your backup file, you must restore the factory-default settings and set up the Edge manually.

See the Configuration File

You can see the contents of the Firebox X Edge configuration file in text format from the View Configuration File page.

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1
2. From the navigation bar, select **Administration > View Configuration**.
The configuration file is shown.



The screenshot shows a web page with a header 'Administration' and a sub-header 'View Configuration File'. Below this, there is a large text area containing the following configuration parameters:

```
FDATE: Dec 27 2007
FTIME: 05:04:31
FVER: 10.0.B164431
admin.external_access: 1
admin.idle_timeout: 0
admin.ipsec_access: 1
admin.max_access: 0
admin.mvpn_access: 0
admin.trusted_access: 1
auth.ldap.domain: test
auth.ldap.enable: 0
auth.ldap_group_attr: isMemberOf
```

Back up your Edge configuration

After you have configured your Firebox X Edge e-Series, you can save your Edge configuration file to your local hard drive for backup purposes. You can use your backup file to restore your Edge to a previous configuration if you make a change that does not work the way you intended, or after you reset the Edge to factory default settings.

Create a backup configuration file

1. To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1
2. From the navigation bar, select **Administration > Backup Configuration**.
The Backup Configuration File page appears.
3. Click the **Backup** button.
4. When the file download dialog box appears, save the backup configuration file to your hard disk.
The backup file is named edgecfg.wgbk by default. You can rename the file, but we suggest you keep the .wgbk filename extension.

Restore your Edge configuration

After you have configured your Firebox X Edge e-Series, you can save your Edge configuration file to your local hard drive for backup purposes. You can use your backup file to restore your Edge to a previous configuration if you make a change that does not work the way you intended, or after you reset the Edge to factory default settings.

You can restore your Firebox X Edge configuration when you run the Quick Setup Wizard, or from an Edge management session.

Before You Begin

- Do not edit your configuration file manually. Always use a Management Server or the Firebox X Edge web interface to make changes to your configuration.
- User passwords in the backup configuration file are encrypted, but the full file is not encrypted. We recommend that you encrypt your backup configuration file and keep it in a safe location.
- When you restore your previous configuration from a backup configuration file, the administrator user name and password used when the backup file was created are used again. If you do not remember the password set in your backup file, you must restore the factory-default settings and set up the Edge manually.

Restore your configuration from a backup file

1. To connect to the System Status page, type **https://** in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1
2. From the navigation bar, select **Administration > Restore Configuration**.
The Restore Configuration File page appears.
3. Type the path to the backup configuration file on your hard disk, or click the **Browse** button to select the file.
4. Click **Restore**.
The Firebox X Edge restarts after 1-2 minutes.

Reconnect the Firebox X Edge to a management server

If your Firebox was managed by a WatchGuard System Manager Management Server, then you must do additional steps to restore communication between your Firebox X Edge and your Management Server after restoring your Edge configuration.

Use these steps to re-enter all WSM access configuration information on the Firebox X Edge:

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`.
2. 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 7.3

Status Passphrase
Confirm Status Passphrase
Configuration Passphrase
Confirm Configuration Passphrase

Management Server Address
Client Name
Shared Key

3. Select the **Enable remote management** check box.
4. From the **Management Type** drop-down list, select **WatchGuard System Manager**.
5. To enable centralized Edge management through WatchGuard System Manager, select the **Use Centralized Management** check box. When the Firebox X Edge is under centralized management, access to the 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 Edge configuration again.
Do not select this check box if you use WatchGuard System Manager only to manage VPN tunnels.
6. Type the status passphrase for your Firebox X Edge and then type it again to confirm. The passphrase must match the passphrase you used when you added the device to WatchGuard System Manager.
7. Type a configuration passphrase for your Firebox X Edge and then type it again to confirm. The passphrase must match the passphrase you used when you added the device to WatchGuard System Manager.

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 that protects the Management Server.
The Firebox that protects 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 required for this to occur.
9. Type the **Client Name** used to identify your Firebox X Edge in the management server configuration.
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.
11. Click **Submit**.

Use these steps to update the Edge from the Management Server.

1. Open WatchGuard System Manager and connect to your Management Server.
2. Click the **Device Management** tab.
3. Right-click the Firebox X Edge you want to restore, and select **Update Device**.
4. Select the **Download Trusted and Optional Network Policies**, **Reset Server Configuration**, and **Expire Lease** check boxes.
5. Click **OK**. The Firebox X Edge restarts and can now connect to the Management Server.

Related questions

What is included in the Edge backup configuration file?

When you back up an Edge configuration file, it includes all Edge policies and settings, user passphrases, and manual VPN configuration information. It does not include any license information, GAV signatures, or configuration information related to WatchGuard System Manager access or managed VPN tunnels.

Can I use the procedure in this document to create a backup configuration file for my Firebox X Edge (non-e-Series) or SOHO6?

Yes. The same restrictions apply.

About 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 any changes. The default network and configuration properties for the Edge are:

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. By default, the IP addresses given can be from 192.168.111.2 to 192.168.111.254.

External network

The Firebox is configured to get an IP address with DHCP.

Optional network

The optional network is disabled.

Firewall settings

All incoming policies are denied. The outgoing policy allows all outgoing traffic. Ping requests received on the external network are denied.

System Security

The Firebox X Edge e-Series 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 for local management from the trusted network only. Additional configuration changes must be made to allow administration from the external network.

Upgrade Options

Upgrade options such as WebBlocker, spamBlocker, and Gateway AV/IPS are always available. You must type the feature keys into the configuration page or use the feature key synchronization feature to activate upgrade options. If you restore the Firebox X Edge to its factory default settings, you do not have to type the feature keys again.

Restore the Firebox to the factory default settings

If you cannot correct a configuration problem and must start over, you can restore the factory default settings. For example, if you do not know the administrator account passphrase or a power interruption causes damage to the Firebox X Edge appliance software, you can restore the Edge to the factory default settings and build your configuration again.

To set the Firebox X Edge e-Series to the factory default settings:

1. Disconnect the power supply.
2. Hold down the **Reset** button on the rear side of the Edge.
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 stays on. This shows you that the Edge was successfully restored to the factory default settings.

This process can take 45 seconds or more.



Do not try to connect to the Edge at this time. You must 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 that shows the message, 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. If you continue to see this page, check the Reset button, and start the Edge again.

5. Disconnect the power supply.
6. Connect the power supply again.

The Power Indicator is on and your Edge is reset.

About feature keys

A feature key is a unique set of alphanumeric characters that enables you to use a set of features on the Firebox. You increase the functionality of your Firebox when you purchase an option or upgrade and get a new feature key.

When you purchase a new feature

When you purchase a new feature for your Firebox, you must:

- [Get a feature key](#)
- [Add a feature key to the Firebox X Edge](#)

Get a current feature key

If your feature key file is not current, you can download a copy of any feature key file from the Firebox to your management station. To download feature keys from a Firebox, from the **Firebox Feature Key** dialog box, click **Download**. A dialog box appears for you to type the status passphrase of the Firebox.

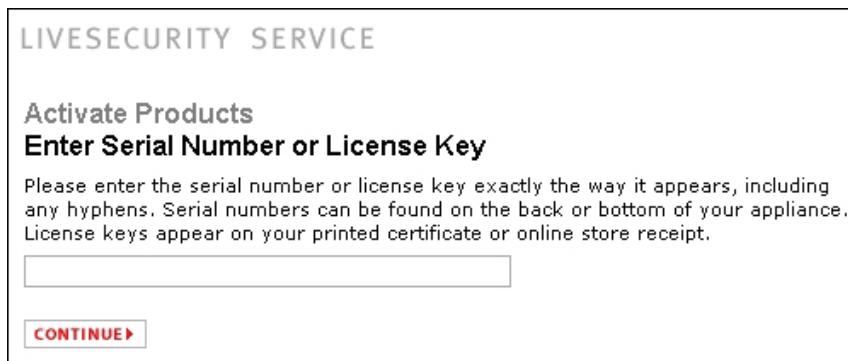
You can also use Firebox System Manager to get a current feature key. If you have already created a LiveSecurity user account, from Firebox System Manager, select **Tools > Synchronize Feature Key**. The Firebox contacts the LiveSecurity web site and downloads the current feature key to your Firebox.

You can use the Feature Key Sync button on your System Status page to get a current feature key. If you have already created a LiveSecurity user account, the Feature Key Sync feature lets the Firebox contact the LiveSecurity web site and download the current feature key to your Edge.

Get a feature key

Before you activate a new feature, you must have a license key certificate from WatchGuard that is not already registered on the LiveSecurity web site.

1. Open a web browser and connect to:
<https://www.watchguard.com/activate>
2. If you have not already logged in to LiveSecurity, you are directed to the LiveSecurity Log In page. Type your LiveSecurity user name and passphrase.
3. Type the serial number or license key for the product as it appears on your printed certificate, including the hyphens. You usually use the serial number to register a new Firebox, and the license key to register add-on features.



LIVESECURITY SERVICE

Activate Products

Enter Serial Number or License Key

Please enter the serial number or license key exactly the way it appears, including any hyphens. Serial numbers can be found on the back or bottom of your appliance. License keys appear on your printed certificate or online store receipt.

CONTINUE

4. Click **Continue**. The Choose Product to Upgrade page appears.
5. From the drop-down list, select the Firebox to which you want to apply the upgrade or renewal. If you added a Firebox name when you registered your Firebox, that name appears in this list. After you select the Firebox, click **Activate**.
6. The Retrieve Feature Key page appears. From your Windows Start menu, open Notepad or any application into which you can save text. Copy the full feature key from this page to a text file and save it on your computer. Click **Finish**.

About Restarting the Firebox

You can restart the Firebox X Edge e-Series from a computer on the trusted network. If you enable external access to the Edge, you also can restart the Edge from a computer on the Internet.

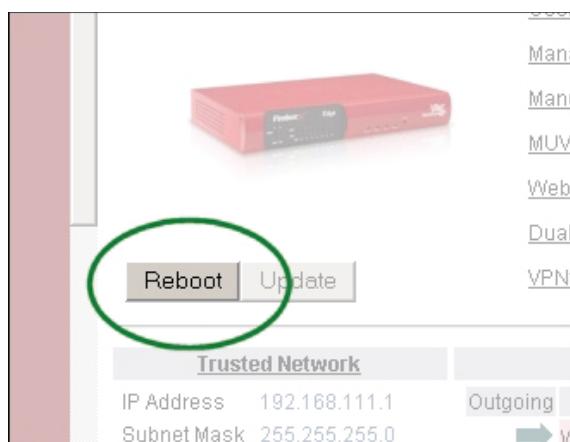
The Firebox X Edge restart cycle is approximately one minute. During the restart cycle, the mode indicator on the front of the Edge turns off and then turns on again.

Restart the Firebox locally

You can locally restart the Firebox X Edge e-Series with one of 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 Firebox X Edge trusted network interface.
The default URL is: `https://192.168.111.1`
2. Click **Reboot**.



Disconnecting the power supply

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

Restart the Firebox remotely

If you want to be able to connect to the Edge to manage it or restart it from a computer external to the Edge, you must first configure the Edge to allow incoming HTTPS traffic to the Edge trusted interface IP address. For more information on how to configure the Edge to receive incoming traffic, see [Set access control options \(incoming\)](#). Remember that if you enable HTTPS connections to the Edge, anyone who has the correct credentials can also connect to the Edge. After HTTPS traffic is allowed, you can remotely manage your Edge using your browser from a trusted IP address.

To do a remote restart:

1. To connect to the System Status page, type `https://` in the browser address bar, and then the IP address of the Firebox X Edge external interface.
The default URL is: `https://192.168.111`.
2. Type your user name and passphrase. You must log in as the Edge administrator, or as a user with administrative access.
3. On the System Status page, click **Reboot**.

About using NTP to set system time

To set the system time for Edge, you can specify a NTP server to set the time automatically. The Network Time Protocol (NTP) synchronizes computer clock times across a network. The Firebox can use NTP to get the correct time automatically from NTP servers on the Internet. Because the Firebox puts the time from its system clock in each log message it generates, the time must be set correctly. You can change the NTP server that the Firebox uses. You can also add more NTP servers or delete existing ones, or you can set the 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 Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`
2. From the navigation bar, select **Administration > System Time**.
The System Time page appears.

Administration
System Time

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

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

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

Set date and time manually

Date Time

3. Select the time zone from the drop-down list.

4. 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.
5. If you set the system time automatically, the Firebox X Edge gets the current time from the selected server in the NTP Servers list. If that server is not available, the Edge uses the next server.
 - o To add a time server, type the server name in the **Add New Server** field and click **Add**.
 - o To remove a time server, select the server from the NTP Servers list and click **Remove**.
 - o 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 both the date and time.
 - o Select the month from the first drop-down list.
 - o Select the year from the second drop-down list.
 - o Click the button with the number that is today's date.
7. To the right of the date, set the time.
 - o Type the hours in the first field.
 - o Type the minutes in the second field.
 - o Type the seconds in the third field.
 - o Select **AM** or **PM** from the drop-down list.
8. Click **Submit**.

About SNMP

Simple Network Management Protocol (SNMP) is a set of tools for monitoring and managing networks. SNMP uses management information bases (MIBs) that give configuration information for the devices the SNMP server manages or monitors. The Firebox X Edge supports SNMPv2c and SNMPv3.

SNMP polls

You can configure the Firebox to accept SNMP polls from an SNMP server. The Firebox reports information to the SNMP server such as the traffic count from each interface, device uptime, the number of TCP packets received and sent, and when each Firebox interface was last modified.

Enable SNMP Polling

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`.
2. From the navigation bar, select **Administration > SNMP**.
The Simple Network Management Protocol page appears.
3. The **Contact E-mail** and **Location** information is given to the SNMP server when it polls the Edge. Type information in these fields that you want the SNMP server administrator to see if they detect a problem with the Edge.
4. Click the **Enable SNMP v2c** check box if the SNMP server uses SNMP v2c. You must type the **Community String** the SNMP server uses when it contacts the Edge. The community string is like a user ID or password that allows access to the statistics of a device. This community string must be included with all SNMP requests.
5. Click the **Enable SNMP v3** check box if your SNMP server uses SNMP v3. You must type the **User name** and **Password** the SNMP server uses when it contacts the Edge.
6. If the SNMP server that polls the Edge is located on the Edge trusted network, click the **Trusted Access** check box. Click **Submit**. You do not need to do steps 7-10. If the SNMP server that polls the Edge is located on the optional network, click the **Optional Access** check box. Click **Submit**. You do not need to do steps 7-10.
7. If the SNMP server that polls the Edge is located on an external network, continue on with steps 7-10. If the SNMP server that polls the Edge is located on an external network, you must add an incoming SNMP policy to your Edge configuration and allow SNMP connections to the Edge external interface. From the navigation bar, select **Firewall > Incoming**.
8. Find **SNMP** in the list of pre-defined policies. Select **Edit**.
9. From the **Incoming Filter** drop-down list, select **Allow**. In the **Policy Host** text box, type the trusted IP address of your Firebox X Edge. This rule allows the SNMP server to connect to the Edge to get SNMP data on TCP port 161. It is a good idea to specify the IP address of your SNMP server in the **From** field so that only connections from the IP address of the SNMP server are allowed by the Firebox.
10. Click **Submit** to save the changes to the Firebox X Edge.

About MIBs

A MIB (Management Information Base) is a database of objects that can be monitored by a network management system. The Firebox X Edge e-Series supports six different public, read-only MIBs:

- IP-MIB
- IF-MIB
- TCP-MIB
- UDP-MIB
- SNMPv2-MIB
- RFC1213-MIB

About 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 you use HTTPS, all information sent between the web server and your browser is encrypted. The Firebox X Edge e-Series uses HTTPS by default, for better security.

To make the Firebox X Edge configuration pages appear more quickly, you can use HTTP. Because HTTP is less secure, we do not recommend that you use HTTP for Edge management. When you use HTTP, all configuration changes are sent to the Edge from your computer in clear text. We recommend that you always use HTTPS to configure your Edge. You must connect to the Firebox X Edge using HTTPS one time before you can connect using HTTP.

Use HTTP instead of HTTPS

1. Type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface. *The default URL is: https://192.168.111.1*
2. From the navigation bar, select **Administration > System Security**.
The System Security page appears.

Administration
System Security

Use non-secure HTTP instead of secure HTTPS for administrative Web site.

HTTP Server Port

Certificate

[Learn more about managing the Firebox X Edge.](#)

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. If you want to use a certificate to help secure the management session, select it from the **Certificate** drop-down list. This option is active only if you have already imported certificates for use on the Edge. For more information on how to use certificates, see [About using certificates on the Firebox X Edge](#).
4. Click **Submit**.

If you select this check box, type `http://` in the browser address bar instead of the default `https://` to see the configuration pages. You can no longer connect to the Edge with `https://` to see the configuration pages.

Change the HTTP server port

HTTPS typically uses TCP port 443 and HTTP typically uses TCP port 80. By default, you must connect to the Firebox X Edge e-Series configuration pages on those ports. You can change the default port on the **Administration > System Security** page. Type the new value in the **HTTP Server Port** field in the System Security configuration page shown above.



After you change the HTTP server port, you must type the port when you connect to the Firebox X Edge. For example, if you change the HTTP server port to 880, when you want to connect to the Edge you must type: <http://192.168.111.1>:

About WatchGuard System Manager access

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

- With WatchGuard System Manager v8.3.1 and above, you can manage policies, updates, and VPNs for many Edge devices from one location.
- With WatchGuard System Manager v7.3 or below, you can use VPN Manager to create managed VPN tunnels between a Firebox X Edge and a different WatchGuard Firebox.

Rename the Firebox X Edge e-series in WSM

When you use WatchGuard System Manager to manage many different Edge devices, you can rename the Firebox X Edge e-Series so that it shows a unique name in WatchGuard System Manager.

1. To connect to the System Status page, type https:// in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1
2. From the navigation bar, select **Administration**. The Administration page appears.
3. Type a name for your Firebox X Edge e-Series in the **Device Name** field.
4. Click **Submit**. When the Edge is shown in WatchGuard System Manager, you see this name.

Enable centralized management with WSM

Use these instructions to configure remote access from WatchGuard System Manager (WSM) 10. WSM 10 allows centralized management of Firebox X Edge e-Series devices running v10.

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

3. Select the **Enable remote management** check box.
4. From the **Management Type** drop-down list, select **WatchGuard Management System**.
5. To enable centralized Edge management through WatchGuard System Manager, select the **Use Centralized Management** check box. When the Firebox X Edge is under centralized management, access to the 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 Edge configuration again.
Do not select this check box if you use WatchGuard System Manager only to manage VPN tunnels.
6. Type a status passphrase for your Firebox X Edge and then type it again to confirm.
7. Type a configuration passphrase for your Firebox X Edge and then type it again to confirm.



If you do not type the same passphrase when you add the device to WatchGuard System Manager, you cannot connect to the Firebox X Edge.

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 that protects the Management Server.
The Firebox that protects 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 required for this to occur.
9. Type the **Client Name** to give to 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. Get the shared key from your network administrator.
11. Click **Submit**.

Enable remote management with WFS v7.3 or earlier

Use these instructions to configure remote access from WatchGuard Firebox System v7.3 or earlier. These versions of WatchGuard Firebox System use VPN Manager and the Firebox is the DVCP Server.

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

3. Select the **Enable remote management** check box.

4. From the **Management Type** drop-down list, select **VPN Manager**.
5. If you use VPN Manager 7.3, select the **VPN Manager 7.3** check box.
6. Select 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 Edge.



If you do not type the same passphrase when you add the device to VPN Manager, you cannot connect to the Firebox X Edge.

7. Select the **Enable Managed VPN** check box to configure the Firebox X Edge as a client to the 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 to 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. Get the shared key from your network administrator.
11. Click **Submit**.

Allow traffic from a management server

If you have a server on the trusted or optional network that you use to manage Fireboxes on the external network, you must change some settings in your configuration to allow that traffic through the Edge. You can use a wizard to apply these configuration changes automatically. Before you begin the wizard, you must have the IP address of the Management Server. From the navigation bar, select **Wizards**. Then select the wizard **Set up policies to allow traffic for WSM management of other Fireboxes**.

About managing the Edge from a remote location

The Firebox X Edge® is configured using a web browser. The Edge web server uses Secure Sockets Layer (SSL), which encrypts your web connections to the Edge. Unencrypted web connections that use HTTP have `http://` in the address bar and connect, by default, on port 80. Web connections that use SSL have `https://` in the address bar and connect, by default, on port 443.

To manage the Edge from a remote location, you must configure the Edge to accept HTTPS connections on the external interface and forward those connections to the trusted interface. Then you can use a web browser to connect to the Edge from a remote location.

Configure the Edge to forward HTTPS connections

You must do this procedure from a computer that is connected to the Edge trusted network.

1. To connect to the System Status page, type `https://` in the browser address bar, and then the IP address of the Firebox X Edge external interface.
The default URL is: `https://192.168.1.11`
2. Type your user name and passphrase. You must log in as the Edge administrator, or as a user with administrative access.
3. From the navigation bar on the left side, select **Firewall > Incoming**.

Filter	Policy	Host	Port Redirect
No Rule	SMTP-Proxy	0.0.0.0	25

Filter	Policy	Host	Port Redirect
No Rule	DNS	0.0.0.0	
Allow	FTP	192.168.111.1	
No Rule	HTTP	192.168.111.1	80
Allow	HTTPS	192.168.111.1	443
No Rule	ILS	0.0.0.0	389
No Rule	IPSec	0.0.0.0	
No Rule	NetMeeting	0.0.0.0	
No Rule	NNTP	0.0.0.0	119
No Rule	Ping	0.0.0.0	
No Rule	POP3	0.0.0.0	110
No Rule	PPTP	0.0.0.0	
No Rule	SMB	0.0.0.0	
No Rule	SMTP	0.0.0.0	25
No Rule	SNMP	0.0.0.0	161
No Rule	ssh	0.0.0.0	22
No Rule	Telnet	192.168.111.1	23
No Rule	WG-Logging	0.0.0.0	
No Rule	WG-Firebox-Mgmt	0.0.0.0	
No Rule	WG-Mgmt-Server	0.0.0.0	

Filter	Policy	Host	Port Redirect
No custom packet filter policies are defined.			

4. From the **Filter** drop-down list adjacent to HTTPS, select **Allow**.
5. In the Host text box, type the IP address of the Edge trusted interface. The default is 192.168.111.1. 7
Scroll to the bottom of the page and click **Submit**.



If your ISP assigns you an address using DHCP or PPPoE, your external IP address may change from day to day. You can [set up the Firebox X Edge for Dynamic DNS](#) so that you do not have to know the current external IP address.

About updating the Firebox X Edge software

One advantage of your LiveSecurity Service is continuous 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 e-Series software. To install any firmware on the Edge, you must have a current LiveSecurity subscription. For Firebox X Edge updates, see the WatchGuard web site at:
<https://www.watchguard.com/archive/softwarecenter.asp> (select Firebox X Edge)

There are two different procedures to install 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, you must use the second procedure.

If for any reason you want to downgrade to an earlier version of Edge firmware, you can apply the firmware with the same procedures. Some newer versions of Edge hardware can be downgraded to only version 8.5.2 or later.

Method 1: Install software automatically

The first method installs the Firebox X Edge e-Series 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. When you see the prompt, type the Firebox X Edge e-Series 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 e-Series. As part of the update process, the Firebox X Edge restarts one or two times—this is usual.
4. Click **Finish**.



Because the Installer uses FTP to transfer files, make sure your Firebox X Edge is not configured to deny FTP traffic. See [Drop DOS flood attacks](#) for more information.

Method 2: Install software manually

The second method uses the Firebox X Edge e-Series 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 compressed file.

1. Extract the .sysa-dl file from the compressed file you downloaded with an archiving utility such as WinZip (for Windows computers), StuffIt (for Macintosh), or the zip program (for Linux).
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. From the navigation bar, select **Administration > Update**.
The Update page appears.
4. Type the name and location 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.
5. 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.

About upgrade options

You use two items to add upgrades to your Firebox X Edge: a feature key and a license key. It is important to understand the differences between these two keys.

Your Firebox X Edge comes with certain features by default. These features are specified by the feature key. If you purchase an upgrade for your Edge, you must apply a new feature key to your Edge.

You do not immediately get a feature key when you upgrade your Edge, however. When you purchase an upgrade, you receive a license key. You must enter this key on the LiveSecurity web site to get a new feature key. You then add the feature key to your Edge configuration or use the feature key synchronization feature to have the Edge connect to the LiveSecurity web site and download the new feature key.

Available 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.

Mobile VPN with IPSec Clients

The Mobile VPN with IPSec Clients upgrade allows a larger number of remote users to connect to the Firebox X Edge through a secure (IPSec) VPN tunnel. These users have access to resources on the trusted and optional networks.

WebBlocker

The WebBlocker upgrade enables you to control access to web content. For more information, see [About WebBlocker](#).

spamBlocker

The spamBlocker upgrade allows you to filter spam and bulk email. For more information, see [About spamBlocker](#).

Gateway AV/IPS

The Gateway AV/IPS upgrade enables you to block viruses and prevent intrusion attempts by hackers. For more information, see [About Gateway AntiVirus and Intrusion Prevention](#).

Edge Pro

The Edge Pro appliance software upgrade allows you to enable a second external interface on your Firebox X Edge e-Series. If you configure your Firebox for multi-WAN, you can use policy-based routing to match a firewall policy with a specific external interface. You can also enable the VLAN tagging feature.

Add a feature to your Firebox X Edge

When you purchase an upgrade for your Firebox X Edge, you receive a license key. This can be a paper certificate or an email message. You can use this procedure to manually apply a new feature key to your Edge, or you can use the feature key synchronization feature available on the System Status page to automatically apply your feature key after you activate it on the LiveSecurity web site.

1. Register the license key and copy the new feature key, as described in [Get a feature key](#).
2. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is `https://192.168.111.1`.
3. Accept the security certificate.
4. Type the **Administrator User Name** and **Password** when prompted.

5. From the navigation bar on the left side, select **Administration > Upgrade**.
The Upgrade window appears.

To download your feature key through LiveSecurity: **Get License Key**

Paste the contents of the feature key in the area below

Learn more about [upgrading the Firebox X Edge](#).

Submit **Reset**

6. Click **Get License Key** or paste in the new feature key.
You can right-click and select Paste or you can use CTRL-V.
7. Click **Submit**.
8. Restart the Edge.

Upgrade your Firebox X Edge model

A model upgrade gives the Firebox X Edge e-Series the same functions as a higher model. A model upgrade increases capacity, user licenses, sessions, and VPN tunnels. For a brochure that shows the features of the different Firebox X Edge models, go to:

http://www.watchguard.com/docs/datasheet/wg_edge-e_ds.pdf

After you purchase an upgrade license key you can upgrade a Firebox X Edge e-Series 10e or a Firebox X Edge 20e to a higher model:

1. Go to the upgrade site on the WatchGuard web site (<http://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 follow the instructions.

5

Network Settings

About network interface setup

A primary component of the WatchGuard Firebox setup is the configuration of network interface IP addresses. When you run the Quick Setup Wizard, the external and trusted interfaces are set up so traffic can flow through the Firebox. You can use the procedures in this section to change this configuration after you run the Quick Setup Wizard, or to add other components of your network to the configuration. For example, you can set up an optional interface for public servers such as a web server.

A firewall physically separates the networks on your Local Area Network (LAN) from those on a Wide Area Network (WAN) like the Internet. One of the basic functions of a firewall is to move packets from one side on the firewall to the other. The common name for this is routing. To route packets correctly, the firewall must know what networks are accessible through each of its interfaces.

The Firebox has three basic types of interfaces:

External

Connects the Firebox to an external Internet service provider (ISP). To configure the external interfaces, see [Configure external interfaces](#)

Trusted

Connects the Firebox to trusted computers that you want to secure. To configure trusted interfaces, see [About configuring the trusted network](#)

Optional

Connects the Firebox to 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 email server. To configure the optional interfaces see [About configuring the optional network](#)

Change the Firebox IP addresses with the Network Setup Wizard

The easiest method to change the network IP addresses of the Firebox X Edge e-Series 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, click **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

Select the procedure your ISP uses to set your IP address. For detailed information, see [About configuring external interfaces](#). You can choose one of these configurations:

DHCP: If your ISP uses DHCP, type the DHCP information that your ISP gave you. For more information, see [If your ISP uses DHCP](#).

PPPoE: If your ISP uses PPPoE, type the PPPoE information that your ISP gave you. For more information, see [If your ISP uses PPPoE](#).

Static IP: 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 addresses](#).

Configure the trusted interface of the Firebox

On this screen, type the IP address of the trusted interface. For more information, see [About configuring the trusted network](#).

After you configure the trusted interface, the Network Setup Wizard is complete.

Configure external interfaces

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

When you configure the external network, set the method your Internet service provider (ISP) uses to give you an IP address for your Firebox. If you do not know the method, get the information from your ISP or corporate network administrator. For information about IP addressing methods, see [Static and dynamic IP addresses](#).

You can also configure your primary external interface as a [wireless interface](#).

If your ISP uses DHCP

In the default configuration, the Firebox X Edge e-Series gets 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 relay agents](#).

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 Firebox X 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 **Release** if you want to give up the current DHCP-assigned IP address for the Edge. Click **Renew** to request a new DHCP-assigned IP address for the Edge from your DHCP server.
6. Click **Submit**.

If your ISP uses static IP addresses

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

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

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

WAN1	
	Settings
Configuration Mode	Manual Configuration
IP Address	192.168.54.63
Subnet Mask	255.255.255.0
Default Gateway	192.168.54.254
Primary DNS	192.168.130.131
Secondary DNS	[optional]
DNS Domain Suffix	[optional]

3. From the **Configuration Mode** drop-down list, select **Manual Configuration**.
4. Enter the IP address information provided by your ISP.
5. Click **Submit**.

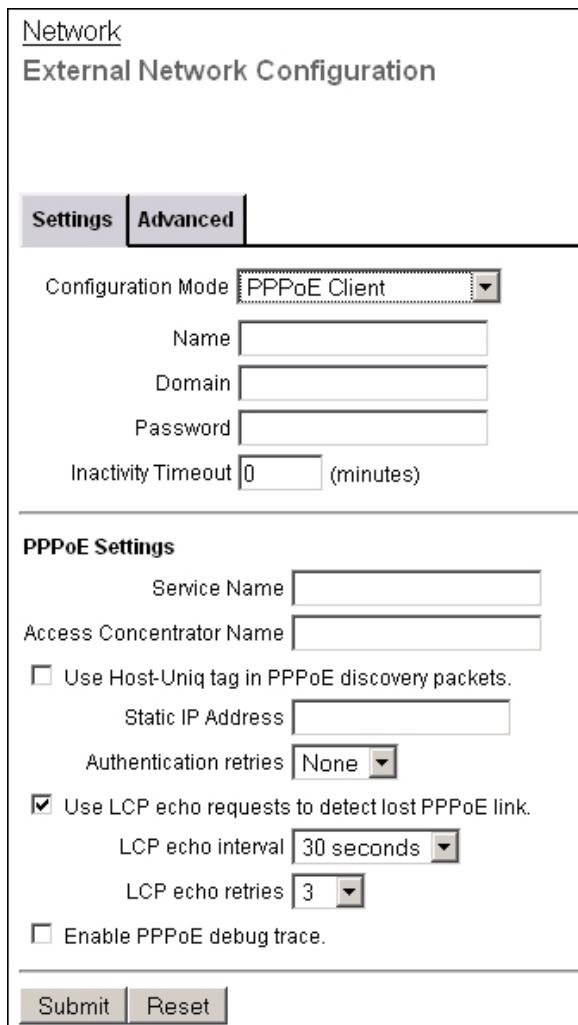
If your ISP uses PPPoE

If your ISP uses PPPoE, you must enter the PPPoE information into your Firebox X Edge before it can send traffic through the external interface. For more information in PPPoE, see [Advanced PPPoE settings](#).

To set your Firebox to use PPPoE on the external interface:

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

The External Network Configuration page appears.



The screenshot shows the 'External Network Configuration' page under the 'Network' tab. The 'Settings' tab is selected. The 'Configuration Mode' dropdown is set to 'PPPoE Client'. The 'Name' and 'Domain' fields are empty. The 'Password' field contains a password. The 'Inactivity Timeout' field is set to 0 minutes. Below this, the 'PPPoE Settings' section is expanded, showing fields for 'Service Name' and 'Access Concentrator Name', both empty. There are checkboxes for 'Use Host-Uniq tag in PPPoE discovery packets.' (unchecked), 'Use LCP echo requests to detect lost PPPoE link.' (checked), and 'Enable PPPoE debug trace.' (unchecked). The 'Static IP Address' field is empty. The 'Authentication retries' dropdown is set to 'None'. The 'LCP echo interval' dropdown is set to '30 seconds'. The 'LCP echo retries' dropdown is set to '3'. At the bottom are 'Submit' and 'Reset' buttons.

3. From the **Configuration Mode** drop-down list, select **PPPoE Client**.
4. 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 that use 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.
5. In the **Inactivity Time-out** field, type the number of minutes before the Firebox X Edge disconnects the active PPPoE connections. We recommend a value of 20. If you set this value to 0, no timeout will occur.
6. Click **Submit**.

Advanced PPPoE settings

The Quick Setup Wizard allows you to set up basic PPPoE settings. If necessary, you can also configure more advanced settings. Click **Submit** when you have completed the configuration of the Advanced PPPoE settings.

Service Name

Use this field to add a service name. The Firebox X Edge starts a session only with a PPPoE server, known as an access concentrator, that supports the specified service. Usually, this option is not used. Use this field 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 an access concentrator. The Firebox X Edge starts a session only with the access concentrator you identify in this field. Usually, this option is not 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 Firebox X Edge feature; this option is included to make the Edge compatible with ISPs that have this requirement.

Static IP Address

Use this field to specify a static PPPoE address. If you specify a static PPPoE address it is not necessary to specify a default gateway. The Edge gets the default gateway address from the PPPoE server.

Authentication retries

This field controls the number of times the Firebox X 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 select this check box, the Firebox X 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 Firebox X 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 Firebox X 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.

Enable PPPoE debug trace

WatchGuard Technical Support uses this check box to troubleshoot PPPoE problems. With this option on, the Firebox X 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.

Configure your external interface as a wireless interface

You can configure your primary external interface (WAN1) for your Edge as a wireless interface.

1. To connect to the System Status page, type `https://` in the browser address bar, followed by the IP address of the Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`
2. From the navigation bar, select **Network > External**. Click the **Wireless** tab.
The External Network Configuration page, Wireless tab appears

WAN1

Settings Advanced Wireless

Enable wireless as an external interface

SSID: WIRELESS_00841

Auth Type: WPA ONLY (PSK)

Encryption Type: Auto

Passphrase: 14cce4f8a14bf155

[Learn more about wireless connectivity.](#)

Submit Reset

3. Select the **Enable wireless as an external interface** check box.
4. In the **SSID** text box, type a unique name for your Edge wireless external network.
5. From the **AuthType** drop-down list, select the type of authentication to enable for wireless connections. We recommend that you use WPA2 if the wireless devices in your network can support WPA2. For more information about wireless authentication methods, see [About wireless security settings](#).
6. From the **Encryption Type** drop-down list, select the type of encryption to use for the wireless connection and add the keys or passwords required for the type of encryption you select. If you select an encryption option with pre-shared keys, a random pre-shared key is generated for you. You can use this key, or type your own.
7. Click **Submit** to save your changes to the Firebox.



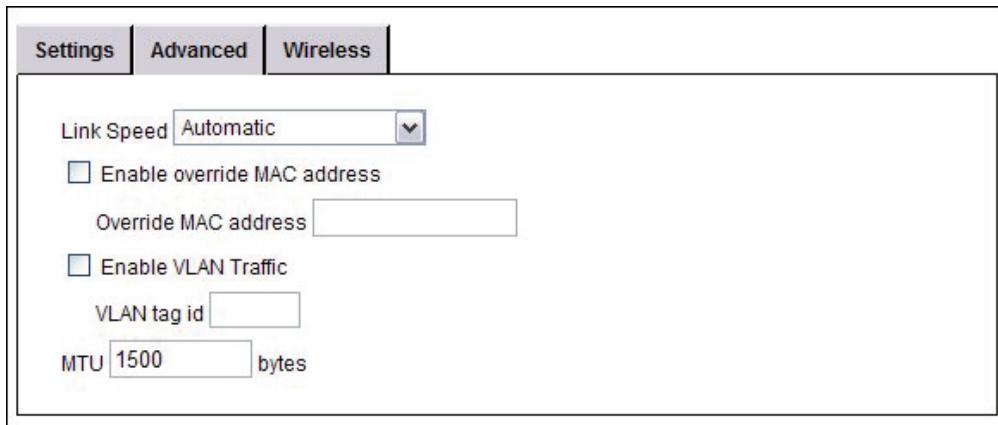
When the external interface is configured with a wireless connection, the Edge can no longer be used as a wireless access point. To provide wireless access for users, connect a wireless access point device to the Edge.

Using an Edge with a wireless external interface to extend network connectivity in areas with limited or no existing network infrastructure, you can use your Edge to provide secure network access. You must physically connect your network devices to the Edge. Then configure your external interface to connect to a wireless access point that connects to a larger network.

To create a wireless bridge and provide additional security, add a BOVPN tunnel between your Edge and the external gateway. You must set the mode to **Aggressive Mode** in the Phase 1 settings of your BOVPN configuration on both devices.

About advanced external network settings

On the **Network > External** configuration page, select the **Advanced** tab to change the settings for link speed or change the MAC address for the Edge's external interface.



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.

From the **Maximum Transmission Unit (MTU)** value control, select the maximum packet size, in bytes, that can be sent through the interface. We recommend that you use the default, 1500 bytes, unless your network equipment requires a different packet size.

Change 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 Firebox X Edge
- You cannot set the MAC address to 000000000000 or ffffffffffffff.

To change the MAC address of the external interface:

1. Connect to the System Status page. Type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`.
2. From the navigation bar, click **Network > External**.
The External Network Configuration page appears.
3. On the **Advanced** tab, select the **Enable override MAC address** check box.
4. In the **Override MAC address** text box, type the new MAC address for the Firebox X Edge external network.
You must enter the MAC address as a hexadecimal number.
Do not use extra characters, such as spaces or hyphens.
5. Click **Submit**.
You must restart the Firebox to see the changes.

If the **Override MAC address** field is cleared and the Firebox X Edge is restarted, the Firebox X Edge uses the default 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 that uses the same MAC address, the Firebox changes back to the standard MAC address for the external interface and starts again.

About 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 e-Series 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 X Edge 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 Edge can give an IP address from 192.168.111.2 to 192.168.111.254. These are private addresses that are not seen outside the trusted network. The factory default settings use the same DNS server information on the internal and external interfaces.

If necessary, you can disable the DHCP server. Or, you can use the Edge 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**. If necessary, the Firebox restarts.

About 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 X Edge devices in a virtual private network, each Edge must use a different trusted network address. If the two sides of the VPN use the same trusted network IP addresses, one side must change the trusted network IP address range so that it is different from the other side. For more information, see [What you need to create a VPN](#).



If you change the IP address of the Firebox X Edge 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, if you change the Firebox X Edge trusted interface IP address from the default 192.168.111.1 to 10.0.0.1, then you must use https://10.0.0.1 to connect to the Firebox X Edge. Your computer's IP address must also be changed so that it is in the new trusted network IP subnet range.

Change the IP address of the trusted network

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 Firebox X 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.

IP Address	192.168.63.1
Subnet Mask	255.255.255.0
<input checked="" type="checkbox"/> Enable DHCP Server on Trusted Network	
First address for DHCP server	192.168.63.2
Last address for DHCP server	192.168.63.254
DHCP Reservations...	
DHCP Lease Duration	0 days 1 hours 0 minutes
WINS Server Address	
DNS Server Address	
Secondary DNS Server Address	
DNS Domain Suffix	
MTU	1500 bytes
<input type="checkbox"/> Enable DHCP Relay	
DHCP relay server	
<input type="checkbox"/> Enable VLAN Traffic	
VLAN tag id	

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.

Enable DHCP server on the trusted network

The DHCP Server option allows the Firebox X Edge e-Series to give IP addresses to the computers on the trusted network. When the Edge receives a DHCP request from a computer on the trusted network, it gives the computer an IP address. By default, the DHCP Server option for the trusted interface is 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. Use the **Days/Hours/Minutes** value control boxes to set the length of time for each DHCP lease the Edge gives.
5. 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 X Edge uses the same values as those used for the external network.
6. Click **Submit**.

Set 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 X Edge 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.

IP Address	MAC Address

Trusted Network IP Address 192.168.111.1
Trusted Network Subnet Mask 255.255.255.0
DHCP Address Pool 192.168.111.2-192.168.111.254

DHCP Address Reservations

IP Address MAC Address

Add

Submit Reset

3. Type a static IP address in the IP Address text box. The IP address must be on the trusted network but outside the DHCP Address pool.

For example, if the trusted network starts with 192.168.111.1, and the DHCP address pool is 192.168.111.2-192.168.111.200, you can enter any address from 192.168.111.201 to 192.168.111.254.

4. Type the MAC address of the computer on the trusted network in the **MAC Address** text box. You must enter the MAC address as 12 hexadecimal digits with no space, dash, or semicolon characters.

*Click **Add**.*

5. Click **Submit**.

About DHCP relay agents

One way to get IP addresses for the computers on the trusted or optional networks is to use a DHCP server on a different network.

The Firebox can send a DHCP request from a DHCP client to a DHCP server at a different location through a VPN tunnel. It gives the reply to computers on the trusted or 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.

You must set up a VPN tunnel between the Edge and the DHCP server for this feature to operate correctly.

Make the Firebox a DHCP relay agent for the trusted interface

To configure the Firebox X Edge 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.

Settings	Allowed MAC Addresses
IP Address	192.168.63.1
Subnet Mask	255.255.255.0
<input checked="" type="checkbox"/> Enable DHCP Server on Trusted Network	
First address for DHCP server	192.168.63.2
Last address for DHCP server	192.168.63.254
DHCP Reservations...	
DHCP Lease Duration	0 days 1 hours 0 minutes
WINS Server Address	
DNS Server Address	
Secondary DNS Server Address	
DNS Domain Suffix	
MTU	1500 bytes
<input type="checkbox"/> Enable DHCP Relay	
DHCP relay server	
<input type="checkbox"/> Enable VLAN Traffic	
VLAN tag id	

2. Select the **Enable DHCP Relay** check box.
3. Type the IP address of the DHCP server in the adjacent text box.
4. Click **Submit**. You must restart the Firebox X Edge for new configuration to start.



If the Firebox X Edge 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.

Use 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 Firebox X 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 Edge trusted interface. Computers on the trusted network with static IP addresses must use the Edge trusted interface IP address for the default gateway. If a computer does not use the Edge as the default gateway, it usually cannot get to the external network or the Internet.

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

Allow wireless connections to the trusted interface

The Firebox X Edge e-Series Wireless can be configured as a wireless access point with three different security zones. You can enable wireless devices to connect to the Edge Wireless as part of the trusted network or part of the optional network. You can also enable a wireless guest services network for Edge users. When you allow wireless connections through the Edge trusted interface, those wireless devices have full access to all computers on the trusted and optional networks, and full Internet access according to the rules you have configured for outgoing access on your Edge.

If you enable wireless access through the trusted interface, we strongly recommend that you enable and use the MAC restriction feature described in the next section to allow access through the Edge only for devices that have been added to the **Allowed MAC Address** list.

To configure the Edge to allow wireless connections through the trusted interface, see [Allow wireless connections to the trusted network](#).

About restricting access to an interface by MAC address

You can control access to a Firebox X Edge e-Series interface by computer hardware (MAC) address. If this feature is enabled, and the MAC address of a computer that tries to connect to the Edge network is not included in this configuration, the connection fails. If you choose to restrict access to the Edge by MAC address, make sure that you include the MAC address for the computer you use to administer the Edge.

Restrict access to the trusted interface by MAC address

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`
2. From the navigation bar, select **Network > Trusted** and click the **Allowed MAC Addresses** tab.

Network

Trusted Network Configuration

Settings **Wireless** **Allowed MAC Addresses**

Restrict access by Hardware MAC Address

The Edge allows traffic only from computers with these hardware addresses:

Hardware Address	Name	
		<input type="button" value="Scan..."/>
		<input type="button" value="Add..."/>
		<input type="button" value="Edit..."/>
		<input type="button" value="Remove"/>

Try to resolve Windows host names during scan

Log attempted access from MAC addresses not in the list

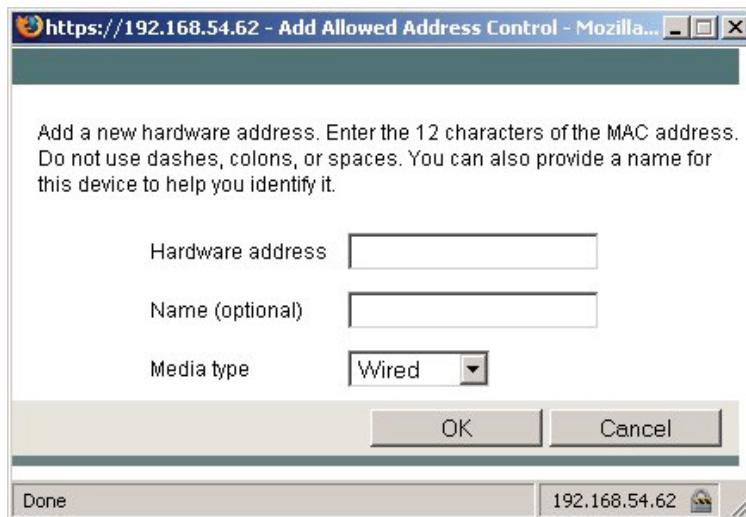
Learn more about [restricting network access with MAC addresses](#).

3. Select the **Restrict Access by Hardware MAC Address** check box.
4. Click **Scan** to have the Edge find all known hardware addresses on the network. If you want the Edge to try to resolve host names for all Windows computers it finds during the scan process, make sure the **Try to resolve Windows host names during scan** check box is selected. This can make the scan procedure take more time.

The Scan Allowed Address Control dialog box appears.
5. Select one or more devices that you want to add to your list of allowed MAC addresses for this interface. Make sure that the Media Type is identified and is correct, because a computer with more than one NIC card can have more than one MAC address. Click **OK** to add the device or devices to your list of allowed MAC addresses.

Press and hold the CTRL key to select more than one device. You can select from more than one column at the same time.

6. To manually add a hardware address and its host name to your configuration, click **Add**.
The Add Allowed Address Control dialog box appears.



7. Select the **Log attempted access from MAC addresses not in the list** check box if you want the Edge to generate a log message each time a computer whose hardware address is not in the list tries to get access to the Edge.
8. Click **Submit**

Find the MAC address of a computer

A MAC address is also known as a hardware address or an Ethernet address. It is a unique identifier specific to the network card in the computer. A MAC address is usually shown in this form: XX-XX-XX-XX-XX-XX, where each X is a digit or letter from A to F. To find the MAC address of a computer on your network:

1. From the command line of the computer whose MAC address you want to find, type `ipconfig /all` (Windows) or `ifconfig` (OS X or Linux).
2. Look for the entry for the computer's physical address. This value is the MAC or hardware address for the computer.

About configuring the optional network

The optional network is an isolated network for less secure public resources. By default, a Firebox X Edge does not allow traffic from the optional network to get to the trusted network. The factory default settings allow traffic that starts from the trusted network to get to the optional network, but you can restrict that traffic. For more information, see [About policies for the optional network](#).

