

WatchGuard System Manager User Guide

WatchGuard System Manager v10.1
Fireware v10.1
Fireware Pro v10.1



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: 04/08/2008

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	Transmission 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

Table of Contents

Chapter 1	Introduction to Networks and Network Security	1
	About networks and network security	1
	About IP addresses.....	1
	Private addresses and gateways.....	2
	About subnet masks	2
	About slash notation	2
	About entering IP addresses.....	3
	Static and dynamic IP addresses	3
	About Domain Name Service (DNS).....	3
	About services and policies	3
	About ports	4
Chapter 2	Introduction to WatchGuard System Manager and Firewall	5
	Introduction to WatchGuard System Manager.....	5
	WatchGuard System Manager tools.....	6
	About WatchGuard Servers.....	6
	Fireware and Fireware Pro	8
	About WatchGuard System Manager and WFS	8
Chapter 3	Getting Started	9
	Before you begin.....	9
	Verify basic components	9
	Get a Firebox feature key	9
	Decide where to install server software.....	11
	Back up your previous configuration.....	12
	Download WatchGuard System Manager software	12
	About software encryption levels.....	13
	About the Quick Setup Wizard	13
	If you have problems with the wizard	14
	After the wizard finishes	15
	Quick Setup Wizard (non-web).....	15
	About setting the log encryption key.....	15
	After the wizard finishes	15
	After your installation.....	16
	Customize your security policy	16
	About LiveSecurity Service	16

Start WatchGuard System Manager	17
Connect to a Firebox.....	17
Disconnect from a Firebox	18
Disconnect from all Fireboxes.....	18
Start security applications	18
Policy Manager.....	18
Firebox System Manager.....	18
HostWatch	18
LogViewer	18
WatchGuard Reports.....	19
Quick Setup Wizard	19
CA Manager.....	19
If you have a backup file	21
If you do not have a backup file.....	21
Install WSM and keep an older version	22
Install WatchGuard Servers on computers with desktop firewalls	22
Add secondary networks to your configuration.....	25
Use the Quick Setup Wizard during installation	25
Add the secondary network after the Firebox installation is complete.....	25
About connecting the Firebox cables	26
Chapter 4 Service and Support	27
About Watchguard Support	27
About LiveSecurity Solutions	27
Threat responses, alerts, and expert advice	27
Access to technical support and training.....	27
LiveSecurity Broadcasts.....	28
Activate LiveSecurity Service.....	30
WatchGuard Users Forum.....	30
Using the WatchGuard Users Forum.....	30
Product documentation.....	30
About WatchGuard technical support.....	31
LiveSecurity Service technical support	31
Firebox installation service.....	32
VPN installation service.....	32
Chapter 5 Firebox Status Monitoring	33
About Firebox System Manager (FSM)	33
Firebox System Manager menus, icons, and buttons.....	34
Firebox System Manager menus	34
Firebox System Manager buttons	35
Start Firebox System Manager	35
Refresh Interval	36
Pause/Continue	36
Warnings	37
Expand and close tree views.....	37
Triangle display.....	38
Star display	38
Traffic volume, processor load, and basic status	39
Firebox status	40
Status and warnings.....	40
Certificates and their current status	42

VPN tunnel status and security services	42
Mobile VPN tunnel status.....	43
Security Services status.....	43
Change Traffic Monitor settings	44
Show log field names	45
Use color for log messages.....	46
Learn more about a message	47
Enable notification for specific messages	47
Visual display of bandwidth usage (Bandwidth Meter tab)	48
Change the scale	49
Add and remove lines	49
Change colors.....	49
Change how interfaces appear	49
Visual display of policy usage (Service Watch tab)	50
Change the scale	51
Display bandwidth used by a policy	51
Add and remove lines	51
Change colors.....	51
Change how policy names appear	51
Show connections by policy or rule	51
Traffic and performance statistics (Status Report).....	52
Add and remove sites.....	55
Security services	55
spamBlocker statistics	57
The HostWatch window	58
DNS resolution and HostWatch	58
Start HostWatch.....	58
Pause HostWatch	58
Select a new interface to monitor	59
Filter content of HostWatch window.....	60
Change HostWatch visual properties	61
Visit or block a site from HostWatch	61
About the Performance Console.....	62
Start the Performance Console	62
Make graphs with the Performance Console.....	62
Types of counters.....	62
Stop monitoring or close the window.....	62
Define performance counters	63
Add charts or change polling intervals.....	66
Add a new chart.....	66
Change the polling interval.....	66
Delete a chart	66
See and manage Firebox certificates.....	67
See current certificates.....	67
Delete a certificate	68
Retrieve the CRL from an LDAP server	70
See and synchronize feature keys	71
Synchronize feature keys	72
Communication log.....	72
Perform operations in Firebox System Manager.....	73
Synchronize time	73
Clear the ARP cache	73

See and synchronize feature keys.....	74
Synchronize feature keys	75
Clear alarms.....	75
Rekey BOVPN tunnels.....	75
To rekey one BOVPN tunnel.....	75
To rekey all BOVPN tunnels	76
Control High Availability	76
Change passphrases from Firebox System Manager.....	76
Chapter 6 Firebox Administration and Global Settings	77
About feature keys	77
When you purchase a new feature.....	77
See features available with the current feature key.....	77
Verify feature key compliance.....	77
Get a feature key	78
Import a feature key to the Firebox.....	79
Remove a feature key	79
See the details of a feature key	80
Download a feature key.....	80
Set the time zone and basic device properties.....	82
About SNMP	83
SNMP polls.....	83
SNMP traps and inform requests.....	83
Enable SNMP polling	84
Enable SNMP traps or inform requests	85
Make the Firebox send a trap for a policy	86
About Management Information Bases (MIBs)	86
About aliases	88
Alias members.....	88
Create an alias	89
If you want to add an address, address range, DNS name, or another alias to the alias..	90
If you want to add an authorized user or group to the alias	90
Enable TCP SYN checking	92
Disable Traffic Management and QoS.....	93
About global VPN settings	93
Enable IPSec Pass-through	93
Enable LDAP server for certificate verification	94
BOVPN Notification	94
Create schedules for Firebox actions.....	95
Chapter 7 Configuration Files	99
About Firebox configuration files.....	99
Open a configuration file	99
Open the configuration file with WatchGuard System Manager	99
Open the configuration file with Policy Manager	100
Open a local configuration file	101
Make a new configuration file.....	101
Save the configuration file.....	101
Save a configuration directly to the Firebox.....	102
Save a configuration to a local hard drive.....	102
Restore a Firebox backup image.....	104

Reset a Firebox to a previous or new configuration	104
Reset a Firebox X e-Series device	104
Reset a Firebox X Core or Peak (non e-Series)	104
Reset a non e-Series device manually	104
Use an existing configuration for a new Firebox model	106
Find the number of interfaces for a Firebox model	106
Chapter 8 Logging and Notification	107
About logging and log files	107
Log Servers	107
LogViewer	107
Logging and notification in applications and servers	108
About log messages	108
Types of log messages	108
Traffic log messages	108
Alarm log messages	108
Event log messages	109
Debug log messages	109
Statistic log messages	109
About notification	109
Configure your Log Server for notification	109
Define where the Firebox sends log messages	110
Add a Log Server	111
Use the Add Event Processor dialog box	111
Set Log Server priority	112
Configure syslog	112
Disable performance statistic logging	114
Enable advanced diagnostics	115
Configure logging and notification for a policy	116
Set logging and notification preferences	117
Send log message	117
Send SNMP trap	118
Send notification	118
Set up a Log Server	119
About passphrases	119
Install the Log Server	119
Configure your system settings	120
Database and SMTP server settings for a Log Server	122
Database Settings	122
SMTP Server Settings	123
Expiration settings for a Log Server	123
Log deletion settings	124
Database backup settings	124
Notification setup	124
Logging and monitoring settings for a Log Server	125
Restore a backup log file	126
Import a log file to a Log Server	127
Move the log data directory	127
Change the Log Server encryption key	128
Reclaim free space from the Log Server database	128
Use LogViewer to see log files	129
Open LogViewer	129
LogViewer toolbars	131

Open logs for the Primary Log Server	132
General settings.....	133
View settings.....	134
Log message details.....	135
Open Search Manager.....	137
Create a Search Query	137
Save a search	138
Remove a search	138
Edit a search	138
Run a search	138
Clear the search history	138
Run local diagnostic tasks	140
Import and export data to LogViewer	141
Import data.....	141
Export data	141
Email, print, or save log messages	141
Send a log message in email.....	141
Print a log message	141
Save a log message	141
Chapter 9 Network Setup and Configuration	143
About network interface setup.....	143
Configure Firebox interfaces	144
Configure the Firebox as a DHCP server.....	146
Make the Firebox a DHCP relay agent	148
Disable an interface.....	149
Configure external interfaces.....	151
If the IP address is static.....	151
If the IP address is assigned through PPPoE	151
If the IP address is assigned through DHCP	153
Set up the Firebox for dynamic DNS.....	153
Network Interface Card (NIC) settings	159
Set Outgoing Interface Bandwidth.....	160
PMTU Setting for IPSec	162
About network configuration in drop-in mode.....	163
Configure related hosts	164
About virtual local area networks (VLANs)	165
VLAN requirements and restrictions.....	165
About tagging	166
Define a new VLAN.....	166
Use DHCP on a VLAN	168
Use DHCP relay on a VLAN.....	168
Assign interfaces to a VLAN.....	169
Chapter 10 Network Setup with Multiple External Interfaces	171
About using multiple external interfaces	171
Multi-WAN requirements and conditions	171
Multi-WAN and High Availability.....	172
About multi-WAN methods	172
About multi-WAN in round-robin order	172
About the WAN Failover method.....	172
About the Interface Overflow method	173
About multi-WAN with the routing table	173
Before you begin	174

Routing Table mode and load balancing	174
Configure the interfaces	174
About the Firebox route table.....	175
Multi-WAN methods and routing	175
When to use the Routing Table method	175
When to use the Round-Robin method.....	176
Routing Table mode and load balancing	176
Before You Begin.....	177
Configure the interfaces	177
Before You Begin.....	179
Configure the interfaces	179
Configure the multi-WAN Round-robin option	180
Before You Begin.....	180
Configure the interfaces	180
About advanced multi-WAN settings	182
About sticky connections.....	182
Set a global sticky connection duration	183
Set the fallback action	183
Time needed for the Firebox to update its route table.....	185
Define a link monitor host	185
Chapter 11 Network Address Translation (NAT)	187
About Network Address Translation (NAT)	187
Types of NAT	187
About dynamic NAT.....	188
Add firewall dynamic NAT entries	188
Reorder dynamic NAT entries.....	189
Disable policy-based dynamic NAT	191
About 1-to-1 NAT.....	191
About 1-to-1 NAT and VPNs.....	192
Use firewall 1-to-1 NAT	192
Define a 1-to-1 NAT rule	193
Configure policy-based 1-to-1 NAT	194
Enable policy-based 1-to-1 NAT	194
Disable policy-based 1-to-1 NAT	194
About static NAT	194
Chapter 12 Authentication	201
About user authentication	201
How users can close a session	202
How administrators can close a user's session.....	202
Use authentication to restrict incoming traffic.....	202
Use authentication through a gateway Firebox	203
Set global authentication timeouts.....	204
Allow multiple concurrent logins.....	205
Use a custom default start page	205
Enable Single Sign-On.....	205
About the WatchGuard Authentication (WG-Auth) policy.....	205
About Single Sign-On (SSO).....	206
Before You Begin	206
Enable and configure SSO	207
Define SSO exceptions	207

Install the WatchGuard Single Sign-On (SSO) agent.....	208
Download the SSO agent software	208
Before you install.....	208
Install the SSO agent service.....	208
Enable SSO on your Firebox.....	209
Authentication server types.....	209
About using third-party authentication servers.....	209
Use a backup authentication server.....	210
Configure the Firebox as an authentication server	210
Types of Firebox authentication.....	210
Firewall authentication	210
Mobile VPN with PPTP connections	211
Configure a Mobile VPN with IPsec connection	211
Mobile VPN with SSL connections	212
Define a new user for Firebox authentication	212
Define a new group for Firebox authentication	214
Configure RADIUS server authentication.....	214
Authentication key	214
Before you begin	215
Use RADIUS server authentication with the Firebox.....	215
How RADIUS server authentication works.....	216
About RADIUS groups	217
Timeout and retry values	218
Configure SecurID authentication.....	221
Configure LDAP authentication	223
About LDAP optional settings.....	224
Before You Begin.....	225
Specify Active Directory or LDAP optional settings	225
About Active Directory optional settings.....	228
Before You Begin.....	229
Specify Active Directory or LDAP optional settings	229
Find your Active Directory search base	230
Special conditions.....	231
DN of Searching User, Password of Searching User fields	231
Change the default port for the Active Directory server	232
Configure the Firebox to use the global catalog port	232
To find out if your Active Directory server is configured to be a global catalog server	232
Use a local user account for authentication.....	232
Define users and groups for Firebox authentication	233
Define users and groups for third-party authentication	233
Add users and groups to policy definitions.....	234
Chapter 13 Firewall Threat Protection	235
About default threat protection.....	235
Set logging and notification options	237
About spoofing attacks.....	237
About port space and address space probes	238
To protect against port space and address space probes.....	239
How the Firebox identifies network probes.....	239
About flood attacks.....	240
About the SYN flood attack setting	241
About unhandled packets	241
See statistics on unhandled packets.....	242

About distributed denial-of-service attacks.....	242
About blocked sites	243
Permanently blocked sites.....	243
Auto-blocked sites/Temporary Blocked Sites list	243
Block a site permanently or block spyware sites	244
Configure logging for blocked sites.....	245
Block spyware sites.....	245
Use an external list of blocked sites	245
Create exceptions to the Blocked Sites list	246
Use an external list of blocked sites exceptions	246
About blocked ports.....	247
Default blocked ports	247
Block a port	248
Block IP addresses that try to use blocked ports	248
Set logging and notification for blocked ports.....	248
Chapter 14 Policies	249
About policies	249
Packet filter and proxy policies	249
About Policy Manager.....	250
Policy Manager window	250
Policy icons.....	250
Open Policy Manager	251
Change the Policy Manager view.....	251
Change colors used for Policy Manager text	253
Find a policy by address, port, or protocol	255
Add policies to your configuration	255
See the list of policy templates	256
Add a policy from the list of templates.....	258
Add more than one policy of the same type	259
See template details and modify policy templates	259
Disable a policy.....	260
Delete a policy.....	260
About custom policies	260
Create or edit a custom policy template	260
About policy properties	263
Policy tab.....	263
Proxy action settings (proxy policies only)	264
Advanced tab	264
Set access rules for a policy	264
Add new members for policy definitions.....	266
Configure logging and notification for a policy	267
Block sites temporarily with policy settings.....	268
Set a custom idle timeout.....	268
Set an operating schedule.....	269
Configure policy-based routing	269
Policy-based routing, failover, and failback	269
Restrictions on policy-based routing	270
Add policy-based routing to a policy	270
Configure policy-based routing with failover.....	271
About using static NAT for a policy	271

Apply a Traffic Management action to a policy	272
Use Traffic Management actions in a multi-WAN environment	273
Apply a Traffic Management action to multiple policies.....	273
About server load balancing for a policy	273
Set traffic priority for a policy	273
Set ICMP error handling.....	273
1-to-1 NAT.....	274
Dynamic NAT	274
Use QoS Marking for a policy.....	274
Add a sticky connection duration to a policy	274
About policy precedence.....	275
Use automatic order	275
Set precedence manually.....	275
About automatic policy order	275
Policy specificity and protocols	276
Traffic rules	276
Firewall actions	277
Schedules	277
Policy types and names	277
Chapter 15 Proxy Policies	279
About proxy policies.....	279
Types of proxies.....	279
About rules and rulesets.....	279
About working with rules and rulesets	280
Simple and advanced views.....	280
Add rules	280
Add rules (simple view).....	280
Add rules (advanced view)	281
Cut and paste rule definitions	282
Change the order of rules	282
About regular expressions.....	283
General guidelines.....	283
How to build a regular expression.....	284
Hexadecimal characters.....	284
Repetition	284
Ranges.....	285
Anchors.....	285
Alternation.....	285
Common regular expressions	286
About proxy actions.....	286
Set the proxy action in a proxy definition.....	286
Edit, delete, or clone proxy actions	287
Import or export proxy actions	287
About predefined and user-defined proxy actions.....	288
Add a proxy policy to your Firebox configuration.....	288
Policy tab.....	291
Properties tab	291
Proxy action settings.....	291
Advanced tab	292
DNS proxy: General settings	292
DNS proxy: OPcodes	293
Adding a new OPcodes rule.....	293

DNS proxy: Query types.....	294
Add a new query types rule	294
DNS proxy: Query names	295
Intrusion prevention in proxy definitions	295
Run the Activate Intrusion Prevention wizard from the Tasks menu in Policy Manager.....	295
Use the Intrusion Prevention ruleset in the proxy definition.....	295
Proxy and AV alarms	296
Finish and save the configuration.....	296
About MX (Mail eXchange) records.....	296
MX lookup.....	296
Reverse MX lookup	297
MX records and multi-WAN.....	297
Add another host name to an MX record.....	297
About the FTP proxy	298
Policy tab.....	298
Properties tab	298
Advanced tab	299
FTP proxy: General settings.....	300
FTP proxy: Commands	301
FTP proxy: Upload and download content.....	302
Configure Gateway AntiVirus actions.....	302
Create alarms or log entries for antivirus actions	304
Intrusion prevention in proxy definitions	305
Run the Activate Intrusion Prevention wizard from the Tasks menu in Policy Manager.....	305
Use the Intrusion Prevention ruleset in the proxy definition.....	305
Proxy and AV alarms	305
Finish and save the configuration.....	306
About the H.323 proxy.....	306
Configure the H.323 proxy action settings	307
About the HTTP proxy.....	307
HTTP and WebBlocker	307
Policy tab.....	307
Properties tab	308
Proxy action settings.....	308
Advanced tab	308
HTTP requests: General settings.....	309
HTTP requests: Request methods	310
HTTP requests: URL paths	312
HTTP requests: Header fields	312
HTTP requests: Authorization.....	313
HTTP responses: General settings.....	313
HTTP responses: Header fields	314
HTTP responses: Content types	314
Add, delete, or modify content types	314
HTTP responses: Cookies.....	315
Change settings for cookies.....	315
HTTP responses: Body content types	316
HTTP proxy exceptions	316
Proxy settings skipped	316
Proxy settings not skipped	316
Configure Gateway AntiVirus actions.....	317

Intrusion prevention in proxy definitions	322
Run the Activate Intrusion Prevention wizard from the Tasks menu in Policy Manager.....	322
Use the Intrusion Prevention ruleset in the proxy definition.....	322
Proxy and AV alarms	322
Allow Windows updates through the HTTP proxy	323
If you still cannot download Windows updates	323
Finish and save the configuration.....	323
About the HTTPS proxy	324
HTTPS and WebBlocker.....	324
Policy tab.....	324
Properties tab.....	324
Advanced tab	325
HTTPS Proxy: General settings	325
Proxy and AV alarms	326
About the POP3 proxy	327
Policy tab.....	327
Properties tab.....	327
Advanced tab	328
POP3 proxy: General settings	329
POP3 proxy: Content types	332
POP3 proxy: Headers	335
Configure Gateway AntiVirus actions.....	336
Create alarms or log entries for antivirus actions	338
POP3 proxy: Deny message	339
Intrusion prevention in proxy definitions	340
Run the Activate Intrusion Prevention wizard from the Tasks menu in Policy Manager.....	340
Use the Intrusion Prevention ruleset in the proxy definition.....	341
POP3 proxy: spamBlocker	341
Proxy and AV alarms	342
Finish and save the configuration.....	342
Configure the SIP proxy action settings	343
About the SMTP proxy	344
Policy tab.....	344
Properties tab.....	344
Advanced tab	345
SMTP proxy: General settings.....	346
SMTP proxy: Greeting rules	348
SMTP proxy: ESMTP settings.....	348
SMTP proxy: Authentication	349
SMTP proxy: Content types	350
Add common content types.....	350
SMTP proxy: File names	351
SMTP proxy: Mail From/Mail To	351
SMTP proxy: Headers	352
Configure Gateway AntiVirus actions.....	352
Create alarms or log entries for antivirus actions	354
SMTP proxy: Deny message	355
Intrusion prevention in proxy definitions	355
Run the Activate Intrusion Prevention wizard from the Tasks menu in Policy Manager.....	355
SMTP proxy: spamBlocker.....	356

Proxy and AV alarms	356
Configure the SMTP proxy to quarantine email	357
Finish and save the configuration.....	357
About the TCP-UDP proxy	358
Policy tab.....	358
Properties tab	358
Proxy action settings.....	358
Advanced tab	358
TCP-UDP proxy: General settings	359
TCP-UDP proxy: Application blocking	359
Intrusion prevention in proxy definitions	360
Run the Activate Intrusion Prevention wizard from the Tasks menu in Policy Manager	360
Use the Intrusion Prevention ruleset in the proxy definition.....	360
Finish and save the configuration.....	360
Policy tab.....	361
Properties tab	361
Proxy action settings.....	361
Advanced tab	361
TFTP proxy: General settings	362
TFTP proxy: Upload and download content	362
Import and export user-defined proxy actions	364
Chapter 16 WatchGuard Reports	367
About the Report Server	367
Set up the Report Server	367
About passphrases	367
Install the Report Server	367
Configure the Report Server	368
Expiration settings	371
Report generation settings.....	372
Logging settings.....	373
Reclaim free space from the Report Server database	374
Start or stop the Report Server.....	374
Report Manager toolbar	375
Open Report Manager.....	377
Connect to a different Report Server	377
Select reports to generate	380
Create Report dialog box settings	380
Create device groups.....	381
Specify a date range.....	381
Find a report in the list	382
Find details in a report	382
Change the report type	382
Send a report in email	383
Print a report.....	383
Save a report	383
Chapter 17 Management Server Setup and Administration	385
About the WatchGuard Management Server.....	385
Install the Management Server	385
About WatchGuard Server passphrases.....	385
Master passphrase	386
Server management passphrase.....	386

Password and key files	386
Microsoft SysKey utility	386
Set up the Management Server.....	387
Find your Management Server license key.....	388
Set properties for the certificate authority	389
Set properties for client certificates	390
Set properties for the Certification Revocation List (CRL)	390
Send diagnostic log messages for the certification authority	390
Add or remove a Management Server license	392
Configure notification	392
Control logging and configuration change settings	392
Update the Management Server with new gateway address	393
If your Management Server is configured with a public IP address	394
Update the Certificate Revocation List (CRL) distribution IP address	394
Update managed Firebox clients.....	395
Define user accounts for the Management Server.....	395
Change logging settings.....	395
Enable or disable logging	395
Add or prioritize Log Servers	396
Send messages to the Windows Event Viewer	396
Send messages to a file.....	396
Back up or restore the Management Server configuration	396
Back up the Management Server for troubleshooting.....	396
Move the WatchGuard Management Server to a new computer.....	397
Disconnecting from the Management Server	398
Chapter 18 Devices and VPNs in WatchGuard System Manager	399
Use the WatchGuard System Manager window.....	399
Device status.....	399
Device management: General navigation	400
About preparing devices for management	402
Configure a Firebox running Fireware as a managed client.....	403
Configure a Firebox III or Firebox X Core running WFS as a managed client	405
Prepare a new Firebox X Edge for management.....	407
Import Firebox X Edge devices into a Management Server	408
Prepare an installed Firebox X Edge for management	409
Configure a Firebox SOHO 6 as a managed client	410
Add managed devices to the Management Server	411
Set device management properties	414
Connection settings	414
IPSec tunnel preferences.....	416
Contact information.....	417
Update a device.....	418
Remove a device	418
VPN tunnels	419
Add a VPN resource.....	419
Configure network settings (Edge devices only)	420
Use the Firebox X Edge policy section	420
Chapter 19 Firebox X Edge Centralized Management	421
About Edge centralized management.....	421
See and delete firmware updates	424
Create and apply Edge Configuration Templates.....	424
Add a pre-defined policy with the Add Policy wizard	426

Add a custom policy with the Add Policy wizard	427
Clone an Edge Configuration Template	427
Apply Edge Configuration Templates to devices	428
Applying the template using drag-and-drop	428
Applying the policy to devices in the device list	428
Remove an Edge from the device list	429
About aliases and Edge devices	429
Give names to aliases	430
Define aliases on a Firebox X Edge	431
Chapter 20 Managed BOVPN Tunnels	433
About managed BOVPN tunnels	433
How to create a managed BOVPN tunnel	433
Tunnel options	434
VPN Failover	434
Global VPN settings	434
BOVPN tunnel status	434
Rekey BOVPN tunnels	434
Get the current resources from a device	435
Create a new VPN resource	436
Add a host or network	437
Add VPN Firewall policy templates	437
Add Security Templates	438
Removing a tunnel	443
Removing a device	443
Mobile VPN tunnel status	444
Security Services status	445
Chapter 21 Manual BOVPN Tunnels	447
About manual BOVPN tunnels	447
How to create a manual BOVPN tunnel	447
Custom tunnel policies	447
One-way tunnels	447
VPN Failover	448
Global VPN settings	448
BOVPN tunnel status	448
Rekey BOVPN tunnels	448
Edit and delete gateways	450
Define the credential method	451
If you selected Pre-Shared Key	451
If you selected Use IPSec Firebox Certificate	451
Define gateway endpoints	452
Define a tunnel	458
Edit and delete a tunnel	460
Add routes for a tunnel	460
Configure Phase 2 settings	461
Use advanced Security Association (SA) settings	462
Add an existing proposal	463
Create a new proposal	464
Edit or clone a proposal	464
Change order of tunnels	464

Define a custom tunnel policy	465
Choose a name for the policies.....	465
Select the policy type	465
Select the BOVPN tunnels.....	465
Create an alias for the tunnels.....	465
The BOVPN Policy Wizard has completed successfully	465
Set up outgoing dynamic NAT through a BOVPN tunnel	465
Define a route for all Internet-bound traffic	467
Configure the remote Firebox.....	467
If the remote Firebox is an Edge device.....	468
Configure VPN Failover.....	470
Define multiple gateway pairs	471
Force a BOVPN tunnel rekey	472
To rekey one BOVPN tunnel	472
To rekey all BOVPN tunnels	472
Security Services status	474
Chapter 22 Certificates and the Certificate Authority	475
About certificates.....	475
Certificate authorities and signing requests	475
Certificate lifetimes and CRLs	475
Create a certificate with FSM or the Management Server	476
Create a certificate with FSM	476
Create a certificate with CA Manager	478
Send the certificate request	479
Issue the certificate.....	479
Download the certificate.....	479
Import a certificate	480
Use certificates for authentication	481
Use certificates for Mobile VPN with IPSec tunnel authentication	481
Configure the web server certificate for Firebox authentication	482
See and manage Firebox certificates.....	484
See current certificates.....	484
Delete a certificate	485
Retrieve the CRL from an LDAP server	487
Use the web-based CA Manager	488
Chapter 23 Mobile VPN with PPTP	491
About Mobile VPN with PPTP	491
Mobile VPN with PPTP connections.....	491
Client requirements	492
Encryption levels	492
Configure WINS and DNS servers	493
Default-route VPN.....	494
Split tunnel VPN.....	494
Default-route VPN setup for Mobile VPN with PPTP	494
Split tunnel VPN setup for Mobile VPN with PPTP	494
Configure the Firebox for Mobile VPN with PPTP	495
Enable RADIUS or VASCO authentication	496
Set encryption for PPTP tunnels	496
MTU and MRU.....	496
Define timeout settings for PPTP tunnels	496
Make outbound PPTP connections from behind a Firebox.....	497

Add IP addresses for Mobile VPN sessions	497
Configure policies to allow Mobile VPN with PPTP traffic.....	499
Prepare client computers	500
Prepare a Windows NT or 2000 client computer: Install MSDUN and service packs.....	500
Create and connect a PPTP Mobile VPN for Windows Vista	500
Create a PPTP connection.....	500
Establish the PPTP connection	501
Create and connect a PPTP Mobile VPN for Windows XP	501
Create the PPTP Mobile VPN.....	501
Connect with the PPTP Mobile VPN	502
Create and connect a PPTP Mobile VPN for Windows 2000.....	502
Create the PPTP Mobile VPN.....	502
Connect with the PPTP Mobile VPN	502
Chapter 24 Mobile VPN with IPSec	503
About a Mobile VPN with IPSec configuration for your Firebox.....	503
Configure a Mobile VPN with IPSec connection.....	503
Client requirements	504
Options for Internet access through a Mobile VPN tunnel.....	504
Default-route VPN.....	504
Split tunnel VPN.....	504
About Mobile VPN client configuration files.....	504
Configure the external authentication server	509
Define advanced Phase 1 settings	516
Define advanced Phase 2 settings	518
Setting Options.....	518
Route Internet access through Mobile VPN tunnels	519
Configure WINS and DNS servers.....	519
Lock down an end-user profile	520
Configure policies to filter Mobile VPN traffic	520
Add individual policies.....	521
Change the view.....	521
Use the Any policy	521
Re-creating end-user profiles	522
Save the profile to a Firebox	522
Distribute the software and profiles	522
Making outbound IPSec connections from behind a Firebox.....	523
Terminate IPSec connections	523
Global VPN settings.....	523
See the number of Mobile VPN licenses.....	523
Purchase additional Mobile VPN licenses	523
Add feature keys.....	523
About the Mobile VPN with IPSec client	524
Client Requirements	524
Install the Mobile VPN with IPSec client software.....	525
Import the end-user profile.....	525
Select a certificate and enter the PIN	526
Uninstall the Mobile VPN client	526
Disconnect the Mobile VPN client	527
Control connection behavior.....	528
Mobile User VPN client icon	529
See Mobile VPN log messages	529

Secure your computer with the Mobile VPN firewall.....	529
About the desktop firewall.....	530
Enable the desktop firewall.....	531
Define friendly networks.....	531
Create firewall rules.....	532
Applications tab.....	536
Chapter 25 Mobile VPN with SSL	537
About Mobile VPN with SSL.....	537
Before You Begin.....	537
Steps required to set up your tunnels.....	537
Options for Mobile VPN with SSL tunnels.....	537
Client requirements.....	538
Options for Internet access through a Mobile VPN tunnel.....	538
Default-route VPN.....	538
Split tunnel VPN.....	538
Configure the Firebox for Mobile VPN with SSL.....	539
Define advanced settings for Mobile VPN with SSL.....	541
If you use the Firebox as an authentication server.....	543
If you use a third-party authentication server.....	543
Distribute the client software.....	543
About the Mobile VPN with SSL client.....	543
Download the client software.....	543
Install the client software.....	544
Windows Vista and Windows XP.....	544
Mac OS X.....	544
Connect to the Firebox with the Mobile VPN with SSL client.....	545
Windows Vista and Windows XP.....	545
Mac OS X.....	545
Mobile VPN with SSL client controls.....	545
Uninstall the Mobile VPN with SSL client.....	546
Mobile VPN with SSL client for Windows Vista and Windows XP.....	546
Mobile VPN with SSL client for Mac OS X.....	546
Chapter 26 WebBlocker	547
About WebBlocker.....	547
Get started with WebBlocker.....	547
Download the WebBlocker database.....	548
Run the Activate WebBlocker Wizard.....	548
Use exception rules to restrict web site access.....	549
Keep the WebBlocker database updated.....	549
Get an incremental update.....	549
Automate WebBlocker database downloads.....	549
See database status.....	550
About WebBlocker categories.....	550
Configure WebBlocker.....	550
Add new servers or change their order.....	551
Add a server.....	551
Change order of servers.....	552
Change categories to block.....	552
Send an alarm when a site is denied.....	552
Log WebBlocker actions.....	553
Add, remove, or change a category.....	554
See whether a site is categorized.....	555

Define advanced WebBlocker options.....	556
Cache size	556
Server timeout.....	556
Define WebBlocker alarms.....	557
Define the action for sites that do not match exceptions.....	558
Components of exception rules	558
Exceptions with part of a URL.....	558
Add exceptions.....	559
Change the order of exception rules	561
Import or export WebBlocker exception rules	561
Export rule to an ASCII file.....	563
Define additional WebBlocker actions	564
Add WebBlocker actions to a policy.....	564
Renew subscriptions from Firebox System Manager	567
Chapter 27 spamBlocker	569
About spamBlocker.....	569
spamBlocker actions, tags, and categories.....	570
spamBlocker tags	570
spamBlocker categories.....	571
Apply spamBlocker settings to your policies	572
About using spamBlocker with multiple proxies	573
Configure spamBlocker	574
About spamBlocker exceptions.....	576
Change the order of exceptions	577
Import and export exception rules.....	577
Import an ASCII exceptions file	578
Export rules to an ASCII file.....	578
Log exceptions.....	578
Configure Virus Outbreak Detection (VOD) actions	579
Configure spamBlocker to quarantine email.....	579
Set global spamBlocker parameters	580
Use an HTTP proxy server for spamBlocker	581
Add trusted email forwarders to improve spam score accuracy	581
Create rules for your email reader	582
Use RefID record instead of message text	584
Find the category a message is assigned to.....	585
spamBlocker statistics	585
Renew subscriptions from Firebox System Manager	586
Chapter 28 Quarantine Server	587
About the Quarantine Server	587
Install server components.....	588
Run the Setup Wizard	588
If you have already set up a Server	588
If you have not set up a Server	588
Define the server location.....	589
Configure the Quarantine Server.....	589
Set general server parameters	590
Change expiration settings and user domains	591
Change logging settings	594
Enable or disable logging	594
Add or prioritize Log Servers	594
Send messages to the Windows Event Viewer	594

Send messages to a file	594
Open the messages dialog box	597
Save messages or send to a user's inbox.....	598
Delete messages manually	598
Delete messages automatically	598
About managing users	599
Add users	600
Remove users	600
Change the notification option for a user.....	600
Get statistics on Quarantine Server activity	601
See statistics from specific dates	601
See specific types of messages	601
Group statistics by month, week, or day	601
Export and print statistics	601
Chapter 29 Signature-Based Security Services	603
About Gateway AntiVirus and Intrusion Prevention	603
Install and upgrade Gateway AV/IPS	603
About Gateway AntiVirus/Intrusion Prevention and proxy policies	604
Activate Gateway AV with a wizard.....	605
Create alarms or log entries for antivirus actions.....	612
Unlock a file locked by Gateway AntiVirus	612
Configure Gateway AntiVirus to quarantine email.....	613
Select proxy policies to enable	615
Configure signature exceptions	620
Copy IPS settings to other policies	620
Activate and configure Intrusion Prevention Service for TCP-UDP	621
Update Gateway AntiVirus/IPS and see status.....	621
Configure Gateway AV engine settings	621
Configure the Gateway AV/IPS update server.....	622
Connect to the update server through an HTTP proxy server.....	623
See status and update signatures or engine manually	623
See service status	623
To see service status:.....	624
See the update history	625
Update services manually	625
Renew security subscriptions	625
Renew subscriptions from Firebox System Manager	626
Chapter 30 Dynamic Routing	627
About dynamic routing	627
About routing daemon configuration files	627
About Routing Information Protocol (RIP)	628
Routing Information Protocol (RIP) commands.....	628
Configure the Firebox to use RIP v1	630
Allow RIP v1 traffic through the Firebox.....	631
Configure the Firebox to use RIP v2.....	631
Allow RIP v2 traffic through the Firebox.....	632
Sample RIP routing configuration file	632
About Open Shortest Path First (OSPF) Protocol	635
OSPF commands	635
Configure the Firebox to use OSPF	639
Allow OSPF traffic through the Firebox	640

About Border Gateway Protocol (BGP)	644
Configure the Firebox to use BGP	647
Allow BGP traffic through the Firebox.....	648
Chapter 31 Traffic Management and Quality of Service	651
About Traffic Management and QoS.....	651
Guarantee bandwidth	651
Restrict bandwidth	652
QoS Marking	652
Traffic priority	652
Set Outgoing Interface Bandwidth	652
Define a Traffic Management action	653
Determine available bandwidth.....	653
Apply a Traffic Management action to a policy	655
Use Traffic Management actions in a multi-WAN environment	655
Set traffic priority in a policy	656
Set connection and bandwidth limits	657
Before you begin	658
Per-interface and per-policy QoS Marking	658
QoS Marking and IPSec traffic	658
Chapter 32 High Availability	663
About WatchGuard High Availability	663
High Availability requirements and restrictions	664
About High Availability and proxy sessions	664
About High Availability and server load balancing	664
High Availability status	664
Install High Availability	664
Configure High Availability	665
Define HA interfaces	665
Select interfaces to be monitored.....	666
Define notification	666
Define HA Group ID and encryption settings	666
Finish the configuration	666
Set up hardware for HA.....	666
Synchronize the configuration.....	666
Create a backup image of a Firebox in an HA pair.....	667
Manually control High Availability	667
Upgrade software in an HA configuration.....	668
Chapter 33 WatchGuard File Locations	669
Locations of WatchGuard System Manager files.....	669
Locations of application and user-created files.....	670
Policy Manager for Fireware appliance software	670
Policy Manager for WFS appliance software.....	670
Flash Disk Management for WFS appliance software.....	671
Report Manager	671
LogViewer	671

1

Introduction to Networks and 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 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 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.

You have two methods to control DNS traffic through your firewall: the DNS packet filter and the DNS proxy policy. A packet filter examines the header information while a proxy examines the contents at the application layer and validates that the packet meets RFC compliance for DNS traffic.

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.

Ports are either open or closed. If a port is open, your computer accepts information and creates connections to other computers using the protocol identified with that port. However, an open port is a security risk. You can protect your network from risks created by open ports in these ways:

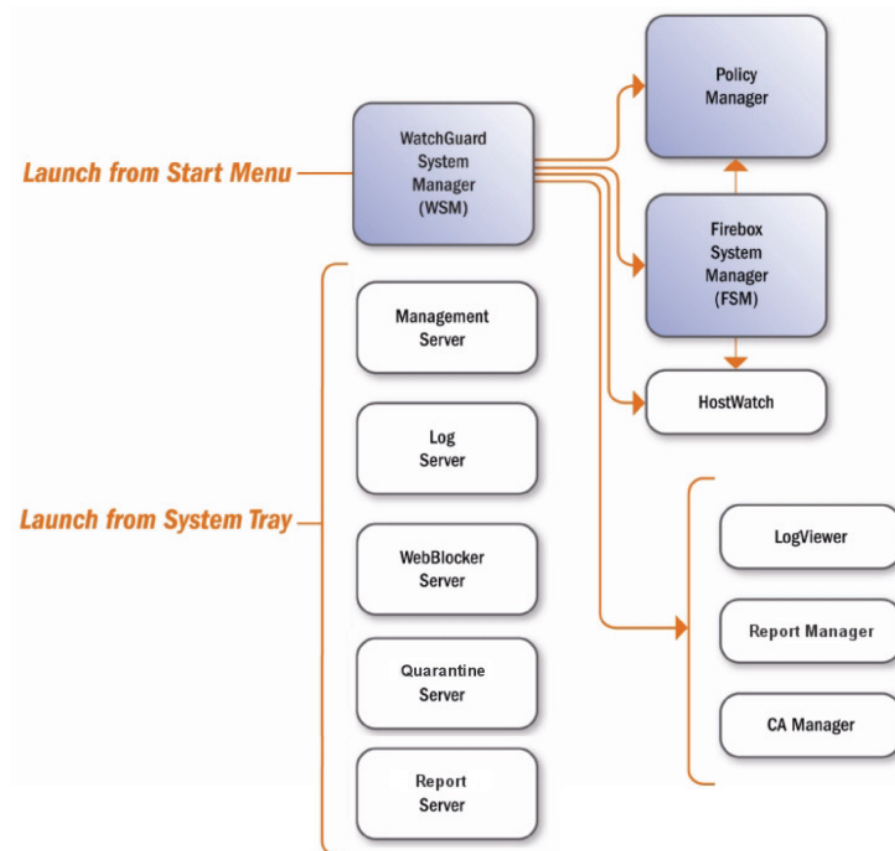
- Block ports used by hackers to attack your network. For more information, see [About blocked ports](#).
- Block port space probes—TCP or UDP traffic that is sent by a host to a range of ports to find information about networks and their hosts. For more information, see [About port space and address space probes](#).

2

Introduction to WatchGuard System Manager and Fireware

Introduction to WatchGuard System Manager

WatchGuard System Manager gives you an easy and efficient way to manage your network and keep it secure. With one computer as a management station, you can view, manage, and monitor each Firebox device in your network. The basic components of WatchGuard System Manager are the WatchGuard System Manager window, and the five WSM server components. WatchGuard System Manager also provides access to other WatchGuard tools, including Policy Manager and Firebox System Manager. The diagram below shows the components of WatchGuard System Manager and how you can access and navigate among them



WatchGuard System Manager tools

When you purchase a WatchGuard Firebox X Core or Peak, you get access to a full suite of management and monitoring tools.

WatchGuard System Manager

WatchGuard System Manager (WSM) is your primary application for connecting to and managing Firebox devices and WatchGuard Management Servers. WSM supports mixed environments. You can manage different Firebox devices that use different versions of software. For more information in WSM, see [Use the WatchGuard System Manager window](#).

You can also manage Firebox X Edge devices. (The Edge must be configured for [centralized management](#) if you want to use WSM to manage it and change its security policy.)

Policy Manager

Policy Manager is the user interface for firewall configuration tasks. Policy Manager includes a full set of preconfigured packet filters and proxies. You can also make a custom packet filter in which you set the ports, protocols, and other parameters. Other features of Policy Manager help you to stop attacks such as SYN Flood attacks, spoofing attacks, and port or address space probes. For more information, see [About Policy Manager](#).

Firebox System Manager

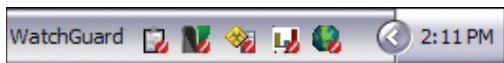
Firebox System Manager gives you one interface to monitor all components of your Firebox. From Firebox System Manager, you can see the real-time status of the Firebox and its configuration. For more information, see [About Firebox System Manager \(FSM\)](#).

About WatchGuard Servers

You use the WatchGuard toolbar to start, stop, and configure the five types of WatchGuard server software:

- Log Server
- Management Server
- Quarantine Server
- Report Server
- WebBlocker Server

The WatchGuard toolbar is one of the toolbars in the Windows System Tray at lower-right corner of your computer screen. (If you have not installed any WatchGuard server software on your management station, you do not see the WatchGuard toolbar.)



From left to right, you can use the icons on the toolbar to start, configure, and manage these servers.

Log Server

The Log Server collects log messages from each WatchGuard Firebox. The log messages are encrypted when they are sent to the Log Server. The log message format is XML (plain text). The information collected from firewall devices includes traffic log messages, event log messages, alarms, and diagnostic messages.

For more information on Log Servers, see [Set up the Log Server](#).

Management Server

The Management Server operates on a Windows computer. With this server, you can manage all firewall devices and create virtual private network (VPN) tunnels using a simple drag-and-drop function. The basic functions of the Management Server are:

- Certificate authority to distribute certificates for Internet Protocol Security (IPSec) tunnels
- Centralized management of VPN tunnel configurations
- Centralized management of multiple Firebox and Firebox X Edge devices

For more information on the Management Server, see [About the WatchGuard Management Server](#).

Quarantine Server

The Quarantine Server collects and isolates email messages that are suspected to be email spam by spamBlocker.

For more information on the Quarantine Server, see [About the Quarantine Server](#).

Report Server

The Report Server periodically consolidates data collected by your Log Servers from your Firebox devices, and then periodically generates reports. Once the data is on the Report Server, you can review it using the Report Manager. For more information about reports and the Report Server, see [About the Report Server](#). For more information about the Report Manager, see [About the Report Manager](#).

WebBlocker Server

The WebBlocker Server operates with the Firebox HTTP proxy to deny user access to specified categories of web sites. During Firebox configuration, the administrator sets the categories of web sites to allow or block. For more information on WebBlocker and the WebBlocker Server, see [About WebBlocker](#).

About Firewall

WatchGuard Firewall is the next generation of security appliance software available from WatchGuard. Appliance software is kept in the memory of your firewall hardware. The Firebox uses the appliance software with a configuration file to operate.

Your organization's security policy is a set of rules that define how you protect your computer network and the information that passes through it. Firewall appliance software has advanced features to manage security policies for the most complex networks.

Fireware and Fireware Pro

Two versions of Firewall are available to WatchGuard customers:

- **Fireware**—This is the default appliance software on Firebox X Core e-Series devices. This next generation appliance software enables WatchGuard to expand the number of features available to Firebox X customers
- **Fireware Pro**—This is the default appliance software on Firebox X Peak e-Series appliances. It enables customers with complex networks to more effectively protect their networks. Fireware Pro is available as an update for previously released Firebox X Core devices. The following features are available only with Fireware Pro:
 - High Availability
 - Traffic Management/Quality of Service (QoS)
 - VLANs
 - Dynamic routing
 - Policy-based routing
 - Server load balancing
 - The multi-WAN configuration options: Weighted Round-robin and Interface Overflow

About WatchGuard System Manager and WFS

WatchGuard System Manager also includes the system tools you must have to configure and manage a Firebox X device that uses WFS appliance software. WFS appliance software is the default appliance software that shipped with earlier models of the Firebox X Core and Peak. For more information about WFS appliance software, see the WFS User Guide.

After a Firebox is put in WSM management, the software automatically identifies which appliance software the Firebox uses. If you select the Firebox and then click an icon on the toolbar, it starts the correct management tool. These tools include:

- Firebox System Manager
- Policy Manager
- HostWatch

For example, if you add a Firebox X700 operating with WFS appliance software to the **Devices** tab of WFS and then click the Policy Manager icon on the WSM toolbar, Policy Manager for WFS automatically starts. If you add a Firebox X700 operating with Fireware appliance software and click the Policy Manager icon, Policy Manager for Fireware starts.

3

Getting Started

Before you begin

Before you begin the installation process, make sure you do the tasks described below.



In these installation instructions, we assume your Firebox has one trusted, one external, and one optional interface configured. To configure additional interfaces on your Firebox, use the configuration tools and procedures described in the [Network Setup and Configuration](#) topic

Verify basic components

Make sure that you have these items:

- WatchGuard Firebox security device
- A serial cable (blue)
- One crossover Ethernet cable (red)
- One straight Ethernet cable (green)
- Power cable

Get a Firebox feature key

When you get a new Firebox, you must activate it on the LiveSecurity web site and get a feature key. The feature key enables the features on your Firebox. If you register your Firebox before you use the Quick Setup Wizard, you can paste a copy of your feature key in the wizard. The wizard then applies it to your Firebox. If you do not paste your feature key into the wizard, you can finish the wizard. But until you add your feature key, only one connection is allowed to the Internet.

You get a new feature key for any optional products when you purchase them. After you register your Firebox or any new feature, you can synchronize your Firebox feature key with the feature keys kept on the LiveSecurity site in your registration profile at any time from the WSM user interface. For more information about feature keys, see [About feature keys](#) or [Import a feature key to the Firebox](#).

Gather network addresses

We recommend that you make two tables when you configure your Firebox. Use the first table for your network IP addresses before you put the Firebox into operation.

WatchGuard uses slash notation to show the subnet mask. For more information, see [About slash notation](#).

For more information on IP addresses, see [About IP addresses](#).

Table 1: Network IP addresses without the Firebox	
Wide Area Network	____.____.____.____ / ____
Default Gateway	____.____.____.____
Local Area Network	____.____.____.____ / ____
Secondary Network (if applicable)	____.____.____.____ / ____
Public Server(s) (if applicable)	____.____.____.____
	____.____.____.____
	____.____.____.____

Use the second table for your network IP addresses after you put the Firebox into operation.

External interface

Connects to the external network (typically the Internet) that is not trusted.

Trusted interface

Connects to the private LAN (local area network) or internal network that you want to protect.

Optional interface(s)

Usually connects to the DMZ or the mixed trust area of your network. Use optional interfaces to create zones in the network with different levels of access.

Table 1: Network IP addresses without the Firebox	
Default Gateway	____.____.____.____
External Interface	____.____.____.____ / ____
Trusted Interface	____.____.____.____ / ____
Optional Interface	____.____.____.____ / ____
Secondary Network (if applicable)	____.____.____.____ / ____

Select a firewall configuration mode

You must decide how to install the Firebox into your network before you install WatchGuard System Manager. The way you install the Firebox controls the interface configuration. To install the Firebox into your network, select the configuration mode—routed or drop-in—that matches the needs of your current network.

Many networks operate best with a routed configuration, but we recommend the drop-in mode if:

- You have already assigned a large number of static IP addresses and do not want to change your network configuration.
- You cannot configure the computers on your trusted and optional networks that have public IP addresses with private IP addresses.

This table and the descriptions below the table show three conditions that can help you to select a firewall configuration mode.

Routed Configuration	Drop-in Configuration
All interfaces of the Firebox are on different networks.	All interfaces of the Firebox are on the same network and have the same IP address.
Trusted and optional interfaces must be on different networks. Each interface has an IP address on its network.	The computers on the trusted or optional interfaces can have a public IP address.
Use static NAT (network address translation) to map public addresses to private addresses behind the trusted or optional interfaces.	Because the computers that have public access have public IP addresses, no NAT is necessary.

For more information on these two modes, see [Routed configuration](#) and [Drop-in configuration](#).

Decide where to install server software

During installation, you can install the management station and WatchGuard System Manager server components on the same computer. Or you can use the same installation procedure to install the Management Server, Log Server, Report Server, WebBlocker Server, or Quarantine Server components on other computers to distribute server load or supply redundancy. The Management Server does not operate correctly on a computer that does not also have WSM software installed. To decide where to install server software, you must examine the capacity of your management station and select the installation method that matches your needs.

If you install server software on a computer with an active desktop firewall other than Windows Firewall, you must open the ports necessary for the servers to connect through the firewall. Windows Firewall users do not have to change their desktop firewall configuration because the installation program opens the necessary ports through Windows Firewall automatically. See [Install WatchGuard Servers on computers with desktop firewalls](#) for more information.

You can now start the installation process. The first step is to [Set up the management station](#).

Set up the management station

You install WatchGuard System Manager (WSM) software on a computer that you designate as the *management station*. You can use tools on the management station to get access to information on the Firebox, such as connection and tunnel status, statistics on traffic, and log messages.

Select one Windows-based computer on your network as the management station and install the management software. To install the WatchGuard System Manager software, you must have administrative privileges on the management station computer. After installation, you can operate with Windows XP or Windows 2003 Power User privileges.

You can install more than one version of WatchGuard System Manager on the same management station. You can install only one version of server software on a computer at a time.

Back up your previous configuration

If you have a previous version of WatchGuard System Manager, make a backup of your security policy configuration before you install a new version. To make a backup of your configuration, see [Make a backup of the Firebox image](#).

Download WatchGuard System Manager software

You can download the most current WatchGuard System Manager software at any time from <http://www.watchguard.com/archive/softwarecenter.asp>. You must log in with your LiveSecurity user name and password. If you are a new user, create a user profile and activate your product at <http://www.watchguard.com/activate> before you try to download the WSM software. For more information, see [Activate LiveSecurity Service](#).



If you install one of the WSM servers on a computer with a personal firewall other than the Microsoft Windows firewall, you must open the ports for the servers to connect through the firewall. To allow connections to the WebBlocker Server, open UDP port 5003. It is not necessary to change your configuration if you use the Microsoft Windows firewall. See the [Install WatchGuard Servers on computers with desktop firewalls](#) topic for more information.

1. On the computer you will use as the management station, download the latest WatchGuard System Manager (WSM) software.
For information on encryption levels, see [About software encryption levels](#).
2. On the same computer, download the latest Fireware appliance software. Make sure that you write down the name and the path of the files when you save them to your hard drive.
3. Open the file and use the installation instructions. The Setup program includes a screen in which you select the components of the software or the upgrades to install. A different license is necessary when you install some software components.



If your management station is currently operating with a Windows toolbar, you might need to restart the toolbar to see the new components installed for WatchGuard Management System.

Now you are ready to run the Quick Setup Wizard. This wizard runs either from the web or as a Windows application.

- For information on how to run the wizard from the web, see [Web Quick Setup Wizard](#).
- For information on how to run the wizard as a Windows application, see [Quick Setup Wizard \(non-web\)](#).

About software encryption levels

The management station software is available in two encryption levels.

Base

Supports 40-bit encryption for Mobile VPN with PPTP tunnels. You cannot create an IPSec VPN tunnel with this level of encryption.

Strong

Supports 40-bit and 128-bit encryption for Mobile VPN with PPTP. Also supports 56-bit and 168-bit DES, and 128-bit, 192-bit, and 256-bit AES.

To use virtual private networking with IPSec, you must download the strong encryption software.

Strong export limits apply to the strong encryption software. It is possible that it is not available for download in your location.

About the Quick Setup Wizard

You can use the Quick Setup Wizard to create a basic configuration for your Firebox X. The Firebox uses this basic configuration file when it starts for the first time. This enables the Firebox to operate as a basic firewall. You can use this same procedure any time you want to reset the Firebox to a new basic configuration for recovery or other reasons.

When you configure the Firebox with the Quick Setup Wizard, you set only the basic policies (TCP and UDP outgoing, FTP packet filter, ping, and WatchGuard) and interface IP addresses. If you have more software applications and network traffic for the Firebox to examine, you must:

- Configure the policies on the Firebox 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

The Quick Setup Wizard runs either from the web or as a Windows application.

- For information on how to run the wizard from the web, see [Web Quick Setup Wizard](#).
- For information on how to run the wizard as a Windows application, see [Quick Setup Wizard \(non-web\)](#).

Web Quick Setup Wizard

You can use the Web Quick Setup Wizard with any model of Firebox X Core or Peak.

If you have configured a Firebox X Core or X Peak before, you must understand that the Web Quick Setup Wizard operates differently than the Quick Setup Wizard that shipped with earlier Firebox X hardware models. With earlier Firebox X Core and Peak devices, the Quick Setup Wizard used device discovery to find a Firebox on the network to configure. With the Web Quick Setup Wizard, you must make a direct network connection to the Firebox and use a web browser to start the wizard. The Firebox uses DHCP from its interface 1 to give a new IP address to your management station to use during configuration.

Before you start the Web Quick Setup Wizard, make sure you have:

- Registered your Firebox with LiveSecurity Service
- Stored a copy of your Firebox feature key in a text file on your management station
- Downloaded WSM and Fireware software from the LiveSecurity Service web site to your management station
- Installed the Fireware executable on your management station

The HTTP connection made to the Firebox when you use the Web Quick Setup Wizard is not encrypted. We recommend that you connect your management station directly to the Firebox when you use the Web Quick Setup Wizard, because passphrases are sent in plain-text format.

To run the Web Quick Setup Wizard:

1. Connect the red crossover Ethernet cable that ships with your Firebox between the Ethernet port on your management station and the interface 1 on your Firebox.
2. Plug the power cord into the Firebox power input and into a power source.
3. On the front of the Firebox X, press the down arrow button while you turn on the power to the Firebox. The Firebox X boots into safe mode. While in this factory-default mode, the LCD shows the model number followed by the word `safe` in lower-case characters.
4. Make sure your management station is configured to accept DHCP-assigned IP addresses. For example, if your management station uses Windows XP: From your Windows Start menu, select **All Programs > Control Panel > Network Connections > Local Area Connections**. Click **Properties**. Select **Internet Protocol (TCP/IP)** and click **Properties**. Make sure **Obtain an IP Address Automatically** is selected.
5. Open a web browser and type: `http://10.0.1.1:8080/`
Make sure you type the preceding `http://` if you use Internet Explorer. This opens an HTTP connection between your management station and the Firebox X device.
The Web Quick Setup Wizard starts automatically. Click through the screens and give the information it asks for. If you leave the Web Quick Setup Wizard idle for 15 minutes or more, you must go back to step 3 and start again.

If you have problems with the wizard

If the Web Quick Setup Wizard is unable to install Fireware appliance software on the Firebox, the wizard times out after six minutes. If you have problems with the wizard, check these things:

- It is possible that the Fireware application software file you downloaded from the LiveSecurity web site is corrupted. If the software image is corrupted, you can sometimes see a message on the LCD interface: File Truncate Error. Download the software again and try the wizard once more.
- If you use Internet Explorer 6, clear the file cache in your web browser and try again. To clear the cache, from the Internet Explorer toolbar select **Tools > Internet Options > Delete Files**.

After the wizard finishes

After you run the Quick Setup Wizard, you might need to wait a minute or so before your Firebox is ready. This is particularly true with the Firebox X Peak models 5500e, 6500e, 8500e, and 8500e-F.

After you finish with all screens in the wizard, the Firebox is configured with a basic configuration that includes four policies (TCP outgoing, FTP packet filter, ping, and WatchGuard) and the interface IP addresses you specified. You can use Policy Manager to expand or change the Firebox configuration.

- For information on how to put the Firebox into operation after the Quick Setup Wizard is finished, see [After your installation](#).
- To start WatchGuard System Manager and begin to use its tools, see [Start WatchGuard System Manager](#).

Quick Setup Wizard (non-web)

The Quick Setup Wizard runs as a Windows application to help you make a basic configuration file. You can use the Quick Setup Wizard with any model of Firebox X Core or Peak. The Firebox uses this basic configuration file when it starts for the first time. This enables the Firebox to operate as a basic firewall.

After the Firebox is configured with this basic configuration, you can use Policy Manager to expand or change the Firebox configuration.

The Quick Setup Wizard uses a device discovery procedure to find the Firebox X model you are configuring. This procedure uses a UDP multicast. Software firewalls, including the firewall in Microsoft Windows XP SP2, can cause problems with device discovery.

You can start the Quick Setup Wizard from the Windows desktop or from WatchGuard System Manager. From the desktop, select:

Start > All Programs > WatchGuard System Manager 10.0 > Quick Setup Wizard

Or, from WatchGuard System Manager, select:

Tools > Quick Setup Wizard

The Quick Setup Wizard starts. Click through the screens and give the information it asks for.

About setting the log encryption key

In the Quick Setup Wizard, you must set a status and configuration passphrase for the Firebox. When you are ready to configure a Log Server to collect log messages from the Firebox, use the status passphrase you set in the Quick Setup Wizard as your default log encryption key. After your Log Server is configured, you can [Change the Log Server encryption key](#).

After the wizard finishes

After you run the Quick Setup Wizard, you might need to wait a minute or so before your Firebox is ready. This is particularly true with the Firebox X Peak models 5500e, 6500e, 8500e, and 8500e-F.

After you finish with all screens in the wizard, the Firebox is configured with a basic configuration that includes four policies (TCP and UDP outgoing, FTP packet filter, ping, and WatchGuard) and the interface IP addresses you specified. You can use Policy Manager to expand or change the Firebox configuration.

- For information on how to put the Firebox into operation after the Quick Setup Wizard is finished, see [After your installation](#).
- To start WatchGuard System Manager and begin to use its tools, see [Start WatchGuard System Manager](#).

After your installation

After you are finished with either the web or the non-web Quick Setup Wizard, you must do the following to put the Firebox into operation on your network:

1. Put the Firebox in its permanent physical location.
2. Make sure the management station and the rest of the trusted network use the IP address of the Firebox's trusted interface as their gateway.
3. In WatchGuard System Manager, select **File > Connect To Device** to connect the management station to the Firebox.
4. If you use a routed configuration, change the default gateway on all computers that you connect to the Firebox trusted IP address.



If you install WatchGuard server software (Management Server, Quarantine Server, and so on) on a computer with an active desktop firewall other than Windows Firewall, you must open the ports necessary for the servers to connect through the firewall. Windows Firewall users do not have to change their configuration. See the section [Install WatchGuard Servers on computers with desktop firewalls](#) for more information.

Other setup tasks you might want to do are:

- [Set up the Management Server.](#)
- [Set up the Log Server](#) and [set up the Report Server](#) to start recording log messages and making reports from them.
- [Start WebBlocker on your Firebox.](#)
- [Start the Quarantine Server.](#)
- As described in "Customize your security policy," below, customize the configuration for your company's own business and security needs.

Customize your security policy

Your security policy controls who can get into your network, where they can go, and who can get out. The configuration file of your Firebox makes the security policy.

The configuration file that you make with the Quick Setup Wizard is only a basic configuration. You can modify this configuration to align your security policy with your company's own business and security requirements. To do this, add packet filter and proxy policies to set what you let in and out of your network. Each policy can have an effect on your network. The policies that increase your network security can decrease access to your network. And the policies that increase access to your network can put the security of your network at risk. For more information on policies, see [About policies](#).

For a new installation, we recommend that you use only packet filter policies until all your systems operate correctly. As necessary, you can add proxy policies.

About LiveSecurity Service

Your Firebox includes a subscription to LiveSecurity Service. Your subscription:

- Makes sure that you get the newest network protection with the newest software upgrades
- Gives solutions to your problems with full technical support resources
- Prevents service interruptions with messages and configuration help for the newest security problems
- Helps you to find out more about network security through training resources
- Extends your network security with software and other features
- Extends your hardware warranty with advanced replacement

For more information about LiveSecurity Service, see [About Watchguard Support](#).

Start WatchGuard System Manager


From the Windows Desktop, select:

Start > All Programs > WatchGuard System Manager 10.0 > WatchGuard System Manager

For basic information on WatchGuard System Manager, see [Introduction to WatchGuard System Manager](#).

For information on how to use WSM, see [Use the WatchGuard System Manager window](#). You can get access to all WatchGuard System Manager functionality through this main window. It is useful to note you can use standard copy/paste procedures in most data fields throughout WatchGuard System Manager.

Connect to a Firebox

1. If you have not already done so, [start WatchGuard System Manager](#).
2. Click .
Or, select **File > Connect to Device**.
Or, right-click anywhere in the WSM window (**Device Status** tab) and select **Connect to Device**.
The Connect to Firebox dialog box appears.




The dialog box is titled "Connect to Firebox" and features the WatchGuard logo. It contains the following fields and controls:

- Name / IP Address:** A text field with a dropdown arrow, containing the value "192.168.54.50".
- Passphrase:** A text field for entering the status passphrase.
- Timeout:** A spinner control set to "25" with the unit "seconds".
- Buttons:** "Login", "Cancel", and "Help" buttons at the bottom.

3. In the **Firebox** drop-down list, type the name or IP address of your Firebox. On subsequent connections, you can select the Firebox name or IP address from the **Firebox** drop-down list. You can also type the IP address or host name. When you type an IP address, type all the numbers and the periods. Do not use the TAB or arrow key.
4. Type the Firebox status (read-only) passphrase.
You use the status passphrase to monitor traffic and Firebox conditions. You must type the configuration passphrase when you save a new configuration to the Firebox.
5. If necessary, change the value in the **Timeout** field. This value sets the time (in seconds) that the management station listens for data from the Firebox before it sends a message that shows that it cannot get data from the device.
If you have a slow network or Internet connection to the device, you can increase the timeout value. Decreasing the value decreases the time you must wait for a timeout message if you try to connect to a Firebox that is not available.
6. Click **Login**.
The Firebox appears in the WatchGuard System Manager window.

Disconnect from a Firebox

Click . (If you are connected to more than one Firebox, select the one you want to disconnect from before you click the icon.)

Or, select **File > Disconnect**.

Or, right-click anywhere in the WSM window (**Device Status** tab) and select **Disconnect**.

Disconnect from all Fireboxes

If you are connected to more than one Firebox, you can disconnect from them all at the same time.

Select **File > Disconnect All**.

Or, right-click anywhere in the WSM window (**Device Status** tab) and select **Disconnect All**.

Start security applications

You can start these tools from WatchGuard System Manager using the icons on the taskbar and menu options.