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, email, or FTP server. We recommend you isolate your private network from these servers because the public can connect to them. The network you create for these public servers, separate from your private network, is sometimes called a DMZ (de-militarized zone). If a server on the optional network is attacked from the Internet, the attacker cannot use it to 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 Firebox X Edge 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 also can change the IP address range of the optional network.

Enable 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 Firebox X 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.

Settings	Allowed MAC Addresses
<input type="checkbox"/> Enable Optional Network	
IP Address <input type="text" value="192.168.112.1"/>	
Subnet Mask <input type="text" value="255.255.255.0"/>	
MTU <input type="text" value="1500"/> bytes	
<input type="checkbox"/> Enable DHCP Server on Optional Network	
First address for DHCP server <input type="text"/>	
Last address for DHCP server <input type="text"/>	
DHCP Reservations...	
DHCP Lease Duration <input type="text" value="0"/> days <input type="text" value="1"/> hours <input type="text" value="0"/> minutes	
WINS Server Address <input type="text"/>	
DNS Server Address <input type="text"/>	
Secondary DNS Server Address <input type="text"/>	
DNS Domain Suffix <input type="text"/>	
<input type="checkbox"/> Enable DHCP Relay on Optional Network	
DHCP relay server <input type="text"/>	
Link Speed <input type="text" value="Automatic"/> <input type="button" value="▼"/>	
<input type="checkbox"/> Enable VLAN Traffic	
VLAN tag id <input type="text"/>	
Submit Reset	

3. Select the **Enable Optional Network** check box. 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. The IP address of the optional network cannot be on the same subnet as the trusted network.
4. Click **Submit**.

Enable DHCP server 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 Edge receives a DHCP request from a computer on the optional network, it gives the computer an IP address. By default, the Edge 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 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. Use the **Days/Hours/Minutes** value control boxes to set the length of time for each DHCP lease the Edge gives.
5. 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 X Edge uses the same values as those used for the external network.
6. Click **Submit**.

Set optional network DHCP address reservations

You can manually assign an IP address to a specified computer on your optional network. The Firebox X Edge 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.

IP Address	MAC Address

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 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**.

About DHCP relay agents

One way to get IP addresses for the computers on the trusted or optional networks is to use a DHCP server on a different network.

The Firebox can send a DHCP request from a DHCP client to a DHCP server at a different location through a VPN tunnel. It gives the reply to computers on the trusted or 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.

You must set up a VPN tunnel between the Edge and the DHCP server for this feature to operate correctly.

Make the Firebox a DHCP relay agent for the optional interface

To configure the Firebox X Edge 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 adjacent text box.
4. Click **Submit**. You must restart the Firebox X Edge for the new configuration to activate.



If the Firebox X Edge 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.

Use 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 also can 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 Firebox X 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. If a computer does not use the Edge for the default gateway, it usually cannot get to the external network or the Internet.

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

Add computers to the optional network

You can directly connect only one computer to the Firebox X Edge e-Series 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 [Set your computer to connect to the Edge](#).
3. Connect each computer to the network. For more information, see [Connect the Edge to more than four devices](#).
4. Restart each computer.

Allow wireless connections to the optional interface

The Firebox X Edge e-Series Wireless can be configured as a wireless access point with three different security zones. You can enable wireless devices to connect to the Edge Wireless as part of the trusted network or part of the optional network. You can also enable a wireless guest services network for Edge users. When you allow wireless connections through the Edge optional interface, those wireless devices have full access to all computers on the optional network, and full Internet access according to the rules you have configured for outgoing access on your Edge.

To configure the Edge to allow wireless connections through the optional interface, see [Allow wireless connections to the optional interface](#).

About restricting access to an interface by MAC address

You can control access to a Firebox X Edge e-Series interface by computer hardware (MAC) address. If this feature is enabled, and the MAC address of a computer that tries to connect to the Edge network is not included in this configuration, the connection fails. If you choose to restrict access to the Edge by MAC address, make sure that you include the MAC address for the computer you use to administer the Edge.

Restrict access to the optional interface by MAC address

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`
2. From the navigation bar, select **Network > Optional** and click the **Allowed MAC Addresses** tab.
3. Select the **Restrict Access by Hardware MAC Address** check box.
4. Click **Scan** to have the Edge find all known hardware addresses on the network. If you want the Edge to try to resolve host names for all Windows computers it finds during the scan process, make sure the **Try to resolve Windows host names during scan** check box is selected. This can make the scan procedure take more time.
5. Select one or more devices that you want to add to your list of allowed MAC addresses for this interface. Press and hold the CTRL key to select more than one device. You can select from more than one column at the same time. Click **OK** to add the device or devices to your list of allowed MAC addresses.
6. To manually add a hardware address and its host name to your configuration, click **Add**.
7. Select the **Log attempted access from MAC addresses not in the list** check box if you want the Edge to generate a log message each time a computer whose hardware address is not in the list tries to get access to the Edge.
8. Click **Submit**.

About static routes

A *route* is the sequence of devices through which network traffic must go to get from its source to its destination. A *router* is the device in a route that finds the subsequent network point through which to send the network traffic to its destination. Each router is connected to a minimum of two networks. A packet can go through a number of network points with routers before it gets to its destination.

The Firebox lets you create *static routes* to send traffic to specific hosts or networks. The router can then send the traffic to the correct destination from the specified route. If you do not add a route to a remote network, all traffic to that network is sent to the Firebox default gateway.

The [WatchGuard User Forum](#) is a good source of data about network routes and routers.

Add 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 Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1
2. From the navigation bar, select **Network > Routes**.
The Routes page appears.

Address	Gateway	
Host	192.168.110.0	192.168.111.1

Add...

Remove

3. Click **Add**.

The Add Route page appears.

Network > Routes

Add Route

Type	Host
Address	192.168.110.0
Gateway	192.168.111.1

Submit Reset Cancel

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

Select **Network** if you have a full network behind a router on your local network. Select **Host** if only one host is behind the router or you want traffic to go to only one host.

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 X Edge trusted, optional, or external network range.

6. Click **Submit**.

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

About the Dynamic DNS service

You can register the external IP address of the Firebox 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 a new IP address. The Firebox gets the IP address of members.dyndns.org when it starts up. It makes sure the IP address is correct every time it restarts and at an interval of every twenty days. If you make any changes to your DynDNS configuration on the Firebox or if you change the IP address of the default gateway configured for your Firebox, it updates DynDNS.com immediately.

For more information on dynamic DNS, go to <http://www.dyndns.com>



WatchGuard is not affiliated with DynDNS.com.

Create a DynDNS account

To set up your account, go to the DynDNS web site: <http://www.dyndns.com>

Use the instructions on this web site to activate your account. You must do this before you configure the Firebox for dynamic DNS.

Set up the Firebox X Edge 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 Firebox X 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

Enable Dynamic DNS client

Domain

Name

Password

System

Options

[Learn more about Dynamic DNS.](#)

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.
For an explanation of each option, see <http://www.dyndns.com/services/>.
 - The option dyndns sends updates for a Dynamic DNS host name. Use the dyndns option when you have no control over your IP address (for example, it is not static, and it changes on a regular basis).

- The option statdns sends updates for a Static DNS host name. A Static DNS host is a dynamically acquired IP address that does not change (for example, it is associated with a MAC address, DHCP host ID, or PPPoE static IP address/login).
- The option custom sends updates for a custom DNS host name. This option is frequently used by businesses that pay to register their domain with dyndns.com.

6. In the **Options** field, you can type these options. You can use one option, or use several options together as shown in the example below:
 For more information, see <http://www.dyndns.com/developers/specs/syntax.html>.

- mx=mailexchanger& specifies a Mail eXchanger for use with the hostname.
- backmx=YES | NO& requests that the MX in the previous parameter be set up as a backup MX by including the host as an MX with a lower preference value.
- wildcard=ON | OFF | NOCHG& enables or disables wildcards for this host (ON to enable).
- offline=YES | NO sets the hostname to offline mode. One or more options can be chained together with the ampersand character like this:
`&mx=backup .kunstlerandsons .com&backmx=YES&wildcard=ON`

7. Click **Submit**.



The Firebox X Edge does not operate with other Dynamic DNS services, only DynDNS.com.

Configure the Firebox to use BIDS

Telstra customers in Australia must use client software to connect to the BigPond network. The Firebox X Edge e-Series uses BIDS to make this connection. If you do not connect to the BigPond network, it is not necessary to use BIDS.

To configure your Firebox to connect to the BigPond network using BIDS:

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

<p>Network BIDS</p> <p>BIDS should only be used if you are attempting to connect via Telstra BigPond Australia. <i>For more information, please visit www.bigpond.com.</i></p> <p><input type="checkbox"/> Enable (WAN1)</p> <p>User Name <input type="text"/></p> <p>Password <input type="password"/></p> <p style="text-align: center;">Submit Reset</p>
--

3. To enable BIDS, select the **Enable (WAN1)** check box.
4. Type your login information in the **User Name** and **Password** text boxes.
5. Click **Submit**.

About using multiple external interfaces

With the Firebox, you can have redundant support for the external interface. Companies use this option if they must have a constant Internet connection.

If you have an Edge Pro license for your Firebox X Edge and have a second Internet connection, you can configure a second external interface on the Edge. If you have a second broadband connection, you can choose to configure the Edge in a WAN failover configuration or a round-robin load balancing configuration. If your second Internet connection is a serial-based modem with a dial-up Internet connection, you must use a WAN failover configuration.

To purchase an Edge Pro upgrade for your Firebox X Edge, contact your reseller or go to the WatchGuard online store:

<https://www.watchguard.com/store>

It is not necessary to configure new policies when you use a second external interface. The second interface uses the same policies and network properties as the primary external interface.

Multiple WAN configuration options

If you have Edge Pro appliance software for your Firebox X Edge e-Series, you can [configure a second external interface](#) for your Edge. You can choose from two configuration options to control how the Edge routes traffic through the second external interface.

WAN Failover

When you [configure the Edge for WAN failover](#), the Edge sends all traffic through the primary external interface. If the primary interface is not active, the Edge sends all traffic through the secondary external interface. The Firebox X Edge e-Series uses two procedures to see whether 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 X Edge sends a ping to the default gateway or a computer specified by the administrator. If there is no reply, the Edge changes to the secondary external network interface (WAN2).

When you enable the WAN Failover feature, the Firebox X Edge e-Series does this:

- If the WAN1 interface connection stops, the Edge starts to use the WAN2 interface.
- If the WAN2 interface connection stops, the Edge starts to use the WAN1 interface.
- If the WAN1 interface and the WAN2 interface stop, the Edge tries the two interfaces until it makes a connection.

When the WAN2 interface is in use, the Firebox X Edge monitors the primary (WAN1) interface. When the WAN1 interface becomes available, the Edge automatically goes back to using the WAN1 interface.

Multi-WAN load balancing

When you [configure the Edge to use multi-WAN in round-robin load balancing](#), the Edge looks at its internal routing table to check for a specific route for each connection. If no specified route is found, the Edge distributes the traffic load between its two external interfaces. If you select **Weighted Round Robin load balancing**, you can use the slider to set the percentage of traffic you want to go through each interface.

When you configure the Edge for multi-WAN round robin load balancing, the Edge continues to monitor the status of each interface. If an interface goes down, the Edge sends all traffic through the other interface.

About multiple external interfaces and DNS

When you configure more than one external interface on your Edge, it is a good idea to enter two DNS server addresses when you configure DHCP settings for the trusted and optional networks. Some ISPs allow queries to their DNS servers only if the query comes from that ISP network. If you leave the DNS server information blank in the trusted network DHCP settings, the Edge continues to use the WAN1 DNS server after it fails over to WAN2. If the WAN2 ISP does not allow that DNS server, WAN failover does not work. To correct this, enter the DNS server address for the WAN1 ISP as the primary address. Enter the DNS server address for the WAN2 ISP as the secondary address. When the Edge fails over from WAN1 to WAN2, the Edge queries the DNS server used by the ISP on WAN1. If it is refused, the Edge uses the secondary DNS server.

Configure a second external interface for a broadband connection

1. If you use a static connection to the Internet, select **Manual Configuration** from the **Configuration Mode** drop-down list.
- If you use DHCP to connect to the external network, select **DHCP Client** from the **Configuration Mode** drop-down list.
- If you use PPPoE to connect to the Internet, select **PPPoE Client** from the **Configuration Mode** drop-down list.

Ethernet (WAN2) Configuration

Settings **Advanced**

Configuration Mode: **Manual Configuration**

IP Address: 0.0.0.0

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Primary DNS server: []

Secondary DNS server: [] [optional]

DNS Domain suffix: [] [optional]

Submit **Reset**

2. Add the information required for the type of connection you use. For more information, see [If your ISP uses DHCP](#), [If your ISP uses static IP addresses](#), or [If your ISP uses PPPoE](#).
3. Click **Submit**.

Configure advanced WAN2 settings

You can configure additional settings for your second WAN interface (WAN2) on the **Advanced** tab below WAN 2.

1. From the **Link Speed** drop-down list, select **Automatic** if you want the Edge to select the best network speed. You can also select one of the half-duplex or full-duplex speeds that you know is compatible with your equipment. We strongly recommend that you do not change this setting unless instructed to by Technical Support. When you set the link speed manually, this can cause a conflict with the NIC device during failback that does not allow WAN1 to reconnect.
2. From the **Maximum Transmission Unit (MTU)** value control, select the maximum packet size, in bytes, that can be sent through the interface. We recommend that you use the default, 1500 bytes, unless your network equipment requires a different packet size.
3. To override the MAC address, select the **Enable override MAC address** check box, and then enter the new MAC address in the **Override MAC address** field.

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:

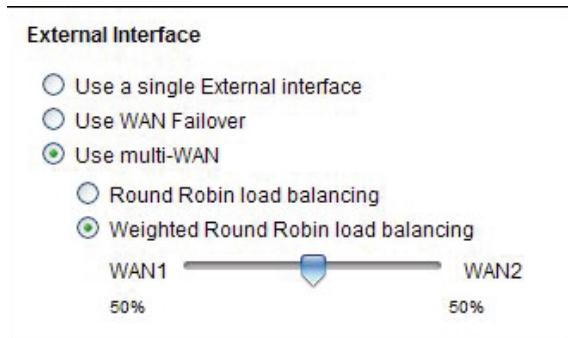
- It must use 12 hexadecimal characters. Hexadecimal characters have a value between 0 and 9 or between a and f.
- It must operate with:
 - One or more addresses on the external network
 - The MAC address of the trusted network for the Firebox X Edge
 - The MAC address of the optional network for the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

The screenshot shows the WAN2 configuration interface. At the top, there are two tabs: "Settings" and "Advanced", with "Advanced" being the active tab. Below the tabs, there are four configuration fields:

- "Link Speed" dropdown set to "Automatic".
- "Enable override MAC address" checkbox, which is currently unchecked.
- "Override MAC address" text input field, which is currently empty.
- "MTU" dropdown set to "1500 bytes".

Configure the Edge to use round-robin load balancing

1. From the navigation bar, select **Network > External**. If you have an Edge Pro license, you see the options to configure your Edge with a multi-WAN configuration.
2. Select the **Use multi-WAN** check box.



3. Select the method you want the Edge to use to route traffic between the two external interfaces. If you select **Round Robin load balancing**, the Edge tries to balance traffic between the two interfaces equally. If you select **Weighted Round Robin load balancing**, you can use the slider to set the percentage of traffic you want to go through each interface.
4. Configure the second external interface as described in [Configure a second external interface for a broadband connection](#).
5. Below **Multi-WAN settings**, type the IP addresses of the hosts to ping for the WAN1 (external) and WAN2 (failover) interfaces. The Firebox X Edge sends pings to the IP addresses you type here. If pings to the host on that network are not successful, the Edge fails over to the other WAN. You control the frequency of pings in the fields below.
6. Type the number of seconds between pings and the number of seconds to wait for a reply.
7. Type the maximum number of pings before timeout in the **No Reply Limit** field.
8. Type the number of successful pings that must be made before the Firebox X Edge uses the WAN1 interface again in the **Ping replies needed for failback** field.

Multi-WAN Settings	
Host to ping on the External Network	192.168.54.254
Host to ping on the Failover Network	192.168.54.254
Ping interval	60 (seconds)
Reply timeout	5 (seconds)
No reply limit	5
Ping replies needed for failback	1
Learn more about Multi-WAN.	

Configure WAN failover

If you have an Edge Pro license, you can configure your Firebox X Edge with a WAN failover configuration and use a second external interface connected to a broadband Internet connection. To configure the WAN failover network:

1. Connect one end of an 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 Firebox X 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 > External configuration page](#).

Enable WAN failover with the 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. Use 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 Firebox X Edge uses.

Configure the broadband or modem interface

Use the screens to configure the secondary interface.

Identify the computers to connect

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

The WAN Failover Setup Wizard is complete

You must restart your Firebox X Edge to activate the WAN Failover feature.

Use the failover settings to specify what computer IP addresses you want the Edge to ping to determine if its WAN interfaces are active or not.

1. From the navigation bar, select **Network > External**. If you have an Edge Pro license, you see the failover settings near the bottom of the page.

Failover Settings

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

Host to ping on the External Network:

Host to ping on the Failover Network:

Ping interval: 60 (seconds)

Reply timeout: 5 (seconds)

No reply limit: 5

Ping replies needed for failback: 1

[Learn more about WAN failover.](#)

2. Select the **Enable failover using the Ethernet (WAN2) interface** check box.

3. Type the IP addresses of the hosts to ping for the WAN1 (external) and WAN2 (failover) interfaces. The Firebox X Edge will send pings to the IP addresses you type here. If pings to the host on that network are not successful, the Edge starts the failover. You control the frequency of pings in the fields below.
4. Type the number of seconds between pings and the number of seconds to wait for a reply.
5. Type the maximum number of pings before timeout in the **No Reply Limit** field.
6. Type the number of successful pings that must be made before the Firebox X Edge uses the WAN1 interface again in the **Ping replies needed for failback** field.

Configure the Edge for serial modem failover

Enable serial modem failover

1. From the navigation bar, select **Network > External**. If you have an Edge Pro license, you see the options to configure your Edge with a multi-WAN configuration.
2. Select the **Use WAN Failover** check box.

External Interface

Use a single External interface
 Use WAN Failover
 Use multi-WAN

Round Robin load balancing
 Weighted Round Robin load balancing

WAN1  WAN2
 50% 50%

3. After you configure WAN 1, from the **Failover to this interface** drop-down list, select **Modem**.
4. Complete the Modem (Serial Port) Configuration settings as described in the topics in this section.
5. The Edge sends regular pings to an IP address you specify to check for interface connectivity. Below **Failover Settings**, type the IP addresses you want the Edge to ping for the WAN1 (external) and WAN2 (failover) interfaces in the correct fields.

Failover Settings

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 failback

6. In the **Ping interval** text box, type the frequency at which you want the Firebox to send pings to check for interface connectivity.
7. In the **Reply timeout** text box, type the number of seconds you want the Edge to wait for a reply. If there is no response before this timeout occurs, the ping fails.
8. In the **No reply limit** text box, type the number of failed pings before timeout occurs. When this limit is reached, WAN failover occurs.
9. In the **Ping replies needed for failback** text box, type the number of successful pings that must be made before the Edge uses the WAN1 interface again.

Configure your modem for WAN failover

Use the settings available in the **Modem (Serial Port) Configuration** area of the **Network > External** page to set up your external modem for failover. The Edge has been tested with 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

Enter your dial-up account settings

1. In the **Telephone** number text box, type the telephone number of your ISP. If you have an alternate telephone number, you can enter that below the telephone number.
2. In the **Account name** text box, type your dial-up account name.
3. If you log in to your account with a domain name (such as msn.com), enter it in **Account Domain** text box.
4. In the **Account password** text box, type the password you use to connect to your dial-up account.
5. Select the **Enable modem and PPP debug trace** check box only if you have problems with your connection. When this option is selected, the Edge sends detailed logs for the serial modem failover feature to the event log file.

Modem (serial port) Configuration			
Account	DNS	Dial Up	
Dial Up Account Settings			
Telephone number	<input type="text"/>		
Alternate telephone number	<input type="text"/> [optional]		
Account name	<input type="text"/>		
Account domain	<input type="text"/> [optional]		
Account password	<input type="text"/>		
<input type="checkbox"/> Enable modem and PPP debug trace			
<input type="button" value="Submit"/> <input type="button" value="Reset"/>			

6. Click **Submit**, or select a different tab to change more settings.

Enter your 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 a DNS server to use after failover occurs.

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 its IP address in the **Secondary DNS server** text box.

Modem (Serial Port) Configuration

Account DNS Dial Up

DNS Settings

Manually configure DNS server IP addresses

Primary DNS server

Secondary DNS server [optional]

MTU 1500 bytes

3. If necessary, change the **MTU** setting. Most users do not have to change this setting.
4. Click **Submit**, or select a different tab to change more settings.

Enter your dial-up configuration settings

1. In the **Dial up timeout** text box, type the number of seconds before a timeout occurs if your modem does not connect.
2. In the **Redial attempts** text box, type the number of times the Edge tries to redial if your modem does not connect.
3. In the **Inactivity Timeout** text box, type the number of minutes to wait if no traffic goes through the modem before a timeout occurs.
4. Use the **Speaker volume** control to set your modem speaker volume.

Modem (serial port) Configuration

Account DNS Dial Up

Dialing Options

Dial up time-out 2 (minutes)

Redial attempts 3

Inactivity Timeout 0 (minutes)

Speaker volume

Submit Reset

5. Click **Submit**, or select a different tab to change more settings.

About virtual local area networks (VLANs)

An 802.1Q VLAN (virtual local area network) is a collection of computers on a LAN or LANs that are grouped together independent of their physical location. When you create a VLAN, you create a new software-based network interface that you can use in your configurations.

You can use VLANs to:

- Group devices according to traffic patterns, instead of proximity
- Split your network into logical, hierarchical segments
- Control network traffic patterns
- Improve network performance and scalability

Since you can have more than one VLAN in your network, each switch in your network must be able to identify the VLAN associated with each network packet. A VLAN-capable switch inserts four bytes of data, called a tag, in the Ethernet header of packets that belong to a VLAN. Other switches on the network can use those tags to send packets to the correct destination.

If you have an Edge Pro license for your Firebox X Edge e-Series device, you can configure the Edge to insert VLAN tags for packets sent to a VLAN-capable switch over one or more network interfaces.

Add a VLAN tag to the External Interface

To mark traffic sent to the external interface on your Edge as part of a VLAN:

1. To connect to the System Status page, type `https://` in the browser address bar, followed by the IP address of the Firebox X 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. Click the **Advanced** tab.

The screenshot shows a configuration interface with the following settings:

- Link Speed:** Automatic
- Enable override MAC address:** Unchecked
- Override MAC address:** (Text input field)
- Enable VLAN Traffic:** Checked
- VLAN tag id:** 32
- MTU:** 1500 bytes

At the bottom are **Submit** and **Reset** buttons.

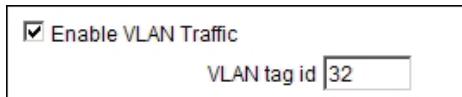
4. Select the **Enable VLAN Traffic** check box.
You must have an Edge Pro license to use the VLAN tag feature.
5. Type the ID of the VLAN you want to use in the **VLAN tag id** text box.
6. Click **Submit** to save your changes.

For more information about VLANs see [About virtual local area networks \(VLANs\)](#).

Add a VLAN tag to the Trusted or Optional Interface

To mark traffic sent to the trusted or optional interface on your Edge as part of a VLAN:

1. To connect to the System Status page, type `https://` in the browser address bar, followed by the IP address of the Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`.
2. From the navigation bar, select **Network > Trusted** or **Network > Optional**.
The Trusted or Optional Network Configuration page appears.
3. Select the **Enable VLAN Traffic** check box.
You must have an Edge Pro license to use the VLAN tag feature.



Enable VLAN Traffic
VLAN tag id

4. Type the ID of the VLAN you want to use in the **VLAN tag id** text box.
5. Click **Submit** to save your changes.

6

Wireless Setup

About wireless setup

The Firebox X Edge e-Series Wireless can be configured as a wireless access point with three different security zones. You can enable wireless devices to connect to the Edge Wireless as part of the trusted network or part of the optional network. You can also enable a wireless guest services network for Edge users. Computers that connect to the guest network connect through the Edge, but have no access to computers on the trusted or optional networks.

Before you begin

The Edge Wireless adheres to 802.11b and 802.11g guidelines set by the Institute of Electrical and Electronics Engineers (IEEE). When you install the Firebox X Edge e-Series Wireless:

- Make sure that the Firebox X Edge Wireless is installed in a location more than 20 centimeters from all persons. This is an FCC requirement for low power transmitters.
- It is a good idea to install the Edge Wireless away from other antennas or transmitters to decrease interference
- The default wireless authentication algorithm configured for each wireless security zone is not the most secure authentication algorithm. We recommend that you increase the authentication level to WPA2 if you can be sure that the wireless devices that will connect to your Edge can operate correctly with WPA2.
- A wireless client that connects to the Edge from the trusted or optional network can be a part of any Branch Office VPN tunnels in which the local network component of the Phase 2 settings includes optional or trusted network IP addresses. To control access to the VPN tunnel, you can force Firebox X Edge users to authenticate.

To configure wireless users as part of your trusted or optional network, use the instructions in this chapter. If you want to configure a wireless guest network, see [Enable a wireless guest network manually](#) or use the Wireless Guest Setup Wizard on the Wizards page.

About wireless configuration settings

When you enable wireless access to the trusted, optional, or wireless guest network, some configuration settings are common to all three security zones.

Settings	Wireless	Allowed MAC Addresses
<input checked="" type="checkbox"/> Enable wireless bridge to Trusted Network <input checked="" type="checkbox"/> Broadcast SSID and respond to SSID queries <input checked="" type="checkbox"/> Log Authentication Events Network name (SSID) <input type="text" value="TRUSTED_00019"/> Fragmentation Threshold <input type="text" value="2346"/> (256-2346 bytes) RTS Threshold <input type="text" value="2346"/> (256-2346 bytes) Authentication <input type="button" value="WPA ONLY (PSK) ▾"/> Encryption <input type="button" value="Auto ▾"/> Passphrase <input type="text" value="9be66ed5ada886a0"/> <input type="checkbox"/> Require encrypted MUVPN connections for wireless clients Learn more about wireless connectivity.		
<input type="button" value="Submit"/> <input type="button" value="Reset"/>		

Change 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 the computer must have the same SSID as the Firebox X Edge e-Series Wireless network the computer will connect to.

The Edge automatically assigns an SSID to each wireless network. This SSID uses a format that contains the interface name and the 5th-9th digits from the Edge serial number. To change the SSID of an Edge interface, type a new name in the SSID field to uniquely identify your wireless network.

Enable/disable SSID broadcasts

Computers with wireless network cards send requests to see whether there are wireless access points to which they can connect. To configure an Edge wireless interface to send and answer these requests, select the **Broadcast SSID and respond to SSID queries** check box. For security, turn this option on only while 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.

Log authentication events

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

Change the fragmentation threshold

The Firebox X Edge e-Series 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.

About the frame size

A collision happens when two devices that use the same medium transmit packets at exactly the same time. The two packets can corrupt each other, and the result is a group of unreadable pieces of data. If a packet results in a collision, the packet is discarded and it must be transmitted again. This adds to the overhead on the network and can reduce the throughput or speed of the network.

Larger frames are more likely to collide with each other than smaller frames. You can make the wireless packets smaller by lowering the fragmentation threshold on the Firebox X Edge. If you lower the maximum frame size, it can reduce the number of retransmissions caused by collisions, and lower the overhead caused by retransmissions. However, making frames smaller introduces a different kind of overhead.

Smaller frames introduce more overhead on the network too. This is especially true on a wireless network, because every fragmented frame sent from one wireless device to another wireless device requires the receiving device to acknowledge the frame. In times of high packet error rates (over five or ten percent collision or errors), lowering the fragmentation threshold can help improve performance of the wireless network. The time that is saved from reducing re-transmissions can be enough to offset the extra overhead added by using smaller packets. This can result in higher throughput.

If the rate of packet error is low and you lower the fragmentation threshold, wireless network performance will decrease. This is because lowering the threshold adds protocol overhead and reduces protocol efficiency.

If you want to experiment, start with the default maximum 2346, and lower the threshold a small amount at a time. To get the most benefit, you must monitor the network for packet errors at different times of the day. Compare the effect on network performance of lowering the threshold when errors are very high with the effect on performance when errors are moderately high. In general, we recommend that you leave this setting at its default of 2346.

Change the RTS threshold

RTS/CTS (Request To Send / Clear To Send) is a function that helps prevent problems when wireless clients can receive signals from more than one wireless access point on the same channel. The problem is sometimes known as hidden node.

We do not recommend that you change the default RTS threshold. When the **RTS Threshold** is set to the default of 2346, it effectively turns off RTS/CTS.

If you must change the RTS threshold, adjust it incrementally. Start by lowering it a small amount each time. After each change, allow enough time to decide whether the change in network performance is positive before you change it again. If you lower this value too much, you can introduce more latency into the network, as Requests to Send are increased so much that the shared medium is reserved more often than necessary.

About wireless security settings

The Firebox X Edge e-Series Wireless uses three security protocol standards to protect your wireless network. They are WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), and WPA2. Each protocol standard can encrypt the transmissions on the wireless LAN between the computers and the access points. They also can prevent unauthorized access to the wireless access point.

WEP and WPA each use pre-shared keys, but WPA and WPA2 use an algorithm to change the encryption key at regular intervals. This keeps the data sent on a wireless connection more secure.

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

Set the wireless authentication method

Five authentication methods are available in the Firebox X Edge e-Series Wireless. We recommend that you use WPA2 if possible because it is the most secure. The five available methods, from least secure to most secure, are:

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.

Shared Key

In Shared Key authentication, only those wireless clients that have the shared key can connect. Shared Key authentication can be used only with WEP encryption.

WPA ONLY (PSK)

When you use WPA (Wi-Fi Protected Access) with pre-shared keys, each wireless user is given the same password to authenticate to the wireless access point.

WPA/WPA2 (PSK)

When you select WPA/WPA2 (PSK) authentication, the Edge accepts connections from wireless devices configured to use WPA or WPA2.

WPA2 ONLY (PSK)

WPA2 authentication with pre-shared keys implements the full 802.11i standard and is the most secure authentication method. It does not work with some older wireless network cards.

Set the encryption level

From the **Encryption** drop-down list, select the level of encryption for your wireless connections. The options change when you use different authentication mechanisms. The Edge automatically creates a random encryption key for you when a key is required. You can use this key, or change it to a key you prefer. Each wireless client must use this same key when they connect to the Edge.

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 also can 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.
 - o A WEP 64-bit hexadecimal key must have 10 hexadecimal (0-f) characters.
 - o A WEP 40-bit ASCII key must have 5 characters.
 - o A WEP 128-bit hexadecimal key must have 26 hexadecimal (0-f) characters.
 - o 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 e-Series Wireless can use only one key at a time. If you select a key other than the first key in the list, you also must set your wireless client to use the same key.

WPA and WPA2 PSK authentication

The encryption options for WPA-PSK and WPA2-PSK authentication are **TKIP**, **AES**, and **Auto**. We recommend that you set the encryption option to **Auto** to have the Firebox X Edge e-Series Wireless accept TKIP and AES settings.

About wireless connections to the trusted interface

If you enable wireless connections to the trusted interface, we recommend that you enable and use the Edge feature that allows you to restrict access to the trusted interface by MAC address. This prevents users from connecting to the Edge from unauthorized computers that could contain viruses or spyware. For more information on the Allowed MAC Address list, see [Restrict access to the trusted interface by MAC address](#).

Allow wireless connections to the trusted interface

1. To connect to the System Status page, type https:// in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1
2. From the navigation bar, select **Network >Trusted**. Select the **Wireless** tab.

The screenshot shows the 'Trusted Network Configuration' page with the 'Wireless' tab selected. The configuration includes:

- Enable wireless bridge to Trusted Network:
- Broadcast SSID and respond to SSID queries:
- Log Authentication Events:
- Network name (SSID): TRUSTED_00019
- Fragmentation Threshold: 2346 (256-2346 bytes)
- RTS Threshold: 2346 (256-2346 bytes)
- Authentication: Open System
- Encryption: Disabled

3. Select the **Enable wireless bridge to Trusted Network** check box to enable the Edge trusted interface as a wireless access point. Any wireless clients on the trusted network will have full access to computers on the trusted and optional networks, and access to the Internet as defined in the outgoing firewall rules on your Edge. If the wireless client sets the IP address on its wireless network card with DHCP, the DHCP server on the Edge's trusted network must be active and configured.
4. To configure the Edge wireless interface to send and answer SSID requests, select the **Broadcast SSID and respond to SSID queries** check box.
5. Select the **Log Authentication Events** check box if you want the Edge to send a log message to the log file each time a wireless computer tries to connect to the Edge trusted interface.
6. In the **Network name (SSID)** text box, type a unique name for your Edge wireless trusted network or use the default name.
7. To change the fragmentation threshold, type a value in the **Fragmentation Threshold** field. The possible values are 256 through 2346. We recommend that you do not change this setting.
8. From the **Authentication** drop-down list, select the type of authentication to enable for wireless connections to the trusted interface. We recommend that you use WPA2 if the wireless devices in your network can support WPA2.
9. From the **Encryption** drop-down list, select the type of encryption to use for the wireless connection and add the keys or passwords required for the type of encryption you select. If you select an encryption option with pre-shared keys, a random pre-shared key is generated for you. You can use this key, or type your own.
10. To only allow wireless users that use Mobile VPN with IPSec, select the **Require encrypted Mobile VPN with IPSec connections for wireless clients** check box.
11. Click **Submit** to save your configuration to the Firebox X Edge e-Series Wireless.

Allow wireless connections to the optional interface

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`
2. From the navigation bar, select **Network > Optional**. Select the **Wireless** tab.

The screenshot shows the 'Optional Network Configuration' page with the 'Wireless' tab selected. The configuration includes:

- Enable wireless bridge to Optional Network
- Broadcast SSID and respond to SSID queries
- Log Authentication Events
- Network name (SSID): OPTIONAL_00019
- Fragmentation Threshold: 2346 (256-2346 bytes)
- RTS Threshold: 2346 (256-2346 bytes)
- Authentication: Open System
- Encryption: Disabled

At the bottom, there is a link to 'Learn more about wireless connectivity.' and 'Submit' and 'Reset' buttons.

3. Select the **Enable wireless bridge to Optional Network** check box to enable the Edge optional interface as a wireless access point. Any wireless clients on the optional network will have full access to computers on the optional network, and access to the Internet as defined in the outgoing firewall rules on your Edge.
If the wireless client sets the IP address on its wireless network card with DHCP, the DHCP server on the Edge's optional network must be active and configured.
4. To configure the Edge wireless interface to send and answer SSID requests, select the **Broadcast SSID and respond to SSID queries** check box.
5. Select the **Log Authentication Events** check box if you want the Edge to send a log message to the log file each time a wireless computer tries to connect to the Edge optional interface.
6. In the **Network name (SSID)** text box, type a unique name for your Edge wireless optional network or use the default name.
7. To change the fragmentation threshold, type a value in the **Fragmentation Threshold** field. The possible values are 256 through 2346. We do not recommend you change this setting.

8. From the **Authentication** drop-down list, select the type of authentication to enable for wireless connections to the optional interface. We recommend that you use WPA2 if the wireless devices in your network can support WPA2.
9. From the **Encryption** drop-down list, select the type of encryption to use for the wireless connection and add the keys or passwords required for the type of encryption you select. If you select an encryption option with pre-shared keys, a random pre-shared key is generated for you. You can use this key, or type your own.
10. Click **Submit** to save your configuration changes.

Enable a wireless guest network manually



You can also use the wireless guest network configuration wizard available on the Wizards page of your Edge configuration menu.

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

The screenshot shows the 'Wireless' tab selected in a configuration interface. The page includes the following fields and options:

- Enable Wireless Guest Network
 - IP Address: 192.168.113.1
 - Subnet Mask: 255.255.255.0
- Enable DHCP Server on Wireless Guest Network
 - First address for DHCP server: []
 - Last address for DHCP server: []
 - [DHCP Reservations...](#)
 - DHCP Lease Duration: [] days [] hours [] minutes
 - WINS Server Address: []
 - DNS Server Address: []
 - Secondary DNS Server Address: []
 - DNS Domain Suffix: []
- Enable DHCP Relay on Wireless Guest Network
 - DHCP relay server: []
 - WebBlocker Profile: No WebBlocker []

At the bottom are 'Submit' and 'Reset' buttons.

3. On the **Settings** tab, select the **Enable Wireless Guest Network** check box to allow wireless connections through the Edge to the Internet according to the rules you have configured for outgoing access on your Edge. These computers have no access to computers on the trusted or optional network.
4. The Edge must assign the wireless guest network and IP address and subnet mask. The default IP address is 192.168.113.1. It is not necessary to change this IP address unless you already use the 192.168.113.0/24 network address on devices configured as part of your trusted or optional network. If you do, then you must select a different private IP address that is not already in use on one of your networks.
5. If you want to configure the Edge as a DHCP server when a wireless device tries to make a connection, select the **Enable DHCP Server on Wireless Guest Network** check box. To learn more about configuring the settings for the DHCP Server, see [Enable DHCP server on the trusted networks](#).
6. To configure the Edge to send DHCP requests to a DHCP server external to the Edge, select the **Enable DHCP Relay** check box. For more information about this feature, see [Make the Firebox a DHCP relay](#).
7. If you use WebBlocker and want to apply a WebBlocker profile for all wireless connections that use the wireless guest network, select the profile you want to apply from the **WebBlocker Profile** drop-down list.
8. On the **Wireless** tab, select the security settings for the wireless guest network. You must select whether you want wireless users to be able to send traffic to each other when they are connected to the wireless guest network. To have wireless guest users be able to send traffic to each other, make sure the **Prohibit client to client wireless network traffic** check box is clear. Other configuration options are described earlier in this chapter.
9. Use the **Allowed MAC Addresses** tab if you want to restrict wireless connections so that only wireless devices with a MAC address you add to the Edge configuration can connect to the Edge wireless guest network. For more information on restricting access by MAC address, see [Restrict access to the trusted interface by MAC address](#).
10. Click **Submit** to save your configuration to the Edge.

About wireless radio settings

The Firebox X Edge e-Series Wireless uses radio frequency signals to send and receive traffic from computers with wireless ethernet cards. Several settings are specific to Edge channel selection. You can see and change these settings if you connect to the Edge Wireless and select **Network > Radio Settings** from the left navigation bar. Most users do not change these settings.

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

The following settings apply to all wireless networks supported on the Firebox X Edge Wireless.

Operating Region **Americas**

Channel **Auto**

Wireless mode **802.11g and 802.11b**

Submit | Reset

Set the operating region and channel

You can choose from nine options for operating region: Americas, Asia, Australia, EMEA, France, Israel, Japan, Taiwan, 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. Your Firebox X Edge e-Series may have this option set at manufacturing.

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 e-Series Wireless automatically selects the channel with the strongest signal available in its physical location.

Set the wireless mode of operation

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 e-Series Wireless, select an option from the **Wireless Mode** drop-down list. There are three wireless modes:

802.11b only

This mode restricts the Edge to connect to devices only in 802.11b mode.

802.11g only

This mode restricts the Edge to connect to devices only in 802.11g mode.

802.11g and 802.11b

This is the default mode. This mode allows the Edge to connect with devices that use 802.11b or 802.11g. The Edge operates in 802.11g mode only 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.

Configure 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 your operating system documentation or help files.

1. Select **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.

7

Firewall Policies

About policies

The *security policy* of your organization is a set of definitions for protecting your computer network and the information that goes through it. The Firebox denies all packets that are not specifically allowed. When you add a *policy* to your Firebox configuration file, you add a set of rules that tell the Firebox to allow or deny traffic based upon factors such as source and destination of the packet or the TCP/IP port or protocol used for the packet.

As an example of how a policy might be used, suppose the network administrator of a company wants to activate a Windows terminal services connection to the company's public web server on the optional interface of the Firebox. He or she manages the web server with a Remote Desktop connection. At the same time, he or she wants to make sure that no other network users can use the Remote Desktop Protocol terminal services through the Firebox. To create this setup, the network administrator adds a policy that allows RDP connections only from the IP address of his or her own desktop computer to the IP address of the public web server.

A policy can also give the Firebox more instructions on how to handle the packet. For example, you can define logging and notification parameters that apply to the traffic or use NAT to change a packet's source IP address to an IP address and port behind the firewall.

Packet filter and proxy policies

The Firebox uses two categories of policies to filter network traffic: *packet filters* and *proxies*. A packet filter examines each packet's IP and TCP/UDP header. If the packet header information is legitimate, then the Firebox allows the packet. Otherwise, the Firebox drops the packet.

A proxy also examines the header information, but it also examines the content. When you activate a proxy, the Firebox uses deep packet inspection to make sure that connections are secure. It opens each packet in sequence, removes the network layer header, and examines the packet's payload. Finally, the proxy puts the network information back on the packet and sends it to its destination.

About adding policies to your Firebox

The Firebox includes many pre-configured packet filters and proxies that you can add to your configuration. For example, if you want a packet filter for all Telnet traffic, you add a pre-defined Telnet policy that you can modify for your needs. You can also make a custom policy for which you set the ports, protocols, and other parameters.

When you configure your Firebox X Edge using the Quick Setup Wizard, the Edge allows only limited outgoing connectivity. If you have more software applications and network traffic for the Edge to examine, you must:

- Configure the policies on the Edge to let necessary traffic through
- Set the approved hosts and properties for each policy
- Balance the requirement to protect your network against the requirements of your users to get access to external resources

We recommend that you set limits on outgoing access when you configure your Firebox.



Throughout WatchGuard documentation, we refer to both packet filters and proxies as policies. Unless we tell you differently, information on policies refers to both packet filters and proxies.

Common policies for the Firebox X Edge

Common Proxy Policies

Policy	Function
FTP-Proxy	Used to transfer files from one computer to another
H323-Proxy	Used to enable Voice-over-IP (VoIP)
HTTP-Proxy	WWW protocol
HTTPS-Proxy	Secure WWW protocol used for secure communications and transactions
Outgoing-Proxy	Applies to all outgoing traffic, including traffic managed by other common policies
POP3-Proxy	Used to move email messages from an email server to an email client
SIP-Proxy	Used to enable Voice-over-IP (VoIP)

Common Packet Filter Policies

Policy	Function
DNS	Internet name resolution
FTP	Used to transfer files from one computer to another
HTTP	WWW protocol
HTTPS	Secure WWW protocol, used for secure communications and transactions
ILS	Internet Locator Service, used by NetMeeting
IPSec	Used to set up a VPN tunnel
NetMeeting	Videoconferencing application
NNTP	Used for Usenet news
Ping	Used to troubleshoot or verify network connectivity
POP3	Used to move email messages from an email server to an email client
PPTP	Used to set up a VPN tunnel
SMB	Used by Microsoft Windows for file and print sharing
SMTP	Used to send email to an Internet Service Provider
SNMP	Used to monitor and control network devices in TCP/IP networks
ssh	Used by UNIX and BSD for secure remote administration
Telnet	Used to log into a remote computer
TFTP	Used to transfer files between computers on the same network
VPN-Any	Used to set up a BOVPN tunnel
WG-Firebox-Mgmt	Used to allow configuration and management connections to be made to the Firebox.
WG-Logging	Used to allow a second Firebox to access a Log Server on the trusted interface of a Firebox
WG-Mgmt-Server	Enabled by the Management Server Setup wizard to configure a Management Server
Outgoing	Applies to all outgoing traffic, including traffic managed by other common proxies

Policy rules

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

- **Allow** lets data or a connection through the Edge.
- **Deny** stops data or a connection from going through the Edge, and sends a response to the source.
- **No Rule** sets a rule to off, or disables the rule.

It is not always easy to decide if you should select **Deny** or **No Rule** for a policy. When you set the rule to **No Rule**, the action the Edge takes for that packet is dependent on lower precedence rules for the policy. If there are no other rules for the policy, then the Edge denies the packet by default.

Use the **Deny** rule when you have a lower precedence rule set to **Allow**, but you want to deny packets from a specific IP address or network. For example, if you want to allow most HTTP traffic, you set the common packet filter policy to **Allow**. If you want to deny HTTP traffic from one IP address, create a custom packet filter for that IP address and set the rule to Deny. When you select **Deny**, the policy uses slightly more network resources. One or two **Deny** rules does not affect system performance, but if you set all common packet filter rules to **Deny** instead of the default **No Rule**, it can dramatically affect system performance.

Incoming and outgoing traffic

Traffic that comes from the external network is incoming traffic. Traffic that goes to the external network is outgoing traffic. By default, the Firebox X Edge e-Series denies incoming traffic to protect your trusted and optional networks.

The default configuration of the 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 Edge denies this traffic:

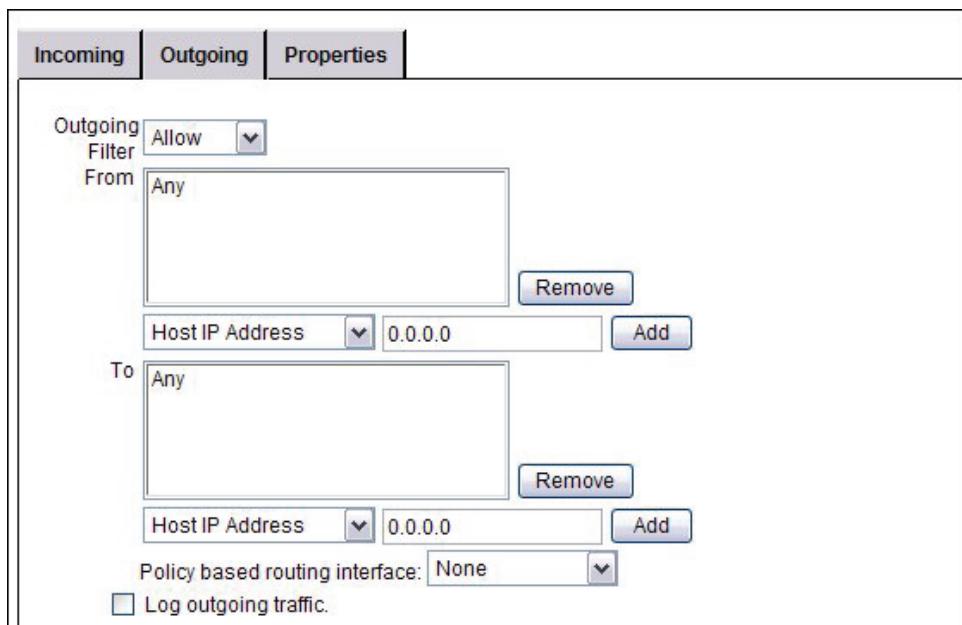
- From the external network to the trusted network
- From the optional network to the trusted network
- From the external network to the optional network

Packet filters are set separately for incoming and outgoing policies.

About policy-based routing

To send network traffic, a router usually examines the destination address in the packet and looks at the routing table to find the next-hop destination. In some cases, you want to send traffic to a different path than the default route specified in the routing table. You can configure a policy with a specific external interface to use for all outbound traffic that matches that policy. This technique is known as policy-based routing.

If you have an Edge Pro license for your Firebox X Edge and you have configured multi-WAN in round robin load balancing mode, you can apply policy-based routing to your firewall rules. When you enable policy-based routing, all traffic for a policy always goes out through the same external interface, even if your multi-WAN configuration is set to send traffic in a round-robin configuration. To apply policy based routing for an outgoing policy, edit the policy, and select the interface from the **Policy based routing interface** drop-down list.



About using common packet filter policies

You can control the traffic between the trusted, optional, and external networks using packet filter policies. The Firebox X Edge supplies a list of frequently used policies, called common policies, that you can use to easily allow or deny the most common traffic categories. You can use the default settings of the packet filters or you can edit them to meet your needs.