Policy Manager

Policy Manager lets you install, configure, and customize a network security policy for a Firebox

For more information on Policy Manager, see [About Policy Manager](#).

To start Policy Manager, click .

Or, select **Tools > Policy Manager**.

Firebox System Manager

WatchGuard Firebox System Manager lets you start many different security tools in one easy-to-use interface. You can also use Firebox System Manager to monitor real-time traffic through the firewall.

For more information on Firebox System Manager, see the [About Firebox System Manager \(FSM\)](#).

To start Firebox System Manager, click .

Or, select **Tools > Firebox System Manager**.

HostWatch

HostWatch shows the connections through a Firebox from the trusted network to the external network, or from and to other interfaces or VLANs you choose. It shows the current connections, or it can show historical connections from a log file.

For more information on HostWatch, see [About HostWatch](#).

To start HostWatch, click .

Or, select **Tools > HostWatch**.

LogViewer

LogViewer shows a static view of a log file. It lets you:

- Apply a filter by data type
- Search for words and fields
- Print and save to a file

For more information on using LogViewer, see [Use LogViewer to see log files](#).

To start LogViewer, click .

Or, select **Tools > Logs > LogViewer**.

WatchGuard Reports

WatchGuard Reports are summaries of the data that you have selected to collect from the Firebox log files.

For more information on using WatchGuard Reports, see [About the Report Manager](#).

To start the Report Manager, click .

Or, select **Tools > Logs > WG Reports**.

Quick Setup Wizard

You can use the Quick Setup Wizard to create a basic configuration for your Firebox. The Firebox uses this basic configuration file when it starts for the first time. This enables the Firebox to operate as a basic firewall. You can use this same procedure any time you want to reset the Firebox to a new basic configuration for recovery or other reasons.

For more information on using the Quick Setup Wizard, see [About the Quick Setup Wizard](#).


To start the Quick Setup Wizard, click .

Or, select **Tools > Quick Setup Wizard**.

CA Manager

In WatchGuard System Manager, the workstation that is configured as the Management Server also operates as a certificate authority (CA). The CA gives certificates to managed Firebox clients when they contact the Management Server to receive configuration updates.

Before you can use the Management Server as a CA, you must [Configure the certificate authority on the Management Server](#).

To set up or change the parameters of the certificate authority, click .

Or, select **Tools > CA Manager**.

Upgrade to a new version of Fireware

Occasionally, we make new versions of WatchGuard System Manager (WSM) and Fireware appliance software available to Firebox users with active LiveSecurity subscriptions. To upgrade from one version of WSM with Fireware to a new version of WSM with Fireware:

1. Back up your current Firebox configuration file and Management Server configuration files.
For more information on how to create a backup image of your Firebox configuration, see [Make a backup of the Firebox image](#). To back up the settings on your Management Server, see [Back up or restore the Management Server configuration](#).
2. Use Windows Add or Remove Programs to uninstall your existing WatchGuard System Manager and WatchGuard Fireware installation. You can have more than one version of WatchGuard System Manager client software installed on your management station, but only one version of WatchGuard server software.
3. Launch the file or files that you downloaded from the LiveSecurity web site and use the on-screen procedure.
4. To save the upgrade to the appliance, use Policy Manager to open your Firebox X Core or Firebox X Peak configuration file. Use the on-screen instructions to convert the configuration file to the newer version and save it to the Firebox.
If you do not see on-screen instructions or have problems with this procedure, open Policy Manager and select **File > Upgrade**. Browse to your installation directory or C:\Program Files\Common Files\WatchGuard\resources\Fireware\9.1 and select the WGU file. Click **OK**.

The upgrade procedure can take up to 15 minutes and automatically reboots the Firebox.

If your Firebox has been operating for some time before you upgrade, you might have to restart the Firebox before you start the upgrade to clear the temporary memory on the Firebox. If, during the upgrade, you see an error message about \var\tmp2\cmm_upgrade_sys.tar, reboot your Firebox and start the upgrade again.

Downgrade to WSM 9.1.x or earlier

If you have problems when you upgrade your management station to v10, you can downgrade your Firebox to an earlier version of Fireware. You can downgrade a Firebox in two ways:

- If you have a backup file created with an earlier version of Fireware, you can restore it to the Firebox. The backup file must have an .fxi file extension. The default location for backup files is C:\Documents and Settings\All Users\Shared WatchGuard\backups.
- If you do not have a backup file, you can use an older version of WSM to save the matching version of Fireware to the Firebox, run the Quick Setup Wizard, and then save your configuration to the Firebox.

If you have a backup file

[Start WatchGuard System Manager](#). The version must match the version used to save the backup file.

1. [Connect to the Firebox](#).
2. [Open Policy Manager](#).
3. Select **File > Restore**.
4. Navigate to the .fxi file and restore the Firebox.
5. When the restore is complete, the Firebox reboots. It will run the version of Fireware it had at the time the backup file was saved.

If you do not have a backup file

1. On your management station, install the version of Fireware that matches your version of WSM (for example v9.1).
2. Open Policy Manager v9.1 and select **File > Upgrade** to install Fireware v9.1.
3. Run the v9.1 Quick Setup Wizard and use it to save a basic configuration to the Firebox.
4. Open your policy in Policy Manager v9.1 and save it to the Firebox.

Additional installation topics

Install WSM and keep an older version

You can install the current version of WSM and keep the old version if you remove the server software (Management Server, Log Server, Report Server, Quarantine Server, and WebBlocker Server) from the older version of WSM. Because you can have only one version of the servers installed, you must remove the previous version before you install the current WSM version together with the current server software.

Install WatchGuard Servers on computers with desktop firewalls

Desktop firewalls can block the ports necessary for WatchGuard server components to operate. Before you install the Management Server, Log Server, Quarantine Server, Report Server, or WebBlocker Server on a computer with an active desktop firewall, you might need to open the necessary ports on the desktop firewall. Windows Firewall users do not need to change their configuration because the installation program opens the necessary ports in Windows Firewall automatically.

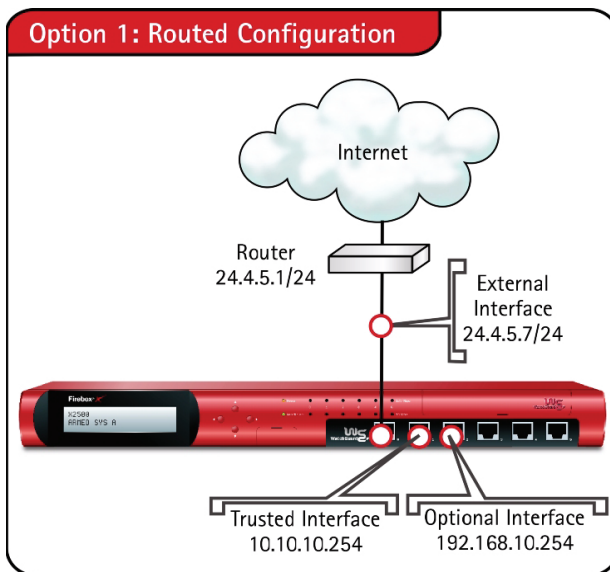
This table shows you the ports you must open on a desktop firewall.

Server Type/Appliance Software	Protocol/Port
Management Server	TCP 4109, TCP 4110, TCP 4112, TCP 4113
Log Server with Fireware appliance software	TCP 4115
Log Server with WFS appliance software	TCP 4107
WebBlocker Server	TCP 5003, UDP 5003
Quarantine Server	TCP 4119, TCP 4120
Report Server	TCP 4122
Log Server	TCP 4121

Routed configuration

Use the routed configuration when you have a small number of public IP addresses or when your Firebox gets its external IP address with PPPoE (point-to-point protocol over Ethernet) or DHCP (dynamic host configuration protocol).

In a routed configuration, you install the Firebox with different subnets on each of its interfaces. The public servers behind the Firebox can use private IP addresses. The Firebox uses [Network Address Translation \(NAT\)](#) to route traffic from the external network to the public servers.



The requirements for a routed configuration are:

- All interfaces of the Firebox must be configured on different subnets. The minimum configuration includes the external and trusted interfaces. You also can configure one or more optional interfaces.
- All computers connected to the trusted and optional interfaces must have an IP address from that network. For example, a computer on a trusted interface in the previous figure could have an IP address of 10.10.10.200 but not 192.168.10.200, which is on the optional interface.

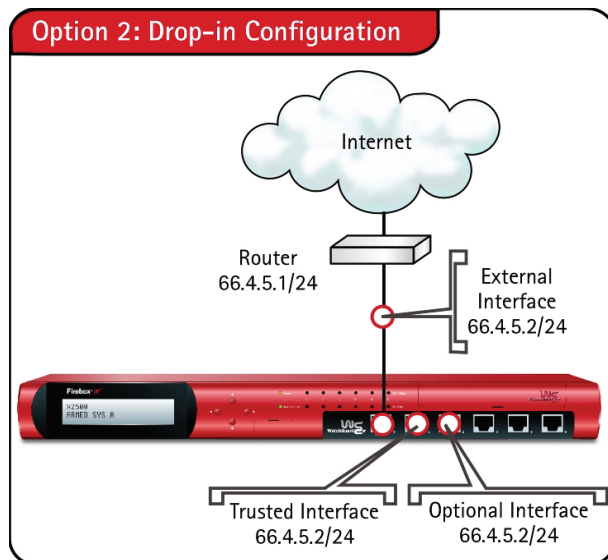
Drop-in configuration

In a drop-in configuration, the Firebox is configured with the same IP address on all interfaces. The drop-in configuration mode distributes the network's logical address range across the Firebox interfaces. You can put the Firebox between the router and the LAN and not have to change the configuration of any local computers. This configuration is known as drop-in because the Firebox is dropped in to a network.

In drop-in mode:

- The same primary IP address is automatically assigned to all interfaces on your Firebox (external, trusted, and optional).
- You can assign secondary networks on any interface.
- You can keep the same IP addresses and default gateways for hosts on your trusted and optional networks, and add a secondary network address to the Firebox interface so the Firebox can correctly send traffic to the hosts on these networks.

The public servers behind the Firebox can continue to use public IP addresses. The Firebox does not use network address translation to route traffic from outside your network to your public servers.



The properties of a drop-in configuration are:

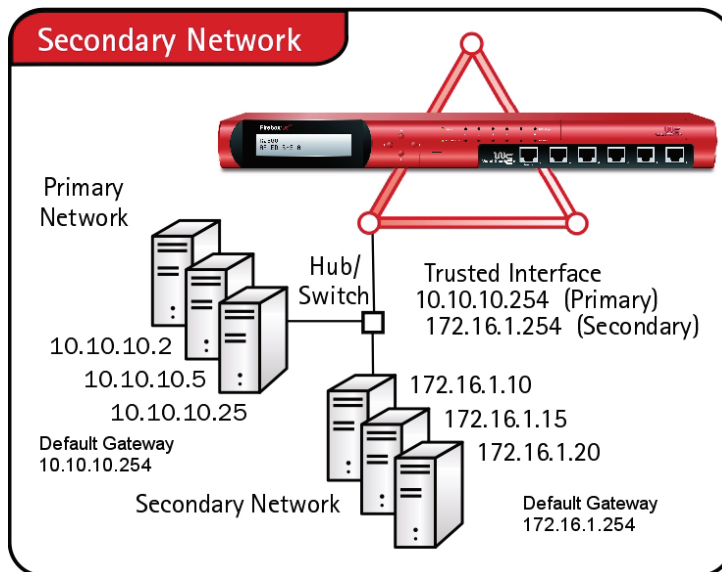
- You must have a static external IP address to assign to the Firebox.
- You use one logical network for all interfaces.

Drop-in mode does not support multi-WAN in Round-robin or Failover mode. For more information on these options, see [About using multiple external interfaces](#).

It is sometimes necessary to [clear the ARP cache](#) of each computer on the trusted network.

Add secondary networks to your configuration

A secondary network is a different network that connects to a Firebox interface with a switch or hub.



When you add a secondary network, you map a second IP address to the Firebox interface. You make (or add) an IP alias to the network interface. This secondary network address you set is the default gateway for all the computers on the secondary network. The secondary network also tells the Firebox that one more network is on the Firebox interface.

To add a secondary network, do one of these procedures:

Use the Quick Setup Wizard during installation

If you configure the Firebox in drop-in mode, you can enter an IP address for the secondary network in the Quick Setup Wizard. This is the default gateway for your secondary private network.

Add the secondary network after the Firebox installation is complete

If you configure the Firebox in routed mode, or at any time after you use a Quick Setup Wizard, you can use Policy Manager to add secondary networks to an interface. For information on how to do this, see [Configure a secondary network](#).

Dynamic IP support on the external interface

If you use dynamic IP addresses, you must configure your Firebox in routed mode when you use the Quick Setup Wizard.

If you select DHCP, the Firebox tells a DHCP server controlled by your Internet service provider (ISP) to give the Firebox its IP address, gateway, and netmask. This server can also give DNS server information for your Firebox. If it does not give you that information, you must add it manually to your configuration. If necessary, you can change the IP addresses that your ISP gives you.

You also can use PPPoE. As with DHCP, the Firebox makes a PPPoE protocol connection to the PPPoE server of your ISP. This connection automatically configures your IP address, gateway, and netmask.

If you use PPPoE on the external interface, you must have the PPP user name and password when you configure your network. If your ISP gives you a domain name to use, type your user name in the format `user@domain` when you use the Quick Setup Wizard.

A static IP address is necessary for the Firebox to use some functions. When you configure the Firebox to receive dynamic IP addresses, the Firebox cannot use these functions:

- High Availability (not available on Firebox 500)
- Drop-in mode
- 1-to-1 NAT on an external interface
- Mobile VPN with PPTP



If your ISP uses a PPPoE connection to give a static IP address, the Firebox allows you to enable Mobile VPN with PPTP because the IP address is static.

About connecting the Firebox cables

Connect the power cable to the Firebox power input and to a power source.

We recommend that you use a straight Ethernet cable (green) to connect your management station to a hub or switch. Use a different straight Ethernet cable to connect your Firebox to the same hub or switch.

You also can use a red crossover cable to connect the Firebox trusted interface to the management station Ethernet port.

4

Service and Support

About Watchguard Support

No Internet security solution is complete without regular updates and security information. New threats appear each day — from the newest hacker to the newest bug in an operating system — and each can cause damage to your network systems. LiveSecurity Service sends security solutions directly to you to keep your security system in the best condition. Training and technical support are available on the WatchGuard site to help you learn more about network security and your WatchGuard products.

About LiveSecurity Solutions

The number of new security problems and the volume of information about network security continues to increase. We know that a firewall is only the first component in a full security solution. The WatchGuard Rapid Response Team is a dedicated group of network security personnel who can help you to control the problem of too much security information. They monitor the Internet security web sites to identify new security problems.

Threat responses, alerts, and expert advice

After a new threat is identified, the WatchGuard Rapid Response Team sends you an email message to tell you about the problem. Each message gives full information about the type of security problem and the procedure you must use to make sure that your network is safe from attack.

LiveSecurity Service saves you time because you receive an email message when we release a new version of the WatchGuard System Manager software. Installation wizards, release notes, and a link to the software update make for a fast and easy installation. These continued updates make sure that you do not have to use your time to find new software.

Access to technical support and training

You can find information about your WatchGuard products quickly with our many online resources. You can also speak directly to one of the WatchGuard technical support personnel. Use our course materials available on the WatchGuard web site to learn more about the WatchGuard System Manager software, Firebox, and network security, or to find a WatchGuard Certified Training Partner in your area.

LiveSecurity Broadcasts

The WatchGuard Rapid Response Team regularly sends messages and software information directly to your computer desktop by email. We divide the messages into categories to help you to identify and make use of incoming information immediately.

Information Alert

Information Alerts give you a fast view of the newest information and threats to Internet security. The WatchGuard Rapid Response Team frequently recommends that you make a security policy change to protect against the new threat. When necessary, the Information Alert includes instructions on the procedure.

Threat Response

If a new security threat makes it necessary, the WatchGuard Rapid Response Team transmits a software update for your Firebox®. The Threat Response includes information about the security threat and instructions on how to download a software update and install it on your Firebox and management station.

Software Update

When necessary, WatchGuard updates the WatchGuard System Manager software. Product upgrades can include new features and patches. When we release a software update, you get an email message with instructions on how to download and install your upgrade.

Editorial

Top network security personnel come together with the WatchGuard Rapid Response Team to write about network security. This continuous supply of information can help your network stay safe and secure.

Foundations

The WatchGuard Rapid Response Team also writes information specially for security administrators, employees, and other personnel that are new to this technology.

Loopback

At the end of each month LiveSecurity® Service sends you an email message with a summary of the information sent that month.

Support Flash

These short training messages can help you to operate WatchGuard System Manager. They are an added resource to the other online resources: - User forum - FAQs - Known Issues pages on the Technical Support web site

Virus Alert

WatchGuard has come together with an antivirus vendor to give you the most current information about computer viruses. We send you messages with a summary of the virus traffic on the Internet. When a hacker releases a dangerous virus on the Internet, we send a special virus alert to help you protect your network.

New from WatchGuard

When WatchGuard releases a new product, we first tell you — our customers. You can learn about new features and services, product upgrades, hardware releases, and promotions.

LiveSecurity Service Self Help Tools

Online Self Help Tools enable you to get the best performance from your WatchGuard products.



You must activate LiveSecurity Service before you can get access to online resources.

Instant Answers

Instant Answers is a guided Help tool designed to give solutions to product questions very quickly. Instant Answers asks you questions and then gives you the best solution based on the answers you give.

Product FAQs

FAQs (frequently asked questions) give you general information about the Firebox®, WatchGuard System Manager, and the Firebox appliance software. FAQs supply important information about configuration options and operation of systems or products.

Known Issues

This Known Issues tool monitors WatchGuard product problems and software updates.

WatchGuard Users Forum

The WatchGuard Technical Support team operates a web site where customers can help each other with WatchGuard products. Technical Support monitors this forum to make sure you get accurate information.

Training

Browse to the training section to learn more about network security and WatchGuard products. You can use training materials available online and get a certification in WatchGuard products. The training includes links to a wide range of documents and web sites about network security. The training is divided into parts, which lets you use only the materials you feel necessary. To learn more about training, browse to <http://www.watchguard.com/training/>.

Product Documentation

The WatchGuard web site has a copy of each product user guide, including user guides for software versions that are no longer supported. The user guides are in .pdf format.

To get access to the LiveSecurity Service Self Help Tools:

1. Start your web browser. In the address bar, type: <http://www.watchguard.com/support>
2. Under **Self Help Tools**, click the tool you want to use.

You are asked to log in to LiveSecurity Service if you have not already done so.

Activate LiveSecurity Service

You activate LiveSecurity Service and register your Firebox service with the activation section of the LiveSecurity Service web pages. You can also find information about feature activation and the Quick Setup Wizard in the *Quick Start Guide* and [About the Quick Setup Wizard](#). You usually activate the Live Security Service when you install your Firebox.



To activate LiveSecurity Service, you must enable JavaScript on your browser.

1. Make sure that you have your Firebox serial number. This is necessary during the LiveSecurity activation procedure. You can find the Firebox serial number on a label on the rear side of the Firebox below the Universal Product Code (UPC), or on a label on the bottom of the Firebox.
2. Use your web browser to go to www.watchguard.com/account/register.asp.
The Account page appears.
3. Complete the LiveSecurity Activation page. Use the TAB key or the mouse to move through the fields on the page.
You must complete all the fields to activate correctly. This information helps WatchGuard to send you the information and software updates that are applicable to your products.
4. Make sure that your email address is correct. Your LiveSecurity emails about product updates and threat responses come to this address. After you complete the procedure, you get an email message that tells you that you activated LiveSecurity Service correctly.
5. Click **Register**.

WatchGuard Users Forum

The WatchGuard Users Forum is an online group. It lets users of WatchGuard products exchange product information about:

- Configuration
- Connecting WatchGuard products and those of other companies
- Network policies

This forum has different categories that you can use to look for information. The Technical Support team controls the forum during regular work hours. You do not get special help from Technical Support when you use the forum. To contact Technical Support directly from the web, log in to your LiveSecurity account. Click on the **Incidents** link to send a Technical Support incident.

Using the WatchGuard Users Forum

To use the WatchGuard Users Forum you must first create an account. For instructions, browse to: <http://www.watchguard.com/forum>

Product documentation

We post all user guides to the web site at <http://www.watchguard.com/help/documentation>.

Training and certification

WatchGuard product training is available through WatchGuard Certified Training Partners (WCTPs). You can install and configure the products with a qualified, experienced instructor to help you learn, and then take a WatchGuard technical certification exam. To find a training partner near you, go to http://www.watchguard.com/training/partners_locate.asp

WatchGuard product training is also available online to help you learn more about network security and WatchGuard products. If you study the WSM/Fireware course materials, you can use these training materials to prepare for the certification exam. To find training materials, go to <http://www.watchguard.com/training/courses.asp>

You must log into LiveSecurity to be able to download any of these courses.

About WatchGuard technical support

Your LiveSecurity Service subscription includes technical support for the WatchGuard System Manager software and Firebox hardware. To learn more about WatchGuard Technical Support, browse to the WatchGuard web site at <http://www.watchguard.com/support>.



You must activate LiveSecurity Service before you can get technical support. For more information, see [Activate LiveSecurity Service](#).

LiveSecurity Service technical support

All new Firebox products include the WatchGuard LiveSecurity Technical Support Service. You can speak with a member of the WatchGuard Technical Support team when you have a problem with the installation, management, or configuration of your Firebox.

Hours

WatchGuard LiveSecurity Technical Support operates from 6:00 AM to 6:00 PM in your local time zone, Monday through Friday.

Telephone number

877.232.3531 (select option #2) in United States and Canada

+1.206.613.0456 in all other countries

Web site

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

Service time

We try for a maximum response time of four hours.

Single Incident Priority Response Upgrade (SIPRU) and Single Incident After Hours Upgrade (SIAU) are also available. For more information about these upgrades, go to the WatchGuard web site at <http://www.watchguard.com/support>.

LiveSecurity Gold

WatchGuard Gold LiveSecurity Technical Support adds to your standard LiveSecurity Service. We recommend that you get this upgrade if you use the Internet or VPN tunnels for most of your work.

With WatchGuard Gold LiveSecurity Technical Support you get:

- Technical support 24 hours a day, seven days a week, including holidays.
- The Technical Support Team operates the support center from 7 PM Sunday to 7 PM Friday (Pacific Time). For weekend support for critical problems, use the on-call paging system.
- We try for a maximum response time of one hour.

To create a support incident, call WatchGuard LiveSecurity Technical Support. A Customer Care representative records the problem and gives you an incident number. A Priority Support technician calls you as quickly as possible. If you have a critical problem when the support center is not open, use the LiveSecurity Technical Support phone number to page a technician. You can also send an incident on the web site at

<http://www.watchguard.com/support/incidents/newincident.asp>.

Firebox installation service

WatchGuard Remote Firebox Installation Service helps you to install and configure your Firebox. You can schedule two hours with a WatchGuard Technical Support team member. The technician helps you to:

- Do an analysis of your network and security policy
- Install the WatchGuard System Manager software and Firebox hardware
- Align your configuration with your company security policy

This service does not include VPN installation.

VPN installation service

WatchGuard Remote VPN Installation Service helps you through a full VPN installation. You can schedule a two-hour time with one of the WatchGuard Technical Support team. During this time, the technician helps:

- Do an analysis of your VPN policy
- Configure your VPN tunnels
- Do a test of your VPN configuration

You can use this service after you correctly install and configure your Firebox devices.

5

Firebox Status Monitoring

About Firebox System Manager (FSM)

WatchGuard Firebox System Manager (FSM) gives you one interface to monitor all components of a Firebox and the work it does. You can see:

- [Basic Firebox and network status](#) (Front Panel tab)
- [Firebox log messages](#) (Traffic Monitor tab)
- [Visual display of bandwidth usage](#) (Bandwidth Meter tab)
- [Visual display of policy usage](#) (Service Watch tab)
- [Traffic and performance statistics](#) (Status Report tab)
- [Authenticated users](#) (Authentication List tab)
- [Blocked Sites list](#) (Blocked Sites tab)
- [Security subscriptions](#) (Security Services tab)

You can also launch these applications from Firebox System Manager:

- [HostWatch](#) is a graphical user interface that shows the connections between different Firebox interfaces.
- [Performance Console](#) is a Firebox utility that you use to make graphs that show how different parts of the Firebox are operating.
- [Communication log](#) keeps messages about connections between the Firebox and Firebox System Manager.

You can use Firebox System Manager to perform these operations:

- [Manage certificates](#)
- [See and synchronize feature keys](#)
- [Synchronize time](#)
- [Clear the ARP cache](#)
- [Clear alarms](#)
- [Rekey BOVPN tunnels](#)
- [Control High Availability](#)
- [Change passphrases](#)

Firebox System Manager menus, icons, and buttons









Firebox System Manager (FSM) commands are in the menus at the top of the main window. The most common tasks are also available as icons on the toolbar or as buttons.

- [Firebox System Manager menus](#)
- [Firebox System Manager icons](#)
- [Firebox System Manager buttons](#)

Firebox System Manager menus

Menu	Command	Function
File	Settings	Changes how Firebox System Manager shows status information in the displays.
	Disconnect	Keeps Firebox System Manager open, but stops the connection to the monitored Firebox.
	Reset	Stops the operating system components on the Firebox and restarts them (soft reboot).
	Reboot	Starts the current Firebox again.
	Shutdown	Turns off the Firebox.
	Close	Closes the Firebox System Manager window.
View	Certificates	Lists the certificates on the Firebox and allows the user to list, add, and remove them.
	Feature Keys	Lists the current Feature Keys on the Firebox.
	Communication Log	Opens the communication log, which contains information such as the success or failure of logins, handshakes, and so on. These are connections between the Firebox and Firebox System Manager.
Tools	Policy Manager	Opens Policy Manager with the configuration of the selected Firebox.
	HostWatch™	Opens HostWatch connected to the current Firebox.
	Performance Console	Opens the Performance Console, which shows graphs of performance aspects of the Firebox.
	Synchronize Time	Synchronizes the time of the Firebox with the system time.
	Clear ARP Cache	Empties the ARP cache of the selected Firebox.
	Clear Alarm	Empties the alarm list on the selected Firebox.
	Rekey all BOVPN Tunnels	Expires all BOVPN tunnels and forces them to be rebuilt.
	Synchronize Feature Key	
	High Availability	Allows you to manually control High Availability functions.
	Change Passphrases	Changes the status and configuration passphrases.
	Firebox System Manager Help	Opens the online Help files for this application.
Help	About	Shows version and copyright information.


Firebox System Manager icons

Icon	Function
	Starts the display again. This icon appears only when you are not connected to a Firebox.
	Stops the display. This icon appears only when you are connected to a Firebox.
	Shows the management and VPN certificates saved on the Firebox.
	Shows the feature keys registered and installed for this Firebox.
	Starts Policy Manager. Use Policy Manager to make or change a configuration file.
	Starts HostWatch, which shows connections for this Firebox.
	Starts the Performance Console where you can configure graphs that show Firebox status.
	Shows the Communication Log dialog box to show connections between Firebox System Manager and the Firebox.

Firebox System Manager buttons

Button	Function
Renew Now	Appears in the upper-right part of the FSM window when a WSM feature or service has expired. To renew it, click the button.
Activate Now	Appears in the upper-right part of the FSM window when the Firebox has not yet been activated. To go to the LiveSecurity web site to activate it, click the button.
Force Failback	Appears in the upper-right part of the FSM window when multi-WAN failback occurs. Click the button to fail back to the other WAN interface.

Start Firebox System Manager

1. If you have not already done so, [start WatchGuard System Manager](#). From WatchGuard System Manager, select the **Device Status** tab.
2. Select the Firebox to examine with Firebox System Manager. (If you have not yet connected to a Firebox, [connect to a Firebox](#).)
3. Click .
Or, select **Tools > Firebox System Manager**.

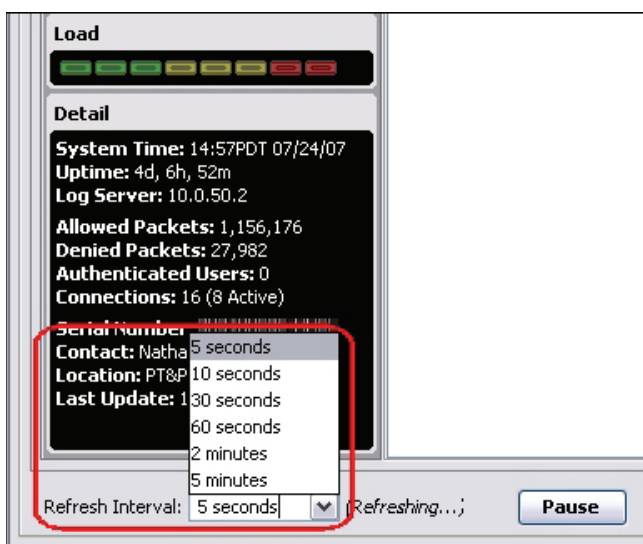
Firebox System Manager appears. You might need to wait a moment for Firebox System Manager to connect to the Firebox before you can see status information.

Set the refresh interval and pause display

All tabs on Firebox System Manager have, at the bottom of the screen, a drop-down list to set the refresh interval, and a **Pause** button to stop the display.

Refresh Interval

The refresh interval is the polling interval; the time between refreshes of the display. You can change the interval of time (in seconds) that Firebox System Manager gets the Firebox information and sends updates to the user interface. You must balance how frequently you get information and the load on the Firebox. Be sure to examine the refresh interval on each tab. When a tab gets new information for its display, the text Refreshing... appears adjacent to the **Refresh Interval** drop-down list. A shorter time interval gives a more accurate display, but creates more load on the Firebox. From Firebox System Manager, use the **Refresh Interval** drop-down list to select a new duration between window refreshes. You can select 5 seconds, 10 seconds, 30 seconds, 60 seconds, 2 minutes, or 5 minutes. You can also type a custom value into this box.




Pause/Continue

You can click the **Pause** button to temporarily stop Firebox System Manager from refreshing this window. After you click the **Pause** button, this button changes to a **Continue** button. Click **Continue** to continue to refresh the window.

Basic Firebox and network status (Front Panel tab)

The **Front Panel** tab of Firebox System Manager shows basic information about your Firebox, your network, and network traffic. It also shows warnings about your Firebox or its components.

To open Firebox System Manager:

1. From WatchGuard System Manager, select the **Device Status** tab.
2. Select the Firebox to examine with Firebox System Manager.
3. Click .

Or, select **Tools > Firebox System Manager**.

Firebox System Manager appears. It may take a moment to connect to the Firebox to get information about the status and configuration.

For details on Firebox and network status, see:

- [Visual display of traffic between interfaces](#)
- [Traffic volume, processor load, and basic status](#)
- [Firebox status](#)
- [VPN tunnel status and security services](#)

Warnings

Any warnings appear before all other status information:

- If the Firebox has not yet been activated, a warning appears and the **Activate Now** button is visible in the upper-right corner of the window. Click it to go to the LiveSecurity Service web site where you can get a feature key for the Firebox.
- If any WSM services will expire soon, a warning appears and the **Renew Now** button is visible in the upper-right corner of the window. Click it to go to the LiveSecurity Service web site where you can renew the services.


Expand and close tree views

To expand a part of the display, click the plus sign (+) adjacent to the entry, or double-click the name of the entry. To close a part, click the minus sign (–) adjacent to the entry. When no plus or minus sign shows, no more information is available.

Visual display of traffic between interfaces

At the upper-left corner of the window, Firebox System Manager has a visual display that shows the direction of traffic between Firebox interfaces. The display also shows whether the current traffic is allowed or denied at each interface. The display can be in the shape of a triangle or a star.

To open Firebox System Manager:

1. From WatchGuard System Manager, select the **Device Status** tab.
2. Select the Firebox to examine with Firebox System Manager.
3. Click .

Or, select **Tools > Firebox System Manager**.

Firebox System Manager appears. It may take a moment to connect to the Firebox to get information about the status and configuration.

The points of the star and triangle show the traffic that flows through the interfaces. A green point shows traffic is being allowed at that interface. A red point shows that traffic is being denied, or that the interface is denying some traffic and allowing other traffic. Each point shows incoming connections and outgoing connections with different arrows. When traffic flows between the two interfaces, the arrows light up in the direction of the traffic.

In the star figure, the location where the points come together can show one of two conditions:

- Red (deny)—The Firebox denies a connection on that interface.
- Green (allow)—There is traffic between this interface and a different interface (but not the center) of the star. When there is traffic between this interface and the center, the point between these interfaces shows as green arrows that blink.

In the triangle, the network traffic shows in the points of the triangle. The points show only the idle or deny condition. One exception is when there is a large quantity of default-route VPN traffic. Default-route VPN traffic refers to packets that are sent through a VPN to a Firebox configured as the default gateway for the VPN network. In this case, the Firebox System Manager traffic level indicator can show very high traffic, but you do not see green lights as more default-route VPN traffic comes in and goes out of the same interface.

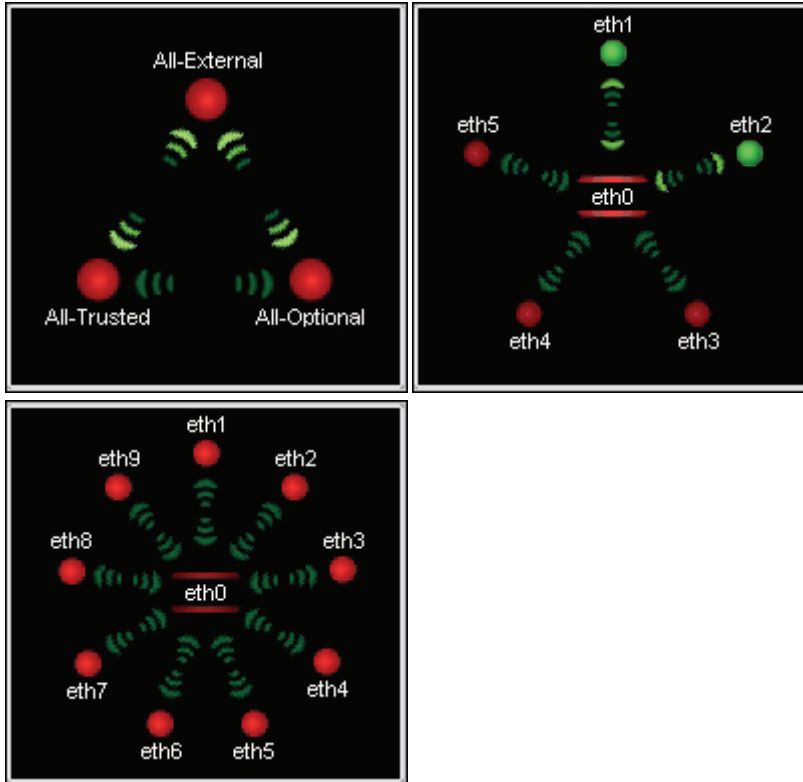
Triangle display

If a Firebox has only three configured interfaces, each corner of the triangle is one interface. If a Firebox has more than three interfaces, each corner of the triangle represents one type of interface. For example, if you have six configured interfaces with one external, one trusted, and four optional interfaces, the All-Optional corner in the triangle represents all four of the optional interfaces.

Star display

The star display shows all traffic in and out of the center interface. An arrow that moves from the center interface to a node interface shows that the Firebox is passing traffic. The traffic comes in through the center interface and goes out through the node interface. For example, if eth1 is at the center and eth2 is at a node, a green arrow shows that traffic flows from eth1 to eth2. There are two star displays — one for a Firebox X Core with 6 interfaces and one for Firebox X Peak with 10 interfaces.

If you use the star figure, you can customize the interface that appears in its center. Click the interface name or its point. The interface then moves to the center of the star. All the other interfaces move clockwise. If you move an interface to the center of the star, you can see all traffic between that interface and all other interfaces. The default display shows the external interface in the center.




To change the display, right-click it and select **Triangle Mode** or **Star Mode**.

Traffic volume, processor load, and basic status

Firebox System Manager shows traffic volume, processor load, and basic status on its front panel.

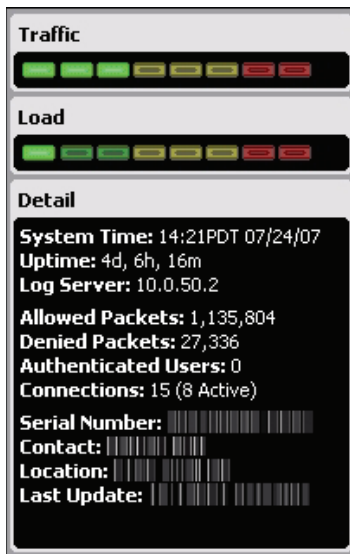
To open Firebox System Manager:

1. From WatchGuard System Manager, select the **Device Status** tab.
2. Select the Firebox to examine with Firebox System Manager.
3. Click .

Or, select **Tools > Firebox System Manager**.

Firebox System Manager appears. It may take a moment to connect to the Firebox to get information about the status and configuration.


Below the **Security Traffic Display** are the traffic volume indicator, processor load indicator, and basic status information (Detail). The two bar graphs show the traffic volume and the Firebox capacity.



Firebox status

Firebox System Manager to the right side of the front panel shows basic status information.

To open Firebox System Manager:

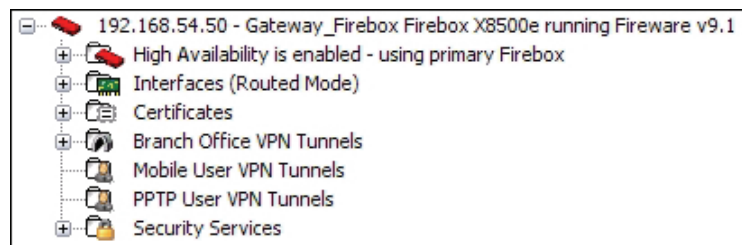
1. From WatchGuard System Manager, select the **Device Status** tab.
2. Select the Firebox to examine with Firebox System Manager.
3. Click .

Or, select **Tools > Firebox System Manager**.

Firebox System Manager appears. It may take a moment to connect to the Firebox to get information about the status and configuration.

Status and warnings

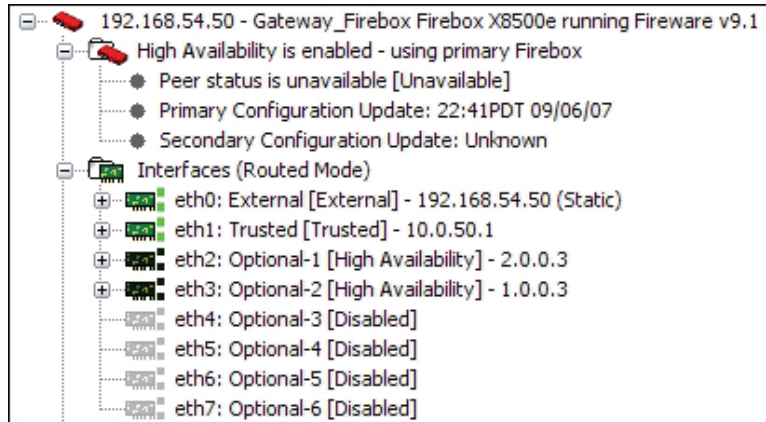
- Status of the Firebox: This includes the Fireware version and patch string.
- Warnings: Appear when updates for Security Services are available or when Subscription Services or other features are soon to expire. To renew, click the **Renew Now** button that appears in the upper-right part of the FSM window.



Firebox, High Availability, and interface details

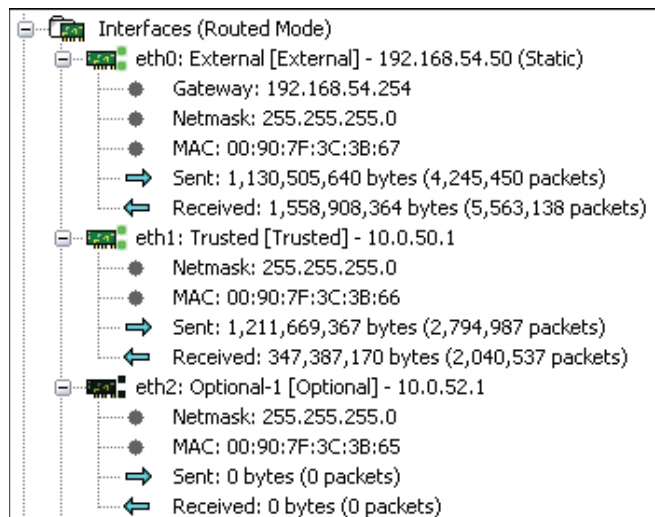
On the **Front Panel** tab of Firebox System Manager (the one visible when you first start FSM), expand the entries to see:

- If High Availability is configured, whether the HA peer is available. The time at which the configuration of the primary and secondary devices was last updated also appears.
- The IP address of each Firebox interface and the configuration mode of the external interface.



If you again expand the entries for each interface, you can see:

- IP address, gateway, and netmask of each configured interface
- Media Access Control (MAC) address of each interface
- Number of bytes and packets sent and received since the last Firebox restart
- Status of the physical link (an interface or link icon in color means an interface or link is configured, and a dark icon indicates the interface or link is down)



Certificates and their current status


FSM shows certificates on the Firebox and their current status. For valid certificates, FSM shows the validity period and fingerprint.



VPN tunnel status and security services

The front panel of Firebox System Manager includes statistics about current VPN tunnels.

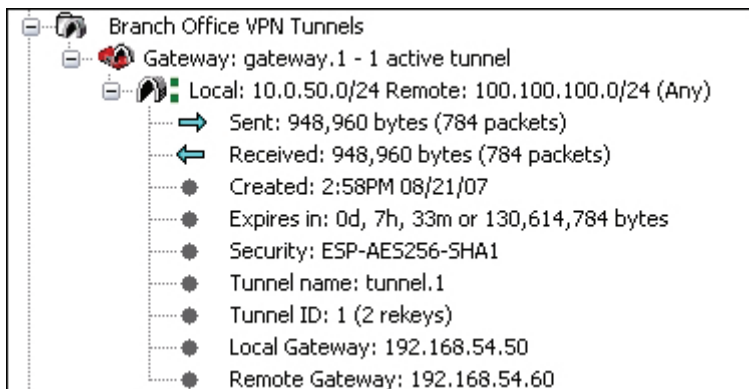
To open Firebox System Manager:

1. From WatchGuard System Manager, select the **Device Status** tab.
2. Select the Firebox to examine with Firebox System Manager.
3. Click .

Or, select **Tools > Firebox System Manager**.

Firebox System Manager appears. It may take a moment to connect to the Firebox to get information about the status and configuration.

Below the Firebox Status section on the right side of the screen is a section on BOVPN tunnels. Firebox System Manager shows the current tunnel status and gateway information for each VPN tunnel as well as data sent and received, creation and expiration information, type of authentication and encryption, and number of rekeys.



Each BOVPN tunnel is shown in one of three states:

Active

The BOVPN tunnel is operational and passing traffic.

Inactive

The BOVPN tunnel has been created, but no tunnel negotiation has occurred. No traffic has been sent through the VPN tunnel.

Expired

The BOVPN tunnel was active, but is no longer active because the tunnel has no traffic or because the link between the gateways is lost.

This information also appears on the **Device Status** tab in WatchGuard System Manager.

Mobile VPN tunnel status

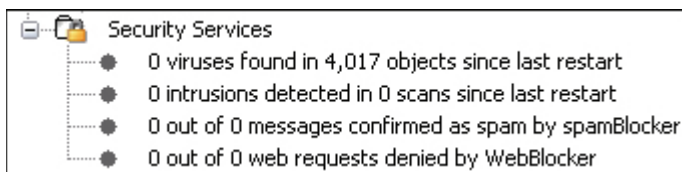
Firebox System Manager shows the user name, IP address information, and the quantity of sent and received packets for the three types of Mobile VPN Tunnels:

- Mobile VPN with IPSec
- Mobile VPN with SSL
- Mobile VPN with PPTP

To log off Mobile VPN users, right-click a user and select **Logoff selected user**.

Security Services status

Below Security Services, Firebox System Manager shows the number of viruses found, the number of intrusions, the number of email messages confirmed as spam, and the number of web requests denied by WebBlocker since the last restart.



Firebox log messages (Traffic Monitor)

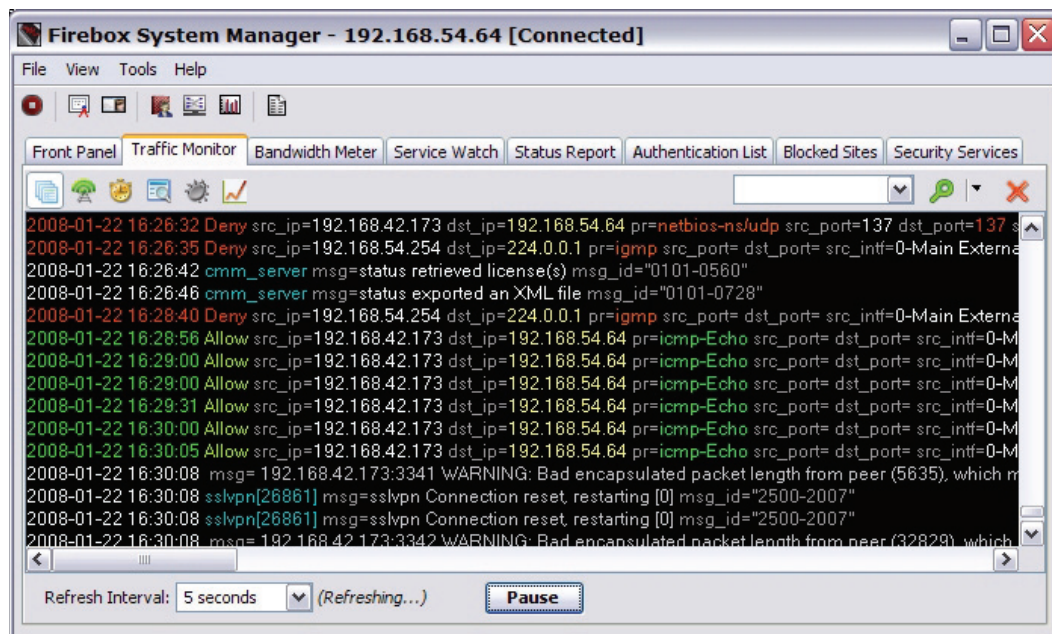
To see near real-time Firebox log messages:

1. [Start Firebox System Manager](#).
2. Click the **Traffic Monitor** tab.

Traffic Monitor can help you troubleshoot network performance. You can see, for example, which policies are used the most or whether external interfaces are constantly used to their maximum capacity.

You can customize Traffic Monitor in these ways:

- [Change Traffic Monitor settings](#)
- [Copy messages to another application](#)
- [Learn more about a message](#)
- [Enable notification for specific messages](#)
- Use the icons at the top of Traffic Monitor to display only specific [types of log messages](#).
- When you set up logging for a Firebox, you can tell the Firebox to show diagnostic messages in Traffic Manager. This can be useful to quickly diagnose a problem. For more information, see [Enable advanced diagnostics](#).



Change Traffic Monitor settings

You can change a number of settings in Traffic Monitor:

1. [Start Firebox System Manager](#).
2. From Firebox System Manager, select **File > Settings**.
The Settings dialog box appears.

Set the maximum number of log messages

You can change the maximum number of log messages that you can keep and see on Traffic Monitor. When you get to the maximum number, the new log messages replace the first entries. If you have a slow processor or a small quantity of RAM, a high value in this field can slow your management system.

If it is necessary to examine a large volume of log messages, we recommend that you use LogViewer, as described in [Use LogViewer to see log files](#).

1. From Firebox System Manager, select **File > Settings**.
The Settings dialog box appears.
2. From the **Maximum Log Messages** drop-down list, select the number of log messages that you want to appear in Traffic Monitor. Click **OK**. The value you type gives the number of log messages in thousands.

Show log field names

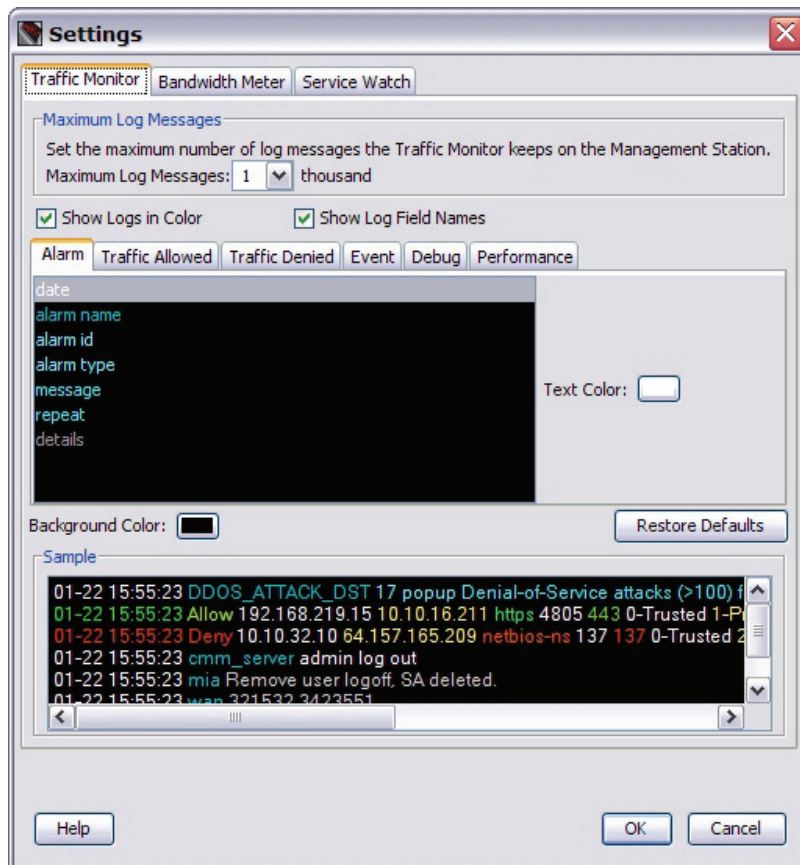
You can specify that Traffic Monitor include labels for message fields, such as src_ip, dst_ip, and src_port.

1. From Firebox System Manager, select **File > Settings**.
The Settings dialog box appears.
2. Select the **Show log field names** check box. Click **OK**.

Use color for log messages

In Traffic Monitor, you can make messages appear in different colors. You can use different colors to differentiate between types of information.

1. From Firebox System Manager, select **File > Settings**. Click the **Traffic Monitor** tab.



2. To disable or enable the display of colors, clear or select the **Show Logs in Color** check box.
3. On the **Alarm, Traffic Allowed, Traffic Denied, Event, Debug, or Performance** tab, click the field to appear in a color. The box next to Text Color on the right side of the tabs shows the color in use for the field.
4. To change the color, click the box next to **Text Color**. Select a color. A sample of how the color will look in Traffic Monitor appears at the bottom of the dialog box. Click **OK** to close the color control dialog box, or **Reset** to go back to the color used for text before you opened the color control dialog box. Click **OK** again to close the **Settings** dialog box.
5. You can also select a background color for Traffic Monitor. Click the box next to **Background Color**. Use the procedures described in the previous step to change the color.

You can cancel the changes you make in this dialog box. Click **Restore Defaults**.

Copy messages to another application

To make a copy of a log message and paste it in a different software application, right-click the message and select **Copy Selection**. If you select **Copy All**, Firebox System Manager copies all the log messages. Open the other software application and paste the message or messages.

You may want to open the log file in LogViewer, which has a richer set of features for working with log messages. For more information on LogViewer, see [Use LogViewer to see log files](#) and the related topics [Import and export log file data](#) and [Email, Print, or Save log messages](#).

Learn more about a message

To learn more about a traffic log message, you can:

Ping the source or destination

To ping the source or destination IP address of a traffic log message, right-click the message, and select **Ping**. The **Diagnostic Tasks** dialog box appears with **Ping** selected in the **Tasks** drop-down list. Enter an address to ping and click **Run Task**.

Trace the route to the source or destination

To trace the route to the source or destination IP address of a traffic log message, right-click the message and select **Trace Route**. The **Diagnostic Tasks** dialog box appears with **Trace Route** selected in the **Tasks** drop-down list. Enter an address and click **Run Task**.

Enable notification for specific messages

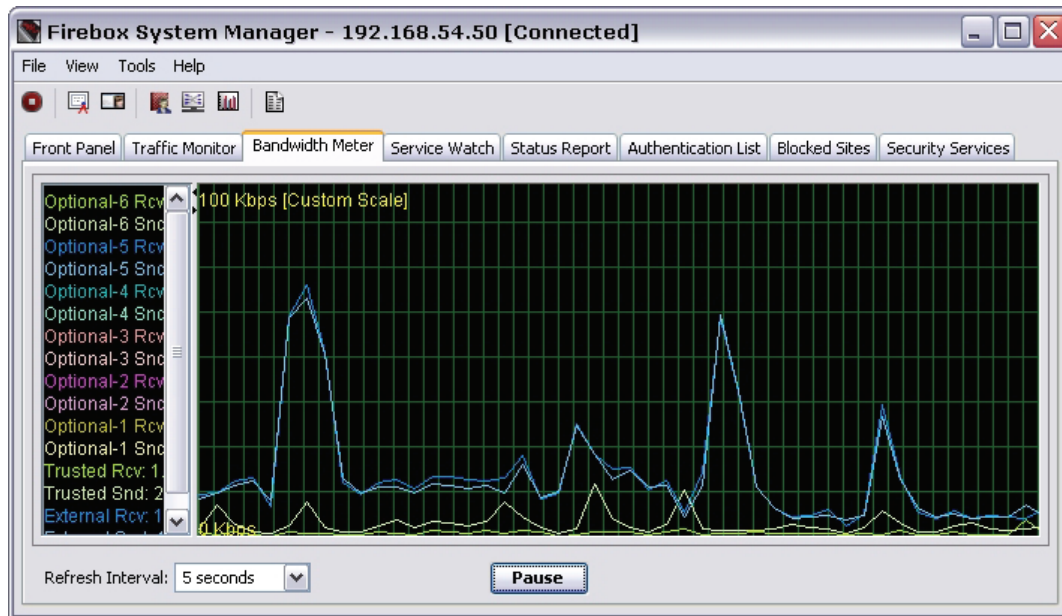
If you want to monitor specific Firebox events that do not normally trigger a notification, you can enable notification for specific messages in the Traffic Log. Subsequent log messages with the same message identifier will trigger a notification.

1. Right-click any message and select **Event Notifications**.
The **Event Notifications** dialog box appears. Identifiers and descriptions of each message appear in a table. To sort by a particular column, click the column heading.
2. Select the **Notify** check box for messages you want notifications for.

The notification parameters at the bottom of the dialog box apply to all event notifications. For information on how to use these fields, see [Set logging and notification preferences](#).

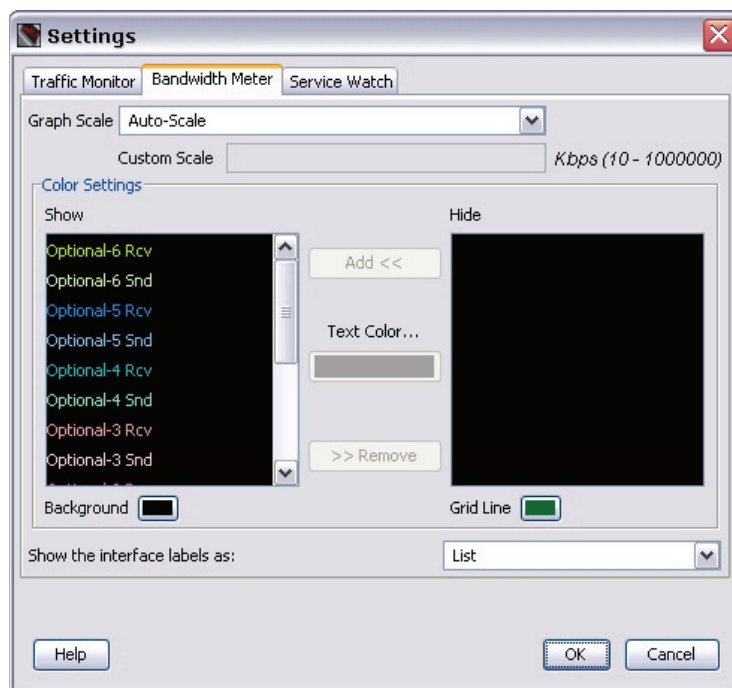
Visual display of bandwidth usage (Bandwidth Meter tab)

Select the **Bandwidth Meter** tab to see the real-time bandwidth for all the Firebox interfaces. The Y axis (vertical) shows the number of connections. The X axis (horizontal) shows the time. If you click any location on the chart, you can get more detailed information in a pop-up window about bandwidth use at that point in time. The meter shows VLAN interfaces, if any are defined, in addition to physical interfaces.



To change how the bandwidth appears:

From Firebox System Manager, select **File > Settings**. Click the **Bandwidth Meter** tab.



Do one or more of the steps in the sections below.

Change the scale

You can change the scale of the **Bandwidth Meter** tab. Use the **Graph Scale** drop-down list to select the value that is the best match for the speed of your network. You can also set a custom scale. Type the value in kilobytes for each second in the **Custom Scale** text box.

Add and remove lines

To add a line to the **Bandwidth Meter** tab, select the interface from the **Hide** list in the Color Settings section. Use the **Text Color** control to select a color for the line. Click **Add**. The interface name appears in the **Show** list with the color you selected.

To remove a line from the **Bandwidth Meter** tab, select the interface from the **Show** list in the Color Settings section. Click **Remove**. The interface name appears in the **Hide** list.

Change colors

You can change the colors of the display of the **Bandwidth Meter** tab. Use the **Background** and **Grid Line** color control boxes to select a new color.

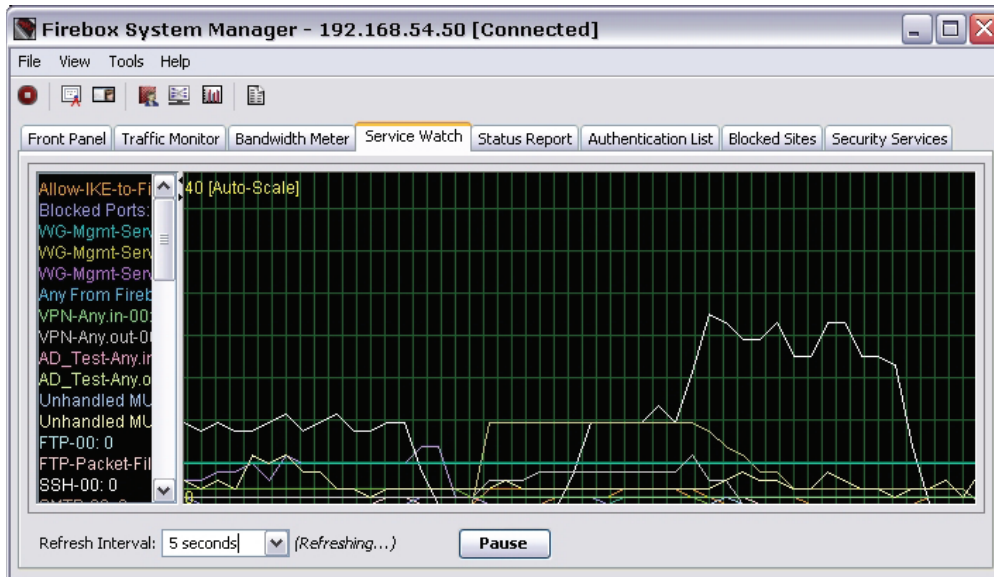
Change how interfaces appear

One option is to change how the interface names appear on the left side of the **Bandwidth Meter** tab. The names can appear as a list. The display can also show an interface name adjacent to the line it identifies. Use the **Show the interface** text as a drop-down list to select **List** or **Tags**.

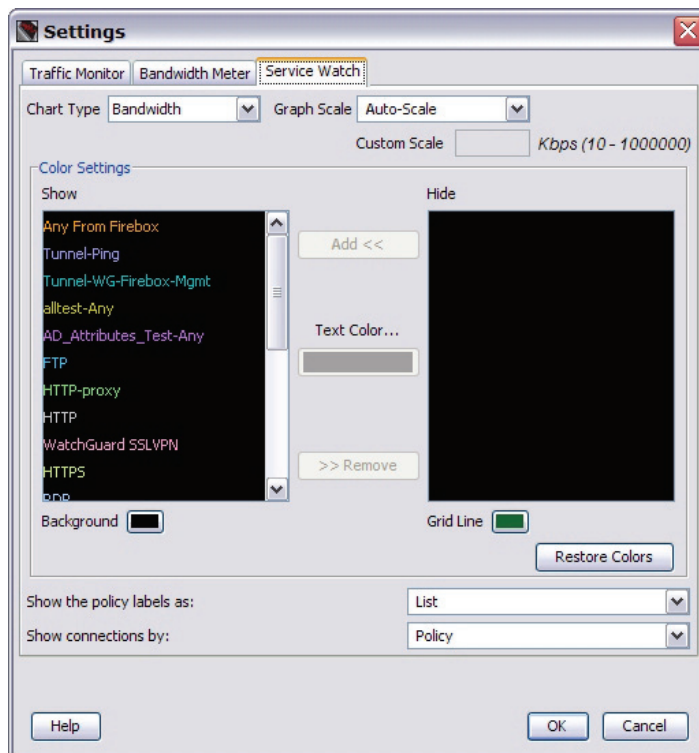
To see bandwidth use by policy instead of interface, see [Visual display of policy usage \(Service Watch tab\)](#).

Visual display of policy usage (Service Watch tab)

Select the **Service Watch** tab of Firebox System Manager to see a graph of the policies that are configured in Policy Manager for a Firebox. The Y axis (vertical) shows the number of connections. The X axis (horizontal) shows the time. If you click any location on the chart, you can get more detailed information in a pop-up window about policy use at this point in time.



1. To change how the policies appear, select **File > Settings**. Click the **Service Watch** tab.
2. Do one or more of the steps in the sections below.



Change the scale

You can change the scale of the **Service Watch** tab. Use the **Graph Scale** drop-down list to select the value that is the best match for the volume of traffic on your network. You can also set a custom scale. Type the number of connections in the **Custom Scale** text box.

Display bandwidth used by a policy

To display bytes per second used by a policy instead of number of connections, from the **Chart Type** drop-down menu, select **Bandwidth**.

To see bandwidth use by interface instead of policy, see [Visual display of bandwidth usage](#) (Bandwidth Meter tab).

Add and remove lines

- To add a line to the **Service Watch** tab, select the policy from the **Hide** list in the **Color Settings** section. Use the **Text Color** control to select a color for the line. Click **Add**. The interface name appears in the **Show** list with the color you selected.
- To remove a line from the **Service Watch** tab, select the policy from the **Show** list in the **Color Settings** section. Click **Remove**. The interface name appears in the **Hide** list.

Change colors

You can change the colors of the display of the **Service Watch** tab. Use the **Background** and **Grid Line** color control boxes to select a new color.

Change how policy names appear

You can change how the policy names appear on the left side of the **Service Watch** tab. The names can show as a list. The tab can also show an interface name adjacent to the line it identifies. Use the **Show the policy labels as** drop-down list to select **List or Tags**.

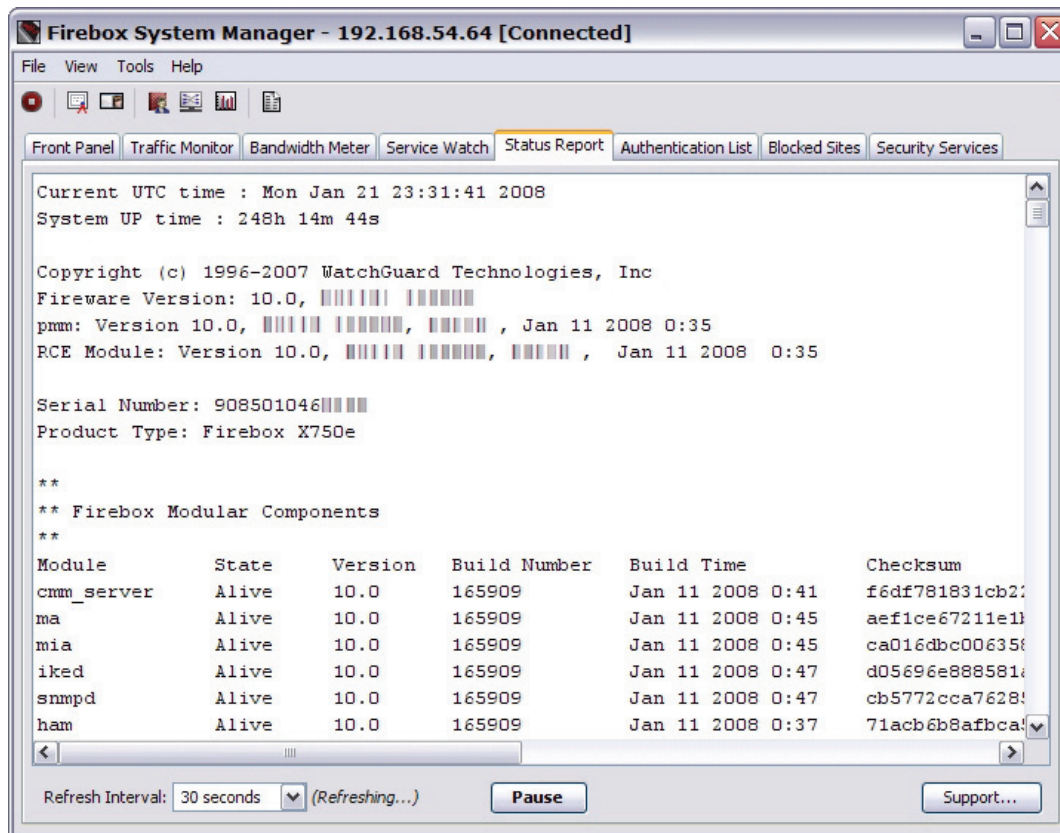
Show connections by policy or rule

Use the **Show connections by** drop-down list to define whether you want the graph to show connections by policy or rule. If you select **Policy**, the left side of the graph changes to a list of policies that corresponds with the policies that appear in the Policy Manager window. This includes policies on the **Firewall** tab and the **Mobile User with IPsec** tab.

If you select **Rule**, the graph changes to show activity based on rules defined in Policy Manager.

Traffic and performance statistics (Status Report)

The **Status Report** tab gives you statistics about Firebox traffic and performance.



To see the Firebox Status Report:

1. [Start Firebox System Manager](#).
2. Click the **Status Report** tab.

The Firebox Status Report contains this information:

Uptime and version information

Firebox uptime, the WatchGuard Firebox System software version, the Firebox model, appliance software version, and patch, if applicable. There is also a list of the status and version of the product components on the Firebox.

Log Servers

IP addresses of all configured Log Servers.

Logging options

Log message options that are configured with the Quick Setup Wizard or Policy Manager.

Memory and load average

Statistics on the memory use (shown in bytes of memory) and load average of the Firebox. The load average has three values that typically show an average over the last minute, 5 minutes, and 15 minutes. Values over 1.00 (100%) indicate some threads are queued until resources are available. (A system load that exceeds 1.00 does not mean the system is overloaded.)

Processes

Process ID, the name of the process, and the status of the process.

Network configuration

Information about the network cards in the Firebox: the interface name, its hardware and software addresses, and its netmask. The display also includes local routing information, IP aliases, and reserved DHCP leases.

Blocked Sites list, Blocked Sites exceptions

Current manually blocked sites and any current exceptions. Temporarily blocked site entries appear on the permanent **Blocked Sites** tab.

Interfaces

Each Firebox interface, along with information about the type of interface it is configured as (external, trusted, or optional), its status, and packet count.

Routes

Firebox kernel routing table. You use these routes to find which Firebox interface is used for each destination address. ECMP groups and dynamic routes that have been accepted by the dynamic routing daemon appear here as well.

ARP table

ARP table on the Firebox. The ARP table is used to match IP addresses to hardware addresses. (When an appliance is in drop-in mode, use the contents of the ARP table only to troubleshoot connectivity over secondary networks on the interfaces.)

Total Dynamic Network Address Translation (DNAT) entries

Number of used and available entries.

Multi-WAN status

Information on gateways and sticky connections. Also includes the sticky connections table.

DHCP client leases

Information on DHCP client leases on the Firebox.

Dynamic Routing

Dynamic routing components in use on the Firebox, if any.

DNS Servers

Address information for DNS servers.

Refresh interval

Rate at which this display updates the information.

Support

Click **Support** to open the **Support Logs** dialog box. This is where you set the location to which you save the diagnostic log file. You save a support log in tarzipped (*.tgz) format. You create this file for troubleshooting, when asked by your support representative.

Authenticated users (Authentication List)

The **Authentication List** tab of Firebox System Manager gives information about all the persons that are authenticated to the Firebox.

To see the Firebox Authentication List:

1. [Start Firebox System Manager](#).
2. Click the **Authentication List** tab.

Information about each authenticated user appears in these four columns:

User

The name the user gives he or she authenticates.

Type

The type of user who authenticated: Firewall or Mobile User.

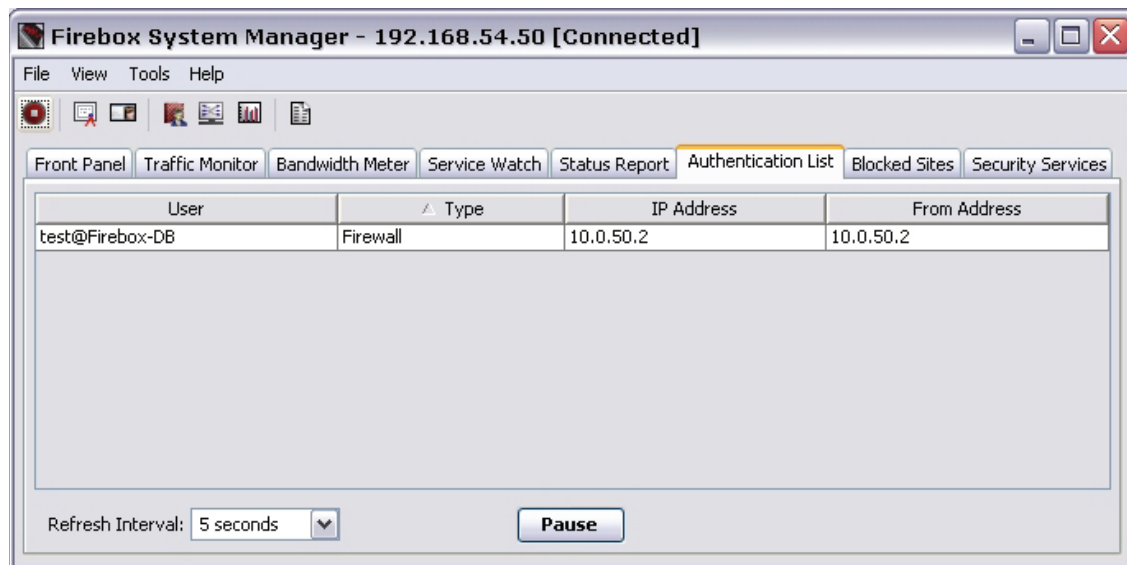
IP Address

The internal IP address being used by the user. For mobile users, the IP address shown here is the IP address assigned to them by the Firebox.

From Address

The IP address on the computer the user authenticates from. For mobile users, the IP address shown here is the IP address on the computer they used to connect to the Firebox. For Firewall users, the IP Address and From Address are the same.

You can click the column headers to sort users. You can also log the user off the Firebox. To do this, right-click the user name and then stop his or her authenticated session.



See or change the Blocked Sites list

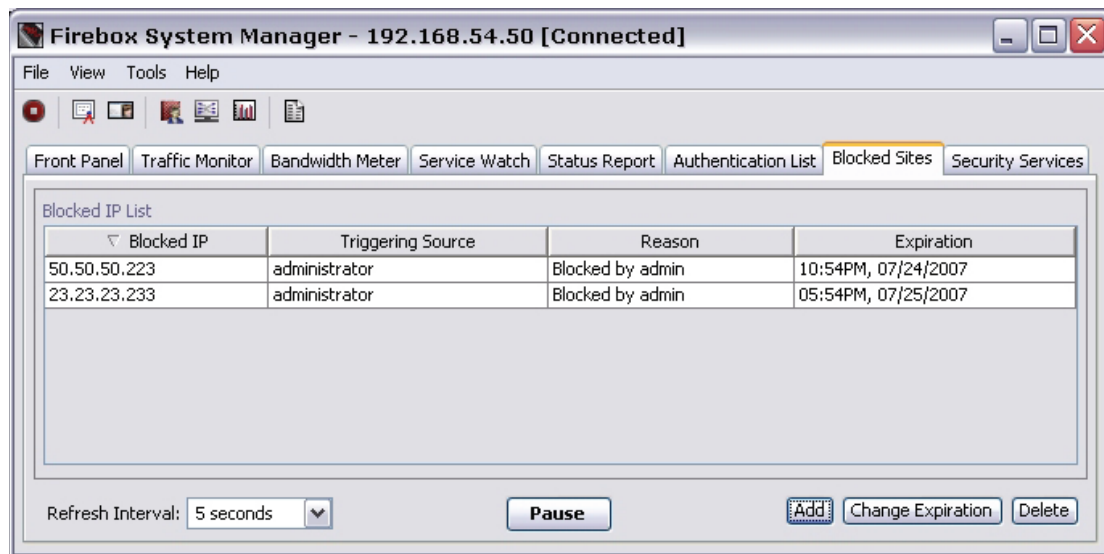
The **Blocked Sites List** tab of Firebox System Manager shows the IP addresses of all the external IP addresses that are temporarily blocked. Many events can cause the Firebox to add an IP address to the **Blocked Sites** tab: a port space probe, a spoofing attack, an address space probe, or an event you configure.

Adjacent to each IP address is the time when it comes off the **Blocked Sites** tab. You can use the **Blocked Sites** dialog box in Policy Manager to adjust the length of time that an IP address stays on the list.

Add and remove sites

Add allows you to temporarily add a site to the Blocked Sites list. Click **Change Expiration** to change the time at which this site is deleted from the list. **Delete** removes the site from the Blocked Sites list.

You can remove a site from the list only if you open the Firebox with the configuration passphrase.



Security services

The **Security Services** tab of Firebox System Manager includes current Firebox statistics about these security subscriptions, if installed:

- [Gateway AntiVirus statistics](#)
- [Intrusion Prevention Service statistics](#)
- [SpamBlocker statistics](#)

You can also use this page to update the signatures and engine for Gateway AntiVirus and Intrusion Protection Service, as described in [See status and update signatures or engine manually](#).

Gateway AntiVirus statistics

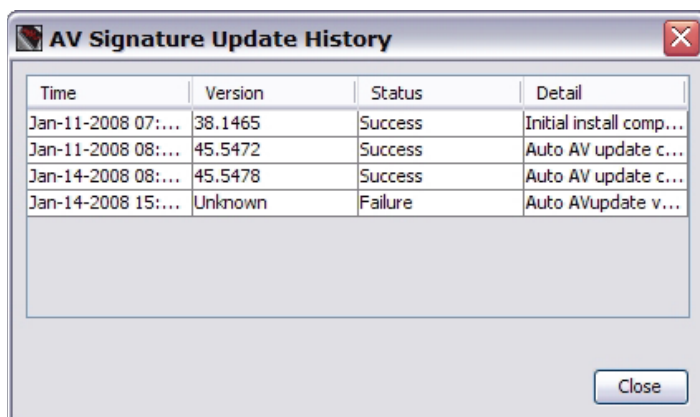
The **Security Services** tab of Firebox System Manager includes current Firebox statistics about the Gateway AntiVirus feature.

Activity since last restart

- Viruses found: Number of viruses found in scanned files since the last Firebox restart.
- Objects scanned/not scanned: Number of files scanned or not scanned for viruses since the last Firebox restart.

Signatures

- Installed version: Version number of the installed signatures.
- Last update: Date of the last signature update.
- Version available: If a new version of the signatures is available.
- Server URL: URL that the Firebox goes to see if updates are available, and the URL that updates are downloaded from.
- History: Click to show a list of all the signature updates. You can right-click to copy information on a selected update, or on the entire list of updates.
- Update: Click to update your virus signatures. This button is active only if a new version of the virus signatures is available.



The screenshot shows a window titled "AV Signature Update History" with a close button in the top right corner. Inside the window is a table with four columns: Time, Version, Status, and Detail. The table contains four rows of update history. Below the table is a large empty rectangular area, and at the bottom right is a "Close" button.

Time	Version	Status	Detail
Jan-11-2008 07:...	38.1465	Success	Initial install comp...
Jan-11-2008 08:...	45.5472	Success	Auto AV update c...
Jan-14-2008 08:...	45.5478	Success	Auto AV update c...
Jan-14-2008 15:...	Unknown	Failure	Auto AVupdate v...

Engine

- Installed version: Version number of the installed engine.
- Last update: Date of the last engine update.
- Version available: If a new version of the engine is available.
- Server URL: URL that the Firebox goes to see if updates are available, and the URL that updates are downloaded from.
- History: Click to show a list of all the engine updates. You can right-click to copy information on a selected update, or on the entire list of updates.
- Update: Click to update your virus signatures.

Intrusion Prevention Service statistics

The **Security Services** tab of Firebox System Manager includes current Firebox statistics about the signature-based Intrusion Prevention Service feature.

Activity since last restart

- Scans performed: Number of files scanned for viruses since the last Firebox restart.
- Intrusions detected: Number of intrusions found in scanned files since the last Firebox restart.
- Intrusions prevented: Number of infected files deleted since the last Firebox restart.

Signatures

- Installed version: Version number of the installed signatures.
- Last update: Date of the last signature update.
- Version available: If a new version of the signatures is available.
- Server URL: URL that the Firebox goes to see if updates are available, and the URL that updates are downloaded from.
- History: Click to show a list of all the signature updates.
- Update: Click to update your intrusion prevention signatures. This button is active only if a new version of the intrusion prevention signatures is available.
- Show: Click to download and show a list of all current IPS signatures. After you download the signatures, you can look for signatures by signature ID.

spamBlocker statistics

The **Security Services** tab of Firebox System Manager includes current Firebox statistics about spamBlocker:

1. [Start Firebox System Manager](#).
2. Click the **Security Services** tab.

The following information appears:

- Number of messages since last restart that are identified as confirmed spam, bulk email, suspected spam, or not spam.
- Number of messages since last restart that are blocked, tagged, or sent to the Quarantine Server.
- Number of messages since last restart that are blocked or allowed because of a spamBlocker exceptions list that you create (exceptions that you create to deny additional sites are sometimes known as a blacklist; exceptions that you create to allow additional sites are sometimes known as a whitelist).

If you reboot the Firebox, all counters reset to zero.

About HostWatch

HostWatch is a graphical user interface that shows the connections between different Firebox interfaces. HostWatch also gives information about users, connections, ports, whether the connection is normal or blocked, and other information.

The HostWatch window

The top part of the HostWatch window has two sides. You can set one interface you want to monitor on the left side. The right side shows the connections to and from the interface configured on the left side.

The lines that connect source hosts and destination hosts use colors that show the type of connection. You can change these colors. The default colors are:

- **Red** — The Firebox denies the connection.
- **Blue** — The connection uses a proxy.
- **Green** — The Firebox uses NAT for the connection.
- **Black** — Normal connection (the connection has been accepted, and it does not use a proxy or NAT).

Icons that show the type of service appear adjacent to the server entries.



Telnet



FTP



HTTP



Other



Email

DNS resolution and HostWatch

Domain name server (DNS) resolution does not occur immediately when you start HostWatch. When HostWatch is configured for DNS resolution, it replaces the IP addresses with the host or user names. If the Firebox cannot identify the host or user name, the IP address stays in the HostWatch window.

If you use DNS resolution with HostWatch, the management station can send a large number of NetBIOS packets (UDP 137) through the Firebox. The only method to stop this is to turn off NetBIOS over TCP/IP in Windows.

Start HostWatch

To start **HostWatch**, from Firebox System Manager, click .
Or, select **Tools > HostWatch**.

Pause HostWatch

You can use the **Pause** and **Continue** icons on the toolbar to temporarily stop and then restart the display.
Or, use **File > Pause** and **File > Continue**.

Select connections and interfaces to monitor

When you first start HostWatch, you see Firebox internal interfaces on the upper-left side of the window, and connections to and from those interfaces on the upper-right side. Double-click an item on either side to get the **Connections For** dialog box for connections that involve that item. The dialog box shows information about the connection, and includes the IP addresses, port number, time, connection type, and direction.

The bottom of the HostWatch window shows all connections to and from all interfaces. The information is shown in a table that includes:

- Source and destination
- Port
- Firebox interface used, and whether traffic was inbound or outbound
- Whether the connection was normal, proxied, blocked
- Details, such as the time the connection was created or the command used to create the connection

Select a new interface to monitor

To select a new interface, select **View > Interface** and select the interface you want to monitor. You can also right-click the current interface name and then select the new interface.

If you want to specify the exact interface name or use a regular expression to match multiple interfaces, select **Other** from the list of interfaces when you select **View > Interface**. This is useful when you want to see VLANs in HostWatch.

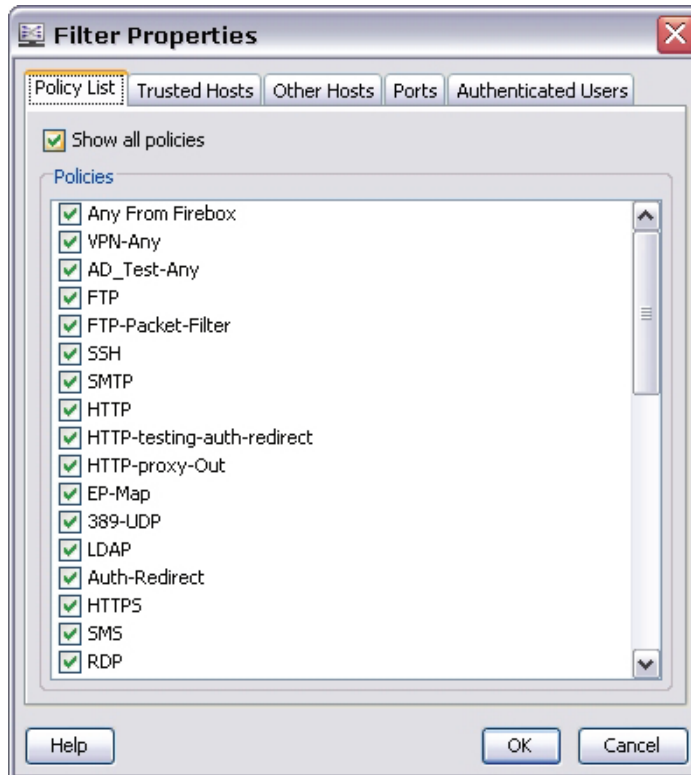
Source	Destination	Port	In	Out	Connection	Details
10.0.50.1	10.0.50.2	4115 / tcp		Trusted	Normal	Tue Jul 24 17:09:19 PDT 2007
10.0.50.2	pr-in-f99.153.238.com	80 / tcp	Trusted	External Proxy		HTTP: GET http://news.153.238.com/new...
10.0.50.2	153.238	80 / tcp	Trusted	External Proxy		HTTP: GET http://www.153.238.com/im...
10.0.50.2	153.238	80 / tcp	Trusted	External Proxy		HTTP: GET http://www.153.238.com/im...
10.0.50.2	pr-in-f99.153.238.com	80 / tcp	Trusted	External Proxy		HTTP: GET http://news.153.238.com/new...
10.0.50.2	.220.80	80 / tcp	Trusted	External Proxy		HTTP: GET http://153.238.com/1275935...
10.0.50.2	po-in-f165.15.21.com	80 / tcp	Trusted	External Proxy		HTTP: GET http://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js
10.0.50.2	.15.21	80 / tcp	Trusted	External Proxy		HTTP: GET http://15.21/get_vid...
10.0.50.2	rc-in-f99.15.21.com	80 / tcp	Trusted	External Proxy		HTTP: GET http://video.15.21.com/s?ns...

Ready Connections at: Tue Jul 24 18:10:29 PDT 2007 Connections shown: 22 (17)

Filter content of HostWatch window

By default, HostWatch shows all policies, hosts, ports, and authenticated users. You can change the HostWatch window to show only the content that you specify. You can use this feature to monitor specified policies, hosts, ports, or users.

1. From HostWatch, select **View > Filter**.

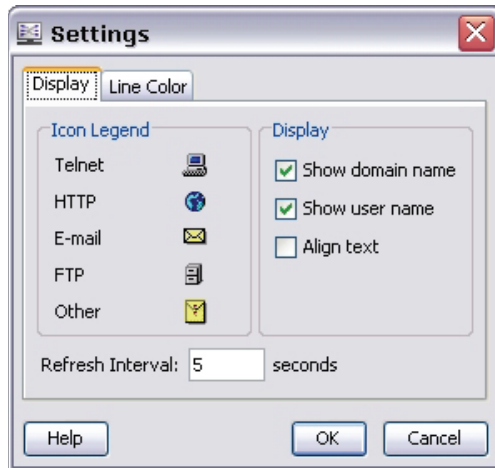


2. Click the tab to monitor: **Policy List, Main External Hosts, Other Hosts, Ports, or Authenticated Users**.
3. On the tab for each item you do want to see, type the IP address, port number, or user name to monitor. Click **Add**. If you are filtering by policies, select the check box next to each policy you want to monitor. You can also select each tab's **Show all** check box to show all items in the category.
4. Click **OK**.

Change HostWatch visual properties

You can change how HostWatch shows information. For example, you can tell HostWatch to show host names instead of addresses.

1. From HostWatch, select **View > Settings**.
2. Use the **Display** tab to change how the hosts appear in the HostWatch window.



3. Use the **Line Color** tab to change the colors of the lines between NAT, proxy, blocked, and normal connections.



4. Click **OK** to close the **Settings** dialog box.

Visit or block a site from HostWatch

If you want to visit a site shown in HostWatch, in the lower pane of the window, right-click the site and select **Visit Proxied Website**. In the pop-up window that appears, give the address of the site.

You can also block an IP address and add it to the Blocked Sites list:


1. In the top pane, right-click an IP address and select **Block Site: site address**. You can also right-click a connection in the lower pane and select either **Block Site: source address** or **Block Site: destination address**.
2. In the pop-up window that appears, give the amount of time for the site to remain blocked.
3. When prompted, type your configuration passphrase.

The Firebox will block all network connections to or from this IP address.

About the Performance Console

The Performance Console is a Firebox utility that you use to make graphs that show how different parts of the Firebox are operating. To get the information, you define the counters that identify the information that is used to make the graph.

Start the Performance Console

To start the Performance Console, from Firebox System Manager, click .

Or, select **Tools > Performance Console**.

The Add Chart window appears.

Make graphs with the Performance Console

To make graphs in the Performance Console:

- [Define performance counters](#). Counters are grouped into the categories listed in “Types of counters” below.
- Modify the chart or add a new one, as described in [Add charts or change polling intervals](#).

Types of counters

You can monitor these types of performance counters:

System Information

Show how the CPU is used.

Interfaces

Monitor and report on the events of selected interfaces. For example, you can set up a counter that monitors the number of packets a specified interface receives.

Policies

Monitor and report on the events of selected policies. For example, you can set up a counter that monitors the number of packets that a specified policy examines.

VPN Peers

Monitor and report on the events of selected VPN policies.

Tunnels

Monitor and report on the events of selected VPN tunnels.


Stop monitoring or close the window

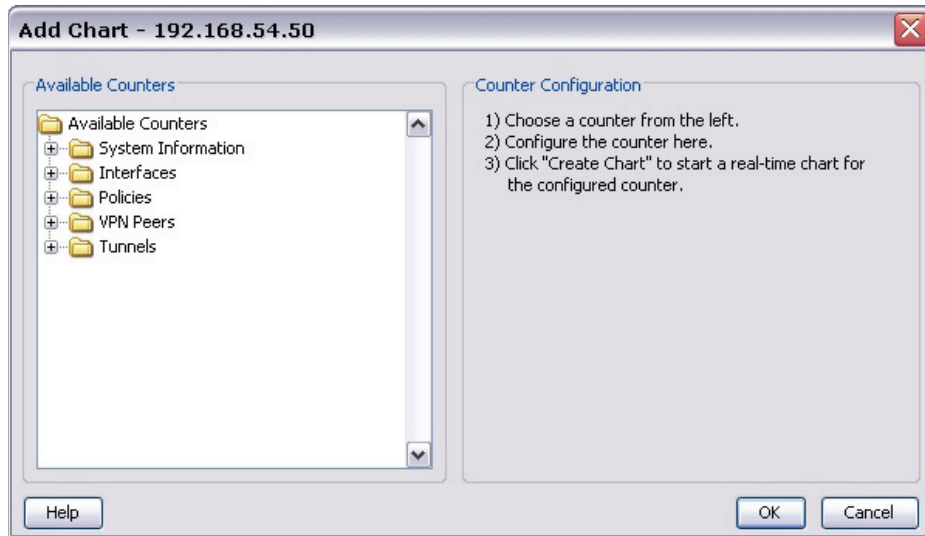
Click **Stop Monitoring** to stop the Performance Console from getting data for this counter. You can stop the monitor to save resources and restart it at different time.

Click **Close** to close the chart window.

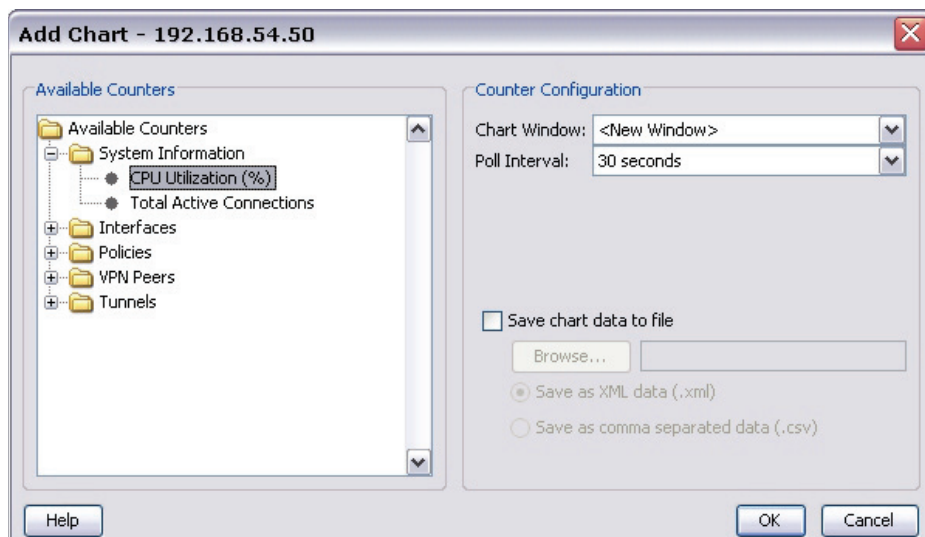
Define performance counters

To identify a counter for any of the categories:

1. From Firebox System Manager, click .
Or, select **Tools > Performance Console**.
The *Add Chart* window appears.



2. From the **Add Chart** window, expand one of the counter categories that appears below **Available Counters**.
Click the + sign adjacent to the category name to see the counters you can use in that category.
3. Click a counter, such as **CPU Utilization**. The Counter Configuration fields automatically refresh, related to the counter you select.



4. From the **Chart Window** drop-down list, select **<New Window>** if you want the graph to appear in a new window. Or, if any are listed, select the name of an open window to add the graph to a window that is open.
5. From the **Poll Interval** drop-down list, select a time interval between five seconds and one hour. This is the frequency that the Performance Console checks for updated information from the Firebox.

6. Add configuration information that applies to the specified counter. Certain fields appear automatically according to which counter you select. Some of the fields are:
 - **Type** — Use the drop-down list to select the type of graph to create: rate, difference, or raw value.

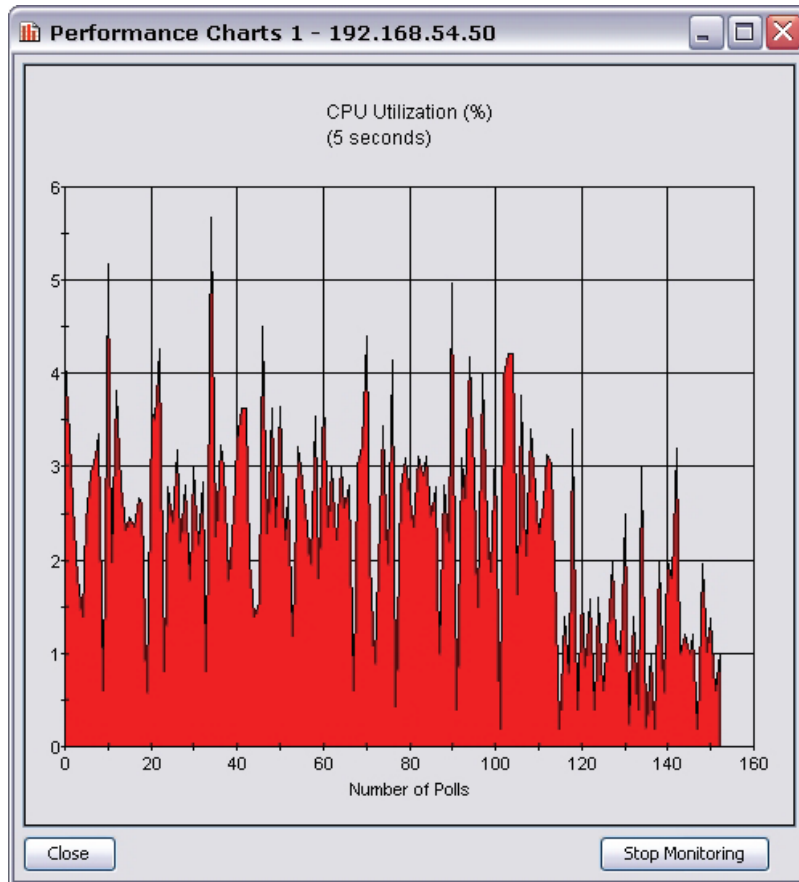
Suppose you want to graph value_1 and time_1, value_2 at time_2, and so on. If you create a graph by **rate**, you use the value difference divided by the time difference: $(\text{value_2} - \text{value_1}) / (\text{time_2} - \text{time_1})$, $(\text{value_3} - \text{value_2}) / (\text{time_3} - \text{time_2})$, and so on.

If you specify **difference**, you use the increase from the previous value to the new value: value_2-value_1, value_3-value_2, and so on.

If you specify **raw value**, you use the value only: value_1, value_2, and so on. The raw values are generally counters of content such as bytes or packets. They can only increase, not decrease
 - **Interface** — Use the drop-down list to select the interface to graph data for.
 - **Policy** — (If you select a Policy counter) Use the drop-down list to select a policy from your Firebox configuration to graph data for. You can update the policy list that appears in the Performance Console when you click the **Refresh Policy List** button.
 - **Peer IP** — (If you select a VPN Peers counter) Use the drop-down list to select the IP address of a VPN endpoint to graph data for. You can update the list of VPN endpoints that appears in the Performance Console when you click the **Refresh Peer IP List** button.
 - **Tunnel ID** — (If you select a Tunnels counter) Use the drop-down list to select the name of a VPN tunnel to graph data for. You can update the list of VPN tunnels that appears in the Performance Console when you click the **Refresh Tunnel ID List** button. If you do not know the tunnel ID for your VPN tunnel, check the Firebox System Manager **Front Panel** tab.
7. Select the **Save Chart Data to File** check box to save the data collected by the Performance Console to an XML data file or a comma-separated data file.

For example, you can open an XML data file in Microsoft Excel to see the counter value recorded for each polling interval. You can use other tools to merge data from more than one chart.

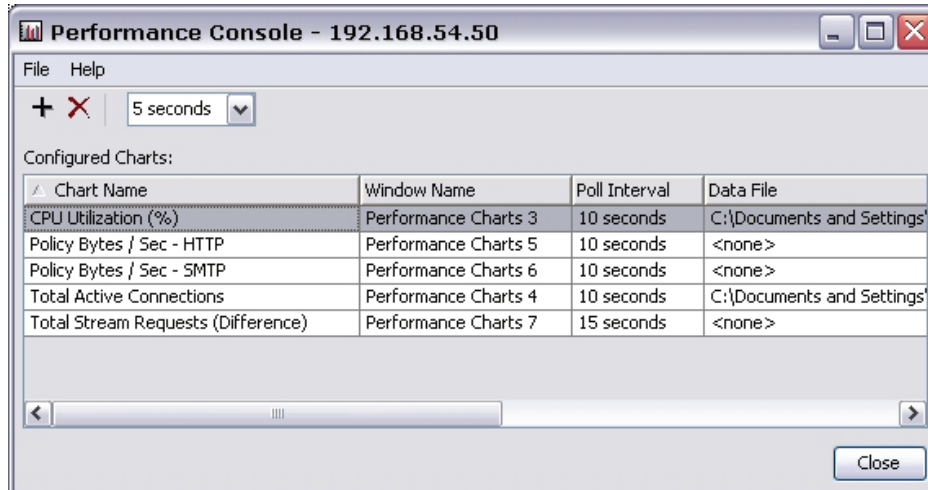
8. Click **OK** to start a real-time graph of this counter.
Graphs are shown in a real-time chart window. You can show one graph in each window, or show many graphs in one window. Graphs automatically scale to fit the data and refresh every 5 seconds.



This performance graph shows CPU usage. You create graphs for other functions in the same way.

Add charts or change polling intervals

The main Performance Console window shows a table with all configured and active performance counters. From this window, you can add a new chart or change the polling intervals for configured counters.



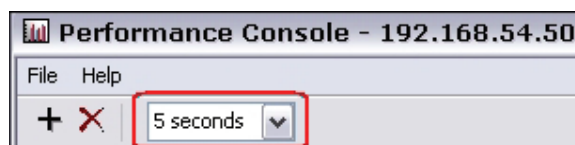
Add a new chart

To add a new chart, click the + button on the Performance Console toolbar or select **File > Add Chart**.



Change the polling interval

To change the polling interval for one performance console, select the chart name from the list. Use the polling interval drop-down list on the Performance Console toolbar to change the frequency for the polls.



Delete a chart

To delete a chart, select the chart name from the list and use the X button on the Performance Console toolbar or select **File > Delete Chart**.



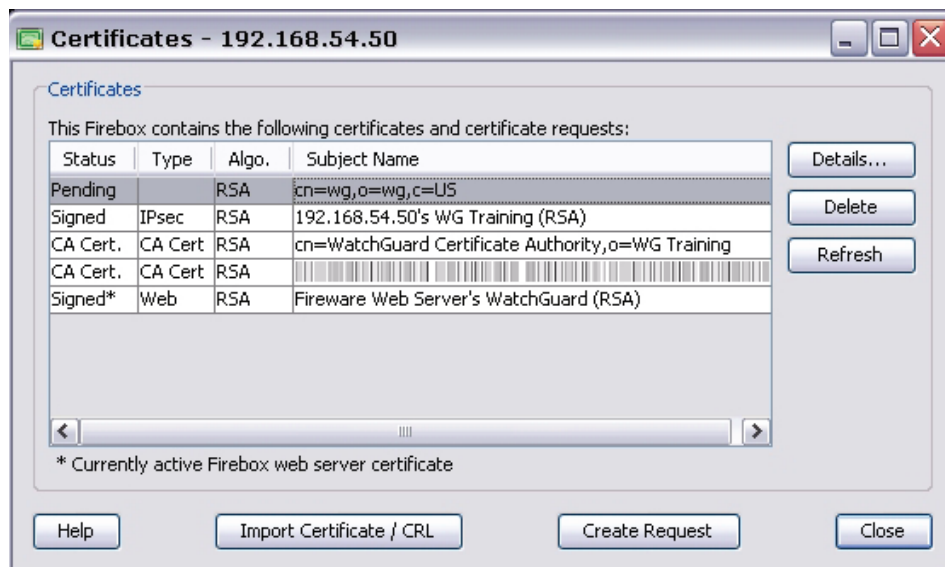
See and manage Firebox certificates

You can do the following from Firebox System Manager:

- See a list of the current Firebox certificates and details on any of them.
- Remove a certificate from the Firebox.
- Make a certificate request.
- Import a third-party CA certificate and store it in the certificate trust list.

See current certificates

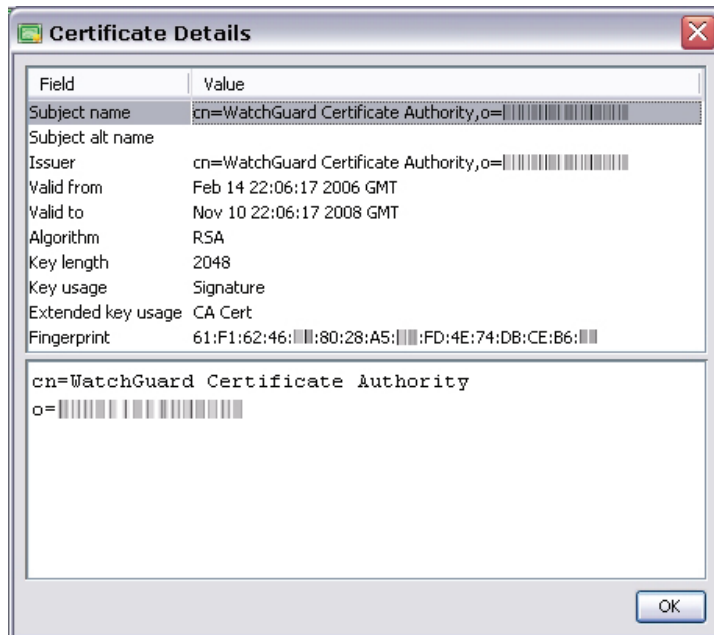
To see the current list of certificates, from Firebox System Manager, select **View > Certificates**.



In this window, you can see a list of all certificates and certificate signing requests (CSRs). The list includes this information:

- The status and type of the certificate. The certificate marked with an asterisk is the currently active Firebox web server certificate.
For more information on options for the web server certificate, see [Firebox authentication](#).
- The algorithm used by the certificate.
- The subject name or identifier of the certificate.

To see additional information on a certificate in the list, select the certificate and click **Details**.



The **Certificate Details** window includes information about which CA signed the certificate and the certificate fingerprint. Use this information to troubleshoot or uniquely identify certificates.

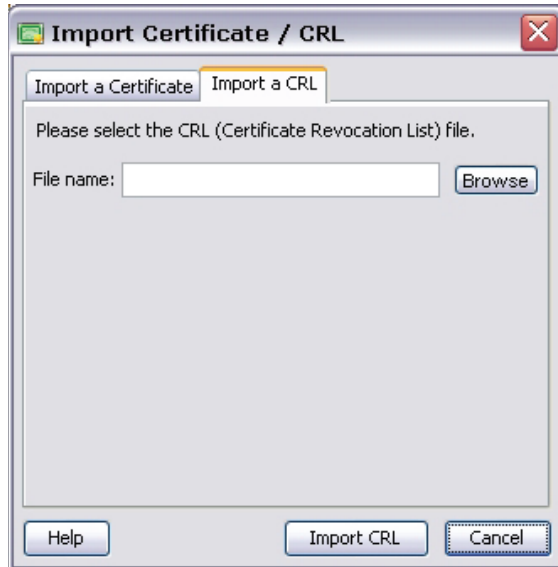
Delete a certificate

To remove a certificate from the Firebox, select the certificate in the **Certificates** dialog box and click **Delete**. You must provide the Firebox configuration (read/write) passphrase to remove a certificate. Certificates you delete can no longer be used for authentication.

Import a CRL from a file

You can import a certificate revocation list (CRL) from a file on your local computer. This is useful when you must restore a Firebox from a backup.

1. From Firebox System Manager, select **View > Certificates**.
2. From the **Certificate** dialog box, click **Import Certificate/CRL**.
3. Click the **Import a CRL** tab. Click **Browse** to find the file.



4. Click **Import CRL**.
The Import CRL dialog box appears.
5. Type the configuration passphrase and click **OK**.
The CRL you specified is appended to the CRL on your Firebox.

Retrieve the CRL from an LDAP server

You can retrieve a CRL from an LDAP server if you have access to the server. You must have LDAP account information provided by a third-party CA service.

1. From Policy Manager, select **VPN > VPN Settings**.

The VPN Settings dialog box appears.

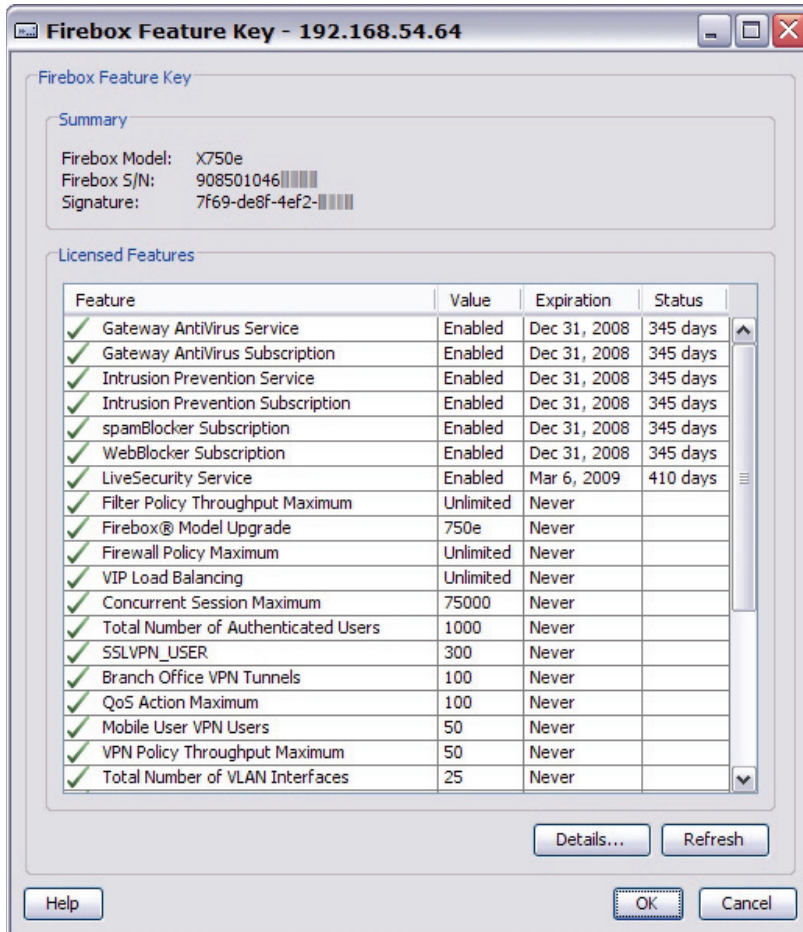
The image shows the 'VPN Settings' dialog box. It has a title bar with a close button. Inside, there are two sections. The first section, 'IPSec Settings', contains two checkboxes: 'Enable IPSec Pass-through' and 'Enable TOS for IPSec'. The second section, 'LDAP Server Settings for CRL', contains a checkbox 'Enable LDAP server for certificate verification'. Below this checkbox are two input fields: '* Server:' and 'Port:'. The 'Port:' field has a dropdown menu showing '389'. At the bottom of the dialog, there is a button labeled 'BOVPN Notification...' and three buttons: 'OK', 'Cancel', and 'Help'. A note at the bottom of the LDAP section states 'Fields marked with an asterisk '*' are required.'

2. Select the **Enable LDAP server for certificate verification** check box.
3. Enter the name or address of the LDAP server.
4. (Optional) Enter the port number.
5. Click **OK**.

Your Firebox checks the CRL stored on the LDAP server when tunnel authentication is requested.

See and synchronize feature keys

To see the feature keys that are installed on this Firebox, from Firebox System Manager, select **View > Feature Keys**.



Feature

Name of the feature, such as spamBlocker subscription.

Value

Such as number of VLAN interfaces or BOVPN tunnels allowed.

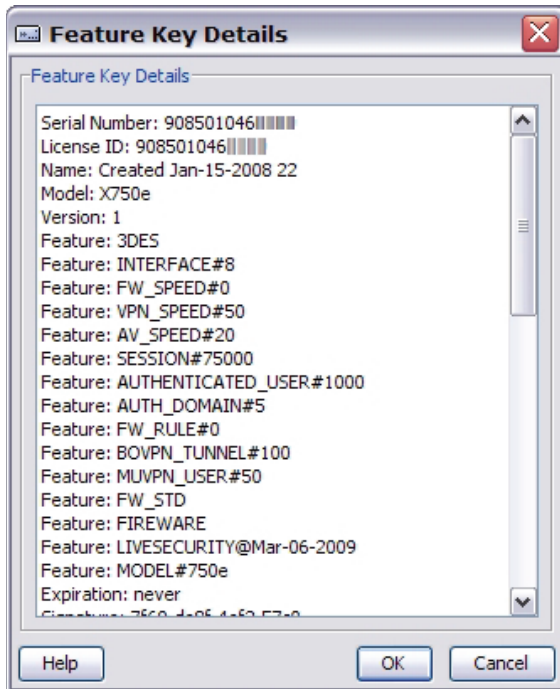
Expiration

The expiration date. If the feature does not expire, this field shows **Never**.

Status

For features with expiration dates, the number of days remaining.

You can click **Details** to see the feature key.



Synchronize feature keys

You can use Firebox System Manager to get a current feature key if you have already created a LiveSecurity user account:

1. From Firebox System Manager, select **Tools > Synchronize Feature Keys**.
2. When prompted, type the configuration passphrase for your Firebox.
The Firebox contacts the LiveSecurity web site and downloads the current feature key to your Firebox.

Communication log

The communication log contains information such as the success or failure of logins, handshakes, and so on. These are connections between the Firebox and Firebox System Manager.

To see the log, from Firebox System Manager, select **View > Communication Log**. This log starts when initial login is successful, and shows information about the current management session.

Perform operations in Firebox System Manager

Synchronize time

Use this command to synchronize the time of the Firebox with the system time.

1. From Firebox System Manager, select **Tools > Synchronize Time**.
2. Type the Firebox configuration passphrase. Click **OK**.

Clear the ARP cache

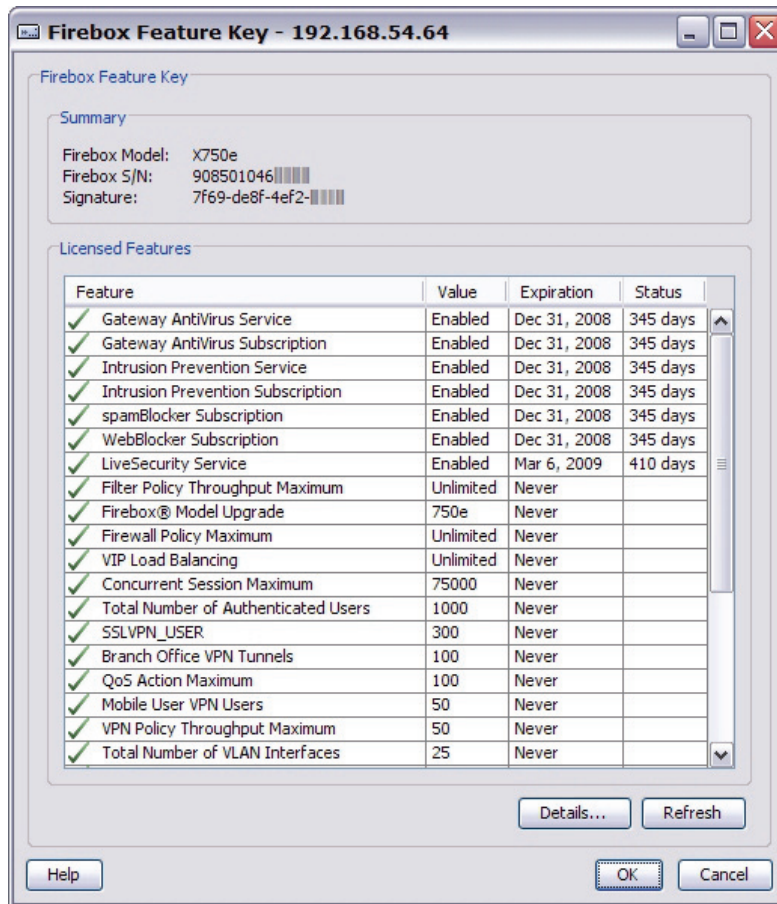
The ARP (Address Resolution Protocol) cache on the Firebox keeps the hardware addresses (also known as MAC addresses) of TCP/IP hosts. Before an ARP request starts, the system makes sure that a hardware address is in the cache. You must clear the ARP cache on the Firebox after installation when your network has a drop-in configuration.

1. From Firebox System Manager, select **Tools > Clear ARP Cache**.
2. Type the Firebox configuration passphrase. Click **OK**.
This flushes the cache entries.

When a Firebox is in drop-in mode, this procedure clears only the content of the ARP table and not the MAC table. The oldest MAC entries in the MAC table are removed if the table has more than 2000 entries. If you want to clear the MAC table, you must restart the Firebox.

See and synchronize feature keys

To see the feature keys that are installed on this Firebox, from Firebox System Manager, select **View > Feature Keys**.



Feature

Name of the feature, such as spamBlocker subscription.

Value

Such as number of VLAN interfaces or BOVPN tunnels allowed.

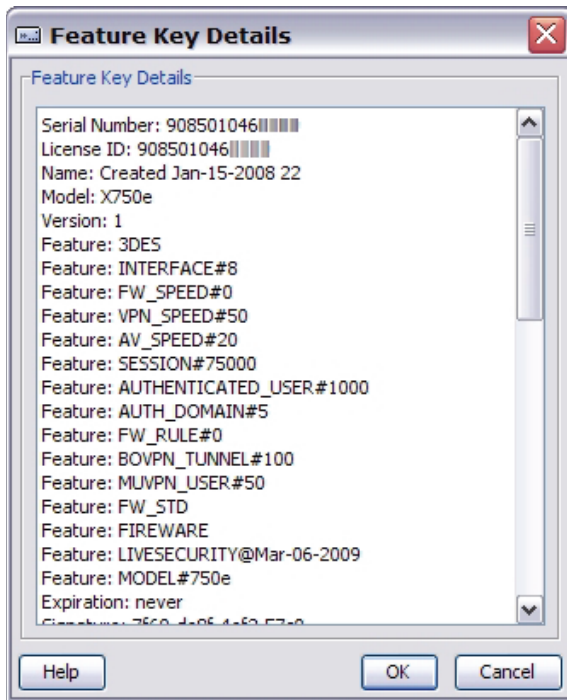
Expiration

The expiration date. If the feature does not expire, this field shows **Never**.

Status

For features with expiration dates, the number of days remaining.

You can click **Details** to see the feature key.



Synchronize feature keys

You can use Firebox System Manager to get a current feature key if you have already created a LiveSecurity user account:

1. From Firebox System Manager, select **Tools > Synchronize Feature Keys**.
2. When prompted, type the configuration passphrase for your Firebox.
The Firebox contacts the LiveSecurity web site and downloads the current feature key to your Firebox.

Clear alarms

Use this command to clear the alarm list on the Firebox.

1. From Firebox System Manager, select **Tools > Clear Alarm**.
2. Type the Firebox configuration passphrase. Click **OK**.

Rekey BOVPN tunnels

Normally, the gateway endpoints of BOVPN tunnels must generate and exchange new keys after a quantity of time or amount of traffic passes. You might sometimes, particularly when you troubleshoot tunnels, want to immediately generate new keys instead of waiting for them to expire. The rekey options in Firebox System Manager expire BOVPN tunnels immediately. Tunnels are triggered by traffic; they are rebuilt when traffic starts to flow through them. If you rekey a tunnel and it has no traffic, it is not automatically rebuilt.

To rekey one BOVPN tunnel

On the front panel of Firebox System Manager, below the **Branch Office VPN Tunnels** heading, select the tunnel you want to rekey. Right-click and select **Rekey Selected BOVPN Tunnel**. When prompted, type the configuration passphrase for the Firebox to which Firebox System Manager is connected.

To rekey all BOVPN tunnels

From Firebox System Manager, right-click anywhere on the front panel of the window. Select **Rekey All BOVPN Tunnels**. When prompted, type the configuration passphrase for the Firebox to which Firebox System Manager is connected.

or

From Firebox System Manager, select **Tools > Rekey All BOVPN Tunnels**. When prompted, type the configuration passphrase for the Firebox to which Firebox System Manager is connected.

Control High Availability

You can perform several High Availability operations from Firebox System Manager. For more information, see [Manually control High Availability](#).

Change passphrases from Firebox System Manager

To change the Firebox passphrases from Firebox System Manager, select **Tools > Change Passphrases**.

A Firebox uses two passphrases:

- Status passphrase
The read-only password or passphrase that allows access to the Firebox
- Configuration passphrase
The read-write password or passphrase that allows an administrator full access to the Firebox

To create a secure passphrase, we recommend that you:

- Use a selection of uppercase and lowercase characters, numbers, and special characters (for example, Im4e@tiN9).
- Do not use a word from standard dictionaries, even if you use it in a different sequence or in a different language.
- Do not use a name. It is easy for an attacker to find a business name, familiar name, or the name of a famous person.

An additional security measure is to change the Firebox passphrases at regular intervals. To do this, you must have the configuration passphrase.

6

Firebox Administration and Global Settings

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](#)
- [Import a feature key to the Firebox](#)

See features available with the current feature key


Your Firebox always has one currently active feature key. To see the features available with this feature key, from Policy Manager, select **Setup > Feature Keys**.

The **Firebox Feature Key** dialog box appears. This dialog box shows:

- A list of available features
- Whether the feature is enabled or disabled
- Value assigned to the feature such as the number of VLAN interfaces allowed
- Expiration date of the feature
- Current status on expiration, such as how many days remain before the feature expires

Verify feature key compliance

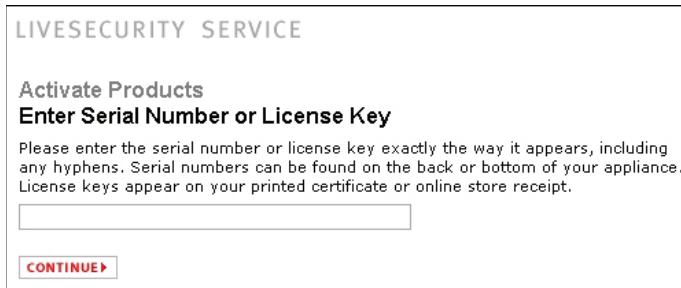
To make sure all features on your Firebox are correctly enabled on your feature key:

1. From Policy Manager, click . The **Feature Key Compliance** dialog box appears. The Description field tells you whether all Features are in compliance with the feature key.
2. If you need to get a new feature key, click **Add Feature Key**. The **Firebox Feature Key** dialog box appears. See either [Import a feature key to the Firebox](#) or [Download a feature key](#).

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.

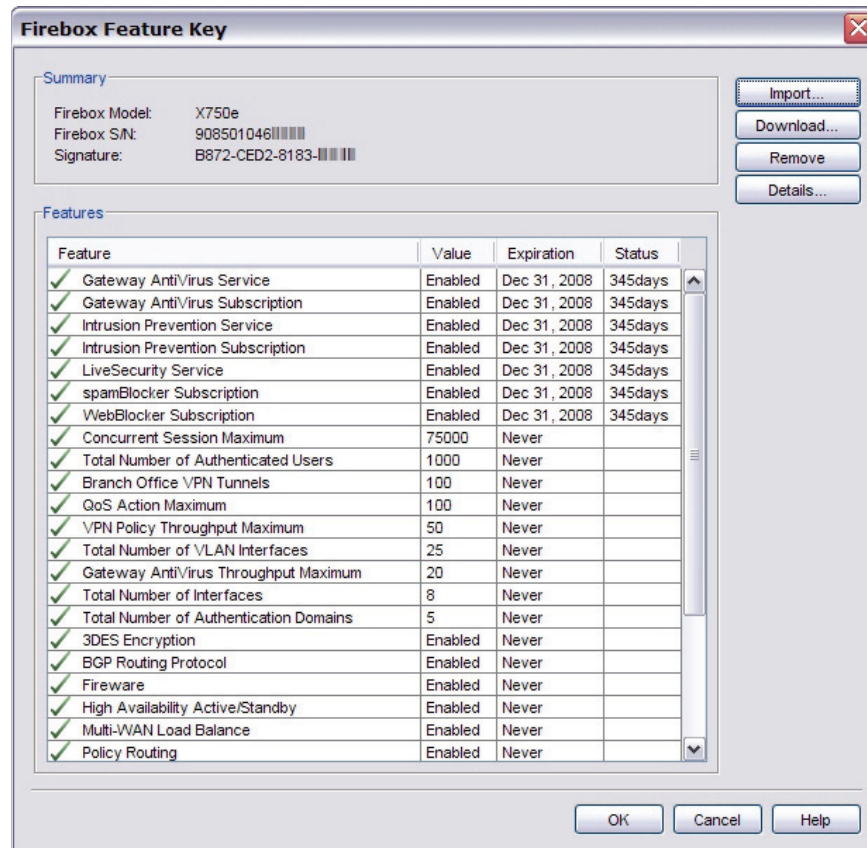


4. Click **Continue**. The Choose Product to Upgrade page appears.
5. From the drop-down list, select the Firebox to which you want to apply the upgrade or renewal. If you added a Firebox name when you registered your Firebox, that name appears in this list. After you select the Firebox, click **Activate**.
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**.

Import a feature key to the Firebox

1. From Policy Manager, select **Setup > Feature Keys**.

The **Firebox Feature Key** dialog box appears. This dialog box shows the features that are available with this feature key. It also shows whether the feature is enabled or disabled, a value assigned to the feature such as the number of VLAN interfaces allowed, the expiration date of the feature, and the current status regarding expiration.



2. Click **Remove** to remove the current feature key. You must remove the entire feature key before you install the new one that includes the feature you want to add.
3. Click **Import**.
The Import Firebox Feature Key dialog box appears.
4. Click **Browse** and find the feature key file. Or, use **Paste** to paste the contents of your feature key file into the dialog box.
5. Click **OK** to close each dialog box.
In some instances, new dialog boxes and menu commands to configure the feature appear in Policy Manager.
6. [Save the configuration file](#).
The feature key does not operate on the Firebox until you save the configuration file to the Firebox.

Remove a feature key

1. From Policy Manager, select **Setup > Feature Keys**.
The Firebox Feature Keys dialog box appears.
2. Expand **Feature Keys**, select the feature key you want to delete, and click **Remove**.
3. Click **OK**.
4. [Save the configuration file](#).

See the details of a feature key

To see the details of a feature key, from the **Firebox Feature Key** dialog box, select the feature key and click **Details**. The **Feature Key Details** dialog box shows the serial number of the Firebox to which this feature key applies, along with its ID and name, the Firebox model and version number, and the available Firebox features.



Download a feature key

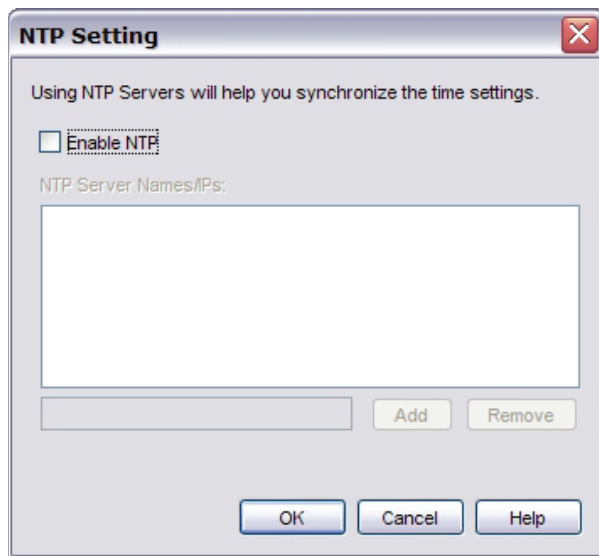
If your feature key file is not current, you can download a copy of any feature key file from the Firebox to your management station. To download feature keys from a Firebox, select the feature key and click **Download**. A dialog box appears for you to type the status passphrase of the Firebox.

Enable NTP and add NTP servers

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 use NTP, your Firebox configuration must allow DNS. DNS is allowed in the default configuration by the Outgoing policy. You must also configure DNS servers for the external interface before you configure NTP. For information on how to these addresses, see [Add WINS and DNS server addresses](#).

1. From Policy Manager, select **Setup > NTP**.
The NTP Setting dialog box appears.



2. Select the **Enable NTP** check box.
3. In the box below the **NTP Server Names/IPs** list, type the IP addresses of the NTP server you want to use. Click **Add**.
The Firebox can use up to three NTP servers.
4. Click **OK**.

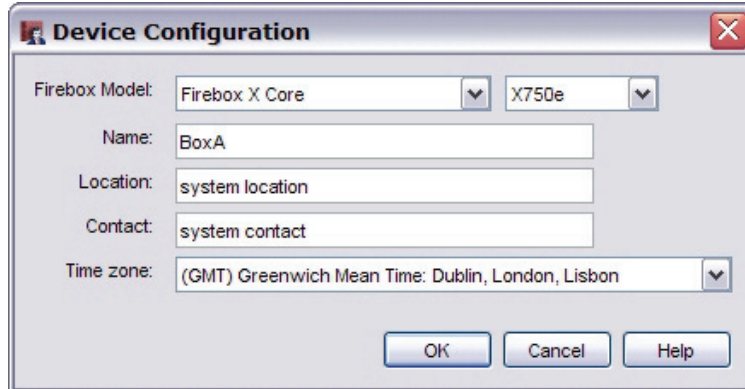
Assign a friendly name

You can give the Firebox a friendly name to use in your log files and reports. Otherwise, the log files and reports use the IP address of the Firebox external interface. Many customers use a Fully Qualified Domain Name if they register such a name with the DNS system. You must give the Firebox a friendly name if you use the Management Server to configure VPN tunnels and certificates.

1. From Policy Manager, click **Setup > System**.
The Device Configuration dialog box appears.
2. If necessary, use the drop-down lists to specify Firebox X Core or Firebox X Peak and the model number.
3. In the **Name** text box, type the friendly name you want for the Firebox. Click **OK**. A pop-up notification tells you if you use characters that are not allowed.
4. In the **Location** and **Contact** fields, type any information that could be helpful to identify and maintain the Firebox.

Set the time zone and basic device properties

1. [Open Policy Manager](#). Click **Setup > System**. The **Device Configuration** dialog box appears.
2. From the **Time zone** drop-down list, select the time zone for the physical location of the Firebox. Click **OK**.



You normally use this dialog box only to set the Firebox time zone. This setting controls the date and time that appear in the log file and on tools such as LogViewer, WatchGuard Reports, and WebBlocker. The Firebox system time is set to Greenwich Mean Time (GMT) by default.