Remember that you must configure incoming and outgoing packet filter policies separately. By default, the common packet filter policy Outgoing is set to **Allow**. With the Outgoing policy, you can allow users on your trusted network to establish connections on the Internet, such as web browsing and email, and not have to create a policy for each type of connection. By default, all incoming traffic is set to **Deny**. You must be careful when you set incoming policies to **Allow**. When you allow an incoming policy, you open the protected networks behind the Firebox X Edge to more traffic, which increases risk.

To set your packet filter policies:

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`
2. From the navigation bar, select **Firewall > Incoming** for incoming policies or **Firewall > Outgoing** for outgoing policies. You can edit both incoming and outgoing traffic from either page.
The Filter Traffic page appears.

The screenshot shows the Firebox X Edge Filter Traffic interface. At the top, there are two tabs: "Firewall" and "Filter Outgoing Traffic". The "Filter Outgoing Traffic" tab is selected. Below the tabs, there are two tables:

Common Proxy Policies

Filter	Policy	Action
No Rule	FTP-Proxy	Edit
Allow	H323-Proxy	Edit
No Rule	HTTP-Proxy	Edit
No Rule	HTTPS-Proxy	Edit
No Rule	Outgoing-Proxy	Edit
No Rule	POP3-Proxy	Edit
No Rule	SIP-Proxy	Edit

Common Packet Filter Policies

Filter	Policy	Action
No Rule	DNS	Edit
No Rule	FTP	Edit
No Rule	HTTP	Edit
No Rule	HTTPS	Edit
No Rule	ILS	Edit

3. Find the common policy you want to allow or deny. From the Filter drop-down list adjacent to the policy name, select **Allow**, **Deny**, or **No Rule**.
If you select **No Rule**, that policy is disabled and the Edge uses the default behavior, which is to deny incoming traffic and allow outgoing traffic. For more information on rules, see [Policy Rules](#).

Editing common packet filter policies

You can edit some default settings of a common packet filter policy.

On the **Incoming** tab, you can define a service host, redirect the port, enable logging, or restrict the IP addresses on the external network that can connect to a computer behind the Firebox X Edge e-Series. On the **Outgoing** tab, you can enable logging and restrict the IP addresses on the trusted or optional networks that can connect to the external network with this policy in the **From** field. You can also restrict the external IP addresses to which trusted or optional computers can connect to in the **To** field.

To edit a common packet filter policy:

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1
2. From the navigation bar, select **Firewall > Incoming** or **Firewall > Outgoing**. You can edit both incoming and outgoing traffic from either page.
The Filter Traffic page appears.
3. Find the common packet filter policy you want to edit and click **Edit**.

Common Packet Filter Policies		
Filter	Policy	
No Rule	DNS	Edit
No Rule	FTP	Edit
No Rule	HTTP	Edit
No Rule	HTTPS	Edit
No Rule	ILS	Edit

Set access control options (incoming)

1. From the **Edit Policies** page, select the **Incoming** tab.
The Incoming tab appears.
2. From the **Incoming Filter** drop-down list, select the rule you want to apply. This rule affects only incoming traffic.
3. If the policy is set to **Allow**, enter the IP address of the computer that you want to receive the traffic in the **Policy Host** field, or select **1-to-1 Nat** and select the IP address pair you want to associate with the policy from the adjacent drop-down list. For more information on 1-to-1 NAT, see [Enable 1-to-1-NAT](#).
4. To use port address translation, enter the new port number in the **Port Redirect** text box. With port address translation, the destination port in the initial packet header is changed to a different destination port as the packet goes through the Edge.
5. Select **Host IP Address**, **Network IP Address**, **Host Range**, or **Alias** from the drop-down list to specify IP addresses or an alias for the external network that can use this policy. Type the IP address or range of IP addresses you want to allow and click **Add**. You can enter more than one address.
Type network IP addresses in slash notation. For more information, see [About slash notation](#).
6. To have the Firebox save log messages for this policy to the log file, select the **Log incoming traffic** check box.
7. Click **Submit**.

Set access control options (outgoing)

- From the **Edit Policies** page, select the **Outgoing** tab.

- From the **Outgoing Filter** drop-down list, select the rule you want to apply. This rule affects only outgoing traffic.
- To specify which computers on your trusted and optional network can use this policy, in the **From** field, select **Any** and click **Remove**. Select **Host IP Address**, **Network IP Address**, **Host Range**, or **Alias** from the drop-down list. Then enter the IP address or range of IP addresses you want to allow and click **Add**. You can add more than one address. If you select **Alias**, you can choose from **Trusted Network**, **Optional Network**, **Wireless Guest Network**, or from groups of Mobile VPN users. *Type network IP addresses in slash notation. For more information, see [About slash notation](#).*
- To limit which computers on the external network can connect to computers on the trusted or optional networks with this policy, in the **To** field, select **Any** and click **Remove**. Select **Host IP Address**, **Network IP Address**, or **Host Range** from the drop-down list. Then enter the IP address or range of IP addresses you want to allow and click **Add**. You can add more than one address.
- If your Firebox uses Edge Pro appliance software and you have configured a second external interface for your Firebox set for multi-WAN round robin load balancing, you can apply policy-based routing to the policy. Use the **Policy-based routing interface** drop-down list to select the external interface you want to use for all traffic managed by this policy. For more information about policy-based routing, see [About policy-based routing](#).
- To have the Firebox save log messages for this policy to the log file, select the **Log outgoing traffic** check box.
- Click **Submit**.

About custom policies

You must define a custom policy for traffic if you need to allow for a protocol that is not included by default as a Firebox configuration option.

A custom policy is also necessary if

- You must create an additional packet filter for a policy.
- You must change the port or protocol for a policy.

You can add a custom policy that uses:

- TCP ports
- UDP ports
- An IP protocol that is not TCP or UDP, such as GRE, AH, ESP, ICMP, IGMP, and OSPF. You identify an IP protocol that is not TCP or UDP with the IP protocol number.

You can create a custom policy [using a wizard](#) or [manually](#).

Add a custom policy using a wizard

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

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.

Policy Name

Type a name to identify the policy.

Protocols and Ports

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

Traffic Direction

Identify if this is an incoming or outgoing policy.

Policy action

Configure the Edge to allow or deny this type of policy traffic through the firewall.

Restrict to remote computers

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

Restrict to local computers

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

Add a custom packet filter policy manually

You can add a custom policy without the wizard.

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`.
2. From the navigation bar, select **Firewall > Incoming** for incoming or **Firewall > Outgoing** for outgoing.
The Filter Traffic page appears.
3. Scroll to the bottom of the page.
4. Below **Custom Packet Filter Policies**, click **Add Packet Filter Policy**.
The Custom Policy page appears.
5. In the **Policy Name** text box, type the name for your policy.
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 single port, type a port number in the first text box. To use a range of ports, type the lower port number in the first text box, and the higher port number in the second text box.



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 protocol numbers include 47 for GRE (Generic Routing Encapsulation) and 50 for ESP (Encapsulated Security Payload). TCP or UDP numbers are the most common. You can find a list of protocol numbers at <http://www.iana.org/assignments/protocol-numbers>.

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

Filter incoming traffic for a custom policy

These steps restrict incoming traffic for a policy to specified computers behind the firewall. For information on how to control outgoing traffic, see [Filter outgoing traffic for a custom policy](#).

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.
3. If you want to redirect traffic managed by this policy to another port, type the port number in the text box adjacent to **Port Redirect**.
For more information, see [About static NAT](#).
4. 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**.
5. In the address text boxes, type the host or network IP address, or type the range of IP addresses that identify the computers on the external network that can send traffic to the service host.
You must type network IP addresses in slash notation. For more information, see [About slash notation](#).
6. Click **Add**. The **From** box shows the host range, host IP address, or network IP address that you typed.
7. Repeat steps 4-6 until all of the address information for this custom policy is set. The **From** box can have more than one entry.
8. If this policy is only for incoming traffic, keep the outgoing filter set to **No Rule**.
9. Click **Submit**.

Filter outgoing traffic for a custom policy

These steps restrict outgoing traffic through the Firebox X Edge. For information on how to restrict incoming traffic, see [Filter incoming traffic for a custom policy](#).

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 policy, skip to step 10.
2. To restrict which computers on the trusted or optional network can send traffic to the external network with this policy, use the drop-down list below the **From** box to select **Host IP Address**, **Network IP Address**, **Host Range**, or **Alias**. If you select **Alias**, you can choose from **Trusted Network**, **Optional Network**, or **Wireless Guest Network**.
To only restrict which computers receive information, skip to step 6.
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 policy to send traffic to the external network.
Network IP addresses must be entered in slash notation.
4. Click **Add**. The **From** box shows the IP addresses you added.
5. Repeat steps 2-4 until all of the address information for this custom policy is set. The **From** box can have more than one entry.
6. To limit which computers on the external network can receive network traffic with this policy, use the drop-down list below the **To** box to select **Host IP Address**, **Network IP Address**, or **Host Range**.
7. 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 with this policy.
Network IP addresses must be entered in slash notation.
8. Click **Add**. The **To** box shows the IP addresses you added.
9. Repeat steps 6-8 until all of the address information for this custom policy is set. The **To** box can have more than one entry.
10. If this policy is only for outgoing traffic, keep the Incoming Filter set to **No Rule**.
11. Click **Submit**.

About policies for the optional network

By default, the Firebox X Edge e-Series 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 accept incoming connections from the external network. This helps to protect the trusted network, because no traffic is allowed to the trusted network from the optional network when the Firebox X Edge 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 access 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 (WAP) or a Firebox X Edge Wireless, you can increase the security of your trusted network by keeping the WAP 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. For more information about allowing traffic between the trusted and optional networks, see [Disable traffic filters between the trusted and optional networks](#).

Control traffic from the trusted to optional network

Do these steps to control traffic that goes from the trusted network 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 Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`.
2. From the navigation bar, select **Firewall > Optional**.
The Filter Outgoing Traffic to Optional Network page appears.
3. To allow all traffic from the trusted network, find the Outgoing policy and select **Allow** from the **Filter** drop-down list.
4. To deny all traffic from the trusted network, find the Outgoing policy and select **Deny** 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 policy to **Deny** from the **Filter** drop-down list. Then, for each policy that is allowed, select **Allow** from the **Filter** drop-down list. If you want to deny the traffic and create a log entry for each time the traffic is denied, select **No Rule**.
6. Click **Submit**.

Disable traffic filters between trusted and optional networks

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.

Firewall

Filter Outgoing Traffic to Optional Network

Disable traffic filters

*When you disable traffic filters, you **allow all traffic** between the Trusted Network and Optional Network in both directions.*

Filter	Policy
No Rule	DNS
No Rule	FTP
No Rule	HTTP
No Rule	HTTPS
No Rule	POP3
No Rule	SMTP
Allow	Outgoing

Submit **Reset**



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

About policy precedence

Precedence is the sequence in which the Firebox examines network traffic and applies a policy rule. The Firebox automatically sorts policies from the most detailed to the most general. It compares the information in the packet to the list of rules in the first policy. The first rule in the list to match the conditions of the packet is applied to the packet. If the detail level in two policies is equal, a proxy policy always takes precedence over a packet filter policy.

For example, if you want to deny most FTP traffic, but you want to allow it from one IP address, you set the common packet filter for FTP to **No Rule**. Because there is no lower precedence, the default action is to deny the packet. Then you create a new FTP packet filter that applies only to that IP address and set the rule to **Allow**. Because the new packet filter applies only to one IP address, it is more detailed and therefore a higher precedence.

8 Proxy Settings

About proxy policies

All WatchGuard policies, whether they are packet filter policies or proxy policies, are important tools for network security. While a packet filter examines each packet's IP and TCP/UDP header, a proxy monitors and scans whole connections. It examines the commands used in the connection to make sure they are in the correct syntax and order. It also uses deep packet inspection to make sure that connections are secure.

A proxy opens each packet in sequence, removes the network layer header, and examines the packet's payload. It then puts the network information back on the packet and sends it to its destination. As a result, a proxy can find forbidden content hidden or embedded in the data payload. For example, an SMTP proxy examines all incoming SMTP packets (email) to find forbidden content, such as executable programs or files written in scripting languages. Attackers frequently use these methods to send computer viruses. The SMTP proxy can enforce a policy that forbids these content types, while a packet filter cannot detect the unauthorized content in the packet's data payload.

If you have purchased and enabled additional security subscriptions (Gateway AntiVirus, Intrusion Prevention Service, spamBlocker, WebBlocker), WatchGuard proxies can apply these services.

About adding and configuring proxy policies

When you add a proxy policy to your Firebox configuration, you specify types of content that the proxy must look for as it filters traffic. If the content matches (or does not match) the criteria you set in the proxy definition, the proxy allows or denies the network traffic.

For each proxy policy, you can use the default settings or you can configure individual settings to suit your needs. You can also create additional proxy policies for each of the protocols to filter different parts of your network.

It is important to remember that a proxy filter adds more work for your firewall for the same volume of network traffic as a packet filter. But a proxy uses methods that packet filters cannot use to catch dangerous packets. Each proxy policy includes a set of parameters that you can adjust to create balance between your security needs and your performance needs.



If you upgrade to v8.6 from an earlier version of Edge firmware (such as v8.0 or v8.5) and you have WebBlocker enabled, the HTTP proxy is enabled by default. WebBlocker uses the HTTP proxy for content filtering.

The common proxy policies on the Firebox are not enabled by default. To add a proxy policy to your configuration, you must first enable it, as described in [Enable a common proxy policy](#).

Enable a common proxy policy

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`.
2. From the navigation bar, select **Firewall > Outgoing** or **Firewall > Incoming**.
The Filter Outgoing Traffic or Filter Incoming Traffic page appears.
3. Below **Common Proxy Policies**, find the proxy you want to enable and select **Allow** from the drop-down list.
4. Click **Submit**.

Add or Edit a Proxy Policy

To add or change the properties of a proxy policy, select **Firewall > Outgoing** or **Firewall > Incoming** from the navigation menu. To create a new proxy policy, click **New Custom Proxy Policy**. To modify an existing proxy, click the **Edit** button adjacent to the proxy name.

When you add or edit a proxy policy, make sure you look at all of the parts of the configuration page. There are three or four tabs for each proxy policy:

- **Incoming** or **Outgoing**. Use this first tab to set general information about the proxy policy, including whether traffic it applies to is allowed or denied. Certain types of proxy policies also allow you to set which computers can send or receive this type of network traffic, or which IP address acts as a policy host.
- **Properties** or **Settings**. The second tab shows information about which port and protocol the proxy policy manages. You cannot change the information on this tab.
- **Content**. The third and/or fourth tabs of a proxy policy include settings that apply only to that type of proxy policy. For example, a POP3 proxy policy includes two tabs, POP3 Settings and POP3 Content. You can use these tabs to create a deny message that users see when an email is rejected, or specify a list of attachment types that you consider unsafe.

To add or edit a custom proxy policy:

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1
2. From the navigation bar, select **Firewall Settings > Outgoing**.
3. In the **Custom Proxy Policies** section, click **Add Proxy Policy**.
The Add Policy - Custom Policy page appears.
4. In the **Policy Name** text box, type a name to identify your custom proxy policy.
5. From the **Protocol** drop-down list, select the protocol you want to manage.

Set access control options

On the **Outgoing** or **Incoming** tab, you can set rules that filter IP addresses, network addresses, or host ranges. This is the same functionality you have in packet filter policies.

1. Select the **Outgoing** tab.
2. From the **Outgoing Filter** drop-down list, select **Deny**, **Allow**, or **No Rule**.
3. Use the **From** drop-down list to add the IP address, network address, range of IP addresses of computers on the trusted or optional network, or an alias for which this policy applies.
Network IP addresses must be entered in slash notation (also known as Classless Inter Domain Routing or CIDR notation). For more information, see [About Slash Notation](#).
4. Click **Add**. The **From** text box shows the IP addresses you added. The **From** text box can have more than one entry.
5. Use the **To** drop-down list to add the IP address, network address, range of IP addresses of computers on the external network, or alias for which this policy applies.
Network IP addresses must be entered in slash notation.
6. Click **Add**.
To add additional IP addresses, repeat steps 3–6.

Use a policy to manage manual VPN network traffic

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1
2. From the navigation bar, select **Firewall > Outgoing** or **Firewall > Incoming**.
The Filter Outgoing Traffic or Filter Incoming Traffic page appears.
3. Create a new policy, or click the **Edit** button adjacent to an existing policy.
4. Select the **Apply to a Manual VPN** check box.
5. To apply the policy to a single VPN tunnel, select the tunnel name from the adjacent drop-down list.
*To apply the policy to all VPN tunnels, select **All Gateways**.*
6. Click **Submit** to save your changes.

About the HTTP proxy

Hyper Text Transfer Protocol (HTTP) is a request/response protocol between clients and servers. The HTTP client is usually a web browser. The HTTP server is a remote resource that keeps or creates HTML files, images, and other content. When the HTTP client starts a request, it establishes a Transmission Control Protocol (TCP) connection on port 80. An HTTP server listens for requests on port 80. When it receives the request from the client, the server replies with the requested file, an error message, or some other information.

The HTTP proxy is a high-performance content filter. It examines web traffic to identify suspicious content that can be a virus or other type of intrusion. It can also protect your web server from attacks from the external network.

With an HTTP proxy filter, you can:

- Adjust timeout and length limits of HTTP requests and responses to prevent the proxy from using too many network resources and to prevent some types of attacks.
- Customize the deny message that users see when they try to connect to a web site that the HTTP proxy blocks.
- Filter web content MIME types.
- Block specified path patterns and URLs.
- Deny cookies from specified web sites.

To enable the HTTP proxy, see [Enable a proxy](#). Then, if you choose, edit the proxy definition as described in [Add or edit a proxy policy](#).

On the **Outgoing** tab, you can set rules that filter traffic based on IP addresses, network addresses or host ranges. For information about these settings, see [Set access control options](#).

For information about the settings on the **HTTP Settings** tab, see:

- [HTTP proxy: Proxy Limits](#)
- [HTTP requests: General settings](#)
- [HTTP responses: General settings](#)
- [HTTP proxy: Deny message](#)
- [HTTP proxy exceptions](#)

For information about filtering HTTP content using the settings on the **HTTP Content** tab, see:

- [HTTP responses: Content types](#)
- [HTTP requests: URL paths](#)
- [HTTP responses: Cookies](#)

You can use the HTTP proxy with the WebBlocker security subscription. For more information, see [About WebBlocker](#).

HTTP proxy: Proxy Limits

On the **HTTP Settings** tab, you can adjust the timeout and length limits of HTTP requests and responses. This stops the HTTP proxy from using too many network resources and can prevent some types of attacks. You can also customize the deny message that users see when they try to connect to a web site that the HTTP proxy blocks, and add the IP addresses of web sites that you want to bypass the HTTP proxy.

HTTP requests: General settings

Idle connection timeout

This setting controls how long the HTTP proxy waits for the client to make a request after it has established a connection to the server. If the client does not make a request in the specified time, the proxy closes the connection. This makes sure that the network resources can be used by the proxy again. The default value is 10 minutes.

When a user clicks on a hyperlink or types a URL into the web browser, it sends an HTTP request to a remote server to get the content. In most browsers, the status bar shows, "Contacting site..." or a similar message. If the remote server does not respond, the HTTP client waits for a reply until it receives an answer or until the request times out. During this time, the HTTP proxy continues to monitor the connection and uses valuable network resources.

Maximum URL length

This setting sets the maximum length of the path component of a URL. This does not include the `http://` or host name. The URL length limit prevents buffer overflow attacks against web server resources. It could be necessary to increase this value for CGI web sites that use long URLs.

HTTP responses: General settings

When the remote HTTP server accepts the connection request from the HTTP client, most browser status bars show, "Site contacted. Waiting for reply..." Then the HTTP server sends the appropriate response to the HTTP client. This is usually a file or series of files. The proxy uses valuable network resources to monitor the network connection to the web server. It could become necessary to limit or expand how the proxy policy uses these resources in your network.

Timeout

This setting controls how long the HTTP proxy waits for the web server to send the web page. The idle timeout makes sure that the proxy can use the network resources after the timeout expires. The default value is 10 minutes.

Maximum line length

This setting controls the maximum allowed length of a line of characters in the HTTP response headers. The maximum line length limit prevents buffer overflow attacks.

HTTP proxy: Deny message

The Firebox gives a default deny message that replaces the content that is denied. You can replace that deny message with one that you write. You can customize the deny message with standard HTML. You can also use Unicode (UTF-8) characters in the deny message. The first line of the deny message is a component of the HTTP header. You must include an empty line between the first line and the body of the message.

You get a deny message in your web browser from the Firebox when you make a request that the HTTP proxy does not allow. You also get a deny message when your request is allowed, but the HTTP proxy denies the response from the remote web server. For example, if a user tries to download an .exe file and you have blocked that file type, the user sees a deny message in the web browser. If the user tries to download a web page that has an unknown content type and the proxy policy is configured to block unknown MIME types, the user sees an error message in the web browser. You can see the default deny message in the **Deny Message** field. To change this to a custom message, use these variables:

`%(transaction)%`

Puts Request or Response to show which side of the transaction caused the packet to be denied.

`%(reason)%`

Puts the reason the Firebox denied the content.

`%(method)%`

Puts the request method from the denied request.

`%(url-host)%`

Puts the server host name from the denied URL. If no host name was included, the IP address of the server is given.

`%(url-path)%`

Puts the path component of the denied URL.

Configure the HTTP proxy policy deny message

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X 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.
3. Under Common Proxy Policies, click the **Edit** button adjacent to the HTTP-Proxy entry.
4. Select the **HTTP Settings** tab.
5. Type the deny message in the **Deny Message** text box.

Deny Message

```
<h3> %(transaction)% denied by WatchGuard HTTP proxy. </h3><br>
<b> Reason: </b> %(reason)% <br>
<hr size="1" noshade><br>
<b> Method: </b> %(method)% <br>
<b> Host: </b> %(url-host)% <br>
<b> Path: </b> %(url-path)% <br>
<hr size="1" noshade>
```

(Max. 800 chars.)

6. Click **Submit** to save your changes.

HTTP proxy exceptions

You use HTTP proxy exceptions to bypass HTTP proxy rules for certain web sites without bypassing the proxy framework. Traffic that matches HTTP proxy exceptions still goes through the standard proxy handling used by the HTTP proxy. However, when a match occurs, some proxy settings are skipped.

Define exceptions

You can add host names or patterns as HTTP proxy exceptions. For example, if you block all web sites that end in .test but want to allow your users to go to the site www.abc.test, you can add www.abc.test as an HTTP proxy exception.

You specify the IP address or domain name of sites to allow. The domain (or host) name is the part of a URL that ends with .com, .net, .org, .biz, .gov, or .edu. Domain names can 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 your users to go to the WatchGuard web site http://www.watchguard.com, type www.watchguard.com. If you want to allow all subdomains that contain watchguard.com, you can use the asterisk (*) as a wildcard character. For example, to allow users to go to watchguard.com, www.watchguard.com, and support.watchguard.com type *watchguard.com.

To add an HTTP proxy exception:

1. From the HTTP proxy configuration, select the **HTTP Settings** tab.
2. In the text box to the left of the **Add** button type the host IP address or domain name of the web site to allow.
3. Click **Add**.
Repeat steps 2 and 3 for each additional host or domain name that you want to add.
4. Click **Submit**.

If you want a log message recorded in your log file each time a web transaction occurs to a web site in the exceptions list, select the **Log each transaction that matches an HTTP proxy exception** check box.

HTTP responses: Content types

When a web server sends HTTP traffic, it usually adds a MIME type, or content type, to the packet header that shows what kind of content is in the packet. The HTTP header on the data stream contains this MIME type. It is added before the data is sent.

Certain kinds of content that users request from web sites can be a security threat to your network. Other kinds of content can decrease the productivity of your users. By default, the Firebox allows some safe content types, and denies MIME content that has no specified content type. If the default proxy definition does not meet all of your business needs, you can add, delete, or modify the definition.

The format of a MIME type is **type/subtype**. For example, if you wanted to allow JPEG images, you would add image/jpg to the proxy definition. You can also use the asterisk (*) as a wildcard. To allow any image format, you add image/*.

For a list of current, registered MIME types, go to <http://www.iana.org/assignments/media-types>.

Add, delete, or modify content types

1. Select the **HTTP Content** tab.
2. Select the **Allow only safe content types** check box if you want to limit content types allowed through the proxy. A list of common MIME types is included by default.
3. To add common content types to the list, select the MIME type in the **Predefined content type** column and click the << button.
4. To add other content types, enter them in the empty field and click **Add**. To remove a content type, select it from the list and click **Remove**.

HTTP requests: URL paths

A URL (Uniform Resource Locator) identifies a resource on a remote server and gives the network location on that server. The URL path is the string of information that comes after the top level domain name. You can use the HTTP proxy to block web sites that contain specified text in the URL path. If the default proxy definition does not meet all of your business needs, you can add, delete, or modify URL path patterns. Here are examples of how to block content using HTTP request URL paths:

- To block all pages that have the host name www.test.com, type the pattern: www.test.com*
- To block all paths containing the word sex, on all web sites: *sex*
- To block URL paths ending in *.test, on all web sites: *.test

Block unsafe URL path patterns

1. Select the **Deny unsafe file name patterns** check box if you want to use URL path rules to filter the content of the host, path, and query-string components of a URL.
The name specifies files names but any pattern entered will be applied to the entire URL path.
2. To add a new path pattern, enter the path and click **Add**.
3. To remove a path pattern, select the pattern and click **Remove**.

HTTP responses: Cookies

HTTP cookies are small files of alphanumeric text put by web servers on web clients. Cookies monitor the page a web client is on to enable the web server to send more pages in the correct sequence. Web servers also use cookies to collect information about an end user. Many web sites use cookies for authentication and other legitimate functions, and cannot operate correctly without cookies.

The proxy looks for packets based on the domain associated with the cookie. The domain can be specified in the cookie. If the cookie does not contain a domain, the proxy uses the host name in the first request. For example, to block all cookies for nosy-adware-site.com, use the pattern: *.nosy-adware-site.com. If you want to deny cookies from all subdomains on a web site, use the wildcard symbol (*) before and after the domain. For example, *google.com* blocks all subdomains of google.com, such as images.google.com and mail.google.com.

Block cookies from a site

1. Select the **Deny Cookies from these sites** check box if you want to block cookies from a particular site.
2. Enter the web site domain name, or partial domain with wildcards, in the field. Click **Add**.
3. Click **Submit**.

About the FTP proxy

FTP (File Transfer Protocol) is used to send files from one computer to a different computer over a TCP/IP network. The FTP client is usually a computer. The FTP server can be a resource that keeps files on the same network or on a different network. The FTP client can be in one of two modes for data transfer: active or passive. In active mode, the server starts a connection to the client on source port 20. In passive mode, the client uses a previously negotiated port to connect to the server. The FTP proxy monitors and scans these FTP connections between your users and FTP servers they connect to.

With an FTP proxy filter, you can:

- Set the maximum user name length, password length, file name length, and command line length allowed through the proxy to help protect your network from buffer overflow attacks.
- Control the type of files that the FTP proxy allows for downloads and uploads.

The FTP proxy only applies to outgoing traffic. It does not apply to an FTP session initiated from the external network. We recommend that you deny all incoming traffic.

To enable the FTP proxy, see [Enable a proxy](#). Then, if you choose, edit the proxy definition as described in [Add or edit a proxy policy](#).

Edit the FTP proxy

To change the default settings of the FTP proxy, select **Firewall > Outgoing** from the navigation menu. Find the FTP proxy and click **Edit**. Make sure you look at all tabs of the FTP proxy configuration. The **Properties** tab shows you what port and protocol the proxy uses. You cannot make changes on this tab.

Set access control options

On the **Outgoing** or **Incoming** tab, you can set rules that filter IP addresses, network addresses, or host ranges. This is the same functionality you have in packet filter policies.

1. Select the **Outgoing** tab.
2. From the **Outgoing Filter** drop-down list, select **Deny**, **Allow**, or **No Rule**.
3. Use the **From** drop-down list to add the IP address, network address, range of IP addresses of computers on the trusted or optional network, or an alias for which this policy applies.
Network IP addresses must be entered in slash notation (also known as Classless Inter Domain Routing or CIDR notation). For more information, see [About Slash Notation](#).
4. Click **Add**. The **From** text box shows the IP addresses you added. The **From** text box can have more than one entry.
5. Use the **To** drop-down list to add the IP address, network address, range of IP addresses of computers on the external network, or alias for which this policy applies.
Network IP addresses must be entered in slash notation.
6. Click **Add**.
To add additional IP addresses, repeat steps 3–6.

FTP proxy: Proxy limits

On the **FTP Settings** tab, you can set the maximum user name length, password length, file name length, and command-line length allowed through the proxy. These limits help protect your network from buffer overflow attacks. Use the default settings or enter a new value in bytes

Firewall

Edit Policy - Common Policy

Policy Name: **FTP-Proxy**
Policy Type: **Proxy** Protocol: **FTP**
 Apply to a Manual VPN **All Gateways**

Outgoing **Properties** **FTP Settings** **FTP Content**

Maximum user name length	64	bytes
Maximum password length	32	bytes
Maximum filename length	1024	bytes
Maximum command line length	1030	bytes

[Learn more about policies.](#)

Submit **Reset**

Maximum username length

Sets a maximum length for user names on FTP sites.

Maximum password length

Sets a maximum length for passwords used to log in to FTP sites.

Maximum filename length

Sets the maximum file name length for files to upload or download.

Maximum command line length

Sets the maximum length for command lines used on FTP sites.

FTP proxy: Upload and download content

You can control the type of files that the FTP proxy allows for downloads and uploads. For example, because many hackers use executable files to deploy viruses or worms on a computer, you could select to deny requests for *.exe files. Or, if you do not want to let users upload Windows Media files to an FTP server, you could add *.wma to the proxy definition and specify that these files are denied. Use the asterisk (*) as a wild card.

1. Select the **FTP Content** tab.
2. In the **Downloads** text box, select the **Deny these file types** check box if you want to limit the types of files that a user can download.
This check box is selected by default and restricts the types of files that users can download through the FTP proxy.
3. If you want to deny additional files or file types, type an asterisk (*) and the file name or extension, and then click **Add**.
4. In the **Uploads** text box, select the **Deny these file types** check box if you want to limit the types of files that a user can upload. If you select this setting, the files listed will not be allowed.
5. If you want to deny any additional files or file types, type an asterisk (*) and the file name or extension, and then click **Add**.
6. Click **Submit**.

About the POP3 proxy

POP3 (Post Office Protocol v.3) is a protocol that moves email messages from an email server to an email client on a TCP connection on port 110. Most Internet-based email accounts use POP3. With POP3, an email client contacts the email server and checks for any new email messages. If it finds a new message, it downloads the email message to the local email client. After the message is received by the email client, the connection is closed.

With a POP3 proxy filter you can:

- Adjust timeout and line length limits to stop the POP3 proxy from using too many network resources and to prevent some types of attacks.
- Customize the deny message that users see when an email they try to receive is blocked.
- Filter content embedded in email with MIME types.
- Block specified path patterns and URLs.

To enable the POP3 proxy, see [Enable a proxy](#). Then, if you choose, edit the proxy definition as described in [Add or edit a proxy policy](#).

Edit the POP3 proxy

To change the default settings of the POP3 proxy, select **Firewall > Outgoing** from the navigation menu. Find the POP3 proxy and click **Edit**. Make sure you look at all tabs of the POP3 proxy configuration. The **Properties** tab shows you what port and protocol the proxy uses. You can change the port and protocol on this tab if necessary.

Set access control options

On the **Outgoing** or **Incoming** tab, you can set rules that filter IP addresses, network addresses, or host ranges. This is the same functionality you have in packet filter policies.

1. Select the **Outgoing** tab.
2. From the **Outgoing Filter** drop-down list, select **Deny**, **Allow**, or **No Rule**.
3. Use the **From** drop-down list to add the IP address, network address, range of IP addresses of computers on the trusted or optional network, or an alias for which this policy applies.
Network IP addresses must be entered in slash notation (also known as Classless Inter Domain Routing or CIDR notation). For more information, see [About Slash Notation](#).
4. Click **Add**. The **From** text box shows the IP addresses you added. The **From** text box can have more than one entry.
5. Use the **To** drop-down list to add the IP address, network address, range of IP addresses of computers on the external network, or alias for which this policy applies.
Network IP addresses must be entered in slash notation.
6. Click **Add**.
To add additional IP addresses, repeat steps 3–6.

POP3 proxy: Proxy limits

On the **POP3 Settings** tab, you can adjust timeout and line length limits. This stops the POP3 proxy from using too many network resources and can prevent some types of attacks. You can also customize the deny message that users see when an email message they try to download from the email server is blocked. For a complete description of the actions the POP3 proxy takes and the results your users see when the POP3 proxy finds and blocks content, see the FAQs for the Edge at <http://www.watchguard.com/support/faq/edge>.

Policy Name: POP3-Proxy
Policy Type: Proxy Protocol: POP3
 Apply to a Manual VPN All Gateways

Outgoing **Properties** **POP3 Settings** **POP3 Content**

Timeout seconds
Maximum line length bytes

Deny Message
The WatchGuard Firebox which protects your network detected a message which may not be safe.
Cause : %(reason)%
Content type : %(type)%
File name : %(filename)%
Virus status : %(virus)%
Action : The Firebox %(action)% %(filename)%.

(Max. 800 chars.)

[Learn more about policies](#)

Submit **Reset**

Timeout

This setting limits the number of seconds that the email client tries to open a connection to the email server before the connection is closed. This prevents the proxy from using too many network resources when the email server is slow or cannot be reached.

Maximum email line length

This setting prevents some types of buffer overflow attacks. It is unlikely that you will need to change this setting unless it prevents access to legitimate mail.

Deny Message

In the **Deny Message** field, you can write a custom plain text message that will appear in the recipient email when the proxy blocks that email. You can use these variables:

`%(type)%`

 Puts the content type of the email.

`%(filename)%`

 Puts the name of the attached file.

`%(virus)%`

 Puts the type of virus found.

`%(action)%`

 Puts the action taken by the proxy policy.

`%(reason)%`

 Puts the reason the proxy policy denied the content.

`%(recovery)%`

 Puts whether you can recover the attachment.

It is important to know how the POP3 proxy denies email. When the proxy blocks a message because of a header, you get a deny message instead of the email. When the proxy blocks an email message because of body or attachment content and the email is less than 100 kilobytes, you get a deny message instead of the email. If the proxy blocks an email message because of body or attachment content and the email is larger than 100 kilobytes, you get a truncated version of the email or attachment and the deny message is attached. When the POP3 proxy detects a protocol anomaly, or the email line length exceeds the maximum email line length, the proxy blocks the message download and the user gets no notification. You can see deny messages for this in the log messages. For information on using the log message tool, see the topic [About logging and logfiles](#).

POP3 proxy: Content types

Certain kinds of content embedded in email can be a security threat to your network. Other kinds of content can decrease the productivity of your users. On the **POP3 Content** tab, you limit content types, and block specified path patterns and URLs. You can use the asterisk (*) as a wildcard character.

Policy Name: POP3-Proxy
Policy Type: Proxy Protocol: POP3
 Apply to a Manual VPN All Gateways

Outgoing Properties POP3 Settings **POP3 Content**

Allow only safe content types

(none)	application/*
text/*	
image/*	
audio/*	
video/*	
multipart/*	
message/*	

<<

(none)	application/*
application/activemessage	
application/andrew-inset	
application/applefile	
application/astound	
application/atomicmail	
application/cals-1840	

Deny unsafe file name patterns

*.ade	
*.asx	
*.bat	
*.chm	
*.cmd	
*.com	
*.cpl	
*.crt	

[Learn more about policies.](#)

POP3 proxy: Allow only safe content types

The headers for email messages include a Content Type header to show the MIME type of the email and the MIME type of any attachments. The content type or MIME type tells the computer the types of media the message contains. Select the check box for this feature if you want to limit the content types that you allow through the proxy. When you select this check box, only the content types shown in the text box are allowed. The format of a MIME type is **type/subtype**. For example, if you want to allow JPEG images, you type `image/jpg`. You can also use the asterisk (*) as a wildcard. To allow any image format, you add `image/*` to the list.

1. To add additional content types to the default list, type the MIME type and click **Add**.
2. To remove a content type, select it from the list and click **Remove**. You cannot remove `message/*` or `multipart/*` because the POP3 proxy cannot work without them. If you try to remove these content types you get an error message.
3. To add common content types to the list, select the MIME type in the **Predefined content type** column and click the << button.

POP 3 proxy: Deny unsafe file name patterns

If you want to deny certain file name attachments, select the **Deny unsafe file name** patterns check box. This is a list of file names or types that you want the proxy to block. Use the asterisk (*) as a wild card. For example, if you want to block all MP3 files, type *.mp3. If you read about a vulnerability in a LiveSecurity Service Alert that affects PowerPoint files and you want to deny them until you install the patch, type *.ppt.

1. To add file name patterns to the blocked list, enter the pattern and click **Add**.
2. To remove a file name pattern from the blocked list, select the pattern and click **Remove**.
3. Click **Submit**.

About the SMTP proxy

SMTP (Simple Mail Transport Protocol) is a protocol used to send email messages between email servers and also between email clients and email servers. It usually uses a TCP connection on port 25. You use the SMTP proxy to control email messages and email content. The proxy scans SMTP messages for a number of filtered parameters, and compares them against the rules in the proxy configuration.

With an SMTP proxy filter you can:

- Adjust timeout, maximum email size and line length limit to stop the SMTP proxy from using too many network resources and can prevent some types of attacks.
- Customize the deny message that users see when an email they try to receive is blocked.
- Filter content embedded in email with MIME types and name patterns.
- Limit the email addresses that email can be addressed to and automatically block email from specific senders.

To enable the SMTP proxy, see [Enable a proxy](#). Then, if you choose, edit the proxy definition as described in [Add or edit a proxy policy](#).

For information about the settings on the **Incoming** tab, see [Set access control options](#).

For information about the settings on the **SMTP Settings** tab, see:

- [SMTP proxy: Proxy limits](#)
- [SMTP proxy: Deny message](#)

For information about filtering messages based on email addresses or content see:

- [SMTP Proxy: Filter email by address pattern](#)
- [SMTP proxy: Email content](#)

If you have a second SMTP email server, you must have an additional external IP address to give to the Edge. You can then [enable 1-to-1 NAT](#) and make a custom incoming proxy policy for SMTP.

Edit the SMTP proxy

To change the default settings of the SMTP proxy, select **Firewall > Incoming** from the navigation menu. Find the SMTP proxy and click **Edit**. Make sure you look at all tabs of the SMTP proxy configuration. The **Properties** tab shows you what port and protocol the proxy uses. You cannot make changes on this tab.

Policy Name: SMTP-Proxy
Policy Type: Proxy Protocol: SMTP
 Apply to a Manual VPN All Gateways

Incoming Properties SMTP Settings SMTP Addressing SMTP Content

Incoming Filter No Rule
Policy Host Policy Host 0.0.0.0
Port Redirect 25
From Any
Remove
Host IP Address 0.0.0.0 Add
 Log incoming traffic.

[Learn more about policies.](#)

Submit Reset

Set access control options

On the **Outgoing** or **Incoming** tab, you can set rules that filter IP addresses, network addresses, or host ranges. This is the same functionality you have in packet filter policies.

1. Select the **Outgoing** tab.
2. From the **Outgoing Filter** drop-down list, select **Deny**, **Allow**, or **No Rule**.
3. Use the **From** drop-down list to add the IP address, network address, range of IP addresses of computers on the trusted or optional network, or an alias for which this policy applies.
Network IP addresses must be entered in slash notation (also known as Classless Inter Domain Routing or CIDR notation). For more information, see [About Slash Notation](#).
4. Click **Add**. The **From** text box shows the IP addresses you added. The **From** text box can have more than one entry.
5. Use the **To** drop-down list to add the IP address, network address, range of IP addresses of computers on the external network, or alias for which this policy applies.
Network IP addresses must be entered in slash notation.
6. Click **Add**.
To add additional IP addresses, repeat steps 3–6.

SMTP proxy: Proxy limits

On the **SMTP Settings** tab, you can adjust timeout, email size, and line length limits. This stops the SMTP proxy from using too many network resources and can prevent some types of attacks. You can also [customize the deny message](#) that users see when an email message is blocked by the SMTP proxy.

Timeout

Set the length of time an incoming SMTP connection can idle before the SMTP proxy closes the connection.

Maximum email size

By default, the SMTP proxy does not restrict email by size (this field is set to zero). Use this setting if you want to set the maximum length of incoming SMTP messages. Most email is sent as 7-bit ASCII text. Encoding can increase the length of files by as much as one-third. To allow messages as large as 1MB (1024Kb) you must set this field to a minimum of 1.4MB (1400Kb) to make sure all email messages and their attachments get through.

Maximum line length

Set the maximum line length for lines in an SMTP message. Very long line lengths can cause buffer overflows on some email systems. Most email clients and systems send short line lengths, but some web-based email systems send very long lines.

Policy Name: **SMTP-Proxy**

Policy Type: **Proxy** Protocol: **SMTP**

Apply to a Manual VPN. **All Gateways** ▼

Incoming
Properties
SMTP Settings
SMTP Addressing
SMTP Content

Timeout seconds

Maximum e-mail size Kb (0 = unlimited size)

Maximum line length bytes (0 = disable limit)

Deny Message

The Watchguard Firebox which protects your network detected a message which may not be safe.

Cause: %(reason)%

Content-type: %(type)%

File name: %(filename)%

Virus status: %(virus)%

Action: The Firebox %(action)% %(filename)%

(Max. 800 chars.)

[Learn more about policies.](#)

SMTP proxy: Deny message

In the **Deny Message** field, you can write a custom plain text message that will appear in the recipient email message when the proxy blocks that message. You can use these variables:

`%(type)%`

Puts the content type of the email message.

`%(filename)%`

Puts the name of the attached file.

`%(virus)%`

Puts the type of virus found.

`%(action)%`

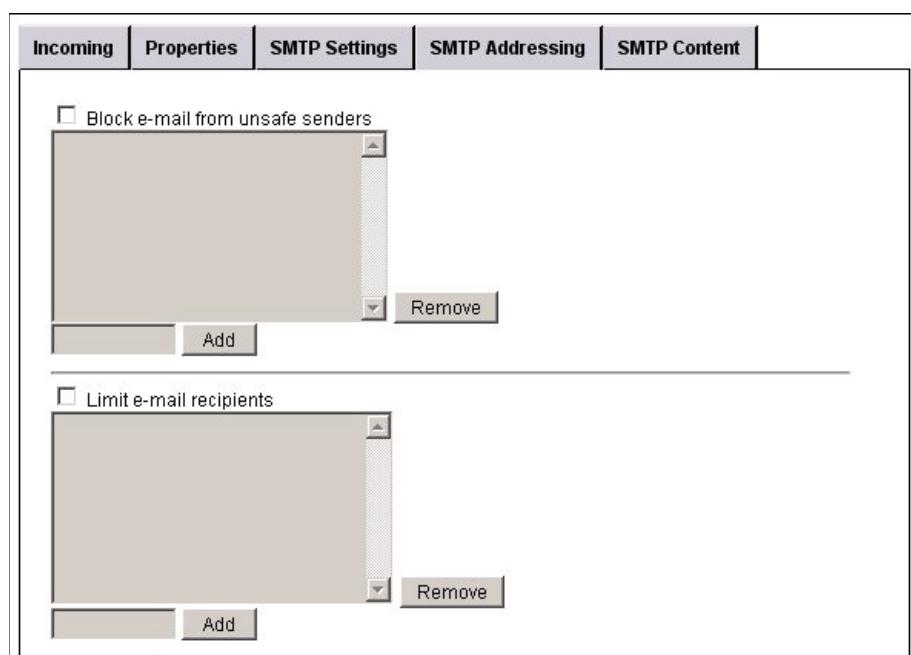
Puts the action taken by the proxy policy.

`%(reason)%`

Puts the reason the proxy policy denied the content.

SMTP Proxy: Filter email by address pattern

The options on the **SMTP Addressing** tab allow you to put limits on who can send email to your email server, and who can receive the email.



Block email from unsafe senders

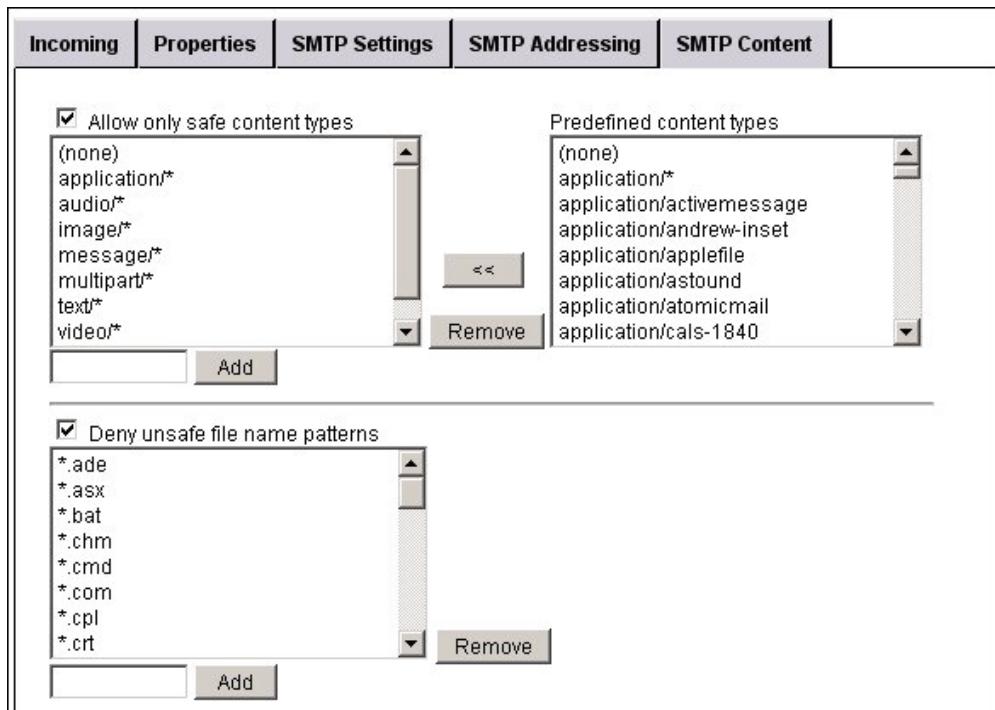
Select this check box if you want to put limits on email to allow email into your network only from specified senders. The default configuration allows email from all senders.

Limit email recipients

Select this check box if you want to allow email to only some of the users on your network. This can be useful if you want to prevent people from using your email server for email relaying. To do this, make sure that all domains for which your email server accepts email messages appear in the rule list. Make sure you use the wildcard format such as *@mywatchguard.com. Any email with an address that does not match the listed domains is denied.

SMTP proxy: Email content

Certain kinds of content embedded in email can be a security threat to your network. Other kinds of content can decrease the productivity of your users. On the **SMTP Content** tab, you limit content types, and block specified path patterns and URLs. You can use the asterisk (*) as a wildcard character.



Allow only safe content types

The headers for email messages include a Content Type header to show the MIME type of the email and of any attachments. The content type or MIME type tells the computer the types of media the message contains. Select the check box for this feature if you want to limit the content types that you allow through the proxy. When you select this check box, only the content types shown in the text box are allowed. The format of a MIME type is **type/subtype**. For example, if you want to allow JPEG images, you add `image/jpg`. You can also use the asterisk (*) as a wildcard character. To allow any image format, you add `image/*` to the list.