Other fields on this dialog box are;

Firebox model

The first drop-down lists specify Firebox X Core or Firebox X Peak and the model number, as determined by Quick Setup Wizard. You normally do not need to change these settings. If you add a new feature key to the Firebox, these fields are automatically updated.

Name, Location, Contact

These fields are filled in by the Quick Setup Wizard if you entered this information there. This information appears on the **Front Panel** tab of Firebox System Manager.

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 supports SNMPV1, SNMPV2, 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.

To enable SNMP polling, see [Enable SNMP polling](#).

SNMP traps and inform requests

A SNMP trap is an event notification the Firebox sends to the SNMP management system. The trap identifies when a specific condition occurs, such as a value that is more than its predefined threshold. You can make the Firebox send a trap for any policy in Policy Manager.

An SNMP inform request is similar to a trap, but the receiver sends a response to them. If the Firebox does not get a response, it sends the inform request again until the SNMP manager sends a response. A trap is sent only once, and the receiver does not send any acknowledgement when it gets the trap.

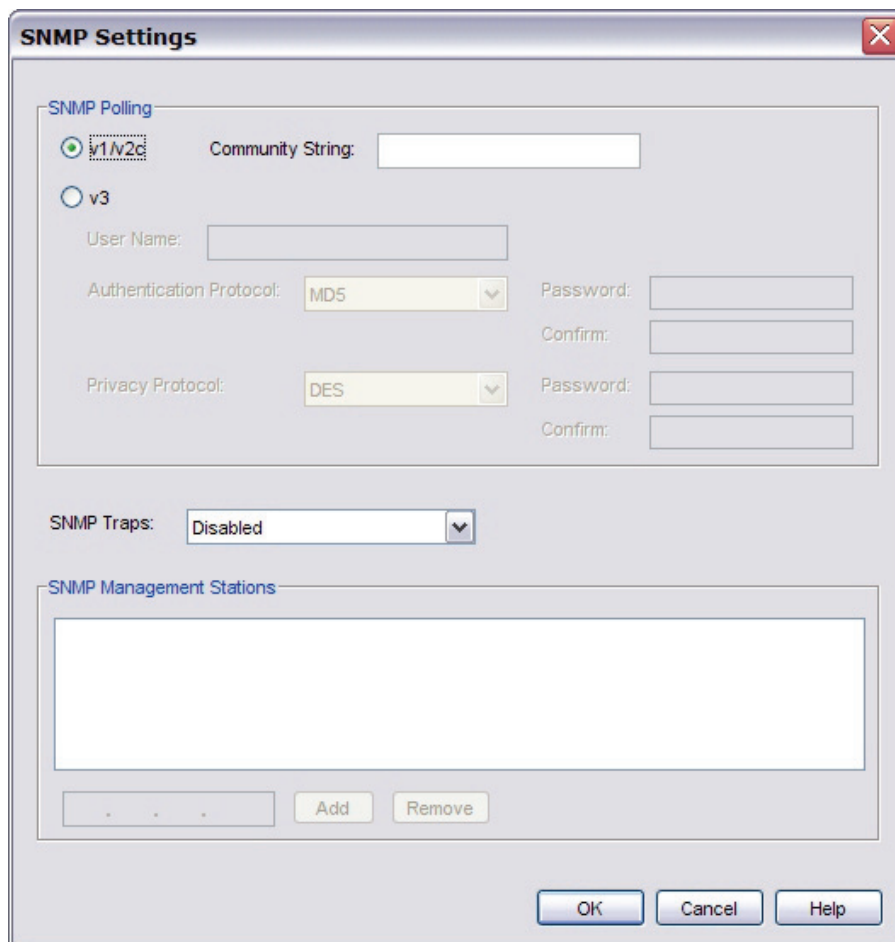
An inform request is more reliable than a trap because the Firebox knows whether it was received. However, inform requests consume more resources. They are held in memory until the sender gets a response. If an inform request must be sent more than once, the retries increase traffic. We recommend you consider whether your need to receive every SNMP notification is worth the use of memory in the router and increase in network traffic.

To enable SNMP inform requests, you must use SNMPV2 or SNMPv3. SNMPv1 supports only traps, not inform requests.

To enable SNMP traps or inform requests, see [Enable SNMP traps or inform requests](#).

Enable SNMP polling

1. From Policy Manager, select **Setup > SNMP**.



The image shows the 'SNMP Settings' dialog box. It has a title bar with a close button. Inside, there's a section titled 'SNMP Polling' with two radio buttons: 'v1/v2c' (selected) and 'v3'. Below 'v1/v2c' is a 'Community String' text field. Below 'v3' are fields for 'User Name', 'Authentication Protocol' (MD5), 'Password', 'Confirm', 'Privacy Protocol' (DES), 'Password', and 'Confirm'. Below this is a 'SNMP Traps' dropdown menu set to 'Disabled'. At the bottom is a section titled 'SNMP Management Stations' with a large empty list box and 'Add' and 'Remove' buttons. At the very bottom are 'OK', 'Cancel', and 'Help' buttons.

2. Select the version of SNMP you want to use: **v1/v2c** or **v3**.

If you chose **v1/v2c**:

type the **Community String** the Firebox must use when it connects to the SNMP server. Click **OK**.

If you chose **v3**:

User Name: Type the user name for SNMPv3 authentication and privacy protection.

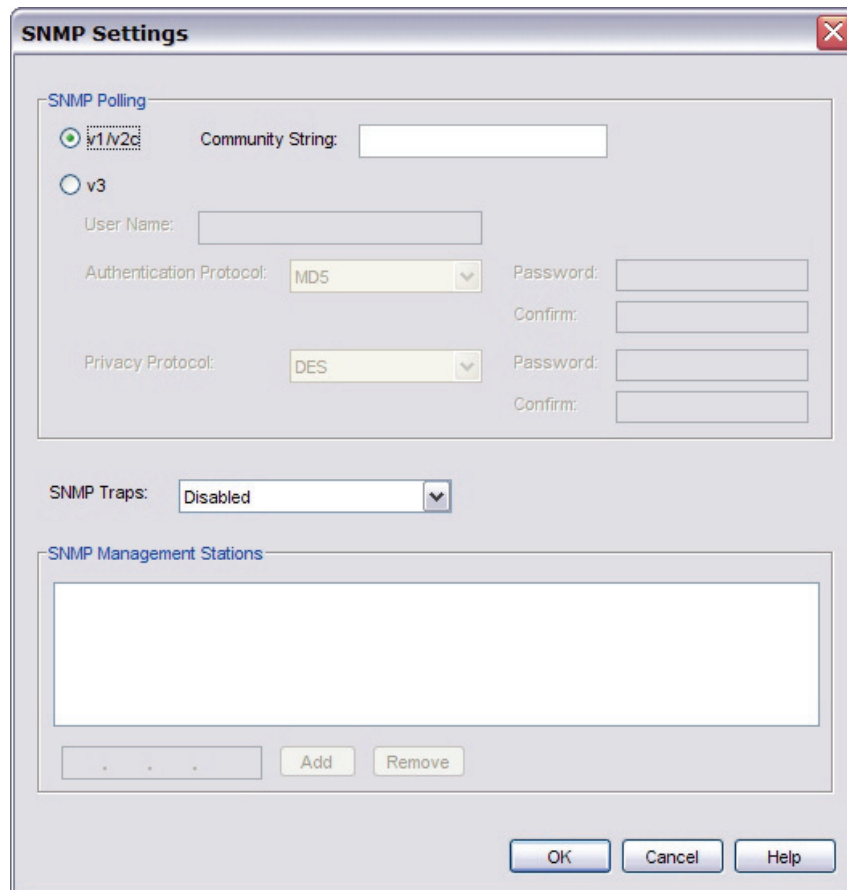
- **Authentication Protocol:** Select Message Digest 5 (MD5) or Secure Hash Algorithm (SHA).
- **Authentication Password:** Type the authentication password.
- **Privacy Protocol:** Select Data Encryption Standard (DES).
- **Privacy Password:** Enter a password to encrypt outgoing messages and decrypt incoming messages.

To make the Firebox able to receive SNMP polls, you must add an SNMP policy to the Firebox.

1. From Policy Manager, select **Edit > Add Policy** (or click the + icon), expand **Packet Filters**, select **SNMP**, and click **Add**.
The New Policy Properties dialog box appears.
2. Below the **From** box, click **Add**. From the **Add Address** dialog box that appears, click **Add Other**.
The Add Member dialog box appears.
3. From the **Choose Type** drop-down list, select **Host IP**. In the **Value** field, type the IP address of your SNMP server computer.
4. Click **OK** twice to return to the **Policy** tab of the new policy.
5. Below the **To** box, click **Add**.
6. From the **Add Address** dialog box that appears, under **Available Members**, select **Firebox**. Click **Add**.
7. Click **OK**, **OK**, and **Close**. [Save the configuration file](#). The Firebox can now receive SNMP polls.

Enable SNMP traps or inform requests

1. From Policy Manager, select **Setup > SNMP**.



The image shows the 'SNMP Settings' dialog box. It has a title bar with a close button. The main area is divided into three sections: 'SNMP Polling', 'SNMP Traps', and 'SNMP Management Stations'. In the 'SNMP Polling' section, there are radio buttons for 'v1/v2c' (selected) and 'v3'. Below 'v1/v2c' is a 'Community String' text field. Below 'v3' are fields for 'User Name', 'Authentication Protocol' (set to 'MD5'), 'Password', 'Confirm', 'Privacy Protocol' (set to 'DES'), and another 'Password' and 'Confirm' pair. In the 'SNMP Traps' section, there is a dropdown menu currently set to 'Disabled'. The 'SNMP Management Stations' section contains a large empty list box with 'Add' and 'Remove' buttons below it. At the bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons.

2. In the **SNMP Traps** drop-down list, select the version of trap or inform you want to use. (SNMPv1 supports only traps, not inform requests.)
3. Type the IP address of your SNMP management station. Click **Add**. Repeat if you want to add more SNMP management stations. Click **OK**.

To make the Firebox able to send SNMP traps and informs, you must add an SNMP policy to the Firebox.

1. From Policy Manager, select **Edit > Add Policy** (or click the + icon), expand **Packet Filters**, select **SNMP**, and click **Add**.
The New Policy Properties dialog box appears.
2. Below the **From** box, click **Add**. From the **Add Address** dialog box that appears, click **Add Other**.
The Add Member dialog box appears.
3. From the **Choose Type** drop-down list, select **Host IP**. In the **Value** field, type the IP address of your SNMP server computer.
4. Click **OK** twice to return to the **Policy** tab of the new policy.
5. Below the **To** box, click **Add**.
6. From the **Add Address** dialog box that appears, under **Available Members**, select **Firebox**. Click **Add**.
7. Click **OK, OK**, and **Close**. Save the configuration to the Firebox.

Make the Firebox send a trap for a policy

You can make the Firebox send an SNMP trap for any policy.

1. Double-click the policy icon shown in Policy Manager to edit the configuration.
2. From the **Edit Policy Properties** dialog box, select the **Properties** tab.
3. Click **Logging** and select the **Send SNMP Trap** check box.

About Management Information Bases (MIBs)

WatchGuard System Manager with Fireware appliance software supports two types of Management Information Bases (MIBs):

- Public MIBs are used in the Fireware product and are copied on to your WatchGuard management station when you install Fireware. These MIBs include IETF standards and MIB2.
- Private MIBs are MIBs created by WatchGuard to provide basic monitoring information for specific components in the Firebox, including CPU and memory utilization, and interface and IPSec metrics.

When you install WatchGuard System Manager, MIBs are installed to My Documents\My WatchGuard\Shared WatchGuard\SNMP.

Change Firebox passphrases

A Firebox uses two passphrases:

- Status passphrase
The read-only password or passphrase that allows access to the Firebox
- Configuration passphrase
The read-write password or passphrase that allows an administrator full access to the Firebox

To create a secure passphrase, we recommend that you:

- Use a selection of uppercase and lowercase characters, numbers, and special characters (for example, Im4e@tiN9).
- Do not use a word from standard dictionaries, even if you use it in a different sequence or in a different language.
- Do not use a name. It is easy for an attacker to find a business name, familiar name, or the name of a famous person.

An additional security measure is to change the Firebox passphrases at regular intervals. To do this, you must have the configuration passphrase.

1. From Policy Manager, open the configuration file on the Firebox.
2. Click **File > Change Passphrases**.
The Change Passphrases dialog box appears.

3. From the **Firebox Address or Name** drop-down list, select a Firebox or type the IP address or name of the Firebox. Type the Firebox configuration (read/write) passphrase.
4. Type and confirm the new status (read-only) and configuration (read/write) passphrases. The status passphrase must be different from the configuration passphrase.
5. Click **OK**.

About aliases

An alias is a shortcut that identifies a group of hosts, networks, or interfaces. When you use an alias, it is easy to create a security policy because the Firebox allows you to use aliases when you create policies.

The default aliases in Policy Manager that you can use are:

- Aliases that correspond to Firebox interfaces, such as Trusted or External
- Any-Trusted: An alias for all Firebox interfaces configured as trusted interfaces (as defined in Policy Manager: select **Network > Configuration**), and any network you can get access to through these interfaces.
- Any-External: An alias for all Firebox interfaces of type external (as defined in Policy Manager: select **Network > Configuration**), and any network you can get access to through these interfaces.
- Any-Optional: Aliases for all Firebox interfaces of type optional (as defined in Policy Manager: select **Network > Configuration**), and any network you can get access to through these interfaces.
- Any-BOVPN: An alias for any BOVPN (IPSec) tunnel. When you use the BOVPN Policy wizard to create a policy to allow traffic through a BOVPN tunnel, the wizard automatically creates .in and .out aliases for the incoming and outgoing tunnels.

Alias names are different from user or group names used in user authentication. With user authentication, you can monitor a connection with a name and not as an IP address. The person authenticates with a user name and a password to get access to Internet protocols. For more information about user authentication, see [About user authentication](#).

Alias members

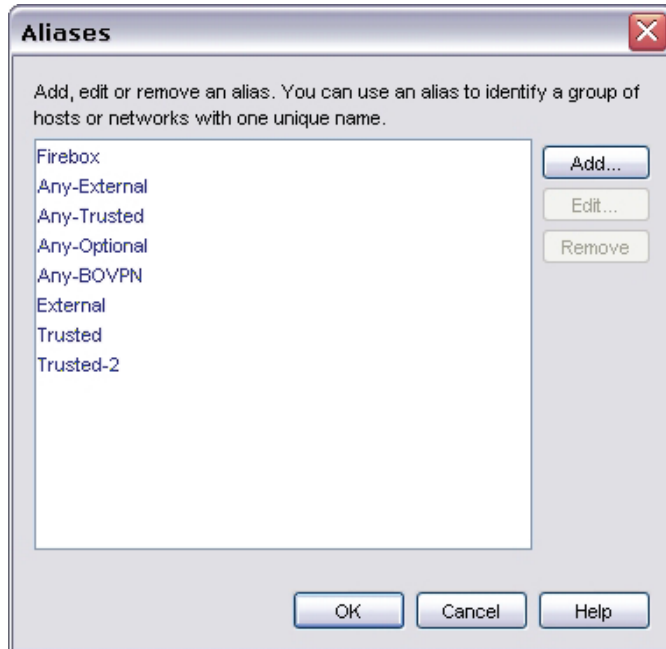
You can add the following to an alias:

- Host IP
- Network IP
- A range of host IP addresses
- DNS name for a host
- Tunnel address: defined by a user or group, address, and name of the tunnel
- Custom address: defined by a user or group, address, and Firebox interface
- Another alias
- An authorized user or group

Create an alias

1. From Policy Manager, select **Setup > Aliases**.

The Aliases dialog box appears. Pre-defined aliases appear in blue and user-defined aliases appear in black.



2. Click **Add**.

The Add Alias dialog box appears.



3. In the **Alias Name** text box, type a unique name to identify the alias.
This name appears in lists when you configure a security policy.
4. In the **Description** field, type a description of the alias.

If you want to add an address, address range, DNS name, or another alias to the alias

1. From the **Add Alias** dialog box, click **Add**.
The Add Member dialog box appears.
2. From the drop-down list, select the type of member you want to add.
3. In the **Value** text field, type the address or name. Click **OK**.
The new member appears in the Alias Members section of the Add Alias dialog box.
4. Repeat steps 1–3 to add more members as needed. Or, use the next procedure to add users or groups. When you have all the users, groups, and members you want in the alias, in the **Add Alias** dialog box, click **OK**.

If you want to add an authorized user or group to the alias

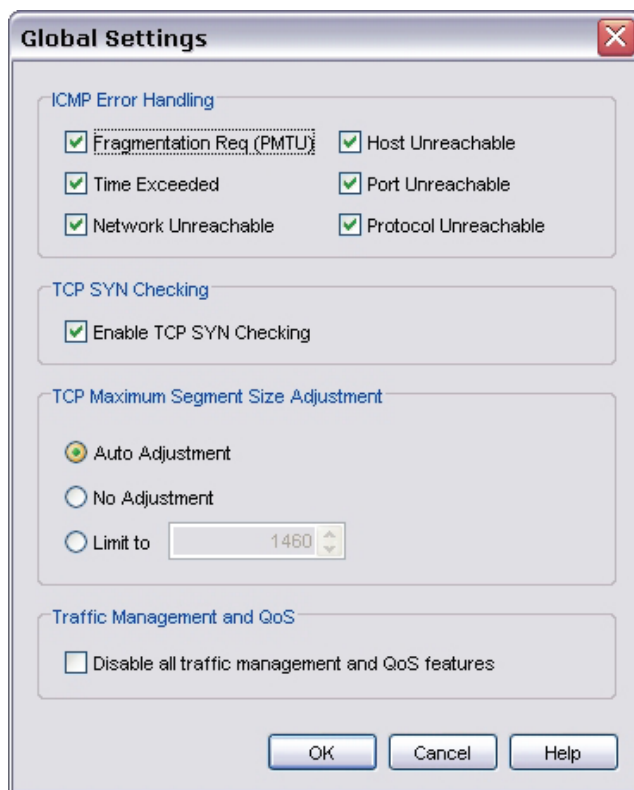
1. Click **User**.
The Add Authorized Users or Groups dialog box appears.
2. From the **Type** drop-down list, select whether the user or group you want to add is authorized as a Firewall user, a PPTP user, or an SSL VPN user.
3. From the drop-down list to the far right of the **Type** box, select **User** if you want to add a user, or **Group** if you want to add a group.
4. If the user or group appears in the list at the bottom of the **Add Authorized Users or Groups** dialog box, select the user or group and click **Select**.
If the user or group does not appear in the list, it is not yet defined as an authorized user or group. You must define it as an authorized user or group before you add it to an alias. For information on how to do this, see [Define a new user for Firebox authentication](#), [Define a new group for Firebox authentication](#), or [Use authorized users and groups in policies](#).
5. Repeat steps 1 - 4 to add more members as needed. Or, use the previous procedure to add an address, address range, DNS name, or another alias to the alias. When you have all the users, groups, and members you want in the alias, in the **Add Alias** dialog box, click **OK**.

Define Firebox global settings

In Policy Manager you can select settings that control the actions of many Firebox features. You set basic parameters for:

- ICMP error handling
- TCP SYN checking
- TCP maximum size adjustment
- Traffic management and QoS

1. From Policy Manager, select **Setup > Global Settings**.
The Global Settings dialog box appears.
2. Configure the different categories of global settings as shown in the sections below.



Define ICMP error handling global settings

Internet Control Message Protocol (ICMP) controls errors during connections. It is used for two types of operations:

- To tell client hosts about error conditions.
- To probe a network to find general characteristics about the network.

The Firebox sends an ICMP error message each time an event occurs that matches one of the parameters you selected. These messages are good troubleshooting tools, but can also decrease security by exposing information about your network. If you deny these ICMP messages, you can increase security by preventing network probes, but this can also cause timeout delays for incomplete connections, which can cause application problems. The global ICMP error handling parameters and their descriptions are:

Fragmentation Req (PMTU)

Select this check box to allow ICMP Fragmentation Req messages. The Firebox uses these messages to find the MTU path.

Time Exceeded

Select this check box to allow ICMP Time Exceeded messages. A router usually sends these messages when a route loop occurs.

Network Unreachable

Select this check box to allow ICMP Network Unreachable messages. A router usually sends these messages when a network link is broken.

Host Unreachable

Select this check box to allow ICMP Host Unreachable messages. Your network usually sends these messages when it cannot use a host or service.

Port Unreachable

Select this check box to allow ICMP Port Unreachable messages. A host or firewall usually sends these messages when a network service is not available or is not allowed.

Protocol Unreachable

Select this check box to allow ICMP Protocol Unreachable messages.

You can override the global ICMP settings for a policy:

1. On the **Advanced** tab of the **New/Edit Policy Properties** dialog box, from the **ICMP Error Handling** drop-down list, select **Specify setting**.
2. Click **ICMP Setting**.
3. From the **ICMP Error Handling Settings** dialog box, use the check boxes to indicate the settings you want. Click **OK**.

Enable TCP SYN checking

TCP SYN checking makes sure that the TCP three-way handshake is done before the Firebox allows a data connection.

Defining TCP maximum segment size adjustment global settings

The TCP segment can be set to a specified size for a connection that must have more TCP/IP layer 3 overhead (such as PPPoE, ESP, AH, and so on). If this size is not correctly configured, users cannot get access to some web sites. The global TCP maximum segment size adjustment settings are:

Auto Adjustment

The Firebox examines all maximum segment size (MSS) negotiations and changes the MSS value to the applicable one.

No Adjustment

The Firebox does not change the MSS value.

Limit to

You set a size adjustment limit.

Disable Traffic Management and QoS

To disable these features, select the **Disable all traffic management and QoS features** check box. You might want to disable these features if you do performance testing or network debugging.

About global VPN settings

You can select settings that apply to manual BOVPN tunnels, managed BOVPN tunnels, and Mobile VPN with IPSec tunnels:

1. From Policy Manager, select **VPN > VPN Settings**.
The VPN Settings dialog box appears.
2. Consider the settings explained below for your VPN tunnels.

Enable IPSec Pass-through

For a user to make IPSec connections to a Firebox behind a different Firebox, you must keep the **Enable IPSec Pass-through** check box selected to enable the IPSec pass-through feature. For example, if mobile employees are at a customer location that has a Firebox, they can use IPSec to make IPSec connections to their network. For the local Firebox to correctly allow the outgoing IPSec connection, you must also add an IPSec policy to Policy Manager.

When you specify or define a Phase 2 proposal and plan to use the IPSec pass-through feature, you must specify ESP (Encapsulating Security Payload) as the proposal method. IPSec pass-through supports ESP but not AH (Authentication Header). For information on how to define a Phase 2 proposal, see [Add a Phase 2 proposal](#).

When you enable IPSec pass-through, a policy called WatchGuard IPSec is automatically added to Policy Manager. The policy allows traffic from Any-Trusted and Any-Optional, and the destination is set to Any. When you disable IPSec pass-through, the WatchGuard IPSec policy is automatically deleted.

Enable TOS for IPSec

The Type of Service (TOS) bits are a set of four-bit flags in the IP header that can tell routing devices to give an IP datagram more or less priority than other datagrams. Fireware gives you the option to allow IPSec tunnels to clear or maintain the settings on TOS-flagged packets. Some ISPs drop all packets that have TOS flags set.

If you do not select the **Enable TOS for IPSec** check box, all IPSec packets have no TOS bits set. If the TOS bits were set before, when Fireware encapsulates the packet in an IPSec header, the TOS bits are cleared.

When the **Enable TOS for IPSec** check box is selected, if the original packet has TOS bits set, then Fireware keeps the TOS bits set when it encapsulates the packet in an IPSec header. If the original packet does not have the TOS bits set, Fireware does not set the TOS bits when it encapsulates the packet in an IPSec header.

Consider the setting of this check box if you want to apply QoS marking to IPsec traffic. QoS marking can involve the setting of the TOS bit. For more information on QoS marking, see [About QoS Marking](#).

Enable LDAP server for certificate verification

When you create a VPN gateway, you specify a credential method for the two VPN endpoints to use when the tunnel is created. If you choose to use an IPSec Firebox certificate, you can identify an LDAP server to use to validate the certificate. Type the IP address for the LDAP server. You can also specify a port if you want to use a port other than 389.

BOVPN Notification

Click to configure the Firebox to send a notification when a BOVPN tunnel is down. A dialog box appears for you to set parameters for the notification. For information on the fields in this dialog box, see [Set logging and notification preferences](#).

This setting does not apply to Mobile VPN with IPSec tunnels.

Create schedules for Firebox actions

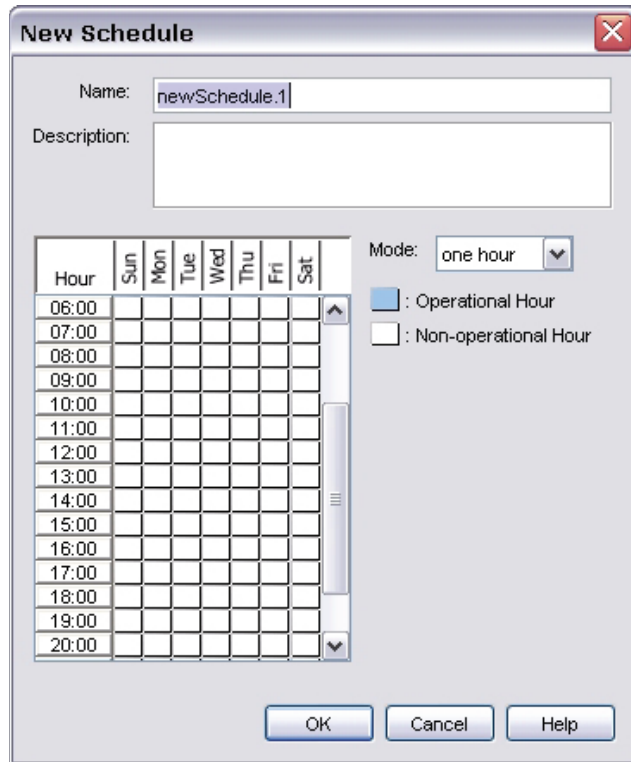
You can use schedules to automate some Firebox actions such as WebBlocker tasks. You can create a schedule for all days of the week, or create a different schedule for each day of the week. You can then use these schedules in policies that you create. For information on how to use schedules in policies, see [Set an operating schedule](#).

1. From Policy Manager, select **Setup > Actions > Schedules**.
The Schedules dialog box appears.



2. Click **Add**.

The New Schedule dialog box appears.



The 'New Schedule' dialog box contains the following elements:

- Name:** A text field containing 'newSchedule.1'.
- Description:** An empty text area.
- Mode:** A drop-down menu set to 'one hour'.
- Legend:**
 - ☒ : Operational Hour
 - ☐ : Non-operational Hour
- Chart:** A grid with days of the week (Sun-Sat) as columns and hours (06:00-20:00) as rows. All cells are currently empty.
- Buttons:** OK, Cancel, and Help.

3. Type a schedule name and description. The schedule name appears in the **Schedules** dialog box. *Make sure that the name is easy to remember.*
4. From the **Mode** drop-down list, select the time increment for the schedule: one hour, 30 minutes, or 15 minutes. *The chart on the left of the New Schedule dialog box shows your entry in the drop-down list.*
5. The chart in the dialog box shows days of the week along the x-axis (horizontal) and increments of the day on the y-axis (vertical). Click boxes in the chart to change them between operational hours (when the policy is active) and non-operational hours (when the policy is not in effect).
6. Click **OK** to close the **New Schedule** dialog box. Click **Close** to close the **Schedules** dialog box.

To edit a schedule, select the schedule name in the **Schedule** dialog box and click **Edit**.

To create a new schedule from an existing one, select the schedule name and click **Clone**.

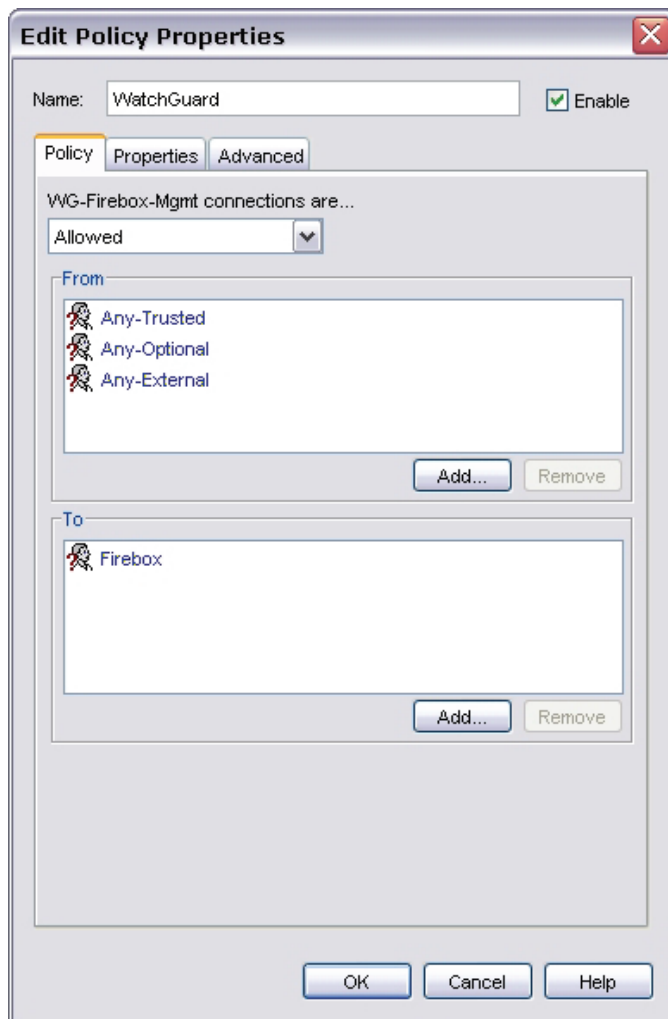
Manage a Firebox from a remote location

When you configure a Firebox with the Quick Setup Wizard, a policy called the WatchGuard policy is created automatically. This policy allows you to connect to and administer the Firebox from any computer on the trusted or optional networks. If you want to manage the Firebox from a remote location (any location external to the Firebox), then you must modify the WatchGuard policy to allow administrative connections from the IP address of your remote location.

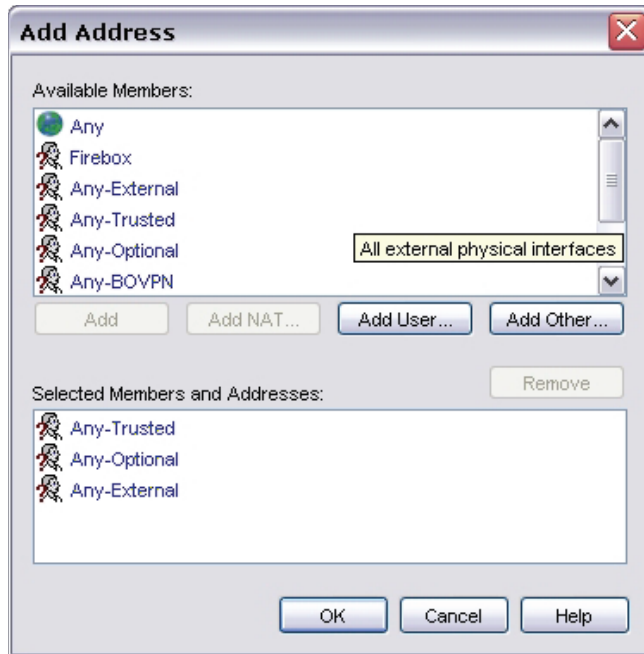
The WatchGuard policy controls access to the Firebox on these four TCP ports: 4103, 4105, 4117, 4118. When you allow connections in the WatchGuard policy, you allow connections to each of these four ports.

Before you modify the WatchGuard policy, we recommend that you consider connecting to the Firebox with a VPN. This greatly increases the security of the connection. If this is not possible, we recommend that you allow access from the external network to only certain authorized users and to the smallest number of computers possible. For example, your configuration is more secure if you allow connections from a single computer instead of from the alias Any-External.

1. From Policy Manager, double-click the **WatchGuard** policy.
You can also right-click the WatchGuard policy and select Edit. The Edit Policy Properties dialog box appears.



2. Below the **From** list, click **Add**.
The Add Address dialog box appears.



3. Enter the IP address of the external computer that will connect to the Firebox: click **Add Other**, make sure **Host IP** is the selected type, and type the IP address.
4. If you want to give access to an authorized user, from the **Add Address** dialog box, click **Add User**. The **Add Authorized Users or Groups** dialog box appears. For information on how to use this dialog box, see the "If you want to add an authorized user or group to the alias" section in [Create an alias](#).

7

Configuration Files

About Firebox configuration files

A Firebox *configuration file* includes all configuration data, options, IP addresses, and other information that makes up your Firebox security policy. Configuration files have the extension .xml.

Policy Manager for Fireware or Fireware Pro is a WatchGuard software tool that lets you make, change, and save configuration files. When you use the Policy Manager user interface on your computer screen, you see a version of your configuration file that is easy to examine and change.


When you work with Policy Manager, you can:


- [Open a configuration file](#), either the configuration file currently in use on the Firebox, or a local configuration file (a configuration file saved on your hard drive but not currently in use on the Firebox)
- [Make a new configuration file](#)
- [Save a configuration file](#)
- Make changes to existing configuration files, as described in topics throughout this Help file.

Open a configuration file

Network administrators often need to make changes to their network's security policy. Perhaps, for example, your company purchased a new software application, and you must open a port and protocol to a server at a vendor location. Your company might have also purchased a new feature for the Firebox or hired a new employee who needs access to network resources. For all of these tasks, and many more, you must open your configuration file, use Policy Manager to modify it, and then save the configuration file.

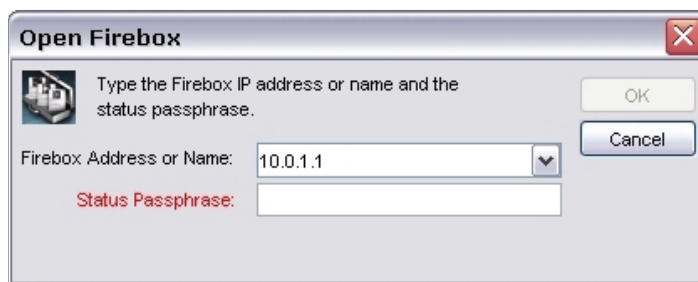
Open the configuration file with WatchGuard System Manager

1. From the Windows desktop, select **Start > All Programs > WatchGuard System Manager 10 > WatchGuard System Manager**. WatchGuard System Manager 10 is the default name of the folder for the Start menu icons. You cannot change this folder name during installation, but you can change it through the Windows user interface if you want.
2. Click .
Or, select **File > Connect To Device**.
The Connect to Firebox dialog box appears.

3. Use the drop-down list to select your Firebox or type its trusted IP address. Type the status (read-only) passphrase. Click **OK**.
The device appears in the WatchGuard System Manager Device Status tab.
4. Select the Firebox on the **Device Status** tab. Then, click .
Or, select **Tools > Policy Manager**.
Policy Manager opens, and it shows the configuration file in use on the selected Firebox. No changes you make to the configuration take effect until you save the configuration to the Firebox.

Open the configuration file with Policy Manager

1. From Policy Manager, click **File > Open > Firebox**.
The Open Firebox dialog box appears.
If you get an error message that tells you that you cannot connect, try again.



2. From the **Firebox Address or Name** drop-down list, select a Firebox.
You can also type the IP address or host name.
3. In the **Passphrase** text box, type the Firebox status (read-only) passphrase.
Use the status passphrase here. You must use the configuration passphrase to save a new configuration to the Firebox.
4. Click **OK**.
Policy Manager opens the configuration file and shows the settings.





If you cannot open Policy Manager, try these steps:

- If the **Connect to Firebox** dialog box immediately comes back after you enter the passphrase, make sure that Caps Lock is off and that you type the passphrase correctly. Remember that the passphrase is case-sensitive.
- If the **Connect to Firebox** dialog box times out, make sure that you have a link on the trusted interface and on your computer. Make sure that you typed the correct IP address for the trusted interface of the Firebox. Also make sure that your computer IP address is in the same network as the trusted interface of the Firebox.

Open a local configuration file


You can open configuration files that are on any network drive to which your management station can connect.

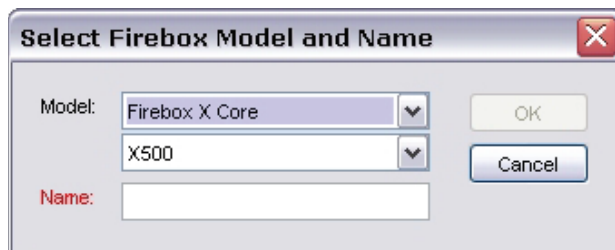
If you want to use an existing configuration file for a Firebox in a factory-default state, we recommend that you first run the Quick Setup Wizard to create a basic configuration and then open the existing configuration file. However, if you do open a configuration file on an appliance in a factory-default state, make sure you change the status and configuration passphrases.

1. From WatchGuard System Manager, click .
Or, select **Tools > Policy Manager**.
The Policy Manager window appears.
2. Click .
Or, select **File > Open > Configuration File**.
A standard Windows open file dialog box appears.
3. Use the **Open** dialog box to find and to select the configuration file. Click **Open**.
Policy Manager opens the configuration file and shows the settings.

Make a new configuration file

The Quick Setup Wizard makes a basic configuration file for your Firebox. We recommend that you use this as the base for each of your configuration files. However, you can also use Policy Manager to make a new configuration file with only the default configuration properties.

1. From WatchGuard System Manager, click .
Or, select **Tools > Policy Manager**.
2. From Policy Manager, select **File > New**.
The Select Firebox Model and Name dialog box appears.



3. Use the **Model** drop-down lists to select your Firebox model. Because some groups of features are unique to each model, select the same model as your hardware device.
4. Type a name for the Firebox. This name will be used as the name of the configuration file. It is also used to identify the Firebox if it is managed by a WatchGuard Management Server and for logging and reporting. Click **OK**.

Policy Manager makes a new configuration with the file name `<name>.xml`, where `<name>` is the name you gave the Firebox.

Save the configuration file

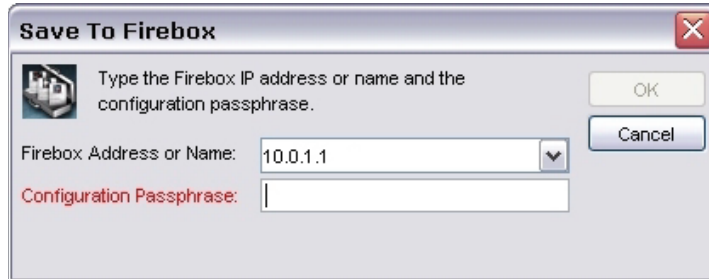
If you make a new configuration file or change the current configuration file and want your changes to take effect on the Firebox, you must save the configuration file directly to the Firebox.

You can also save the current configuration file to a local hard disk. If you plan to make one or more major changes to your configuration file, we recommend that you save the old configuration file to a local hard drive first. If you have problems with your new configuration, you can restore the old version.

Save a configuration directly to the Firebox

1. From Policy Manager, click **File > Save > To Firebox**.

The Save to Firebox dialog box appears.

The image shows a Windows-style dialog box titled "Save To Firebox". It has a close button (X) in the top right corner. Inside the dialog, there is a small icon of a server rack on the left. To the right of the icon, the text reads: "Type the Firebox IP address or name and the configuration passphrase." Below this text, there are two input fields. The first field is labeled "Firebox Address or Name:" and contains the text "10.0.1.1". To the right of this field is a small downward-pointing arrow, indicating a drop-down menu. The second field is labeled "Configuration Passphrase:" and is currently empty. To the right of the input fields are two buttons: "OK" and "Cancel".

2. From the **Firebox Address or Name** drop-down list, type an IP address or name, or select a Firebox. If you use a Firebox name, the name must resolve through DNS. When you type an IP address, type all the numbers and the periods. Do not use the TAB key or arrow key.
3. Type the Firebox configuration passphrase. You must use the configuration passphrase to save a file to the Firebox.
4. Click **OK**.

Save a configuration to a local hard drive

1. From Policy Manager, click **File > Save > As File**.

You can also use CTRL-S. A standard Windows save file dialog box appears.

2. Type the name of the file.

The default procedure is to save the file to the `My Documents\My WatchGuard\configs` directory. You can also browse to any folder to which you can connect from the management station. For better security, we recommend that you save the files in a safe folder that no other users can get access to.

3. Click **Save**.

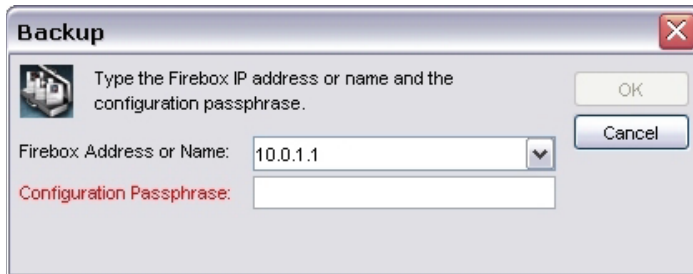
The configuration file saves to directory you specify.

Make a backup of the Firebox image

A Firebox backup image is an encrypted and saved copy of the flash disk image from the Firebox flash disk. It includes the Firebox appliance software, configuration file, licenses, and certificates. You can save a backup image to your management station or to a directory on your network.

We recommend that you regularly make backup files of the Firebox image. We also recommend that you create a backup image of the Firebox before you make significant changes to your Firebox configuration, or before you upgrade your Firebox or its appliance software.

1. From Policy Manager, select **File > Backup**.
The Backup dialog box appears.



Backup

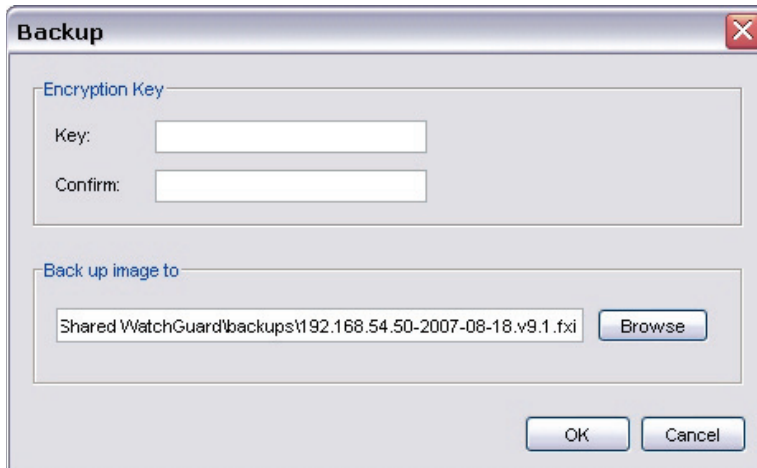
Type the Firebox IP address or name and the configuration passphrase.

Firebox Address or Name: 10.0.1.1

Configuration Passphrase:

OK Cancel

2. Type the configuration passphrase for your Firebox.
The second part of the Backup dialog box appears.



Backup

Encryption Key

Key:

Confirm:

Back up image to

Shared WatchGuard\backups\192.168.54.50-2007-08-18.v9.1.fxi

Browse

OK Cancel

3. Type and confirm an encryption key.
This key is used to encrypt the backup file. If you lose or forget this encryption key, you will not be able to restore the backup file.
4. Select the directory in which to save the backup file. Click **OK**.
The default location for a backup file with a .fxi extension is:
C:\Documents and Settings\All Users\Shared WatchGuard\backups\<Firebox IP address>-<date>.<wsm_version>.fxi.

Restore a Firebox backup image

1. From Policy Manager, select **File > Restore**.
The Restore dialog box appears.
2. Type the configuration passphrase for your Firebox. Click **OK**.
3. Type the encryption key you used when you created the backup image.
The Firebox restores the backup image and restarts. It uses the backup image on restart. Wait for two minutes before you connect to the Firebox again.

If you cannot successfully restore your Firebox image, you can reset the Firebox. Depending on the Firebox model you have, you can reset a Firebox to its factory-default settings or rerun the Quick Setup Wizard to create a new configuration. For more information, see [Reset a Firebox to a previous or new configuration](#).

Reset a Firebox to a previous or new configuration

You can reset a Firebox to its factory-default settings or reset it with a completely new configuration. The procedure to reset a Firebox X Core or Peak e-Series device is different from the procedure to recover an earlier model of a Firebox X Core or Peak. Make sure you use the correct procedure for your Firebox.

Reset a Firebox X e-Series device

To put a new configuration on a Firebox X Core or Peak e-Series device, use the Web Quick Setup Wizard. For more information, see [Web Quick Setup Wizard](#).

If you use the Web Quick Setup Wizard for recovery and you have purchased a Firebox hardware model upgrade, you must make sure that the feature key you put in the wizard is the feature key that you received with the model upgrade.

Reset a Firebox X Core or Peak (non e-Series)

With an earlier model Firebox X Core or Peak, you can use the Quick Setup Wizard to reset the Firebox with a completely new configuration. This is the easiest way to reset a Firebox and the most common procedure used.

There are times, however, when you cannot use the Quick Setup Wizard to reset a Firebox. When you use the Quick Setup Wizard, you must be able to make a network connection to the Firebox from your management station and discover the Firebox on the network. If this is not possible, you can use the manual reset procedure described below.

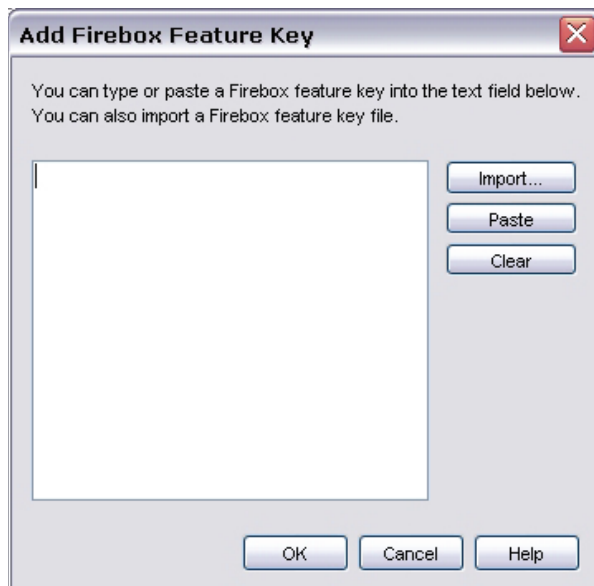
Reset a non e-Series device manually

You must have a valid Firebox feature key to use this procedure.

1. Turn the Firebox off. On the front of the Firebox, find and press the up arrow button.



2. Hold down the up arrow button while you turn on the Firebox, and continue to hold the button down until the LCD display shows the Firebox is running in safe mode. When the Firebox runs in safe mode, it is running in factory-default mode. In factory-default mode, the Firebox trusted interface is set to 10.0.1.1.
3. Connect a cross-over Ethernet network cable between your WatchGuard management station and the trusted interface of the Firebox. The trusted interface is labeled interface 1 on the Firebox.
4. Change the IP address on your management station to 10.0.1.2 (or another IP address from which you can connect to the Firebox trusted interface at 10.0.1.1/24). If your management station uses Windows XP: From your Windows Start menu, select **Control Panel > Network Connections > Local Area Connections**. Click **Properties**. Select **Internet Protocol (TCP/IP)** and click **Properties**. We recommend that you ping the trusted interface from your management station to make sure you have an operational network connection.
5. Open Policy Manager. You can open an existing configuration file, or create a new configuration file. Use the options available from the **File** drop-down menu.
6. Select **Setup > Feature Keys**. Click **Import** and either paste a copy of your feature key in the text box, or import a feature key file.



7. When you are ready, select **File > Save > To Firebox**. Save your configuration to the Firebox at IP address 10.0.1.1, with the administrative passphrase admin.
8. After the Firebox restarts with its new configuration, we recommend that you change the passphrases for the Firebox. Select **File > Change Passphrases** to set new passphrases.
9. You can now put the Firebox back on to your network and connect to it with the IP addresses and passphrases you set in your new configuration.

If you did not change the IP address or passphrase, you can connect to the trusted IP address 10.0.1.1 with the passphrase admin.

Use an existing configuration for a new Firebox model

When you upgrade your Firebox model, you can continue to use the same configuration file. When you import a new feature key, the Firebox can automatically change your existing configuration file so that it operates correctly with a new Firebox model. Use this procedure if you want to use an existing configuration for a new Firebox:

1. If you have not already done so, [get a feature key](#) for your new Firebox.
2. If your new Firebox has more interfaces than your existing one, you must [disable the extra interfaces](#) so the two have the same number. For example, if you upgrade from a Firebox with six interfaces to a Firebox with eight interfaces, you must disable two of interfaces on the new Firebox. If you do not know how many interfaces a Firebox has, see the procedure below.
3. On your existing Firebox, [open Policy Manager](#).
4. Select **Setup > Feature Keys**.
The Firebox Feature Key dialog box appears.
5. Click **Remove** to remove the current feature key.
6. Click **Import**.
The Import Firebox Feature Key dialog box appears.
7. When you got a feature key for your new Firebox, you copied the full feature key to a text file and saved it on your computer. Open this file and paste the contents of the feature key file for the new Firebox into the **Import Firebox Feature Key** dialog box.
8. Click **OK**. Policy Manager uses the new feature key to change the model of the Firebox in the configuration file. You can verify that this occurs correctly. From Policy Manager, select **Setup > System**. You should see the new model information.
9. Select **File > Save > To Firebox** to save the configuration to the Firebox.

Find the number of interfaces for a Firebox model

If you are not sure how many interfaces your new Firebox has, see the product comparison page on the WatchGuard web site <http://www.watchguard.com/products/compare.asp>.

8

Logging and Notification

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 Log Server collects log message data from each WatchGuard Firebox.

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.

After your Log Server has collected the log data from your Firebox devices, the Report Server periodically consolidates the data and generates reports. For more information about the Report Server and Report Viewer, see [About the Report Server](#) and [About the Report Manager](#).

LogViewer

LogViewer is the WatchGuard System Manager tool you use to see log file data. It can show the log data page by page, or search and display by key words or specified log fields.

For more information about LogViewer and how to use it, see [Use LogViewer to see log files](#).

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.

For more information about sending log messages from your Firebox, see [Configure logging and notification for a policy](#).

For more information about sending log messages from your WatchGuard server, see [Logging and monitoring settings](#).

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.

You can use Firebox System Manager to see log messages in the **Traffic Monitor** tab. For more information, see [Firebox log messages \(Traffic Monitor\)](#). You can also examine log messages with LogViewer. The log messages are kept on the Log Server in the WatchGuard directory in an SQL database file with a .wgl.xml extension.

To learn more about the different kinds of log messages that the Firebox sends, see [Types of log messages](#).

Types of log messages

The Firebox sends five types of log messages. The type appears in the text of the message. The five types of log messages are:

- Traffic
- Alarm
- Event
- Debug
- Statistic

Traffic log messages

The Firebox sends traffic log messages as it applies packet filter and proxy rules to traffic that goes through the Firebox.

Alarm log messages

Alarm log messages are sent when an event occurs that triggers the Firebox to run a command. When the alarm condition is matched, the Firebox sends an Alarm log message to the Traffic Monitor and Log Server and then it does the specified action.

You can set some alarm log messages. For example, you can use Policy Manager to configure an alarm to occur when a specified value matches or is more than a threshold. Other alarm log messages are set by the appliance software, and you cannot change the value. For example, the Firebox sends an alarm log message when a network connection on one of the Firebox interfaces fails or when a Denial of Service attack occurs. For more information about alarm log messages, see the *Reference Guide*.

There are eight categories of alarm log messages: System, IPS, AV, Policy, Proxy, Counter, Denial of Service, and Traffic. The Firebox does not send more than 10 alarms in 15 minutes for the same conditions.

Event log messages

The Firebox sends event log messages because of user activity. Actions that can cause the Firebox to send an event log message include:

- Firebox start up and shut down
- Problems with the Firebox hardware components
- Firebox and VPN authentication
- Any task done by the Firebox administrator
- Process start up and shut down

Debug log messages

Debug log messages include diagnostic information that you can use to help troubleshoot problems. There are 27 different product components that can send debug log messages. You can select whether the debug (diagnostic) log messages appear in Traffic Monitor, as described in [Enable advanced diagnostics](#).

Statistic log messages

Statistic log messages include information about the performance of the Firebox. By default, the Firebox sends log messages about external interface performance and VPN bandwidth statistics to your log file. You can use these logs to change your Firebox settings as necessary to improve performance. For more information about statistic log messages, see [Define where the Firebox sends log messages](#) and [Disable performance statistic logging](#).

About notification

A notification is a message that the Firebox sends to an administrator when an event occurs that is a possible security threat. The notification can be an email message or a popup window. Notifications can also be sent by way of an SNMP trap. (For more information about SNMP traps, see [About SNMP](#).)

For example, WatchGuard recommends that you configure default packet handling options to send a notification when the Firebox finds a port space probe. The Firebox finds a port space probe by counting the number of packets sent from one IP address to all of the Firebox's external interface IP addresses. If the number is greater than a configured value, the log host sends a notification to the network administrator about the rejected packets.

As with log files, network administrators can examine notifications and make decisions about how to add more security to an organizations's network. With the port space probe example, some possible changes might be:

- Block the ports on which the probe was used
- Block the IP address that sent the packets
- Send a notification email message to your network administrator

Configure your Log Server for notification

The Firebox sends notifications only if you enable and configure them on the Log Server that your Firebox uses:

- To enable notification on the Log Server, see [Expiration settings for a Log Server](#) and select the **Enable notifications for events from any device or server logging to this Log Server** check box.
- To define the email address that appears as the sender of the notification email messages, see [Expiration settings for a Log Server](#) and enter the email address in the **Send email from** field.
- To define the email recipient, see [Database and SMTP server settings for a Log Server](#), select the **Send a warning if the database reaches the warning threshold** check box, and enter the recipient's email address in the **Send warning message to** field. Use the **Subject** field to define the text that appears in the Subject field of notification email messages. If you do not want to use the database warning feature, you can then clear the **Send a warning if the database reaches the warning threshold** check box.

Define where the Firebox sends log messages

You can configure your Firebox to log events that occur at the Firebox. You can then examine the log files and make decisions about how to add more security to your network. You must tell the Firebox where to send log messages.

1. From Policy Manager, select **Setup > Logging**.
The *Logging Setup* dialog box appears.

2. Configure the logging settings for the WatchGuard Log Server, syslog server, and Firebox Internal Storage.
The available options are described below.

WatchGuard Log Server

Select the **Send log messages to the log servers at these IP addresses** check box to send log messages to your Log Servers. A Firebox can send log messages to a Log Server and a syslog server at the same time.

Click **Configure** to add or edit the IP addresses for your Log Servers. For more information, see [Add a Log Server](#).

Syslog Server

Select the **Send log messages to the Syslog server at this IP address** check box to send log messages to your syslog server. A Firebox can send log messages to a Log Server and a syslog server at the same time.

Click **Configure** to add or edit the IP addresses for your syslog server. For more information, see [Configure syslog](#).

Firebox Internal Storage

Select the **Send log messages in Firebox internal storage** to enable the Firebox to store the log messages.

Performance Statistics

By default, the Firebox sends log messages about external interface performance and VPN bandwidth statistics to your log file. To disable this type of log message, see [Disable performance statistic logging](#).

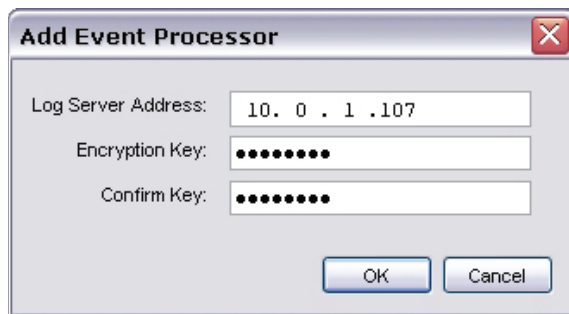
Advanced Diagnostics

To set the level of diagnostic logging to write to your log file or to [Traffic Monitor](#) for each logging category, see [Enable advanced diagnostics](#).

Add a Log Server

If you select the **Send log messages to the log servers at these IP addresses** check box when you [define where the Firebox sends log messages](#), you can then add one or more Log Servers to the Firebox.

1. From Policy Manager, select **Setup > Logging**.
The Logging Setup dialog box appears.
2. Click **Configure**. Click **Add**.
The Add Event Processor dialog box appears.



The image shows a dialog box titled "Add Event Processor" with a close button (X) in the top right corner. It contains three input fields: "Log Server Address:" with the value "10. 0 . 1 .107", "Encryption Key:" with a masked key "••••••••", and "Confirm Key:" with a masked key "••••••••". At the bottom, there are "OK" and "Cancel" buttons.

Use the Add Event Processor dialog box

1. In the **Log Server Address** field, type the IP address of the Log Server you want to add.
2. In the **Encryption Key** and **Confirm** text boxes, type the Log Server encryption key that you set when you used the Log Server Configuration Wizard, as described in [Set up the Log Server](#).
The allowed range for the encryption key is 8–32 characters. You can use all characters but spaces and slashes (/ or \).
3. Click **OK**.
The Add Event Processor dialog box disappears.

Save the changes and verify logging

1. Click **OK** to close the **Configure Log Servers** dialog box.
2. Click **OK** to close the **Logging Setup** dialog box.
3. [Save the configuration file.](#)

To verify that the Firebox is logging correctly, from WSM, select **Tools > Firebox System Manager**. In the **Detail** section on the left, next to **Log Server**, you should see the IP address of the log host.

Set Log Server priority

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.

1. From Policy Manager, select **Setup > Logging**.
The Logging Setup dialog box appears.
2. Click **Configure**.
The Configure Log Servers dialog box appears.
3. Select a Log Server from the list and click the **Up** and **Down** buttons to change the order.
4. Click **OK**.
The Logging Setup dialog box appears with the new priority order of the Log Servers displayed in the WatchGuard Log Server list.

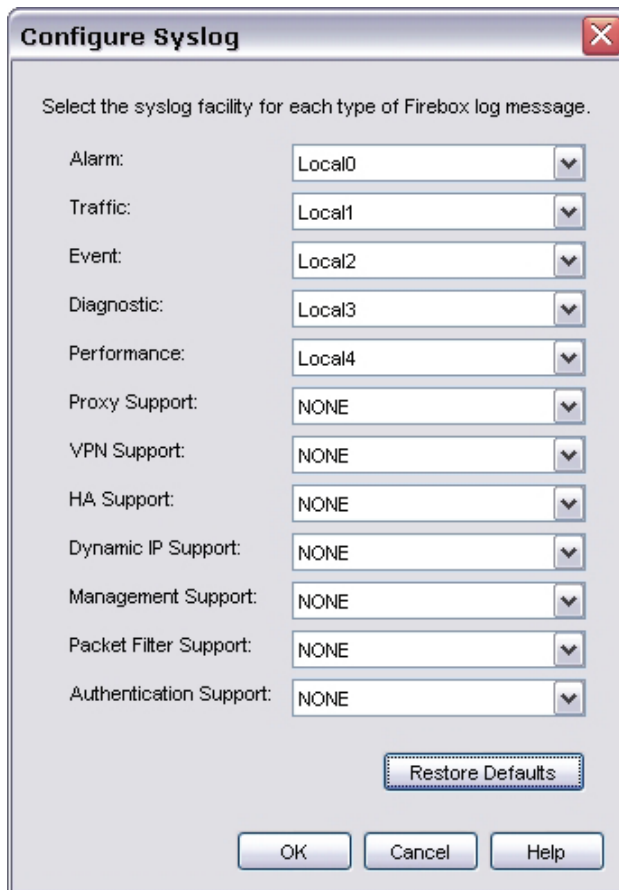
Configure syslog

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.

1. From Policy Manager, select **Setup > Logging**.
The Logging Setup dialog box appears.
2. Select the **Send Log Messages to the Syslog server at this IP address** check box.
3. In the address box, type the IP address of the syslog server.

4. Click **Configure**.

The Configure Syslog dialog box appears.



The image shows a 'Configure Syslog' dialog box with a title bar and a close button. Inside, it says 'Select the syslog facility for each type of Firebox log message.' Below this is a list of log message types, each with a corresponding dropdown menu for selecting a syslog facility. The facilities are Local0 through Local7, or NONE. At the bottom, there are buttons for 'Restore Defaults', 'OK', 'Cancel', and 'Help'.

Log Message Type	Syslog Facility
Alarm:	Local0
Traffic:	Local1
Event:	Local2
Diagnostic:	Local3
Performance:	Local4
Proxy Support:	NONE
VPN Support:	NONE
HA Support:	NONE
Dynamic IP Support:	NONE
Management Support:	NONE
Packet Filter Support:	NONE
Authentication Support:	NONE

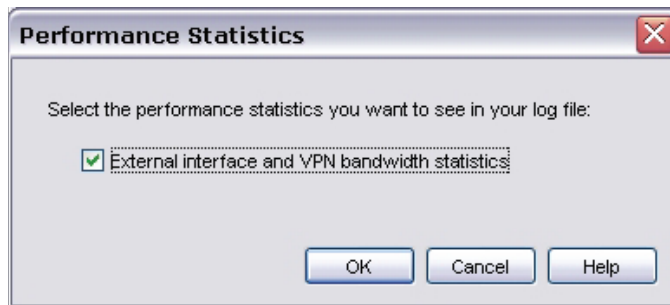
Buttons: Restore Defaults, OK, Cancel, Help

5. For each type of log message, select the syslog facility to which you want it assigned. For information about the different types of messages, see [Types of log messages](#). The syslog facility refers to one of the fields in the syslog packet and to the file syslog sends a log message to. You can use Local0 for high priority syslog messages, such as alarms. You can use Local1 - Local7 to assign priorities for other types of log messages (with lower numbers having greater priority). See your syslog documentation for more information on logging facilities.
6. Click **OK** to close the **Configure Syslog** dialog box.
7. Click **OK** to close the **Logging Setup** dialog box.
8. [Save the configuration file](#).

Disable performance statistic logging

By default, the Firebox sends log messages about external interface performance and VPN bandwidth statistics to your log file. To disable this type of log message:

1. From Policy Manager, select **Setup > Logging**.
The Logging Setup dialog box appears.
2. Click **Performance Statistics**.
The Performance Statistics dialog box appears.

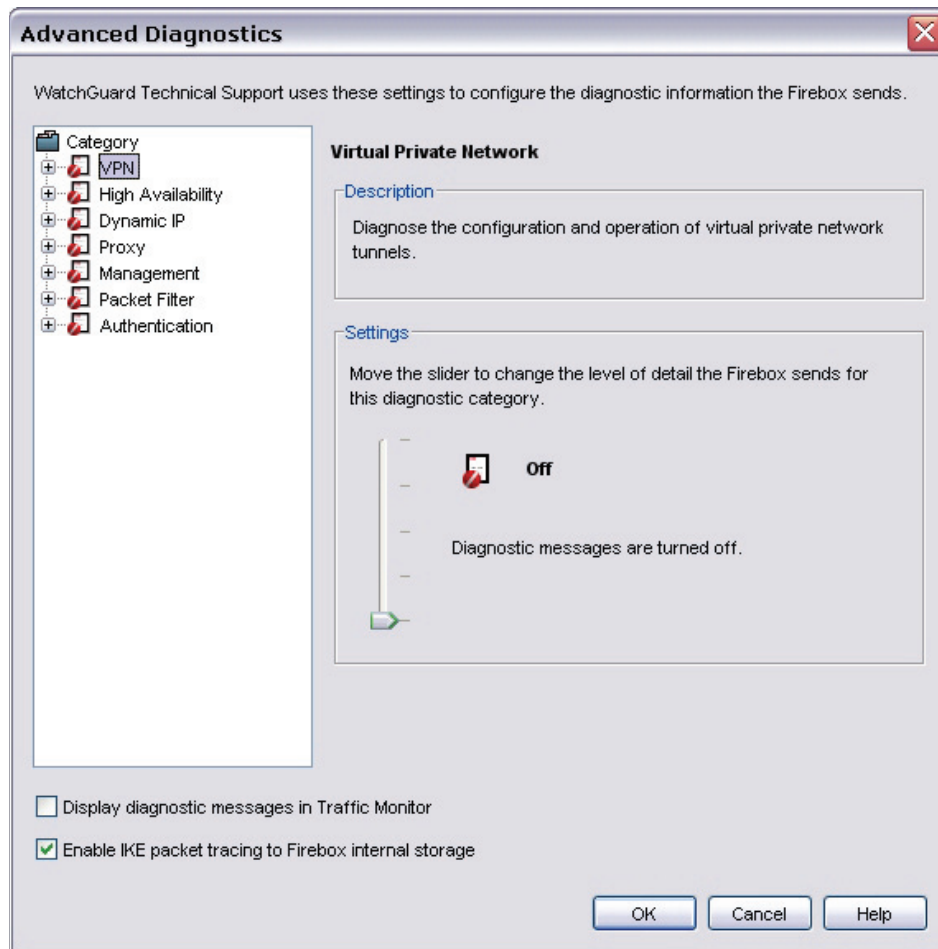


3. Clear the **External interface and VPN bandwidth statistics** check box.
4. Click **OK**. [Save the configuration file.](#)

Enable advanced diagnostics

You can select the level of diagnostic logging to write to your log file or to [Traffic Monitor](#). We do not recommend that you set the logging level to the highest level unless a technical support representative tells you to while you troubleshoot a problem. Using the highest level can cause the log file to fill up very quickly. It can also create a high load on the Firebox.

1. From Policy Manager, select **Setup > Logging**.
The Logging Setup dialog box appears.
2. Click **Advanced Diagnostics**.
The Advanced Diagnostics dialog box appears.

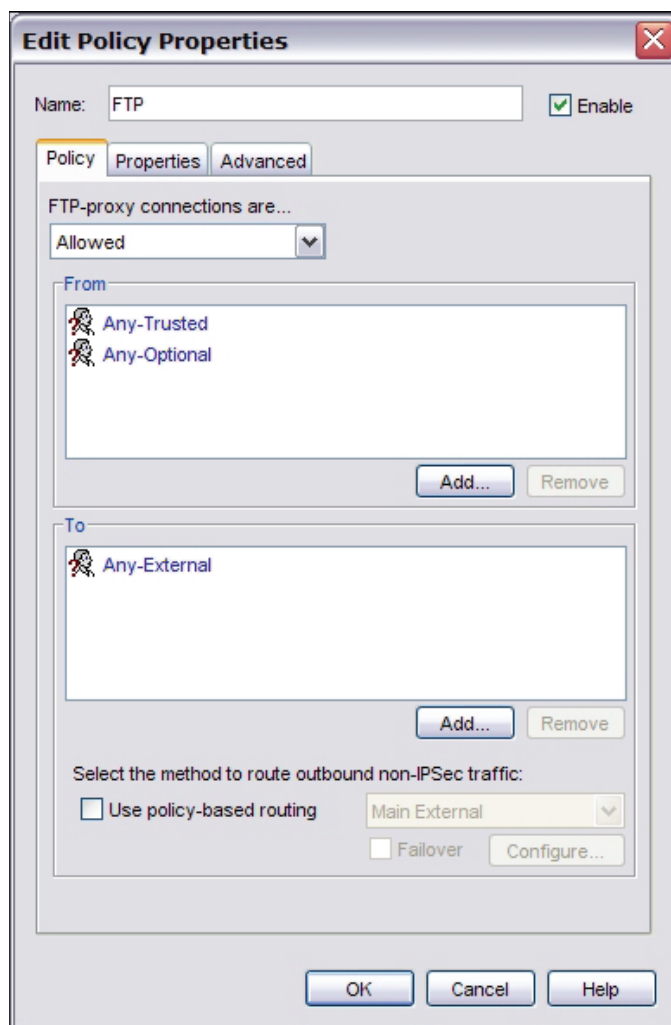


3. Select a category from the **Category** list.
A description of the category appears in the Description box.
4. Use the slider below **Settings** to set the level of information that a log of each category includes in its log message.
When the lowest level is set, diagnostic messages for that category are turned off.
When the highest level is set, you can set the detail level for the diagnostic log messages.
5. To show diagnostic messages in Traffic Manager, select the **Display diagnostic messages in Traffic Monitor** check box.
This can be useful to quickly diagnose a problem. Diagnostic messages can be sent to Traffic Monitor for all categories except the Policy Management Module (PMM). Messages for the Policy Management Module are sent to the log file only and cannot be seen in Traffic Monitor.

6. To have the Firebox collect a packet trace for IKE packets, select the **Enable IKE packet tracing to Firebox internal storage** check box.
7. To see the packet trace information the Firebox collects, [Start Firebox System Manager](#) and click the **Status Report** tab.
8. Click **Support** to have Firebox System Manager get the packet trace information from the Firebox.
9. Turn off diagnostic logging when done.

Configure logging and notification for a policy

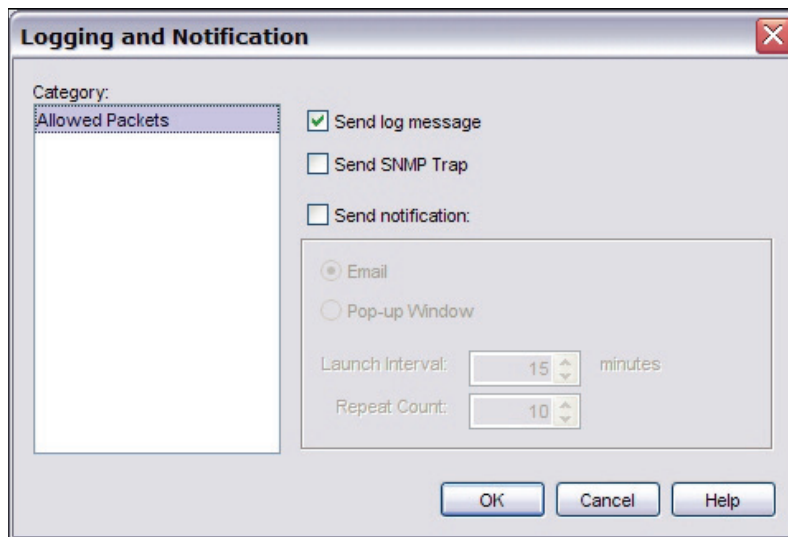
1. From Policy Manager, [add a policy](#) or double-click a policy icon to edit an existing policy. The *Edit Policy Properties* dialog box appears.



2. Click the **Properties** tab.

3. Click **Logging**.

The *Logging and Notification* dialog box appears.

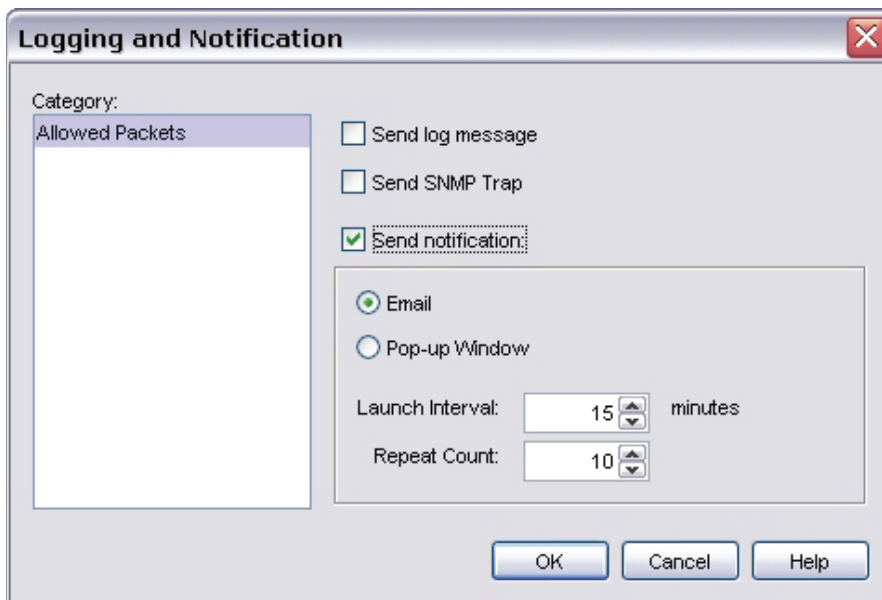


4. Set the parameters to match your security policy.

For information on fields in the **Logging and Notification** dialog box, see [Set logging and notification preferences](#).

Set logging and notification preferences

The settings for logging and notification are similar throughout WatchGuard System Manager, Policy Manager, and the WatchGuard servers. For each place you define logging and notification preferences, most or all of the fields described below are available.



Send log message

When you select this check box, the Firebox sends a log message when an event occurs.

Send SNMP trap

When you select this check box, the Firebox sends an event notification to the SNMP management system. Simple Network Management Protocol (SNMP) is a set of tools for monitoring and managing networks. An SNMP trap is an event notification the Firebox sends to the SNMP management system when a specified condition occurs.

If you want to enable SNMP traps, from Policy Manager select **Setup > SNMP** to configure SNMP parameters for your Firebox. Or, if you select the **Send SNMP Trap** check box and you have not yet configured SNMP, a dialog box appears and asks you if you want to do this. Click **Yes** to go to the **SNMP Settings** dialog box. For more information on SNMP, see [About SNMP](#).

To enable SNMP traps or inform requests, see [Enable SNMP traps or inform requests](#).

Send notification

When you select this check box, the Firebox sends a notification when a packet is denied. To configure notification, see [About notification](#). You can tell the Firebox to do one of these actions:

Email

The Log Server sends an email message when the event occurs.

Notification email messages have the format [friendly_name]@[domain_name]

Where:

- friendly_name = the Firebox friendly name.
(For information on how to set or change this, see [Assign a friendly name](#).)
- domain_name = the name in the **Mail Host** field on this dialog box.

Pop-up Window

The Firebox makes a dialog box appear on the management station when the event occurs.

You can control the time of the notification, together with the Repeat Count, as follows:

Launch Interval

The minimum time (in minutes) between different notifications. This parameter prevents more than one notification in a short time for the same event.

Repeat Count

This setting keeps track of how frequently an event occurs. When the number of events reaches the selected value, a special repeat notification starts. This notification creates a repeat log entry about that specified notification. Notification starts again after this number of events.

Here is an example of how to use these two values. The values are configured as:

- Launch interval = 5 minutes
- Repeat count = 4

A port space probe starts at 10:00 a.m. and continues each minute. This starts the logging and notification mechanisms. These are the times and the actions that occur:

1. 10:00 — Initial port space probe (first event)
2. 10:01 — First notification starts (one event)
3. 10:06 — Second notification starts (reports five events)
4. 10:11 — Third notification starts (reports five events)
5. 10:16 — Fourth notification starts (reports five events)

The launch interval controls the time intervals between the events 1, 2, 3, 4, and 5. This was set to 5 minutes. Multiply the repeat count by the launch interval. This is the time interval an event must continue to start the repeat notification.

Set up a Log Server

The Log Server collects log message data from each WatchGuard Firebox managed by WatchGuard System Manager.

You can install a Log Server on the computer you are using as a management station. Or, you can install the Log Server software on a different computer using the WatchGuard System Manager installation program. Run the installation program and select to install only the Log Server component. You can also add additional Log Servers for backup.



If you install a WatchGuard server on a computer with a firewall other than Windows Firewall, you must open the ports necessary for the servers to connect through the firewall. Windows Firewall users do not have to change their configuration. See [Install WatchGuard Servers on computers with desktop firewalls](#) for more information.

About passphrases

All WatchGuard servers share the same master passphrase and server management passphrase. If you set up another server first, you do not have to set the passphrase again when you set up the Log Server. For more information about server passphrases, see [About WatchGuard Server passphrases](#).

Install the Log Server



If you run the Log Server Setup Wizard from a remote desktop connection to a Windows 2000 or Windows 2003 Server Terminal Services session, the PostgreSQL database fails to install if you do not open the remote desktop session as a console or remote administration session, and configure Terminal services to run in Remote Administration Mode.

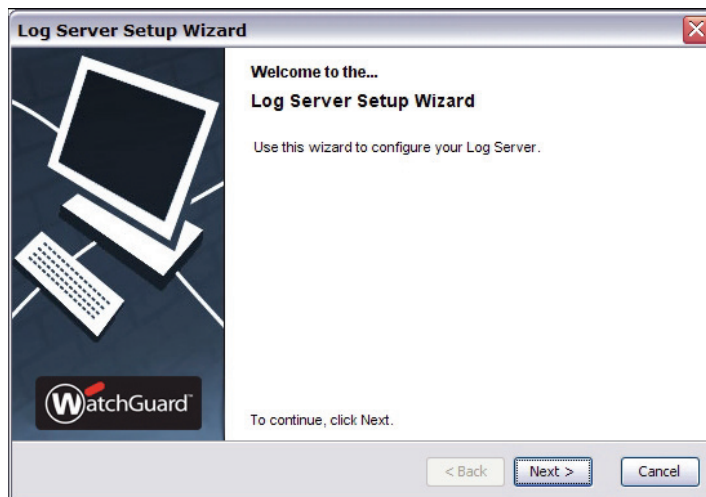
1. On the computer that has the Log Server software installed, click in the WatchGuard toolbar (in the system tray at the lower- right of your screen).

Or, right-click and select **Setup Wizard**.

If the WatchGuard toolbar does not appear, right-click in the system tray and select **Toolbars > WatchGuard**.



The Log Server Configuration wizard starts.



2. Type and confirm the encryption key to use for the secure connection between the Firebox and the Log Servers. The allowed range for the encryption key is 8–32 characters. You can use all characters but spaces and slashes (/ or \).
Make sure you remember the encryption key. You will need it when you add this Log Server to a Firebox or to the Quarantine Server.
3. Select the **Data Directory Path**, where all log files, report files, and report definition files are kept. We recommend that you use the default location: **C:\Documents and Settings\WatchGuard\logs**.



Select the **Data Directory Path** carefully. After you have installed the database you cannot change the directory location through the Log Server user interface. If you must change the **Data Directory Path**, see [Move the log data directory](#).


4. Click **Open**.
The Log Server Setup Wizard reappears.
5. Click **Next**. Type and confirm your master passphrase. Click **Next**.
6. Type and confirm your Server Management passphrase. Click **Next**.
The wizard installs the Postgres database.
7. Type the name of your organization. Click **Next**.
The wizard configures your server.
8. Click **Finish** to exit the wizard.

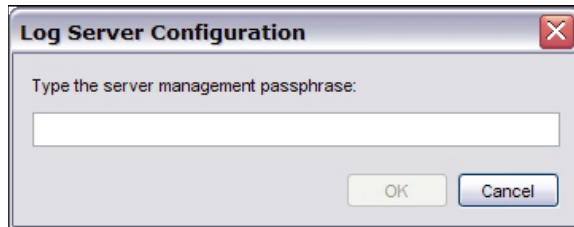
Configure your system settings

1. Click **Start > Control Panel**. Go to Power Options. Select the **Hibernate** tab and disable hibernation. This is to prevent the Log Server from shutting down when the computer hibernates.
2. Make sure the Log Server and the Firebox are set to the same system time. To synchronize the time of the Firebox with the system time, [Start Firebox System Manager](#). Select **Tools > Synchronize Time**.

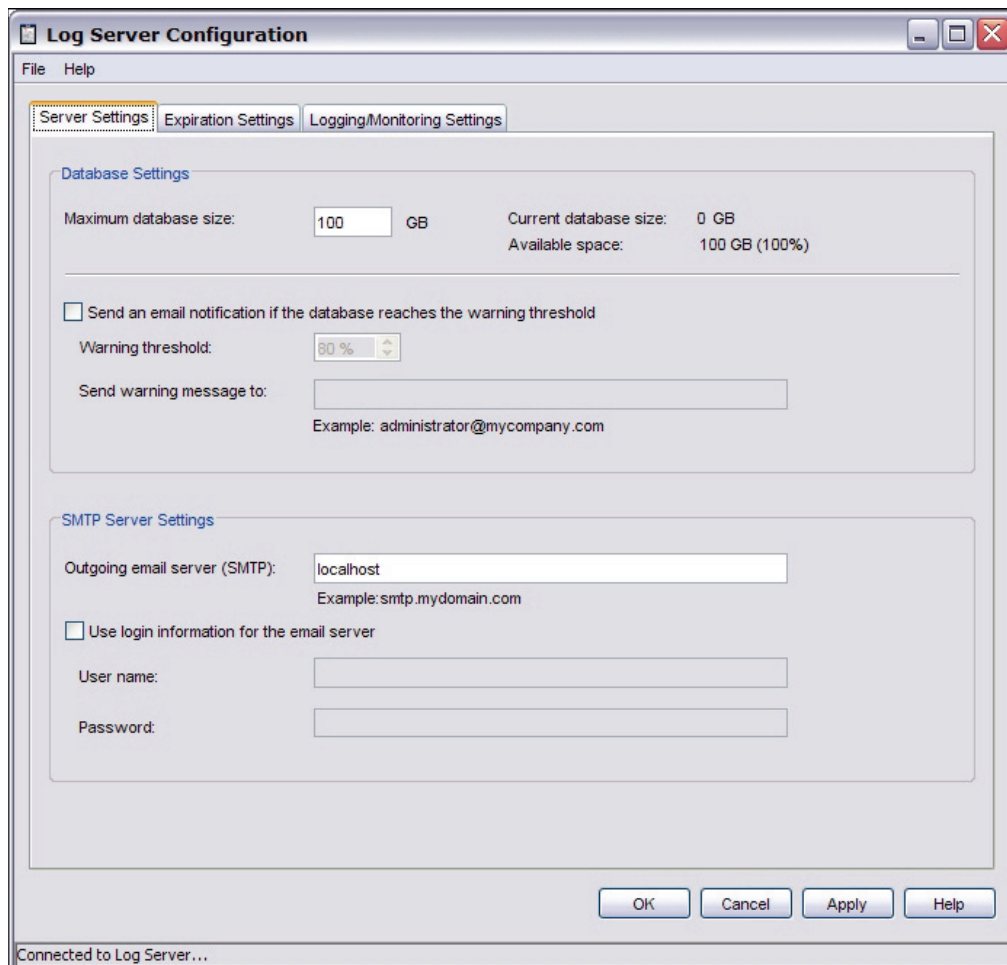
Configure a Log Server

Before you use this procedure, you must first [set up the Log Server](#). Then, follow these steps to configure the server:

1. Right-click  in the system tray and select **Configure**.
The Log Server Configuration dialog box appears.



2. Type the server management passphrase and click **OK**.
The Log Server Configuration dialog box appears.



3. Change the default settings as appropriate for your network. When you are finished, click **OK**.

To change your default server settings, click the [Server Settings tab](#).

To change the settings for log file back up and deletion, and notification setup, click the [Expiration Settings tab](#).

To change the settings for logging, click the [Logging/Monitoring Settings tab](#).

Database and SMTP server settings for a Log Server

You can choose the database and SMTP server settings for your Log Server on the **Server Settings** tab in the **Log Server Configuration** dialog box.

The screenshot shows the 'Log Server Configuration' dialog box with the 'Server Settings' tab selected. The 'Database Settings' section includes a 'Maximum database size' of 100 GB, a 'Current database size' of 0 GB, and 'Available space' of 100 GB (100%). There is a checkbox for 'Send an email notification if the database reaches the warning threshold', a 'Warning threshold' set to 80%, and a 'Send warning message to' field with an example email address. The 'SMTP Server Settings' section includes an 'Outgoing email server (SMTP)' field set to localhost, a checkbox for 'Use login information for the email server', and fields for 'User name' and 'Password'. At the bottom are 'OK', 'Cancel', 'Apply', and 'Help' buttons. A status bar at the very bottom says 'Connected to Log Server...'.

Database Settings

Maximum database size

Type the maximum size for the Log Server database. When the server runs out of drive space, it refuses to accept new messages and drops any subsequent email messages it receives. The minimum database size is 10 GB.

The dialog box displays the current size of the database and the number of GB currently available.

Send an email notification if the database reaches the warning threshold

If you want to receive a warning message when the database is near its limit, select this check box.

Warning threshold

To specify when the database sends you a threshold warning message, press the up or down arrows.

Send warning message to

Type the full email address of the account where you want to send the notifications.

For example, if you select to receive a warning message, set the default warning threshold to 90%, and set the default maximum database size to 10000 MB, the Log Server sends the warning message when 9000 MB have been used and only 1000 MB are available.

SMTP Server Settings

Outgoing email server (SMTP)

Type the address of the outgoing SMTP email server.

Use login information for the email server

If your email server requires authentication, select this check box.

User name

Type the user name for the email server. If the user name is not required for your SMTP server, you can keep this field blank.

Password

Type the password for the email server. If the password is not required for your SMTP server, you can keep this field blank.



When the Log Server databases are regularly purged, and the number of records sent to the server remains fairly constant, space freed by the purge process is simply reused by subsequent reports and logs. However, if the purge interval (defined in the **Retain log messages for** field on the [Expiration Settings](#) tab in the **Log Server Configuration** dialog box) is reduced, or debug logging is disabled after being used for a period of time, we recommend you use the `vacuumdb` command-line utility to [Reclaim free space from the Log Server database](#). This utility reduces the physical file size of the database by marking for reuse the objects that were purged.

Expiration settings for a Log Server

You can choose the log deletion settings, database backup settings, and notification setup for your Log Server on the **Expiration Settings** tab in the **Log Server Configuration** dialog box.

The screenshot shows the 'Log Server Configuration' dialog box with the 'Expiration Settings' tab selected. The dialog has a menu bar with 'File' and 'Help'. Below the menu bar are three tabs: 'Server Settings', 'Expiration Settings' (active), and 'Logging/Monitoring Settings'. The main area is divided into three sections: 'Log Deletion Settings', 'Database Backup Settings', and 'Notification Setup'. Each section contains various settings, checkboxes, and text fields. At the bottom are 'OK', 'Cancel', 'Apply', and 'Help' buttons. A status bar at the very bottom says 'Connected to Log Server...'.

Log Server Configuration

File Help

Server Settings | **Expiration Settings** | Logging/Monitoring Settings

Log Deletion Settings

☐ Enable log message deletion

Retain log messages for: 30 day(s) Messages last deleted:

Delete expired log messages at: 2:30 AM Next deletion scheduled: 01/24/2008 02:30 AM

Database Backup Settings

☐ Back up log messages automatically

Back up log data every: 1 day(s) Last backup date:

Back up log data at: 2:30 AM Next backup scheduled: 01/24/2008 02:30 AM

Directory path for backup files: c:/Documents and Settings/WatchGuard/wlogserver/tmp Browse

Notification Setup

☐ Enable notifications for events from any device or server logging to this Log Server

Send email from: Example: logServer@mycompany.com

Subject:

Test Email

OK Cancel Apply Help

Connected to Log Server...

Log deletion settings

Enable log message deletion

Select this check box to enable the Log Server to delete log messages from your device.

Retain log messages for

To specify the number of days messages remain on the Log Server, press the up or down arrows.
The dialog box shows the date messages were last deleted.

Delete expired log messages at

To set the time of day the expired messages are deleted, press the up or down arrows.
The dialog box shows the date and time of the next scheduled deletion.

Database backup settings

Back up log messages automatically

Select this check box to enable the Log Server to automatically create a backup copy of log messages.

Back up log data every

To specify how often the log data is backed up, press the up or down arrows.
The dialog box shows the date the last log backup occurred.

Back up log data at

To set the time of day the log data is backed up, press the up or down arrows.
The dialog box shows the date and time of the next scheduled backup.

Directory path for backup files

To select the folder where you want to save the backup files, click **Browse**.



Because your Log Server backup file is on the same computer as your database log files, we recommend that you configure your Log Server to save the backup files to a drive other than your computer hard drive, such as an external hard drive or a tape drive. Then, if you have a problem with your computer that prevents you from accessing files on the hard drive, you can still access your back up files.

Notification setup

Enable notifications for events from any device or server logging to this Log Server

Select this check box to enable the notification feature. You must select this check box for the notification events that you configure in Policy Manager to occur.

Send email from

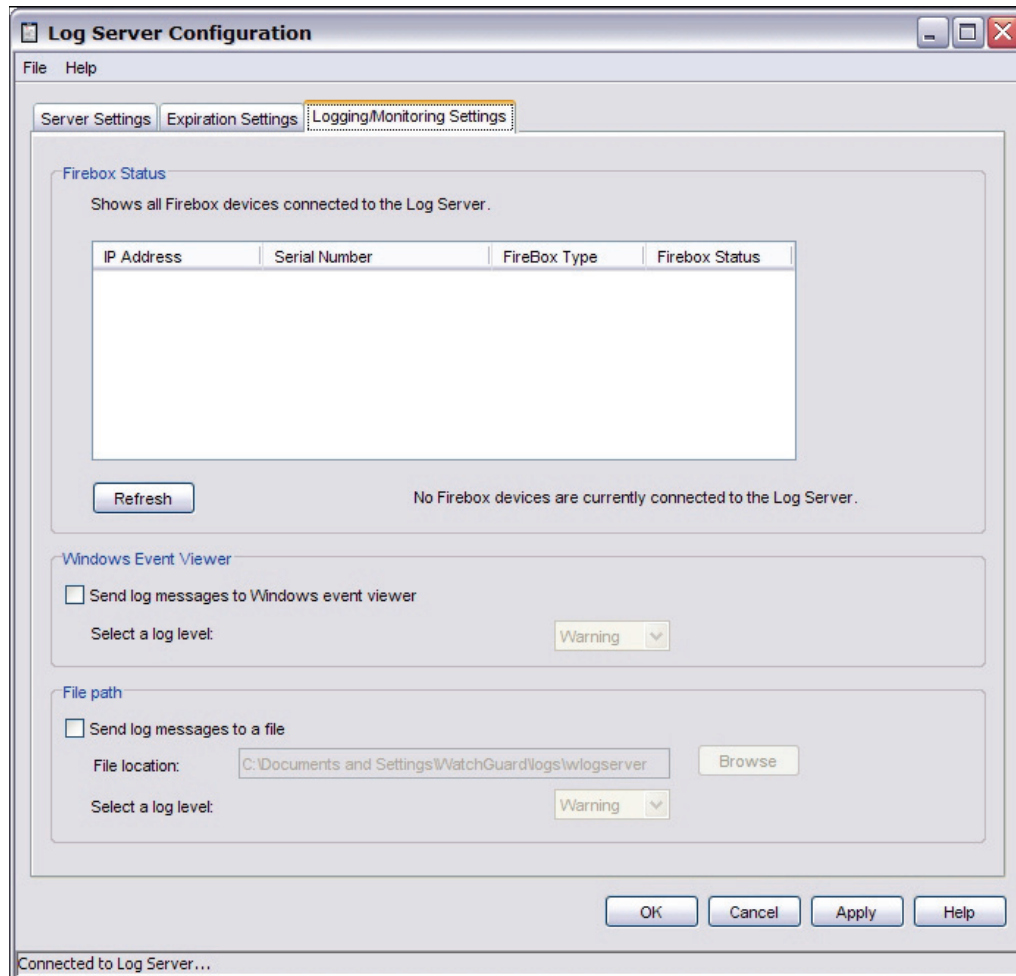
Type the full email address of the account you want to send notifications from.

Subject

Type the subject line you want users to see when they receive a notification email.

Logging and monitoring settings for a Log Server

You can choose the Firebox status, Windows Event Viewer, and file path settings for your Log Server on the **Logging/Monitoring Settings** tab in the **Log Server Configuration** dialog box.



Firebox Status

This window shows the list of all Firebox devices connected to the Log Server.

To see the current status of the connections, click **Refresh**.

The dialog box displays a message if no Firebox devices are connected to the Log Server.

Windows Event Viewer

Send log messages to Windows event viewer

Select this check box if you want the Log Server to send messages to Windows event viewer.

Select a log level

If you selected the **Send the log messages to Windows event viewer** check box, you can select the level that is assigned to log messages.

- Error
- Warning
- Information
- Debug

File path

Send log messages to a file

Select this check box to send log messages to the log file. To discard log messages, clear this check box.

File location

If you selected the **Send the log messages to a file** check box, you can select the location where log messages are sent and stored.

Select a log level

If you selected the **Send the log messages to a file** check box, you can select the level that is assigned to log messages.

- Error
- Warning
- Information
- Debug

Restore a backup log file

You can restore a backup log data file to your Log Server. Before you can restore your log data, you must set up your Log Server.

For more information about Log Server set up, see [Set up the Log Server](#).

If you enable your Log Server to back up log messages automatically, the Log Server saves the contents of the database in a CSV file in a directory that you choose. For each device that logs to the Log Server, a set of four separate files is created. When you restore the log files from the backup server, you must convert and import the set of files for each device one at a time.

To restore your log data to a Log Server, you must first convert the CSV file into an XML file with the `wlconvert.exe` application. If you have configured a secondary Log Server, the log files from each Log Server are in a separate CSV file.

For more information about enabling your Log Server to back up log files, see [Expiration settings for a Log Server](#).

The `wlconvert.exe` application is a command line application. Before you can run `wlconvert` to convert the backup files, you will need to have the information for two arguments: `-d` (directory) and `-f` (filename). The directory is the folder path where the backup files are saved, and is an optional argument. The filename is the `sn_timestamp` portion of the filename for each of the four files in the set, where `sn` is the serial number of the device and the timestamp is in the format `YYYYMMDDhhmmss`.

For example, if your Log Server back up files are located in the **C:\old_logs** directory, and the `sn_timestamp` for the file set is **209188121122_0070731000006**, the argument information is:

-d C:\old_logs -f 209188121122_0070731000006.

To convert the log file set:

1. From the command prompt, run the `wlconvert.exe` application, located in the **C:\Program Files\WatchGuard\wsm10.0\wlcollector\bin** folder.
2. Type the information for the `-d` and `-f` arguments.
3. Press **Enter** on your keyboard.

The set of four log files are converted to one XML file with the `sn_timestamp` from the four separate files as the file name.

For example, 209188121122_0070731000006.xml.

The new XML file appears in the folder with the set of four CSV files.

After you have converted the log data file from CSV to XML format, you can import the XML file into the Log Server with the `wlimport.exe` application. To import a log file, follow the steps in [Import a log file to a Log Server](#).

Import a log file to a Log Server

You can import XML log files to your Log Server with the `wlimport.exe` application. If you want to restore your Log Server backup log files, you must first convert the CSV files to XML.

For information about how to convert CSV files to XML format, see [Restore a backup log file](#).

The `wlimport.exe` application is a command line application. Before you can run `wlimport` to import the backup files, you will need to have the information for two arguments: `-e` (the log encryption key) and `-i` (the **Display Name** for the Log Server).



You only need the `-i` argument information to import XML files from an old Log Server into a new Log Server. If you want to import the backup files from your current Log Server, the `-i` argument is not necessary.

To import the XML log file:

1. From the command prompt, run the `wlimport.exe` application, located in the **C:\Program Files\WatchGuard\wsm10.0\wlcollector\bin** folder.
2. Type the information for the `-e` and `-i` arguments.
3. Press **Enter** on your keyboard.
The XML file is imported into your Log Server and a counter appears to show how many log entries have been imported.
This will take several minutes. The length of time is determined by the size of the log files.

After the file import is complete, you can use LogViewer see your log file. For more information, see [Use LogViewer to see log files](#).

Move the log data directory





When you install the Log Server, you choose the directory where your log data files are stored. After installation is complete, you cannot change the directory in the Log Server application. If you run the Log Server Setup Wizard again, a new Log Server directory is created, but the data in the old directory is not moved to the new directory.

You can manually move the current log data directory to a new location and then create a new Log Server directory.


1. Stop the Log Server and the Report Server.
2. Use the Windows **Add or Remove Programs** dialog box to uninstall the PostgreSQL program.
The Log Server database is not deleted.
3. Copy the original log data directory to the new location. Be sure to include all the folders and files within the directory.
For example, C:\Documents and Settings\WatchGuard\logs\data.
4. Start the Log Server Setup Wizard.
5. Select the new log data directory. Do not include the **\data** folder in the **Data Directory Path** field.
For example, C:\Documents and Settings\WatchGuard\Log Server2\logs.
6. Click through the remainder of the wizard and add the information it asks for.
The wizard re-installs the PostgreSQL program and creates a new Log Server directory in the new location.

Start and stop the Log Server

You can manually start or stop the Log Server service at any time without disconnecting from your Log Server.

- To start service, right-click  in your system tray and select **Start Service**.
Or, you can select **File > Start Server** in the **Log Server Configuration** dialog box.
The system tray icon changes to .
- To stop service, right-click  in your system tray and select **Stop Service**.
Or, you can select **File > Stop Server** in the **Log Server Configuration** dialog box.
The system tray icon changes to .

Change the Log Server encryption key

1. Right-click  on the WatchGuard toolbar and select **Configuration**.
2. Select **File > Set Log Server Encryption Key**.
3. Type the old log encryption key.
4. Type the new log encryption key two times. Click **OK**.
5. In Policy Manager, select **Setup > Logging**.
6. Select the IP address for the Log Server with the new encryption key in the WatchGuard Log Server list and click **Configure**.
The Configure Log Servers dialog box appears.
7. Select the Log Server name or IP address and click **Edit**.
8. Type and confirm the new log encryption key you want to use for this Log Server.
9. Click **OK**. [Save the configuration file.](#)

Reclaim free space from the Log Server database

When the Log Server database is regularly purged, and the number of records sent to the server remains fairly constant, space freed by the purge process is simply reused by subsequent logs. However, if the purge interval (defined in the **Retain log messages for** field on the [Expiration Settings tab in the Log Server Configuration dialog box](#)) is reduced, or debug logging is disabled after being used for a period of time, we recommend you use the vacuumdb command-line utility. This utility reduces the physical file size of the database by marking for reuse the objects that were purged.

Because this utility might take a long time to run, we recommend you set up a backup Log Server for your appliances if you do not already have one.

The vacuumdb utility can also be used to [Reclaim free space from the Report Server database](#).

To run the vacuumdb utility:


1. Stop the Log Server whose databases you want to perform this maintenance task on.
2. From the command line, run:
C:\Program Files\WatchGuard\wsm10.0\postgresql\bin\vacuumdb -v -f -d wglog -U wguser
(You can omit the -v option to disable verbose output.)
3. When prompted, enter the server management passphrase.

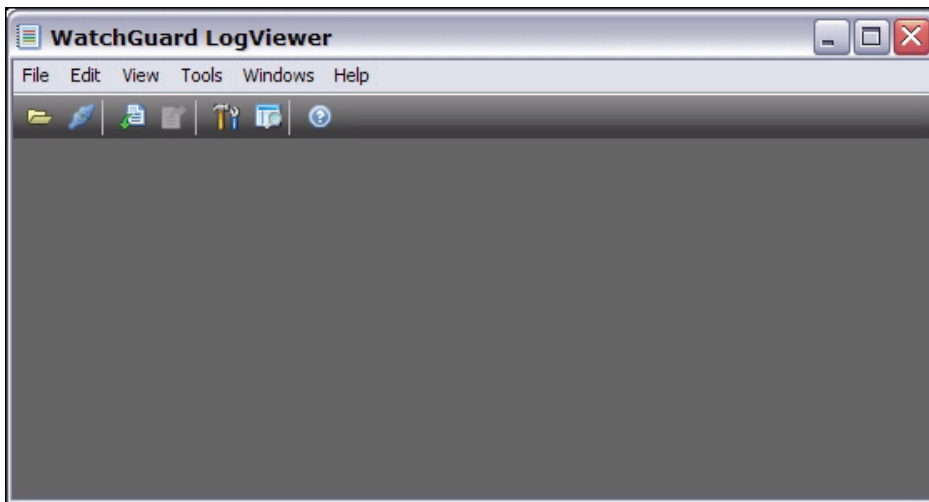
Depending on the size of the database, the operation can take from a few minutes to several hours to run. After the command finishes, restart the Log Server.

Use LogViewer to see log files

LogViewer is the WatchGuard System Manager tool you use to see log file data. It can show the log data page by page, or search and display by key words or specified log fields.

Open LogViewer

Click  on the WatchGuard System Manager toolbar.
Or, from WatchGuard System Manager, select **Tools > Logs > LogViewer**.
WatchGuard LogViewer appears.




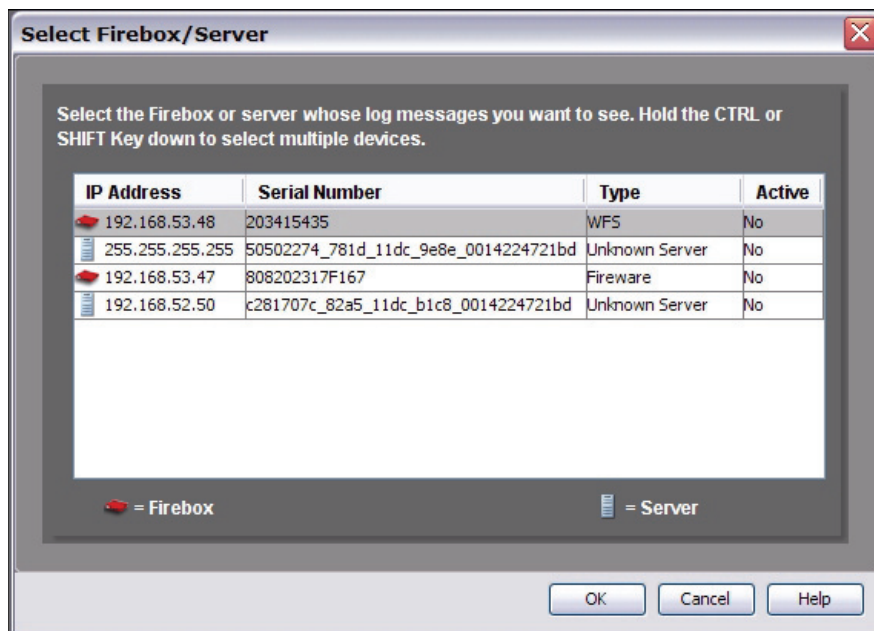
Connect to a device

You can connect to Firebox devices or to Log Servers. When you connect to a Firebox, you can filter the log data based on the type of log message, date and time, and string searches. When you connect to a Server, you can only filter the data by date and time, or simple text string searches.

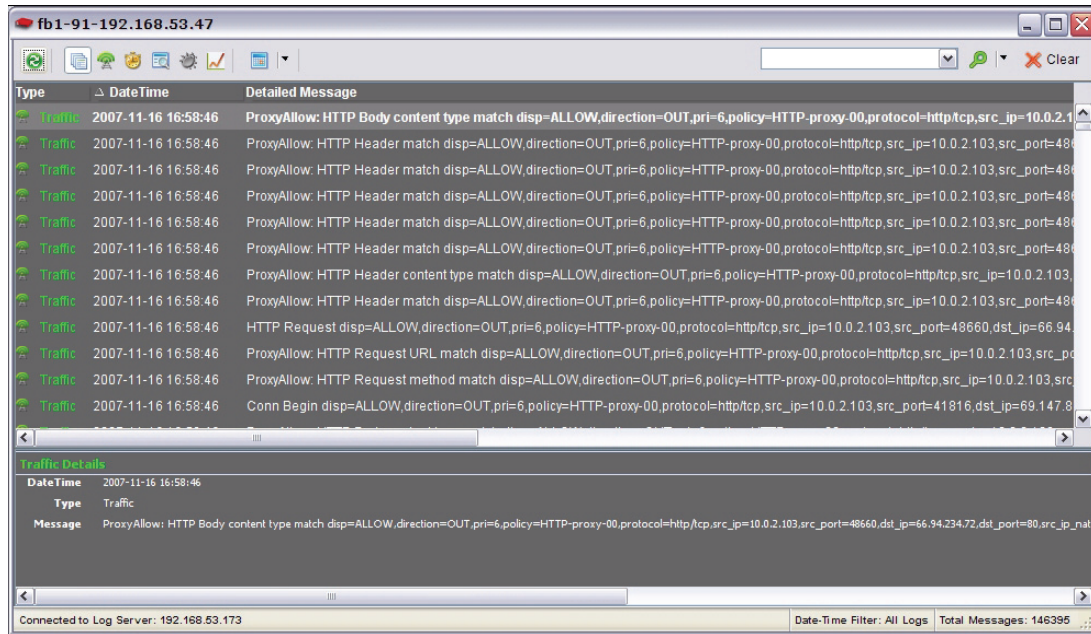
For more information about log message details, see [Set LogViewer user preferences](#) and [Log message details](#).

All WatchGuard servers share the same master passphrase.

1. Click  on the LogViewer toolbar.
Or, select **File > Connect** to connect to a Log Server.
The Connect to Log Server dialog box appears.
2. Type the IP address and passphrase for your Log Server. Click **OK**.
The Connect to Log Server dialog box disappears, and the Select Firebox/Server dialog box appears.



3. Select a Firebox or Log Server from the list and click **OK**.
You can select to connect to multiple devices at the same time.
A device window appears for each selected device. The IP address of the device appears in the window title bar. The contents for a Firebox device window and a Server window are different.



4. Select a log message to see more information about the message.
The selected log message details appear in the Details pane at the bottom of the device window.

If the details pane is not visible, select **View > Details Pane** to enable it.











For more information about displaying device data, see [Set LogViewer user preferences](#).

LogViewer toolbars





The main LogViewer toolbar includes icons to help you navigate the interface.

Icon	Name	Action
	Open Logs on Primary Log Server	Opens the log files on the primary Log Server without first connecting to the Log Server.
	Connect to Log Server	Connect to a Log Server.
	Import Data	Import data from an existing log into LogViewer.
	Export Selection	Export data from a selected log message into a database file.
	Local Diagnostics	Open the Local Diagnostics dialog box to run diagnostic tasks and review results.
	Search Manager	Open Search Manager to search logs for specific details.
	Help	Open LogViewer Help.

The LogViewer Firebox window toolbar includes icons to help you filter and refine your view of the log messages.

Icon	Name	Action
	Refresh	Update the selected log view with the latest data from the Log Server.
	All Logs	Display all logs for the selected device.
	Traffic	Display only traffic logs for the selected device.
	Alarms	Display only alarm logs for the selected device.
	Event	Display only event logs for the selected device.
	Debug	Display only debug logs for the selected device.
	Statistic	Display only statistics logs for the selected device.
	Date-Time Filter	Filter the selected data by date and time.
	Search logs for matches	Search the selected logs for specific details.
	Clear	Clear all applied filters.

The LogViewer Server window toolbar includes icons to help you filter the log messages.

Icon	Name	Action
	Refresh	Update the selected log view with the latest data from the Log Server.
	Date-Time Filter	Filter the selected data by date and time.
	Search logs for matches	Search the selected logs for specific details.
	Clear	Clear all applied filters.

Open logs for the Primary Log Server

If you have specified a Primary Log Server, you can open the log files for this server from the main LogViewer window without connecting to it first. You can then see the list of Firebox devices that are currently logging to the Primary Log Server. You must select a Primary Log Server to enable this option.

For more information about selecting a Primary Log Server, see [Set LogViewer user preferences](#).

To open logs for the primary Log Server:

Click  on the LogViewer toolbar.

Or, select **File > Open Logs For**.

The Select Firebox/Server dialog box appears with the list of connected devices displayed.

Set LogViewer user preferences

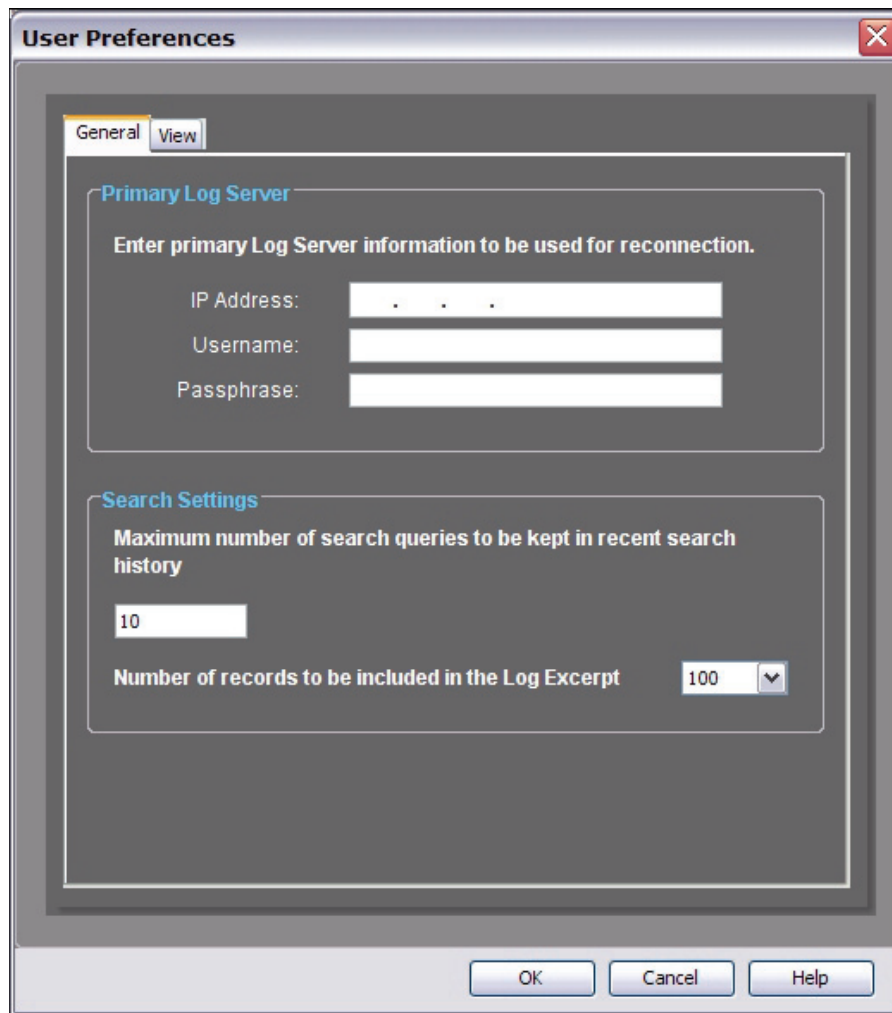
You can adjust the content and the format of the LogViewer window.

From LogViewer, select **View > Preferences**.

The User Preferences dialog box appears.

The **User Preferences** dialog box includes two tabs for configuring settings: **General** and **View**. The **General** tab includes options for setting a primary log server. The **View** tab includes options for configuring the log window settings and column settings for the different log message types.

General settings

The image shows the 'User Preferences' dialog box with the 'General' tab selected. The dialog has a title bar with 'User Preferences' and a close button. Inside, there are two tabs: 'General' and 'View'. The 'General' tab contains two sections. The first section, 'Primary Log Server', has a subtitle 'Enter primary Log Server information to be used for reconnection.' and three input fields: 'IP Address:' (with a dotted placeholder), 'Username:', and 'Passphrase:'. The second section, 'Search Settings', has a subtitle 'Maximum number of search queries to be kept in recent search history' and a text input field containing '10'. Below this is a label 'Number of records to be included in the Log Excerpt' followed by a spinner box set to '100'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

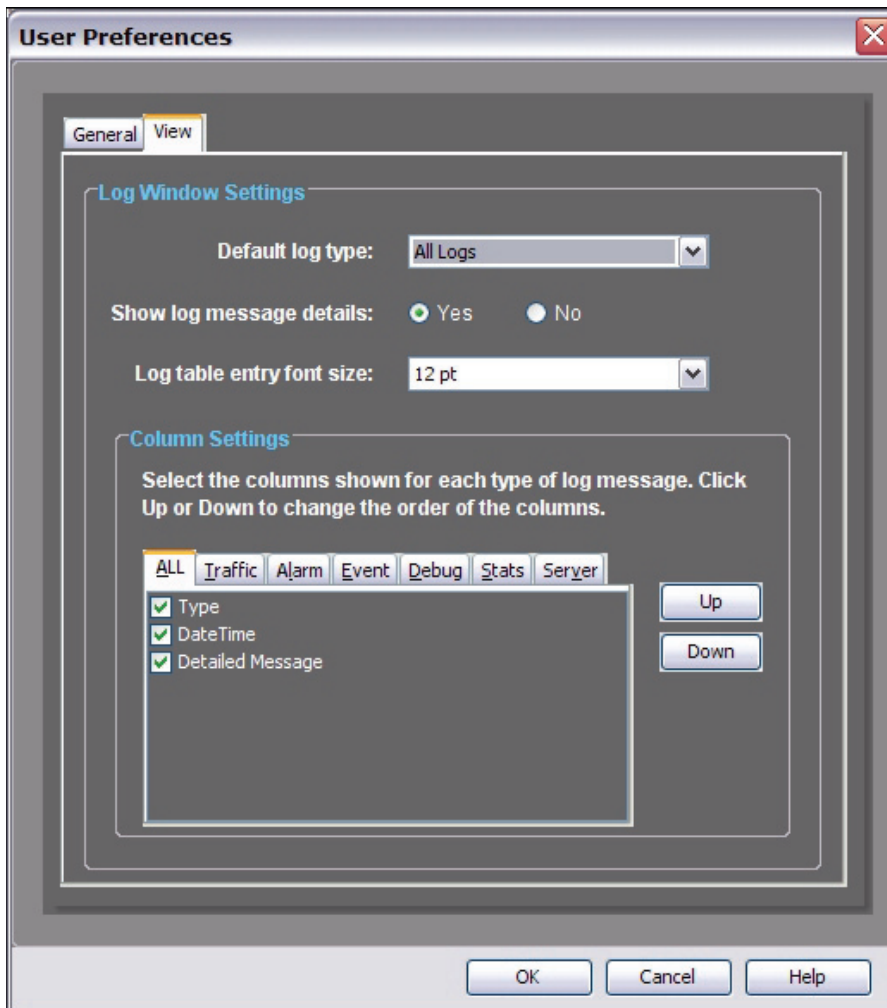
Primary Log Server

You can specify a log server to automatically reconnect to. Type the IP address, user name, and passphrase for the Log Server.

Search Settings

Type the maximum number of search queries to keep in your search history.

View settings



Default log type

Select which types of logs are automatically included when you review log messages.

Show log message details

Select to include or exclude message details in the log messages.

Log table entry font size

Select the font size you want to use for the log table entries from the drop-down list.

Column Settings

The **Column Settings** pane has a tab for each type of log message. Each tab includes a list of available details for that message type. Use these tabs to select which columns of details appear for each message type. You can also click **Up** or **Down** to change the order of the columns.

For more information about the available log message types, see [Log message details](#).

Log message details

You can select the details you see in each type of log message by the columns you select to include in the different types of log messages. The following is a complete list of all available columns. Not all columns will appear for all message types.

Log Message Column	Description
Additional Info	Additional details about the log message for proxy logs. For example: hostname, filename, rule_name, content_type.
Alarm ID	The number associated with the alarm.
Alarm Name	The category of the alarm (System, IPS, AV, Policy, Proxy, Probe, Denial of service, or Traffic).
Alarm Type	The type of alarm (email, popup).
Application Provider	The name of the server that provides the data.
Bytes Received	The number of bytes received by a device (WAN or Tunnel) within the statistics log period.
Bytes Sent	The number of bytes sent by a device (WAN or Tunnel) within the statistics log period.
Connection ID	The number of the server connection.
DateTime	The date and time on the server when the log message was received.
Destination Interface	The name of the destination interface.
Destination IP	The destination IP address for this packet.
Destination IP-NAT	The way NAT (network address translation) was handled for the destination IP address for this packet.
Destination Port	The destination port for this packet.
Destination Port-NAT	The way NAT (network address translation) was handled for the destination port for this packet.
Detailed Message	All the log message fields, comma-separated.
Device	The name of the device that sent out the performance log (WAN or Tunnel).
Direction	The direction of the action. Can be incoming or outgoing.
Disposition	The packet disposition. Can be deny or allow.
Message	The message field.
Message Code	The code for the message type.
Message Timestamp (s.ms)	The timestamp for the message in second.millisecond format.
Misc. Details	Additional details from the columns you selected to include for the log message type. For example: rc (return code), packet length, and TTL (packet time to live in seconds).
Policy	The name of the policy in Policy Manager that handled this packet.
Priority	The priority level of the log message.
Process ID	The ID for the process completed in the log message action.
Protocol	The protocol used in this packet.

Log Message Column	Description
Proxy Action	The name of the proxy action handling this packet. A proxy action is a set of rules for a proxy that can be applied to more than one policy.
Request ID	The ID for the server process requested in the log message.
Return Code	Return code for the packet.
Source Interface	The name you have given the source interface for this packet (as defined in Policy Manager).
Source IP	The source IP address of this packet.
Source IP-NAT	The way NAT (network address translation) was handled for the source IP address for this packet.
Source Port	The source port for this packet.
Source Port-NAT	The way NAT (network address translation) was handled for the source port for this packet.
Type	The type of log message. All logs include a log type in the message: "al" for alarms, "ev" for events, "db" for debug, "pe" for statistic logs, and tr for Traffic.

For information about selecting log message details, see [Set LogViewer user preferences](#).

For information about the different types of log messages, see [Types of log messages](#).

Use Search Manager

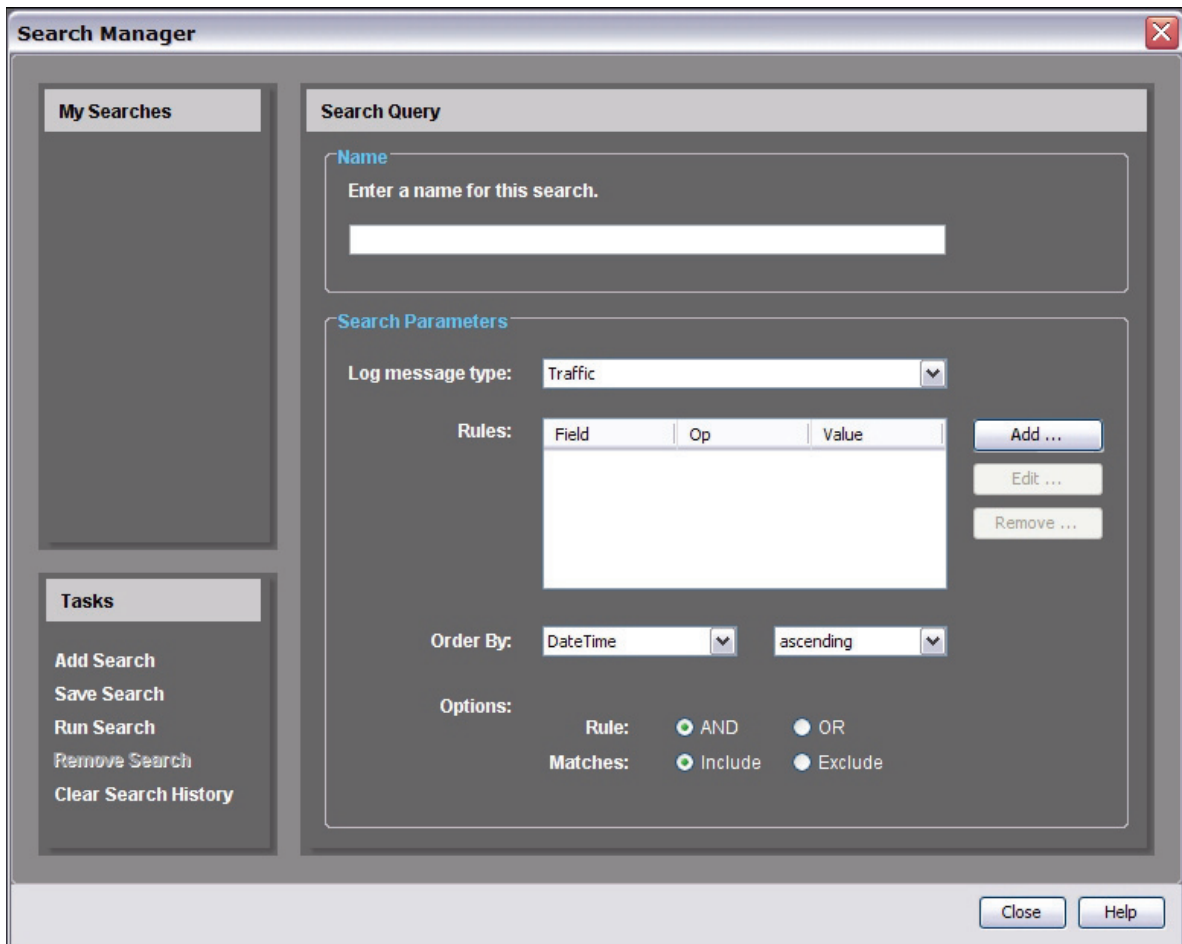
You can use the LogViewer Search Manager to create rules for searches and then search the data shown in LogViewer. You can create custom searches and save them so you can run them again and again. You can also remove or edit a saved search, and clear the search history.

Open Search Manager

Click .

Or, select **Tools > Search Manager**.

The Search Manager dialog box appears.



Create a Search Query

1. Click **Add Search** in the **Tasks** pane.
2. Type a name for your search in the **Name** field.
3. Select the **Search Parameters**.
For more information about search parameters, see [Search parameter settings](#).

Save a search

After you have created a search query you can save it so you can run it again.

Click **Save Search** in the **Tasks** pane.

The search name appears in the My Searches list.

Remove a search

When you no longer want to include a saved search in the My Searches list, you can remove it.

1. Select a search in the My Searches list. You can remove only one saved search at a time.
2. Click **Remove Search** in the **Tasks** pane.

The search name disappears from the My Searches list.

Edit a search

You can edit a saved search to change the search parameters.

1. Select the search name in the **My Searches** list.
The selected search name appears in the Name field.
2. Edit the search parameters.
3. Click **Save Search** in the **Tasks** pane.

The Save Search message appears.

Run a search

You can select to run a saved or a new search query.

To run a saved search:

1. Select a search name in the **My Searches** list.
2. Click **Run Search** in the **Tasks** pane.
The log messages that match the saved search query parameters appear in the LogViewer window.

To run a new Search Query:

1. Follow the steps under *Create a Search Query* to define the search query.
2. Click **Run Search** in the **Tasks** pane.
The log messages that match the saved search query parameters appear in the LogViewer window.

Clear the search history

You can remove all recent searches from the search history.

Click **Clear Search History** in the **Tasks** pane.

Search parameter settings

Select from the available options for each field to create a search query.

For more information about search queries, see [Use Search Manager](#).

Search Parameters

Log message type: Traffic

Rules:

Field	Op	Value

Add ...
Edit ...
Remove ...

Order By: DateTime ascending

Options:

Rule: ☒ AND ☐ OR

Matches: ☒ Include ☐ Exclude

Log message type

Select the type of log message that you want to search for.

- All logs
- Traffic
- Alarm
- Event
- Debug
- Statistic
- Server

Rules

Click **Add** to apply column, operator, and value rules to your search query.

- **Column** *Select a column to search in from the list.*
- **Operator**
Select the operation to apply: EQUAL TO, NOT EQUAL TO, CONTAINS.
- **Value**
Type a value for the operator to search on.

Order By

You can choose to display the results by any column that can be sorted and is available for the selected log type. You can choose to see the results in **ascending** or **descending** order.

Options

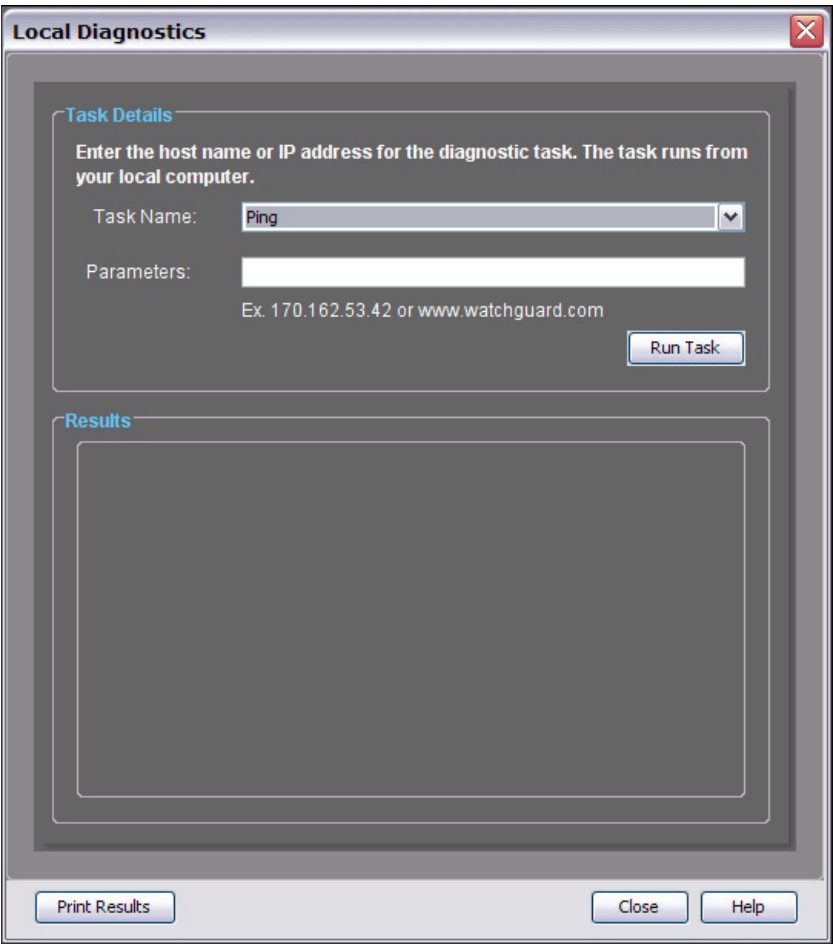
Rule — If you choose **AND**, only results that match all rules are displayed. If you choose **OR**, results that match any of the rules are displayed. If there is only one rule in your search, this setting does not apply.

Matches — Select whether the search query results **Include** or **Exclude** log messages that match the set parameters.

Run local diagnostic tasks

You can use LogViewer to run diagnostic tasks on any IP address or host. Diagnostic tasks include **Ping**, **Tracert**, or **NSLookup**.

1. Click .
Or, select **Tools > Local Diagnostics** and select a task.
The Local Diagnostics dialog box appears.

The image shows a 'Local Diagnostics' dialog box. It has a title bar with a close button. Inside, there's a 'Task Details' section with instructions: 'Enter the host name or IP address for the diagnostic task. The task runs from your local computer.' Below this is a 'Task Name' dropdown menu currently set to 'Ping', and a 'Parameters' text input field. An example text 'Ex. 170.162.53.42 or www.watchguard.com' is shown below the parameters field. A 'Run Task' button is at the bottom right of the 'Task Details' section. Below this is a large 'Results' section, which is currently empty. At the bottom of the dialog box are three buttons: 'Print Results', 'Close', and 'Help'.

2. Select a task in the **Task name** drop-down list.


Task	Action
Ping	Make sure an IP address or host is active
Tracert	Trace the route to the IP address or host and see the route transfer time.
NSLookup	Verify the server name and actual IP address of the selected IP address or host.

3. Type an IP address or host name in the **Parameters** field.
4. Click **Run Task**.
The task results appear in the **Results** field.
5. To print the task results, click **Print Results**.
The Print dialog box appears.
6. Select the print parameters and click **Print**.