Add or remove a content type

1. To add additional content types to the default list, type the MIME type and click **Add**.
2. To remove a content type, select it from the list and click **Remove**. You cannot remove `message/*` or `multipart/*` because the SMTP proxy cannot work without them. If you try to remove these content types, you get an error message.
3. To add common content types to the list, select the MIME type in the **Predefined content type** column and click the **<<** button.

Add or remove file name patterns

1. To add file name patterns to the blocked list, enter the pattern and click **Add**.
2. To remove a file name pattern from the blocked list, select the pattern and click **Remove**.
3. Click **Submit**.

Deny unsafe file name patterns

If you want to deny certain file name attachments, select the **Deny unsafe file name patterns** check box. This is a list of file names or types that you want the proxy to block. Use the asterisk (*) as a wildcard character. For example, if you want to block all MP3 files, type *.mp3. If you read about a vulnerability in a LiveSecurity Service Alert that affects PowerPoint files and you want to deny them until you install the patch, type *.ppt.

About the HTTPS proxy

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a request/response protocol between clients and servers used for secure communications and transactions. HTTPS is more secure than HTTP because HTTPS uses a digital certificate to encrypt and decrypt user page requests as well as the pages that are returned by the web server. The HTTPS client is usually a web browser. The HTTPS server is a remote resource that keeps or creates HTML files, images, and other content.

By default, when an HTTPS client starts a request, it establishes a TCP (Transmission Control Protocol) connection on port 443. Most HTTPS servers listen for requests on port 443. When it receives the request from the client, the server replies with the requested file, an error message, or some other information.

To enable the SMTP proxy, follow the steps in [Enable a proxy](#). Then, if you choose, edit the proxy definition as described in [Add or edit a proxy policy](#).

You can set rules that filter traffic based on IP addresses, network addresses or host ranges. For information about these settings on the **Outgoing** tab, see [Set access control options](#).

On the **Settings** tab you can change the Idle connection timeout. This setting controls how long the HTTPS proxy waits for the web server to send the web page. The idle timeout makes sure that the proxy can use the network resources after the timeout expires. The default value is 10 minutes.

About the H.323 proxy

If you use Voice-over-IP (VoIP) in your organization, you can add an H.323 or SIP (Session Initiation Protocol) proxy policy to open the ports necessary to enable VoIP through your Firebox. These proxy policies have been created to work in a NAT environment to maintain security for privately addressed conferencing equipment behind the Firebox.

H.323 is used commonly on older videoconferencing equipment and voice installations. SIP is a newer standard that is more common in hosted environments, where only endpoint devices such as telephones are hosted at your business location and a VoIP provider manages the connectivity. You can use both H.323 and SIP proxy policies at the same time, if necessary. To determine which proxy policy you need to add, consult the documentation for your VoIP devices or applications.

It is important to understand that you usually implement VoIP by using either:

Peer-to-peer connections

In a peer-to-peer connection, each of the two devices knows the IP address of the other device and connect to each other directly.

Hosted connections

Connections hosted by a call management system (PBX)

With H.323, the key component of call management is known as the GateKeeper. We do not support H.323 connections hosted by call management systems at this time. In this release, the H.323 proxy supports only peer-to-peer connections.

Coordinating the many components of a VoIP installation can be difficult. We recommend you make sure that VoIP connections work successfully before you try to use the system with the Firebox proxy policies. This can help you to troubleshoot any problems.



Some manufacturers use the TFTP protocol to send periodic updates to the VoIP equipment under management. If your equipment requires TFTP for updates, make sure you add a TFTP policy to your Firebox configuration to allow these connections.

When you enable an H.323 proxy policy, your Firebox:

- Automatically responds to VoIP applications and opens the appropriate ports
- Makes sure that VoIP connections use standard H.323 protocols
- Generates log messages for auditing purposes

To enable the H.323 proxy, see [Enable a proxy](#). Then, if you choose, edit the proxy definition as described in [Add or edit a proxy policy](#).

About the SIP proxy

If you use Voice-over-IP (VoIP) in your organization, you can add a SIP (Session Initiation Protocol) or H.323 proxy policy to open the ports necessary to enable VoIP through your Firebox. These proxy policies have been created to work in a NAT environment to maintain security for privately-addressed conferencing equipment behind the Firebox.

H.323 is used commonly on older videoconferencing equipment and voice installations. SIP is a newer standard that is more common in hosted environments, where only endpoint devices such as phones are hosted at your business location and a VoIP provider manages the connectivity. You can use both H.323 and SIP proxy policies at the same time if necessary. To determine which proxy policy you need to add, consult the documentation for your VoIP devices or applications.

It is important to understand that you usually implement VoIP by using either:

Peer-to-peer connections

In a peer-to-peer connection, each of the two devices knows the IP address of the other device and connect to each other directly.

Hosted connections

Connections hosted by a call management system (PBX)

In the SIP standard, two key components of call management are the SIP Registrar and the SIP Proxy. Together, these components provide the functionality of the H.323 Gatekeeper, and work together to manage connections hosted by the call management system. The WatchGuard SIP proxy and the standard SIP Proxy are different. The WatchGuard SIP proxy is a transparent proxy that opens and closes ports necessary for SIP to operate. The WatchGuard SIP proxy can support both the SIP Registrar and the SIP Proxy when used with a call management system that is external to the Firebox. In this release, we do not support SIP when your call management system is protected by the Firebox.

Coordinating the many components of a VoIP installation can be difficult. We recommend you make sure that VoIP connections work successfully before you try to use the system with the Firebox proxy policies. This can help you to troubleshoot any problems you have.



Some manufacturers use the TFTP protocol to send periodic updates to the VoIP equipment under management. If your equipment requires TFTP for updates, make sure you add a TFTP policy to your Firebox configuration to allow these connections.

When you enable a SIP proxy policy, your Firebox:

- Automatically responds to VoIP applications and opens the appropriate ports
- Ensures that VoIP connections use standard SIP protocols
- Generates log messages for auditing purposes

You can create both incoming and outgoing SIP proxy policies. To create a custom SIP proxy policy, see [Enable a proxy](#). Then, if you choose, edit the proxy definition as described in [Add or Edit a proxy policy](#).

About the Outgoing Proxy

The Outgoing policy applies to all outgoing network traffic, including traffic managed by other common policies such as HTTP or FTP. As a packet filter policy, you can restrict which IP addresses can send traffic from the trusted or optional interfaces to the external interface. As a proxy policy, you can set specific options for different types of traffic and monitor connections for instant messaging (IM) or peer-to-peer (P2P) applications. You can also apply the Outgoing policy to a manual VPN tunnel.

When you enable the Outgoing proxy policy, you can:

- Choose to allow or deny different types of network traffic.
- Select an HTTP, HTTPS, or SIP proxy policy to manage those traffic types.
- Block or log packets sent by IM and/or P2P applications.

To enable the Outgoing proxy policy, see [Enable a common proxy policy](#). Then, if you choose, edit the proxy definition as described in [Add or edit a proxy policy](#). The options that are available only for the Outgoing proxy policy are described below.

Settings tab

You can use the Settings tab of the Outgoing proxy policy to quickly manage different types of outgoing network traffic. To change the setting for a protocol, select an option from the adjacent drop-down list. To permit all outgoing network traffic for the specified protocol, select **Allow**. To block all outgoing network traffic for the specified protocol, select **Deny**. If you want to use a common or custom proxy policy to manage HTTP, HTTPS, or SIP traffic, select a proxy policy.

Content tab

Many organizations do not allow users to operate IM or P2P applications, or permit the use of only one approved application. You can allow or block all outgoing traffic from these programs:

- Instant messaging applications: MSN, Yahoo IM, AIM, IRC, ICQ IM
- Peer-to-peer applications: BitTorrent, Ed2k, Gnutella, Kazaa, Napster

To allow or block one or more IM or P2P applications, select the adjacent check boxes, then choose **Allow** or **Deny** from the drop-down list. When you select **Allow**, the Edge adds information about the network traffic sent by the specified applications to the system log.

About additional security subscriptions for proxies

You can purchase additional security subscriptions that work with the Firebox X Edge proxies to add even greater security to your network. These are subscription-based services offered by WatchGuard. For purchase information, visit the WatchGuard LiveSecurity web site at <http://www.watchguard.com/store> or contact your WatchGuard reseller.

About intrusion prevention

The Firebox X Edge e-Series includes a set of default threat protection features designed to keep out network traffic from systems you know or think are a security risk. This set of features includes:

Permanently blocked site

The Blocked Sites list is a list of IP addresses you add manually to your configuration file. The IP addresses on this list cannot connect to or through the Edge on any port.

Auto-blocked sites

IP addresses that the Firebox adds or removes on a temporary blocked site list. The Firebox uses the packet handling rules that are specified for each service. For example, you can configure the Firebox to automatically block the source IP address of a computer that tries to connect through the Edge with the telnet service on port 23. If a computer tries to connect and gets denied, that computer cannot make any connections through the Edge, on any port, for a time period you control. This is known as the Temporary Blocked Sites list.

Blocked ports

You can block the ports that you know can be used to attack your network. This stops specified external network services. When you block a port, you override all the rules in your firewall configuration.

Denial of Service protection

A full set of denial of service protection rules allows you to set your own thresholds to prevent common denial of service attacks such as SYN flood attacks or ICMP flood attacks. You can also set connection limits to protect your network from distributed denial of service attacks.

Firewall options

A set of global firewall rules to control features such as default logging rules and FTP access to the Edge.

About blocked sites

A blocked site is an IP address that cannot make a connection through the Firebox. You tell the Firebox to block specific sites you know or think are a security risk. After you find the source of suspicious traffic, you can block all connections from that IP address. You can also define the Firebox to send a log message each time the source tries to connect to your network. From the log file, you can see the services that the sources use to launch attacks.

All traffic from a blocked IP address is denied. You can define two different types of blocked IP addresses: permanent or auto-blocked.

Permanently blocked sites

Network traffic from permanently blocked sites is always denied. These IP addresses are stored in the Blocked Sites list and must be added manually. For example, you can add an IP address that constantly attempts to scan your network to the Blocked Sites list to prevent port scans from that site.

To block a site, see [Block a site permanently](#).

Auto-blocked sites/Temporary Blocked Sites list

Packets from auto-blocked sites are denied for the amount of time you specify. You can choose to automatically block sites that send unhandled network traffic.

To automatically block unhandled traffic, see [Block sites temporarily](#).

Block a site permanently

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is `https://192.168.111.1`
2. From the navigation bar, click Firewall > Default Threat Protection. Click on the **Blocked Sites Tab**.

Firewall
Default Threat Protection

Blocked Sites Blocked Ports Auto-Block DoS Defense

Blocked Sites

Host IP Address: 0.0.0.0 Add

Log denied traffic from blocked sites

[Learn more about blocking sites.](#)

Submit Reset

3. Use the drop-down list to select whether you want to enter a host IP address, a network address, or a range of IP addresses. Type the value in the adjacent text box and click **Add**. You cannot add internal IP or network addresses to the Blocked Sites list.
4. Click **Submit**.

Block sites temporarily



To see a list of IP addresses auto-blocked by the Edge, go to **System Status > Hostile Sites**. You can look at the temporary Blocked Sites list together with your log messages to help you make decisions about which IP addresses to block permanently.

Follow these steps to configure your Firebox to automatically block sites temporarily:

1. Connect to the System Status page. Type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is `https://192.168.111.1`
2. From the navigation bar, click **Firewall > Default Threat Protection**. Click the **Auto-Block** tab.

Firewall
Default Threat Protection

Blocked Sites Blocked Ports Auto-Block DoS Defense

Duration for automatically blocked sites 30 minutes

Auto-block source of packets not handled.

Auto-Block exceptions

Host IP Address 0.0.0.0

[Learn more about automatically blocking sites](#)

3. Select the **Auto-block source of packets not handled** check box to add the IP addresses of any site denied by the Edge's default firewall policy to the temporary Blocked Sites list. To understand your Edge's default firewall policy, look at **Firewall > Incoming**. If you enable the auto-block feature, the source IP address of any traffic that is denied by the Edge because there is no rule to allow it will be added to the auto-blocked sites list.
4. Change the amount of time a site stays on the auto-blocked sites list with the **Duration for automatically blocked sites** drop-down list. The default is 30 minutes.
5. You can create exceptions to the auto-blocked sites rules. No traffic from an IP address on the Auto-block exceptions list is ever blocked by the auto-blocking feature. Use the drop-down list to select whether you want to enter a host IP address, a network address, or a range of IP addresses. Type the value in the adjacent text box and click **Add**.

About blocked ports

You can block the ports that you know can be used to attack your network. This stops specified external network services. Blocking ports can protect your most sensitive services.

When you block a port, you override all the rules in your firewall configuration. To block a port, see [Block a port](#).

Default blocked ports

With the default configuration, the Firebox blocks some destination ports. This gives a basic configuration that you usually do not have to change. TCP and UDP packets for these ports are blocked:

X Window System (ports 6000-6005)

The X Window System (or X-Windows) client connection is not encrypted and is dangerous to use on the Internet.

X Font Server (port 7100)

Many versions of X-Windows operate X Font Servers. The X Font Servers operate as the super-user on some hosts.

NFS (port 2049)

NFS (Network File System) is a frequently used TCP/IP service where many users use the same files on a network. New versions have important authentication and security problems. To supply NFS on the Internet can be very dangerous.



The portmapper frequently uses the port 2049 for NFS. If you use NFS, make sure that NFS uses the port 2049 on all your systems

rlogin, rsh, rcp (ports 513, 514)

These services give remote access to other computers. They are a security risk and many attackers probe for these services.

RPC portmapper (port 111)

The RPC Services use port 111 to find which ports a given RPC server uses. The RPC services are easy to attack through the Internet.

port 8000

Many vendors use this port, and many security problems are related to it.

port 1

The TCPmux service uses Port 1, but not frequently. You can block it to make it more difficult for the tools that examine ports.

port 0

This port is always blocked by the Firebox. You cannot allow traffic on port 0 through the Firebox.



If you must allow traffic through for the types of software applications that use recommended blocked ports, we recommend that you allow the traffic only through an IPSec VPN tunnel or use ssh to get access to the port.

Block a port



Be very careful if you block port numbers higher than 1023. Clients frequently use these source port numbers.

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is `https://192.168.111.1`.
2. From the navigation bar, click **Firewall > Intrusion Prevention**. Click on the **Blocked Ports** tab.

Firewall
Intrusion Prevention

Blocked Ports	0	1	111	513	514	2049	6000	6001	6002	6003
---------------	---	---	-----	-----	-----	------	------	------	------	------

Port Add

Auto-block sites that attempt to use blocked ports.

[Learn more about blocking ports.](#)

Submit Reset

3. In the **Ports** text box, type the name of the port you want to block. Click **Add**.
4. If you want the Edge to automatically block any external computer that tries to get access to a blocked port, select the **Auto-block sites that attempt to use blocked ports** check box.

About denial-of-service attacks

The Firebox X Edge e-Series includes an integrated denial-of-service (DoS) protection feature to protect against some of the most common and frequent DoS and Distributed DoS (DDos) attacks used on the Internet. A DoS attack is an attempt to make a computer resource unavailable to its intended users. Most frequently, DoS attacks try to prevent an Internet site or service from efficient operation for some period of time by using large amounts of bandwidth or resources on the system that is being attacked. This type of attack is usually called a flood. To configure the Firebox to protect you from DoS flood attacks, see [Drop DoS flood attacks](#).

In a distributed denial of service (DDoS) attack, many different computers send traffic to a single target computer at the same time. This causes the target computer to become so busy and use so many resources trying to establish connections with each malicious computer that it cannot handle legitimate traffic. To configure the Firebox to protect you from DDoS attacks, see [Distributed denial-of-service prevention](#).

Drop DoS flood attacks

You can configure the Edge to protect you from the most common DoS flood attacks. For each type of DoS flood attack, configure the Edge with a limit on the number of new connection packets per second that are allowed to pass through an interface. The Edge drops packets that exceed the configured limit.

Firewall
Intrusion Prevention

Blocked Sites	Blocked Ports	Auto-Block	DoS Defense																					
<p>Dangerous Activities</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;"><input type="checkbox"/> Drop IPSec Flood Attack</td> <td style="width: 10%; text-align: right;">1500</td> <td style="width: 60%;">packets/sec (threshold)</td> </tr> <tr> <td><input type="checkbox"/> Drop IKE Flood Attack</td> <td style="text-align: right;">1000</td> <td>packets/sec (threshold)</td> </tr> <tr> <td><input type="checkbox"/> Drop ICMP Flood Attack</td> <td style="text-align: right;">1000</td> <td>packets/sec (threshold)</td> </tr> <tr> <td><input type="checkbox"/> Drop SYN Flood Attack</td> <td style="text-align: right;">100</td> <td>packets/sec (threshold)</td> </tr> <tr> <td><input type="checkbox"/> Drop UDP Flood Attack</td> <td style="text-align: right;">1000</td> <td>packets/sec (threshold)</td> </tr> </table> <p>Distributed Denial-of-Service Prevention</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;"><input type="checkbox"/> Server Quota</td> <td style="width: 10%; text-align: right;">100</td> <td style="width: 60%;">connections/sec</td> </tr> <tr> <td><input type="checkbox"/> Client Quota</td> <td style="text-align: right;">100</td> <td>connections/sec</td> </tr> </table> <p>Learn more about DoS Defense.</p> <p style="text-align: center;">Submit Reset</p>				<input type="checkbox"/> Drop IPSec Flood Attack	1500	packets/sec (threshold)	<input type="checkbox"/> Drop IKE Flood Attack	1000	packets/sec (threshold)	<input type="checkbox"/> Drop ICMP Flood Attack	1000	packets/sec (threshold)	<input type="checkbox"/> Drop SYN Flood Attack	100	packets/sec (threshold)	<input type="checkbox"/> Drop UDP Flood Attack	1000	packets/sec (threshold)	<input type="checkbox"/> Server Quota	100	connections/sec	<input type="checkbox"/> Client Quota	100	connections/sec
<input type="checkbox"/> Drop IPSec Flood Attack	1500	packets/sec (threshold)																						
<input type="checkbox"/> Drop IKE Flood Attack	1000	packets/sec (threshold)																						
<input type="checkbox"/> Drop ICMP Flood Attack	1000	packets/sec (threshold)																						
<input type="checkbox"/> Drop SYN Flood Attack	100	packets/sec (threshold)																						
<input type="checkbox"/> Drop UDP Flood Attack	1000	packets/sec (threshold)																						
<input type="checkbox"/> Server Quota	100	connections/sec																						
<input type="checkbox"/> Client Quota	100	connections/sec																						

Default Threat Protection

On the **Firewall > Intrusion Prevention** page, select the **DoS Defense** tab and set the packet/second threshold for these types of DoS flood attacks:

IPSec flood attack

A DoS attack where the attacker overwhelms a computer system with a large number of IPSec connections.

IKE flood attack

A DoS attack where the attacker overwhelms a computer system with a large number of IKE (Internet Key Exchange) connections.

ICMP flood attack

A DoS attack where the attacker overwhelms a computer system with ICMP Echo Request (ping packets).

SYN flood attack

A DoS attack where the attacker overwhelms a computer system with a large number of SYN requests.

UDP flood attack

A DoS attack where the attacker overwhelms a computer system with a large number of UDP (User Datagram Protocol) connections.

Distributed denial-of-service prevention

Use the Distributed DoS prevention feature to set limits for server and client traffic. Use the **Server Quota** setting to set a maximum number of simultaneous connections allowed incoming through the Firebox from external computers. Use the **Client Quota** to set a maximum number of simultaneous connections allowed out from computers protected by the Edge. If the total number of client or server connections per second exceeds the connection limit you set, new connection packets are dropped.

Blocked Sites	Blocked Ports	Auto-Block	DoS Defense
Dangerous Activities			
<input type="checkbox"/> Drop IPSec Flood Attack	1500	packets/sec (threshold)	
<input type="checkbox"/> Drop IKE Flood Attack	1000	packets/sec (threshold)	
<input type="checkbox"/> Drop ICMP Flood Attack	1000	packets/sec (threshold)	
<input type="checkbox"/> Drop SYN Flood Attack	100	packets/sec (threshold)	
<input type="checkbox"/> Drop UDP Flood Attack	1000	packets/sec (threshold)	
Distributed Denial-of-Service Prevention			
<input type="checkbox"/> Server Quota	100	connections/sec	
<input type="checkbox"/> Client Quota	100	connections/sec	

[Learn more about DoS Defense.](#)

Submit | Reset

Configure firewall options

You can use the Firewall Options page to configure rules that increase your network security.

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`.
2. From the navigation bar, click **Firewall > 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 respond to PING requests received on Optional Network
 Do not allow FTP access to the Edge from the Trusted Network
 Do not allow FTP access to the Edge from the Optional Network
 Log all allowed outbound access
 Log denied broadcast traffic
 Log denied spoofed traffic
 Log traffic denied because of IP options
 Log inbound traffic that is denied by default
 Log outbound traffic that is denied by default

[Learn more about firewall options.](#)

Firewall options are pre-configured to meet the needs of many Edge customers. Select the check box of any option you want to enable and click **Submit** to save your changes to the Edge. Firewall options include:

Do not respond to ping requests

You can configure the Firebox X Edge e-Series to deny ping requests received on the trusted, external, or optional network. This option overrides all other Edge settings.

Do not allow FTP access to the Edge

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



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 Firebox X Edge firmware with the automatic installer. If you do not clear this check box, the Software Update Installer cannot move firmware files to the Edge.**

Log all allowed outbound access

If you use the standard property settings, the Firebox X Edge e-Series 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. When you record all outgoing traffic, it 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. For more information, see [See the event log file](#) topic.

Log denied broadcast traffic

If you use the standard property settings, the Firebox X Edge e-Series 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 denied network traffic that was sent to many destinations at the same time.

Log denied spoofed traffic

If you use the standard property settings, the Firebox X Edge e-Series 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 when the source IP address of network traffic does not match the IP address of the host that sent the traffic.

Log traffic denied because of IP options

IP options are extensions of the Internet Protocol. The Edge uses the extensions for special software applications or for advanced troubleshooting. An attacker can use the IP options in the packet header to find a path into your network. Select this check box to create a log message when traffic is denied because of IP options.

Log inbound traffic that is denied by default

Select this check box to have the Edge send a log message to the log file each time an incoming connection is denied by the default rules configured in your Edge.

Log outbound traffic that is denied by default

Select this check box to have the Edge send a log message to the log file each time an outgoing connection is denied by the default rules configured in your Edge.

10 Traffic Management

About Traffic Management

The Firebox X Edge e-Series supplies many different ways to manage the traffic on your network. You can:

- limit the rate of traffic sent to the external or IPSec interface using QoS (Quality of Service) through Traffic Control
- manage data transmission by giving more or less bandwidth to different traffic types
- change the visible network address of incoming or outgoing traffic to prevent conflicts using NAT (Network Address Translation).

For information about enabling traffic control, see [Enable Traffic Control](#).

About network traffic

Bandwidth is the quantity of data that can be sent through the network in a specified increment of time. It is usually expressed in bits per second (bps), kilobits per second (Kbps), or megabits per second (Mbps). A T1 line supplies approximately 1.5 Mbps, while a dial-up connection supplies approximately 56 Kbps. Latency is the quantity of time necessary for a packet to go from a source to a destination.

Together, latency and bandwidth define the speed and capacity of a network. You can improve latency by configuring Traffic Control. You must upgrade your Internet connection with your ISP to improve bandwidth.

When too many users or devices try to send data at the same time, the Firebox X Edge cannot send all of the data quickly. When the Edge has more traffic than the external connection can send at the same time, some programs appear to operate slowly.

Causes for slow network traffic

Many programs use as much bandwidth as possible to operate. If too many users operate these programs, other users cannot use the network. Peer-to-peer (P2P) services, instant messaging, and file downloads are programs that frequently use large quantities of bandwidth.

To limit the quantity of bandwidth those software applications can use, you must use Traffic Control. To deny or allow traffic from those software applications, you must configure a policy. For more information on policies, see [About policies](#).

Traffic Categories

The Firebox X Edge e-Series allows you to limit data sent through policies and Traffic Control filters. A policy can allow or deny all data of a specified type. Traffic Control does not allow or deny data, but creates filters that separate important network traffic from other data. For example, you can create a filter that identifies email (SMTP) traffic or secure shell (SSH) connections.

When you create a filter, you must select the priority for the traffic it identifies. There are four categories of network traffic: interactive, high, medium, and low. You can create as many as 100 traffic filters in each traffic category. Filters can be based on the IP protocol type, the source or destination IP address, and the source or destination port.

Interactive traffic is routed before all other traffic. Bandwidth not used for interactive traffic is divided between high, medium, and low priority traffic. Unused bandwidth is automatically given to other categories. For example, if there is no interactive or low priority traffic, all of the bandwidth is divided between high and medium priority traffic.

Interactive traffic

Interactive traffic is sent before any other traffic and is limited only by the speed of your connection. Use the interactive category for traffic that must have low latency. Some examples of interactive traffic are Telnet, Secure Shell (SSH), video communication, and Voice over Internet Protocol (VoIP).

High priority

High priority traffic is given 75% of the bandwidth not used by interactive traffic. Use the high priority category for traffic that is very important to your company or uses a lot of bandwidth. Some examples of high priority traffic are secure HTTP (HTTPS) and virtual private network (VPN) traffic.

Medium priority

Medium priority traffic is given 20% of the bandwidth not used by interactive traffic. When traffic control is enabled, any traffic that is not in a different filter is automatically put in the medium category. This traffic is represented by the All other traffic entry on the Traffic Control page.

Low priority

Low priority traffic is given 5% of the bandwidth not used by interactive traffic. Use the low priority category for low priority traffic that does not use much bandwidth, or is not important. Some examples of low priority traffic are peer-to-peer (P2P) file transfers or instant messaging (IM).



To use prioritization, you must know your upstream bandwidth limit in kilobits per second (Kbps). If you do not know your upstream bandwidth limit, ask your network administrator or ISP. For better traffic control, the Edge subtracts 5% from the upstream bandwidth rate limit to decrease packet latency. If you enter an incorrect upstream bandwidth limit, traffic control does not operate correctly.

Traffic Marking

If your Firebox X Edge is part of a larger network that uses Quality of Service (QoS) and your upstream device, LAN equipment, and IPS support it, you can apply marking to each category of network traffic you define on your Edge. The Edge then marks all traffic that matches the criteria in your Traffic Control rule. When you mark traffic, you change up to six bits on packet header fields defined for this purpose. The Edge and other marking-capable external devices use these bits to control how a packet is handled as it is sent over a network.

The use of marking procedures on a network requires that you do extensive planning. You can first identify theoretical bandwidth available and then determine which network applications are high priority, particularly sensitive to latency and jitter, or both.

The Firebox X Edge supports two types of Traffic Control marking: IP Precedence marking and DSCP (Differentiated Service Code Point) marking. IP Precedence marking affects only the first three bits in the IP type of service (ToS) octet. DSCP marking expands marking to the first six bits in the IP ToS octet. With both methods, you can choose to:

- Preserve the bits in the header, which may have been marked previously by an external device or
- Change the bits to a new value

DSCP values can be expressed in numeric form or by special keyword names that correspond to per-hop behavior (PHB). Per-hop behavior is the priority applied to a packet when traveling from one point to another in a network. DSCP marking supports three defined types of per-hop behavior

Best-Effort

Best-Effort is the default type of service and is recommended for traffic that is not critical or real-time. All traffic falls into this class if you do not use Traffic Control marking.

Assured Forwarding (AF)

Assured Forwarding PHB is recommended for traffic that needs better reliability than the best-effort service.

Expedited Forwarding (EF)

This type has the highest priority. It is generally reserved for mission-critical and real-time traffic.

Class-Selector (CSx) code points are defined to be backward compatible with Type of Service values. CS1 through CS7 are identical to the last seven options in the **Marking** drop-down list when IP Precedence is selected as the marking type.

The following table shows the DSCP values you can select, the corresponding IP Precedence value (which is the same as the CS value), and the description in PHB keywords.

DSCP Value	Equivalent IP Precedence value (CS values)	Description: Per-hop Behavior keyword
0		Best-Effort (same as no marking)
8	1	Scavenger* (Low)
10		AF Class 1 - Low - Low
12		AF Class 1- Low - Medium
14		AF Class 1- Low - High
16	2	Low/med
18		AF Class 2 - Low/med-Low
20		AF Class 2- Low/med-Medium
22		22 AF Class 2- Low/med-High
24	3	Med/high
26		AF Class 3 - Med/high-Low
28		AF Class 3- Med/high-Medium
30		AF Class 3- Med/high-High
32		High
34	4	AF Class 4 - High - Low
36		AF Class 4 - High - Medium
38		AF Class 4- High - High
40	5	Video, voice
46		EF
48	6	Internet Control (Reserved)
56	7	Network Control

* Scavenger class is intended for the lowest priority traffic such as media sharing or gaming applications. This traffic has a lower priority than Best-Effort.

For more information on DSCP values, see RFC 2474 at <http://www.ietf.org/rfc/rfc2474.txt>.

About Traffic Control Options

The Firebox X Edge e-Series has many different traffic control options, including:

Traffic control is off

The Edge sends network traffic in the sequence it was received.

Traffic control is on, but prioritization is off

This option limits all traffic to the upstream bandwidth limit.

Traffic control and prioritization are on

This option allows you to configure filters for all traffic categories.

Traffic control is on, and traffic marking is on

The Edge marks all traffic that matches the criteria in your Traffic Control rule.

Enable Traffic Control

You must have at least one packet filter policy, proxy policy, or VPN tunnel enabled to add traffic filters. You can use any enabled policy or active VPN tunnel as a Traffic Control filter. Incoming and outgoing policies are identified by **[Out]** or **[In]** adjacent to the policy name. Traffic Control is used only for outgoing network traffic. If you add an incoming policy to a Traffic Control category, the Firebox applies Traffic Control rules to outgoing traffic managed by that policy on the same port. For example, if you have a DNS server in your network that responds to requests from the external network, you can use Traffic Control to manage the amount of bandwidth those responses use. This is because DNS requests and responses use the same network port.

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

Network

Traffic Control

Checking **Enable traffic control** limits all outgoing traffic to specified Upstream bandwidth limit. All traffic has the same priority. See the documentation for more information on the use of this feature.

Checking **Prioritization** allows you to give different priorities to different types of outgoing traffic, while maintaining the upstream limit for all traffic.

WAN1: Enable traffic control. Upstream bandwidth limit: Kb/s

Prioritization Log traffic prioritization.

Marking Type:

Interactive Traffic

Mark:

Add... Remove

Bandwidth allocation by traffic priority

High

Mark:

Add... Remove

Medium

Mark:

[All other traffic]

Add... Remove

Low

Mark:

Add... Remove

Learn more about [configuring traffic control](#) or [traffic control marking](#).

3. Select the **Enable Traffic Control** check box.
The Interactive traffic list is enabled.

4. In the **Upstream bandwidth limit** text box, type the upstream bandwidth limit of your external network connection (WAN1). Enter a value from 19 Kbps to 100,000 Kbps. The default setting is 512 Kbps.
5. Select the **Prioritization** check box if you want to add filters to other network traffic categories.
The prioritization lists are enabled.

Bandwidth allocation by traffic priority

High	Medium	Low
<p>Mark: 0 (Best Effort)</p> <div style="border: 1px solid #ccc; height: 150px; width: 100%;"></div> <p style="text-align: center;"><input type="button" value="Remove"/> <input type="button" value="Add..."/></p>	<p>Mark: 0 (Best Effort)</p> <div style="border: 1px solid #ccc; height: 150px; width: 100%;"><p style="margin-left: 10px;">[All other traffic]</p></div> <p style="text-align: center;"><input type="button" value="Remove"/> <input type="button" value="Add..."/></p>	<p>Mark: 0 (Best Effort)</p> <div style="border: 1px solid #ccc; height: 150px; width: 100%;"></div> <p style="text-align: center;"><input type="button" value="Remove"/> <input type="button" value="Add..."/></p>

[Learn more about configuring traffic control](#) or [traffic control marking](#).

6. To create filters for the interactive, high, medium, or low traffic categories, click the **Add** button adjacent to the category name. Choose a policy or VPN tunnel, then click **Select**. Hold down CTRL to select more than one at a time. To delete a filter, click **Remove**.
7. To use Traffic Control marking, select **IP Precedence** or **DSCP** from the **Marking Type** drop-down list. For each priority of network traffic, use the **Mark** drop-down list to select the type of mark to apply for each traffic category.
For more information on DSCP values, see RFC 2474 at <http://www.ietf.org/rfc/rfc2474.txt>.
8. Click **Submit**.
Traffic control is enabled.

Related Questions

What if I want to deny a program or software application instead of only limiting it?

The Firebox® X Edge allows you to limit data sent through Traffic Control filters. A policy can allow or deny all data of a specified type. Traffic Control does not allow or deny data, but creates filters that separate important network traffic from other data. To deny or allow traffic from specific software applications, you must configure a policy. For more information on policies, see [About adding and configuring proxy policies](#).

Can I apply Traffic Control marking to IPSec traffic?

No, IPSec traffic does not use QoS marking.

About Network Address Translation (NAT)

Network Address Translation (NAT) is a term used to describe any of several forms of IP address and port translation. At its most basic level, NAT changes the IP address of a packet from one value to a different value.

The primary purposes of NAT are to increase the number of computers that can operate off a single publicly routable IP address, and to hide the private IP addresses of hosts on your LAN. When you use NAT, the source IP address is changed on all the packets you send.

You can apply NAT as a general firewall setting, or as a setting in a policy. Note that firewall NAT settings do not apply to BOVPN or Mobile VPN policies.

Types of NAT

The Firebox supports three different forms of NAT. Your configuration can use more than one type of NAT at the same time. You apply some types of NAT to all firewall traffic, and other types as a setting in a policy.

Dynamic NAT

Dynamic NAT is also known as IP masquerading. The Firebox can apply its public IP address to the outgoing packets for all connections or for specified services. This hides the real IP address of the computer that is the source of the packet from the external network. Dynamic NAT is generally used to hide the IP addresses of internal hosts when they get access to public services. For more information, see [About dynamic NAT](#).

Static NAT

Also known as port forwarding, you configure static NAT when you configure policies. Static NAT is a port-to-host NAT. A host sends a packet from the external network to a port on an external interface. Static NAT changes this IP address to an IP address and port behind the firewall. For more information, see [About static NAT](#).

1-to-1 NAT

1-to-1 NAT creates a mapping between IP addresses on one network and IP addresses on a different network. This type of NAT is often used to give external computers access to your public, internal servers. For more information, see [About 1-to-1 NAT](#).

NAT behavior

When you configure NAT:

- Each interface on the Firebox X Edge e-Series must use a different TCP subnet.
- You can have only one trusted network, one optional network, and one external network. You can use a router to connect more subnets to these networks. For more information, see [Connecting the Edge to more than four devices](#).
- The Edge always uses Dynamic NAT for traffic that goes from the trusted or optional networks to the external network.
- Dynamic NAT is not applied to BOVPN or Mobile VPN traffic.

Secondary IP addresses

You can assign eight public IP addresses to the primary external interface (WAN1). These addresses are used for 1-to-1 NAT.

When you configure secondary IP addresses on the external network:

- The primary IP address must be a static IP address. The first IP address is the primary IP address.
- All secondary IP addresses must be on the same external subnet as the primary IP address.
- You cannot configure multiple IP addresses for the WAN2 interface. The WAN2 interface must be on a different subnet than the WAN1 interface.

About dynamic NAT

Dynamic NAT is the most frequently used type of NAT. It changes the source IP address of an outgoing connection to the public IP address of the Firebox. Outside the Firebox, you see only the external interface IP address of the Firebox on outgoing packets.

Many computers can connect to the Internet from one public IP address. Dynamic NAT gives more security for internal hosts that use the Internet, because it hides the IP addresses of hosts on your network. With dynamic NAT, all connections must start from behind the Firebox. Malicious hosts cannot start connections to the computers behind the Firebox when the Firebox is configured for dynamic NAT.

The Edge automatically uses dynamic NAT on all outgoing traffic. If you want outgoing traffic from a host on the trusted or optional network to show an IP address that is different from the primary IP address on the external network, you must use 1-to-1 NAT. For more information, see [About 1-to-1 NAT](#).

About static NAT

Static NAT, also known as port forwarding, is a port-to-host NAT. A host sends a packet from the external network to a port on an external interface. Static NAT changes this IP address to an IP address and port behind the firewall. If a software application uses more than one port and the ports are selected dynamically, you must use 1-to-1 NAT or check whether a proxy on the Firebox will manage this kind of traffic.

When you use static NAT, you use an external IP address of your Firebox instead of the IP address of a public server. You could do this because you choose to, or because your public server does not have a public IP address. For example, you can put your SMTP email server behind the Firebox with a private IP address and configure static NAT in your SMTP policy. The Firebox receives connections on port 25 and makes sure that any SMTP traffic is sent to the real SMTP server behind the Firebox.

You configure static NAT with incoming firewall policies. For more information, see [About using common packet filter policies](#).

About 1-to-1 NAT

When you enable 1-to-1 NAT, the Firebox changes and routes all incoming and outgoing packets sent from one range of addresses to a different range of addresses. A 1-to-1 NAT rule always has precedence over dynamic NAT.

1-to-1 NAT is frequently used when you have a group of internal servers with private IP addresses that must be made public. You can use 1-to-1 NAT to map public IP addresses to the internal servers. You do not have to change the IP address of your internal servers. When you have a group of similar servers (for example, a group of email servers), 1-to-1 NAT is easier to configure than static NAT for the same group of servers.

To understand how to configure 1-to-1 NAT, we give this example:

Company ABC has a group of five privately addressed email servers behind the trusted interface of their Firebox. These addresses are:

10.1.1.1
10.1.1.2
10.1.1.3
10.1.1.4
10.1.1.5

Company ABC selects five public IP addresses from the same network address as the external interface of their Firebox, and creates DNS records for the email servers to resolve to. These addresses are:

- 50.1.1.1
- 50.1.1.2
- 50.1.1.3
- 50.1.1.4
- 50.1.1.5

Company ABC configures a 1-to-1 NAT rule for their email servers. The 1-to-1 NAT rule builds a static, bi-directional relationship between the corresponding pairs of IP addresses. The relationship looks like this:

- 10.1.1.1 <--> 50.1.1.1
- 10.1.1.2 <--> 50.1.1.2
- 10.1.1.3 <--> 50.1.1.3
- 10.1.1.4 <--> 50.1.1.4
- 10.1.1.5 <--> 50.1.1.5

When the 1-to-1 NAT rule is applied, the Firebox creates the bi-directional routing and NAT relationship between the pool of private IP addresses and the pool of public addresses.

About 1-to-1 NAT and VPNs

When you create a VPN tunnel, the networks at each end of the VPN tunnel must have different network address ranges. You can use 1-to-1 NAT when you must create a VPN tunnel between two networks that use the same private network address. If the network range on the remote network is the same as on the local network, you can configure both gateways to use 1-to-1 NAT. Then, you can create the VPN tunnel and not change the IP addresses of one side of the tunnel. 1-to-1 NAT for a VPN tunnel is configured when you configure the VPN tunnel and not in the **Network > NAT** dialog box.

Enable 1-to-1-NAT

You can assign a maximum of eight secondary IP addresses. When you configure a secondary IP addresses on the external network:

- The primary IP address must be a static IP address.
- All secondary IP addresses must be on the same external subnet as the primary IP address.
- You cannot configure multiple IP addresses for the WAN2 failover interface. The WAN2 interface is reserved for WAN failover. Your failover IP address must be on a different subnet.

Three steps are necessary to enable 1-to-1 NAT:

- Add at least one secondary external IP address to the Firebox.
A secondary external IP address is a public IP address on the external interface that also has an IP address on the trusted or optional (private) network. You must have at least one secondary external IP address to enable 1-to-1 NAT.
- Configure a custom policy for 1-to-1 NAT.
You can use an existing policy or you can add a custom policy that defines the kinds of network traffic that can be sent or received by the device that uses the secondary external IP address.
- Enable the secondary IP addresses on the Firebox

Add a secondary external IP address for 1-to1 NAT mapping

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`.
2. From the navigation bar, select **Firewall > NAT**.
The NAT (Network Address Translation) page appears.
3. Type a **public IP address** from the external network and a **private IP address** from the trusted or optional network, then click **Add**.
The Firebox X Edge maps the private IP address you typed to the secondary external IP address. You can create up to eight (8) IP address pairs for 1-to-1 NAT.
4. Click **Submit** to save your changes.

Add or edit a policy for 1-to-1 NAT

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X 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. Adjacent to an existing policy you want to change, click **Edit**.
To add a custom packet filter or proxy policy, click **Add Packet Filter Policy** or **Add Proxy Policy**.
4. On the **Incoming** tab, select **1-to-1 NAT** from the **Policy Host** drop-down list. If you have more than one secondary external IP address configured, select the IP address pair you want to associate with the policy from the adjacent drop-down list.
5. If this is an existing policy, click **Submit**.
If this is a new custom packet filter or proxy policy, use the instructions in [Filter incoming traffic for a custom policy](#) or [Add or Edit a Proxy Policy](#) to configure the other settings.

Enable secondary addresses

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`.
2. From the navigation bar, select **Firewall > NAT**.
The NAT (Network Address Translation) page appears.
3. Select the **Enable secondary IP addresses** check box.
4. Click **Submit**. 1-to-1 NAT is now enabled.

Add or edit a policy for 1-to-1 NAT

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X 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. Adjacent to an existing policy you want to change, click **Edit**.
To add a custom packet filter or proxy policy, click **Add Packet Filter Policy** or **Add Proxy Policy**.
4. On the **Incoming** tab, select **1-to-1 NAT** from the **Policy Host** drop-down list. If you have more than one secondary external IP address configured, select the IP address pair you want to associate with the policy from the adjacent drop-down list.
5. If this is an existing policy, click **Submit**.
If this is a new custom packet filter or proxy policy, use the instructions in [Filter incoming traffic for a custom policy](#) or [Add or Edit a Proxy Policy](#) to configure the other settings.

11 Logging

About logging and log files

An important feature of a good network security policy is to gather messages from your security systems, to examine those records frequently, and to keep them in an archive. You can use logs to monitor your network security and activity, identify any security risks, and address them.

A *log file* is a list of events, along with information about those events. An *event* is one activity that occurs on the Firebox. An example of an event is when the Firebox denies a packet. Your Firebox can also capture information about allowed events to give you a more complete picture of the activity on your network.

The log message system has several components.

Log Servers

The Firebox Edge can send log data to a syslog server or a WatchGuard Log Server, a component of WatchGuard System Manager (WSM). You must have a Firebox III, Firebox X Core, or Firebox X Peak to download and install WSM and the WatchGuard Log Server software. Syslog server software is available from third party vendors.

If your Firebox X Edge is configured to send log files to a WatchGuard Log Server and the connection fails, the log files are not collected. Configuring your Edge to also send log messages to a syslog host that is on the local trusted network prevents the loss of those log files.

You can install the WatchGuard Log Server on a computer you are using as a management station. Or, you can install the Log Server software on a different computer. To do this, use the WatchGuard System Manager installation program and select to install only the Log Server component. You can also add additional Log Servers for backup.

Log messages that are sent to the WatchGuard Log Server are encrypted. The log message format is XML (plain text). The information collected from firewall devices includes traffic, alarm, event, debug, and statistic log messages.

For more information about the WatchGuard Log server, see [About logging to a WatchGuard Log Server](#).

For more information about syslog, see [About Syslog](#).

Event Log and System Status Syslog

You can see the Event Log on the **Logging** page. The event log contains data on the most recent activity on the Firebox. You can see the same information, without other logging settings at **System Status > Syslog**. The **Syslog** page can display continuous real time log information. Click the **Start Continuous Refresh** button to have the log data updated in real time.

Logging and notification in applications and servers

The Log Server can receive log messages from your Firebox or a WatchGuard server. After you have configured your Firebox and Log Server, the Firebox sends log messages to the Log Server. You can enable logging in the various WSM applications and policies that you have defined for your Firebox to control the level of logs that you see. If you choose to send log messages from another WatchGuard server to the Log Server, you must first enable logging on that server.

About log messages

The Firebox sends log messages to the Log Server. It can also send log messages to a syslog server or keep logs locally on the Firebox. You can choose to send logs to either or both of these locations.

See the event log file

The Firebox X Edge e-Series uses up to 640KB of memory for log messages. New information appears 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.

The Firebox X Edge log file 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.

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.

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 Firebox X 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)

About logging to a WatchGuard Log Server

The WatchGuard Log Server (previously known as the WatchGuard System Event Processor, or WSEP) is a component of 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 e-Series. 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 then sends log messages to the backup Server until it cannot connect to that Server. Then, it tries the primary Server again. For instructions on how to configure the Log Server to accept log messages, see the *WatchGuard System Manager User Guide*.

If you have not already done so, it is a good idea to configure the Edge with a device name. 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 file by the IP address of the Edge external interface. To give your Edge a device name, go to the **Administration** web page.

To configure the Firebox to send event logs to a WatchGuard Log Server, see [Send your event logs to the Log Server](#).

Send your event logs to the Log Server

To configure the Edge to send your event logs to a WatchGuard Log Server:

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

Logging
WatchGuard Logging

Send logs to WSM Log Server
 Send logs in native XML format

Primary Log Server

Log Server IP Address

Log Encryption Key

Confirm Key

Backup Log Server

Log Server IP Address

Log Encryption Key

Confirm Key

[Learn more about WatchGuard logging.](#)

3. Select the **Send logs to WSM Log Server** check box if you want the Edge to send log messages to a WatchGuard Log Server you specify.

4. Select the **Send logs in native XML format** check box to have the Edge log messages sent to the WatchGuard Log Server in the XML format standard for Fireware v8.0 or higher. The WSM/Log Server installation must be WSM v8.3 or greater.
If you select this option, the Edge generates log messages in native XML, which includes more detail for each log message. This allows the WSM administrator to create Reports that include these details for the Edge.
If you keep this check box unselected, the Edge sends log messages in the proprietary format used with WFS appliance software v7.x. The Log Server then converts the log messages to XML.
5. Below **Primary Log Server**, type the IP address of the primary Log Server in the **Log Server 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 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 again connect to the primary Log Server, it automatically starts to send log messages to the primary Log Server again.
8. Click **Submit**.

About Syslog

Syslog is a log interface developed for UNIX but also used by a number of computer systems. You can [configure the Firebox to send log information to a syslog server](#). A Firebox can send log messages to a Log Server and a syslog server at the same time, or send log messages to one or the other. Syslog log messages are not encrypted. We recommend that you do not select a syslog host on the external interface.

Send logs to a Syslog host

Use these instructions to configure the Edge to send log messages to a syslog host. You must have a syslog host already configured and operational for it to receive log messages from the Edge.

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

[Learn more about Syslog logging.](#)

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 Firebox X Edge that sends syslog messages to the same syslog host.
7. Click **Submit**.



Because syslog traffic is not encrypted, syslog messages that are sent through the Internet decrease the security of the trusted network. It is more secure if you put your syslog host on your trusted network.

12 Certificates

About certificates

When you use local authentication to connect to your Firebox over secure HTTP, the Firebox uses a certificate to secure your session. You can also use certificates for VPN authentication.

Certificates are files that use a digital signature to match the identity of a person or organization with an encryption key. Certificates use a security component called a key pair, which consists of two mathematically related numbers. The user keeps one number, the private key, secret. The user can supply the other number, known as the public key, to other users. The private key has the ability to unlock data that was encrypted using the public key. Use a new key pair for each CSR you create.