Import and export data to LogViewer


You can use LogViewer to see data from existing database log files or to export selected data to a database file.

Import data

1. On the LogViewer toolbar, click .
Or, select **File > Import Data**.
The Import Data dialog box appears.
2. Browse to select a database file.
3. Click **Import**.
The selected data appears in a new Server window.

For more information about LogViewer Server windows, see [Use LogViewer to see log files](#).

Export data

1. Select the log messages to export in the LogViewer Firebox or Server window.
2. On the LogViewer toolbar, click .
Or, select **File > Export Selected Data**.
The Export Selected Data dialog box appears with the default file name displayed in the File name field.
3. Browse to select a directory where you want to save the database file.
4. If necessary, type a new name for the database file in the **File name** field.
5. Click **Export**.
The database file is saved to the selected directory.

Email, print, or save log messages

After you select one or more log messages in LogViewer, you can email, print, or save them.

Send a log message in email

Select **File > Send Selection As** and select from the following options:

- Comma Separated Values (*.csv)
- Portable Document Format (*.pdf)

An email message opens with the log message attached in the selected file format.

Print a log message

1. Select **File > Print Selection**.
The Print dialog box appears.
2. Select a printer and the print parameters, and click **Print**.

Save a log message

1. Select **File > Save Selection as >** and select from the following options:
Comma Separated Values (*.csv)
Web Page (*.htm, *.html)
Portable Document Format (*.pdf)
Extensible Markup Language (*.xml)
The Save dialog box appears.
2. Select a location and type a file name. Click **Save**.

9

Network Setup and Configuration

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 Interfaces

Used for interfaces that connect to a WAN and can have a static or dynamic IP address. For more information on external interfaces and how to configure them, see [Configure external interfaces](#).

Trusted Interfaces

Connects to the private LAN (local area network) or internal network that you want to secure. To configure trusted interfaces, see [Configure Firebox interfaces](#).

Optional Interfaces

Optional interfaces are mixed-trust or DMZ environments that are separate from your trusted network. Examples of computers often found on an optional interface are public web servers, FTP servers, and mail servers. To configure optional interfaces, see [Configure Firebox interfaces](#).

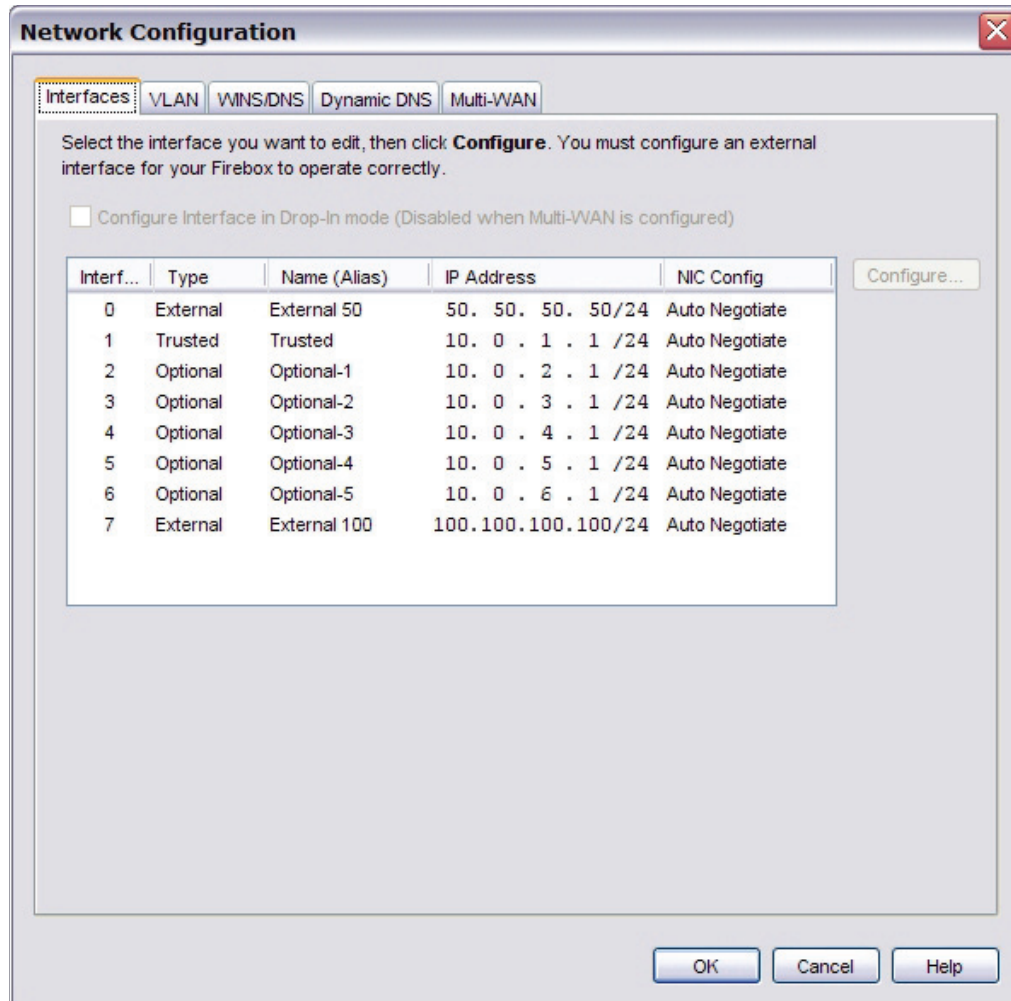
You can add other components and functionality to your network:

- [Add a static route](#)
- [Configure the Firebox as a DHCP server](#)
- [Configure a secondary network](#)
- [Use DHCP relay agents](#)
- [Set advanced interface settings](#)
- [Define a virtual local area network \(VLAN\)](#)
- [About network configuration in drop-in mode](#)

When you configure the interfaces on a Firebox, you must use [slash notation](#) to denote the subnet mask. For example, you would enter the network range 192.168.0.0 subnet mask 255.255.255.0 as 192.168.0.0/24. A trusted interface with the IP address of 10.0.1.1/16 has a subnet mask of 255.255.0.0.

Configure Firebox interfaces

1. From Policy Manager, select **Network > Configuration**.
The Network Configuration dialog box appears.



2. Select the interface you want to configure. Click **Configure**.
The *Interface Settings* dialog box appears.

Interface Settings - Interface # 1

General Secondary Advanced

Interface Name (Alias): Trusted

Interface Description:

Interface Type: Trusted

IP Address: 10.0.1.1/24

☐ Disable DHCP

☒ Use DHCP Server

Address Pool:

Starting IP	Ending IP

Add Edit Delete

Reserved Addresses:

Reservation Name	Reserved IP	MAC Address

Add Edit Delete

DNS Servers: (If not defined, use the Network DNS Servers)

Domain Name:

--

Add Edit Delete

Leasing Time: 8 hours

☐ User DHCP Relay

IP Address (for all DHCP Relay enabled interfaces and VLANs):

OK Cancel Help

3. In the **Interface Name (Alias)** field, you can retain the default name or change it to one that more closely reflects your own network and its own trust relationships.
Make sure the name is unique among interface names as well as all MUVPN group names and tunnel names.
4. (Optional) Enter a description of the interface in the **Interface Description** field.
5. In the **Interface Type** field, you can change the interface type from its default value.

6. You can change the interface IP address. Type the IP address in slash notation. When you type an IP address, type all the numbers and the periods. Do not use the TAB or arrow key.
7. If you are configuring a trusted or optional interface, select **Disable DHCP**, **Use DHCP Server**, or **Use DHCP Relay**.
See [Configure the Firebox as a DHCP server](#), and see [Make the Firebox a DHCP relay agent](#) for the DHCP relay option. If you are configuring the external interface, see [Configure external interfaces](#).
8. Click **OK**.

Configure the Firebox as a DHCP server

You can configure the Firebox as a DHCP server for networks behind the Firebox.

If you have a configured DHCP server, we recommend that you continue to use that server for DHCP.



You cannot use this option on any interface in which High Availability is enabled.

1. Select **Network > Configuration**.
The Network Configuration dialog box appears.

Network Configuration

Interfaces | VLAN | WINS/DNS | Dynamic DNS | Multi-WAN

Select the interface you want to edit, then click **Configure**. You must configure an external interface for your Firebox to operate correctly.

☐ Configure Interface in Drop-In mode (Disabled when Multi-WAN is configured)

Interf...	Type	Name (Alias)	IP Address	NIC Config
0	External	External 50	50. 50. 50. 50/24	Auto Negotiate
1	Trusted	Trusted	10. 0 . 1 . 1 /24	Auto Negotiate
2	Optional	Optional-1	10. 0 . 2 . 1 /24	Auto Negotiate
3	Optional	Optional-2	10. 0 . 3 . 1 /24	Auto Negotiate
4	Optional	Optional-3	10. 0 . 4 . 1 /24	Auto Negotiate
5	Optional	Optional-4	10. 0 . 5 . 1 /24	Auto Negotiate
6	Optional	Optional-5	10. 0 . 6 . 1 /24	Auto Negotiate
7	External	External 100	100.100.100.100/24	Auto Negotiate

Configure...

OK Cancel Help

2. Select the trusted or an optional interface.

- Click **Configure** and select the **Use DHCP Server** check box.

Interface Settings - Interface # 1

General Secondary Advanced

Interface Name (Alias): Trusted

Interface Description:

Interface Type: Trusted

IP Address: 10.0.1.1/24

☐ Disable DHCP

☒ Use DHCP Server

Address Pool:

Starting IP	Ending IP

Add Edit Delete

Reserved Addresses:

Reservation Name	Reserved IP	MAC Address

Add Edit Delete

DNS Servers: (If not defined, use the Network DNS Servers)

Domain Name:

Add Edit Delete

Leasing Time: 8 hours

☐ User DHCP Relay

IP Address (for all DHCP Relay enabled interfaces and VLANs):

OK Cancel Help

- Add an address pool. Click **Add** next to the **Address Pool** box and specify starting and ending IP addresses on the same subnet. Click **OK**.
The address pool must belong either to the interface's primary or secondary IP subnet.
You can configure a maximum of six address ranges.
- To reserve a specific IP address for a client, click **Add** next to the **Reserved Addresses** box. Enter a name for the reservation, the IP address you want to reserve, and the MAC address of the client's network card. Click **OK**.

6. By default, the Firebox gives out the DNS server information configured on the **Network Configuration > WINS/DNS** tab when it is configured as a DHCP server. If you want, you can specify a different DNS server for the Firebox to assign when it gives out IP addresses. Click **Add** next to the **DNS servers** box to add the IP address of the DNS server you want the Firebox to use.
7. Use the arrow buttons to change the **Default Lease Time**. This is the time interval that a DHCP client can use an IP address that it receives from the DHCP server. When the time is near its limit, the client sends data to the DHCP server to get a new lease.

Make the Firebox a DHCP relay agent

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.

You can use this feature only if you set up the Firebox in a drop-in configuration. For more information, see [Drop-in configuration](#).



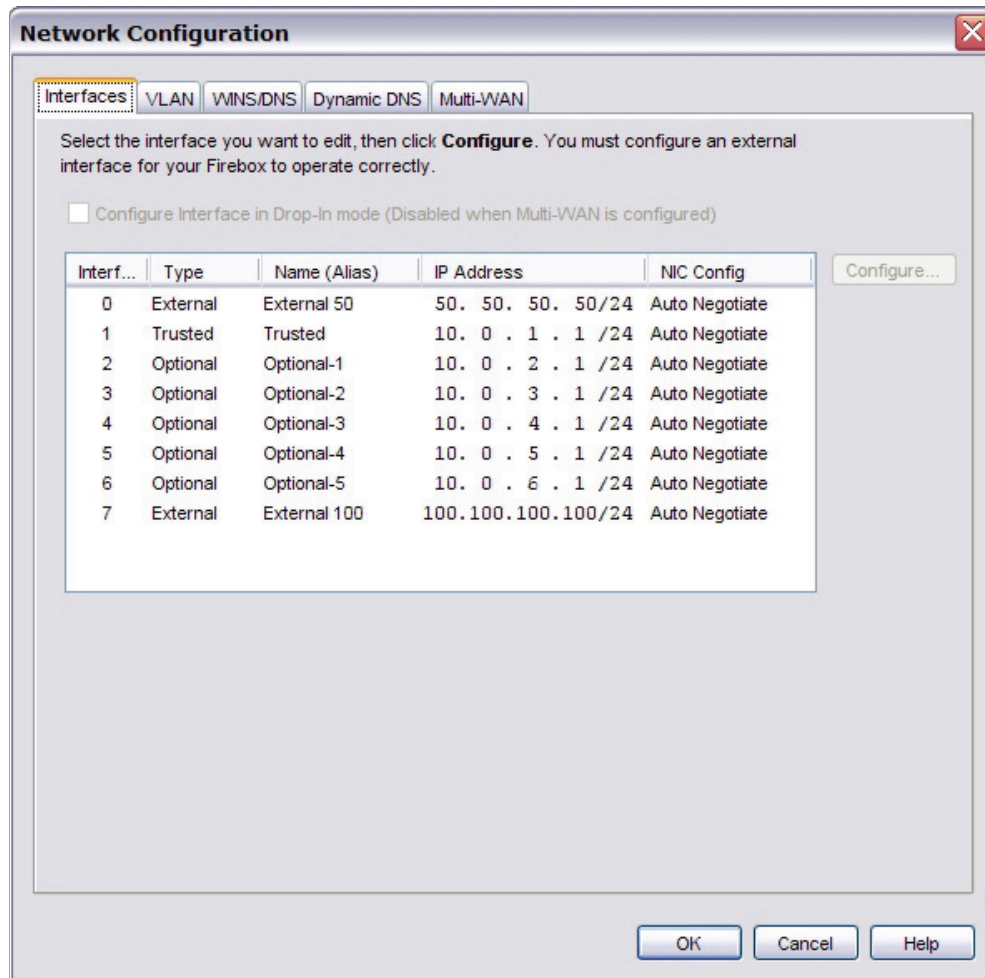
You cannot use DHCP Relay on any interface in which High Availability is enabled.

1. Select **Network > Configuration**.
The Network Configuration dialog box appears.
2. Select the trusted or an optional interface.
3. Click **Configure** and click **Use DHCP Relay**.
4. Type the IP address of the DHCP server in the related field. Make sure to add a route to the DHCP server, if necessary.
5. Click **OK** and save your changes to the Firebox.

Disable an interface

1. From Policy Manager, select **Network > Configuration**.

The Network Configuration dialog box appears.



2. Select the interface you want to disable. Click **Configure**.
The *Interface Settings* dialog box appears.

Interface Settings - Interface # 1

General Secondary Advanced

Interface Name (Alias): Trusted

Interface Description:

Interface Type: Trusted

IP Address: 10.0.1.1/24

☐ Disable DHCP

☒ Use DHCP Server

Address Pool

Starting IP	Ending IP

Add Edit Delete

Reserved Addresses:

Reservation Name	Reserved IP	MAC Address

Add Edit Delete

DNS Servers: (If not defined, use the Network DNS Servers)

Domain Name:

--

Add Edit Delete

Leasing Time 8 hours

☐ User DHCP Relay

IP Address (for all DHCP Relay enabled interfaces and VLANs):

OK Cancel Help

3. From the **Interface Type** drop-down list, select **Disabled**. Click **OK**.
In the **Network Configuration** dialog box, the interface now appears as type **Disabled**.

Configure external interfaces

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](#).

If the IP address is static

1. Select **Network > Configuration**.
The Network Configuration dialog box appears.
2. Select an external interface. Click **Configure**.
3. From the **Interface Settings** dialog box, select **Static**.
4. Type the IP address of the interface.
5. Type the IP address of the default gateway.
6. Click **OK**.

The screenshot shows a configuration window titled 'Use Static IP'. It contains two input fields: 'IP Address' with the value '50.50.50.10/24' and 'Default Gateway' with the value '50.50.50.1'. Both fields have dropdown arrows on the right side.

If the IP address is assigned through PPPoE

If your ISP uses PPPoE, you must enter the PPPoE information into your Firebox before it can send traffic through the external interface.

1. Select **Network > Configuration**.
The Network Configuration dialog box appears.
2. Select an external interface. Click **Configure**.
3. From the **Interface Settings** dialog box, select **PPPoE**.
4. If you selected **Use IP Address**, enter the IP address in the text box to the right.
5. Type the **User Name** and **Password**. You must type the password two times.
Frequently, ISPs use the email address format for user names, such as myname@ispdomain.net.

The screenshot shows a configuration window titled 'Use PPPoE'. It has two radio buttons: 'Obtain an IP address automatically' (which is selected) and 'Use IP address:'. Below these are three text input fields labeled 'User Name:', 'Password:', and 'Reenter Password:'. At the bottom right, there is a button labeled 'Advanced Properties...'.

6. Click **Advanced Properties** to configure PPPoE parameters. The *PPPoE Properties* dialog box appears. Your ISP can tell you if it is necessary to change the timeout or LCP values.

PPPoE Properties

Connection Settings

☒ Always-on

PPPoE initialization retry every seconds

☐ Dial-on-demand

Idle timeout in minutes

Retry Settings

LCP echo failure in tries

LCP echo timeout in seconds

Authentication Settings

Service Name:

Access Concentrator Name:

OK Cancel Help

7. Use the radio buttons to select when the Firebox connects with the PPPoE server. If you selected **Always On**, in the **PPPoE Initialization Retry Interval** field, use the arrows to set the number of seconds that PPPoE tries to initialize before it times out. If you selected **Dial-on-Demand**, in the **Idle Timeout** in field, set the length of time the user can stay connected when idle (not passing any traffic to the external network).
8. In the **LCP echo failure** in field, use the arrows to set the number of failed LCP echo requests allowed before the PPPoE connection is considered inactive and closed.
9. In the **LCP echo timeout** in field, use the arrows to set the length of time, in seconds, that the response to each echo timeout must be received.
10. In the **Service Name** field, type a PPPoE service name. This is either an ISP name or a class of service that is configured on the PPPoE server. 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.
11. In the **Access Concentrator Name** field, enter the name of a PPPoE access concentrator, also known as a PPPoE server. Usually, this option is not used. Use it only if you know there is more than one access concentrator.

If the IP address is assigned through DHCP

1. From the **Interface Settings** dialog box, select **Use DHCP Client**.
2. If your DHCP server makes you use an optional identifier in your DHCP exchange, type this identifier in the **Host Name** text box.

The screenshot shows a configuration window titled "Use DHCP Client". It contains a "Host Name" text input field. Below it is a "Host IP" section with two radio buttons: "Obtain an IP automatically" (which is selected) and "Use IP address:" (which is unselected). To the right of the "Use IP address:" radio button is a text input field. At the bottom, there is a "Leasing Time" section with a checkbox and a dropdown menu currently showing "8 hours".

3. Below **Host IP**, select the **Obtain an IP automatically** radio button if you want DHCP to assign an IP address to the Firebox. If you want to manually assign an IP address and use DHCP just to give this assigned address to the Firebox, select the **Use IP address** radio button and enter the IP address in the adjacent field.
4. IP addresses assigned by a DHCP server have a one-day lease, which means the address is valid for one day. If you want to change the leasing time, select the **Leasing Time** check box and select the value in the field adjacent to the check box.

Set up the Firebox for dynamic DNS

You can register the external IP address of the Firebox with the dynamic Domain Name Server (DNS) service called Dynamic Network Services (DynDNS). This is a free service for a maximum of five host names. (The Firebox does not support any other dynamic DNS providers.)

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.

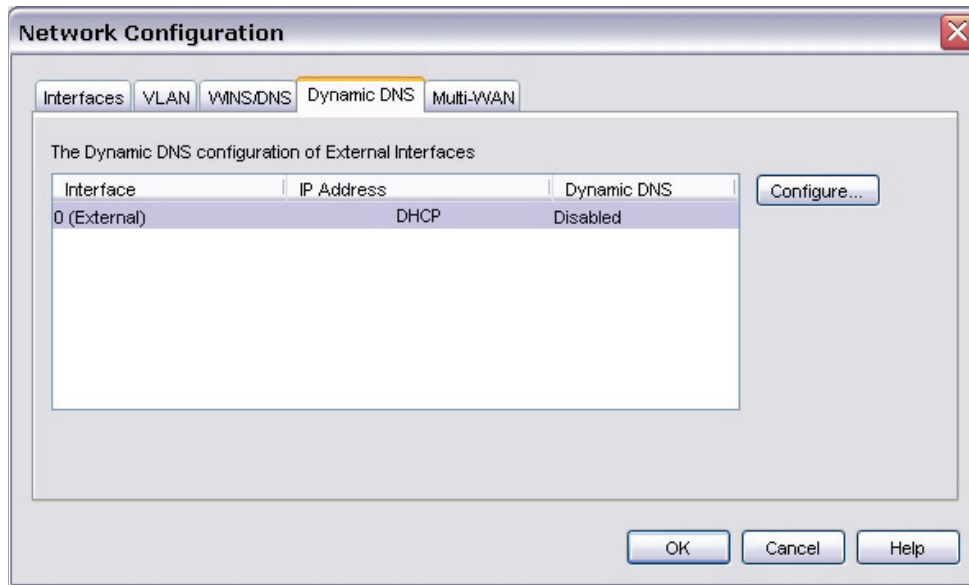
For more information on dynamic DNS, go to <http://www.dyndns.com>



WatchGuard is not affiliated with DynDNS.com.

1. Set up a dynDNS account. To set up your account, go to the DynDNS web site and follow the instructions on the site <http://www.dyndns.com>.
2. From Policy Manager, select **Network > Configuration**. Click the **WIN/DNS** tab.
3. Make sure you have defined at least one DNS server. If you have not, use the procedure in [Add WINS and DNS Server Addresses](#).
4. Click the **Dynamic DNS** tab.

5. Select the external interface you want to configure dynamic DNS for and click **Configure**.
The *Per Interface Dynamic DNS* dialog box appears.



6. To enable dynamic DNS, select the **Enable Dynamic DNS** check box.
7. Type the user name, password, and domain name you used to set up your dynamic DNS account.
8. In the **Service Type** drop-down list, select the system to use for this update. For more information on each option, see <http://www.dyndns.com/services/>:
 - o dyndns sends updates for a Dynamic DNS host name.
 - o statdns sends updates for a Static DNS host name.
 - o custom sends updates for a Custom DNS host name.
9. In the **Options** field, you can type any of the options shown below. You must type an & character before and after each option you add. If you add more than one option, you must separate the options with the & character.
 For example: &backmx=NO&wildcard=ON&
 mx=mailexchanger
 backmx=YES|NO
 wildcard=ON|OFF|NOCHG
 offline=YES|NO
 For more information on options, see <http://www.dyndns.com/developers/specs/syntax.html>.
10. Use the arrows to set a time interval, in days, to force an update of the IP address.

Add WINS and DNS server addresses

A number of the features of the Firebox have shared Windows Internet Name Server (WINS) and Domain Name System (DNS) server IP addresses. These features include DHCP and Mobile VPN. Access to these servers must be available from the trusted interface of the Firebox.

This information is used for two purposes:

- The Firebox uses the DNS server shown here to resolve names to IP addresses for IPSec VPNs and for the spamBlocker, Gateway AV, and IPS features to operate correctly.
- The WINS and DNS entries are used by DHCP clients on the trusted or optional networks, and Mobile VPN users to resolve DNS queries.

Make sure that you use only an internal WINS and DNS server for DHCP and Mobile VPN. This helps to make sure that you do not create policies that have configuration properties that prevent users from connecting to the DNS server.

1. From Policy Manager, select **Network > Configuration**. Click the **WINS/DNS** tab.
The information on the WINS/DNS tab appears.

The screenshot shows the 'Network Configuration' dialog box with the 'WINS/DNS' tab selected. The dialog has a title bar with a close button. Below the title bar are five tabs: 'Interfaces', 'VLAN', 'WINS/DNS' (which is highlighted with a yellow border), 'Dynamic DNS', and 'Multi-WAN'. The main content area is divided into two sections. The first section is titled 'DNS (Domain Name System) Servers' and contains a 'Domain Name:' text box and three 'DNS Servers:' text boxes, each with a placeholder '. . .'. The second section is titled 'WINS (Windows Internet Naming Service) Servers' and contains two 'WINS Servers:' text boxes, each with a placeholder '. . .'. At the bottom right of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

2. Type the primary and secondary addresses for the WINS and DNS servers. You can specify up to three DNS servers. You can also type a domain suffix in the **Domain Name** text box for a DHCP client to use with unqualified names such as watchguard_mail.

Configure a secondary network

A secondary network is a network that shares one of the same physical networks as one of the Firebox interfaces. When you add a secondary network, you make (or add) an IP alias to the interface. This IP alias is the default gateway for all the computers on the secondary network. The secondary network tells the Firebox that there is one more network on the Firebox interface.

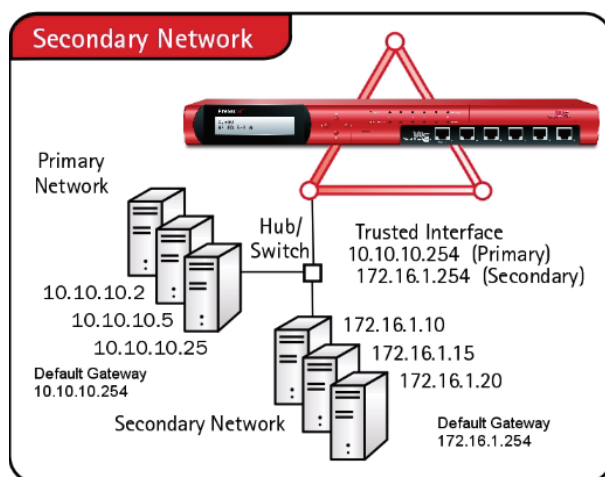
For example, if you configure a Firebox in drop-in mode, you give each Firebox interface the same IP address. However, you probably use a different IP address scheme on your trusted network. You can add this private network as a secondary network to the trusted interface of your Firebox. When you add a secondary network, you make a route from an IP address on the secondary network to the IP address of the Firebox interface.

If your Firebox is configured with a static IP address, you can add an IP address on the same subnet as your primary external interface as a secondary network. You can then configure static NAT for more than one of the same type of server. For example, configure an external secondary network with a second public IP address if you have two public SMTP servers and you want to configure a static NAT rule for each.

You can add up to 255 secondary networks per Firebox interface. You can use secondary networks with either a drop-in or a routed network configuration. You can also add a secondary network to the external interface of a Firebox if the external interface is configured to get its IP address through PPPoE or DHCP.

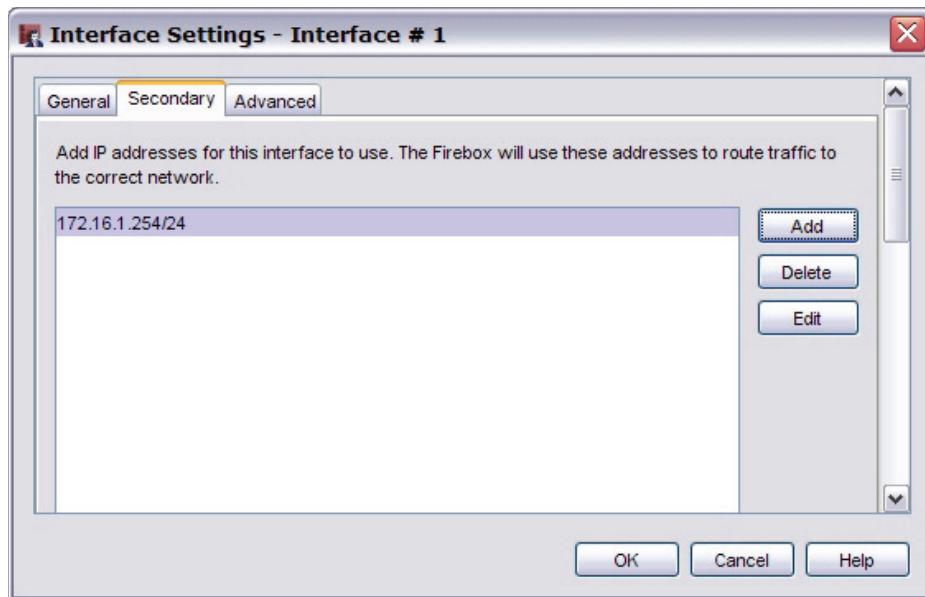
To define a secondary IP address, you must have an:

- Unused IP address from the secondary network to assign to the Firebox interface it connects to
- Unused IP address from the same network as the Firebox external interface



1. Select **Network > Configuration**.
The Network Configuration dialog box appears.
2. Select the interface for the secondary network and click **Configure**.
The Interface Settings dialog box appears.
3. Select the **Secondary** tab.

- Click **Add**. Type an unassigned IP address from the secondary network.
When you type IP addresses, type all the numbers and the stops. Do not use the TAB or arrow key.



- Click **OK**. Click **OK** again.



Be careful to add secondary network addresses correctly. The Firebox does not tell you if the address is correct. We recommend that you do not create a subnet as a secondary network on one interface that is a component of a larger network on a different interface. If you do this, spoofing can occur and the network cannot operate correctly.

Add a static route

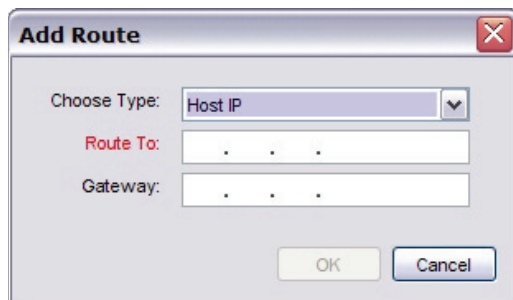
A *route* is the sequence of devices through which network traffic must go to get from its source to its destination. A *router* is the device in a route that finds the subsequent network point through which to send the network traffic to its destination. Each router is connected to a minimum of two 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. Add a network route if you have a full network behind a router on your local network. If you do not add a route to a remote network, all traffic to that network is sent to the Firebox default gateway.

Before you start, you must understand the difference between a network route and a host route. A network route is a route to a full network behind a router located on your local network. Use a host route if there is only one host behind the router, or if you want traffic to go to only one host.

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

1. From Policy Manager, select **Network > Routes**.
The Setup Routes dialog box appears.
2. Click **Add**.
The Add Route dialog box appears.



3. From the drop-down list, select **Network IP** if you have a full network behind a router on your local network.
Select **Host IP** if only one host is behind the router or you want traffic to go to only one host.
4. In the **Route To** text box, type the network address or host address, depending on whether you want to create a route to a network or a host. If you type a network address, use slash notation.
For more information about slash notation, see [About slash notation](#).
5. In the **Gateway** text box, type the IP address of the router. Make sure that you enter an IP address that is on one of the same networks as the Firebox.
6. Click **OK** to close the **Add Route** dialog box.
The Setup Routes dialog box shows the configured network route.
7. Click **OK** again to close the **Setup Routes** dialog box.

About advanced interface settings

You can use several advanced settings for Firebox interfaces:

Network Interface Card (NIC) settings: Configures the speed and duplex parameters for Firebox interfaces to automatic or manual configuration. We recommend you keep the link speed configured for automatic negotiation. If you use the manual configuration option, you must make sure the device the Firebox connects to is also manually set to the same speed and duplex parameters as the Firebox. Use the manual configuration option only when you must override the automatic Firebox interface parameters to operate with other devices on your network.

Outgoing Interface Bandwidth: Makes sure, when you use Traffic Management settings to guarantee bandwidth to policies, that you do not guarantee more bandwidth than actually exists for an interface. This setting also helps you make sure the sum of guaranteed bandwidth settings does not fill the link such that non-guaranteed traffic cannot pass.

QoS Marking: Creates different classifications of service for different kinds of network traffic. You can set the default marking behavior as traffic goes out of an interface. These settings can be overridden by settings defined for a policy.

DF bit for IPSec: Determines the setting of the Don't Fragment (DF) bit for IPSec.

PMTU Setting for IPSec: (External interfaces only) Controls the length of time that the Firebox lowers the MTU for an IPSec VPN tunnel when it gets an ICMP Request to Fragment packet from a router with a lower MTU setting on the Internet.

Static MAC/IP address binding: Controls access to a Firebox interface by computer hardware (MAC) address.

Network Interface Card (NIC) settings

1. Select **Network > Configuration**. Click the interface you want to configure, and then click **Configure**.
2. Select the **Advanced** tab.



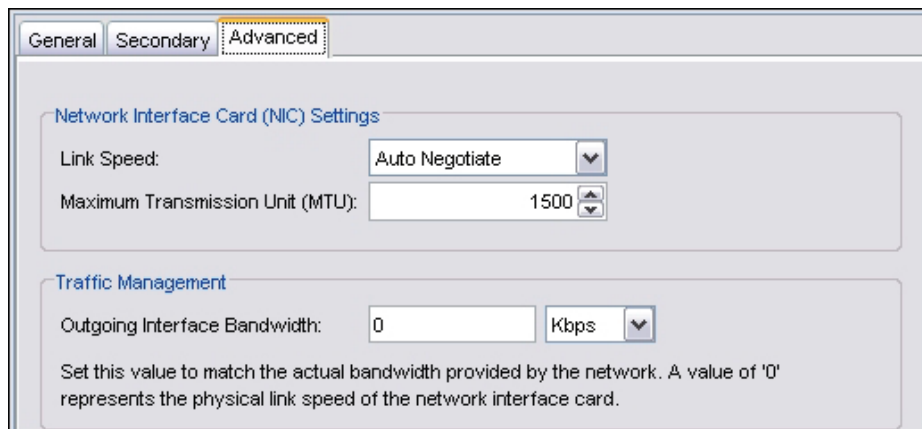
3. From the **Link Speed** drop-down list, select **Auto Negotiate** if you want the Firebox to select the best network speed. You can also select one of the half-duplex or full-duplex speeds that you know is compatible with your equipment.
We strongly recommend that you do not change this setting unless 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 your Firebox interface to reconnect.
4. 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.

Set Outgoing Interface Bandwidth

Before you use Traffic Management features, you must give each interface a bandwidth limit, known as Outgoing Interface Bandwidth, for traffic sent from that interface to the network segment to which it is connected. After you set this limit, Fireware will refuse packets that exceed the limit. Also, Policy Manager gives a warning if you allocate too much bandwidth as you create or adjust traffic management actions.

If you keep the Outgoing Interface Bandwidth setting for any interface at its default value of 0, it is set to the auto-negotiated link speed for that interface.

1. From Policy Manager, select **Setup > Global Settings**.
The Global Settings dialog box appears.
2. At the bottom of the dialog box, make sure the **Disable all traffic management and QoS features** check box is cleared. If it is not, clear it.
3. Click **OK**.
You might want to disable these features at a later time if you do performance testing or network debugging.
4. From Policy Manager, select **Network > Configuration**.
The Network Configuration dialog box appears.
5. Select the interface for which you want to set bandwidth limits and click **Configure**.
The Interface Settings dialog box appears.
6. Click the **Advanced** tab.



The screenshot shows the 'Advanced' tab of the 'Interface Settings' dialog box. It contains two sections: 'Network Interface Card (NIC) Settings' and 'Traffic Management'. In the NIC section, 'Link Speed' is set to 'Auto Negotiate' and 'Maximum Transmission Unit (MTU)' is set to '1500'. In the Traffic Management section, 'Outgoing Interface Bandwidth' is set to '0' Kbps. A note below states: 'Set this value to match the actual bandwidth provided by the network. A value of '0' represents the physical link speed of the network interface card.'

7. In the **Outgoing Interface Bandwidth** field, enter the amount of bandwidth provided by the network. Use your Internet connection upload speed (in Kbps rather than KBps) as the limit for external interfaces. Set your LAN interface bandwidth based on the minimum link speed supported by your LAN infrastructure.

Enable QoS Marking for an interface

Use this procedure to set the default marking behavior as traffic goes out of an interface. These settings can be overridden by settings defined for a policy.

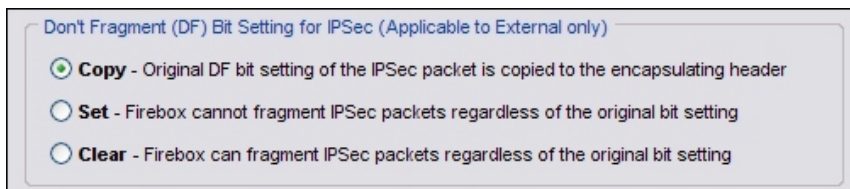
1. From Policy Manager, select **Setup > Global Settings**.
The Global Settings dialog box appears.
2. At the bottom of the dialog box, clear the **Disable all traffic management and QoS features** check box and click **OK**.
You might want to disable these features at a later time if you do performance testing or network debugging.
3. From Policy Manager, select **Network > Configuration**.
The Network Configuration dialog box appears.
4. Select the interface for which you want to enable QoS Marking and click **Configure**.
The Interface Settings dialog box appears.
5. Click the **Advanced** tab.

The screenshot shows the 'Advanced' tab of the 'Interface Settings' dialog box. It contains three main sections: 'Network Interface Card (NIC) Settings', 'Traffic Management', and 'QoS'. In the 'QoS' section, 'Marking Type' is set to 'IP Precedence', 'Marking Method' is set to 'Preserve', and 'Value' is set to '0 (Normal)'. There is an unchecked checkbox labeled 'Prioritize traffic based on QoS Marking'.

6. From the **Marking Type** drop-down list, select either **DSCP** or **IP Precedence**.
7. Set the marking method:
 - o **Preserve**: Do not change the bit's current value. The Firebox prioritizes the traffic based on this value.
 - o **Assign**: Assign the bit a new value.
 - o **Clear**: Clear the bit (set it to zero).
8. If you selected **Assign** in the previous step, select a marking value. If you chose the IP precedence marking type you can select values from 0 (normal priority) through 7 (highest priority). If you selected the DSCP marking type, the values are 0 - 56.
For more information on these values, see [Marking types and values](#).
9. Select the **Prioritize traffic based on QoS Marking** check box.
10. Click **OK**.

Set DF bit for IPSec

When you configure the external interface, select one of three radio buttons to determine the setting of the Don't Fragment (DF) bit for IPSec.



Don't Fragment (DF) Bit Setting for IPSec (Applicable to External only)

- ☒ **Copy** - Original DF bit setting of the IPSec packet is copied to the encapsulating header
- ☐ **Set** - Firebox cannot fragment IPSec packets regardless of the original bit setting
- ☐ **Clear** - Firebox can fragment IPSec packets regardless of the original bit setting

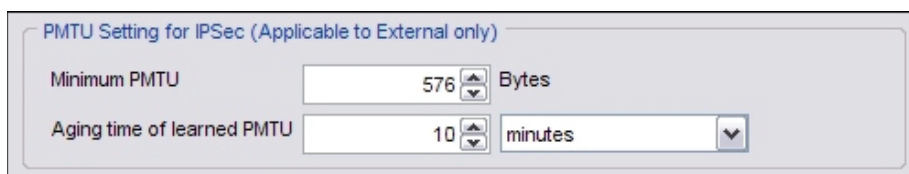
Copy: The Type of Service (TOS) bits are a set of four-bit flags in the IP header that can tell routing devices to give an IP datagram more or less priority than other datagrams. Fireware gives you the option to allow IPSec tunnels to pass TOS flagged packets. Some ISPs drop all packets that have TOS flags set. When the **Copy** check box is selected, if the original packet has TOS bits set, then Fireware keeps the TOS bits set when it encapsulates the packet in an IPSec header. If the original packet does not have the TOS bits set, Fireware does not set the TOS bits when it encapsulates the packet in an IPSec header. If you do not select the **Copy** check box, all IPSec packets have no TOS bits set. If the TOS bits were set before, when Fireware encapsulates the packet in an IPSec header, the TOS bits are cleared.

Set: Select **Set** to prevent the Firebox from fragmenting the frame regardless of the original bit setting. If a user must make IPSec connections to a Firebox from behind a different Firebox, you must clear this check box to enable the IPSec pass-through feature. For example, if mobile employees are at a customer location that has a Firebox, they can make IPSec connections to their network using IPSec. For the local Firebox to correctly allow the outgoing IPSec connection, you must also add an IPSec policy to Policy Manager.

Clear: Select **Clear** to tell the Firebox to break the frame into pieces that can fit in an IPSec packet with the ESP or AH header, regardless of the original bit setting.

PMTU Setting for IPSec

This advanced interface setting applies to external interfaces only.



PMTU Setting for IPSec (Applicable to External only)

Minimum PMTU: 576 Bytes

Aging time of learned PMTU: 10 minutes

The Path Maximum Transmission Unit (PMTU) controls the length of time that the Firebox lowers the MTU for an IPSec VPN tunnel when it gets an ICMP Request to Fragment packet from a router with a lower MTU setting on the Internet.

We recommend that you keep the default settings. This can protect you from a router on the Internet with a very low MTU setting.

Use static MAC address binding

You can control access to a Firebox interface by computer hardware (MAC) address. This feature can protect your network from ARP poisoning attacks, in which hackers use spoofed ARP entries to gain access to your network.

If this feature is enabled, and the MAC address of a computer that tries to connect to the Firebox is not included in this configuration, the connection fails. If you choose to restrict access to the Firebox by MAC address, make sure that you include the MAC address for the computer you use to administer the Firebox.

1. Select **Network > Configuration**. Click the interface you want to configure, and then click **Configure**.
2. Select the **Advanced** tab.

3. Next to the **Static MAC/IP Address Binding** table, click **Add**.
4. Enter an IP address and MAC address pair. Click **OK**.
5. Select the **Only allow traffic sent from or to these MAC/IP addresses** check box if you want this interface to pass only traffic that matches an entry in the **Static MAC/IP Address Binding** table. Keep this check box clear if you do not want to block traffic that does not match an entry in the table.

About network configuration in drop-in mode

In a drop-in configuration, the Firebox is configured with the same IP address on all interfaces. The drop-in configuration mode distributes the network's logical address range across the Firebox interfaces. You can put the Firebox between the router and the LAN and not have to change the configuration of any local computers. This configuration is known as drop-in because the Firebox is dropped in to a network.

In drop-in mode:

- You must assign the same primary IP address to all interfaces on your Firebox (external, trusted, and optional).
- You can assign secondary networks on any interface.
- You can keep the same IP addresses and default gateways for hosts on your trusted and optional networks, and add a secondary network address to the Firebox interface so the Firebox can correctly send traffic to the hosts on these networks.
- The public servers behind the Firebox can continue to use public IP addresses. The Firebox does not use network address translation to route traffic from outside your network to your public servers.

The properties of a drop-in configuration are:

- You must have a static external IP address to assign to the Firebox.
- You use one logical network for all interfaces.
- You cannot configure more than one external interface when your Firebox is configured in drop-in mode. Multi-WAN functionality is automatically disabled.

It is sometimes necessary to flush the ARP cache of each computer on the trusted network, but this is not common.



If you move an IP address from a computer located behind one Firebox interface to a computer located behind a different Firebox interface, it can take several minutes for traffic between that IP address and the Firebox itself to start to flow. The Firebox must update its internal routing table before traffic can pass. This affects only Firebox traffic such as logging, SNMP, and Firebox management connections.

Configure related hosts

In a drop-in configuration, the Firebox is configured with the same IP address on each interface. The drop-in configuration mode distributes the network's address range across the Firebox interfaces. Related hosts are sometimes required when you have configured your Firebox in drop-in mode and automatic host mapping is not functioning correctly. This sometimes happens because of interference with the Firebox trying to discover devices on an interface. When this occurs, turn off automatic host mapping and add related host entries for computers that share a network address with the Firebox. This creates a static routing relationship between the related host IP address and the interface designated for that IP address. When there are problems with dynamic/automatic host mapping, you must use related host entries.

1. From Policy Manager, select **Network > Configuration**.

The Network Configuration dialog box appears.

2. Click **Properties**.

The Drop-In Mode Properties dialog box appears.

Drop-In mode Properties

Automatic Host Mapping

When an interface is enabled with Automatic Host Mapping, a Firebox X appliance in Drop-in mode will automatically learn new MAC entries for host devices that are connected to that interface.

☐ External
 ☐ External2

☒ Trusted
 ☒ Optional-3

☒ Optional-1
 ☒ Optional-4

If an interface's Automatic Host Mapping is not enabled, the appliance will only connect to the related hosts of that interface.

Related Hosts

Host	Interface Name	Interface
50. 50. 50. 1	External	0

Add

Delete

OK Cancel Help

3. Disable automatic host mapping on any interface on which automatic host mapping is not operating correctly.

4. Click **Add**. Type the IP address of the computer for which you want to build a static route from the Firebox.
5. Click on the **Interface Name** column to select the interface the related host is connected to.
6. After you have added all related host entries, click **OK**. Save the configuration to the Firebox.

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 in a single broadcast domain independent of their physical location. This allows the grouping of devices according to traffic patterns instead of physical proximity. Members of a VLAN can share resources as if they were connected to the same LAN. You can also use VLANs to split a switch into multiple segments. For example, suppose your company has full-time employees and contract workers on the same LAN. You want to restrict the contract employees to a subset of the resources used by the full-time employees. You also want to use a more restrictive security policy for the contract workers. In this case, you split the interface into two VLANs.

Because VLANs use bridges and switches, broadcasts are more efficient because they go only to people in the VLAN, not everyone on the wire. Consequently, traffic across your routers is reduced, which means a coincidental reduction in router latency.

VLANs allow you to divide your network into groups with a logical, hierarchical structure or grouping instead of a physical one. This helps free IT staff from the restrictions of their existing network design and cabling infrastructure. VLANs make designing, implementing, and managing your network easier. Because VLANs are software based, you can quickly and easily adapt your network to additions, relocations, and reorganizations.

VLAN requirements and restrictions

- You must have Fireware Pro installed on your Firebox.
- VLANs are supported from trusted and optional interfaces only. The external interface does not allow VLAN configuration.
- The WatchGuard VLAN implementation does not support the spanning tree link management protocol.
- If your Firebox is configured with a drop-in configuration, you cannot use VLANs.
- One Firebox physical interface can be an untagged VLAN member of only one VLAN. For example, if eth0 is an untagged member of a VLAN named VLAN-1, it cannot be an untagged member of a different VLAN at the same time.
- A Firebox interface can send untagged data to only one VLAN.
- A Firebox interface can receive untagged data frames for only one VLAN.
- The Firebox can untag packets for a specific VLAN on only one of its interfaces.
- Your Firebox model and license controls the number of VLANs you can add to the Firebox. To see the number of VLANs you can add to your Firebox, [open Policy Manager](#) and select **Setup > Feature Keys**. Find the row labeled **Total number of VLAN interfaces**.
- All network segments you want to add to a VLAN must have IP addresses on the VLAN network.



If you define VLANs, you can ignore messages with the text 802.1d unknown version. These occur because the WatchGuard VLAN implementation does not support spanning tree link management protocol.

About tagging

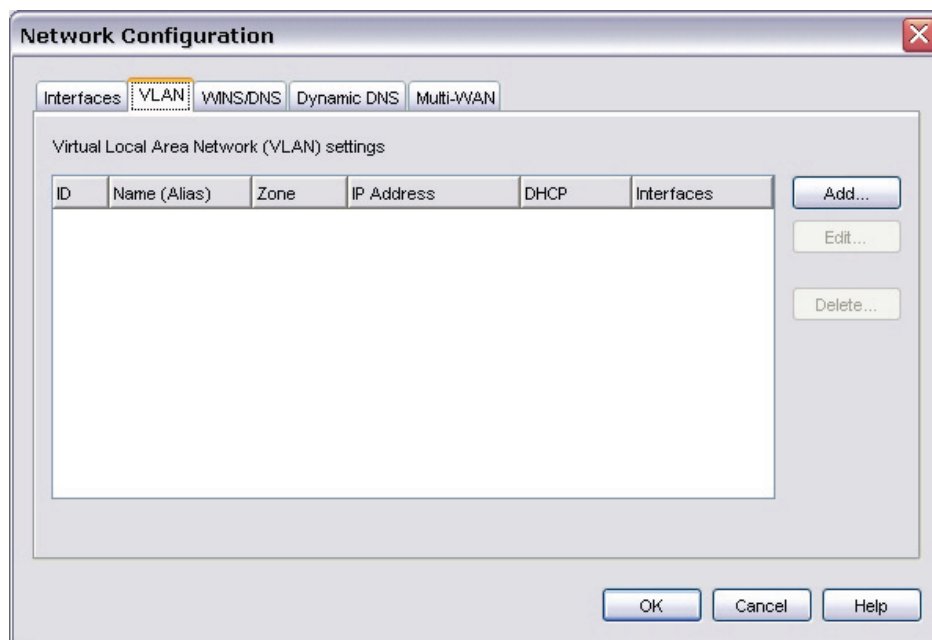
To enable VLANs, VLAN-capable switches must be deployed in each site. The switch interfaces insert tags at layer 2 of the data frame. These tags, which add an extra four bytes to the Ethernet header, identify the frame as belonging to a specific VLAN. Tagging is specified by the IEEE 802.1Q standard.

The VLAN definition includes disposition of tagged and untagged data frames. You must specify whether the VLAN receives tagged, untagged, or no data from each interface enabled on the Firebox. The Firebox can insert tags for packets that are sent to a VLAN-capable switch. The Firebox can also remove tags from packets that are sent to a network segment that belongs to a VLAN which has no switch.

Define a new VLAN

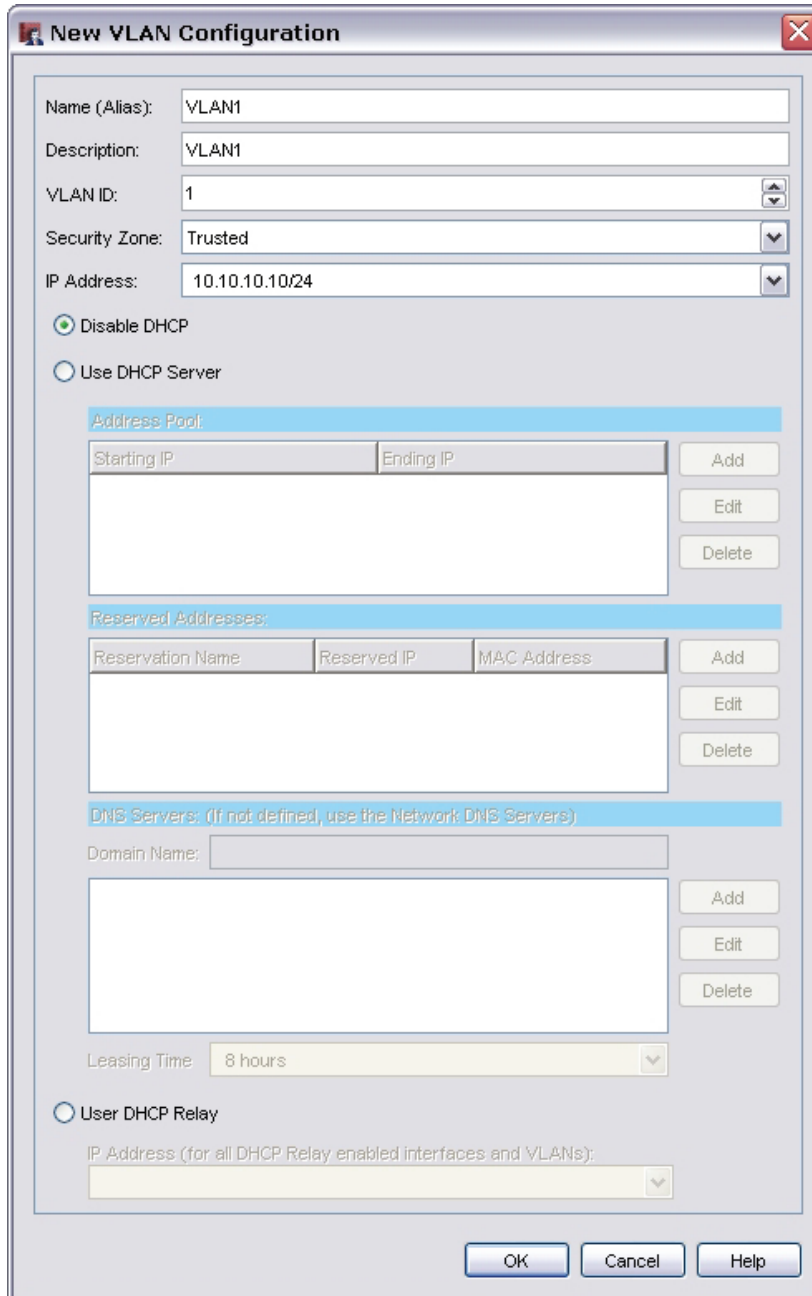
Before you begin to define a new VLAN, make sure you understand the concepts about, and restrictions for VLANs, as described in [About virtual local area networks \(VLANs\)](#).

1. From Policy Manager, select **Network > Configuration**.
The Network Configuration dialog box appears.
2. Click the **VLAN** tab.
A table of existing user-defined VLANs and their settings appears:
 - o You can click on a column header to sort the table based on the values in that column.
 - o The table can be sorted in descending or ascending order.
 - o The values in the Interface column show the physical interfaces that are members of this VLAN.
 - o The interface number in bold is the interface that sends untagged data to that VLAN.



3. Click **Add**.

The *New VLAN Configuration* dialog box appears.



The **New VLAN Configuration** dialog box contains the following fields and controls:

- Name (Alias):** Text field with value "VLAN1".
- Description:** Text field with value "VLAN1".
- VLAN ID:** Spin box with value "1".
- Security Zone:** Dropdown menu with value "Trusted".
- IP Address:** Dropdown menu with value "10.10.10.10/24".
- Disable DHCP:** Radio button (selected).
- Use DHCP Server:** Radio button (unselected).
- Address Pool:**
 - Table with columns: Starting IP, Ending IP.
 - Buttons: Add, Edit, Delete.
- Reserved Addresses:**
 - Table with columns: Reservation Name, Reserved IP, MAC Address.
 - Buttons: Add, Edit, Delete.
- DNS Servers: (If not defined, use the Network DNS Servers)**
 - Domain Name: Text field.
 - Buttons: Add, Edit, Delete.
- Leasing Time:** Spin box with value "8 hours".
- User DHCP Relay:** Radio button (unselected).
- IP Address (for all DHCP Relay enabled interfaces and VLANs):** Dropdown menu.
- Buttons:** OK, Cancel, Help.

4. In the **Name (Alias)** field, type a name for the VLAN you want to add.
5. In the **Description** field, type a description of the VLAN. This is optional and for your reference only.
6. Use the arrows in the **VLAN ID** field, or type a number into the field, to assign an integer value to the VLAN.
7. In the **Security Zone** field, select either **Trusted** or **Optional**.
Security zones correspond to aliases for interface security zones. For example, VLANs of type trusted are handled by policies that use the alias "any-trusted" as a source or destination. VLANs can be defined as trusted or optional.
8. Enter the address of the VLAN gateway in the **IP Address** field.

Use DHCP on a VLAN

You can configure the Firebox as a DHCP server for the computers on your VLAN network.

1. Select the **Use DHCP Server** radio button to configure the Firebox as the DHCP server for your VLAN network.
2. To add an IP address range, click **Add** and type the first and last IP addresses assigned for distribution. Click **OK**.
You can configure a maximum of six address ranges.
3. To reserve a specific IP address for a client, click **Add** next to the **Reserved Addresses** box. Enter a name for the reservation, the IP address you want to reserve, and the MAC address of the client's network card. Click **OK**.
4. Use the arrow buttons next to **Leasing Time** to change the default lease time.
This is the time interval that a DHCP client can use an IP address that it receives from the DHCP server. When the time is near its limit, the client sends data to the DHCP server to get a new lease.

Use DHCP relay on a VLAN

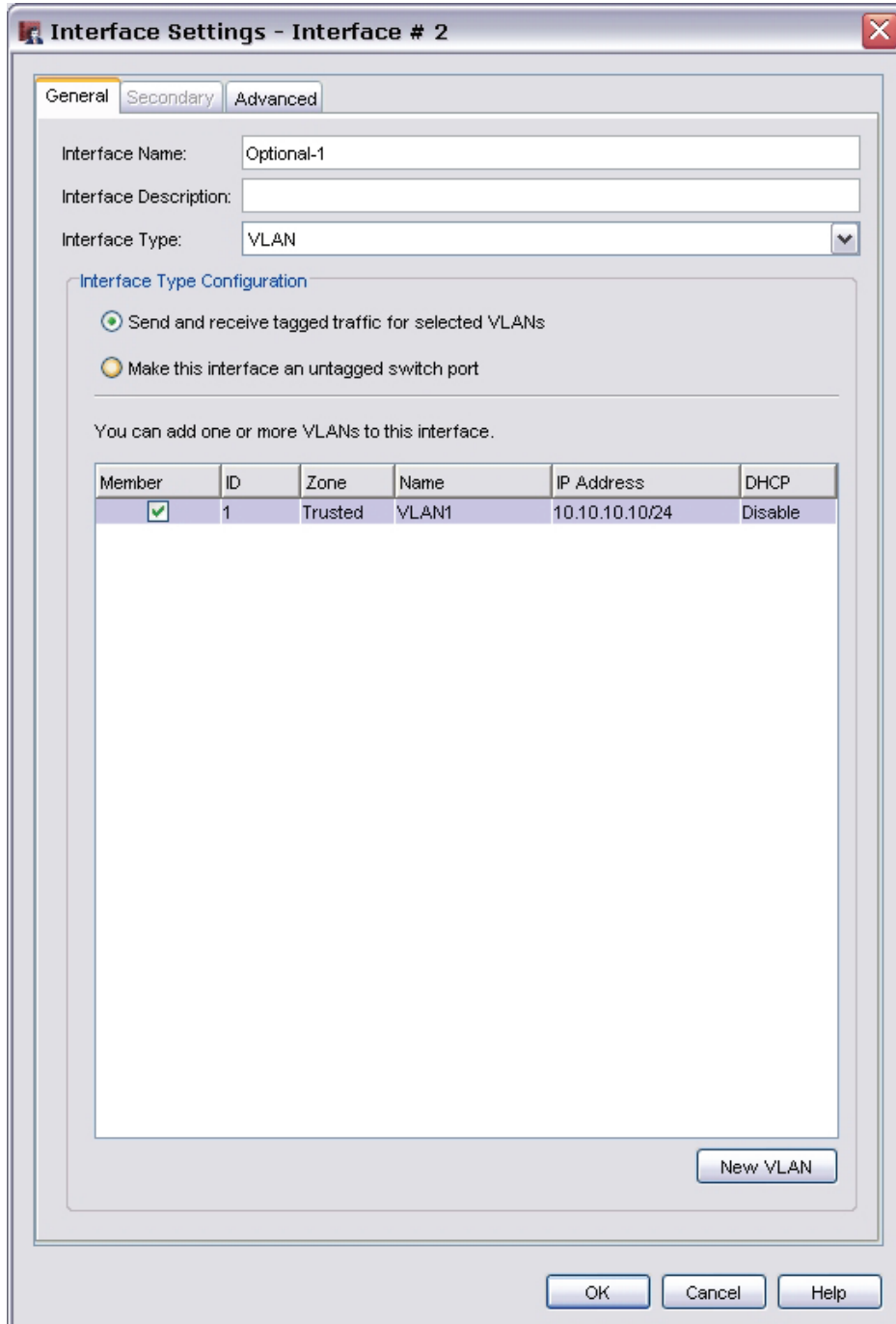
1. Select the **Use DHCP Relay** radio button.
2. Type the IP address of the DHCP server. Make sure to add a route to the DHCP server, if necessary.

Next, you [Assign interfaces to a VLAN](#).

Assign interfaces to a VLAN

When you create a new VLAN, you specify the type of data it receives from Firebox interfaces. However, you can also make an interface a member of a VLAN that is currently defined. You can also cancel an interface's VLAN membership.

1. From the **Interfaces** tab, click an interface and click **Configure**.
The Interface Settings dialog box appears.
2. Next to **Interface Type**, select **VLAN**.
A table that shows all current VLANs appears.



The dialog box titled "Interface Settings - Interface # 2" has three tabs: "General", "Secondary", and "Advanced". The "General" tab is active. It contains the following fields:

- Interface Name: Optional-1
- Interface Description: (empty)
- Interface Type: VLAN (dropdown menu)

Below these fields is the "Interface Type Configuration" section with two radio buttons:

- ☒ Send and receive tagged traffic for selected VLANs
- ☐ Make this interface an untagged switch port

Below the radio buttons is the text: "You can add one or more VLANs to this interface."

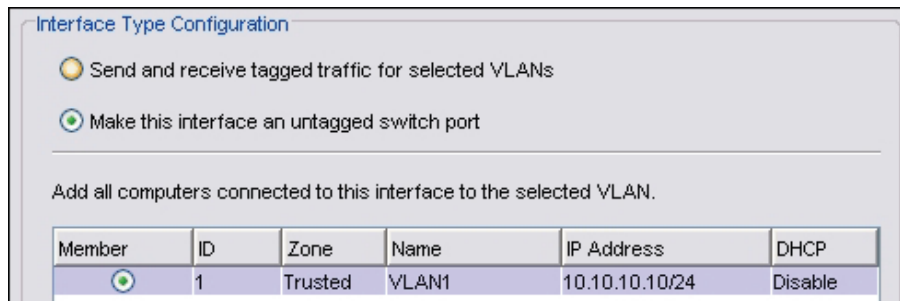
A table shows the current VLAN configuration:

Member	ID	Zone	Name	IP Address	DHCP
<input checked="" type="checkbox"/>	1	Trusted	VLAN1	10.10.10.10/24	Disable


Below the table is a large empty rectangular area. At the bottom right of this area is a button labeled "New VLAN".

At the bottom of the dialog box are three buttons: "OK", "Cancel", and "Help".

3. You must specify what type of data VLANs receive from this interface. To define the VLANs that send and receive tagged data, select the **Send and receive tagged traffic for selected VLANs** radio button. Select the **Member** box of each VLAN to receive tagged data from this interface. To cancel membership, clear the **Member** box.
4. To make the interface receive untagged data, select the **Make this interface an untagged switch port** radio button. Select the **Member** box of computers connected to this interface to the selected LAN. To cancel membership, clear the **Member** box.
5. Click **OK**.



The dialog box titled "Interface Type Configuration" contains two radio buttons. The first, "Send and receive tagged traffic for selected VLANs", is unselected. The second, "Make this interface an untagged switch port", is selected. Below the radio buttons is a text instruction: "Add all computers connected to this interface to the selected VLAN." Underneath this instruction is a table with six columns: Member, ID, Zone, Name, IP Address, and DHCP. The table contains one row with a green plus icon in the Member column, ID 1, Zone Trusted, Name VLAN1, IP Address 10.10.10.10/24, and DHCP Disable.

Member	ID	Zone	Name	IP Address	DHCP
	1	Trusted	VLAN1	10.10.10.10/24	Disable

10 Network Setup with Multiple External Interfaces

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.

With the multi-WAN feature, you can configure up to four external interfaces, each on a different subnet. This allows you to connect the Firebox to more than one Internet Service Provider (ISP). When you configure a second interface, the multi-WAN feature is automatically enabled.

Multi-WAN requirements and conditions

You must have a second internet connection to use this option.

When you use multi-WAN, you must remember:

- If you have a policy configured with an individual external interface alias in its configuration, you must change the configuration to use the alias Any-External or another alias you configure for the Firebox's external interfaces. If you do not do this, some traffic could be denied by your firewall policies.
- Multi-WAN settings do not apply to incoming traffic. When you configure a policy for inbound traffic, you can ignore all multi-WAN settings.
- You can override the multi-WAN configuration in any individual policy. On the **Policy** tab of a policy, select the **Use policy-based routing** check box and specify the external interface you want the Firebox to use. For more information on policy-based routing, see [Configure policy-based routing](#).
- Map your company's Fully Qualified Domain Name to the external interface IP address of the lowest order. If you add a multi-WAN Firebox to your Management Server configuration, you must add the Firebox using its lowest-ordered external interface to identify it.
- You cannot use drop-in mode.
- To use the Interface Overflow method, you must have a Fireware Pro license and Fireware Pro installed on your Firebox. You must also have a Fireware Pro license if you use the Round-robin method and configure different weights for the Firebox's external interfaces.

Multi-WAN and DNS

Make sure the DNS server can be reached through every WAN. Otherwise, you must modify your DNS policy such that:

- The **From** list includes Firebox.
- Select **Use policy-based routing**. If only one WAN can reach the DNS server, select that interface in the adjacent drop-down list.
If more than one WAN can reach the DNS server, select any one of them, select **Failover**, select **Configure**, and select all the interfaces that can reach the DNS server. The order does not matter.

Multi-WAN and High Availability

You can use multi-WAN failover with the High Availability (HA) feature, but they are configured separately. Multi-WAN failover caused by a failed connection to a link monitor host does not trigger HA failover. HA failover occurs only when the physical interface is down or does not respond. HA failover takes precedence over multi-WAN failover.

About multi-WAN methods

When you configure multiple external interfaces, you have four options to control which interface an outgoing packet uses. Some of these options require that you have Fireware Pro installed on your Firebox.

About multi-WAN in round-robin order

When you configure multi-WAN with the Round-robin method, the Firebox looks at its internal routing table to check for specific static or dynamic routing information for each connection. If no specified route is found, the Firebox distributes the traffic load among its external interfaces. The Firebox uses the average of sent (TX) and received (RX) traffic to balance the traffic load across all external interfaces you specify in your round-robin configuration. If you use Fireware Pro, you can assign a weight to each interface used in your round-robin configuration. By default and for all Fireware users, each interface has a weight of 1. The weight refers to the proportion of load that the Firebox sends through an interface. If you have Fireware Pro and you assign a weight of 2 to an interface, you double the portion of traffic that will go through that interface compared to an interface with a weight of 1. For example, if you have three external interfaces with 6M, 1.5M, and .075M bandwidth and want to balance traffic across all three interfaces, you would use 8, 2, and 1 as the weights for the three interfaces. Fireware will try to distribute connections so that 8/11, 2/11, and 1/11 of the total traffic flows through each of the three interfaces.

About the WAN Failover method

When you use the Failover method to route traffic through the Firebox's external interfaces, you select one external interface to be the primary external interface. Other external interfaces are backup interfaces, and you set the order for the Firebox to use the backup interfaces. The Firebox monitors the primary external interface. If it goes down, the Firebox sends all traffic to the next external interface in its configuration. While the Firebox sends all traffic to the backup interface, it continues to monitor the primary external interface. When the primary interface is active again, the Firebox immediately starts to send all new connections through the primary external interface again. You control the action for the Firebox to take for existing connections; these connections can failback immediately, or continue to use the backup interface until the connection is complete. Multi-WAN Failover and High Availability are configured separately. Multi-WAN Failover caused by a failed connection to a link monitor host does not trigger HA failover. HA failover occurs only when the physical interface is down or does not respond. HA failover takes precedence over multi-WAN Failover.

About the Interface Overflow method

When you use the Interface Overflow multi-WAN configuration method, you select the order you want the Firebox to send traffic through external interfaces and configure each interface with a bandwidth threshold value. The Firebox starts to send traffic through the first external interface in its Interface Overflow configuration list. When the traffic through that interface reaches the bandwidth threshold you have set for that interface, the Firebox starts to send traffic to the next external interface you have configured in your Interface Overflow configuration list.

This multi-WAN configuration method allows the amount of traffic sent over each WAN interface to be restricted to a specified bandwidth limit. To determine bandwidth, the Firebox examines the amount of sent (TX) and received (RX) packets and uses the higher number. When you configure the interface bandwidth threshold for each interface, you must consider the needs of your network for this interface and set the threshold value based on these needs. For example, if your ISP is asymmetrical and you set your bandwidth threshold based on a large TX rate, interface overflow will not be triggered by a high RX rate.

If all WAN interfaces have reached their bandwidth limit, the Firebox uses the ECMP (Equal Cost MultiPath Protocol) routing algorithm to find the best path.

You must have a Fireware Pro license to use this multi-WAN routing method.

About multi-WAN with the routing table

When you select the Routing Table option for your multi-WAN configuration, the Firebox uses the routes in its internal route table or routes it gets from dynamic routing processes to send packets through the correct external interface. To see whether a specific route exists for a packet's destination, the Firebox examines its route table from the top to the bottom of the list of routes. You can see the list of routes in the Firebox route table on the **Status** tab of Firebox System Manager. Routing Table option is the default multi_WAN option.

If the Firebox does not find a specified route, it selects the route to use based on source and destination IP hash values of the packet, using the ECMP (Equal Cost Multipath Protocol) algorithm specified in:

<http://www.ietf.org/rfc/rfc2992.txt>.

With ECMP, the Firebox uses an algorithm to decide which next-hop (path) to use to send each packet. This algorithm does not consider current traffic load.

You must decide whether the Routing Table method is the correct multi-WAN method for your needs. For more information, see [Multi-WAN methods and routing](#).

Configure the multi-WAN Routing Table option

Before you begin

- To use the multiple WAN feature, you must have more than one external interface configured. If necessary, use the procedure described in [Configure external interfaces](#).
- You must decide whether the Routing Table method is the correct multi-WAN method for your needs. For more information, see [Multi-WAN methods and routing](#).
- Make sure you understand the concepts and requirements for multi-WAN and the method you choose, as described in [About using multiple external interfaces](#) and [About multi-WAN methods](#).

Routing Table mode and load balancing

It is important to note that the Routing Table option does not do load balancing on connections to the Internet. The Firebox reads its internal route table from top to bottom. Static and dynamic routes that specify a destination appear at the top of the route table and take precedence over default routes. (A default route is a route with destination 0.0.0.0/0.) If there is no specific dynamic or static entry in the Firebox route table for a destination, the traffic to that destination is routed among the Firebox's external interfaces through the use of ECMP algorithms. This may or may not result in even distribution of packets among multiple external interfaces.

Configure the interfaces

1. From Policy Manager, select **Network > Configuration** and click the **Multi-WAN** tab.

The screenshot shows the 'Network Configuration' dialog box with the 'Multi-WAN' tab selected. The 'Multi-WAN Configuration' section has a dropdown menu set to 'Routing table' and a 'Configure...' button. Below this, the 'Link Monitor' section is active, showing a list of 'External Interfaces' with 'External 50' and 'External 100'. The 'Settings' for 'External 50' are configured with 'Ping' and 'TCP' methods, both using 'IP Address' and a port of '80'. The 'Both Ping and TCP must be successful to define the interface as active' checkbox is unchecked. The 'Use these settings for External 50:' section shows 'Probe interval: 15 Seconds', 'Deactivate after: 3 Failures', and 'Reactivate after: 3 Successes'.

2. From the drop-down list, select **Routing table**. By default, all external interface IP addresses are included in the configuration. If you want to remove external interfaces from the multi-WAN configuration, click **Configure** and clear the check box adjacent to the external interface you want to exclude from the multi-WAN configuration. You can have as few as one external interface included in your configuration. This can be useful if you want to use policy-based routing for specific traffic and keep only one WAN for default traffic.
3. To complete your configuration, you must add link monitor information as described in [About WAN interface status](#). For information on advanced multi-WAN configuration options, see [About advanced multi-WAN settings](#).

About the Firebox route table

When you select the Routing Table configuration option, it is a good idea to know how to look at the routing table kept on the Firebox. From WatchGuard System Manager, [start Firebox System Manager](#) and select the **Status Report** tab. Scroll down until you see **Kernel IP routing table**. This shows the internal route table on the Firebox. The ECMP group information appears below the routing table.

Routes in the internal route table on the Firebox include:

- The routes the Firebox learns from dynamic routing processes running on the Firebox (RIP, OSPF, and BGP) if you enable dynamic routing.
- The permanent network routes or host routes you add to Policy Manager at **Network > Routes**.
- The routes the Firebox automatically makes when it reads the network configuration information from Policy Manager at **Network > Configuration**.

If the Firebox detects that an external interface is down, it removes any static or dynamic routes that use that interface. This is true if the hosts specified on the **Link Monitor** tab become unresponsive and if the physical Ethernet link is down. For more information on interface status and route table updates, see [About WAN interface status](#).

Multi-WAN methods and routing

Routing method affects which type of routine method you should use.

You can use either the Routing Table or Round-Robin multi-WAN configuration option if you use dynamic routing. Routes that use a gateway on an internal (optional or trusted) network are not affected by the multi-WAN method you select.

When to use the Routing Table method

The Routing Table method is a good choice if:

- You enable dynamic routing (RIP, OSPF, or BGP) and the routers on the external network advertise routes to the Firebox so that the Firebox can learn the best routes to external locations.
- You must get access to an external site or external network through a specific route on an external network. Examples include:
 - You have a private circuit that uses a frame relay router on the external network.
 - You want all traffic to an external location to always go through a specific Firebox external interface

The Routing Table method is the fastest way to load balance more than one route to the Internet. After you enable this option, the ECMP algorithm manages all connection decisions. No additional configuration is necessary on the Firebox.

When to use the Round-Robin method

Load balancing traffic to the Internet using ECMP is based on connections, not bandwidth. Routes configured statically or learned from dynamic routing are used before the ECMP algorithm. If you have Fireware Pro, the weighted round-robin option gives you options to send more traffic through one external interface than another. At the same time, the round-robin algorithm distributes traffic to each external interface based on bandwidth, not connections. This gives you more control over how many bytes of data are sent through each ISP.

Routing Table mode and load balancing

It is important to note that the Routing Table option does not do load balancing on connections to the Internet. The Firebox reads its internal route table from top to bottom. Static and dynamic routes that specify a destination appear at the top of the route table and take precedence over default routes. (A default route is a route with destination 0.0.0.0/0.) If there is no specific dynamic or static entry in the Firebox route table for a destination, the traffic to that destination is routed among the Firebox's external interfaces through the use of ECMP algorithms. This may or may not result in even distribution of packets among multiple external interfaces.

Configure the multi-WAN Interface Overflow option

Before You Begin

- To use the multiple WAN feature, you must have more than one external interface configured. If necessary, use the procedure described in [About configuring external interfaces](#).
- Make sure you understand the concepts and requirements for multi-WAN and the method you choose, as described in [About using multiple external interfaces](#) and [About multi-WAN methods](#).

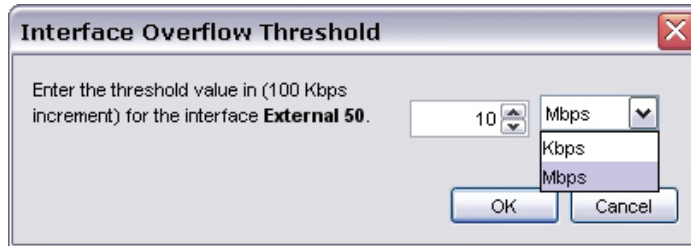
Configure the interfaces

1. From Policy Manager, select **Network > Configuration**.
2. Select the **Multi-WAN** tab. From the drop-down list, select **Interface Overflow**.

The screenshot shows the 'Network Configuration' dialog box with the 'Multi-WAN' tab selected. The 'Multi-WAN Configuration' section is active, displaying a message: 'Select the method to route non-IPSec traffic among more than one external interface. Click **Configure** to set more properties.' Below this message, a drop-down menu is set to 'Interface Overflow', and a 'Configure...' button is visible. A red circle highlights the 'Interface Overflow' drop-down and the 'Configure...' button. Below this, the 'Link Monitor' section is visible, with the 'Advanced' sub-tab selected. It shows a list of 'External Interfaces' on the left, including 'External 50' and 'External 100'. To the right, under 'Settings', there are options to 'Monitor External 50 by:' with checkboxes for 'Ping' and 'TCP', each followed by an 'IP Address' field and a 'Port' field. There is also a checkbox for 'Both Ping and TCP must be successful to define the interface as active'. Below these are settings for 'External 50': 'Probe interval: 15 Seconds', 'Deactivate after: 3 Failures', and 'Reactivate after: 3 Successes'. At the bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons.

3. Click **Configure**. In the **Include** column, select the check box for each interface you want to include in your configuration.

4. To configure a bandwidth threshold for an external interface, select the interface from the list and click **Configure**. Use the drop-down list to select **Mbps** or **Kbps** as the unit of measurement for your bandwidth setting and type the threshold value for the interface. It is important to remember that the Firebox calculates bandwidth based on the higher value of sent or received packets. Click **OK**.



5. To complete your configuration, you must add information as described in [About WAN interface status](#). For information on advanced multi-WAN configuration options, see [About advanced multi-WAN Settings](#).

Configure the multi-WAN Failover option

Before You Begin

- To use the multiple WAN feature, you must have more than one external interface configured. If necessary, use the procedure described in [About configuring external interfaces](#).
- Make sure you understand the concepts and requirements for multi-WAN and the method you choose, as described in [About using multiple external interfaces](#) and [About multi-WAN methods](#).

Configure the interfaces

1. From Policy Manager, select **Network > Configuration**.
2. Select **the Multi-WAN** tab. From the drop-down list, select **Failover**.

Network Configuration

Interfaces | VLAN | WINS/DNS | Dynamic DNS | **Multi-WAN**

Multi-WAN Configuration

Select the method to route non-IPSec traffic among more than one external interface. Click **Configure** to set more properties.

Failover [v] **Configure...**

Link Monitor | **Advanced**

Select a method for the Firebox to use to check the status of each external interface. By default, the Firebox pings the default gateway of the interface to check if the interface is active.

External Interfaces: External 50, External 100

Settings:

Monitor **External 50** by:

☐ Ping IP Address [v] [.] [.] [.]

☐ TCP IP Address [v] [.] [.] [.] Port: 80

☐ Both Ping and TCP must be successful to define the interface as active

Use these settings for **External 50**:

Probe interval: 15 Seconds

Deactivate after: 3 Failures

Reactivate after: 3 Successes

OK Cancel Help

3. Click **Configure** to specify a primary external interface and select backup external interfaces for your configuration. In the **Include** column, select the check box for each interface you want to use in the failover configuration. Use the **Move Up** and **Move Down** buttons to set the order for failover. The first interface in the list is the primary interface.
4. Click **OK**.
5. To complete your configuration, you must add link monitor information as described in [About WAN interface status](#). For information on advanced multi-WAN configuration options, see [About advanced multi-WAN settings](#).

Configure the multi-WAN Round-robin option

Before You Begin

- To use the multiple WAN feature, you must have more than one external interface configured. If necessary, use the procedure described in [About configuring external interfaces](#).
- Make sure you understand the concepts and requirements for multi-WAN and the method you choose, as described in [About using multiple external interfaces](#) and [About multi-WAN methods](#).

Configure the interfaces

1. From Policy Manager, select **Network > Configuration**.
2. Select the **Multi-WAN** tab. From the drop-down list, select **Round-robin**.

Network Configuration

Interfaces | VLAN | WINS/DNS | Dynamic DNS | **Multi-WAN**

Multi-WAN Configuration

Select the method to route non-IPSec traffic among more than one external interface. Click **Configure** to set more properties.

Round-robin (selected)

Round-robin
Failover
Interface Overflow
Routing table

Check the status of each external interface. By default, the Firewall pings the default gateway of the interface to check if the interface is active.

External Interfaces:

- External 50
- External 100

Settings:

Monitor **External 50** by:

☐ Ping IP Address . . .

☐ TCP IP Address . . . Port: 80

☐ Both Ping and TCP must be successful to define the interface as active

Use these settings for **External 50**:

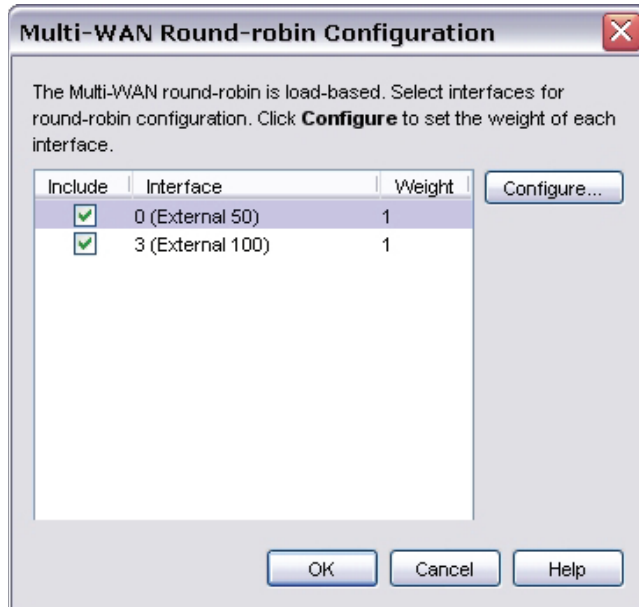
Probe interval: 15 Seconds

Deactivate after: 3 Failures

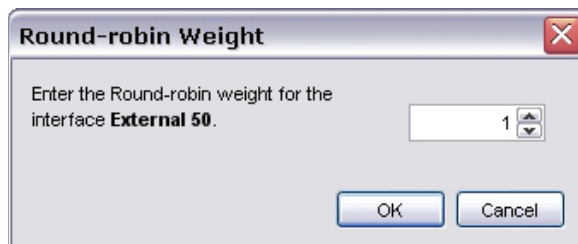
Reactivate after: 3 Successes

OK Cancel Help

3. Adjacent to the drop-down list, click **Configure**. In the Include column, select the check box for each interface you want to use in the round-robin configuration. It is not necessary to include all external interfaces in your round-robin configuration. For example, you may have one interface that you want to use for policy-based routing that you do not want to include in your round-robin configuration.



4. If you use Fireware Pro appliance software on your Firebox and you want to change the weights assigned to one or more interfaces, click **Configure**. Use the value control to set an interface weight. The weight of an interface sets the percentage of load through the Firebox that will use that interface. When you are done, click **OK**.
You can change the weight from its default of 1 only if you have a Fireware Pro license. Otherwise, you will see an error when you try to close the **Network Configuration** dialog box. For information on changing the weight, see [Find how to assign weights to interfaces](#).



5. Click **OK**.
6. To complete your configuration, you must add link monitor information as described in Checking WAN Interface Status. For information on advanced multi-WAN configuration options, see [About advanced multi-WAN settings](#).

Find how to assign weights to interfaces

If you use Fireware Pro, you can assign a weight to each interface used in your round-robin configuration. By default, each interface has a weight of 1. The weight refers to the proportion of load that the Firebox sends through an interface.

You can use only whole numbers for the interface weights; no fractions or decimals are allowed. For optimal load balancing, you might have to do a calculation to know the whole-number weight to assign for each interface. Use a common multiplier so that the relative proportion of the bandwidth given by each external connection is resolved to whole numbers.

For example, suppose you have three Internet connections. One ISP gives you 6 Mbps, another ISP gives you 1.5 Mbps, and a third gives you 768 Kbps. Convert the proportion to whole numbers:

- First convert the 768 Kbps to approximately .75 Mbps so that you use the same unit of measurement for all three lines. Your three lines are rated at 6, 1.5, and .75 Mbps.
- Multiply each value by 100 to remove the decimals. Proportionally, these are equivalent: [6 : 1.5 : .75] is the same ratio as [600 : 150 : 75]
- Find the greatest common divisor of the three numbers. In this case, 75 is the largest number that evenly divides all three numbers 600, 150, and 75.
- Divide each of the numbers by the greatest common divisor.

The results are 8, 2, and 1. This gives the whole-number weights to use for the example.

About advanced multi-WAN settings

Use the multi-WAN configuration **Advanced** tab to set your preferences for sticky connections, failback, and notification of multi-WAN events. Not all configuration options are available for all multi-WAN configuration options. If a setting does not apply to the multi-WAN configuration option you selected, those fields are not active.

About sticky connections

A sticky connection is a connection that continues to use the same WAN interface for a defined period of time. You can set sticky connection parameters if you use the Round-robin, Interface Overflow, options for multi-WAN. Stickiness makes sure that, if a packet goes out through an external interface, any future packets between the source and destination address pair use the same external interface for a specified period of time. By default, sticky connections use the same interface for 3 minutes.

If a policy definition contains a sticky connection setting, this setting can override any global sticky connection duration.

Set a global sticky connection duration

Use the **Advanced** tab to configure a global sticky connection duration for TCP connections, UDP connections, and connections that use other protocols.

Network Configuration

Interfaces | VLAN | WINS/DNS | Dynamic DNS | **Multi-WAN**

Multi-WAN Configuration

Select the method to route non-IPSec traffic among more than one external interface. Click **Configure** to set more properties.

Interface Overflow ▼ Configure...

Link Monitor | **Advanced**

Sticky Connection

Set the sticky connection interval for TCP, UDP, and Others (nonTCP, nonUDP) protocols.

TCP sticky connection: minutes ▼

UDP sticky connection: minutes ▼

Others sticky connection: minutes ▼

Failback for Active Connections

If a Multi-WAN failover event occurs and the original interface becomes available again, the Firebox automatically sends all **new** connections to the original interface. For **active** non-IPSec connections, select the option you want the Firebox to take.

Immediate failback: Stop all active connections immediately. ▼

Logging and Notification

All Multi-WAN events are logged automatically. Click **Notification** to configure the notification settings for Multi-WAN events. Notification...

OK Cancel Help

If you set a sticky connection duration in a policy, you can override the global sticky connection duration. For more information, see [Add a sticky connection duration to a policy](#).

Set the failback action

Use the drop-down list in the **Failback for Active Connections** box to set the action you want the Firebox to take when a failover event has occurred and then the primary external interface becomes active again. When this occurs, all new connections immediately fail back to the primary external interface. You select the method you want to use for connections in process at the time of failback. Select **Immediate failback** if you want the Firebox to immediately stop all existing connections. Select **Gradual failback** if you want the Firebox to continue to use the failover interface for existing connections until each connection is complete.

This failback setting also applies to any policy-based routing configuration you set to use failover external interfaces.

The screenshot shows the 'Network Configuration' window with the 'Multi-WAN' tab selected. The 'Multi-WAN Configuration' section is expanded, showing a 'Failover' dropdown menu and a 'Configure...' button. Below this, the 'Link Monitor' section is expanded, showing 'Sticky Connection' settings for TCP, UDP, and Others, each with a value of 3 minutes. The 'Failback for Active Connections' section is highlighted with a red rectangle. It contains a dropdown menu set to 'Immediate failback: Stop all active connections immediately.' and a 'Notification...' button. The 'Gradual failback' option is also visible but not selected.

Network Configuration

Interfaces | VLAN | WINS/DNS | Dynamic DNS | **Multi-WAN**

Multi-WAN Configuration

Select the method to route non-IPSec traffic among more than one external interface. Click **Configure** to set more properties.

Failover ▼ Configure...

Link Monitor | **Advanced**

Sticky Connection

Set the sticky connection interval for TCP, UDP, and Others (nonTCP, nonUDP) protocols.

TCP sticky connection: minutes ▼

UDP sticky connection: minutes ▼

Others sticky connection: minutes ▼

Failback for Active Connections

If a Multi-WAN failover event occurs and the original interface becomes available again, the Firebox automatically sends all **new** connections to the original interface. For **active** non-IPSec connections, select the option you want the Firebox to take.

Immediate failback: Stop all active connections immediately. ▼

Immediate failback: Stop all active connections immediately.

Gradual failback: Allow active connections to use failover interface.

All Multi-WAN events are logged automatically. Click **Notification** to configure the notification settings for Multi-WAN events.

Notification...

OK Cancel Help

About WAN interface status

In the **Multi-WAN** tab in the **Network Configuration** dialog box, click the **Link Monitor** sub-tab to set the method and frequency you want the Firebox to use to check the status of each WAN interface. If you do not configure a specified method for the Firebox to use, it pings the interface default gateway to check interface status.

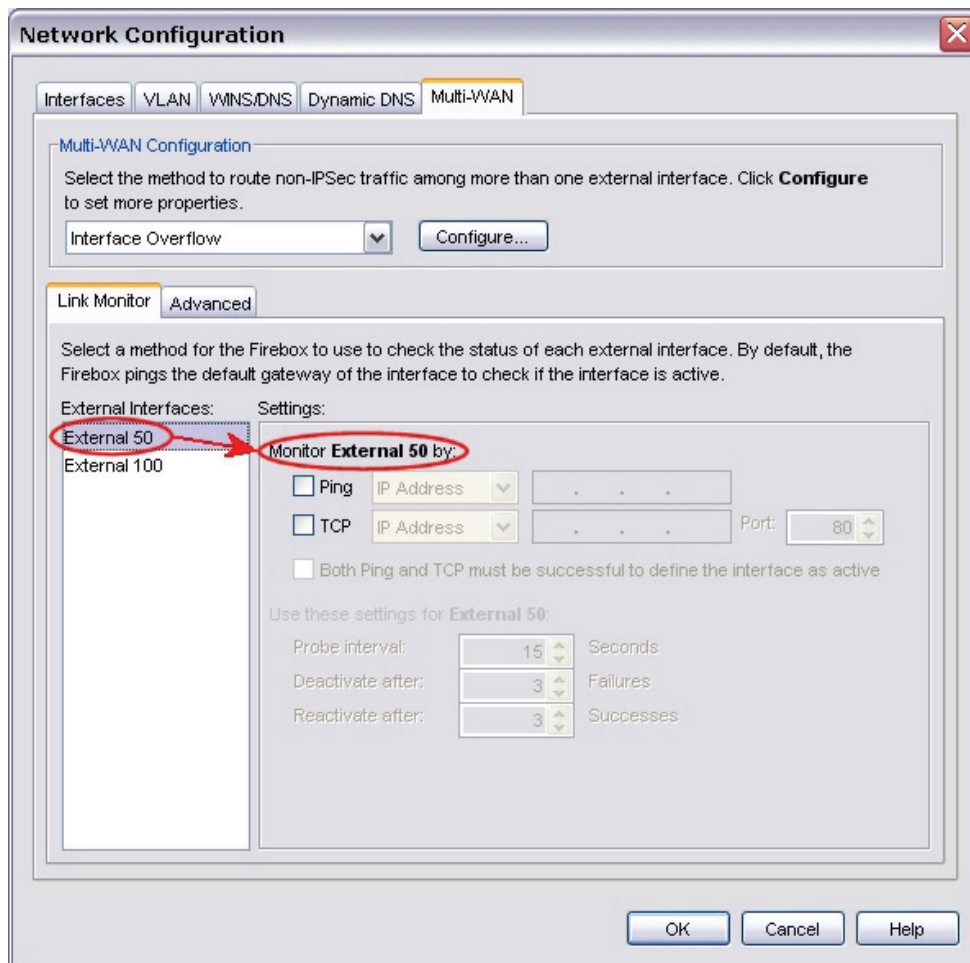
Time needed for the Firebox to update its route table

If a link monitor host does not respond, it can take from 40 – 60 seconds for the Firebox to update its route table. When the same Link Monitor host starts to respond again, it can take from 1– 60 seconds for the Firebox to update its route table.

The update process is much faster when the Firebox detects a physical disconnect of the Ethernet port. The Firebox updates its route table immediately. When the Firebox detects the Ethernet connection is back up, it updates its route table within 20 seconds.

Define a link monitor host

1. Highlight the interface in the **External Interface** column. The **Settings** information changes dynamically to show the settings for that interface.



2. Select the **Ping** check box to add an IP address or domain name for the Firebox to ping to check for interface status. You can also select the **TCP** check box to add the IP address or domain name of a computer that the Firebox can negotiate a TCP handshake with to check the status of the WAN interface. Select the **Both ping and TCP must be successful to define the interface as active** check box if you want the interface to be considered active unless both a ping and TCP handshake fail. Note that if an external interface is a peer in a High Availability configuration, a multi-WAN failover caused by a failed connection to a link monitor host does not trigger HA failover. HA failover occurs only when the physical interface is down or does not respond. If you add a domain name for the Firebox to ping and any one of the Firebox external interfaces has a static IP address, you must configure a DNS server, as described in [Add WINS and DNS server addresses](#).

The screenshot shows the 'Network Configuration' dialog box with the 'Multi-WAN' tab selected. The 'Link Monitor' section is active, showing settings for 'External 50' and 'External 100'. The 'Monitor External 50 by:' section has 'Ping' and 'TCP' checked, with 'Both Ping and TCP must be successful to define the interface as active' unchecked. The 'Probe interval' is set to 15 seconds, 'Deactivate after' is 3 failures, and 'Reactivate after' is 3 successes.

Network Configuration

Interfaces | VLAN | WINS/DNS | Dynamic DNS | **Multi-WAN**

Multi-WAN Configuration

Select the method to route non-IPSec traffic among more than one external interface. Click **Configure** to set more properties.

Interface Overflow [v] [Configure...]

Link Monitor | Advanced

Select a method for the Firebox to use to check the status of each external interface. By default, the Firebox pings the default gateway of the interface to check if the interface is active.

External Interfaces: External 50
External 100

Settings:

Monitor **External 50** by:

☒ Ping IP Address [v] 50. 50. 50. 150

☒ TCP Domain Name [v] firebox.net Port: 80 [v]

☐ Both Ping and TCP must be successful to define the interface as active

Use these settings for **External 50**:

Probe interval: 15 [v] Seconds

Deactivate after: 3 [v] Failures

Reactivate after: 3 [v] Successes

[OK] [Cancel] [Help]

3. Use the **Probe Interval** setting to configure the frequency you want the Firebox to use to check the status of the interface. By default, the Firebox checks every 15 seconds.
4. Use the **Deactivate after** setting to change the number of consecutive probe failures that must occur before failover. By default, after three probe failures, the Firebox starts to send traffic through the next specified interface in the multi-WAN failover list.
5. Use the **Reactivate after** setting to change the number of consecutive successful probes through an interface before an interface that was inactive becomes active again.
6. Repeat these steps for each external interface.
7. Click **OK**. [Save the configuration file](#).

11 Network Address Translation (NAT)

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.

If you have Fireware Pro, you can use the Server Load Balancing feature as part of a static NAT rule. The server load balancing feature is designed to help you increase the scalability and performance of a high-traffic network with multiple public servers protected by your Firebox. With server load balancing, you can have the Firebox control the number of sessions initiated to as many as ten servers for each firewall policy you configure. The Firebox controls the load based on the number of sessions in use on each server. The Firebox does not measure or compare the bandwidth that is used by each server.

For more information on server load balancing, see [Configure server load balancing](#).

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](#).

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.

In most networks, the recommended security policy is to apply NAT to all outgoing packets. With Firewall, dynamic NAT is enabled by default in the **Network > NAT** dialog box. It is also enabled by default in each policy you create. You can override the firewall setting for dynamic NAT in your individual policies, as described in Apply NAT rules.

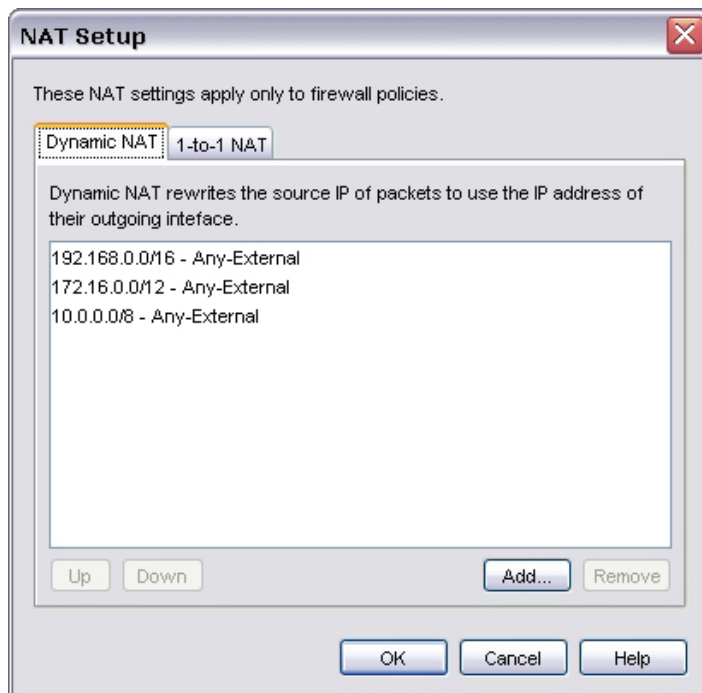
Add firewall dynamic NAT entries

The default configuration of dynamic NAT enables dynamic NAT from all private IP addresses to the external network. The default entries are:

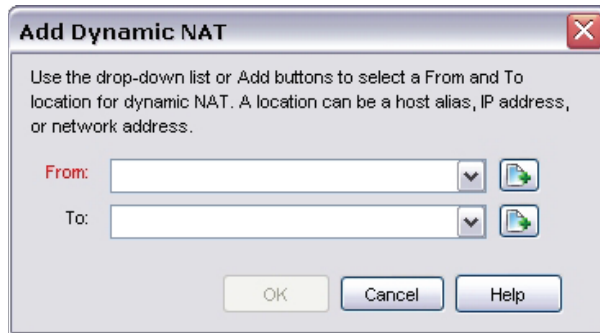
- 192.168.0.0/16 - Any-External
- 172.16.0.0/12 - Any-External
- 10.0.0.0/8 - Any-External


These three network addresses are the private networks reserved by the Internet Engineering Task Force (IETF) and usually are used for the IP addresses on LANs. To enable dynamic NAT for private IP addresses other than these, you must add an entry for them. The Firebox applies the dynamic NAT rules in the sequence that they appear in the Dynamic NAT Entries list. We recommend that you put the rules in a sequence that matches the volume of traffic the rules apply to.

1. From Policy Manager, select **Network > NAT**.
The NAT Setup dialog box appears.



2. On the **Dynamic NAT** tab of the **NAT Setup** dialog box, click **Add**.
The *Add Dynamic NAT* dialog box appears.



3. Use the **From** drop-down list to select the source of the outgoing packets.
For example, use the *trusted host alias* to enable NAT from all of the trusted network. For more information on built-in Firebox aliases, see [About aliases](#).
4. Use the **To** drop-down list to select the destination of the outgoing packets.
5. To add a host or a network IP address, click . Use the drop-down list to select the address type. Type the IP address or the range. You must type a network address in slash notation.
When you type an IP address, type all the numbers and the periods. Do not use the TAB or arrow key.
6. Click **OK**.
The new entry appears in the *Dynamic NAT Entries* list.

You cannot change an existing dynamic NAT entry. If a change is necessary, you must delete the entry with **Remove**. Use **Add** to enter it again.

Reorder dynamic NAT entries

To change the sequence of the dynamic NAT entries, select the entry to change. Then click **Up** or **Down**.

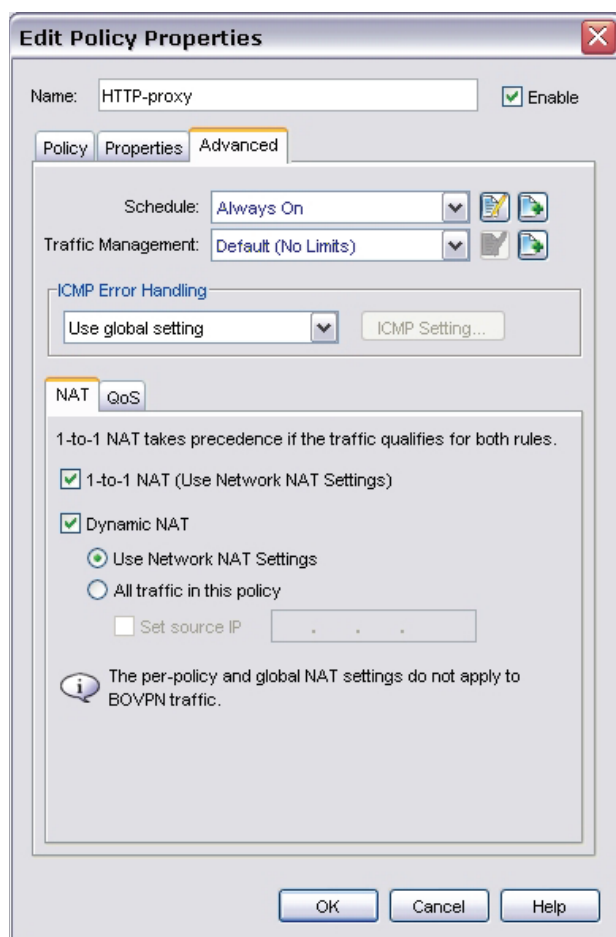
Configure policy-based dynamic NAT

With this type of NAT, the Firebox maps private IP addresses to public IP addresses. Dynamic NAT is enabled in the default configuration of each policy. You do not have to enable it unless you previously disabled it.

For policy-based dynamic NAT to work correctly, use the **Policy** tab of the **Edit Policy Properties** dialog box to make sure the policy is configured to allow traffic out through only one Firebox interface.

1-to-1 NAT rules have higher precedence than dynamic NAT rules.

1. From Policy Manager, right-click a policy and select **Modify Policy**.
The Edit Policy Properties dialog box appears.
2. Click the **Advanced** tab.



3. Select **Use Network NAT Settings** if you want to use the dynamic NAT rules set for the Firebox. Select **All traffic in this policy** if you want to apply NAT to all traffic in this policy.

4. If you selected **All traffic in this policy**, you can set a dynamic NAT source IP address for any policy that uses dynamic NAT. Select the **Set source IP** check box to do this. This makes sure that any traffic that uses this policy shows a specified address from your public or external IP address range as the source. You would most often do this to force outgoing SMTP traffic to show your domain's MX record address when the IP address on the Firebox's external interface is not the same as your MX record IP address. This source address must be on the same subnet as the interface you specified for outgoing traffic. If you do not select the **Set source IP** check box, the Firebox changes each packet's source IP address to the IP address of the interface from which the packet is sent out. We recommend that you do not use the **Set source IP** option if you have more than one external interface configured on your Firebox.
5. Click **OK**. [Save the configuration file](#).

Disable policy-based dynamic NAT

Dynamic NAT is enabled in the default configuration of each policy. To disable dynamic NAT for a policy:

1. From Policy Manager, right-click a policy and select **Modify Policy**.
The Edit Policy Properties dialog box appears.
2. Click the **Advanced** tab.
3. Clear the check box in front of **Dynamic NAT** to turn NAT off for the traffic this policy controls.
4. Click **OK**. [Save the configuration file](#).

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.

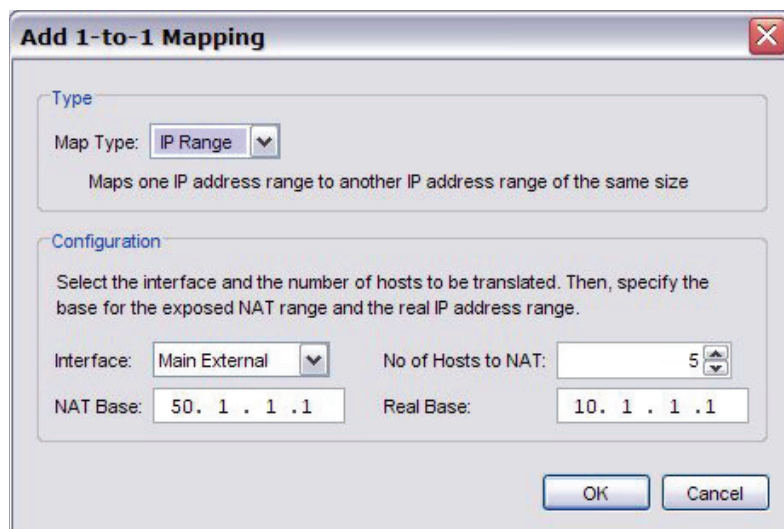
About 1-to-1 NAT and VPNs

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.

Use firewall 1-to-1 NAT

1. From Policy Manager, select **Network > NAT**. Click the **1-to-1 NAT** tab.
2. Click **Add**.

The 1-1 Mapping dialog box appears.



The dialog box is titled "Add 1-to-1 Mapping" and contains two sections: "Type" and "Configuration".

Type

Map Type: (dropdown arrow)

Maps one IP address range to another IP address range of the same size

Configuration

Select the interface and the number of hosts to be translated. Then, specify the base for the exposed NAT range and the real IP address range.

Interface: (dropdown arrow) No of Hosts to NAT: (spin box)

NAT Base: Real Base:

Buttons: OK, Cancel

3. In the **Map Type** drop-down list, select **Single IP**, **IP range**, or **IP subnet** if you want to map to one host, a range of hosts, or a subnet. If you select **IP range** or **IP subnet**, do not include more than 256 IP addresses in that range or subnet. If you have more than 256 IP addresses you want to apply 1-to-1 NAT to, you must create more than one rule.
4. Complete all the information in the Configuration section of the dialog box. For more information on how to use these fields, see “Define a 1-to-1 NAT rule,” below. Click **OK**.
5. When you are done, click **OK** to close the **NAT Setup** dialog box. Save the changes to the Firebox.
6. After you configure a global 1-to-1 NAT rule, you must configure the NAT base IP addresses in the appropriate policies. In the example given above, we must configure our SMTP policy to allow SMTP traffic from Any to 50.50.50.55-10.0.1.55.



To connect to a computer located on a different Firebox interface that uses 1-to-1 NAT, you must use that computer's private (NAT base) IP address. If this is a problem, you can disable 1-to-1 NAT and use static NAT.

Define a 1-to-1 NAT rule

In each 1-to-1 NAT rule, you can configure a host, a range of hosts, or a subnet. You must also configure:

Interface

The name of the Firebox Ethernet interface on which 1-to-1 NAT is applied. The Firebox will apply 1-to-1 NAT for packets sent in to, and out of, the interface. In our example above, the rule is applied to the external interface.

NAT base

When you configure a 1-to-1 NAT rule, you configure the rule with a from and a to range of IP addresses. The NAT base is the first available IP address in the to range of addresses. The NAT base IP address is the address that the real base IP address changes to when the 1-to-1 NAT is applied. You cannot use the IP address of one of your Firebox interfaces as your NAT base. In our example above, the NAT base is 50.50.50.55.

Real base

When you configure a 1-to-1 NAT rule, you configure the rule with a from and a to range of IP addresses. The Real base is the first available IP address in the from range of addresses. It is the IP address assigned to the physical Ethernet interface of the computer to which you will apply the 1-to-1 NAT policy. When packets from a computer with a real base address go through the interface specified, the 1-to-1 action is applied. In our example above, the Real base is 10.0.1.50.

Number of hosts to NAT (for ranges only)

The number of IP addresses in a range to which the 1-to-1 NAT rule applies. The first real base IP address is translated to the first NAT Base IP address when 1-to-1 NAT is applied. The second real base IP address in the range is translated to the second NAT base IP address when 1-to-1 NAT is applied. This is repeated until the Number of hosts to NAT is reached. In our example above, the number of hosts to apply NAT to is five.

You can also use 1-to-1 NAT to solve the problem when you must create a VPN tunnel between two networks that use the same private network address. When you create a VPN tunnel, the networks at each end of the VPN tunnel must have different network address ranges. 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.

Configure policy-based 1-to-1 NAT

With this type of NAT, the Firebox uses the private and public IP ranges that you set when you configured global 1-to-1 NAT, but the rules are applied to an individual policy. 1-to-1 NAT is enabled in the default configuration of each policy. If traffic matches both 1-to-1 NAT and dynamic NAT policies, the 1-to-1 NAT gets precedence.

Enable policy-based 1-to-1 NAT

Because policy-based 1-to-1 NAT is enabled by default, you do not need to do anything else to enable it.

Disable policy-based 1-to-1 NAT

1. From Policy Manager, right-click a policy and select **Modify Policy**.
The Edit Policy Properties dialog box appears.
2. Click the **Advanced** tab.
3. Clear the **1-to-1 NAT** check box to turn NAT off for the traffic this policy controls.
4. Click **OK**. [Save the configuration file.](#)

About static NAT

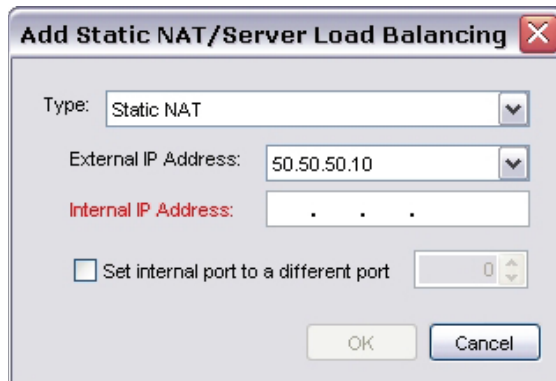
Static NAT, also known as port forwarding, is a port-to-host NAT. A host sends a packet from the external network to a port on an external interface. Static NAT changes this IP address to an IP address and port behind the firewall. If a software application uses more than one port and the ports are selected 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.

1. Double-click a policy icon in the Policy Manager window.
2. From the **Connections are** drop-down list, select **Allowed**.
To use static NAT, the policy must let incoming traffic through.
3. Below the **To** list, click **Add**.
The Add Address dialog box appears.

4. Click **Add NAT**.

The Add Static NAT/Server Load Balancing dialog box appears.



The dialog box is titled "Add Static NAT/Server Load Balancing" with a close button (X) in the top right corner. It contains the following fields and controls:

- Type:** A drop-down menu currently showing "Static NAT".
- External IP Address:** A drop-down menu currently showing "50.50.50.10".
- Internal IP Address:** A text input field containing three dots " . . . ".
- Set internal port to a different port:** A checkbox that is currently unchecked. To its right is a port number input field showing "0" with up and down arrow buttons.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.



*Because of how static NAT operates, it is available only for policies that use a specified port, which includes TCP and UDP. A policy that uses a different protocol cannot use incoming static NAT. The **NAT** button in the **Properties** dialog box of that policy does not operate. You also cannot use static NAT with the Any policy.*

5. Make sure the **Type** drop-down list is set to **Static NAT**.
6. From the **External IP Address** drop-down list, select the public IP address to use for this service.
7. Type the internal IP address. The internal IP address is the destination on the trusted or optional network.
8. If necessary, select the **Set internal port to a different port than this policy** check box. This enables port address translation (PAT).
You usually do not use this feature. It enables you to change the packet destination not only to a specified internal host but also to a different port. If you select this check box, type the different port number or use the arrow buttons in the Internal Port box.
9. Click **OK** to close the **Add Static NAT** dialog box.
The static NAT route appears in the Members and Addresses list.
10. Click **OK** to close the **Add Address** dialog box. Click **OK** to close the **Policy Properties** dialog box.

Configure server load balancing



You must have Fireware Pro to use the server load balancing feature.

The server load balancing feature in Fireware Pro is designed to help you increase the scalability and performance of a high-traffic network with multiple public servers. With server load balancing, you can have the Firebox control the number of sessions initiated to as many as 10 servers for each firewall policy you configure. The Firebox controls the load based on the number of sessions in use on each server. The Firebox does not measure or compare the bandwidth that is used by each server.

You configure server load balancing as part of a static NAT rule. The Firebox can balance connections among your servers with two different algorithms. When you configure server load balancing, you must choose the algorithm you want the Firebox to apply:

Round-robin

If you select this option, the Firebox distributes incoming sessions among the servers you specify in the policy in round-robin order. The first connection is sent to the first server specified in your policy. The next connection is sent to the next server in your policy, and so on.

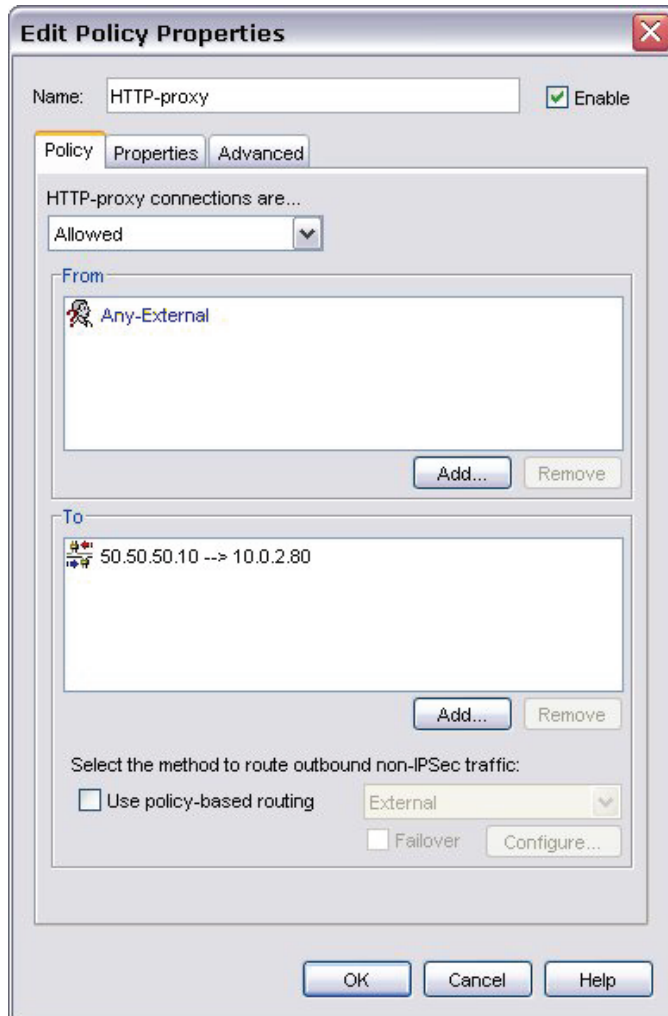
Least Connection

If you select this option, the Firebox sends each new session to the server in the list that currently has the lowest number of open connections to the Firebox. The Firebox cannot tell how many connections the server has open on other interfaces. If you want to, you can apply weights to your servers in the server load balancing configuration to make sure that your most powerful servers are given the heaviest load. By default, each interface has a weight of one. The weight refers to the proportion of load that the Firebox sends to a server. If you assign a weight of 2 to a server, you double the number of sessions that the Firebox sends to that server, compared to a server with a weight of 1.

When you configure server load balancing, it is important to know:

- You can configure server load balancing for any policy to which you can apply static NAT.
- If you apply server load balancing to a policy, you cannot set policy-based routing or other NAT rules in the same policy.
- When you apply server load balancing to a policy, you can add a maximum of 10 servers to the policy.
- If you use High Availability and server load balancing, no real-time synchronization occurs when a failover event occurs. The secondary Firebox sends connections to all servers in the server load balancing list to see which servers are available. It then applies the server load balancing algorithm to all available servers.

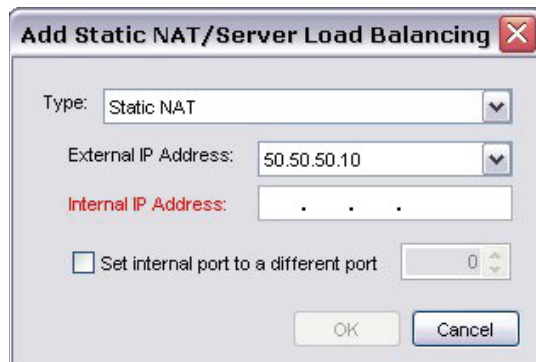
1. From Policy Manager, find the policy to which you want to apply server load balancing and double-click to open it for edit.
Or, highlight the policy and select **Edit > Modify Policy**. To create a new policy and enable server load balancing in that policy, select **Edit > Add Policy**.



- Below the **To** field, click **Add**.
The Add Address dialog box appears.



- Click **Add NAT**.
The Add Static NAT/Server Load Balancing dialog box appears.



4. From the **Type** drop-down list, select **Server Load Balancing**.

Add Static NAT/Server Load Balancing

Type: **Server Load Balancing**

External IP Address: **50.50.50.10**

Method: **Round-robin**

Servers:

IP Address	Weight

Add...
Edit...
Remove

☐ Enable sticky connection 8 hours

OK **Cancel**

5. From the **External IP address** drop-down list, select the external IP address or alias you want to use in this policy. For example, you can have the Firebox apply server load balancing for this policy for packets received on only one external IP address. Or, you can have the Firebox apply server load balancing for packets received on any external IP address if you select the Any-External alias.
6. From the **Method** drop-down list, select the algorithm you want the Firebox to use for server load balancing. You can choose from **Round-robin** or **Least Connection**.
7. Click **Add** to add the IP addresses of your internal servers for this policy. You can add a maximum of 10 servers in a policy. You can also add a weight to the server. By default, each interface has a weight of 1. The weight refers to the proportion of load that the Firebox sends to a server. If you assign a weight of 2 to a server, you double the number of sessions that the Firebox sends to that server, compared to a server with a weight of 1.

Add Server

IP Address: . . .

Weight: 1

☐ Set internal port to a different port 0

OK **Cancel**

8. A sticky connection is a connection that continues to use the same server for a defined period of time. Stickiness makes sure that all packets between a source and destination address pair are sent to the same server for a time period you specify. Select the **Enable sticky connection** check box if you want to set sticky connections for your internal servers.



The dialog box titled "Add Static NAT/Server Load Balancing" contains the following fields and controls:

- Type: Server Load Balancing (dropdown)
- External IP Address: 50.50.50.10 (dropdown)
- Method: Round-robin (dropdown)
- Servers: A table with two columns, IP Address and Weight.

IP Address	Weight
10.0.2.80	1
10.0.2.81	1
10.0.2.82	1

Buttons: Add..., Edit..., Remove

☐ Enable sticky connection 8 hours (dropdown)

Buttons: OK, Cancel

9. Click **OK**. [Save the configuration file.](#)

12 Authentication

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 use users and groups in your firewall policies to give access to specified network resources. This is useful in network environments where different users share a single computer or IP address.

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. To authenticate, a user must connect to the authentication web page on the Firebox. The address is:

`https://IP address of a Firebox interface:4100/`

or

`https://Host name of the Firebox:4100`

An authentication web form appears. The user must type his or her user name and password, and select the authentication server from the drop-down list if more than one type of authentication is configured. The Firebox sends the name and password to the authentication server using PAP (Password Authentication Protocol). When the user is authenticated, the user is then allowed to use the approved network resources.



Because Fireware uses a self-signed certificate, you see a security warning from your web browser when you authenticate. You can safely ignore this security warning. If you want to remove this warning, you can use a third-party certificate, or create a custom certificate that matches the IP or domain name used for authentication. For more information, see [Configure the web server certificate for Firebox authentication](#).

How users can close a session

To close an authenticated session before the timeout occurs, a user can click **Logout** on the Authentication web page. If the page is closed, the user must open it again to disconnect. To prevent a user from authenticating, the administrator must disable that user's account on the authentication server.

How administrators can close a user's session

An administrator can close a user's session by right-clicking the user's name on the **Authenticated Users** tab in Firebox System Manager. For more information, see [Authenticated users](#).

Use authentication to restrict incoming traffic

One function of the authentication tool is to authenticate outgoing traffic. You can also use it to restrict incoming network traffic. When you have an account on the Firebox, you can always authenticate to the Firebox from a computer external to the Firebox. For example, you can type this address in your browser at home:

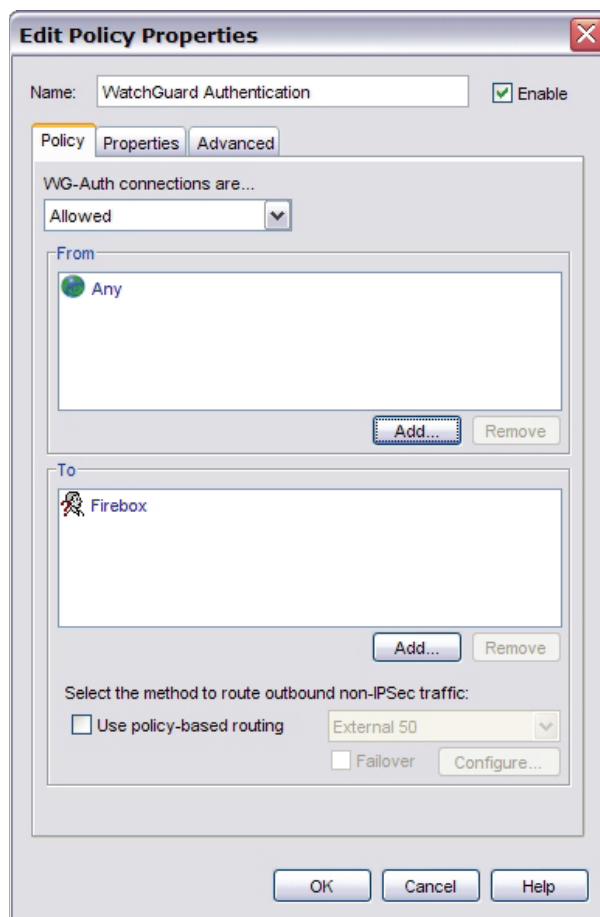
`https://IP address of Firebox external interface:4100/`

After you authenticate, you can use the policies that are configured for you on the Firebox.

Use this procedure to let a remote user authenticate from the external network. This lets the person use resources through the Firebox.

1. From Policy Manager, double-click the **WatchGuard Authentication** policy icon. This policy appears after you add a user or group to a policy configuration.
You see a warning to be careful when you edit an automatically configured policy.
2. From the **WG-Auth connections are** drop-down list, make sure **Allowed** is selected.
3. Below the **From** box, click **Add**. Select **Any** from the list and click **Add**. Click **OK**.

4. The **To** box should contain **Firebox**. If it does not, below the **To** box, click **Add**. Select **Firebox** from the list and click **Add**. Click **OK**.



Use authentication through a gateway Firebox

To send an authentication request through a gateway Firebox to a different Firebox, it can be necessary to add a policy that allows the authentication traffic on the gateway Firebox. If authentication traffic is denied on the gateway Firebox, use Policy Manager to add the WatchGuard Authentication policy. This policy controls traffic on TCP port 4100. Configure the policy to allow traffic to the IP address of the destination Firebox.

Set global authentication values

To define global authentication values, select **Setup > Authentication > Authentication Settings**. The **Authentication Settings** dialog box appears.

Authentication Settings

Firewall Authentication

These timeout settings apply to users who authenticate to external third-party authentication servers that do not already have a timeout configured. **Note:** A value of 0 means "never time out".

Session Timeout: 0 seconds

Idle Timeout: 2 hours

☒ Allow multiple concurrent firewall authentication logins from the same account

☐ Send a redirect to the browser after successful authentication

Type the URL to use for the redirect. After successful authentication, the user's browser automatically goes to this URL. (For example, <http://company.com>)

Single Sign-On

☒ Enable Single Sign-On (SSO) with Active Directory

SSO Agent IP address: . . .

Cache data for: 600 seconds

SSO Exceptions

. . . Add... Remove

OK Cancel Help

Set global authentication timeouts

Users are authenticated for some time after they close their last authenticated connection. This timeout is set either here, or in the **Setup Firebox User** dialog box described in [Define a new user for Firebox authentication](#). The Firebox User setting overrides the global setting. The global setting is used only if no Firebox User value is defined.

For users authenticated by third-party servers, the timeouts set on those servers also override the global authentication timeouts.

Authentication timeout values do not apply to Mobile VPN with PPTP users.

Session Timeout

Maximum length of time the user can send traffic to the external network. If you set this field to zero (0) seconds, minutes, hours, or days, no session timeout is used and the user can stay connected for any length of time.

Idle Timeout

Maximum length of time the user can stay authenticated when idle (not passing any traffic to the external network). If you set this field to zero (0) seconds, minutes, hours, or days, no idle timeout is used and the user can stay idle for any length of time.

Allow multiple concurrent logins

From the **Authentication Settings** dialog box, select the **Allow multiple concurrent firewall authentication logins from the same account** check box to allow more than one user to authenticate, with the same user credentials at the same time, to one authentication server. This is useful for guest accounts or in laboratory environments.

This feature is supported only if you use the Firebox as an authentication server.

For Mobile VPN with IPSec and Mobile VPN with SSL users, current logins from the same account are always supported regardless of whether this check box is selected. These users must log in from different IP addresses if they want to do concurrent logins, which means that they cannot use the same account to log in if they are behind a Firebox that uses NAT. Mobile VPN with PPTP users do not have this restriction.

Use a custom default start page

Normally, the Firebox web authentication page appears as the start page of your web browser. If you want the browser to go to a different page after your users successfully log in, you can use the **Authentication Settings** dialog box to define a redirect. Select the **Send a redirect to the browser after successful authentication** check box and type the URL in the field below.

Enable Single Sign-On

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. For more information, see [About Single Sign-On \(SSO\)](#).

About the WatchGuard Authentication (WG-Auth) policy

Fireware adds the WatchGuard Authentication policy to your Firebox configuration for you automatically when you first configure a policy with a user or group name in the **From** field on the **Policy** tab of the policy definition. This policy controls access to port 4100 on the Firebox itself. This is the port your users will use to send authentication requests to the Firebox from their web browsers. For example, to authenticate to a Firebox with an IP address of 10.10.10.10, a user types in his or her web browser address bar:

```
https://10.10.10.10:4100
```

One situation in which you may need to add the WatchGuard Authentication policy manually is when you want to send an authentication request through a gateway Firebox to a different Firebox. If authentication traffic is denied on the gateway Firebox, you must use Policy Manager to add the WatchGuard Authentication policy. You then modify the policy to allow traffic to the IP address of the destination Firebox.

For more information on when to modify the WatchGuard Authentication policy, see [Use authentication to restrict incoming traffic](#).

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.

Enable and configure SSO

1. From Policy Manager, select **Setup > Authentication > Authentication Settings**.
The *Authentication Settings* dialog box appears.

Authentication Settings

Firewall Authentication

These timeout settings apply to users who authenticate to external third-party authentication servers that do not already have a timeout configured. **Note:** A value of 0 means "never time out".

Session Timeout: 0 seconds

Idle Timeout: 7 minutes

☒ Allow multiple concurrent firewall authentication logins from the same account

☐ Send a redirect to the browser after successful authentication

Type the URL to use for the redirect. After successful authentication, the user's browser automatically goes to this URL. (For example, <http://company.com>)

Single Sign-On

☒ Enable Single Sign-On (SSO) with Active Directory

SSO Agent IP address: . . .

Cache data for: 600 seconds

SSO Exceptions

. . . Add... Remove

OK Cancel Help

2. Select the **Enable Single Sign-On (SSO) with Active Directory** check box.
3. Type the IP address of your SSO Agent in the **SSO Agent IP address** field.
4. Select the amount of time the SSO Agent caches data in the **Cache data for** field.
5. Add or remove SSO exceptions for IP addresses that do not require authentication, such as network servers. (For more information about SSO exceptions, see the next section.)
You can type a host IP address, a network IP address in slash notation, or a range of IP addresses.
6. Click **OK** to save your changes.

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.

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 SSO on your Firebox

To enable SSO on your Firebox, see [About Single Sign-On \(SSO\)](#).

Authentication server types

Fireware supports six authentication methods:

- [Firebox as an authentication server](#)
- [RADIUS server authentication](#)
- [VASCO server authentication](#)
- [SecurID authentication](#)
- [LDAP authentication](#)
- [Active Directory authentication](#)

You can configure one or more authentication server types for a Firebox. If you use more than one type of authentication server, the user must select the authentication server type from a drop-down list when they authenticate.

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 RADIUS server authentication](#)
- [Configure VASCO server authentication](#)
- [Configure SecurID authentication](#)
- [Configure LDAP authentication](#)
- [Configure Active Directory authentication](#)

Use a backup authentication server

You can configure a primary and backup authentication server with all types of third-party authentication. If the Firebox cannot connect to the primary authentication server after three attempts, the primary server is marked as dead and an alarm message is generated. The Firebox then connects to the backup authentication server.