Certificate authorities and signing requests

To create a third-party certificate, you need to put part of a cryptographic key pair in a certificate signing request (CSR) and send the CSR to a certificate authority. A certificate authority (CA) is an organization or application that issues and revokes certificates. The CA issues a certificate after they receive the CSR and verify your identity. We recommend that you choose a prominent CA, such as Verisign or GeoTrust to sign your CSR. Using a prominent CA ensures that your certificate will be automatically trusted by most users.

About certificates and the Firebox X Edge

You can import one Local Firebox X Edge certificate for local authentication, up to 25 Remote VPN Gateway certificates (one per gateway), and up to 10 CA certificates. The certificates you import on the Firebox X Edge are not included in a configuration backup. However, the distinguished names of the certificates selected for VPN tunnels are saved.

You must import a certificate to make it active. If you plan to use a certificate for VPN authentication on an existing tunnel, you must also change the VPN tunnel configuration to use the new certificate. No additional configuration is necessary for CA certificates.

Local certificates must include an unencrypted private key in the certificate file to operate correctly.

Create a certificate

Use OpenSSL to generate a CSR

OpenSSL is installed with most GNU/Linux distributions. To download the source code or a Windows binary file, go to <http://www.openssl.org/> and follow the installation instructions for your operating system. You can use OpenSSL to convert certificates and certificate signing requests from one format to another. For more information, see the OpenSSL man page or online documentation.

1. Open a command line interface terminal.
2. Type:
`openssl genrsa -out privkey.pem 1024` to generate a private key file called `privkey.pem` in your current working directory.
3. Type:
`openssl req -new -key privkey.pem -out request.csr`
This command generates a CSR in the PEM format in your current working directory.
4. When you are prompted for the x509 Common Name attribute information, type your fully-qualified domain name (FQDN). Use other information as appropriate.
5. Follow the instructions from your certificate authority to send the CSR.

To create a temporary, self-signed certificate until the CA returns your signed certificate, type at the command line:

```
openssl x509 -req -days 30 -in request.csr -key privkey.pem -out sscert.cert
```

This command creates a certificate inside your current directory that expires in 30 days.



You cannot use a self-signed certificate for VPN remote gateway authentication. We recommend that you use certificates signed by a trusted third-party Certificate Authority.

Use Microsoft CA to create a certificate

Certification Authority is distributed with Windows Server 2003 as a component. If the Certification Authority is not installed in the Administrative Tools folder of the Control Panel, follow the manufacturer's instructions for installation.

When you use this procedure, you act as the certificate authority (CA) and digitally sign your own request. For the final certificate to be useful, we recommend that you acquire other certificates that connect your private CA to a widely trusted, third-party certificate authority. You can import these additional certificates on the Firebox X Edge Certificates page.

Send the certificate request

1. Open your web browser. In the location or address bar, type the IP address of the server where the Certification Authority is installed, followed by **certsrv**.
Example: <http://10.0.2.80/certsrv>
2. Click the **Request a Certificate** link.
3. Click the **advanced certificate request** link.
4. To submit a CSR you created using OpenSSL, click the **Submit a certificate** link.
5. Paste the contents of your CSR file into the **Saved Request** text box.
The CSR must be in Base-64 PKCS10 or PKCS7 format.
6. Close your web browser.

Issue the certificate

1. Connect to the server where the Certification Authority is installed, if necessary.
2. From the Start Menu, select **Control Panel > Administrative Tools > Certification Authority**.
3. From the **Certification Authority (Local)** tree in the left navigation pane, select **Your Domain Name > Pending Requests**.
4. Select the CSR in the right navigation pane.
5. From the **Action** menu, select **All Tasks > Issue**.
6. Close the Certification Authority window.

Download the certificate

1. Open your web browser. In the location or address bar, type the IP address of the server where the Certification Authority is installed, followed by **certsrv**.
Example: http://10.0.2.80/certsrv
2. Click the **View the status of a pending certificate request** link.
3. Click the certificate request with the time and date you submitted.
4. Select the **Base 64 encoded** radio button to choose the PKCS7 format.
5. Click **Download certificate** to save the certificate on your hard drive.

About using certificates on the Firebox X Edge

You must import a certificate to make it active. If you plan to use a certificate for VPN authentication on an existing tunnel, you must also change the VPN tunnel configuration to use the new certificate. No additional configuration is necessary for Trusted CA certificates.



Local certificates must include an unencrypted private key in the certificate file to operate correctly.

Import a certificate

1. From the System Status page on the Firebox X Edge, select **Administration > Certificates**.
2. Adjacent to the type of certificate you want to add, click **Import**.
3. If your certificate is in the PEM format, copy and paste the certificate contents into the text box, or select the second radio button and click **Browse** to select the certificate file.
4. If your certificate is in the PKCS12 format, select the last radio button and click **Browse** to select the certificate file.
This option is available only for Local Firebox X Edge certificates.
5. Click **Import**.
You can repeat steps 2-5 to add more certificates.

Use a local certificate

1. From the System Status page on the Firebox X Edge, select **Administration > System Security**.
2. Select the local certificate you imported from the **Certificate** drop-down list.
3. Click **Submit**.

Remove a certificate

1. From the System Status page on the Firebox X Edge, select **Administration > Certificates**.
2. Select the certificate you want to delete, and then click the adjacent **Remove** button.



VPN tunnels do not operate correctly if you remove a certificate that is currently in use. We recommend that you change the VPN tunnel authentication method before you remove a Remote VPN Gateway certificate.

Examine the properties of a certificate

You can examine a certificate you have already imported to see its properties, including its expiration date, issuing authority, or other information.

1. From the System Status page on the Firebox X Edge, select **Administration > Certificates**.
2. Select the certificate you want to examine, and then click the adjacent **Detail** button.

Related questions

Can I sign my own certificates?

Yes, you can use a local certificate authority to sign the certificate. However, we recommend that you use a certificate signed by a trusted third-party certificate authority (CA).

I have a certificate or CSR that is not in the format I need. What do I do?

You can use OpenSSL to convert certificates and certificate signing requests from one format to another. For more information, see the OpenSSL man page or online documentation.

What is the maximum number of certificates I can import on the Firebox X Edge?

You can import one Local Firebox X Edge certificate for local authentication, up to 25 Remote VPN Gateway Certificates (one per gateway), and up to 10 Trusted CA Certificates.

If I make a backup of my Firebox X Edge configuration, are my certificates saved?

No, your certificates are not included in a configuration backup. However, the distinguished names of the certificates selected for VPN tunnels are saved, so you only need to re-import the certificates.

13 User and Group Management

About user licenses

Your Firebox X Edge firewall is enabled with a set number of user licenses (also called nodes). The total number of available sessions is determined by the Edge model you have, and any upgrade licenses you apply. The number of licenses limits the number of sessions.

License upgrades are available from your reseller or from the WatchGuard web site: <http://www.watchguard.com/products/purchaseoptions.asp>.

When a user license is used

A user license is not used by all sessions. User licensing works differently depending on whether Firebox User authentication is required to access the external network:

When user authentication is not required to access the external network

A user license is used when user authentication for access to the external network is not required and the Edge allows traffic to be passed from a computer on the trusted or optional network to the external network. When a user browses the Internet, the Edge adds the computer IP address to a list of users. When the limit is reached, all further connections from computers are denied.

When user authentication is required to access the external network.

A user license is used when user authentication is required for access to the external network, and a Firebox User authenticates. In this case a license is used as soon as a Firebox User authenticates to the Edge, whether or not traffic is passed from the user's computer to the external network.



If a single computer makes both a wired and wireless connection to a Firebox X Edge Wireless at the same time, it uses two user licenses when it sends traffic to the external network.

When a user license is not used

A user license is not used when:

- Traffic is passed between the trusted and optional networks.
- Traffic is passed from a computer on the trusted or optional network to a computer on the other end of a Branch Office VPN.
- Incoming traffic of any kind is passed to the Edge protected network.
- Traffic is passed from a computer to the Edge itself when no user authentication is required for access to the external network.

Managing user sessions

To control the number of users at any time, close one or more sessions. When you close a session, you make that user license available for another user. Sessions can be closed in several ways:

- If you require users to authenticate, the Firebox user can manually log out and return his or her license.
- The Edge Administrator can close the session manually. He or she can close the session for a individual user or close all sessions.
- If you require users to authenticate, you can assign a maximum timeout and an idle timeout for each user.
- The Edge Administrator can set a global session maximum timeout.
- You must reboot the Edge to close all sessions.

About user authentication

User authentication is the process of finding whether a user is who he or she is declared to be. On the Firebox, the use of passwords allows a user name to be associated with an IP address. This helps the Firebox administrator to monitor connections through the Firebox. With authentication, users can log in to the network from any computer, but get access to only the network ports and protocols for which they are authorized. All the connections that start from that IP address also transmit the session name while the user is authenticated.

You can configure the Edge as a local authentication server, or use your existing Active Directory or LDAP authentication server, or an existing RADIUS authentication server. When you use third-party authentication, account privileges for users that authenticate to the third-party authentication servers are based on group membership.

The WatchGuard user authentication feature allows a user name to be associated with a specific IP address to help you authenticate and track a user's connections through the Firebox. With the Firebox, the fundamental question that is asked and answered with each connection is "Should I allow traffic from source X to go to destination Y?" The WatchGuard authentication feature depends on the relationship between the person using a computer and the IP address of that computer to not change during the period of time that the person is authenticated to the Firebox.

In most environments, the relationship between an IP address and the person that uses it is stable enough to be used to authenticate that person's traffic. Environments in which the association between the person and an IP address is not consistent, such as a kiosk or terminal server-centric networks, are usually not good candidates for the successful use of our user authentication feature. WatchGuard currently supports Authentication, Accounting, and Access control (AAA) in the firewall products, based on a stable association between IP address and person.

The WatchGuard user authentication feature also supports authentication to an Active Directory domain via Single Sign-On and support other frequently used authentication servers. In addition, it supports inactivity settings and session time limits. These controls restrict the amount of time an IP address is allowed to pass traffic through the Firebox before the users must supply their passwords again.

If you control SSO access with a white list, manage inactivity timeouts, session timeouts, and who is allowed to authenticate, you can significantly improve your control of authentication, accounting, and access control.

How users authenticate

An HTTPS server operates on the Firebox to accept authentication requests. The users then must connect to the authentication web page on the Firebox using the procedure described in [Require users to authenticate to the Edge](#). When you set up user authentication for all users, you can choose to automatically present users with a login dialog when they attempt to access the Internet.

Set authentication options for all users

Some authentication options have an effect on 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 Firebox X 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.

Firebox User Access Restriction Enforcement and Options	
<input checked="" type="checkbox"/>	Require user authentication (enable local user accounts)
<input checked="" type="checkbox"/>	Automatically prompt for login on Web access
<input type="checkbox"/>	Reset idle timer on Firebox X Edge embedded Web site access
<input type="checkbox"/>	Enable automatic session termination every <input type="text" value="hour"/> <input type="button" value="▼"/>

3. Use the definitions below to help you change your parameters. Click **Submit**.

Require user authentication (enable local user accounts)

When you select this check box, all hosts must authenticate to the Firebox X Edge to send or receive network traffic. If you do not select this check box, there is no user-based control for access to the Internet or VPN tunnels.



If you configure an incoming service and you enable Firebox User accounts, you must add the servers that accept incoming connections to the Trusted Hosts list. For more information, go to [See current sessions and users](#).

Automatically prompt for login on Web access

When you select this check box, the authentication dialog box launches any time a user who has not yet authenticated tries to get access to the Internet. If you do not select this check box, the users must manually navigate to the authentication dialog, as described in [Require users to authenticate to the Edge](#).

Reset idle timer on Firebox X Edge embedded Web site access

When you select this check box, the Firebox X Edge does not disconnect a session when an idle timeout occurs if the **Login Status** dialog box is on the desktop. Clear this check box to override the **Login Status** dialog box. The **Login Status** box sends traffic to the Firebox X Edge from the user's computer every two minutes. If you select this check box, the Edge resets the idle timer to zero each time the Edge receives traffic from the **Login Status box**.

Enable 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. Select this check box to disconnect all sessions at the specified time in the drop-down list. All sessions are disconnected at the same time. The time limit is the number of hours since the Firebox X Edge first starts up, not the length of time a session has been active.

About user accounts

When you create a local user for the Firebox X Edge e-Series, 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 also can enable Mobile VPN with PPTP, enable Mobile VPN with SSL, add a WebBlocker profile to the user account, and configure the user's Mobile VPN with IPSec settings.

Three levels of Administrative Access are available for the Firebox X Edge:

- **None:** This level allows users 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 level for users who need to see Edge configuration properties and status. A user who uses this access level cannot change the configuration file.
- **Full:** Use this level for users who can see and change Edge configuration properties. A user with this access level 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 password for all user accounts.

Configure an individual user account

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X 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 MOVPN

Account name

Full name

Description

Password

Confirm password

Administrative access

Session maximum timeout minutes

Session idle timeout minutes

Allow access to the External Network

Allow access to manual and managed VPN tunnels

Allow remote access with Mobile VPN with PPTP

Allow remote access with Mobile VPN with SSL

[Learn more about creating local user accounts.](#)

User Guide

183

4. In the **Account Name** field, type a name for the account. The user types this name to authenticate. 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 to authenticate.
6. In the **Description** field, type a description for the user. This is for your information only. A user does not use this description to authenticate.
7. In the **Password** field, type a password with a minimum of eight characters. Mix at least 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 Firebox X Edge configuration properties: None, Read-Only, or Full.
For a description of administrative access levels see [About user accounts](#)
10. In the **Session maximum timeout** field, set the maximum length of time the computer can send traffic to the external network or through a Branch Office VPN tunnel. If this field is set to zero (0) minutes, there is no session timeout and the user can stay connected for any length of time.
11. In the **Session idle timeout** field, set the length of time the computer can stay authenticated when it is idle (not passing any traffic to the external network, through a Branch Office VPN, or to the Firebox X Edge itself). A setting of zero (0) minutes means there is no idle timeout.
12. If you want this user to have Internet access, select the **Allow access to the External Network** check box. You must require user authentication for this setting to have an effect.
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 manual and managed VPN tunnels** check box. You must require user authentication for this setting to have an effect.
14. If you want this user to be able to use Mobile VPN with PPTP to the Edge for secure remote access, select the **Allow Remote Access with Mobile VPN with PPTP** check box. You must also enable PPTP on the **VPN > Mobile VPN** page for Mobile VPN with PPTP to work.
15. If you want this user to be able to use Mobile VPN with SSL to the Edge for secure remote access, select the **Allow Remote Access with Mobile VPN with SSL** check box. You must also enable WatchGuard Mobile VPN with SSL on the **VPN > Mobile VPN with SSL** page.
16. Click **Submit**.

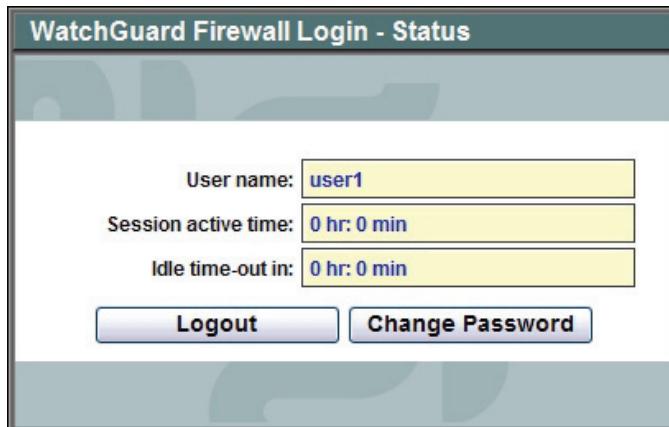
Require users to authenticate to the Edge

When you configure user authentication options for all users, you can choose to have users see the login dialog box automatically when they open their web browser. If you do not use this setting, users must use this procedure to authenticate:

1. Open a web browser. You can use Mozilla Firefox, Microsoft Internet Explorer, or Netscape Navigator. You can use other web browsers, but this is not supported. You must enable JavaScript and allow pop-up windows from the Firebox X Edge in your web browser to authenticate.
2. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`
3. A security dialog box appears. Accept the warning to continue.
4. Type your user name and password. If you use a third-party authentication server, such as Active Directory or RADIUS, you must type in the user name in the form of: domain\user

Authenticate a session without administrative access

If you require authentication to the Edge for the user to access resources such as the external network, the user must connect to the trusted interface IP address of the Edge using HTTPS, and type a user name and password. The default URL for the trusted interface IP address of the Edge is <https://192.168.111.1>. If the user's administrative access is set to **None**, the user sees the Login Status page instead of the Edge System Status page.



If the Firebox is configured to use local authentication, the user must type his or her user name as it appears in the Firebox User list. If the Firebox is configured to use LDAP, Active Directory, or RADIUS servers for authentication, the user must include the domain name. For example, if a user authenticates using the local Firebox user list, he or she types **jsmith**. If the user authenticates with an LDAP or RADIUS authentication server through the Edge, the user must type **MyCompany\jsmith**.

When a user authenticates with the Firebox X Edge and makes an Internet connection, their user name appears in the **Active Sessions** section of the Firebox Users page.

The Login Status page can be seen at any time when the user returns to the URL for the Edge. If the user is logged in, the user can use this page to:

- See how long their session has been active.
- See how long they can be idle before the session times out.
- Change their password.
- Log out of their session.

Create a read-only administrative account

You can create a local user account with access to see Firebox X Edge e-Series configuration pages, but not to save configuration changes to the Firebox. When a user logs in as a read-only administrator, the user 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 the user tries to do these things, the user sees a message that says the user has insufficient access rights to make changes to the Edge configuration.

To create a read-only user account, edit the user account. Use the **Administrative Access** drop-down list to select **Read Only**.

Use the built-in administrator account

The Firebox X Edge e-Series 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.

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 X Edge to the factory default settings. For more information, see [About factory default settings](#).

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 uppercase and lowercase letters for increased security.

Set 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:

1. Click the **WebBlocker** tab.
2. Select a profile from the drop-down list. You must do this even if you have only one WebBlocker profile. The default setting for all new users and groups is to bypass WebBlocker.

Adult		Shopping	
Adult/Sexually Explicit	<input type="checkbox"/>	Advertisements	<input type="checkbox"/>
Alcohol & Tobacco	<input type="checkbox"/>	Food & Drink	<input type="checkbox"/>
Gambling	<input type="checkbox"/>	Motor Vehicles	<input type="checkbox"/>
Intimate Apparel & Swimwear	<input type="checkbox"/>	Real Estate	<input type="checkbox"/>
Sex Education	<input type="checkbox"/>	Shopping	<input type="checkbox"/>
Tasteless & Offensive	<input type="checkbox"/>		
Crime		Computers	
Criminal Activity	<input type="checkbox"/>	Chat	<input type="checkbox"/>
		Computing & Internet	<input type="checkbox"/>
		Hosting Sites	<input type="checkbox"/>

3. Click **Submit**.

If you want to use different WebBlocker profiles for each group, you must first create the WebBlocker profiles in the **WebBlocker > Profiles** area of the Firebox X Edge configuration pages. For more information on WebBlocker profiles, see [Create a WebBlocker profile](#).

Change 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 Firebox X 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 new account name or leave the field empty to keep the current name. Type the new password. Confirm the new password.
6. Click **Submit**.

The screenshot shows the 'Edit User' page for 'user1'. The 'Settings' tab is selected. The account name is 'user1'. The 'Full name' field contains 'User1'. The 'Description' field is empty. The 'Change Identification' button is highlighted. The 'Administrative access' dropdown is set to 'None'. The 'Session maximum timeout' is '0' minutes. The 'Session idle timeout' is '0' minutes. Under 'Allow access to the External Network', the following checkboxes are checked: 'Allow access to the External Network', 'Allow access to manual and managed VPN tunnels', and 'Allow remote access with Mobile VPN with SSL'. The 'Allow remote access with Mobile VPN with PPTP' checkbox is unchecked. At the bottom are 'Submit' and 'Reset' buttons.

Account name	user1
Full name	User1
Description	
Change Identification	
Administrative access	None
Session maximum timeout	0 minutes
Session idle timeout	0 minutes
<input checked="" type="checkbox"/> Allow access to the External Network	
<input checked="" type="checkbox"/> Allow access to manual and managed VPN tunnels	
<input type="checkbox"/> Allow remote access with Mobile VPN with PPTP	
<input checked="" type="checkbox"/> Allow remote access with Mobile VPN with SSL	
Submit Reset	

About LDAP/Active Directory authentication

If you use LDAP authentication, you do not have to keep a separate user database on the Firebox X Edge. You can configure the Edge to forward 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 X Edge configuration and assign privileges and a WebBlocker profile. When users authenticate to the Edge, 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).

About using third-party authentication servers

If you use a third-party authentication server, you do not have to keep a separate user database on the Firebox. You configure a third-party server with the instructions from its manufacturer, install the server with access to the Firebox, and put it behind the Firebox for security. You then configure the Firebox to forward user authentication requests to that server. If you create a user group on the Firebox that authenticates to a third-party server, make sure you create a group on the server that has the same name as the user group on the Firebox.

To configure the Firebox for third-party authentication servers, see:

[Configure the LDAP/Active Directory authentication service](#)

[Enable RADIUS authentication](#)

Configure 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 Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`.
2. From the navigation bar, select **Firebox Users > Settings**.
The Firebox Users Settings page appears.

LDAP Authentication Service

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

Enable LDAP authentication.

Domain name

LDAP server type

LDAP server IP address

LDAP server port

LDAP timeout

Search Base

Enable Single Sign-On (SSO)

SSO agent IP address

Agent cache timeout seconds

SSO exceptions list

Host IP Address

3. Click the **LDAP** tab.
4. 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.
5. In the **Domain Name** text box, type the name of the LDAP domain. Do not include the top-level domain.
6. From the **LDAP server type** drop-down list, select the type of LDAP implementation you use in your organization: **Active Directory** or **Standard LDAP**.
7. 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 Edge interface or available through a VPN tunnel.
8. 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. Usually you do not have to change this number.

9. Use the **LDAP Timeout** drop-down list to select the number of seconds to use as a timeout for any LDAP operation.
10. 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 You can find more information about how to find your search base at www.watchguard.com/support/faq.
11. If you select Standard 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.
12. Select the **Enable Single Sign-On (SSO)** check box. For information on SSO, see [About Single Sign-On](#).
13. Click **Submit**.

Use the LDAP authentication test feature

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

To use the test feature, click **Test LDAP Account** 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.

Configure 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.

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.

Add a group for LDAP authentication

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X 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.

The screenshot shows the 'New Group' configuration page. At the top, there are tabs: 'Settings' (selected), 'WebBlocker', and 'MOVPN'. Below the tabs are fields for 'Account name' and 'Description'. A dropdown menu for 'Administrative access' is set to 'None'. The 'Session maximum timeout' is 0 minutes, and the 'Session idle timeout' is also 0 minutes. There are several checkboxes: 'Allow access to the External Network' (checked), 'Allow access to manual and managed VPN tunnels' (checked), 'Allow remote access with Mobile VPN with PPTP' (unchecked), and 'Allow remote access with Mobile VPN with SSL' (unchecked). A link 'Learn more about [creating local user accounts](#)' is present. At the bottom are 'Submit' and 'Reset' buttons.

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 X Edge 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 X Edge.
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 manual and managed VPN tunnels** check box to allow the members of this group to access VPN tunnels using the Firebox X Edge.

10. Select the **Allow remote access with Mobile VPN with PPTP** check box to allow the members of this group to establish PPTP connections with the Edge from remote locations.
11. Select the **Allow remote access with Mobile VPN with SSL** check box to allow the members of this group to establish SSL VPN connections with the Edge.
12. Click **Submit**.

Set a WebBlocker profile for an LDAP group

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 a group, click the **WebBlocker** tab on the Firebox Users New Group or Edit Group page and select a profile from the drop-down list. You must first create WebBlocker profiles in the **WebBlocker > Profiles** area of the Firebox X Edge 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 [Create a WebBlocker profile](#) topic.

LDAP authentication and Mobile VPN with IPSec

Mobile VPN with IPSec access for users that authenticate using LDAP is configured at the group level. A group must be added to the Firebox X Edge that matches the name of the group assigned to user entries in the LDAP directory. Click the MOVPN tab for the Firebox group and configure the Mobile VPN with IPSec settings.

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.

About Single Sign-On (SSO)

When users log on to a computer using Active Directory authentication, they must enter a user ID and password. If you use your Firebox to restrict outgoing network traffic to specified users or groups, users must log on again to access network resources such as the Internet. You can use Single Sign-On (SSO) so that users on the trusted or optional networks are automatically authenticated with the Firebox when they log on to their computer. While SSO offers convenience to your end users, there are access control limitations you must be aware of.

For SSO to work, you must install SSO agent software. The SSO agent software makes a *NetWkstaUserEnum* call to the client computer and uses the information it gets to authenticate a user for Single Sign-On. It is possible that the SSO agent can get more than one answer from the computer it queries. This can occur if more than one user logs in to the same computer, or because of service or batch logons that occur on the computer. The SSO agent uses only the first answer it gets from the computer, and reports that user to the Firebox as the user that is logged on.

For example, for services installed in on a client computer (such as a centrally administered antivirus client) that have been deployed so that they log on with domain account credentials, the Firebox gives all users access rights as defined by that user (and the groups of which that user is a member), and not the credentials of individual users that log on interactively. Also, all log messages generated from the user's activity show the user name of the service account, and not the individual user.

You can find more information about how the Single Sign-On feature works in the presentation *What's New in WSM/Fireware v10.0?* available at <https://www.watchguard.com/training/courses.asp>. You must log in with your LiveSecurity account to see this presentation.



SSO is not recommended for environments where multiple users share a single computer or IP address, where users log in using Mobile VPN, or on computers with service or batch logons. When more than one user is associated with an IP address, network permissions may not operate correctly. This can be a security risk.

To use SSO, you must install the WatchGuard Authentication Gateway software, also known as the SSO agent software, on a domain computer in your network. When a user logs on to a computer, the SSO agent gathers all the information from the user and sends it to the Firebox. The Firebox can then check the user information against all the defined policies for that user and/or user group at one time. The SSO agent caches this data for about 10 minutes by default so that a query does not have to be generated for every packet. For more information about installing the SSO agent, see [Install the WatchGuard SSO Agent](#).

Before You Begin

- You must have an Active Directory server configured on your trusted or optional network. Additionally, DHCP and DNS servers must be configured on the same domain as the Active Directory server.
- Your Firebox must be set to use Active Directory authentication.
- Each user must have an account set up on the Active Directory server.
- Each user must log on to a domain account for Single Sign-On (SSO) to operate correctly. If users log on to an account that exists only on their local computer, their credentials are not checked and the Firebox does not recognize that they are logged in.
- If you use third-party firewall software on your network computers, make sure that TCP port 445 (Samba/ Windows Networking) is open on each client.
- Make sure that printing and file sharing is enabled on every computer from which users authenticate using SSO.
- Make sure that NetBIOS and SMB ports are not blocked on every computer from which users authenticate using SSO. NetBIOS uses TCP/UDP ports 137, 138, 139 and SMB uses TCP port 445.
- Make sure that all computers from which users authenticate using SSO are members of the domain with unbroken trust relationships.

Define SSO exceptions If your network includes devices with IP addresses that do not require authentication, such as network or print servers, it is a good idea to add them to the SSO Exception list in the SSO configuration. Each time a connection from one of these devices occurs and the IP address for the device is not in the exceptions list, the Firebox contacts the SSO agent to try to associate the IP address with a user name. This takes about 10 seconds. Use the exceptions list to prevent the additional 10-second processing time for each connection and reduce unnecessary network traffic.

Enable Single Sign-On

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1
2. From the navigation bar, select **Firebox Users > Settings**.
The Firebox Users Settings page appears.
3. Make sure that the **Require user authentication (enable local user accounts)** check box is selected.
4. If necessary, select other access options. For more information, see [Set authentication options for all users](#).
5. Select the **Enable Single Sign-On (SSO)** check box.
6. Type the **SSO agent IP address** in the adjacent text box. This is the IP address of the computer on which you installed the WatchGuard Authentication Gateway software.
7. In the **Agent cache timeout** text box, type the number of seconds before the SSO agent must check a user's login status a second time. We recommend that you keep this value small if you use short DHCP lease times.
8. Add or remove **SSO exceptions** for IP addresses that the Firebox will not query for user information, such as computers with multiple users or servers that are not part of your Active Directory domain. If you reference these devices in your policies by name, they must authenticate with the Firebox using a web browser.
You can type a host IP address, a network IP address in slash notation, or a range of IP addresses.
9. Click **Submit** to save your changes.

Install the WatchGuard Single Sign-On (SSO) agent

To use Single Sign-On (SSO), you must install the WatchGuard SSO agent. The SSO agent is a service that receives requests for Firebox authentication and checks the user's status with the Active Directory server. The service runs with the name *WatchGuard Authentication Gateway* on the computer on which you install the SSO agent software. The computer on which you install the SSO agent software must have the Microsoft .NET Framework 2.0 installed.



To use Single Sign-On with your Firebox, you must install the SSO agent on a domain computer with a static IP address. We recommend that you install the SSO agent on your domain controller.

Download the SSO agent software

1. Use your browser to go to <http://www.watchguard.com/>.
2. Log in with your LiveSecurity Service user name and password.
3. Click the **Software Downloads** link.
4. Select your Firebox type and model number.
5. Download the WatchGuard Authentication Gateway software and save the file to a convenient location.

Before you install

The SSO agent service must be run as a user. We recommend that you create a new user account for this purpose. For the SSO agent service to operate correctly, configure the user account with the following properties:

- Add the account to the Domain Admin group.
- Make the Domain Admin group the primary group.
- Allow the account to log on as a service.
- Set the password to never expire.

Install the SSO agent service

Double-click `WG-Authentication-Gateway.exe` to start the Authentication Gateway setup wizard. You may need to type a local administrator password to run the installer on some operating systems. Follow the instructions to install the software:

Setup - Authentication Gateway

Click **Next** to start the wizard.

Select Destination Location

Type or select a location to install the software, then click **Next**.

Select Start Menu Folder

Type or select a location in the Start Menu to add program shortcuts. If you do not want to add program shortcuts to your Start Menu, select the **Don't create a Start Menu folder** check box. When you are finished, click **Next**.

Domain User Login

Type the **domain user name** and **password** of a user with an active account on your current LDAP or Active Directory domain. You must enter the user name in the form: `domain\username`. Note that this does not include the .com or .net part of the domain name. For example, if your domain is `mywatchguard.com` and you use the domain account `ssoagent`, enter the user name in this step as `mywatchguard\ssoagent`. Click **Next**.



If the user account you specify does not have enough privileges, some users cannot use SSO and must authenticate with the Firebox normally. We recommend you follow the instructions in the previous section to create a user account for the SSO agent service.

Ready to Install

Review your settings, then click **Install** to install the service on your computer.

Setup - Authentication Gateway

Click **Finish** to close the wizard. The WatchGuard Authentication Gateway service starts automatically when the wizard completes, and starts each time the computer restarts.

Enable RADIUS authentication

When you enable RADIUS authentication, you define one authentication server and its properties. When you set up your RADIUS server, you must make sure that, when it sends a message to the Firebox that a user is authenticated, it also sends a FilterID string, for example "engineeringGroup" or "financeGroup". The FilterID is RADIUS attribute 11. This information is then used for access control; it must match the Account Name of a group configured on the **Firebox Users** page.

To enable RADIUS authentication:

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

Learn more about [user authentication](#).

3. To enable the RADIUS server and enable the fields on this dialog box, select the **Enable RADIUS authentication** check box.
4. In the **RADIUS server IP address** text box, type the IP address of your RADIUS server.
5. In the **RADIUS server port** text box, make sure that the port number RADIUS uses for authentication appears. The default port number is 1812. Older RADIUS servers might use port 1645.
6. In the RADIUS server secret text box, type the shared secret between the Firebox and the RADIUS server. The shared secret is case-sensitive and must be the same on the Edge and the RADIUS server.
7. To set the timeout value, use the **Timeout** value control to set the value you want. The timeout value is the amount of time the Edge waits for a response from the authentication server before it tries to connect again.
8. To test whether the Firebox can successfully connect to the RADIUS server to verify a user credentials, click the **Test RADIUS Account** button.
9. Click **Submit**.

See active sessions and users

On the Firebox Users page, you see information about the users who are online.

1. To connect to the System Status page, type `https://` in the browser address bar, with the IP address of the Firebox X 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 user settings

Below **Firebox Users Settings**, you can see the current values for all global user and session settings.



Firebox Users

Firebox User Settings

Firebox User accounts are [enabled](#) [Configure](#)

- Automatic prompt for login on Web access: [Enabled](#)
- Reset idle on Firebox X Edge access: [Enabled](#)

Periodic automatic global session time-out is [disabled](#)

Active sessions

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.

If local user accounts are enabled, the **Active Sessions** section of the Firebox Users page shows information for all active sessions, including the name and IP address of the user who started the session.

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

Stop a session

The Firebox X Edge e-Series monitors and records the properties of each user session.

If the Automatic Session Termination time limit for all sessions is reached, or if the Firebox X Edge restarts, all sessions are stopped at the same time. The Edge administrator also can 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 Firebox X 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.

Active Sessions					
Active session total is 1. Number of user licenses in use: 0 (maximum is Unrestricted).					
User	Host	On-line Time	Idle Timeout	License	Close
admin	192.168.42.173	2 hr: 49 min	0 hr: 0 min	No	
Close All					

3. In the **Active Sessions** list, click the **Close** button adjacent to the session you want to stop. To stop all sessions, click the **Close All** button.

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

- The idle timeout limit set for that account is reached.
- The maximum time limit set for that account is reached.
- The authenticated 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.

Local User account

Below **Local User Accounts**, you can see information on the users you configured:

- **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.
- **Options:** You can configure a user to use WebBlocker, MOVPN (Mobile VPN with IPSec), PPTP (Mobile VPN with PPTP) and SSL (Mobile VPN with SSL).

Local User Accounts						
Name	Admin Level	WebBlocker	MUVPN	PPTP	Edit	Delete
admin	Full	No WebBlocker	Disabled	Disabled		
buffster	None	No WebBlocker	Disabled	Enabled		

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 [About user accounts](#).

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. You cannot delete the admin account.

Allow internal devices to bypass user authentication

You can make a list of internal devices that bypass user authentication settings. If a device is on this list, a user at that device does not have to authenticate to get access to the Internet. No WebBlocker rules apply to web traffic originating from devices on this list.

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

The screenshot shows the 'Trusted Hosts' page. At the top, the title 'Firebox Users' and the page name 'Trusted Hosts' are displayed. Below this, a table lists 'Trusted Hosts' with a single entry: '0.0.0.0'. To the right of the list is a vertical scroll bar. Below the list are buttons for 'Remove' and 'Add'. The 'Add' button is currently active. Below the list is a text input field labeled 'Host IP Address' containing '0.0.0.0', and an 'Add' button. A link 'Learn more about bypassing user authentication.' is also present. 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 device on your trusted or optional network to allow users to browse the Internet without authentication restrictions.
3. Click **Add**.
4. Repeat steps 2–3 for other trusted devices.
5. To remove a device from the list, select the address and click **Remove**.
6. Click **Submit** to save changes to the Firebox.

14 WebBlocker

About WebBlocker

If you give users unlimited web site access, your company can suffer lost productivity and reduced bandwidth. Uncontrolled Internet surfing can also increase security risks and legal liability. The WebBlocker security subscription gives you control of the web sites that are available to your users.

WebBlocker uses a database of web site addresses controlled by SurfControl, a leading web filter company. When a user on your network tries to connect to a web site, the Firebox 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.

WebBlocker works with the HTTP and HTTPS proxies to filter web browsing. If you have not configured an HTTP or HTTPS proxy, a proxy is automatically configured and enabled for you when you enable WebBlocker.

You must purchase the WebBlocker upgrade to use this feature. For more information, visit the WatchGuard LiveSecurity web site at <http://www.watchguard.com/store>.

Configure global WebBlocker settings

The first WebBlocker page in the Firebox X Edge e-Series configuration pages is the WebBlocker Settings page. Use this page to:

- Activate WebBlocker
- Set the full access password
- Set the inactivity timeout
- Set an action if the Edge cannot connect to the WebBlocker server
- Set an action if the WebBlocker license expires

To configure WebBlocker:

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X 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.

Enable WebBlocker for all HTTPS proxies

Enable WebBlocker for all HTTP proxies

Enable WebBlocker override

Full access password

Confirm password

Inactivity timeout (minutes)

When the WebBlocker Server is unavailable, access to all sites is

When the WebBlocker license expires, access to all sites is

Use a custom WebBlocker Server

Ip Address

Message for blocked user field:
To change the message users see when web access is blocked, edit your [HTTP proxy policy](#).

[Learn more about finding the category of a blocked web site](#)

3. Select the **Enable WebBlocker** check box to activate WebBlocker for HTTP or HTTPS.
4. If you want to allow users to bypass WebBlocker if they know the full access password, select the **Enable WebBlocker override** check box. Type a password in the **Full Access Password** field, and then type the same password again in the **Confirm 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. This feature operates only with HTTP proxy policies.

5. Type a number, in minutes, in the **Inactivity Timeout** field.
The **Inactivity Timeout** field 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 or HTTPS traffic is sent from that user's computer for the length of time set in the **Inactivity Timeout** field, WebBlocker rules start again. The value can be from 1 to 1440 minutes.
6. Use the **When the WebBlocker Server is unavailable, access to all sites** is drop-down list to select if the Firebox X Edge 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 X Edge to try to connect to the WebBlocker Server and time out. After 45 seconds, the Edge allows access to the web site. When the Edge can connect to the WebBlocker Server again, it will automatically start to apply WebBlocker rules again.
7. Use the **When the WebBlocker license expires, access to all sites** is drop-down list to select if the Firebox X Edge is to allow or deny all web traffic if the WebBlocker subscription expires.
If the WebBlocker subscription is renewed, the Firebox X Edge keeps the previous configuration and applies WebBlocker rules again.
8. By default, WebBlocker connects to a WebBlocker Server maintained by WatchGuard to check to see if a web site matches a WebBlocker category. If you prefer, you can install and maintain your own WebBlocker Server on your local network. If you have install WebBlocker Server on a computer in your local network, select the **Use a custom WebBlocker Server** check box. Type the IP address of the server in the adjacent text box.
For instructions on how to install your own WebBlocker Server, see [Install the Quarantine Server and WebBlocker Server](#).
9. Click **Submit**.



WebBlocker shows users a deny message when it blocks access to a web site. You can customize this message when you configure your HTTP proxy policy. For more information, see [HTTP proxy: Deny message](#).

Install the Quarantine Server and WebBlocker Server

To use the quarantine feature of spamBlocker or Gateway AntiVirus, or if you want to install and maintain your own WebBlocker Server, you must download and install the WatchGuard Quarantine Server and WebBlocker Server. You can install the server software on a computer with Windows 2003, Windows XP, or Windows Vista. We recommend at least 512 MB RAM, a 2.0 GHz processor and 60 GB disk space if you plan to install both servers on the same computer.

Download the server software

1. Use your browser to go to <http://www.watchguard.com/>.
2. Log in with your LiveSecurity Service user name and password.
3. Click the **Software Downloads** link.
4. Select your Firebox type and model number.
5. Download the WatchGuard Quarantine Server and WebBlocker Server for Edge software and save the file to a convenient location.

Install Quarantine Server and WebBlocker Server

Double-click `WGEedge10QWB.exe` to start the setup wizard. You may need to type a local administrator password to run the installer on some operating systems. Follow the instructions to install the software:

WatchGuard WebBlocker and Quarantine Server for Edge Setup

Click **Next** to start the wizard.

Read the license agreement

Select the **Accept** radio button, then click **Next**.

Set the destination folder

Click **Browse** to select a location to install the software, or click **Next**.

Select the components to install

Both servers are installed by default. If you do not want to install a server, clear the adjacent check box. When you are finished, click **Next**.

Configure WatchGuard Toolbar

Follow the instructions on the screen to activate your WatchGuard Toolbar. When you are finished, click **Next**. After the installation, you can start and stop the WebBlocker Server or the Quarantine Server with the WebBlocker Server and Quarantine Server icons on your WatchGuard Toolbar.

WatchGuard WebBlocker and Quarantine Server for Edge Setup

Click **Finish** to close the wizard.

About 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 must apply them when you set up Firebox X Edge user accounts. Even if you have only one set of WebBlocker rules, you must choose to apply the WebBlocker rules to each new user or group you create as described in [Create a WebBlocker profile](#).

Create a WebBlocker profile

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X 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

New Profile

Profile Name

Blocked Categories

<input checked="" type="checkbox"/> Adult	<input checked="" type="checkbox"/> Shopping
<input type="checkbox"/> Adult/Sexually Explicit	<input type="checkbox"/> Advertisements
<input type="checkbox"/> Alcohol & Tobacco	<input type="checkbox"/> Food & Drink
<input type="checkbox"/> Gambling	<input type="checkbox"/> Motor Vehicles
<input type="checkbox"/> Intimate Apparel & Swimwear	<input type="checkbox"/> Real Estate
<input type="checkbox"/> Sex Education	<input type="checkbox"/> Shopping
<input type="checkbox"/> Tasteless & Offensive	<input checked="" type="checkbox"/> Computers
<input checked="" type="checkbox"/> Crime	<input type="checkbox"/> Chat
<input type="checkbox"/> Criminal Activity	<input type="checkbox"/> Computing & Internet
<input type="checkbox"/> Hacking	<input type="checkbox"/> Hosting Sites
<input type="checkbox"/> Intolerance & Hate	<input type="checkbox"/> Proxies & Translators
<input type="checkbox"/> Violence	<input type="checkbox"/> Web-based Email
<input type="checkbox"/> Weapons	<input type="checkbox"/> Downloads
<input type="checkbox"/> Spyware	<input type="checkbox"/> Ringtones/Mobile Phone
<input type="checkbox"/> Phishing & Fraud	<input type="checkbox"/> Downloads
<input type="checkbox"/> Illegal Drugs	<input type="checkbox"/> Peer-to-Peer
<input checked="" type="checkbox"/> Entertainment	<input type="checkbox"/> Spam URLs
<input type="checkbox"/> Entertainment	<input type="checkbox"/> Infrastructure
<input type="checkbox"/> Games	<input checked="" type="checkbox"/> News
<input type="checkbox"/> Hobbies & Recreation	<input type="checkbox"/> News
<input type="checkbox"/> Kids Sites	<input type="checkbox"/> Blogs & Forums
<input type="checkbox"/> Sports	<input checked="" type="checkbox"/> Search
<input type="checkbox"/> Streaming Media	<input type="checkbox"/> Photo Searches
<input type="checkbox"/> Travel	<input type="checkbox"/> Search Engines
<input type="checkbox"/> Arts	<input checked="" type="checkbox"/> Research
<input checked="" type="checkbox"/> Personal	<input type="checkbox"/> Finance & Investment
<input type="checkbox"/> Education	<input type="checkbox"/> Government
<input type="checkbox"/> Society & Culture	<input type="checkbox"/> Health & Medicine
<input type="checkbox"/> Job Search & Career Development	<input type="checkbox"/> Reference
<input type="checkbox"/> Personals & Dating	<input type="checkbox"/> Politics
<input type="checkbox"/> Religion	<input type="checkbox"/> Business

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 that have worked at your company for less than 90 days.
5. In **Blocked Categories**, select the categories of web sites to block by selecting the check box adjacent to the category name.
For more information on categories, see [About WebBlocker categories](#). 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 are unselected.
6. Click **Submit**.

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



If you do not use user authentication, the default WebBlocker profile is applied to all users. For more information about user authentication, see topics under User and Group Management in the Table of Contents.

About WebBlocker categories

The WebBlocker database contains nine category groups, with 54 website categories.

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

The **Other** category includes new sites and categories released by SurfControl that are not yet part of a Firebox X Edge software update. The **Uncategorized** category includes sites that do not meet the criteria for any other category.

See whether a site is categorized

To see whether WebBlocker denies access to a web site as part of a category block, go to the Filter Testing and Submissions form on the SurfControl web site.

1. Open a web browser and go to <http://mtas.surfcontrol.com/mtas/WatchGuardTest-a-Site.asp>.
The WatchGuard Test-a-Site page appears.

2. Type the URL or IP address of the site to check.
3. Click **Test Site**.

The WatchGuard Test-a-Site Results page appears.

Add, remove, or change a category

If you receive a message that the URL you entered is not in the SurfControl list, you can submit it on the Test Results page.

1. Click **Submit A Site**.

The Submit A Site page appears.

WatchGuard Test-a-Site powered by SurfControl

SurfControl®

Submit-a-Site

Add a site

Do You Want To:

Delete a site

Change the category

URL (Internet Address):

http://

Choose Category:

None

Submit Reset

2. Select whether you want to **Add a site, Delete a site, or Change the category**.
3. Enter the site URL.
4. If you want to request that the category assigned to a site is changed, select the new category from the drop-down menu.
5. Click **Submit**.

About allowing sites to bypass WebBlocker

WebBlocker might deny a web site that is necessary for your business. You can override WebBlocker by defining a web site normally denied by WebBlocker as an *exception* to allow users to access it. For example, suppose 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 specify the web site's IP address or its domain name. You can also deny sites that WebBlocker normally allows.

WebBlocker exceptions apply only to HTTP traffic. If you deny a site with WebBlocker, the site is not automatically added to the Blocked Sites list.

To add WebBlocker exceptions, see [Add an allowed site](#) and [Add a denied site](#).

Add an allowed site

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

Allowed Sites	64.12.10.124	
<input type="button" value="Remove"/>		
Host IP Address	<input type="button" value="64.12.10.124"/>	<input type="button" value="Add"/>
<input type="button" value="Submit"/> <input type="button" value="Reset"/>		

3. Type the host IP address or domain name of the web site to allow.
4. Repeat step 3 for each additional host or domain name that you want 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.
5. Click **Add**.
The site is added to the Allowed Sites list.
6. Click **Submit**.

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

Add a denied site

1. From the navigation bar, select **WebBlocker > Denied Sites**.
The WebBlocker Denied Sites page appears.

Denied Sites	64.12.10.127
--------------	--------------

Host IP Address 64.12.10.127

2. From the drop-down list, select **Host IP Address** or **Domain Name/URL**
3. Type the host IP address or domain name of the denied web site.
4. Repeat step 3 for each additional host, IP address, or domain name you want 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 also can 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.
5. Click **Add**.
The site is added to the Denied Sites list.
6. Click **Submit**.

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

Allow internal hosts to bypass 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.

1. From the navigation bar, select **Firebox Users > Trusted Hosts**.

The Firebox Users Trusted Hosts page appears.

Firebox Users

Trusted Hosts

Trusted Hosts

Host IP Address Add

[Learn more about bypassing user authentication.](#)

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 users to browse the Internet without authentication restrictions.
3. Click **Add**.
4. Repeat step 2 for other trusted computers.
5. Click **Submit**.

To remove a computer from the list, select the address and click **Remove**.

15 spamBlocker

About spamBlocker

Unwanted email, also known as spam, fills the average inbox at an astonishing rate. A large volume of spam decreases bandwidth, degrades employee productivity, and wastes network resources. The WatchGuard spamBlocker option uses industry-leading pattern detection technology from Commtouch to block spam at your Internet gateway and keep it from getting to your email server.

Commercial mail filters use many methods to find spam. Blacklists keep a list of domains that are used by known spam sources or are open relays for spam. Content filters search for key words in the header and body of the email message. URL detection compares a list of domains used by known spam sources to the advertised link in the body of the email message. However, all of these procedures scan each individual email message. Attackers can easily bypass those fixed algorithms. They can mask the sender address to bypass a blacklist, change key words, embed words in an image, or use multiple languages. They can also create a chain of proxies to disguise the advertised URL.

spamBlocker uses the Recurrent-Pattern Detection (RPD) solution created by Commtouch to detect these hard-to-find spam attacks. RPD is an innovative method that searches the Internet for spam outbreaks in real time. RPD finds the patterns of the outbreak, not only the pattern of individual spam messages. Because it does not use the content or header of a message, it can identify spam in any language, format, or encoding. To see an example of real-time spam outbreak analysis, visit the Commtouch Outbreak Monitor at <http://www.commtouch.com/Site/ResearchLab/map.asp>.

spamBlocker also provides optional virus outbreak detection functionality. For more information, see [About Virus Outbreak Detection \(VOD\)](#).

spamBlocker requirements

Before you install spamBlocker, you must have:

- spamBlocker feature key. To get a feature key, contact your WatchGuard reseller or to the WatchGuard LiveSecurity web site at:
<http://www.watchguard.com/store>
- POP3 or SMTP email server. spamBlocker works with the WatchGuard POP3 and Incoming SMTP proxies to scan your email. If you have not configured the POP3 or SMTP proxy, they are enabled when you configure the spamBlocker service. If you have more than one proxy policy for POP3 or for SMTP, spamBlocker works with all of them.
- Connection to the Internet

About Virus Outbreak Detection (VOD)

Virus Outbreak Detection (VOD) is a technology that identifies email virus outbreaks worldwide within minutes. Provided by Commtouch, an industry leader in email spam and virus protection, VOD is incorporated into the spamBlocker security service. VOD uses traffic analysis technology to provide zero hour protection against viruses. If you use both spamBlocker and Gateway AntiVirus, the two features work together to keep viruses out of your network.

The VOD feature works on both SMTP and POP3 email traffic. If VOD detects a virus in a POP3 email message, the virus is automatically stripped from the message and the Edge generates a log message to tell you that a zero hour virus was detected. If VOD detects a virus in an SMTP email message, you can configure the Edge to automatically strip the virus, or to quarantine the email message.

spamBlocker actions, tags, and categories

The Firebox uses spamBlocker actions to apply decisions about the delivery of email messages. When a message is assigned to a category, the related action is applied.

Not all categories are supported when you use spamBlocker with the POP3 proxy.

Allow

Let the email message go through the Firebox normally.

Add a subject tag

Let the email message go through the Firebox, but insert text in the subject line of the email message to mark it as spam or possible spam. You can keep the default tags or you can customize them, as described in spamBlocker tags. You can also create rules in your email reader to sort the spam automatically, as described in [Create rules for your email reader](#).

Quarantine (SMTP only)

Send the email message to the Quarantine Server. Note that the **Quarantine** option is supported only if you use spamBlocker with the SMTP proxy. The POP3 proxy does not support this option.

Deny (SMTP only)

Stop the email message from being delivered to the mail server. The Firebox sends this 571 SMTP message to the sending email server: *Delivery not authorized, message refused*. The **Deny** option is supported only if you use spamBlocker with the SMTP proxy. The POP3 proxy does not support this option.

spamBlocker tags

If you select the spamBlocker action to add a tag to certain email messages, the Firebox adds a text string to the subject line of the message. You can use the default tags provided, or you can create a custom tag.

This example shows the subject line of an email message that was found to be spam. The tag added is the default tag: ***SPAM***.

Subject: ***SPAM*** Free auto insurance quote

This example shows a custom tag: [SPAM]

Subject: [SPAM] You've been approved!

spamBlocker categories

The Commtouch Recurrent-Pattern Detection (RPD) solution classifies spam attacks in its Anti-Spam Detection Center database according to severity. spamBlocker queries this database and assigns a category to each email message.

spamBlocker has three categories:

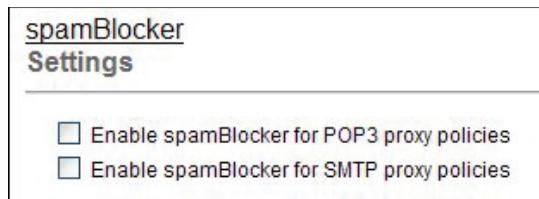
The **Confirmed** category includes email messages that come from known spammers. We recommend you use the **Deny** action for this type of email if you use spamBlocker with the SMTP proxy, or **Add a subject tag** if you use spamBlocker with the POP3 proxy.

The **Bulk** category includes email messages that do not come from known spammers, but do match some known spam structure patterns. We recommend you use the **Add subject tag** action for this type of email, or the **Quarantine** action if you use spamBlocker with the SMTP proxy.

The **Suspect** category includes email messages that look like they could be associated with a new spam attack. Frequently, these messages are legitimate email messages. We recommend that you consider a suspect email message as a "false positive" and therefore not spam unless you have verified that is not a false positive for your network. We also recommend that you use the **Allow** action for suspect email.

Enable spamBlocker

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



3. To enable spamBlocker for POP3, select the **Enable spamBlocker for POP3 proxy proxies** check box. To enable spamBlocker for SMTP, select the **Enable spamBlocker for SMTP proxy proxies** check box.

Configure spamBlocker

You set actions for spamBlocker to take with POP3 email and SMTP email in similar ways. To set actions for POP3 email, use the **POP3** tab; to set actions for SMTP email, use the **SMTP** tab.

1. At the top of the page, make sure that the **Enable spamBlocker for POP3/SMTP proxy policies** check boxes are selected.
2. To scan incoming and outgoing email for new viruses that may not be in the Gateway AntiVirus database, select the **Enable Virus Outbreak Detection (VOD) for POP3 and SMTP** check box.
For more information about Virus Outbreak Detection, see About Virus Outbreak Detection (VOD).

3. By default, VOD scans inbound email messages up to a 40 kilobyte limit. You can increase or decrease this limit with the **Limit VOD scanning to first** text box. If you configure a larger limit for spamBlocker as described in step 5, the larger limit is used.
If you type a very large number in this text box, your network throughput may be slow. We recommend that you keep the scan limit under 50 kilobytes (KB).
4. If spamBlocker VOD detects a virus in a POP3 message, the virus is automatically stripped. Use the **Virus is detected (SMTP only)** drop-down list to select the action you want spamBlocker to take if a virus is detected in an SMTP message.
5. At the bottom of the page, you can set the number of bytes of an email message that spamBlocker checks with the **Limit scanning to first** text box.
If you type a very large number in this text box, your network throughput may be slow. We recommend that you keep the scan limit under 50 kilobytes (KB).

spamBlocker
Settings

Enable spamBlocker for POP3 proxy policies
 Enable spamBlocker for SMTP proxy policies
 Enable Virus Outbreak Detection (VOD) for POP3 and SMTP

Limit VOD scanning to first kb

Virus is detected (SMTP or POP3 only)

POP3 **SMTP** **Common**

POP3 Actions

Confirmed	<input type="button" value="Allow"/>	<input type="text" value="*** SPAM ***"/>
Bulk	<input type="button" value="Allow"/>	<input type="text" value="*** BULK ***"/>
Suspect	<input type="button" value="Allow"/>	<input type="text" value="*** SUSPECT ***"/>

When the spamBlocker server is unavailable, access to POP3 email is:

Send log message for each email that does not fall into one of the above categories

Exceptions

Action	Sender	Recipient	Subject Tag	Up	Down	Remove	Add
<input type="button" value="Allow"/>				<input type="button" value="Up"/>	<input type="button" value="Down"/>	<input type="button" value="Remove"/>	<input type="button" value="Add"/>

Log all the actions

Limit scanning to first bytes

Learn more about [configuring spamBlocker](#).

Set POP3 email actions

1. From the **Confirmed** drop-down list, select **Allow** or **Add a subject tag**. The default action is **Allow**. If you choose **Add a subject tag**, a text box appears with the default tag *****SPAM*****. You can change this tag to some text you prefer.
2. From the **Bulk** drop-down list, select **Allow** or **Add a subject tag**. The default action is **Allow**. The default tag is *****BULK*****. You can change this tag to some text you prefer.
3. From the **Suspect** drop-down list, select **Allow** or **Add a subject tag**. The default action is **Allow**. The default tag is *****SUSPECT*****. You can change this tag to some text you prefer.
4. Use the **When the spamBlocker server is unavailable, access to POP3 email is** drop-down list to select whether the Firebox X Edge is to **Allow** or **Deny** all POP3 traffic when it cannot connect to the spamBlocker server. The default action is to **Allow**.



If you configure the Edge to deny POP3 email when it cannot contact the spamBlocker server, it causes a conflict with Microsoft Outlook. When Outlook starts a connection to the email server, spamBlocker tries to contact the spamBlocker server. If the spamBlocker server is not available, spamBlocker stops the email download. When this happens, a cycle starts. Outlook tries to download email and spamBlocker stops the download. This continues until the Edge can connect to the spamBlocker server, until the request is dropped because the proxy times out, or until you cancel the request.

5. Select the **Send log message for each email that does not fall into one of the above categories** check box to enable this logging option.

Set SMTP email actions

1. In the **Incoming Host IP** text box, type the IP address of the SMTP mail server you use for your network.
2. From the **Confirmed** drop-down list, select **Allow**, **Add a subject tag**, **Deny**, or **Quarantine**. The default action is **Allow**. If you choose **Add a subject tag**, a text box appears with the default tag *****SPAM*****. You can change this tag to some text you prefer.
3. From the **Bulk** drop-down list, select **Allow**, **Add a subject tag**, **Deny**, or **Quarantine**. The default action is **Allow**. The default tag is *****BULK*****. You can change this tag to some text you prefer.
4. From the **Suspect** drop-down list, select **Allow**, **Add a subject tag**, **Deny**, or **Quarantine**. The default action is **Allow**. The default tag is *****SUSPECT*****. You can change this tag to some text you prefer.
5. Use the **When the spamBlocker server is unavailable, access to SMTP email is** drop-down list to select whether the Firebox X Edge is to **Allow** or **Deny** all SMTP traffic when it cannot connect to the spamBlocker server. The default action is to **Allow**.



If you configure the Edge to deny SMTP email when it cannot contact the spamBlocker server, it causes a conflict with Microsoft Outlook. When Outlook starts a connection to the email server, spamBlocker tries to contact the spamBlocker server. If the spamBlocker server is not available, spamBlocker stops the email download. When this happens, a cycle starts. Outlook tries to download email and spamBlocker stops the download. This continues until the Edge can connect to the spamBlocker server, until the request is dropped because the proxy times out, or until you cancel the request.

6. Select the **Send a log message for each email classified as not spam** check box to enable this logging option.
7. If you selected **Quarantine** as an action for an email category above, type the IP address of your Quarantine Server in the **IP address** text box.

About spamBlocker exceptions

You can create an exception list to the general spamBlocker actions that is based on the sender's or recipient's address. For example, if you want to allow a newsletter that spamBlocker identifies as Bulk email, you can add that sender to the exception list and use the **Allow** action regardless of the spamBlocker category the sender is assigned to. Or, if you want to apply a tag to a sender that spamBlocker designates as safe, you can add that to the exceptions list as well.

Make sure you use the sender's actual address that is listed in the Mail-From field in the email message header, which may not match the address in the From: field that you see at the top of the email message. To get the actual address for an exception, get the full email message header (from Microsoft Outlook, with the message open, select

View > Options and look in the **Internet headers** box). The addresses of the sender and recipient are in these lines:

X-WatchGuard-Mail-From:
X-WatchGuard-Mail-Recipients:

Use care when you add wildcards to an exception. Spammers can spoof header information. The more specific the addresses in your exception list, the more difficult it will be to spoof them.

To change the order of the rules listed in the dialog box, see [Change the order of exceptions](#).

Create exceptions

To add sender or recipient exceptions to spamBlocker actions:

1. From the drop-down list beneath the **Action** column, select **Allow** or **Add a subject tag**.
2. In the text box below the **Sender** column, type the sender email address. You can use the asterisk (*) as a wild card. For example, if you type `*@watchguard.com`, the exception refers to any email address sent from the WatchGuard domain. You can also type only an asterisk in the text box if the exception applies to any sender.
3. In the text box below the **Recipient** column, type the recipient email address. You can use the asterisk(*) as a wild card. For example, if you type `*@watchguard.com`, the exception refers to any email address received by the WatchGuard domain. You can also type only an asterisk in the text box if the exception applies to any recipient.
4. If you select **Add a subject tag** as the action, type a tag in the text box below the **Subject Tag** column. This tag is added to the subject line of email messages that match this exception.
5. Click **Add** to enter the exception.
6. You can highlight an exception and click **Remove** to remove the exception.
7. You can change the precedence of the exception list. Select an exception, and then click **Up** or **Down** to adjust the precedence of that exception. For more information, see [Change the order of exceptions](#).
8. Click **Submit**.

Change the order of exceptions

The order that the exception rules are listed in the dialog box shows the order in which email messages are compared to the rules. The proxy compares messages to the first rule in the list and continues in sequence from top to bottom. When a message matches a rule, the Firebox performs the related action. It performs no other actions, even if the message matches a rule or rules later in the list.

To change the order of rules, select the rule whose order you want to change. Click the **Up** or **Down** button to move the rule up or down in the list.

About using spamBlocker with multiple proxies

You can configure more than one SMTP or POP3 proxy service to use spamBlocker. This lets you create custom rules for different groups in an organization. For example, you can allow all email to your management and use a spam tag for the marketing team.

If you want to use more than one proxy service with spamBlocker, your network must use one of these configurations:

- Each proxy policy must send email to a different internal email server.
- or
- You must set the external source or sources that can send email for each proxy policy.

Create rules for your email reader

To use the **Tag** action in spamBlocker, it is best to configure your email reader to sort messages. Most email readers, such as Outlook, Thunderbird, and Mac Mail, allow you to set rules that automatically send email messages with tags to a subfolder. Some email readers also let you create a rule to automatically delete the message.

Because you can use a different tag for each spamBlocker category, you can set a different rule for each category. For example, you can set one rule to move any email message with the ***BULK*** tag in the subject line to a Bulk subfolder in your inbox. You can set another rule that deletes any email message with the ***SPAM*** tag in the subject line.

For instructions on how to configure the Microsoft Outlook email client, see [Send spam or bulk email to special folders in Outlook](#). For information about how to use this procedure on other types of email clients, look at the user documentation for those products.



If you use spamBlocker with the SMTP proxy, you can have spam email sent to the Quarantine Server. For more information on the Quarantine Server, see [About the Quarantine Server](#).

Send spam or bulk email to special folders in Outlook

This procedure shows you the steps to create rules for bulk and suspect email in Microsoft Outlook. You can have email with a spam or bulk tag delivered directly to special folders in Outlook. When you create these folders, you keep possible spam email out of your usual Outlook folders, but you can get access to the email if it becomes necessary.

Before you start, make sure that you configure spamBlocker to add a tag for spam and bulk email. You can use the default tags, or create custom tags. The steps below describe how to create folders with the default tags.

1. From your Outlook Inbox, select **Tools > Rules and Alerts**.
2. Click **New Rule** to start the Rules wizard. Select **Start from a blank rule**.
3. Select **Check messages when they arrive**. Click **Next**.
4. Select the condition check box: **with specific words in the subject**. Then, in the bottom pane, edit the rule description by clicking on **specific**.
5. In the **Search Text** dialog box, type the spam tag as ***SPAM***. If you use a custom tag, type it here instead.
6. Click **Add** and then click **OK**.
7. Click **Next**.

8. The wizard asks what you want to do with the message. Select the **move it to the specified folder** check box. Then, in the bottom pane, click **specified** to select the destination folder.
9. In the **Choose a Folder** dialog box, click **New**.
10. In the folder name field, type `Spam`. Click **OK**.
11. Click **Next** two times.
12. To complete the rule setup, type a name for your spam rule and click **Finish**.
13. Click **Apply**.

Repeat these steps to create a rule for bulk email, using the bulk email tag. You can send bulk email to the same folder, or create a separate folder for bulk email.

Send a report about false positives or false negatives

A false positive email message is a legitimate message that spamBlocker incorrectly identifies as spam. A false negative email message is a spam message that spamBlocker does not correctly identify as spam. If you find a false positive or false negative email message, you can send a report directly to Commtouch. You can also send a report about a false positive for a solicited bulk email message. This is a message that spamBlocker identifies as bulk email when a user actually requested the email message.



Do not send a report a false positive when the email is assigned to the Suspect category. Because this is not a permanent category, Commtouch does not investigate error reports for suspected spam.

You must have access to the email message to send a false positive or false negative report to Commtouch. You must also know the category into which spamBlocker put the email message. If you do not know the category, see the "Find the category a message is assigned to" section below.

1. Save the email as a `.msg` or `.eml` file.
You cannot forward the initial email message because Commtouch needs the email header. If you use email software such as Microsoft Outlook or Mozilla Thunderbird, you can drag and drop the email message into a computer desktop folder. If you use email software that does not have drag-and-drop functionality, you must select **File > Save As** to save the email message to a folder.
2. Create a new email message addressed to:
`reportfp@blockspam.biz` for false positives
`reportfn@blockspam.biz` for false negatives
`reports@blockspam.biz` for false positive solicited bulk email
3. Type the following on the subject line of your email message:
`FP Report <Your Company Name> <Date of submission> for false positives`
`FN Report <Your Company Name> <Date of submission> for false negatives`
`FP Report <Your Company Name> <Date of submission> for false positive solicited bulk email`
4. Attach the `.msg` or `.eml` file to the email message and send the message.

If you have many messages to tell Commtouch about, you can put them all into one Zip file. Do not put the Zip file into a Zip archive. The Zip file can be compressed to only one level for Commtouch to analyze it automatically.

Use RefID record instead of message text

If you want to send a report to Commtouch send but cannot send the initial email message because the information in the message is confidential, you can use the RefID record from the email header instead. The RefID record is the reference number for the transaction between the Firebox and the Commtouch Detection Center.

spamBlocker adds an X-WatchGuard-Spam-ID header to each email. The header looks like this:

X-WatchGuard-Spam-ID: 0001.0A090202.43674BDF.0005-G-[gg8BuArWNRYK9/VKO3E51A==](#)

The long sequence of numbers and letters after X-WatchGuard-Spam-ID: part of the header is the RefID record.

Instead of attaching the initial email, put the RefID record in the body of your email message. If you have more than one email message you want to send a report about, put each RefID record on a separate line.

To see email headers if you use Microsoft Outlook:

1. Open the email message in a new window or select it in Outlook.
2. If you open the email in a separate window, select **View > Options**.
If you highlight the email in Outlook, right-click the email message and select **Options**.
The headers appear at the bottom of the Message Options window.

To see email headers if you use Microsoft Outlook Express:

1. Open the email message in a new window or highlight it in Outlook Express.
2. If you open the email in a separate window, select **File > Properties**.
If you highlight the email in Outlook Express, right-click the email and select **Properties**.
3. Click the **Details** tab to view the headers.

To see email headers if you use Mozilla Thunderbird:

1. Open the email messages in a new window.
2. Select **View > Headers > All**.

Find the category a message is assigned to

Tagging messages is the only way to know which category a message is assigned to. Change the action to **Add subject tag** and use a unique sequence of characters to add to the beginning of the email subject line. For more information on how to use spamBlocker tags, see [spamBlocker actions, tags, and categories](#).

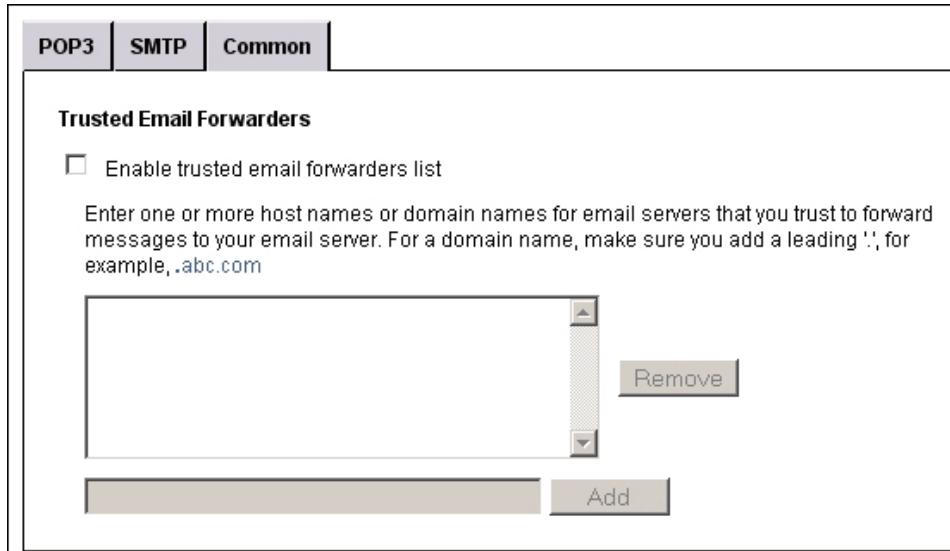
Add trusted email forwarders to improve spam score accuracy

Part of the spam score for an email message is calculated using the IP address of the server that the message was received from. If an email forwarding service is used, the IP address of the forwarding server is used to calculate the spam score. Because the forwarding server is not the initial source email server, the spam score can be inaccurate.

To improve spam scoring accuracy, you can enter one or more host names or domain names of email servers that you trust to forward email to your email server. After you add one or more trusted email forwarders, spamBlocker ignores the trusted email forwarder in email message headers. The spam score is calculated using the IP address of the source email server.

Add Trusted Email Forwarders

On the spamBlocker Settings **Common** tab, you can enter one or more host names or domain names of email servers that you trust to forward email to your email server.



16 Quarantine Server

About the Quarantine Server

The WatchGuard Quarantine Server provides a safe, full-featured quarantine mechanism for any email messages suspected or known to be spam or to contain viruses. This repository receives email messages from the SMTP proxy and are filtered by spamBlocker. Granular control allows you to configure preferences for mail disposition, storage allocations, and other parameters.



To quarantine spam email, the Quarantine Server operates only with the SMTP proxy and spamBlocker. If you do not use spamBlocker, or if you use spamBlocker with the POP3 proxy and not the SMTP proxy, you cannot use the Quarantine Server. To quarantine email that contains viruses, the Quarantine Server operates only with the SMTP proxy and Gateway AntiVirus.

The Quarantine Server provides tools for both users and administrators. Users get periodic email message notifications from the Quarantine Server that they have email stored on the Quarantine Server. Users can then click a URL in the email message to go to the Quarantine Server. On the Quarantine Server, they see the sender and the subject of the suspicious email messages. For spam email, they can release any email messages they choose to their email inbox and delete the others. Administrators can configure the Quarantine Server to automatically delete future messages from a specific domain or sender, or those that contain specific text in the subject line.

You can see statistics on Quarantine Server activity, such as the number of messages quarantined during a specific range of dates, or the number of suspected spam messages.

The Quarantine Server has several classifications for quarantined messages:

- Suspected spam: Could be spam, but not enough information to decide.
- Confirmed spam: Definitely spam.
- Bulk: The message is part of a commercial bulk mailing.
- Virus: The message has a high probability of containing a virus.
- Possible virus: The message may contain a virus.

Install the Quarantine Server and WebBlocker Server

To use the quarantine feature of spamBlocker or Gateway AntiVirus, or if you want to install and maintain your own WebBlocker Server, you must download and install the WatchGuard Quarantine Server and WebBlocker Server. You can install the server software on a computer with Windows 2003, Windows XP, or Windows Vista. We recommend at least 512 MB RAM, a 2.0 GHz processor and 60 GB disk space if you plan to install both servers on the same computer.

Download the server software

1. Use your browser to go to <http://www.watchguard.com/>.
2. Log in with your LiveSecurity Service user name and password.
3. Click the **Software Downloads** link.
4. Select your Firebox type and model number.
5. Download the WatchGuard Quarantine Server and WebBlocker Server for Edge software and save the file to a convenient location.

Install Quarantine Server and WebBlocker Server

Double-click `WGEdge10QWB.exe` to start the setup wizard. You may need to type a local administrator password to run the installer on some operating systems. Follow the instructions to install the software:

WatchGuard WebBlocker and Quarantine Server for Edge Setup

Click **Next** to start the wizard.

Read the license agreement

Select the **Accept** radio button, then click **Next**.

Set the destination folder

Click **Browse** to select a location to install the software, or click **Next**.

Select the components to install

Both servers are installed by default. If you do not want to install a server, clear the adjacent check box. When you are finished, click **Next**.

Configure WatchGuard Toolbar

Follow the instructions on the screen to activate your WatchGuard Toolbar. When you are finished, click **Next**. After the installation, you can start and stop the WebBlocker Server or the Quarantine Server with the WebBlocker Server and Quarantine Server icons on your WatchGuard Toolbar.

WatchGuard WebBlocker and Quarantine Server for Edge Setup

Click **Finish** to close the wizard.

Start the Quarantine Server

To start the Quarantine Server, you must:

- [Install Quarantine Server](#)
- [Run the Setup Wizard](#)
- [Define the server location](#)

Install server components

You can install Quarantine Server as part of WatchGuard System Manager, or as part of a special installer for Firebox X Edge users. When you run the installer, you are asked which client and server components you want to install. Under the Server Components section, make sure you select Quarantine Server.

If you have already run the Quarantine Server and WebBlocker Server installer but you did not install the Quarantine Server, you can run the installer again. For more information, see [Install the Quarantine Server and WebBlocker Server](#).

After you install the Quarantine Server, run the Quarantine Server Setup Wizard. For more information, see [Run the Setup Wizard](#).

Run the Setup Wizard

Right-click the Quarantine Server icon (middle icon) in the System Tray and select **Start Service**.

The Quarantine Server Setup Wizard starts.

Click through the wizard and add the information it asks for.

Create a master passphrase

The master passphrase encrypts all server data.

Create a server manager passphrase

You will be prompted for this passphrase whenever you click a menu choice to configure the server and its users.

Identify your organization name

The Quarantine Server Setup Wizard is complete

You can now define the server location, as described in [Define the server location](#).

Define the server location

You must tell the Firebox where the Quarantine Server is located. The Firebox will send email messages to this location to be quarantined.

If you use the Quarantine Server to quarantine spam messages detected by spamBlocker, add the IP address of the Quarantine Server on the **spamBlocker > Settings** page, **SMTP** tab.

If you use the Quarantine Server to quarantine emails with viruses detected by Gateway AntiVirus, add the IP address of the Quarantine Server on the **Gateway AV/IPS > Settings** page.

Configure the Quarantine Server

When you configure the Quarantine Server, you have these options:

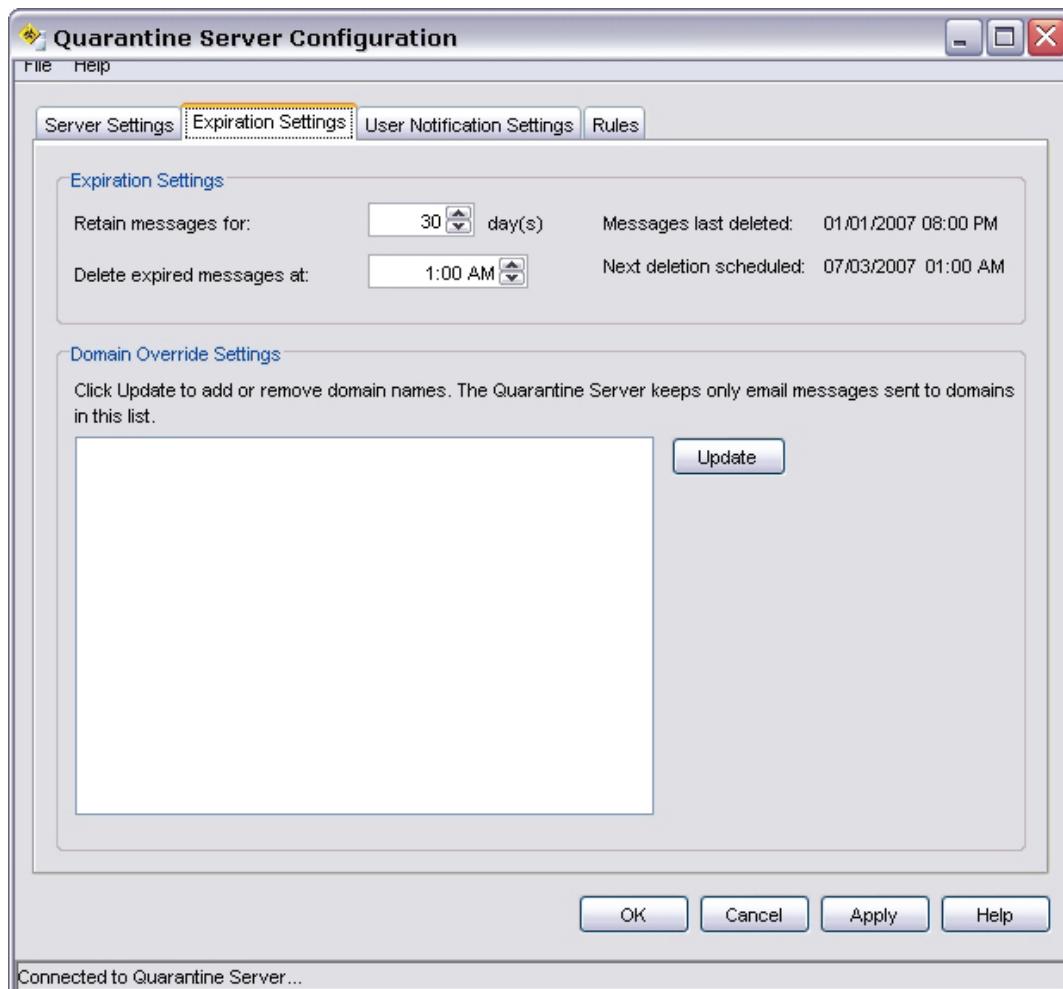
- [Set general server parameters](#)
- [Change the expiration and user domain settings](#): When to delete or how long to keep messages, and add and delete user domains. Only users in the domains that are in this list can have their messages sent to the Quarantine Server.
- [Change notification settings](#): The message sent to users that tells them they have messages on the Quarantine Server.
- [Change logging settings](#)
- [Change Quarantine Server rules](#): Add, change, or delete rules that determine messages to that the Quarantine Server will automatically delete.

Set general server parameters

1. To open the **Quarantine Server Configuration** dialog box, right-click  and select **Configure**.
2. Type the server management passphrase. This is the server management passphrase you created in the second screen of the Quarantine Server Setup Wizard or when you configured your Management Server.
The Quarantine Server Configuration dialog box appears.
3. To change the default maximum database size of 10000 MB, type a new value in the **Maximum database size** field. The current database size and available space appear to the right of this field. When the Quarantine Server runs out of drive space, it refuses to accept new messages and drops any subsequent email messages it receives.
4. You can specify that you want to be warned when the database approaches its limit. Select the **Send a warning if the database reaches the warning threshold** check box. Use the arrows to specify the warning threshold, and type the email address of the person to receive the warning in the **Send warning message to** field.
For example, if you select the check box, use the default warning threshold of 90%, and use the default maximum database size of 10000 MB (10 GB), the Quarantine Server sends the warning message when 9000 MB have been used and only 1000 MB are available.
5. In the **Outgoing email server** field, type the address of the outgoing SMTP email server.
6. If your email server requires authentication, select the **User login information for the E-mail server** check box and type the user name and password for the email server. If the user name and password are not required for your SMTP server, keep the fields blank.

Change expiration settings and user domains

1. To open the **Quarantine Server Configuration** dialog box, right-click  and select **Configure**. Type the server management passphrase. This is the server management passphrase you created in the second screen of the Quarantine Server Setup Wizard or when you configured your Management Server.
The Quarantine Server Configuration dialog box appears.
2. From the **Quarantine Server Configuration** dialog box, click the **Expiration Settings** tab.



3. In the **Retain messages for** field, specify the number of days to maintain messages on the Quarantine Server.
4. In the **Delete expired messages at** field, enter the time of day to delete expired messages after the period of time in the previous field.

Add or remove user domains

The **Expiration Settings** tab of the **Quarantine Server Configuration** dialog box shows the domain names for which the Quarantine Server will accept email messages. Only users in the domains that are in the list can have messages sent to the Quarantine Server for them. Messages sent to users that are not in one of these domains are deleted.

1. To add or remove a domain name from the server, click **Update**.
The Add Domains dialog box appears.



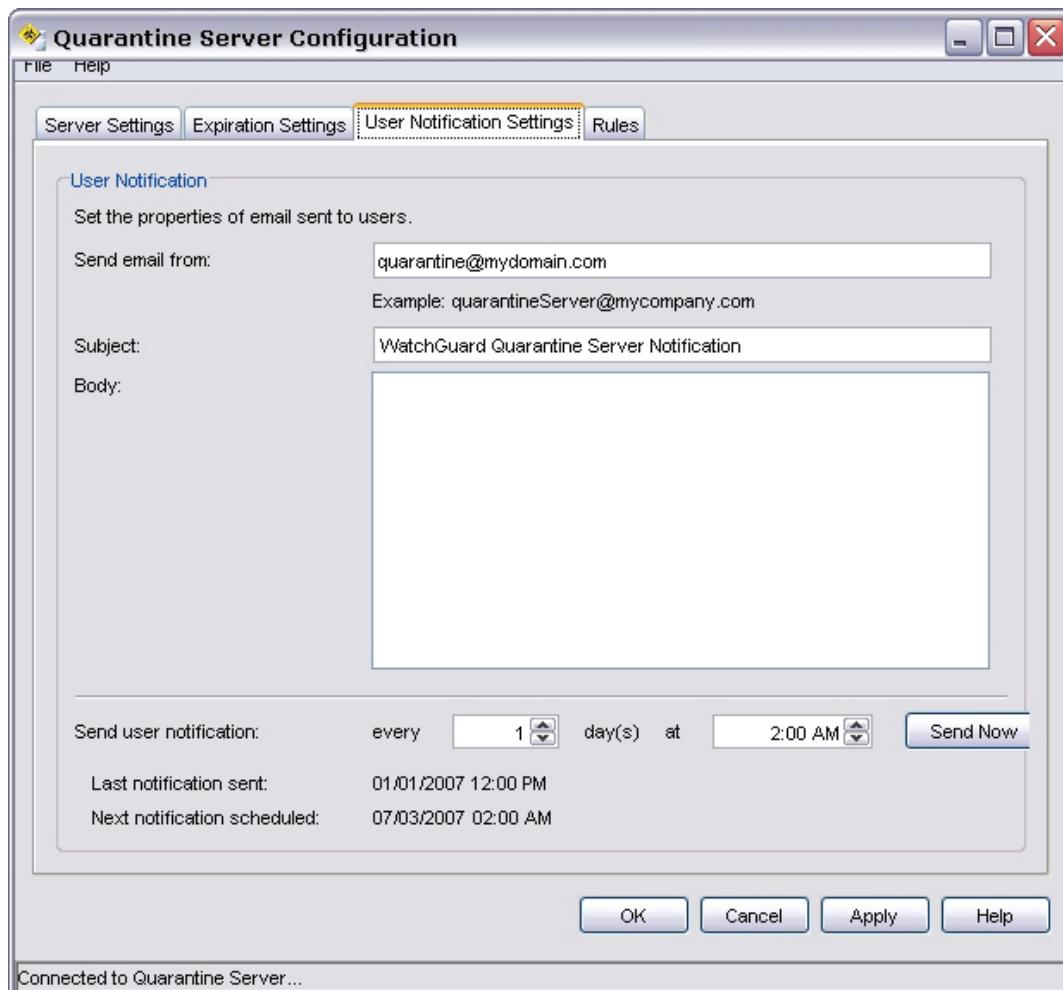
2. To add a domain, type it in the top field and click **Add**.
3. To remove a domain, select it from the list and click **Remove**.

Change notification settings

Users receive periodic email messages on their email client that include a list of the messages currently stored for them on the Quarantine Server. You can specify the account from which these messages are sent. You can also specify the title and body of the message. You can configure the interval for which the Quarantine Server sends notifications, although it cannot be more than once a day. You can also set the hour and minute of the day.

1. To open the **Quarantine Server Configuration** dialog box, right-click  and select **Configure**.
2. Type the server management passphrase. This is the server management passphrase you created in the second screen of the Quarantine Server Setup Wizard or when you configured your Management Server.
The Quarantine Server Configuration dialog box appears.

3. From the **Quarantine Server Configuration** dialog box, click the **User Notification Settings** tab.



4. To enable or disable notification (and the fields on this dialog box), use the **Send notification to users** check box.

5. In the **Send email from** field, type the full email address of the account you want to send from.

6. In the **Subject** field, type a name for the subject of the notification messages. The default is *WatchGuard Quarantine Server Notification*.

7. In the **Body** field, type the body of the notification message. You can use either text or HTML to specify the message body.

8. Next to **Send user notification**, enter a time interval for notification and the time of day you want the notifications sent. If you want to immediately send notifications to all users, click **Send Now**.



Some email readers might flag the notification message sent by the Quarantine Server as a scam or phishing attempt. This is because these readers classify any URL that uses an IP address as suspect. The URL that gives users access to the Quarantine Server includes the IP address of the Quarantine Server instead of a host name.

Change logging settings

You can enable or disable logging for the server, and define where the server will send log messages.

To open the configuration dialog box:

1. Right-click the icon for the server and select **Configure**.
2. Type the management server passphrase when prompted.
3. From the dialog box that appears, click the **Logging** tab.

Enable or disable logging

If you want the server to send log messages to one or more WatchGuard Log Servers, select the **Enable log messages to WatchGuard log server** check box.

Add or prioritize Log Servers

1. If you want to add Log Servers for the server, click **Add**.
2. You can create a priority list for Log Servers. If the Firebox cannot connect to the Log Server with the highest priority, it connects to the next Log Server in the priority list. If the Firebox examines each Log Server in the list and cannot connect, it tries to connect to the first Log Server in the list again. To change the priority list, select a Log Server from the list and click the **Up** and **Down** buttons.
3. With the **Select a log level** drop-down list, you can assign a level to the log messages sent by the server: **Error**, **Warning**, **Informational**, or **Debug**.

Send messages to the Windows Event Viewer

Event Viewer is a Windows program that keeps records of events that occur in the applications running on your computer. To control whether the server sends messages to this program, use the **Send the log messages to Windows event viewer** check box.

Use the **Select a log level** drop-down list to assign a level to the log messages sent by the server to the Event Viewer: **Error**, **Warning**, **Informational**, or **Debug**.

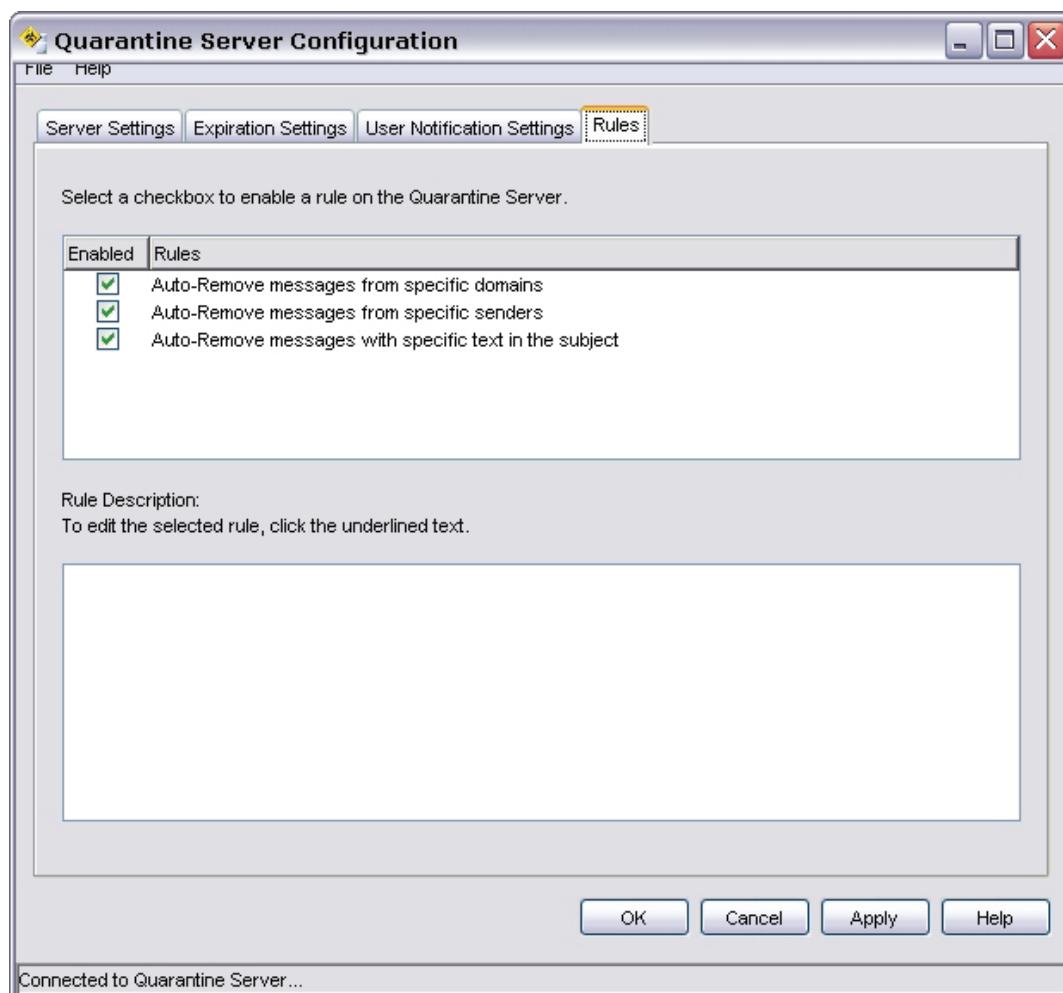
Send messages to a file

To control whether the server sends log messages to a file, use the **Send the log messages to a file** check box. Define the location of the file to receive the log message, and use the **Select a log level** drop-down list to assign a level to the log messages.

Change Quarantine Server rules

You set up rules to automatically remove certain messages if they come from a specific domain or sender, or if they contain specific text strings in the subject line.

1. To open the **Quarantine Server Configuration** dialog box, right-click  and select **Configure**.
2. Type the server management passphrase. This is the server management passphrase you created in the second screen of the Quarantine Server Setup Wizard or when you configured your Management Server.
The Quarantine Server Configuration dialog box appears.
3. From the **Quarantine Server Configuration** dialog box, click the **Rules** tab.
4. To modify a rule, select it.
The description of the rule appears in the Rules Description block.



5. Click the underlined words in the rule to add a specific domain, sender, or text string in the subject line.
The Edit Auto-Remove Rule dialog box appears.



6. To add a new domain, sender, or string, type it in the top box and click **Add**.
7. To remove a domain, sender, or string, select it in the bottom box and click **Remove**.

Note the following restrictions on modifying rules:

- Rules do not support wildcard characters. For example, you cannot enter the rule Auto-Remove messages from *.gov to auto-remove all domains with the .gov extension.
- When you remove a domain, sender, or string, Quarantine Server deletes only subsequent email messages that match this rule. It does not delete current messages in the database.
- Rules that auto-block messages with a specific text string apply only to text in the subject line. If the specified text is contained in the body of the message, but not in the subject line, the message is not removed.

Manage messages

You can see all messages on the Quarantine Server in a dialog box. You can sort messages by user, quarantine status, sender, subject, and date/time received.

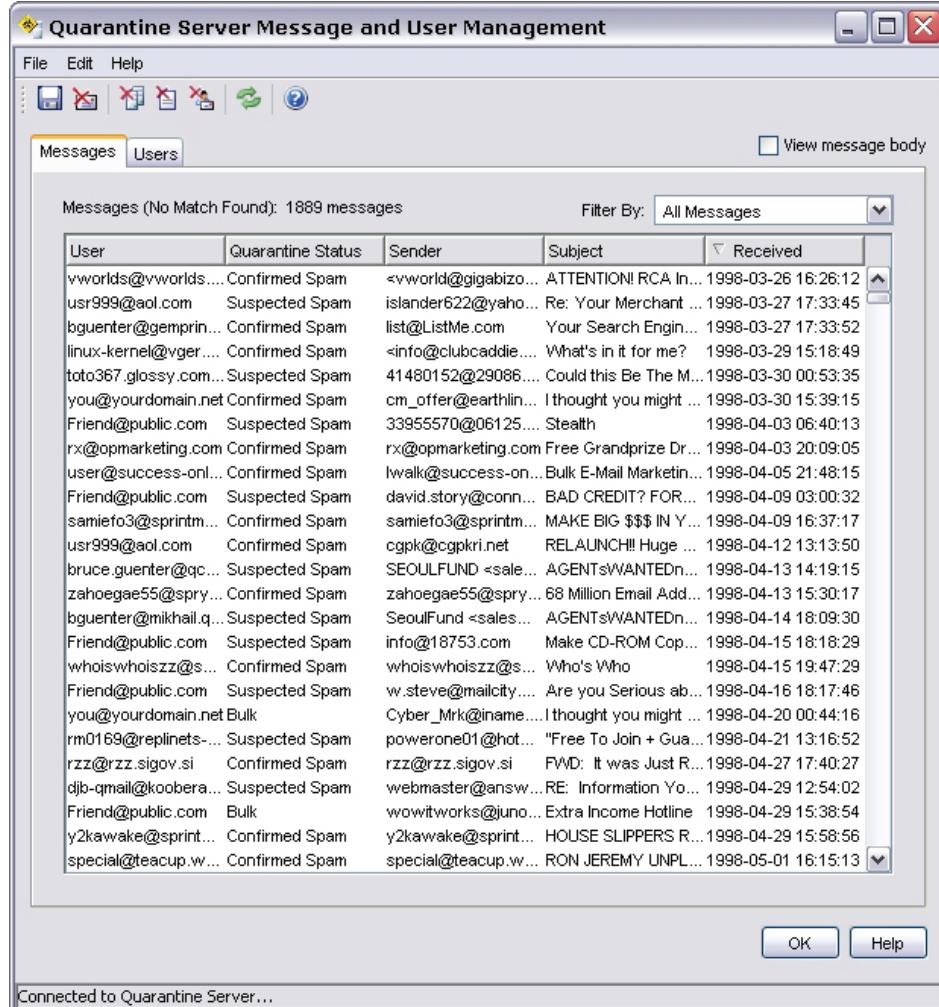


You can only have one Quarantine Server dialog box open at a time. After you are done with one Quarantine Server dialog box, you must close it before you open a new one.

Open the messages dialog box

1. Right-click  and select **Manage Messages**.
2. Type the server management passphrase.

The Quarantine Server Message and User Management dialog box appears.



Set viewing options

You can use the **Filter By** drop-down list to see all messages or only those with a particular quarantine status.

To see the body of a message, select the **View message body** check box. Select any message. A second pane appears at the bottom of the dialog box that shows the message body. You can also select any message and click **Edit > View Message Body**, or right-click any message and select **View Message Body**.

Save messages or send to a user's inbox

If you want to keep a message on the Quarantine Server, you save it to a file.

1. On the **Messages** tab of the **Quarantine Server Message and User Management** dialog box, select the message you want to save. You can save only one message at a time.
2. Click . Or, select **File > Save As**. Or, right-click the message and select **Save As**.
3. Type or select the location where you want to save the file. Click **Save**.

To send a message to a user's inbox, select **File > Release Message**.

Only spam email messages can be released to users. Messages that contain or may contain viruses cannot be released to users.

Delete messages manually

1. On the **Messages** tab of the **Quarantine Server Message and User Management** dialog box, select the message or messages you want to delete.
 - o To select a range of messages, click the first in the range, press the **Shift** key, and click the last message in the range.
 - o To select multiple messages that are not in a range, hold down **Ctrl** as you select messages.
 - o To select all messages, select **Edit > Select All**. Or, right-click any message and select **Select All**.
2. Click . Or, select **Edit > Delete**.

Delete messages automatically

You can specify to automatically delete all future email messages from a particular domain or sender, or that contain certain text in the subject line. All subsequent email to any user with this characteristic is automatically deleted before it is sent to the Quarantine Server.

1. On the **Messages** tab of the **Quarantine Server Message and User Management** dialog box, select the message or messages associated with the characteristic you want to automatically delete.
 - o To select a range of messages, click the first in the range, press the **Shift** key, and click the last message in the range.
 - o To select multiple messages that are not in a range, hold down **Ctrl** as you select messages.
 - o To select all messages, select **Edit > Select All**. Or, right-click any message and select **Select All**.
2. Choose the appropriate options for deletion.
 - o From the **Edit** menu, select **Auto-Remove > Sender Domain**, **Auto-Remove > Sender**, or **Auto-Remove > Subject**. These options are also available from the right-click (context) menu.
 - o You can also use the equivalent icons to select these options.

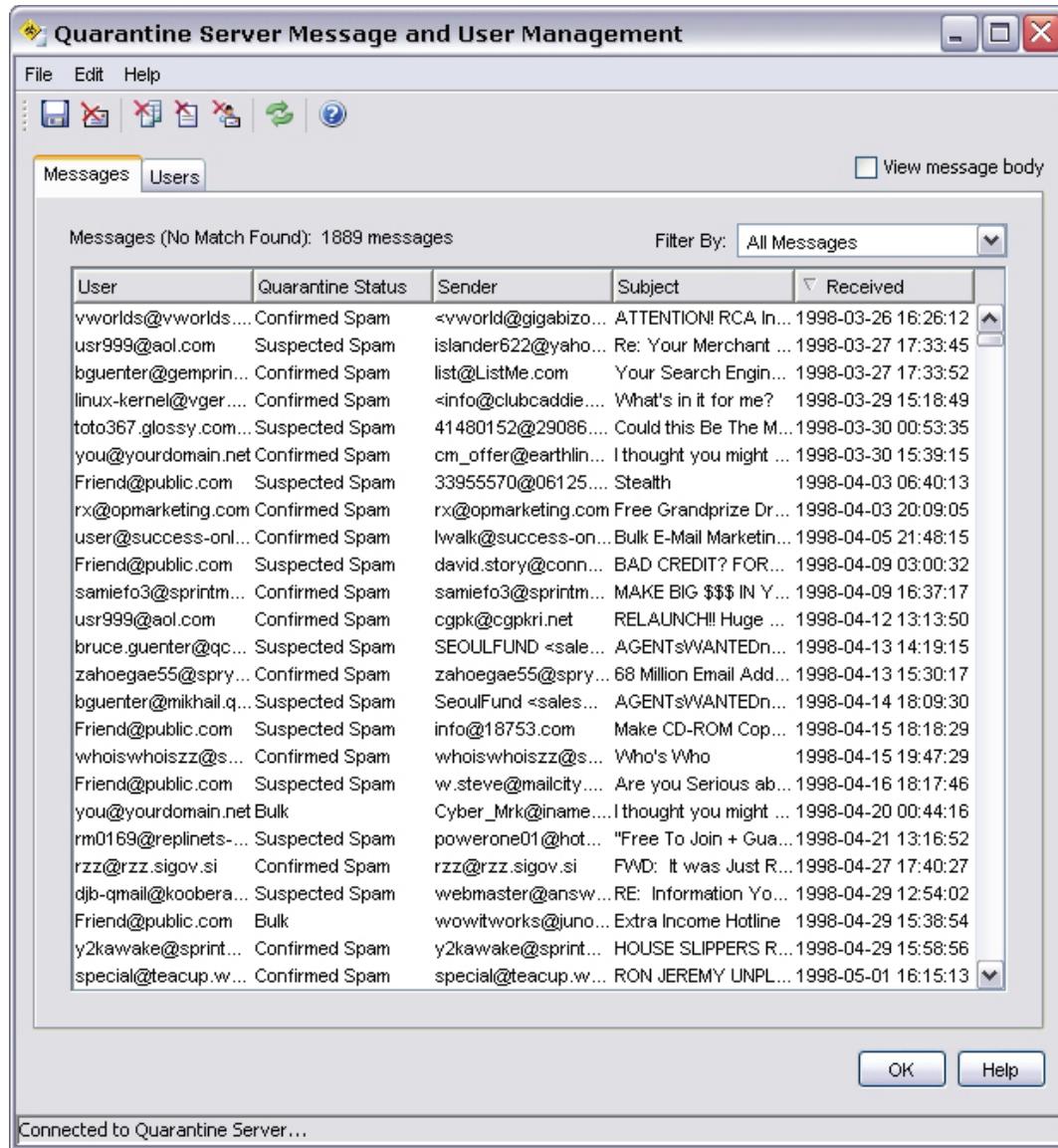
Open the messages dialog box



You can only have one Quarantine Server dialog box open at a time. After you are done with one Quarantine Server dialog box, you must close it before you open a new one.

1. Right-click the Quarantine Server icon and select **Manage Messages**.
2. Type the server management passphrase.

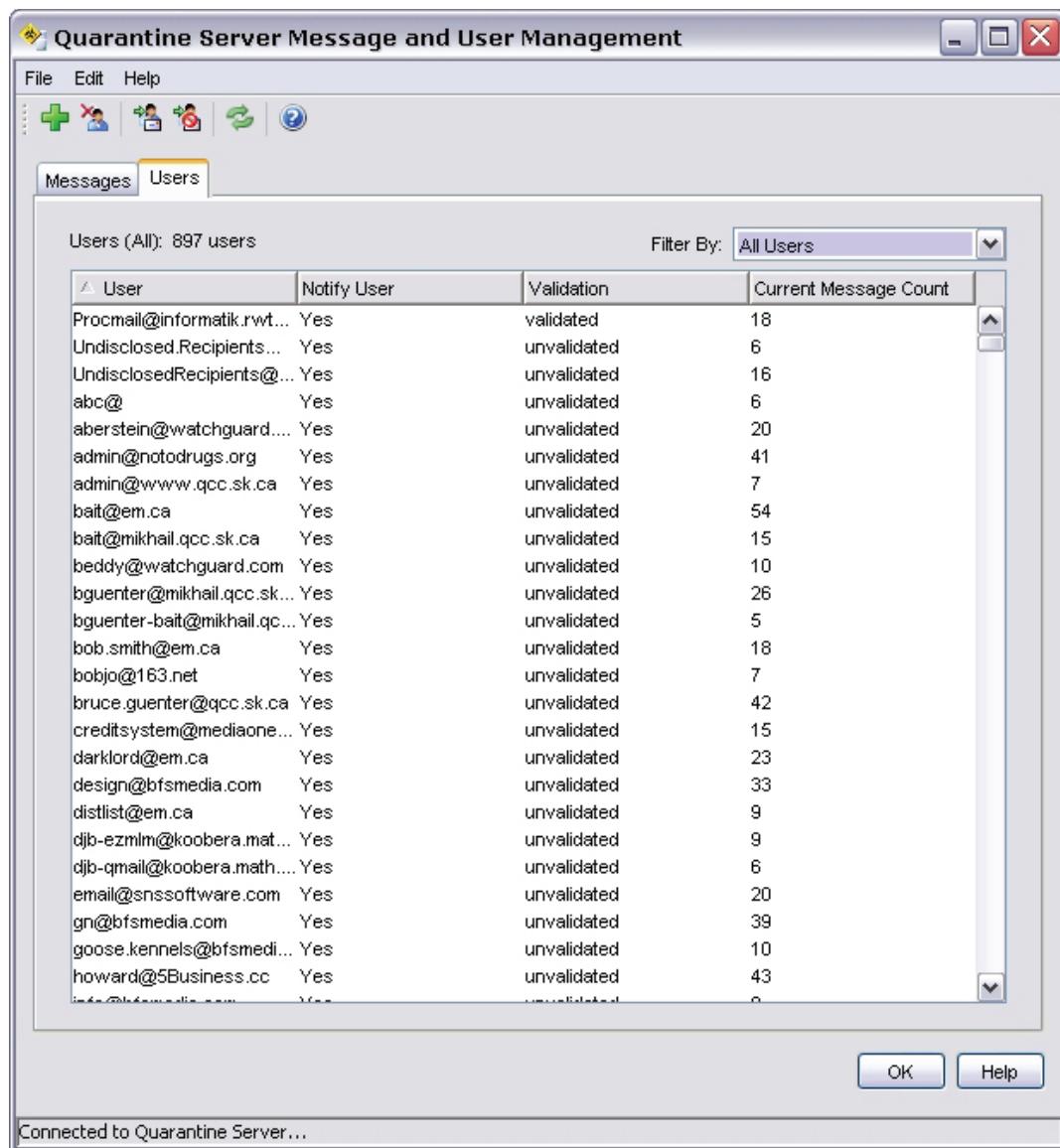
The Quarantine Server Message and User Management dialog box appears.



About managing users

You add, delete, and configure users from the **Users** tab of the **Quarantine Server Message and User Management** dialog box. This dialog box shows:

- Email addresses of users that can have email messages sent to the Quarantine Server.
- Whether users are notified when they have email on the Quarantine Server.
- Whether users are validated or unvalidated. A user is validated when he or she gets a message in an email client about messages on the Quarantine Server, and the user clicks the link to go to the Quarantine Server. Many users shown on the Quarantine Server will never be validated because the email address is created by a spammer and does not match an actual user.
- The number of messages currently on the Quarantine Server that are addressed to that user. If you want to see only validated or unvalidated users, from the **Filter by** drop-down list, select **Validated Users** or **Unvalidated Users**.



Add users

Users are automatically added when messages are sent to the Quarantine Server for them. Use this procedure to manually add users:

1. From the **Quarantine Server Message and User Management** dialog box, click the **Users** tab. Select **Edit > Add User**.

The Add User dialog box appears.



2. Type the full email address of the user, such as `myname@mydomain.com`.
3. Select the **Send notification for this user** or **Do not send notification** radio button to specify whether you want the user to be notified whenever the Quarantine Server receives a message for him or her.
4. Click **OK**.

Remove users

When you remove a user, all email messages stored on the Quarantine Server for that user are also deleted.

1. From the **Quarantine Server Message and User Management** dialog box, click the **Users** tab.
2. Select the user you want to delete and click .

Or, select **Edit > Delete**.

Change the notification option for a user

You can set or change whether you want to notify users when they have email messages on the server.

1. From the **Quarantine Server Message and User Management** dialog box, click the **Users** tab.
2. To enable notification for a user, select the user and click .

Or, select **Edit > Notify User > Yes**.

3. To disable notification for a user, select the user and click .

Or, select **Edit > Notify User > No**.

Get statistics on Quarantine Server activity

Quarantine Server statistics include those messages that have been deleted, either manually or automatically.



You can only have one Quarantine Server dialog box open at a time in this release of WatchGuard System Manager. After you are done with one Quarantine Server dialog box, you must close it before you open a new one.

1. Right-click and select **View Statistics**.
2. Type the server management passphrase.
The Quarantine Server Statistics dialog box appears.

See statistics from specific dates

You can limit the statistics to those from a specific range of dates:

1. From the **Quarantine Server Statistics** dialog box, select the **Select dates** radio button.
2. Type the start and end dates in the **From** and **To** fields.

See specific types of messages

You can specify whether you want to see statistics only for messages that are suspected spam, confirmed spam, or part of bulk mailings, or that contain or possibly contain viruses. Select the **Select only these messages** radio button and then choose the type or types of messages you want to see.

Group statistics by month, week, or day

By default, only summary data is shown. You can specify that you want the data grouped by month, week, or day.

1. From the **Quarantine Server Statistics** dialog box, select the **Break the data into groups** radio button.
2. Select either the **By Month**, **By Week**, or **By Day** radio button.

Export and print statistics

To export Quarantine Server statistics to a Microsoft Excel spreadsheet (.xls format):

From the **Quarantine Server Statistics** dialog box, select **File > Export to Excel**.

To export Quarantine Server statistics to comma-separated values (CSV) format:

From the **Quarantine Server Statistics** dialog box, select **File > Export to Csv**.

To print Quarantine Server statistics:

From the **Quarantine Server Statistics** dialog box, select **File > Print**.

17 Gateway AntiVirus and Intrusion Prevention Service

About Gateway AntiVirus and Intrusion Prevention

Hackers use many methods to attack computers on the Internet. The two primary categories of attack are viruses and intrusions.

Viruses, including worms and Trojans, are malicious computer programs that self-replicate and put copies of themselves into other executable code or documents on your computer. When a computer is infected, the virus can destroy files or record key strokes.

Intrusions are direct attacks on your computer. Usually the attack exploits a vulnerability in an application. These attacks are created to cause damage to your network, get sensitive information, or use your computers to attack other networks.

To help protect your network from viruses and intrusions, you can purchase the optional Gateway AntiVirus/Intrusion Prevention Service (Gateway AV/IPS) for the Firebox to identify and prevent attacks. Intrusion Prevention Service and Gateway AntiVirus operate with the SMTP, POP3, HTTP, FTP, and TCP-UDP proxies. When a new attack is identified, the features that make the virus or intrusion attack unique are recorded. These recorded features are known as the signature. Gateway AV/IPS uses these signatures to find viruses and intrusion attacks when they are scanned by the proxy.



WatchGuard cannot guarantee that Gateway AV/IPS can stop all viruses or intrusions, or prevent damage to your systems or networks from a virus or intrusion attack.

You must purchase the Gateway AV/IPS upgrade to use these services. For more information, visit the WatchGuard LiveSecurity web site at <http://www.watchguard.com/store> or contact your WatchGuard reseller.

You can see statistics on current Gateway AntiVirus and Intrusion Prevention Service activity on the Gateway AV/IPS page, and trend reporting for Gateway AV/IPS on the **System Status > Security Services** page.

New viruses and intrusion methods appear on the Internet frequently. To make sure that Gateway AV/IPS gives you the best protection, you must update the signatures frequently. You can configure the Firebox to update the signatures automatically from WatchGuard, as described in [Update Gateway AV/IPS](#).

About Gateway AntiVirus settings

WatchGuard Gateway AntiVirus (Gateway AV) stops viruses before they get to computers on your network. Gateway AV operates with the WatchGuard SMTP, POP3, HTTP, and FTP proxies. When you enable Gateway AV, the SMTP, POP3, HTTP, and FTP proxy looks at various types of traffic and performs an action that you specify.

Gateway AntiVirus scans different types of traffic according to which proxy or proxies you use the feature with:

- If you enable Gateway AntiVirus with the SMTP or POP3 proxy, it finds viruses encoded with frequently used email attachment methods. These include base64, binary, 7-bit, 8-bit encoding, and uuencoding. You can also use Gateway AV and the SMTP proxy to send virus-infected email to the Quarantine Server.
- If you enable Gateway AntiVirus with the HTTP proxy, it finds viruses in web pages that users try to download.
- If you enable Gateway AntiVirus with the FTP proxy, it finds viruses in uploaded or downloaded files.

POP3 proxy deny messages and Gateway AV/IPS

It is important to know what your users see when an email message is blocked because of the POP3 proxy. You can find a complete description of the actions taken by the POP3 proxy in an FAQ you can find at <http://www.watchguard.com/support/faqs/edge/>.

Some of the actions include:

- Send a message that an email message was denied when it blocks a message because of a problem in the header, or because of the body or attachment content, and the message is less than 100 kilobytes.
- Truncate an email message when it blocks a message because of a problem with the body or attachment content, and the message is larger than 100 kilobytes.
- Block an email message with no notification to the user when an email message is blocked because of a protocol anomaly.

You can see deny messages for all blocked email in the log messages. For information on using the log message tool, see [To see the event log file](#).



Signatures for Gateway AV are not automatically updated by default. To make sure Gateway AV has current signatures, see [Update Gateway AV/IPS](#).

Configure Gateway AV

1. To connect to the System Status page, type `https://` in the browser address bar, followed by the IP address of the Firebox X Edge trusted interface.
The default URL is: https://192.168.111.1
2. From the navigation bar, select **Gateway AV/IPS > Settings**.

Gateway AV/IPS
Settings

Gateway AntiVirus

Enable Gateway AntiVirus for SMTP
 Enable Gateway AntiVirus for POP3
 Enable Gateway AntiVirus for FTP
 Enable Gateway AntiVirus for HTTP

Virus is detected for SMTP: Strip
When an error is encountered: Remove

Limit Scanning to first: 512 kb

Quarantine Server IP address: []

3. Select the **Enable Gateway AntiVirus for SMTP** check box to scan email sent to an email server protected by your Edge for viruses.
4. Select the **Enable Gateway AntiVirus for POP3** check box to scan email downloaded from the email server for viruses.
5. Select the **Enable Gateway AntiVirus for FTP** check box to scan file transfer traffic for viruses.
6. Select the **Enable Gateway AntiVirus for HTTP** check box to scan HTTP content for viruses.
7. If you enable Gateway AntiVirus for SMTP, use the **Virus is detected (SMTP only)** drop-down list to select whether you want the Edge to remove (strip) viruses from email messages when they are found or to quarantine the email message. You must have a WatchGuard Quarantine Server installed to use the **Quarantine** option.
8. There is a very large set of file formats used on the Internet. Use the **When an error is encountered** drop-down list to select the action you want Gateway AV to take when it cannot successfully scan a file. The default action is **Remove**.

9. Select the **Limit Scanning** check box if you want the Gateway AV service to stop scanning each file after it examines the specified number of kilobytes. This improves the performance of the Edge. Most viruses are small and many are in the first hundred kilobytes of a file. You must select the correct balance of performance and security for your network.
10. If you have downloaded, installed, and configured a WatchGuard Quarantine Server, type the IP address of the Quarantine Server computer. For information about how to install a Quarantine Server, see [Install the Quarantine Server and WebBlocker Server](#).
11. When you enable Gateway AV/IPS for SMTP, you must specify the IP address of your SMTP email server in the **Email Server IP Address** field near the bottom of the page. The Edge creates a policy for you to allow incoming SMTP traffic to this IP address.

Common SMTP Proxy Host

When you enable Gateway AV/IPS for SMTP, you must specify your email server IP address. The Edge creates a policy to enable incoming SMTP to this address.

Email server IP address



Gateway AV does not scan archive file formats such as .zip or packed executables.

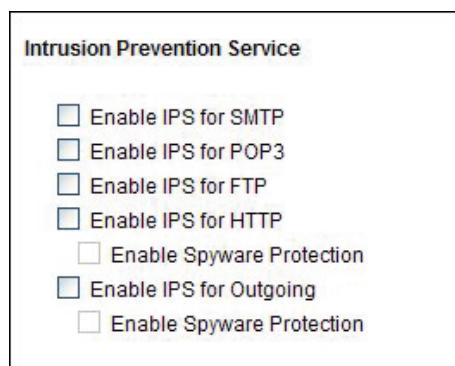
About Intrusion Prevention Service settings

The Intrusion Prevention Service includes a set of signatures associated with specific commands or text found in commands that could be harmful. The Intrusion Prevention Service works together with the SMTP, POP3, HTTP, and FTP proxies. If you have not configured these proxies, they are automatically configured when you enable Gateway AV or IPS for that protocol.

You can see the name of an intrusion that IPS has blocked in the log records. Select **Logging** from the sidebar menu. You can also view general statistics for Gateway AV/IPS on the Gateway AV/IPS page, and trend reporting for Gateway AV/IPS in **System Status > Security Services**.

Configure the Intrusion Prevention Service

1. To connect to the System Status page, type `https://` in the browser address bar, followed by the IP address of the Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`
2. From the navigation bar, select **Gateway AV/IPS > Settings**.



3. Select one or more check boxes to enable IPS for SMTP, POP3, FTP, HTTP, or the Outgoing service on your Edge. If you enable IPS for HTTP or the Outgoing service, you can also enable the additional Spyware Protection feature that automatically protects your network from spyware applications such as adware, trackware, or dialer or hijacker attacks.
4. When you enable Gateway AV/IPS for SMTP, you must specify the IP address of your SMTP email server in the **Email Server IP Address** field near the bottom of the page. The Edge creates a policy for you to allow incoming SMTP traffic to this IP address.



Update Gateway AV/IPS

New viruses and intrusion methods appear on the Internet frequently. The Gateway AV/IPS service uses a database of signatures to check for viruses and intrusions. WatchGuard frequently publishes updates to the signature database to our customers as new signatures become known. Usually, new Gateway AV signatures are published several times a day. New IPS signatures are published less frequently. To make sure that Gateway AV/IPS gives you the best protection, you must update the signatures on the Firebox X Edge frequently. By default, the Firebox X Edge e-Series checks for signature updates automatically. You can change this setting if you want to update the signatures manually.

To update your Gateway AV/IPS signatures manually:

1. Select **Gateway AV/IPS > Update** from the navigation bar
The Gateway AV/IPS Update page appears.

The screenshot shows the 'Gateway AV/IPS Update' page. It has three main sections: 'Update status', 'Gateway AntiVirus', and 'Intrusion Prevention Service'.
Update status: Shows the last update was for Gateway AntiVirus signatures, starting on Friday, January 04, 2008 at 12:31:34 PM, with no update necessary and the server being https://services.watchguard.com.
Gateway AntiVirus: Shows the current signature database version is 586x573, published on Jan-04-2008 07:39:44, and the version available for download is 45.5363. The Gateway AntiVirus license expires on Thu Jan 1 2009. There is a checked checkbox for 'Enable automatic updates for Gateway AntiVirus signatures' with an 'Update' button next to it.
Intrusion Prevention Service: Shows the current signature database version is 10.1.5, published on Jan-04-2008 11:07:17, and the version available for download is 10.1.5. The Intrusion Prevention Service license expires on Thu Jan 1 2009. There is a checked checkbox for 'Enable automatic updates for Intrusion Prevention Service signatures' with an 'Update' button next to it.

[Learn more about updating Gateway AV/IPS.](#)

2. Decide if you want automatic updates or manual updates. If you want manual updates, clear the **Enable automatic updates** check box.
3. If you want to update the signatures manually, compare the current signature database version to the version available for download. If there is a more recent version available, click **Update**. The new signature database downloads and installs automatically.

18

Branch Office Virtual Private Networks

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

Branch Office Virtual Private Networks (BOVPNs) enable businesses to deliver secure, encrypted connectivity between geographically separated offices. The networks and hosts on a VPN tunnel can be corporate headquarters, branch offices, remote users, or telecommuters. These communications often contain the types of critical data exchanged inside the corporate firewall. In this scenario, a BOVPN ensures confidential connections between these offices, streamlines communication, reduces the cost of dedicated lines, and retains security at each end.

Process required to create a tunnel

Do these steps to create a BOVPN tunnel:

1. Make sure you understand the requirements of a Firebox X Edge VPN network, as described in [What you need to create a VPN](#).
2. Configure the Firebox X Edge to be the endpoint of a VPN tunnel created and managed by a WatchGuard Firebox X Core or Peak Management Server. This procedure is different for different versions of WatchGuard System Manager appliance software installed on the Firebox X Core or Peak.
Or
Configure Manual VPN on the Edge, as described in [Create Manual VPN tunnels on your Edge](#).
3. (Optional) Use Traffic Control features with VPN tunnels.

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. To use this option, you must get information from the administrator of the Firebox X on the other side of the VPN tunnel.
- You must know whether the IP address assigned to your Firebox X Edge external interface is static or dynamic. To learn about IP addresses, see [About IP addresses](#).
- Your Firebox X Edge e-Series 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 [Upgrade your Firebox X Edge model](#).
- 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 issue, and not a limit of the Firebox X Edge e-Series.
- 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 Firebox X 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 the 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 [Enable DHCP server on the trusted network](#).
- You must know the network address of the private (trusted) networks behind your Firebox X Edge e-Series and of the network behind the other VPN device, and their subnet masks.



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.

About VPN Failover

Failover is an important function of networks that require a high degree of availability. If a system fails or becomes unavailable, failover automatically shifts the functionality of the failed or unavailable system to a backup system. On the Firebox X Edge e-Series, you can define up to eight multiple remote gateways for the VPN endpoint. The Edge uses Dead Peer Detection (DPD) technology to check the health of the remote gateway. It uses the next available remote gateway when it cannot send or receive traffic from the primary remote gateway. The first remote gateway in the list is the primary remote gateway.

A WAN failover event also causes a VPN failover to occur.

About managed VPNs

You can configure a VPN tunnel on the Firebox X Edge e-Series with two procedures: Managed VPN and Manual VPN. For information on creating a Manual VPN tunnel, see [Create Manual VPN tunnels on your Edge](#).

The WatchGuard Management Server (previously known as the DVCP Server) uses DVCP (Dynamic VPN Configuration Protocol) to keep the VPN tunnel configuration. DVCP is the WatchGuard protocol that you can use to create IPSec tunnels easily. We use the name Managed VPN because the Management Server manages the VPN tunnel and sends the VPN configuration to your Firebox X 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 [About WatchGuard System Manager access](#).

Set 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 Edge.

What you need for Manual VPN

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

- You must know whether the IP address assigned to the other VPN device is static or dynamic. If the other VPN device is dynamic, your Firebox X 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, 3DES, AES-128 bit, AES-192 bit, or AES-256 bit). The two VPN devices must use the same method.

You must know the authentication method for each end of the tunnel (MD5 or SHA1). The two VPN devices 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. See the [Sample VPN address information table](#) to record this information.

Sample VPN address information table

Item	Description	Assigned by
External IP Address	The IP address that identifies the IPSec-compatible device on the Internet. ISP Example: 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 computers 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 You Example: 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. Example: Site A: OurSharedSecret Site B: OurSharedSecret	You
Encryption Method	DES uses 56-bit encryption. 3DES uses 168-bit encryption. AES encryption is available at the 128-bit, 192-bit, and 256-bit levels. AES-256 bit is the most secure encryption. The two devices must use the same encryption method. Example: Site A: 3DES; Site B: 3DES	You
Authentication	The two devices must use the same authentication method. Example: Site A: MD5 (or SHA1) Site B: MD5 (or SHA1)	You

Create Manual VPN tunnels on your Edge

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X 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

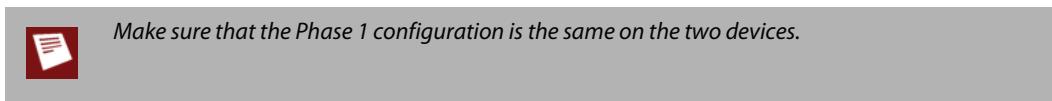
Name	<input type="text"/>		
Credential Method	Shared Key		
Shared Key	<input type="text"/>		
Phase 1 Settings			
Mode	Main Mode		
Local ID	192.168.54.62		
Type	IP Address		
Remote Gateway Configuration			
Remote Gateway IP	Remote ID	Type	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Up"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Down"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Remove"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>
Domain Name			<input type="text"/>

4. Type a name for your tunnel. This name is used for identification only.
5. The **Credential Method** is set to **Shared Key** and can be changed only if you have imported a remote VPN gateway certificate. For more information on third-party certificates, see [About certificates](#).
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 Edge devices. Many users keep the factory default settings.



Phase 1 Settings

Mode	Main Mode
Local ID	192.168.54.62
Type	IP Address

Remote Gateway Configuration

Remote Gateway IP	Remote ID	Type	
			Up
			Down
			Remove
		Domain Name	Add

Authentication Algorithm: SHA1-HMAC

Encryption Algorithm: DES-CBC

Negotiation expires in 0 kilobytes

Negotiation expires in 24 hours

Diffie-Helman Group: 1

Send IKE Keep Alive Messages
Keep alive interval: 60 seconds

Enable Dead Peer Detection
Maximum DPD attempts: 0
DPD Timeout: 0

To change Phase 1 configuration:

1. Select the negotiation mode from the **Mode** drop-down list. You can use Main Mode only when the two devices have static IP addresses. If one or both 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.
 - o 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.
 - o 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 [About the Dynamic DNS service](#). Set the local ID type to **Domain Name**. Enter the DynDNS domain name of the device as the local ID.



If your Firebox X Edge 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 [If your Edge is behind a device that does NAT](#) 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). SHA1-HMAC is more secure.
4. From the **Encryption Algorithm** drop-down list, select the type of encryption. The options, from least secure to most secure, are DES-CBC, 3DES-CBC, AES (128 bit), AES (192 bit), and AES (256 bit).
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. The Edge supports Diffie-Hellman groups 1, 2, and 5. Diffie-Hellman groups securely negotiate secret keys through a public network. Diffie-Hellman groups 2 and 5 use larger key modules and are more secure, but they require more processor time. Each side of the VPN tunnel must use the same Diffie-Hellman Group.
7. Select the **Send IKE Keep Alive Messages** check box to help find when the tunnel is down. When this check box is selected, the Edge sends short packets across the tunnel at regular intervals. This helps the two devices to see whether the tunnel is up. If the Keep Alive packets get no response after three tries, the Firebox X Edge starts the tunnel again.
8. Select the **Enable Dead Peer Detection (DPD)** check box to check the status of the remote gateway when you want to use VPN failover. During a DPD check, the Firebox pings the remote gateway and waits for a response. If there is no response, VPN failover occurs and the Firebox will use the next available remote gateway. You can configure the amount of time before each ping timeout in seconds, and the maximum number of ping attempts.

If your Edge is behind a device that does NAT

The Firebox X Edge e-Series can use NAT Traversal. This means that you can make VPN tunnels if your ISP does NAT (Network Address Translation) or if the external interface of your Edge is connected to a device that does NAT. We recommend that the Firebox X Edge 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 e-Series 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 Firebox X Edge e-Series 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 the private external IP address of your Edge through the Internet.

- If the NAT device to which the Firebox X Edge is connected has a dynamic public IP address:
 - First, set the device to Bridge Mode. In Bridge Mode, the Edge gets the public IP address on its external interface. Refer to the manufacturer of your NAT device for more information.
 - Set up Dynamic DNS on the Firebox X Edge. For information, see [About the Dynamic DNS service](#). 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 Firebox X 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 Firebox X Edge by domain name, and it must use the 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.

Phase 2 Settings

Authentication Algorithm	<input type="button" value="SHA1-HMAC ▾"/>
Encryption Algorithm	<input type="button" value="3DES-CBC ▾"/>
<input type="checkbox"/> Enable TOS for IPSEC	
<input type="checkbox"/> Enable Perfect Forward Secrecy	
Key expires in <input type="text" value="8192"/> kilobytes	
Key expires in <input type="text" value="24"/> hours	

The Firebox X Edge creates a tunnel for each remote network you define. To operate correctly, you must configure the remote peer the same way.

Local Network	Remote Network
<input type="button" value="Remove"/>	

Local Network

 Remote Network



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. TOS bits are a set of four-bit flags in the IP header that can tell routing devices to give some VPN traffic higher priority. Some ISPs drop all packets that have TOS flags set. If you select the **Enable TOS for IPSec** check box, the Edge preserves existing TOS bits in VPN traffic packets. If the check box is not selected, the Edge removes TOS bits.
4. 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.
5. 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.

6. 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
7. Click **Add**.
8. Repeat step 5 if you must add additional networks.
9. Click **Submit**.

Configure 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 e-Series sends a ping each minute to the specified host. Use the IP address of a host that is always online and that 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 also can use more than one IP address so the 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 Firebox X 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.

The screenshot shows the 'VPN Keep Alive' configuration page. At the top, it displays the title 'VPN' and 'VPN Keep Alive'. Below this, there is a table-like structure for managing echo hosts. The first row shows an 'Echo Hosts' column with the IP address '64.23.103.18' and a 'Remove' button to its right. Below this row, there is a 'Host Address' input field containing '64.23.103.18' and an 'Add' button to its right. At the bottom of the page are 'Submit' and 'Reset' buttons.

3. Type the IP address of an echo host. Click **Add**.
4. Repeat step 3 to add additional echo hosts.
5. Click **Submit**.

See VPN statistics

You can monitor Firebox X Edge e-Series 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 Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`.
2. From the navigation bar, select **System Status > VPN Statistics**.
The VPN Statistics page appears.

Related 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 [About the Dynamic DNS service](#).

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 to the local interface IP address of the remote Firebox X Edge, use 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 allowed VPN tunnels on my Edge?

The number of VPN tunnels that you can create on your Firebox X Edge e-Series is set by the Edge model you have. You can purchase a model upgrade for your Edge to make more VPN tunnels. You can purchase a Firebox X Edge Model Upgrade from a reseller or from the WatchGuard web site:

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

19

About Mobile VPN with PPTP

You can configure the Firebox X Edge e-Series as a PPTP VPN endpoint and allow up to 10 users to make simultaneous secure connections to the Edge and access the networks protected by the Edge.

Before remote users can connect to the Firebox with PPTP, you must:

- On the Edge, activate PPTP and enter the IP address of the first of 10 available sequential IP addresses on the trusted or optional network that are currently not in use. The Edge must be able to give these IP addresses to remote users when they make a PPTP connection.
- With local authentication, enable PPTP connections in each remote user's Firewall user profile. When a user makes a PPTP connection to the Edge, the user is then given full access to the trusted or optional networks.
- With Active Directory or RADIUS authentication, add a group to the Edge that has the same name as the group on the authentication server that needs PPTP access. Enable PPTP connections for the group.
- Configure the PPTP connection on the client computer.

Enable PPTP on the Edge

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

VPN
Mobile User

Firebox Mobile VPN with IPSec Configuration

The following settings apply to all Mobile VPN with IPSec clients.

You can allow secure access to your trusted network using WatchGuard Mobile VPN with IPSec client software. You will need to install the software on each remote device and then enable Mobile VPN with IPSec for each user.

Make the Mobile VPN with IPSec client security policy read-only. Virtual Adapter **Disabled** 

Firebox Mobile VPN with PPTP Configuration

You can enable a PPTP server on the Firebox and allow remote users to connect to networks protected by the Firebox using PPTP VPN tunnels. The Firebox assigns an IP address to PPTP clients from an address pool of up to 10 sequential IP addresses. Type the first available IP address in the field below.

Activate remote user VPN with Mobile VPN with PPTP.
 Allow drop from 128-bit to 40-bit encryption.
 Log all allowed PPTP traffic.

Start of IP address pool:

Note: You must create Firebox user accounts and enable Mobile VPN with PPTP access for each account.

WINS/DNS Setting for Mobile VPN with IPSec and PPTP Clients

The Firebox assigns this name server information to Mobile VPN with IPSec and PPTP clients:

DNS Server IP Address [optional]
WINS Server IP Address [optional]

[Learn more about Mobile VPN with PPTP.](#)

Submit **Reset**

3. To enable PPTP, select the **Activate remote user VPN with Mobile VPN with PPTP** check box.
4. Select the **Enable drop from 128-bit to 40-bit** check box to allow the tunnels to drop from 128-bit to 40-bit encryption for connections that are less reliable.
The Firebox X Edge always tries to use 128-bit encryption first. It uses 40-bit encryption if the client cannot use the 128-bit encrypted connection. Usually, only customers outside the United States use this check box.
5. Select the **Log all allowed PPTP traffic** to have the Edge record a log message for all PPTP traffic.

6. When a PPTP user connects to the Edge, the Edge must assign that user's computer an available IP address from the network the user wants to connect to. Type the first IP address in the address pool the Edge can use to assign PPTP user IP addresses in the **Start of IP address pool** field. The Edge gives out this IP address to the first PPTP user that connects. The Edge increments the IP address by 1 and assigns an address to each subsequent PPTP user that connects (up to 10 users).
The IP address that you set as the start of the IP address pool must be the first of ten sequential IP addresses available and identified on your Edge as part of the trusted or optional network.

Configure DNS and WINS settings

The Domain Name Service (DNS) changes host names into IP addresses. The Windows Internet Naming Service (WINS) changes NetBIOS names to IP addresses. By default, PPTP users that connect to the Edge use the WINS and DNS servers identified on the **Network > Trusted** page of your Edge configuration.

If you want to specify a different WINS or DNS server, add it in the **DNS Server** and **WINS Server IP Address** text boxes in the last section of the Mobile User page.

Enable PPTP access for firewall users

When you enable Mobile VPN with PPTP on your Edge, you must enable PPTP access for each remote user who uses PPTP to connect to the Edge.

1. To connect to the System Status page, type `https://` and the IP address of the Firebox X Edge trusted interface in the browser address bar.
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 Users Accounts**, click the **Edit** button to edit an existing user account, or **Add** to add a new user account.
4. From the **New** or **Edit** page that appears, select the **Allow remote access with Mobile VPN with PPTP** check box.

The screenshot shows the 'Firebox Users' interface with a 'New User' form. The 'MOVPN' tab is active. The 'Allow remote access with Mobile VPN with PPTP' checkbox is checked. Other visible fields include 'Account name', 'Full name', 'Description', 'Password', 'Confirm password', 'Administrative access' (set to 'None'), 'Session maximum timeout' (0 minutes), 'Session idle timeout' (0 minutes), and checkboxes for 'Allow access to the External Network' and 'Allow access to manual and managed VPN tunnels'.

Firebox Users

New User

Settings WebBlocker MOVPN

Account name

Full name

Description

Password

Confirm password

Administrative access

Session maximum timeout minutes

Session idle timeout minutes

Allow access to the External Network

Allow access to manual and managed VPN tunnels

Allow remote access with Mobile VPN with PPTP

Allow remote access with Mobile VPN with SSL

[Learn more about creating local user accounts.](#)

Prepare the client computers

You must make sure each remote user's computer is prepared to use PPTP. Each computer must have Internet access, and must have the necessary version of Microsoft Dial-Up Networking and any necessary service packs. Some operating systems can require a VPN adapter. You can find Microsoft upgrades and service packs on the Microsoft Download Center web site at <http://www.microsoft.com/downloads/search.aspx>.

Create and connect a PPTP Mobile VPN for Windows Vista

Create a PPTP connection

To prepare a Windows Vista client computer, you must configure the PPTP connection in the network settings.

From the Windows Desktop of the client computer:

1. Click **Start > Settings > Control Panel**.
The Start button in Windows Vista is located in the lower-left corner of the screen.
2. Click **Network and Internet**.
This opens the Network and Sharing Center.
3. In the left column, below **Tasks**, click **Connect to a network**.
The New Connection Wizard starts.
4. Select **Connect to a workplace** and click **Next**.
The Connect to a workplace dialog box appears.
5. Select **No, create a new connection** and click **Next**.
The How do you want to connect dialog box appears.
6. Click **Use my Internet connection (VPN)**.
The Type the Internet address to connect to dialog box appears.
7. Type the host name or IP address of the Firebox external interface in the **Internet address** field.
8. Type a name for the Mobile VPN (such as "PPTP to Firebox") in the **Destination name** text box.
9. Select whether you want other people to be able to use this connection.
10. Select the **Don't connect now; just set it up so I can connect later** check box so that the client computer does not try to connect at this time.
11. Click **Next**.
The Type your user name and password dialog box appears.
12. Type the **User name** and **Password** for this client.
13. Click **Create**.
The connection is ready to use dialog box appears.
14. To test the connection, click **Connect now**.

Establish the PPTP connection

To connect a Windows Vista client computer, replace **[name of the connection]** with the actual name you used when configuring the PPTP connection.

Make sure you have an active connection to the Internet before you begin.

1. Click **Start > Settings > Network Connections > [name of the connection]**
The Windows Vista Start button is located in the lower-left corner of your screen.
2. Type the user name and password for the connection and click **Connect**.
3. The first time you connect you must select a network location. Select Public location.

Create and connect a PPTP Mobile VPN for Windows XP

To prepare a Windows XP client computer, you must configure the PPTP connection in the network settings.

Create the PPTP Mobile VPN

From the Windows Desktop of the client computer:

1. Click **Start > Control Panel > Network Connections**.
2. Click **Create a new connection** from the menu on the left.
Or click **New Connection Wizard** in Windows Classic view.
The New Connection wizard appears.
3. Click **Next**.
4. Select **Connect to the network at my workplace** and click **Next**.
5. Select **Virtual Private Network connection** and click **Next**.
6. Type a name for the new connection (such as "Connect with Mobile VPN") and click **Next**.
7. Select if Windows ensures the public network is connected:
 - For a broadband connection, select **Do not dial the initial connection**.
Or
 - For a modem connection, select **Automatically dial this initial connection**, and then select a connection name from the drop-down list.
8. Click **Next**.
The VPN Server Selection screen appears. The wizard includes this screen if you use Windows XP SP2. Not all Windows XP users see this screen.
9. Type the host name or IP address of the Firebox external interface and click **Next**.
The Smart Cards screen appears.
10. Select whether to use your smart card with this connection profile and click **Next**.
The Connection Availability screen appears.
11. Select who can use this connection profile and click **Next**.
12. Select **Add a shortcut to this connection to my desktop**. Click **Finish**.

Connect with the PPTP Mobile VPN

1. Make an Internet connection through a dial-up network, or directly through a LAN or WAN.
2. Double-click the shortcut to the new connection on your desktop.
Or select **Control Panel > Network Connections** and select your new connection from the Virtual Private Network list.
3. Type the user name and passphrase for the connection.
4. Click **Connect**.

Create and connect a PPTP Mobile VPN for Windows 2000

To prepare a Windows 2000 remote host, you must configure the PPTP connection in the network settings.

Create the PPTP Mobile VPN

From the Windows Desktop of the client computer:

1. Click **Start > Settings > Network Connections > Create a New Connection**.
The New Connection wizard appears.
2. Click **Next**.
3. Select **Connect to the network at my workplace** and click **Next**.
4. Click **Virtual Private Network connection**.
5. Type a name for the new connection (such as "Connect with Mobile VPN") and click **Next**.
6. Select to not dial (for a broadband connection), or to automatically dial (for a modem connection) this connection, and click **Next**.
7. Type the host name or IP address of the Firebox® external interface and click **Next**.
8. Select **Add a shortcut to this connection to my desktop** and click **Finish**.

Connect with the PPTP Mobile VPN

1. Make an Internet connection through a dial-up network, or directly through a LAN or WAN.
2. Double-click the shortcut to the new connection on your desktop.
Or, select **Control Panel > Network Connections** and select your new connection from the Virtual Private Network list.
3. Type the user name and passphrase for the connection.
4. Click **Connect**.

Options for Internet access through a Mobile VPN with PPTP tunnel

You can enable remote users to access the Internet through a Mobile VPN tunnel. This option affects your security because Internet traffic is not filtered or encrypted. You have two options for Mobile VPN tunnel routes: default-route VPN and split tunnel VPN.

Default-route VPN

The most secure option is to require that all remote user Internet traffic is routed through the VPN tunnel to the Firebox. From the Firebox, the traffic is then sent back out to the Internet. With this configuration (known as default-route VPN), the Firebox is able to examine all traffic and provide increased security, although more processing power and bandwidth on the Firebox is used.



*If you use the route print or ipconfig commands after you start a Mobile VPN tunnel on a computer with Microsoft Windows installed, you see incorrect default gateway information. You will see correct information if you look at the **Details** tab of the **Virtual Private Connection Status** dialog box.*

Split tunnel VPN

Another configuration option is to enable split tunneling. This configuration enables users to browse the Internet without sending Internet traffic through the VPN tunnel. Split tunneling decreases security because Firebox policies are not applied to the Internet traffic, but it does increase performance. If you use split tunneling, client computers should have a software firewall.

Default-route VPN setup for Mobile VPN with PPTP

The default PPTP settings in Windows Vista, XP and 2000 create a default-route VPN.

Split tunnel VPN setup for Mobile VPN with PPTP

On the client computer, edit the PPTP connection properties to not send all traffic through the VPN.

1. For Windows Vista, XP or 2000, go to **Control Panel > Network Connections** and right-click the VPN connection.
2. Select **Properties**.
The VPN properties dialog box appears.
3. Select the **Networking** tab.
4. Select **Internet Protocol (TCP/IP)** in the list box and click **Properties**.
The Internet Protocol (TCP/IP) Properties dialog box appears.
5. On the **General** tab, click **Advanced**.
The Advanced TCP/IP Settings dialog box appears.
6. Windows XP and Windows 2000 - On the **General** tab (XP and Windows 2000), clear the **Use default gateway on remote network** check box.
Windows Vista - On the **Settings** tab (XP and Windows 2000), clear the **Use default gateway on remote network** check box.

20 About Mobile VPN with IPSec

The WatchGuard Mobile VPN with IPSec 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 Mobile VPN client uses Internet Protocol Security (IPSec) to secure the connection.

Client requirements

Before you install the client, make sure you understand these requirements.

You can install the Mobile VPN with IPSec client software on any computer running these operating systems:

- Windows 2000 Professional
- Windows XP (32-bit)
- Windows Vista (32-bit and 64-bit).

Before you install the client software, make sure the remote computer does not have any other IPSec mobile user VPN client software installed. You must also uninstall any desktop firewall software (other than Microsoft firewall software) from each remote computer.

WatchGuard does not provide a Mobile User VPN with IPSec client software package for the Apple Mac OS X platform. WatchGuard does provide a [Mobile VPN with SSL](#) client for the Mac OS X platform.

There are third-party vendors that make IPSec clients that they say are compatible with WatchGuard products. WatchGuard does not support or endorse any third-party IPSec clients. To learn more about them, see:

IPSecuritas: <http://www.lobotomo.com/products/IPSecuritas/index.html>

VPNTracker: <http://www.equinix.com/us/products/vpntracker/vendor.html?vendor=watchguard>

You can also check the WatchGuard User Forum at <http://www.watchguard.com/forum/> to learn more about the experiences of other users with Mobile User VPN with IPSec.

Enable Mobile VPN for a Firebox user account

1. To connect to the Edge System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`.
2. To add a new Firebox user, select **Firebox Users > New User**.
You can also edit the properties of an existing user. Go to the main Firebox User page and find the name of the user account you want to edit.
3. On the **Settings** tab, type an **Account Name** for the user. Type the password for the user. This is different from the shared secret you type in step 7 below.
The Full Name and Description fields are optional.
4. Click the **MOVPN** tab.

Firebox Users

New User

Settings WebBlocker MOVPN

Enable Mobile VPN with IPSec for this account

Shared key

Virtual IP address

Authentication algorithm

Encryption algorithm

Key expires in kilobytes

Key expires in hours

VPN client type

All traffic uses tunnel (0.0.0.0/0 IP Subnet)

[Learn more about creating local user accounts.](#)

5. Select the **Enable Mobile VPN with IPSec for this account** check box.
6. Type a shared key in the **Shared key** field.
The .wgx file is encrypted with this shared key. Do not give the shared key to any user that is not authorized to use this Firebox user account.
7. Type the virtual IP address in the related field.
The virtual IP address must be an address on the Firebox X Edge trusted or optional network that is not used and is not included within any range of DHCP addresses assigned by the Edge. This address is used by the remote computer to connect to the Firebox X Edge.
8. If necessary, change the **Authentication Algorithm** or **Encryption Algorithm** settings.
9. Set Mobile VPN 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).

10. Select **Mobile User** in the **VPN Client Type** drop-down list. This selection is required if you use a Windows desktop, laptop, or handheld PC.
11. Select the **All traffic uses tunnel (0.0.0.0/0 IP Subnet)** check box if the remote client sends all its traffic (including usual web traffic) through the VPN tunnel to the Firebox X Edge. This can also let the Mobile VPN client connect with other networks that the Edge connects to.
If you do not select this check box, the remote user can connect with only the Firebox X Edge trusted network. You must select this check box for a remote user to connect to:
 - o Networks on the other side of a Branch Office VPN tunnel that the Edge has connected.
 - o Computers on the Edge's optional network.
 - o Networks that are behind a static route on the trusted or optional interface.
12. Click **Submit**.

Enable Mobile VPN for a group

1. To connect to the Edge System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is: `https://192.168.111.1`
2. To add a new Firebox user group, select **Firebox Users > New Group**.
You can also edit the properties of an existing group. Go to the main Firebox User page and find the name of the group you want to edit.
3. On the **Settings** tab, type an **Account Name** for the group. If you are using LDAP or RADIUS authentication the Account Name must be identical to the group name on the authentication server.
The Description field is optional.
4. Click the **MOVPN** tab.
5. Select the **Enable Mobile VPN with IPSec for this account** check box.
6. Type a shared key in the **Shared key** field.
The .wgx file is encrypted with this shared key. Do not give the shared key to any user that is not part of this group.
7. If necessary, change the **Authentication Algorithm** or **Encryption Algorithm** settings.
8. Set Mobile VPN 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 the Clear type of service (TOS) check box if you want the Edge to remove the TOS bit setting from packets that go through the VPN tunnel
10. Select the **All traffic uses tunnel (0.0.0.0/0 IP Subnet)** check box if the remote client sends all its traffic (including usual web traffic) through the VPN tunnel to the Firebox X Edge. This can also let the Mobile VPN client connect with other networks that the Edge connects to.
If you do not select this check box, the remote user can connect with only the Firebox X Edge trusted network. You must select this check box for a remote user to connect to:
 - o Networks on the other side of a Branch Office VPN tunnel that the Edge has connected.
 - o Computers on the Edge's optional network.
 - o Networks that are behind a static route on the trusted or optional interface.
11. Type a starting and ending IP address in the **Virtual IP address range** text boxes. The virtual IP addresses must be IP addresses on the Firebox X Edge trusted or optional network that are not used and are not included within any range of DHCP addresses assigned by the Edge. These IP addresses are used by remote computers to connect to the Firebox X Edge.
12. Click **Submit**.

About Mobile VPN Client configuration files

With Mobile VPN with IPSec, the Firebox X Edge administrator controls end-user profiles. You use the Edge web configuration interface to set the name of the end user and create a client configuration file, or profile, with the file extension .wrx. The .wrx file contains the shared key, user identification, IP addresses, and settings that are used to create a secure tunnel between the remote computer and the Edge. This file is encrypted with a key that is eight characters or greater in length. This key must be known to the administrator and the remote user. When the remote client imports the .wrx file, this key is used to decrypt the file for use in the client software.

The Firebox X Edge creates a .wrx file for a user when a Firebox user's account is configured for Mobile VPN.

If you want to lock mobile users profiles and make them read-only, see [Configure global Mobile VPN with IPSec client settings](#).

Configure global Mobile VPN with IPSec client settings

Some Mobile VPN client settings apply to all Firebox X Edge Mobile VPN with IPSec connections. Select **VPN > Mobile VPN** to set these options.

VPN

Mobile User

Firebox Mobile VPN with IPSec Configuration

The following settings apply to all **Mobile VPN with IPSec** clients.

You can allow secure access to your trusted network using WatchGuard Mobile VPN with IPSec client software. You will need to install the software on each remote device and then enable Mobile VPN with IPSec for each user.

Make the Mobile VPN with IPSec client security policy read-only.

Virtual Adapter **Disabled** 

Make the Mobile VPN with IPSec client security policy read-only

Select this check box to make the .wrx file read-only so that the user cannot change the security policy file.

Virtual Adapter

The default setting is **Disabled**. Do not change this setting.



*Because the Mobile VPN with IPSec client always uses a virtual adapter, you should not change the **Virtual Adapter** setting. This setting applies only to Mobile User VPN versions prior to 10.0. Mobile VPN with IPSec software version 10.0 and later always use a virtual adapter, regardless of the selection made in this field.*

WINS/DNS Settings for Mobile VPN with IPSec

Mobile VPN clients use shared Windows Internet Naming Service (WINS) and Domain Name System (DNS) server addresses. DNS changes host names into IP addresses, while WINS changes NetBIOS names to IP addresses. The trusted interface of the Edge must have access to these servers.

WINS/DNS Setting for Mobile VPN with IPSec and PPTP Clients

The Firebox assigns this name server information to Mobile VPN with IPSec and PPTP clients:

DNS Server IP Address	<input type="text"/>	[optional]
WINS Server IP Address	<input type="text"/>	[optional]

[Learn more about Mobile VPN with PPTP.](#)

DNS Server IP Address

Type a DNS server IP address to enable DNS to change host names to IP addresses.

WINS Server IP Address

Type a WINS server IP address to enable WINS to change NetBIOS names to IP addresses.

Get the user's .wgx file

The Firebox X Edge makes an encrypted Mobile VPN with IPSec client configuration (.wgx) file for every Firebox User that you give access to. To download a user's .wgx file:

1. Connect to the System Status page: Type `https://` and the IP address of the Firebox X Edge trusted interface in the browser address bar.
The default URL is: `https://192.168.111.1`
2. From the navigation bar, select **Firebox Users**.
3. Below **Secure Mobile VPN with IPSec Client Configuration Files**, select the .wgx file to download by clicking on the link **username.wgx** where **username** is the Firebox user's name.
4. At the prompt, save the .wgx file to your computer.

Distribute the software and profiles

WatchGuard recommends distributing end-user profiles by encrypted email or by another secure method. Each client computer must have:

- **Software installation package**

The packages are located on the WatchGuard LiveSecurity Service web site at:

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

Log in to the site using your LiveSecurity Service user name and password. Click the **Latest Software** link, click **Add-ons/Upgrades** on the left side, and then click the link for **Mobile VPN with IPSec**.

- **End-user profile**

This file contains the user name, shared key, and settings that enable a remote computer to connect securely over the Internet to a protected, private computer network. For information on how to get the profile from the Edge, see [Get the user's .wgx file](#).

- **User documentation**

Documentation to help the remote user install the Mobile VPN client and import their Mobile VPN configuration file can be found in the topics [About the Mobile VPN with IPSec client](#)

- **Shared key**

To import the end-user profile, the user is requested to type a shared key. This key decrypts the file and imports the security policy into the Mobile VPN client. The key is set when you enable the Firebox User account to use Mobile VPN with IPSec.



The shared key, user name, and password are highly sensitive information. For security reasons, we recommend that you do not provide this information by email message. Because email is not secure, an unauthorized user can get the information and gain access to your internal network. Give the user the information by telling it to the user, or by some other method that does not allow an unauthorized person to intercept it.

About the Mobile VPN with IPSec client

The WatchGuard Mobile VPN with IPSec client is installed on a user's computer, whether the user travels or works from home. The user connects with a standard Internet connection and activates the Mobile VPN client.

The Mobile VPN client then creates an encrypted tunnel to your trusted and optional networks, which are protected by a WatchGuard Firebox. The Mobile VPN client allows you to supply remote access to your internal networks and not compromise your security.

Client Requirements

Before you install the client, make sure you understand these requirements and recommendations.

You must configure your Firebox to work with Mobile VPN with IPsec. If you have not, see the topics that describe how to configure your Firebox to use Mobile VPN.

- You can install the Mobile VPN with IPSec client software on any computer running Windows 2000 Professional, Windows XP (32-bit), or Windows Vista (32-bit and 64-bit). Before you install the client software, make sure the remote computer does not have any other IPSec mobile user VPN client software installed. You must also uninstall any desktop firewall software (other than Microsoft firewall software) from each remote computer.
- If the client computer is running Windows XP, you must log on using an account that has administrator rights to install the Mobile VPN client software and to import the .wgx configuration file. Administrator rights are not required to connect after the client has been installed and configured.
- If the client computer is running Windows Vista, you must log on using an account that has administrator rights to install the Mobile VPN client software. Administrator rights are not required to import a .wgx file or to connect after the client has been installed.
- We recommend that you check to make sure all available service packs are installed before you install the Mobile VPN client software.
- WINS and DNS settings for the Mobile VPN client are obtained in the client profile you import when you set up your Mobile VPN client.
- We recommend that you do not change the configuration of any Mobile VPN client setting not explicitly described in this documentation.

Import the end-user profile

When the computer restarts, the WatchGuard Mobile VPN Connection Monitor dialog box opens. When the software starts for the first time after you install it, you see this message:

There is no profile for the VPN dial-up! Do you want to use the Configuration Assistant for generating a profile now?

Click **No**.

To turn off the Connection Monitor auto-start functionality, select **Window > AutoStart > No Autostart**.

To import a Mobile VPN configuration .wgx file:

1. Select **Configuration > Profile Import**.
The Profile Import Wizard starts.
2. On the **Select User Profile** screen, browse to the location of the .wgx configuration file supplied by your network administrator. Click **Next**.
3. On the **Decrypt User Profile** screen, type the shared key or passphrase supplied by your network administrator. The shared key is case-sensitive. Click **Next**.

4. On the **Overwrite or add Profile** screen, you can select to overwrite a profile of the same name. This is useful if your network administrator gives you a new .wgx file and you must reimport it. Click **Next**.
5. If you connect to a Firebox X Edge, click **Finish**.
If you connect to a Firebox running Fireware appliance software, click **Next**.
6. On the **Authentication** screen, you can select whether to type the user name and password that you use to authenticate the VPN tunnel. If you keep these fields clear, you are prompted to enter your user name and password each time you connect to the VPN.
If you type your user name and password here, the Firebox stores it and you do not have to enter this information each time you connect. However, this is a security risk. Optionally, you can type just your user name and keep the **Password** field clear. This can minimize the amount of data required for the VPN connection.
Click **Next**.



If the password you use is your password on an Active Directory or LDAP server and you choose to store it, the password becomes invalid when it changes on the authentication server.

7. Click **Finish**.
The computer is now ready to use Mobile VPN with IPSec.

Select a certificate and enter the PIN

If you use certificates for authentication, you must select the correct certificate for the connection.

1. Select **Configuration > Certificates**.
2. On the **User Certificate** tab, select **from PKS#12 file** from the **Certificate** drop-down list.
3. Adjacent to the **PKS#12 Filename** text box, click the button and browse to the location of the .p12 file supplied by your network administrator. Click **OK**.
4. Select **Connection > Enter PIN**.
5. Type the PIN and click **OK**.
The PIN is the passphrase entered to encrypt the file when running the Add Mobile User VPN Wizard.

Uninstall the Mobile VPN client

At some point, it can become necessary to uninstall the Mobile VPN client. We recommend that you use the Windows Add/Remove Programs tool to uninstall the Mobile VPN client. After the Mobile VPN client software is installed the first time, it is not necessary to uninstall the Mobile VPN client software before you apply any upgrades to the client software.

Before you start, disconnect all tunnels and close the Mobile VPN Connection Monitor. Then, from the Windows desktop:

1. Click **Start > Settings > Control Panel**.
The Control Panel window appears.
2. Double-click the **Add/Remove** Programs icon.
The Add/Remove Programs window appears.
3. Select **WatchGuard Mobile VPN** and click **Change/Remove**.
The InstallShield Wizard window appears.
4. Click **Remove** and click **Next**.
The Confirm File Deletion dialog box appears.
5. Click **OK** to completely remove all of the components. If you do not select this box at the end of the uninstall, the next time you install the Mobile VPN software the connection settings from this installation populate in the next installation.

Connect and disconnect the Mobile VPN client

The WatchGuard Mobile VPN with IPSec client software makes a secure connection from a remote computer to your protected network over the Internet. To start this connection, you must connect to the Internet and use the Mobile VPN client to connect to the protected network.

Start your connection to the Internet through a Dial-Up Networking connection or LAN connection. Then, use the instructions below or select your profile, connect, and disconnect by right-clicking the Mobile VPN icon on your Windows toolbar.

1. From your Windows desktop, select **Start > All Programs > WatchGuard Mobile VPN > Mobile VPN Monitor**.
2. From the **Profile** drop-down list, select the name of the profile you created for your Mobile VPN connections to the Firebox. Click **Connect**.



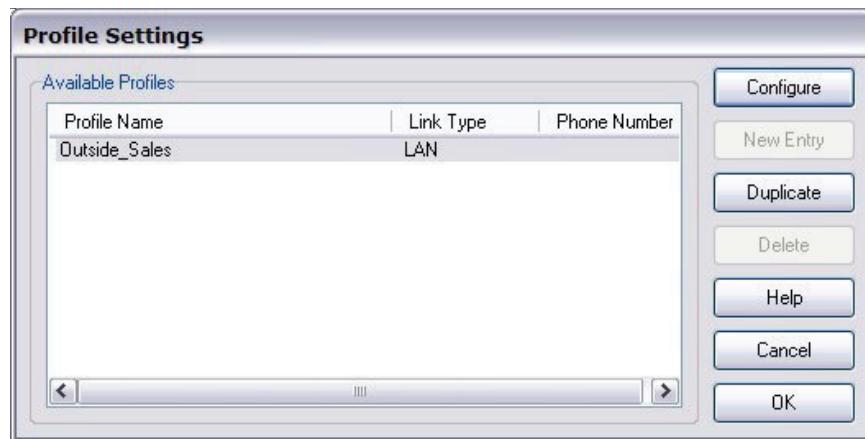
Disconnect the Mobile VPN client

From the Mobile VPN Monitor, click **Disconnect**.

Control connection behavior

For each profile you import, you can control the action the Mobile VPN client software takes when the VPN tunnel goes down for any reason. To set the behavior of the Mobile VPN client when the VPN tunnel goes down:

1. From the WatchGuard Mobile VPN Connection Monitor, select **Configuration > Profile Settings**.
2. Select the name of the profile and click **Configure**.



3. From the left pane, select **Line Management**.



4. Use the **Connection Mode** drop-down list to set a connection behavior for this profile.
 - **Manual** - When you select **manual** connection mode, the client does not try to restart the VPN tunnel automatically if the VPN tunnel goes down. To restart the VPN tunnel, you must click the **Connect** button in Connection Monitor or right-click the Mobile VPN icon on your Windows desktop toolbar and click **Connect**.
 - **Automatic** - When you select **automatic** connection mode, the client tries to start the connection when your computer sends traffic to a destination that you can reach through the VPN. The client also tries to restart the VPN tunnel automatically if the VPN tunnel goes down.
 - **Variable** - When you select **variable** connection mode, the client tries to restart the VPN tunnel automatically until you click **Disconnect**. The client does not try to restart the VPN tunnel again until after the next time you click **Connect**.
5. Click **OK**.

Mobile User VPN client icon

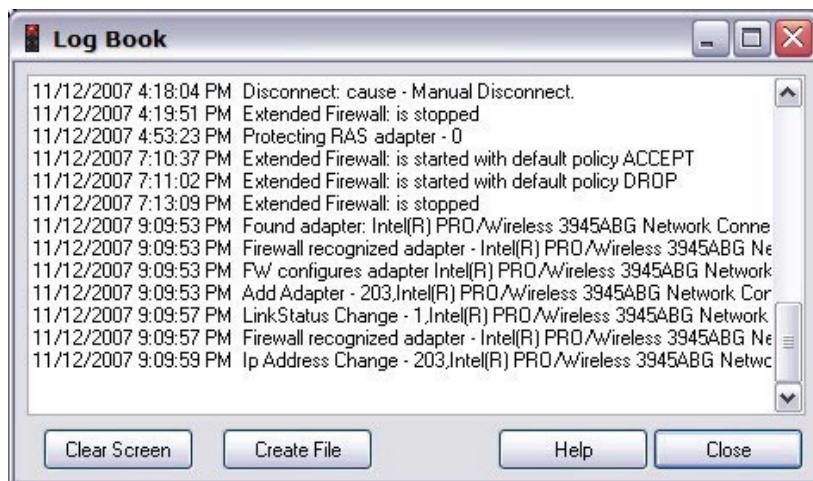
The Mobile User VPN icon appears in the Windows desktop system tray to show the status of the full featured desktop firewall, the link firewall, and the VPN network. You can right-click the icon to easily connect and disconnect your Mobile VPN and see which profile is in use.

See Mobile VPN log messages

You can use the Mobile VPN client log file to troubleshoot problems with the negotiations that occur during the VPN client connection.

To access Mobile VPN log messages, select **Log > Logbook** from the Connection Monitor.

The Log Book dialog box appears.



Secure your computer with the Mobile VPN firewall

The WatchGuard Mobile VPN with IPSec client includes two firewall components:

Link firewall

The link firewall is not enabled by default. When the link firewall is enabled, your computer will discard any packets received from other computers. You can choose to enable the link firewall only when a Mobile VPN tunnel is active, or enable it all the time.

Desktop firewall

This full-featured firewall can control connections to and from your computer. You can define friendly networks and set access rules separately for friendly and unknown networks.

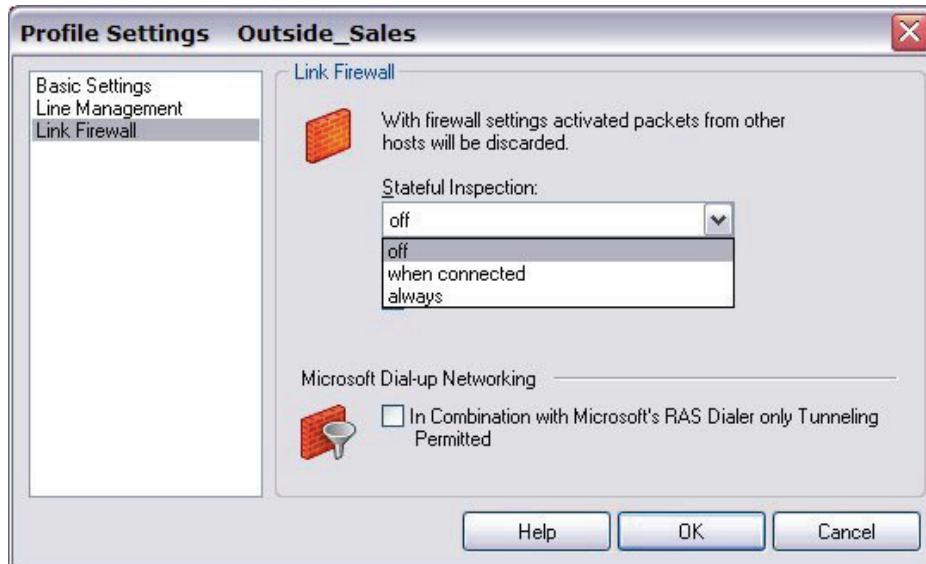
Enable the link firewall

When the link firewall is enabled, the Mobile VPN client software drops any packets sent to your computer from other hosts. It allows only packets sent to your computer in response to packets your computer sends. For example, if you send a request to an HTTP server through the tunnel from your computer, the reply traffic from the HTTP server is allowed. If a host tries to send an HTTP request to your computer through the tunnel, it is denied.

To enable the link firewall:

1. From the WatchGuard Mobile VPN Connection Monitor, select **Configuration > Profile Settings**.
2. Select the profile you want to enable the link firewall for and select **Configure**.

3. From the left pane, select **Link Firewall**.



4. From the **Stateful Inspection** drop-down list, select **when connected** or **always**. If you select when connected, the link firewall operates only when the VPN tunnel is active for this profile. If you select **always**, the link firewall is always active, whether the VPN tunnel is active or not.
5. Click **OK**.

About the desktop firewall

When you enable a rule in your firewall configurations, you must specify what type of network the rule applies to. In the Mobile VPN client, there are three different types of networks:

VPN networks

Networks defined for the client in the client profile they import.

Unknown networks

Any network not specified in the firewall.

Friendly networks

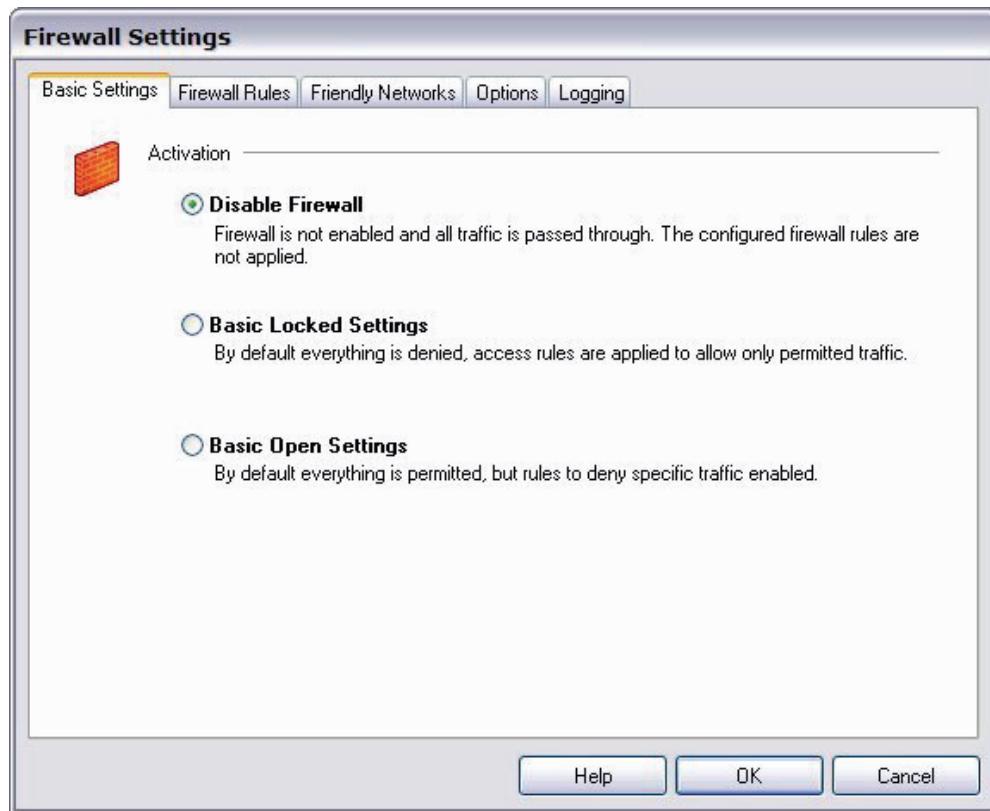
Any network specified in the firewall as a known network.

For information about how to enable the desktop firewall, see [Enable the desktop firewall](#).

Enable the desktop firewall

To enable the full-featured desktop firewall:

1. From the WatchGuard Mobile VPN Connection Monitor, select **Configuration > Firewall Settings**.
The firewall is disabled by default.
2. When you enable the firewall, you must choose between two firewall modes:
 - o **Basic Locked Settings** - When you enable this mode, the firewall denies all connections to or from your computer unless you have created a rule to specifically allow the connection.
 - o **Basic Open Settings** - When you enable this mode, the firewall allows all connections unless you have created a rule to specifically deny the connection.



3. Click **OK**.

After you have enabled the desktop firewall, you can configure your firewall settings.

For more information about how to define friendly networks and create firewall rules, see [Define friendly networks](#) and [Create firewall rules](#).

Define friendly networks

You can generate a firewall rule set for specific known networks that you define. For example, if you want to use the Mobile VPN client on a local network where you want your computer available to other computers, you can add the network address of that LAN as a friendly network. This differentiates the firewall rules for that LAN from the firewall rules you create for connections to the Internet and to remote VPN networks.

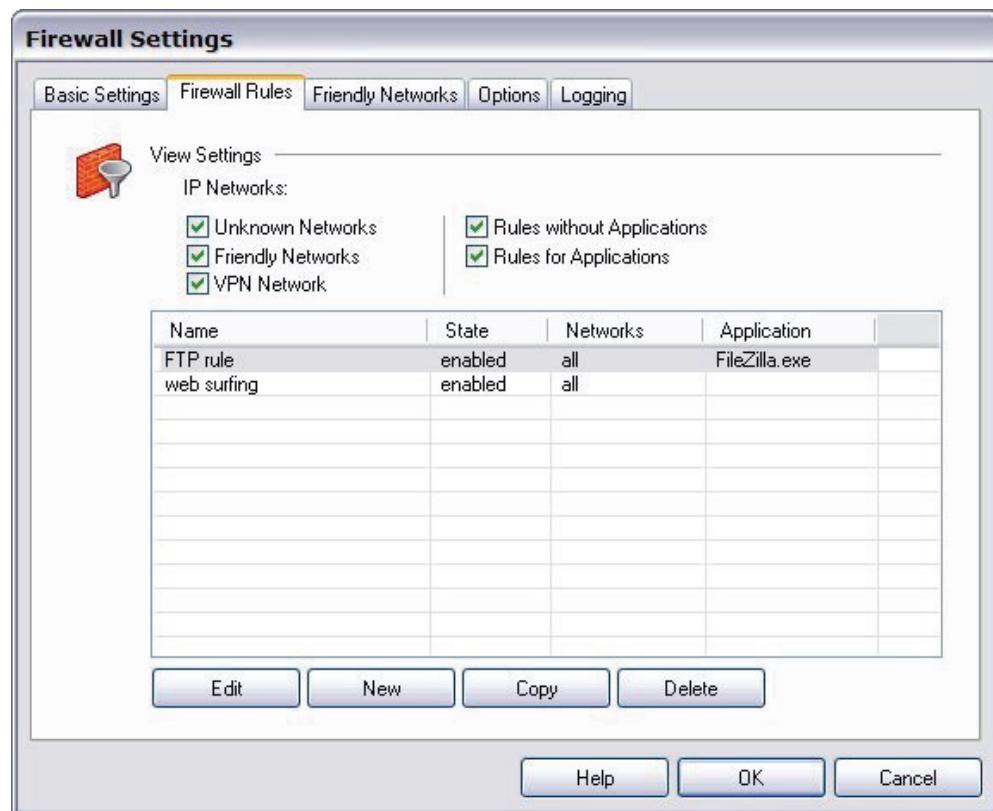
1. From the **Firewall Settings** dialog box, click the **Friendly Networks** tab.
2. Click **New** to add a new friendly network.

The Automatic Friendly Network detection feature does not work in this release of the Mobile VPN with IPSec client software.

Create firewall rules

You can create exceptions to the firewall mode you set when you enabled the firewall on the **Firewall Rules** tab of the **Firewall Settings** dialog box. For example, when you enabled the firewall if you selected **Basic Locked Settings**, then the rules you create here allow traffic. If you selected **Basic Open Settings**, then the rules you create here deny traffic. Firewall rules can include multiple port numbers from a single protocol.

Select or clear the check boxes below **View Settings** to show or hide categories of firewall rules.



To create a rule, click **New**. Use the four tabs in the **Firewall Rule Entry** dialog box to define the traffic you want to control:

- [General tab](#)
- [Local tab](#)
- [Remote tab](#)
- [Applications tab](#)

General tab

You can define the basic properties of your firewall rules on the **General** tab of the **Firewall Rule Entry** dialog box.

Rule Name

Type a descriptive name for this rule. For example, you might create a rule called Web surfing that includes traffic on TCP ports 80 (HTTP), 8080 (alternate HTTP), and 443 (HTTPS).

State

To make a rule inactive, select **Disabled**. New rules are enabled by default.

Direction

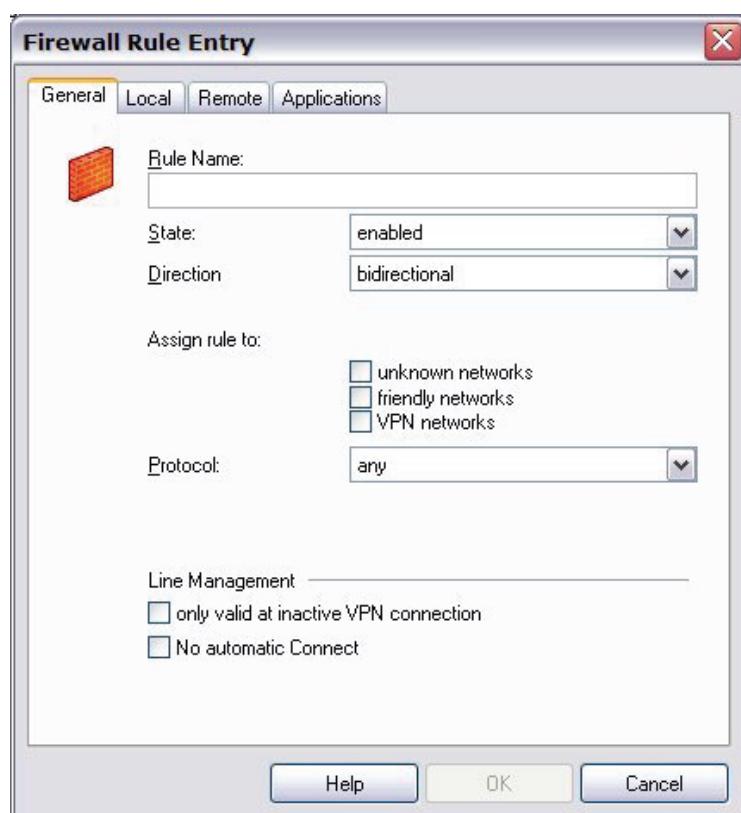
To apply the rule to traffic that comes from your computer, select **outgoing**. To apply the rule to traffic that is sent to your computer, select **incoming**. To apply the rule to all traffic, select **bidirectional**.

Assign rule to

Select the check boxes adjacent to the network types that this rule applies to.

Protocol

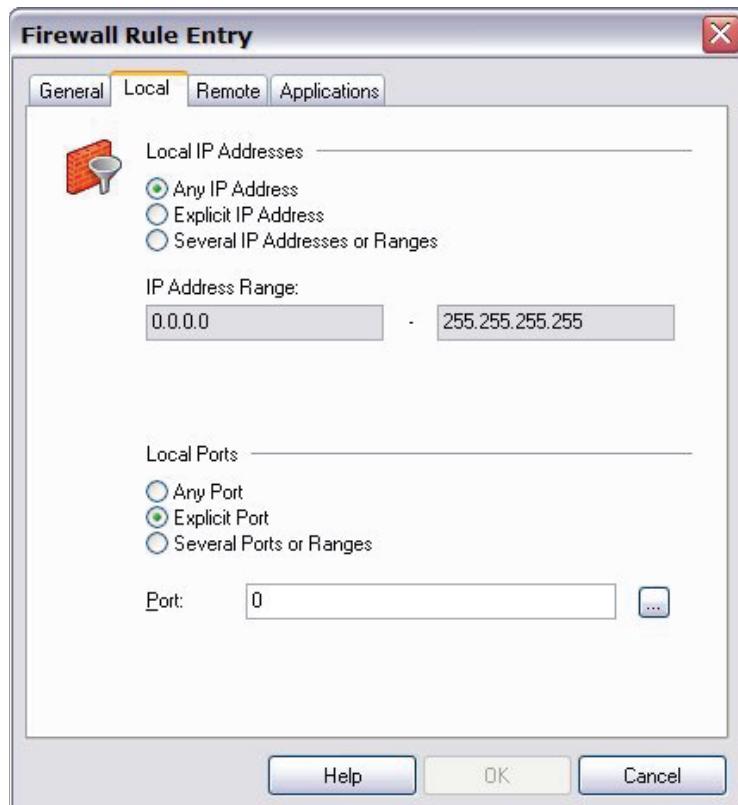
Use this drop-down list to select the type of network traffic you want to control.



Local tab

You can define any local IP addresses and ports that are controlled by your firewall rule on the **Local** tab of the **Firewall Rule Entry** dialog box. We recommend that, in any rule, you configure the **Local IP Addresses** setting to enable the **Any IP address** radio button. If you are configuring an incoming policy, you can add the ports to control with this policy in the Local Ports settings. If you want to control more than one port in the same policy, select **Several Ports or Ranges**. Click **New** to add each port.

If you select the **Explicit IP Address** radio button, make sure you specify an IP address. The IP address must not be set to 0.0.0.0.

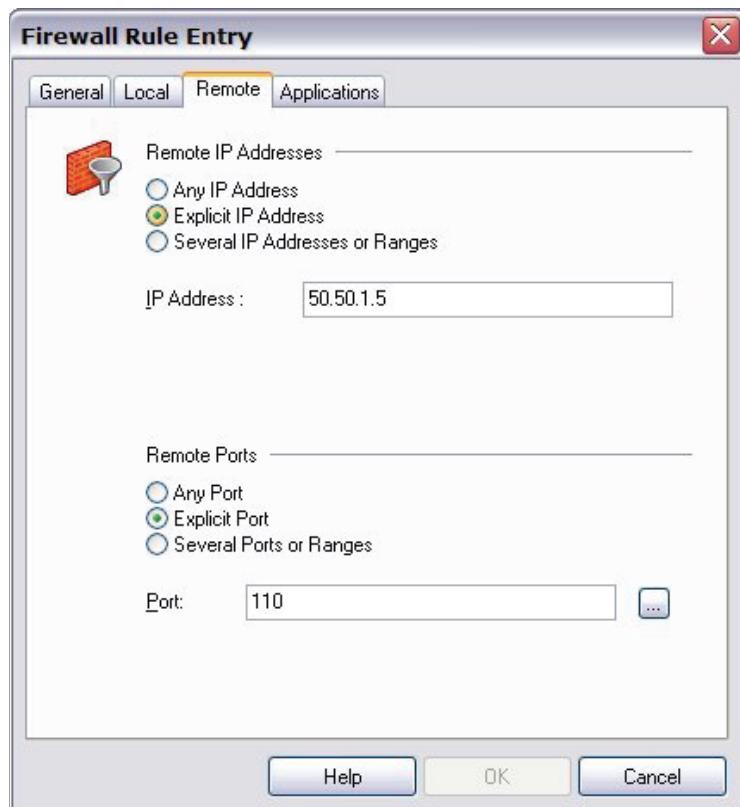


Remote tab

You can define any remote IP addresses and ports that are controlled by this rule on the **Remote** tab of the **Firewall Rule Entry** dialog box.

For example, if your firewall is set to deny all traffic and you want to create a rule to allow outgoing POP3 connections, add the IP address of your POP3 server as an **Explicit IP Address** in the **Remote IP Addresses** section. Then, in the **Remote Ports** section, specify port 110 as an **Explicit Port** for this rule.

If you select the **Explicit IP Address** radio button, make sure you specify an IP address. The IP address must not be set to 0.0.0.0.



Applications tab

You can limit your firewall rule so that it applies only when a specific application is used.

1. On the **Applications** tab of the Firewall Rule Entry dialog box, select the **Bind Rule To Application below** check box.



2. Click **Select Application** to browse your local computer for a list of available applications.
3. Click **OK**.

21 About Mobile VPN with SSL

The WatchGuard Mobile VPN with SSL client is installed on a user's computer, whether the user travels or works from home. The user can then connect with a standard Internet connection and activate the Mobile VPN client.

The Mobile VPN client then creates an encrypted tunnel to your trusted and optional networks, which are protected by a WatchGuard Firebox. The Mobile VPN client allows you to supply remote access to your internal networks and not compromise your security.

The Mobile VPN with SSL client uses Secure Sockets Layer (SSL) to secure the connection.

Before You Begin

- Make sure your client meets these basic [client requirements](#).
- Decide whether you want to require that all remote user Internet traffic routes through the VPN tunnel to the Firebox. For more information, see [Options for Internet access through a Mobile VPN tunnel](#).

Steps required to set up your tunnels

1. [Configure the Firebox for Mobile VPN with SSL](#). This process automatically creates a Firebox authentication group called SSLVPN-Users.
2. [Add remote users to authentication groups](#). If you want to use the Firebox as an authentication server, add users to the SSLVPN-Users group. If you want to use a third-party authentication server, use the instructions provided in that vendor's documentation.
3. Tell your remote users to [download the client software](#) from your Firebox.
4. Tell your remote users to [install the client software](#) on their computers.

Remote users can now [connect to the Firebox with the Mobile VPN with SSL client](#).

Options for Mobile VPN with SSL tunnels

If your network has special security needs, you can modify the advanced settings for your Mobile VPN with SSL tunnels.

Client requirements

The WatchGuard Mobile VPN with SSL product supplies a VPN client for all Firebox X e-Series devices. It does not provide endpoint security.

You can install the Mobile VPN with SSL client software on computers with the following operating systems:

- Microsoft Windows Vista (32 bit)
- Microsoft Windows XP (32 bit)
- Microsoft Windows 2000
- Mac OS X, versions 10.3 through Leopard

If the client computer is running Windows Vista or Windows XP, you must log on using an account that has administrator rights to install the Mobile VPN client software. Administrator rights are not required to connect after the client has been installed and configured.

If the client computer is running Mac OS X, admin rights are not required to install or to run the client.

Enable Mobile VPN with SSL for a Firebox user

When you enable Mobile VPN with SSL on your Edge, you must enable access for each remote user who uses SSL to connect to the Edge.

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X 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 Users Accounts, click the **Edit** button to edit an existing user account, or **Add** to add a new user account.
4. From the New or Edit page that appears, select the **Allow remote access with Mobile VPN with SSL** check box.

Enable Mobile VPN with SSL for a group

When you enable Mobile VPN with SSL on your Edge, you must make sure to enable access for each remote user or group who uses SSL to connect to the Edge. If you use extended authentication, you must configure the group name to match exactly the name of the group on your authentication server. The Firebox supports extended authentication to an LDAP/Active Director or a RADIUS authentication server.

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

3. In the **Account name** text box, type the name for the group. If you use extended authentication to an LDAP, Active Directory, or RADIUS authentication server, make sure you type the name of the group exactly the same as it was entered on the authentication server.
4. 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.
5. In the **Administrative Access** drop-down list, set the level to which the members of this group can see and change the Firebox X Edge configuration properties: **None**, **Read-Only**, or **Full**.
6. In the **Session maximum timeout** field, set the maximum length of time the computers in this group can send traffic to the external network or through a Branch Office VPN tunnel. If this field is set to zero (0) minutes, there is no session timeout and the user can stay connected for any length of time.
7. In the **Session idle timeout** field, set the length of time the computers in this group can stay authenticated when idle (not passing any traffic to the external network, through the Branch Office VPN, or to the Firebox X Edge itself). A setting of zero (0) minutes means there is no idle timeout.
8. If you want the users in this group to have Internet access, select the **Allow access to the External Network** check box.

9. If you want the users in this group to have access to computers on the other side of a Branch Office VPN tunnel, select the **Allow access to manual and managed VPN tunnels** check box.
10. If you want the users in this group to be able to use Mobile VPN with PPTP to the Edge for secure remote access, select the **Allow remote access with Mobile VPN with PPTP** check box.
11. If you want the users in this group to be able to use Mobile VPN with SSL to the Edge for secure remote access, select the **Allow remote access with Mobile VPN with SSL** check box.
12. Click **Submit**.

Enable the Edge to use Mobile VPN with SSL

1. To connect to the System Status page, type `https://` in the browser address bar, and the IP address of the Firebox X Edge trusted interface.
The default URL is `https://192.168.111.1`
2. From the navigation bar, select **VPN > Mobile VPN with SSL**.
The SSL VPN page appears.
3. To enable Mobile VPN with SSL, select the **Enable Mobile VPN with SSL** check box.
4. Configure the settings on the **General** and **Advanced** tabs. Each setting is described below.

SSL VPN General Tab

VPN

WatchGuard Mobile VPN with SSL

Enable WatchGuard Mobile VPN with SSL

General **Advanced**

Gateway

Primary: 192.168.54.63 Secondary:

Routes

Force all traffic through tunnel.

Virtual IP Address Range

Start: 0.0.0.0 End: 0.0.0.0

[Learn more about configuring Mobile VPN with SSL.](#)

Submit **Reset**

Gateway

The Gateway is the public IP address that Mobile VPN clients connect to. You must type an IP address assigned to the external interface of your Edge. If you have configured more than one IP address for your external interface, or you have configured WAN failover with the WAN2 port on your Edge, add this IP address in the **Secondary** text box. The Edge tries to connect to the secondary IP address if it cannot connect to the primary IP address.

If you use the dynDNS service because your Firebox has a dynamic IP address, you can type the domain name instead of an IP address in these fields.

Routes

Select **Force all traffic through the tunnel** if you want all client traffic to be routed through the Mobile VPN tunnel. If this check box is clear, only traffic sent to the trusted or optional networks is routed through the tunnel.

Virtual IP Address Range

When a Mobile VPN user connects to the Edge, the Edge must assign that user's computer an available IP address from a network behind the Edge. Type the first IP address in the address pool the Edge can use to assign Mobile VPN connections in the **Start of IP address pool** field. The Edge gives out this IP address to the first Mobile VPN with SSL client that connects. The Edge increments the IP address by 1 and assigns an address to each subsequent Mobile VPN client that connects. If the virtual IP address range you specify is from the trusted network, Mobile VPN with SSL clients bridge to the trusted network. If the virtual IP address range you specify is from the optional network, clients bridge to the optional network.

SSL VPN Advanced tab

[Enable WatchGuard Mobile VPN with SSL](#)

General **Advanced**

Authentication:

Encryption:

Protocol: Port:

Keep Alive: Interval: Seconds

 Timeout: Seconds

DNS and WINS Servers

Domain Name:

DNS Servers:

WINS Servers:

Enable debug logging

[Learn more about configuring Mobile VPN with SSL.](#)

Submit **Reset**

Authentication

From the **Authentication** drop-down list, select the authentication algorithm to use.

Encryption

From the Encryption drop-down list, select the encryption algorithm to use.

Protocol and Port

By default, SSL traffic uses the TCP protocol on port 443. Most users do not change this setting. You must configure Mobile VPN with SSL to use a different port and protocol if you have a firewall policy that allows incoming HTTPS. The Edge cannot apply static NAT to allow incoming HTTPS and allow Mobile VPN with SSL connections on the same port.

Keep Alive

The **Keep Alive** interval controls how often the Edge sends traffic through the tunnel to keep the tunnel active when no other traffic is being sent through the tunnel. If no response is received before the timeout value the tunnel will be dropped.

DNS and WINS Servers

The Domain Name Service (DNS) changes host names into IP addresses. WINS changes NetBIOS names to IP addresses. By default, SSL VPN users that connect to the Edge use the WINS and DNS servers identified on the **Network > Trusted** page of your Edge configuration. If you want to specify a different WINS or DNS server, add it in the **DNS Server** and **WINS Server IP Address** text boxes near the bottom of the Mobile User page.

If your DNS provider requires it, specify a search name for your domain.

Enable debug logging

Select this check box to increase the verbosity of log messages for Mobile VPN with SSL. This is useful if you have a problem that you must troubleshoot.

Download the client software

To download the Mobile VPN client software, connect to the Firebox with a web browser.

Each user must type:

`https://IP address of a Firebox interface:4100/`

or

`https://Host name of the Firebox:4100/`

The client software is also available on the Software Downloads section of the LiveSecurity web site.

You can download a version of the client software after you connect and authenticate. There are two available versions: Windows and Mac OS X. If you are not configured as a Mobile VPN with SSL user, you see the standard authentication dialog box.

After you download and install the client software, the Mobile VPN client software automatically connects to the Firebox to get its configuration. Each time you connect to the Firebox, the client software checks for configuration updates to make sure the client configuration is always current.

About the Mobile VPN with SSL client

The WatchGuard Mobile VPN with SSL client is installed on a user's computer, whether the user travels or works from home. The user can then connect with a standard Internet connection and activate the Mobile VPN client. The Mobile VPN client then creates an encrypted tunnel to the trusted and optional networks, which are protected by a WatchGuard Firebox.

As a remote user, you must do the following to set up the Mobile VPN with SSL client on your computer:

1. [Download the client software](#).
2. [Install the client software](#) on your computer.

You can now [Connect to the Firebox with the Mobile VPN with SSL client](#).

Install the Mobile VPN with SSL client software (Windows Vista and Windows XP)

After Mobile VPN with SSL has been enabled on the Firebox and users are added to the SSL-VPN Users group, remote clients can install the client software.

1. Open a web browser on the remote client computer to connect and authenticate to the Firebox.
For more information about how to connect and authenticate to your Firebox, see [About the client software](#).
2. Click the **Download** button for WG-MVPN-SSL.exe.
3. Save the file to the hard drive of the client PC.
If Mobile VPN with SSL is not enabled on the Firebox, or the user is not part of the SSL-VPN Users group, the Download button does not appear.
4. Double click **WG-MVPN-SSL.exe**.
The Mobile VPN with SSL client Setup Wizard starts.
5. Accept the default settings in the Wizard.
6. If you want to add a desktop icon or a Quick Launch icon, select the corresponding check box in the Wizard.
A desktop or Quick Launch icon is not required. The client icon is added to the Windows Start menu.
7. Finish and exit the wizard.

To run the client software, you do not need to reboot the computer.

Install the Mobile VPN with SSL client software (Mac OS X)

After Mobile VPN with SSL has been enabled on the Firebox and users are added to the SSL-VPN Users group, remote clients can install the client software.

1. Open a web browser on the remote client computer to connect and authenticate to the Firebox.
For more information about how to connect and authenticate to your Firebox, see [About the client software](#).
2. Click the **Download** button for WG-MVPN-SSL.dmg.
3. Save the file to the hard drive of the client PC.
If Mobile VPN with SSL is not enabled on the Firebox, or the user is not part of the SSL-VPN Users group, the Download button does not appear.
4. Double click **WG-MVPN-SSL.dmg**.
A volume named WatchGuard Mobile VPN is created.
5. In the WatchGuard Mobile VPN volume, double-click **WatchGuard Mobile VPN with SSL Installer V15.mpkg**.
The client installer starts.
6. Accept the default settings in the installer.
7. Finish and exit the installer.

To run the client software, you do not need to reboot the computer.

Connect to the Firebox with the Mobile VPN with SSL client (Windows Vista and Windows XP)

After you have installed the Mobile VPN with SSL client, you can connect to your Firebox.

1. Use one of these three methods to start the client software:
 - Select **Start > All Programs > WatchGuard > Mobile VPN with SSL client > Mobile VPN with SSL client**.
 - Double click the Mobile VPN with SSL client icon on the desktop.
 - Click the Mobile VPN with SSL client Quick Launch icon.
2. Type the information for the Firebox you are connecting to, and the username and password for the user.
The Server is the IP address of the primary external interface of the Firebox.
3. Click **Connect**.

Connect to the Firebox with the Mobile VPN with SSL client (Mac OS X)

After you have installed the Mobile VPN with SSL client, you can connect to your Firebox.

1. Open a Finder window and go to **Applications > WatchGuard** and double-click **WatchGuard Mobile VPN with SSL.app**.
The WatchGuard logo appears in the menu bar.
2. Click the icon and select **Connect**.
3. Enter the information for the Firebox you are connecting to, and the username and password for the user.
The Server is the IP address of the primary external interface of the Firebox.
4. Click **Connect**.

Mobile VPN with SSL client controls

When the Mobile VPN with SSL client is running, the WatchGuard logo icon appears in the System Tray (Win) or on the right side of the menu bar (Mac). The VPN connection status is displayed in the icon's magnifying glass.

-  The client is running but the VPN connection is not established.
-  The VPN connection has been established. You can securely connect to resources behind the Firebox.
-  The client is in the process of connecting or disconnecting the SSL VPN.

To see the client controls list, right-click (Win), or click (Mac), the WatchGuard logo icon.

Connect or Disconnect

Connect or disconnect the SSL VPN connection.

View Logs

Opens LogViewer to see the available log files.

Properties

Windows — Select **Launch program on startup** to start the client when Windows starts. Type a number for **Log level** to change the level of detail included in the logs.

Mac OS X — Show detailed information about the SSL VPN connection. You can also set the log level.

About

The WatchGuard Mobile VPN dialog box opens with information about the client software.

Exit (Win) or Quit (Mac)

Disconnect any SSL VPN connection and shut down the client.

Uninstall the Mobile VPN with SSL client

You can use the uninstall application to uninstall the Mobile VPN with SSL client.

Mobile VPN with SSL client for Windows Vista and Windows XP

1. Select **Start > All Programs > WatchGuard > Mobile VPN with SSL client > Uninstall Mobile VPN with SSL client**.
The Mobile VPN with SSL client Uninstall starts.
2. Click **Yes** to remove the Mobile VPN with SSL client and all of its components.
3. When the uninstall is complete, click **OK**.

Mobile VPN with SSL client for Mac OS X

1. Open a Finder window and go to **Applications > WatchGuard**. Double-click **Uninstall WG SSL VPN.app**.
2. Click **OK** in the **Warning** dialog box.
3. Click **OK** in the **Done** dialog box.
4. Drag the **Applications > WatchGuard** folder to the trash.
The uninstall application cannot delete itself or the folder it is in. If you do not drag the folder to the trash, it is not deleted.