If the Firebox cannot connect to the backup authentication server, it waits ten minutes, and then tries to connect to the primary authentication server again. The dead server is marked as active after the dead time interval is reached.

Configure the Firebox as an authentication server

If you do not use a third-party authentication server, you can use the Firebox as an authentication server. This procedure divides your company into groups and users for authentication. The group to which you assign a person is controlled by the tasks they do and information they use. For example, you can have an accounting group, a marketing group, and a research and development group. You can also have a new employee group, with controlled access to the Internet.

In a group, you set the authentication procedure for the users, the system type, and the information to which they have access. A user can be a network or a computer. If your company changes, you can add or remove users or systems from your groups.

The Firebox authentication server is enabled by default. You do not need to do anything to enable it before you add users and groups.

Types of Firebox authentication

You can configure the Firebox to authenticate users for four different types of authentication:

- [Firewall authentication](#)
- [Mobile VPN with PPTP connections](#)
- [Mobile VPN with IPSec connections](#)
- [Mobile VPN with SSL connections](#)

When the authentication is successful, the Firebox makes a mapping between these items:

- User name
- Firebox User group (or groups) of which the user is a member
- IP address on the user's computer when the user authenticates
- Virtual IP address on the user's computer if the user is connected with Mobile VPN

Firewall authentication

When a user authenticates to the Firebox, the user credentials and IP address of the user's computer are both used to find whether a policy applies to the traffic starting from or going to that user's computer.

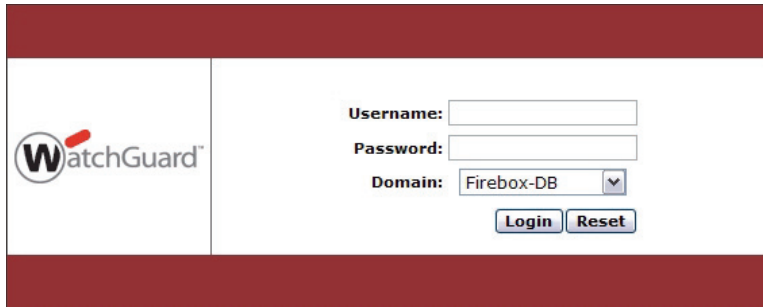
To create a Firebox user account, see [Define a new user for Firebox authentication](#). After you create the user account, you can [Define a new group for Firebox authentication](#) and put the user in that group.

Next, create a policy that allows traffic only to or from a list of Firebox user names or a list of Firebox groups. This policy is applied only if a packet comes from or goes to the authenticated user's IP address.

A user authenticates with an HTTPS connection to the Firebox over port 4100 by typing:

```
https://IP address of a Firebox interface:4100/
```


If the user name and password are valid, the user is authenticated.



Mobile VPN with PPTP connections

When you activate Mobile VPN with PPTP on your Firebox, users included in the Mobile VPN with PPTP group can use the PPTP feature included in their computer operating system to make a PPTP connection to the Firebox.

Because the Firebox allows the PPTP connection from any Firebox user that gives the correct credentials, it is important that you make a policy for PPTP sessions that includes only users you want to allow to send traffic over the PPTP session. You can also add a group or individual user to a policy that restricts access to resources behind the Firebox. The Firebox creates a pre-configured group called *PPTP-Users* for this purpose.

To configure a Mobile VPN with PPTP connection:

1. From Policy Manager select **VPN > Mobile VPN > PPTP**.
2. Select **Activate Mobile VPN with PPTP**.
3. Clear the **Use Radius authentication to authenticate Mobile VPN with PPTP users** check box, to allow the Firebox to authenticate the PPTP session.
The Firebox checks to see whether the user name and password the user enters into the VPN connection box matches the user name and password in the Firebox User database that is a member of the PPTP-Users group.
If the credentials supplied by the user match an account in the Firebox User database, the user is authenticated for a PPTP session.
4. Create a policy that allows traffic only from or to a list of Firebox user names, or a list of Firebox groups.
The Firebox does not look at this policy unless traffic comes from or goes to the authenticated user's virtual IP address.

Configure a Mobile VPN with IPSec connection

You can configure the Firebox to host Mobile VPN with IPSec sessions. From Policy Manager, select **VPN > Mobile VPN > IPSec**.

For more information about the Mobile VPN with IPSec client, see [About the Mobile VPN with IPSec client](#).

For more information about installing the Mobile VPN with IPSec client, see [Install the Mobile VPN with IPSec client software](#).

You create the Mobile VPN group using the **Add Mobile VPN with IPSec** wizard.

When the wizard is finished, Policy Manager does two things:

- Makes a client configuration profile (called a .wgx file) and puts it on the management station computer that created the Mobile VPN account. The user must have this .wgx file to configure the Mobile VPN client computer.
- Automatically adds an Any policy to the **Mobile VPN** tab that allows traffic to pass to and from the authenticated Mobile VPN user.

When the user's computer is correctly configured, the user makes the Mobile VPN connection. If the user name and password the user enters into the Mobile VPN authentication dialog box match an entry in the Firebox User database, and if the user is in the Mobile VPN group you create, the Mobile VPN session is authenticated. Policy Manager automatically makes a policy that allows any traffic from the authenticated user. To restrict the ports the Mobile VPN client can access, delete the Any policy and add policies for those ports to the **Mobile VPN with IPSec** tab.

To learn how to add policies, see [About Policy Manager](#).

Mobile VPN with SSL connections

You can configure the Firebox to host Mobile VPN with SSL sessions.

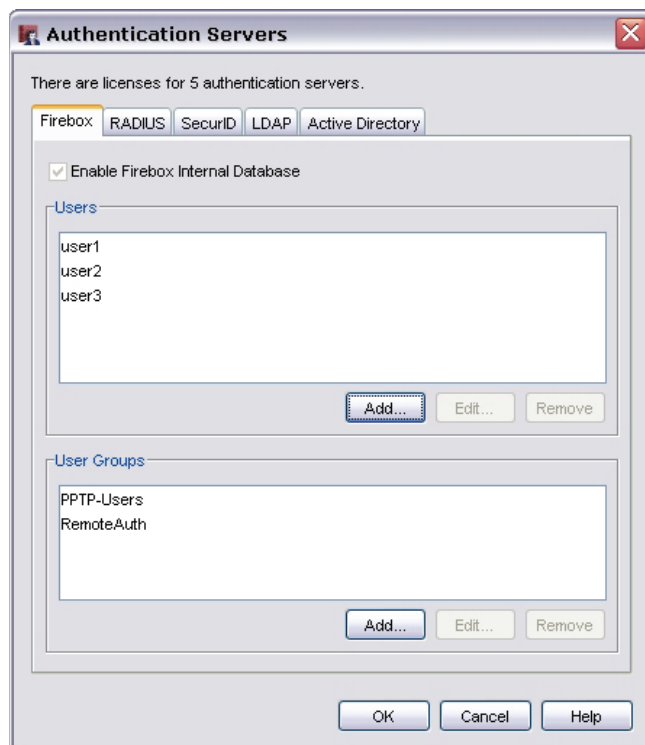
When the Firebox is configured with a Mobile VPN with SSL connection, users included in the Mobile VPN with SSL group can install and use the Mobile VPN with SSL client software to make an SSL connection.

Because the Firebox allows the SSL connection from any Firebox user that gives the correct credentials, it is important that you make a policy for SSL VPN sessions that includes only users you want to allow to send traffic over SSL VPN. You can also add these users to a Firebox User group and make a policy that allows traffic only from this group. The Firebox creates a pre-configured group called *SSLVPN-Users* for this purpose.

To configure a Mobile VPN with SSL connection in Policy Manager, select **VPN > Mobile VPN > SSL**.

Define a new user for Firebox authentication

1. From Policy Manager, select **Setup > Authentication > Authentication Servers**.
The Authentication Servers dialog box appears.



- From the **Firebox** tab of the **Authentication Servers** dialog box, click **Add** below the **Users** list. The *Setup Firebox User* dialog box appears.

- Type the name and (optional) a description of the new user.
- Type, and type again to confirm, the passphrase you want the person to use to authenticate to the Firebox.
When this passphrase is set, you cannot see the passphrase in simple text again. If you lose the passphrase, you must set a new passphrase.
- In the **Session Timeout** field, set the maximum length of time the user can send traffic to the external network. If you set this field to zero (0) seconds, minutes, hours, or days, no session timeout is used and the user can stay connected for any length of time.
- In the **Idle Timeout** field, set the length of time the user can stay authenticated when idle (not passing any traffic to the external network). If you set this field to zero (0) seconds, minutes, hours, or days, no idle timeout is used and the user can stay idle for any length of time.
For both timeout fields, the global authentication timeouts for the Firebox are used if the values are not defined in this dialog box. To set the global timeout value, see [Set global authentication values](#).
- To add the user to a group, select the user name in the **Available** list. Click the double arrow that points left to move the name to the **Member** list.
You can also double-click the group name.
- After you add the user to selected groups, click **OK**.
The user is added to the user list. You can then add more users.
- To close the **Setup Firebox User** dialog box, click **OK**.
The Firebox Users tab appears with a list of the new users.

Define a new group for Firebox authentication

1. From the **Firebox** tab of the **Authentication Servers** dialog box, click **Add** below the **User Groups** list. *The Setup Firebox Group dialog box appears.*



2. Type the group name that you want.
3. (Optional) Type a description for the new group.
4. To add a user to the group, select the user name in the **Available** list. Click the double arrow that points left to move the name to the **Member** list. *You can also double-click the group name.*
5. After you add all necessary users to the group, click **OK**.

At this time, you can use the users and groups to configure policies and authentication, as described in [Use authorized users and groups in policies](#).

Configure RADIUS server authentication

Remote Authentication Dial-In User Service (RADIUS) authenticates the local and remote users on a company network. RADIUS is a client/server system that keeps the authentication information for users, remote access servers, VPN gateways, and other resources in one central database.

For more information on RADIUS authentication, see [How RADIUS server authentication works](#).

Authentication key

The authentication messages to and from the RADIUS server always use an authentication key. This authentication key, or shared secret, must be the same on the RADIUS client and server. Without this key, hackers cannot get to the authentication messages. Note that RADIUS sends a key, and not a password, during authentication.

RADIUS authentication methods

For web and Mobile VPN with IPsec or SSL authentication, RADIUS supports only PAP (Password Authentication Protocol) authentication.

For authentication with PPTP, RADIUS supports only MSCHAPv2 (Microsoft Challenge-Handshake Authentication Protocol version 2).

Before you begin


Before you configure the Firebox to use your RADIUS authentication server, you must know your:

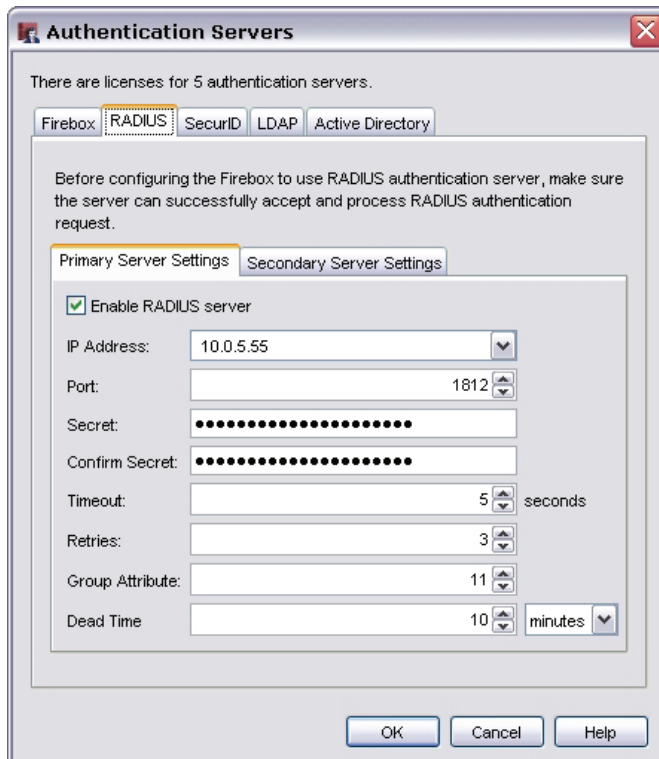
- RADIUS server IP address and port.
- If you have a backup RADIUS server, you must know its IP address and the port it uses for RADIUS.
- Shared secret — The shared secret is a password that is case-sensitive. It must be the same on the Firebox and the RADIUS server
- Authentication methods — Your RADIUS server must allow the authentication method the Firebox uses: PAP or MS CHAP v2.

Use RADIUS server authentication with the Firebox

To use RADIUS server authentication with the Firebox, you must:

- Add the IP address of the Firebox to the RADIUS server, as described in the RADIUS vendor documentation.
- Enable and specify the RADIUS server in your Firebox configuration.
- Add RADIUS user names or group names into your policies.

1. From Policy Manager, click .
Or, select **Setup > Authentication > Authentication Servers**.
2. Click the **RADIUS Server** tab.



Authentication Servers

There are licenses for 5 authentication servers.

Firebox **RADIUS** SecurID LDAP Active Directory

Before configuring the Firebox to use RADIUS authentication server, make sure the server can successfully accept and process RADIUS authentication request.

Primary Server Settings Secondary Server Settings

☒ Enable RADIUS server

IP Address: 10.0.5.55

Port: 1812

Secret:

Confirm Secret:

Timeout: 5 seconds

Retries: 3

Group Attribute: 11

Dead Time: 10 minutes

OK Cancel Help

3. To enable the RADIUS server and enable the fields on this dialog box, select the **Enable RADIUS server** check box.
4. In the **IP Address** box, type the IP address of the RADIUS server.
5. In the **Port** 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 **Secret** box, type the shared secret between the Firebox and the RADIUS server. Retype the shared secret in the **Confirm Secret** box.
The shared secret is case-sensitive, and it must be the same on the Firebox 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 Firebox waits for a response from the authentication server before it tries to connect again.
8. To set how many connection attempts the Firebox makes, use the **Retries** value control to set the number you want. This is the number of times the Firebox tries to connect to the authentication server (using the timeout specified above) before it reports a failed connection for one authentication attempt.
9. To set the group attribute, use the **Group Attribute** value control to set the attribute you want. The default group attribute is **FilterID**, which is RADIUS attribute 11.
The group attribute value is used to set which attribute carries the User Group information. You must configure the RADIUS server so that, when it sends a message to the Firebox that a user is authenticated, it also sends a FilterID string; for example, engineerGroup or financeGroup. This information is then used for access control; it matches the FilterID string to the group name configured in the Firebox policies.
10. To set a time after which a dead server is marked as active again, enter it in the **Dead Time** field.
After an authentication server has not responded for a period of time, it is marked as dead. Subsequent authentication attempts will not try this server until it is marked as active again.
11. To add a backup RADIUS server, select the **Secondary Server Settings** tab, and select the **Enable a secondary RADIUS server** check box. Enter the information in the required fields. Make sure the shared secret is the same on the primary and backup RADIUS server. For more information, see [Use a backup authentication server](#).
12. Click **OK**. [Save the configuration file](#).

How RADIUS server authentication works

RADIUS is a protocol that was originally designed for authenticating remote users to a dial-in access server. RADIUS is now used in a wide range of authentication scenarios. RADIUS is a client-server protocol, with the Firebox as the client and the RADIUS server as the server. (The RADIUS client is sometimes called the Network Access Server or NAS.) When a user tries to authenticate, the Firebox sends a message to the RADIUS server. If the RADIUS server is properly configured to have the Firebox as a client, RADIUS sends an accept or reject message back to the Firebox (the Firebox is the Network Access Server).

When the Firebox uses RADIUS for an authentication attempt, these things happen:

1. The user tries to authenticate, either by making a browser-based HTTPS connection to the Firebox over port 4100, or by trying to make a connection using Mobile VPN with PPTP or IPSec. The Firebox reads the user's name and password.
2. The Firebox creates a message called an Access-Request message and sends it to the RADIUS server. The Firebox uses the RADIUS shared secret in the message. The user's password is always encrypted in the Access-Request message.
3. The RADIUS server makes sure that the Access-Request message is from a known client (the Firebox). If RADIUS is not configured with the Firebox as a client, RADIUS discards the Access-Request message and does not send a message back.

4. If the Firebox is a client known to the RADIUS server and the shared secret is correct, RADIUS looks at the authentication method requested in the Access-Request message.
5. If the Access-Request message uses an allowed authentication method, RADIUS gets the user's credentials from the message and looks for a match in a user database. If the user name and password match an entry in the database, the RADIUS server can get additional information about the user from the user database (such as remote access approval, group membership, logon hours, and so on).
6. RADIUS checks to see whether it has an access policy or a profile in its configuration that matches all the information it has about the user. If such a policy exists, RADIUS sends a response.
7. If any of the previous conditions fail, or if the RADIUS server has no matching policy, RADIUS sends an Access-Reject message that shows authentication failure. The RADIUS transaction ends and the user is denied access.
8. If the Access-Request message meets all the previous conditions, RADIUS sends an Access-Accept message to the Firebox.
9. RADIUS uses the shared secret for any response it sends. If the shared secret does not match between the RADIUS server and the Firebox, Fireware rejects any response from RADIUS. To see diagnostic messages for authentication, [enable advanced diagnostics](#) and expand the **Authentication** category.
10. The Firebox reads the value of any Filter-Id attribute in the message. It connects the user name with the Filter-Id attribute to put the user in a RADIUS Group.
11. RADIUS can put a large amount of additional information in the Access-Accept message, but the Firebox ignores most of it. Additional information can include the protocols the user is allowed to use (such as PPP or SLIP), the ports the user can access, idle timeouts, and other attributes that the Firebox ignores.
12. The only attribute the Firebox looks for in the Access-Accept message is the Filter-Id attribute (RADIUS attribute number 11). The Filter-Id is a string of text that you configure RADIUS to include in the Access-Accept message. The Filter-Id attribute is necessary for the Firebox to assign the user to a RADIUS Group. For more information on RADIUS Groups, see the next section.

About RADIUS groups

When you configure RADIUS authentication, you can set the Group Attribute number. Fireware reads the Group Attribute number from Policy Manager to tell which RADIUS attribute carries RADIUS Group information. Fireware recognizes only RADIUS attribute number 11, Filter-Id, as the Group Attribute. In the steps to configure the RADIUS server, do not change the Group Attribute number from its default value of 11.

When the Firebox gets the Access-Accept message from RADIUS, it reads the value of the Filter-Id attribute and uses this value to associate the user to a RADIUS Group. (You must manually configure the Filter-Id in your RADIUS configuration.) Thus, the value of the Filter-Id attribute is the name of the RADIUS Group the Firebox puts the user in.

The RADIUS Groups you use in Policy Manager are not the same as the Windows groups defined in your domain controller, or any other groups that exist in your domain's user database. A RADIUS Group is only a logical grouping of users the Firebox uses. Give consideration to the string of text you use for the Filter-Id. If you want, you can make the value of the Filter-Id match the name of a local group or domain group in your organization, but this is not necessary. We suggest you use a descriptive name that helps you remember the reason to group users this way.

Practical use of RADIUS groups

If your organization has many users to authenticate, you can make your Firebox policies easier to administer by configuring RADIUS to send the same Filter-Id value for many users. The Firebox puts those users into one logical group so you can more easily administer user access. When you make a policy in Policy Manager that allows only authenticated users to access a network resource, you use the RADIUS Group name instead of adding a list of many individual users.

For example, if the Filter-Id string RADIUS sends when Mary authenticates is Sales, that is the name of the RADIUS Group the Firebox puts Mary in for as long as Mary is authenticated. If users John and Alice subsequently authenticate, and RADIUS puts the same Filter-Id value Sales in the Access-Accept messages for John and Alice, then Mary, John, and Alice are all in the Sales group. Now you can make a policy in Policy Manager that allows the group Sales to access a resource.

You can configure RADIUS to return a different Filter-Id, for example IT Support, for the members of your internal support organization. You make a different policy to allow IT Support users to access resources.

For example, you might allow the Sales group to access the Internet using the Proxied-HTTP policy. Then you can filter their web access with WebBlocker. A different policy in Policy Manager can allow the IT Support users to access the Internet with the Filtered-HTTP policy, so that they access the web without WebBlocker filtering. You use the RADIUS group name (or user names) in the From field of a policy to show which group (or which users) can use the policy.

Timeout and retry values

Fireware starts to use the backup server after three authentication attempts fail because of no response. (Note that this number is not the same as the Retry number. You cannot change this failover threshold.)

The Firebox sends an Access-Request message to the first RADIUS server shown. If there is no response, Fireware waits the number of seconds shown in the Timeout box, and then it sends another Access-Request. This continues for the number of times indicated in the Retry box (or until there is a valid response). If there is no valid response from the RADIUS server after this, Fireware counts this as one failed authentication attempt due to no response. (Note that if the RADIUS shared secret does not match, Fireware treats the bad response as no response.)

After three authentication attempts fail due to no response, Fireware uses the backup RADIUS server for its next authentication attempt. If the same thing happens with the backup server (three authentication attempts fail due to no valid response), Fireware waits ten minutes for an administrator to correct the problem. After ten minutes Fireware tries to use the primary RADIUS server again.


Configure VASCO server authentication

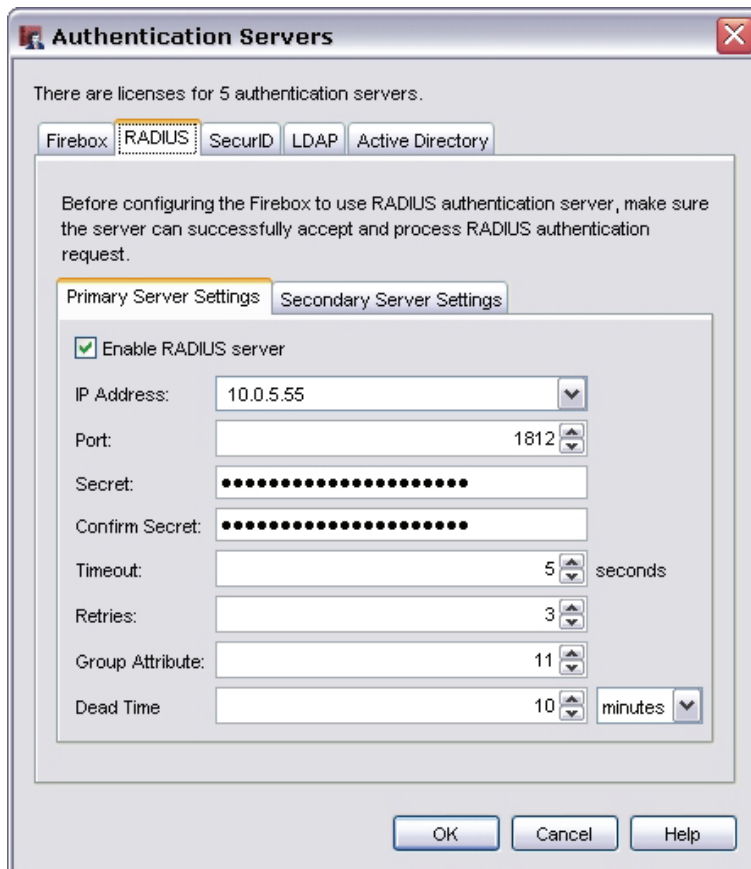
VASCO server authentication uses the VACMAN Middleware software to authenticate remote users on a company network through a RADIUS or web server environment. VASCO also supports multiple authentication server environments. The VASCO one-time password token system enables you to eliminate the weakest link in your security infrastructure — the use of static passwords.

To use VASCO server authentication with the Firebox, you must:

- Add the IP address of the Firebox to the VACMAN Middleware server, as described in the VASCO vendor documentation.
- Enable and specify the VACMAN Middleware server in your Firebox configuration.
- Add user names or group names into the policies in Policy Manager.

VASCO server authentication is configured using the RADIUS server settings. The **Authentication Servers** dialog box does not have a separate tab for VACMAN Middleware servers.

1. From Policy Manager, click .
Or, select **Setup > Authentication > Authentication Servers**.
2. Click the **RADIUS** tab.




The screenshot shows the 'Authentication Servers' dialog box with the 'RADIUS' tab selected. The dialog has a title bar with a close button. Inside, it says 'There are licenses for 5 authentication servers.' Below this are tabs for 'Firebox', 'RADIUS', 'SecurID', 'LDAP', and 'Active Directory'. The 'RADIUS' tab is active. A message states: 'Before configuring the Firebox to use RADIUS authentication server, make sure the server can successfully accept and process RADIUS authentication request.' Below this are two sub-tabs: 'Primary Server Settings' (selected) and 'Secondary Server Settings'. Under 'Primary Server Settings', there is a checked checkbox 'Enable RADIUS server'. Below it are several fields: 'IP Address' (10.0.5.55), 'Port' (1812), 'Secret' (masked with dots), 'Confirm Secret' (masked with dots), 'Timeout' (5 seconds), 'Retries' (3), 'Group Attribute' (11), and 'Dead Time' (10 minutes). At the bottom are 'OK', 'Cancel', and 'Help' buttons.

3. To enable the VACMAN Middleware server and enable the fields on this dialog box, select the **Enable RADIUS server** check box.
4. In the **IP Address** box, type the IP address of the VACMAN Middleware server.
5. In the **Port** box, make sure that the port number VASCO uses for authentication appears. The default port number is 1812.

6. In the **Secret** box, type the shared secret between the Firebox and the VACMAN Middleware server. Retype the shared secret in the **Confirm Secret** box.
The shared secret is case-sensitive, and it must be the same on the Firebox 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 Firebox waits for a response from the authentication server before it tries to connect again.
8. To set how many connection attempts the Firebox makes, use the **Retries** value control to set the number you want.
This is the number of times the Firebox tries to connect to the authentication server (using the timeout specified above) before it reports a failed connection for one authentication attempt.
9. To set the group attribute, use the **Group Attribute** value control to set the attribute you want.
The default group attribute is **FilterID**, which is VASCO attribute 11.
The group attribute value is used to set which attribute carries the User Group information. You must configure the VASCO server so that, when it sends a message to the Firebox that a user is authenticated, it also sends a FilterID string; for example, engineerGroup or financeGroup. This information is then used for access control; it matches the FilterID string to the group name configured in the Firebox policies.
10. To set a time after which a dead server is marked as active again, enter it in the **Dead Time** field.
After an authentication server has not responded for a period of time, it is marked as dead. Subsequent authentication attempts will not try this server until it is marked as active again.
11. To add a backup VACMAN Middleware server, select the **Secondary Server Settings** tab, and select the **Enable a secondary RADIUS server** check box.
Enter the information in the required fields. Make sure the shared secret is the same on the primary and backup VACMAN Middleware server. For more information, see [Use a backup authentication server](#).
12. Click **OK**. [Save the configuration file](#).

Configure SecurID authentication

To use SecurID authentication, you must configure the RADIUS, VASCO, and ACE/Server servers correctly. The users must also have an approved SecurID token and a PIN (personal identification number). Refer to the RSA SecurID instructions for more information.

1. From Policy Manager, click .
Or, select **Setup > Authentication > Authentication Servers**.
2. Click the **SecurID** tab.




The screenshot shows the 'Authentication Servers' dialog box with the 'SecurID' tab selected. The dialog has a title bar with a close button. Inside, it says 'There are licenses for 5 authentication servers.' Below this are tabs for 'Firebox', 'RADIUS', 'SecurID' (selected), 'LDAP', and 'Active Directory'. A note states: 'Before configuring the Firebox to point to SecurID authentication server, make sure that the users can successfully authenticate to the server.' Below the note are two sub-tabs: 'Primary Server Settings' (selected) and 'Backup Server Settings'. Under 'Primary Server Settings', there is a checked checkbox 'Enable SecurID server'. Below this are several fields: 'IP Address' (text box with '10.0.1.55'), 'Port' (spin box with '1812'), 'Secret' (password field with dots), 'Confirm' (password field with dots), 'Timeout' (spin box with '10' and 'seconds' label), 'Retry' (spin box with '3'), 'Group Attribute' (spin box with '11'), and 'Dead Time' (spin box with '10' and 'minutes' label). At the bottom are 'OK', 'Cancel', and 'Help' buttons.

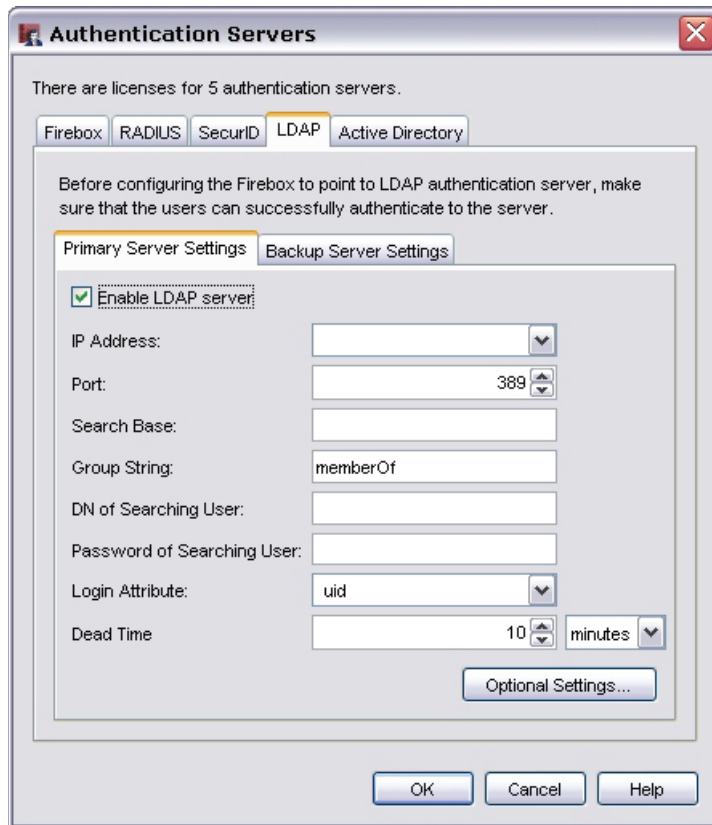
3. To enable the SecurID server and enable the fields on this dialog box, select the **Enable SecurID server** check box.
4. In the **IP Address** box, type the IP address of the SecurID server.
5. In the **Port** box, use the value control to select the port number to use for SecurID authentication. The default number is 1812.
6. In the **Secret** box, type the shared secret between the Firebox and SecurID server. The shared secret is case-sensitive and must be the same on the Firebox and SecurID 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 Firebox waits for a response from the authentication server before it tries to connect again.
8. To set how many connection attempts the Firebox makes, use the **Retry** value control. This is the number of times the Firebox tries to connect to the authentication server (using the timeout specified above) before it reports a failed connection for one authentication attempt.

9. Select the group attribute. We recommend that you do not change this value.
The group attribute value is used to set which attribute carries the User Group information. When the SecurID server sends a message to the Firebox that a user is authenticated, it also sends a User Group string; for example, engineerGroup or financeGroup. This information is then used for access control.
10. To set a time after which a dead server is marked as active again, enter it in the **Dead Time** field. After an authentication server has not responded for a period of time, it is marked as dead. Subsequent authentication attempts will not try this server until it is marked as active again after the dead time value is reached.
11. To add a backup SecurID server, select the **Secondary Server Settings** tab, and select the **Enable a secondary SecurID server** check box. Enter the information in the required fields. Make sure the shared secret is the same on the primary and backup SecurID server. For more information, see [Use a backup authentication server](#).
12. Click **OK**. [Save the configuration file](#).

Configure LDAP authentication

You can use an LDAP (Lightweight Directory Access Protocol) authentication server to authenticate your users to the Firebox. LDAP is an open-standard protocol for using online directory services, and it operates with Internet transport protocols, such as TCP. Before you configure your Firebox for LDAP authentication, make sure you check your LDAP vendor documentation to see if your installation requires case-sensitive attributes.

1. From Policy Manager, click .
Or, select **Setup > Authentication > Authentication Servers**.
2. Click the **LDAP** tab.



Authentication Servers

There are licenses for 5 authentication servers.

Firebox | RADIUS | SecurID | **LDAP** | Active Directory

Before configuring the Firebox to point to LDAP authentication server, make sure that the users can successfully authenticate to the server.

Primary Server Settings | Backup Server Settings

☒ **Enable LDAP server**

IP Address:

Port:

Search Base:

Group String:

DN of Searching User:

Password of Searching User:

Login Attribute:

Dead Time: minutes

[Optional Settings...](#)

OK Cancel Help

3. To enable the LDAP server and enable the fields on this dialog box, select the **Enable LDAP server** check box.
4. In the **IP Address** box, type the IP address of the primary LDAP server for the Firebox to contact with authentication requests.
The LDAP server can be located on any Firebox interface. You can also configure your Firebox to use an LDAP server through a VPN tunnel.
5. From the **Port** drop-down list, select the TCP port number for the Firebox to use to connect to the LDAP server. The default port number is 389.
We do not support LDAP over TLS.

6. Type the **Search Base**. The standard format for the search base setting is: ou=organizational unit,dc=first part of distinguished server name,dc=any part of the distinguished server name that appears after the dot.
You set a search base to put limits on the directories on the authentication server the Firebox searches in for an authentication match. For example, if your user accounts are in an OU (organizational unit) you refer to as accounts and your domain name is mywatchguard.com, your search base is: ou=accounts,dc=mywatchguard,dc=com.
7. Type the **Group String**.
This attribute string holds user group information on the LDAP server. On many LDAP servers, the default group string is uniqueMember; on other servers it is member.
8. In the **DN of Searching User** field, type the distinguished name (DN) for a search operation. You can enter any user DN with the privilege to search LDAP/Active Directory, such as Administrator. A weaker user DN with only searching privilege is usually sufficient, and some administrators create a user with searching privileges but limited permissions to use in this field.
9. In the **Password of Searching User** field, type the password associated with the distinguished name for a search operation.
10. In the **Login Attribute** field, type the LDAP login attribute to use for authentication. The login attribute is the name used for the bind to the LDAP database.
The default login attribute is uid. If you use uid, the **DN of Searching User** field and the **Password of Searching User** field can be empty.
11. To set a time after which a dead server is marked as active again, enter it in the **Dead Time** field.
After an authentication server has not responded for a period of time, it is marked as dead. Subsequent authentication attempts will not try this server until it is marked as active again.
12. To add a backup LDAP server, select the **Backup Server Settings** tab, and select the **Enable a secondary LDAP server** check box. Enter the information in the required fields. Make sure the shared secret is the same on the primary and backup LDAP server. For more information, see [Use a backup authentication server](#).

About LDAP optional settings

Fireware can get additional information from the directory server (LDAP or Active Directory) when it reads the list of attributes in the server's search response. This lets you use the directory server to assign extra parameters to the authenticated user's session, such as timeouts and Mobile VPN with IPsec address assignments. Because the data comes from LDAP attributes associated with individual user objects, you can set these parameters for each individual user instead of being limited to global settings in Policy Manager.

For more information, see [Use Active Directory or LDAP optional settings](#).

Use Active Directory or LDAP optional settings

Fireware can get additional information from the directory server (Active Directory or LDAP) when it reads the list of attributes in the server's search response. This lets you use the directory server to assign extra parameters to the authenticated user's session, such as timeouts and Mobile VPN address assignments. Because the data comes from LDAP attributes associated with individual user objects, you can set these parameters for each individual user instead of being limited to global settings in Policy Manager.

Before You Begin

You must perform several steps to use these optional settings:

- Extend the directory schema to add new attributes for these items.
- Make the new attributes available to the object class that user accounts belong to.
- Give values to the attributes for the user objects that should use them.

You should do careful planning and testing before you extend your directory schema. Additions to the Active Directory schema, for example, are generally permanent and cannot be undone. Use the Microsoft web site to get resources to plan, test, and implement changes to an Active Directory schema. Consult the documentation from your LDAP vendor before you extend the schema for other directories.

Specify Active Directory or LDAP optional settings

To specify additional attributes for Fireware to look for in the directory server's search response, click **Optional Settings** on the **LDAP** tab or the **Active Directory** tab at **Setup > Authentication > Authentication Servers**.

Fireware looks for the attributes you type in this dialog box in the list of attributes it gets from the search result, and then uses the attribute's value as follows:

IP Attribute String

This field applies only to Mobile VPN clients.

Type the name of the attribute Fireware should use to assign the Mobile VPN client a virtual IP address. This should be a single-valued attribute. The attribute's value should be a normal dotted-decimal IP address. The IP address must be within the pool of virtual IP addresses you specify when you create the Mobile VPN Group.

If the Firebox does not see the IP attribute in the search response, or if you do not specify an attribute in Policy Manager, it assigns the Mobile VPN client a virtual IP address from the virtual IP address pool you create when you make the Mobile VPN Group.

Netmask Attribute String

This field applies only to Mobile VPN clients.

Type the name of the attribute for Fireware to use to assign a subnet mask to the Mobile VPN client's virtual IP address. This should be a single-valued attribute. The attribute's value should be a normal dotted-decimal subnet mask.

The Mobile VPN software automatically assigns a netmask if the Firebox does not see the netmask attribute in the search response, or if you do not specify one in Policy Manager.

DNS Attribute String

This field applies only to Mobile VPN clients.

Type the name of the attribute Fireware should use to assign the Mobile VPN client one or more DNS addresses for the duration of the Mobile VPN session. This can be a multi-valued attribute. Each value for the attribute should be a normal dotted-decimal IP address. If the Firebox does not see the DNS attribute in the search response, or if you do not specify an attribute in Policy Manager, it uses the WINS addresses you enter when you [Configure WINS and DNS servers](#).

WINS Attribute String

This applies only to Mobile VPN clients. Type the name of the attribute Fireware should use to assign the Mobile VPN client one or more WINS addresses for the duration of the Mobile VPN session. This can be a multi-valued attribute. Each value for the attribute should be a normal dotted-decimal IP address. If the Firebox does not see the WINS attribute in the search response or if you do not specify an attribute in Policy Manager, it uses the WINS addresses you enter when you [Configure WINS and DNS servers](#).

Lease Time Attribute String

This can apply to Mobile VPN clients and to clients that use Firewall Authentication. Type the name of the attribute for Fireware to use to control the absolute amount of time a user can stay authenticated (session timeout). After this amount of time, Fireware removes the user from its list of authenticated users. This should be a single-valued attribute. Fireware interprets the attribute's value as a decimal number of seconds. It interprets zero as *never time out*.

Idle Timeout Attribute String


This applies to Mobile VPN clients and to clients that use Firewall Authentication. Type the name of the attribute Fireware should use to control the amount of time a user can stay authenticated with no traffic passing to the Firebox from the user (idle timeout). If no traffic passes to the Firebox for this amount of time, Fireware removes the user from its list of authenticated users. This should be a single-valued attribute. Fireware interprets the attribute's value as a decimal number of seconds. It interprets zero as *never time out*.

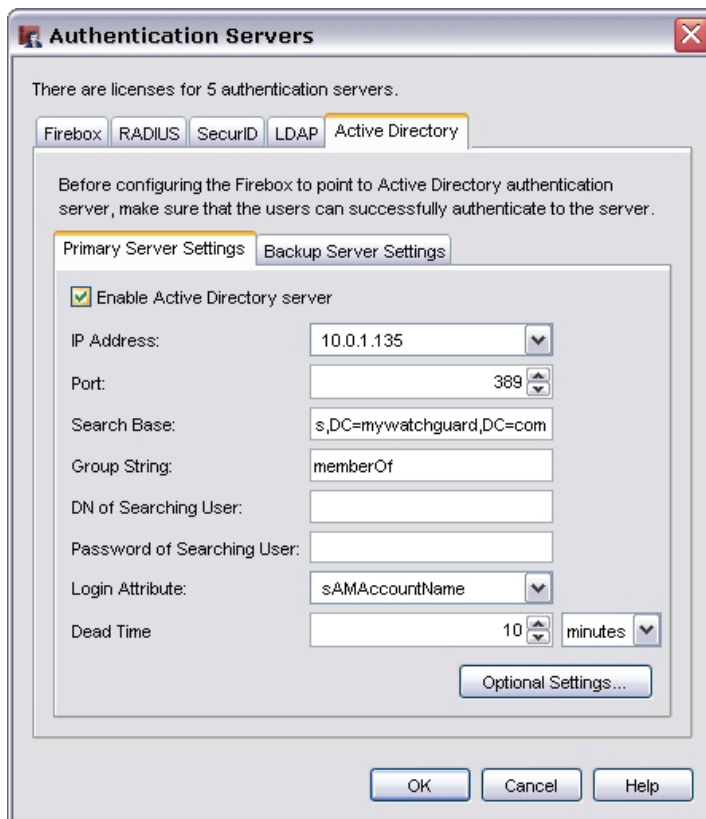
Configure Active Directory authentication

Active Directory is the Microsoft Windows-based application of LDAP directory structure. Active Directory lets you expand the concept of domain hierarchy used in DNS to an organizational level. It keeps information and settings for an organization in a central, easy-to-access database.

You can use an Active Directory authentication server to authenticate your users to the Firebox. You must configure both the Firebox and the Active Directory server.

Before you begin, make sure your users can successfully authenticate to the Active Directory server.

1. From Policy Manager, click .
Or, select **Setup > Authentication > Authentication Servers**.
2. Click the **Active Directory** tab.



The screenshot shows the 'Authentication Servers' dialog box with the 'Active Directory' tab selected. The dialog has a title bar with a close button. Inside, it says 'There are licenses for 5 authentication servers.' Below this are tabs for 'Firebox', 'RADIUS', 'SecurID', 'LDAP', and 'Active Directory'. The 'Active Directory' tab is active and contains a message: 'Before configuring the Firebox to point to Active Directory authentication server, make sure that the users can successfully authenticate to the server.' Below this message are two sub-tabs: 'Primary Server Settings' (selected) and 'Backup Server Settings'. Under 'Primary Server Settings', there is a checked checkbox 'Enable Active Directory server'. Below this are several input fields: 'IP Address' (10.0.1.135), 'Port' (389), 'Search Base' (s,DC=mywatchguard,DC=com), 'Group String' (memberOf), 'DN of Searching User' (empty), 'Password of Searching User' (empty), 'Login Attribute' (sAMAccountName), and 'Dead Time' (10 minutes). There is an 'Optional Settings...' button at the bottom right of the settings area. At the very bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons.

3. Select the **Enable Active Directory Server** check box.
4. Type the IP address of the primary Active Directory server. The Active Directory server can be located on any Firebox interface. You can also configure the Firebox to use an Active Directory server available through a VPN tunnel.
5. Select the TCP port number for the Firebox to use to connect to the Active Directory server. The default port number is 389.
If your Active Directory server is a global catalog server, it can be useful to change the default port. For more information, see [Change the default port for the Active Directory server](#).

6. In the **Search Base** field, type the location in the directory to begin the search. The standard format for the search base setting is: ou=organizational unit,dc=first part of distinguished server name,dc=any part of the distinguished server name that appears after the dot.
You set a search base to put limits on the directories on the authentication server the Firebox searches in for an authentication match. For example, if your user accounts are in an OU (organizational unit) you refer to as accounts and your domain name is HQ_main.com, your search base is:
ou=accounts,dc=HQ_main,dc=com.
For more information, see [Find your Active Directory search base](#).
7. In the **Group String** field, type the attribute string that is used to hold user group information on the Active Directory server. If you have not changed your Active Directory schema, the group string is always memberOf.
8. In the **DN of Searching User** field, type the distinguished name (DN) for a search operation. It is not necessary to enter anything in this text box if you keep the login attribute of sAMAccountName. If you change the login attribute, you must add a DN of Searching User to your configuration. You can enter any user DN with the privilege to search LDAP/Active Directory, such as Administrator. However, a weaker user DN with only searching privilege is usually sufficient.
9. In the **DN of Searching Password** field, type the password associated with the distinguished name for a search operation.
10. In the **Login Attribute** field, type an Active Directory login attribute to use for authentication. The login attribute is the name used for the bind to the Active Directory database.
The default login attribute is sAMAccountName. If you use sAMAccountName, the **DN of Searching User** field and the **DN of Searching Password** field can be empty.
11. To set a time after which a dead server is marked as active again, enter it in the **Dead Time** field.
After an authentication server has not responded for a period of time, it is marked as dead. Subsequent authentication attempts will not try this server until it is marked as active again.
12. To add a backup Active Directory server, select the **Backup Server Settings** tab, and select the **Enable a secondary Active Directory server** check box. Enter the information in the required fields. Make sure the shared secret is the same on the primary and backup Active Directory server. For more information, see [Use a backup authentication server](#).

About Active Directory optional settings

Fireware can get additional information from the directory server (LDAP or Active Directory) when it reads the list of attributes in the server's search response. This lets you use the directory server to assign extra parameters to the authenticated user's session, such as timeouts and MUVPN address assignments. Because the data comes from LDAP attributes associated with individual user objects, you can set these parameters for each individual user instead of being limited to global settings in Policy Manager.

For more information, see [Use Active Directory or LDAP optional settings](#).

Use Active Directory or LDAP optional settings

Fireware can get additional information from the directory server (Active Directory or LDAP) when it reads the list of attributes in the server's search response. This lets you use the directory server to assign extra parameters to the authenticated user's session, such as timeouts and Mobile VPN address assignments. Because the data comes from LDAP attributes associated with individual user objects, you can set these parameters for each individual user instead of being limited to global settings in Policy Manager.

Before You Begin

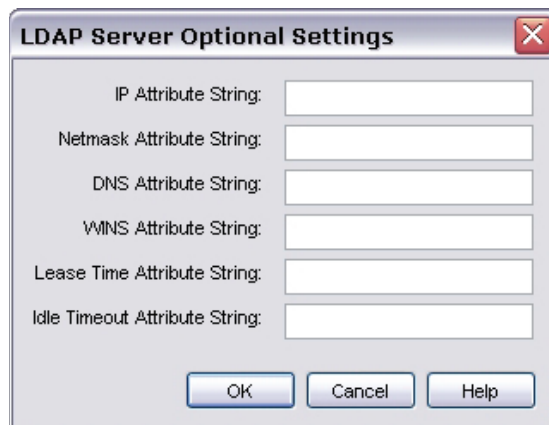
You must perform several steps to use these optional settings:

- Extend the directory schema to add new attributes for these items.
- Make the new attributes available to the object class that user accounts belong to.
- Give values to the attributes for the user objects that should use them.

You should do careful planning and testing before you extend your directory schema. Additions to the Active Directory schema, for example, are generally permanent and cannot be undone. Use the Microsoft web site to get resources to plan, test, and implement changes to an Active Directory schema. Consult the documentation from your LDAP vendor before you extend the schema for other directories.

Specify Active Directory or LDAP optional settings

To specify additional attributes for Fireware to look for in the directory server's search response, click **Optional Settings** on the **LDAP** tab or the **Active Directory** tab at **Setup > Authentication > Authentication Servers**.



The dialog box is titled "LDAP Server Optional Settings" and has a close button (X) in the top right corner. It contains six text input fields, each with a label to its left: "IP Attribute String:", "Netmask Attribute String:", "DNS Attribute String:", "WINS Attribute String:", "Lease Time Attribute String:", and "Idle Timeout Attribute String:". At the bottom of the dialog box are three buttons: "OK", "Cancel", and "Help".

Fireware looks for the attributes you type in this dialog box in the list of attributes it gets from the search result, and then uses the attribute's value as follows:

IP Attribute String

This field applies only to Mobile VPN clients.

Type the name of the attribute Fireware should use to assign the Mobile VPN client a virtual IP address. This should be a single-valued attribute. The attribute's value should be a normal dotted-decimal IP address. The IP address must be within the pool of virtual IP addresses you specify when you create the Mobile VPN Group.

If the Firebox does not see the IP attribute in the search response, or if you do not specify an attribute in Policy Manager, it assigns the Mobile VPN client a virtual IP address from the virtual IP address pool you create when you make the Mobile VPN Group.

Netmask Attribute String

This field applies only to Mobile VPN clients.

Type the name of the attribute for Firewall to use to assign a subnet mask to the Mobile VPN client's virtual IP address. This should be a single-valued attribute. The attribute's value should be a normal dotted-decimal subnet mask.

The Mobile VPN software automatically assigns a netmask if the Firebox does not see the netmask attribute in the search response, or if you do not specify one in Policy Manager.

DNS Attribute String

This field applies only to Mobile VPN clients.

Type the name of the attribute Firewall should use to assign the Mobile VPN client one or more DNS addresses for the duration of the Mobile VPN session. This can be a multi-valued attribute. Each value for the attribute should be a normal dotted-decimal IP address. If the Firebox does not see the DNS attribute in the search response, or if you do not specify an attribute in Policy Manager, it uses the WINS addresses you enter when you [Configure WINS and DNS servers](#).

WINS Attribute String

This applies only to Mobile VPN clients. Type the name of the attribute Firewall should use to assign the Mobile VPN client one or more WINS addresses for the duration of the Mobile VPN session. This can be a multi-valued attribute. Each value for the attribute should be a normal dotted-decimal IP address. If the Firebox does not see the WINS attribute in the search response or if you do not specify an attribute in Policy Manager, it uses the WINS addresses you enter when you [Configure WINS and DNS servers](#).

Lease Time Attribute String

This can apply to Mobile VPN clients and to clients that use Firewall Authentication. Type the name of the attribute for Firewall to use to control the absolute amount of time a user can stay authenticated (session timeout). After this amount of time, Firewall removes the user from its list of authenticated users. This should be a single-valued attribute. Firewall interprets the attribute's value as a decimal number of seconds. It interprets zero as *never time out*.

Idle Timeout Attribute String

This applies to Mobile VPN clients and to clients that use Firewall Authentication. Type the name of the attribute Firewall should use to control the amount of time a user can stay authenticated with no traffic passing to the Firebox from the user (idle timeout). If no traffic passes to the Firebox for this amount of time, Firewall removes the user from its list of authenticated users. This should be a single-valued attribute. Firewall interprets the attribute's value as a decimal number of seconds. It interprets zero as *never time out*.

Find your Active Directory search base

When you configure the Firebox to use an existing Active Directory server to authenticate users, you add a *search base*. The search base gives a place in the Active Directory hierarchical structure to start the search for user account entries. This can help to make the authentication procedure faster.

Before you start, you must have an operational Active Directory server that contains account information for all users who you want to configure authentication for on the Firebox.

1. On your Active Directory server, select **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
2. Find your domain name in the tree. Expand the tree to find the path through your Active Directory hierarchy. Look for the lowest organizational unit that contains all users who you want to authenticate through the Firebox. Remember that organizational units can contain other organizational units.

- After you find the organizational unit that contains the users you want to authenticate, write the path through the tree to this organizational unit. Start at the lowest organization unit and write all higher organization units as you move up the tree to your domain name. Organizational units have the format `ou=organizational unit name` and are comma-delimited. Domain name components have the format `dc=domain name component`, are appended to the end of the search base string, and comma-delimited.

For example, suppose your domain name in the tree looks like this after you expand it:



In this example, all the users that must authenticate to the Firebox are in the Active Directory organizational unit Outside Sales. The search base string to enter in the Firebox configuration would be:

`OU=Outside Sales,OU=Sales,OU=Accounts,DC=Kunstlerandsons,DC=com`

The search string is not case-sensitive. When you type your search string, you can use either uppercase or lowercase letters.

Special conditions

Suppose all the users in your domain are in the Users folder, shown at the bottom of the hierarchy in the figure above. The Users folder is a container, not an organizational unit. You identify a container with the format `cn=container name`. If all the users are in the Users container, you can use this format for the search base: `UN=Users,DC=Domain name component,DC=Domain name component`

For the Kunstler and Son example, the search base would be: `CN=Users,DC=Kunstlerandsons,DC=com`

Suppose some of your users are in the Users folder, and some users are in organizational units. The lowest path in the Active Directory that contains all the accounts is the domain itself. If your domain is like this, your search base must be: `DC=Domain name component,DC=Domain name component`

For the Kunstler and Sons example, the search base would be: `DC=Kunstlerandsons,DC=com`

DN of Searching User, Password of Searching User fields

You must fill in these fields only if you select an option for the **Login Attribute** field that is different from the default value `sAMAccountName`. Most organizations that use Active Directory do not change this. When you leave this field at the default `sAMAccountName`, a user supplies their usual Active Directory login name for their user name when they authenticate. This is the name you see in the **User** logon name field on the **Account** tab when you edit the user account in Active Directory Users and Computers.

If you use a different value for the **Login Attribute** field, a user who tries to authenticate gives a different form of the user name. In this case, you must add Searching User credentials to your Firebox configuration.


Change the default port for the Active Directory server

If your Firebox is configured to authenticate users with an Active Directory (AD) authentication server, it connects to the Active Directory server by default on the standard LDAP port, which is TCP port 389. If the Active Directory servers that you add to your Firebox configuration are set up to be Active Directory global catalog servers, you can tell the Firebox to use the global catalog port, TCP port 3268, to connect to the Active Directory server.

A *global catalog server* is a domain controller that stores information about all objects in the forest so that applications can search Active Directory without referring to specific domain controllers that store the requested data. If you have only one domain, Microsoft recommends that you configure all domain controllers as global catalog servers.

If the primary (and secondary if you use it) Active Directory server you list in your Firebox configuration is also configured as a global catalog server, changing the port the Firebox uses to connect to the Active Directory server can increase the speed of authentication requests. At the same time, it is not recommended that you create additional Active Directory global catalog servers just to speed up authentication requests. The replication that occurs among multiple global catalog servers can use significant bandwidth on your network.

Configure the Firebox to use the global catalog port

1. From Policy Manager, click .
Or, select **Setup > Authentication > Authentication Servers**.
2. Click the **Active Directory** tab.
3. Clear the contents of the **Port** text box and type **3268**.
4. Click **OK**.
5. [Save the configuration file](#).

To find out if your Active Directory server is configured to be a global catalog server

1. Select **Start Menu > Administrative Tools > Active Directory Sites and Services**.
2. Expand the **Sites** tree view in the left pane to find the name of your Active Directory server.
3. Right-click **NTDS Settings** for your Active Directory server and look at **Properties**. If the **Global Catalog** check box is selected, the Active Directory server is configured to be a global catalog.

Use a local user account for authentication

Any user can authenticate as a Firewall user, PPTP user, or Mobile VPN user, and open a PPTP or Mobile VPN tunnel if PPTP or Mobile VPN is enabled on the Firebox. However, after an authentication or tunnel has been successfully established, users can send traffic through the VPN tunnel only if the traffic is allowed by a policy on the Firebox. For example, a Mobile VPN-only user can send traffic through a Mobile VPN tunnel, but not a PPTP tunnel even though the user can authenticate and bring up a PPTP tunnel.

If you use Active Directory authentication and a user's group membership does not match your Mobile VPN policy, you can see an error message that says *decrypted traffic does not match any policy*. If you see this error message, make sure that the user is in a group with the same name as your Mobile VPN group.

Use authorized users and groups in policies

When you configure the Firebox to use an authentication server, you can start to use specified user and group names when you create policies in Policy Manager. For example, you can define all policies so that connections are allowed only for authenticated users. Or, you can limit connections on a policy to particular users.

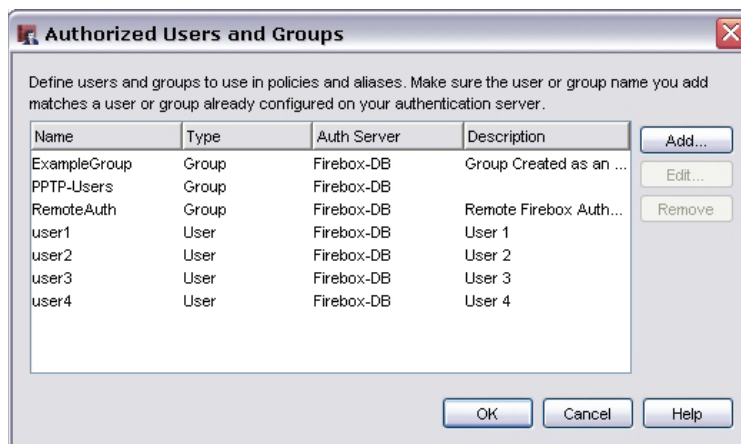
The term *authorized users and groups* refers to users and groups that are allowed to access network resources.

Define users and groups for Firebox authentication

If you use the Firebox as an authentication server and want to define users and groups that authenticate through the Firebox, see [Define a new user for Firebox authentication](#) and [Define a new group for Firebox authentication](#).

Define users and groups for third-party authentication

1. Create a group on your third-party authentication server that contains all the user accounts on your system.
2. In Policy Manager, select **Setup > Authentication > Authorized Users/Groups**.
The Authorized Users and Groups dialog box appears.



3. Click **Add**.
The Define New Authorized User or Group dialog box appears.



4. Type a user or group name you created on the authentication server.
5. (Optional) Type a description of the user or group.
6. Select the **Group** or **User** radio button.
7. From the **Auth Server** drop-down list, select either **RADIUS** (for authentication through a RADIUS or VACMAN Middleware server) or **Any** (for authentication through any other server). Click **OK**.

Add users and groups to policy definitions

Any user or group that you want to use in your policy definitions must be added as an authorized user. All users and groups you create for Firebox authentication and all Mobile VPN users are automatically added to the list of authorized users and groups on the **Authorized Users and Groups** dialog box. You can add any users or groups from third-party authentication servers to the authorized user and group list with the above procedure. You are then ready to add users and groups to your policy configuration.

1. From Policy Manager, double-click the icon for the policy definition.

The Edit Policy Properties dialog box appears.

2. Below the **From** box, click **Add**.

The Add Address dialog box appears.

3. Click **Add User**.

The Add Authorized Users or Groups dialog box appears.



4. In the **Type** box, select whether the user or group is authorized as a Firewall, PPTP, or SSLVPN user. For more information on these authentication types, see [Types of Firebox authentication](#).
5. In the drop-down list to the far right of the **Type** box, select either **User** or **Group**.
6. If your user or group appears in the list below, select the user or group and click **Select**. The **Add Address** dialog box reappears with the user or group in the **Selected Members or Addresses** box. Click **OK** to close the **Edit Policy Properties** dialog box.
If your user or group does not appear in the list in the **Add Authorized Users or Groups** dialog box, see [Define a new user for Firebox authentication](#), [Define a new group for Firebox authentication](#), or the "Define users and groups for third-party authentication" procedure above.

After you add a user or group to a policy configuration, WatchGuard System Manager automatically adds a WatchGuard Authentication policy to your Firebox configuration. Use this policy to control access to the authentication web page. For information on modifying this policy, see [Use authentication to restrict incoming traffic](#).

13 Firewall Threat Protection

About default threat protection

WatchGuard Fireware and the policies you create in Policy Manager give you strict control over access to your network. A strict access policy helps keep hackers out of your network. But, there are other types of attacks that a strict policy cannot defeat. Careful configuration of the Firebox default threat protection options can stop attacks such as SYN flood attacks, spoofing attacks, and port or address space probes.

With default threat protection, a firewall examines the source and destination of each packet it receives. It looks at the IP address and port number and monitors the packets to look for patterns that show your network is at risk. If a risk exists, you can configure the Firebox to automatically block against the possible attack. This proactive method of intrusion detection keeps attackers out of your network.

To configure default threat protection, see:

- [About default packet handling options](#)
- [About blocked sites](#)
- [About blocked ports](#)

You can also purchase an upgrade for your Firebox to use signature-based intrusion prevention. For more information, see [About Gateway AntiVirus and Intrusion Prevention](#).

About default packet handling options

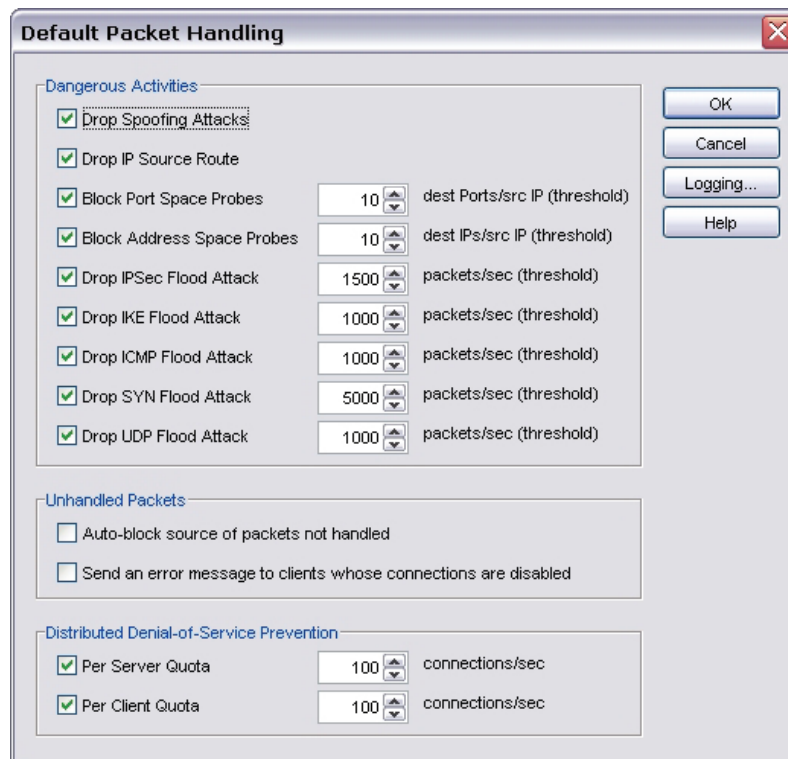
The firewall examines the source and destination of each packet it receives. It looks at the IP address and the port number. The firewall also monitors the packets to look for patterns that can show that your network is at risk.

Default packet handling:

- Rejects a packet that can be a security risk, including packets that could be part of a spoofing attack or SYN flood attack
- Can automatically block all traffic to and from a source IP address
- Adds an event to the log file
- Sends an SNMP trap to the SNMP management server
- Sends a notification of possible security risks

Most default packet handling options are enabled in the default Firebox configuration. You can change the thresholds at which the Firebox takes action. You can also disable some or all default packet handling options.

1. From Policy Manager, click .
Or, select **Setup > Default Threat Protection > Default Packet Handling**.
The Default Packet Handling dialog box appears.



Default Packet Handling

Dangerous Activities

- ☒ Drop Spoofing Attacks
- ☒ Drop IP Source Route
- ☒ Block Port Space Probes 10 dest Ports/src IP (threshold)
- ☒ Block Address Space Probes 10 dest IPs/src IP (threshold)
- ☒ Drop IPSec Flood Attack 1500 packets/sec (threshold)
- ☒ Drop IKE Flood Attack 1000 packets/sec (threshold)
- ☒ Drop ICMP Flood Attack 1000 packets/sec (threshold)
- ☒ Drop SYN Flood Attack 5000 packets/sec (threshold)
- ☒ Drop UDP Flood Attack 1000 packets/sec (threshold)

Unhandled Packets

- ☐ Auto-block source of packets not handled
- ☐ Send an error message to clients whose connections are disabled

Distributed Denial-of-Service Prevention

- ☒ Per Server Quota 100 connections/sec
- ☒ Per Client Quota 100 connections/sec

OK Cancel Logging... Help

2. Select the check boxes for the traffic patterns you want to take action against, as explained in these topics:
 - [About spoofing attacks](#)
 - [About IP source route attacks](#)
 - [About port space and address space probes](#)
 - [About flood attacks](#)
 - [About unhandled packets](#)
 - [About distributed denial-of-service attacks](#)

Set logging and notification options

The default Firebox configuration tells the Firebox to send a log message when one of these events as specified in the **Default Packet Handling** dialog box occurs. To configure an [SNMP trap](#) or [notification](#), click **Logging**. For more information about the parameters on this dialog box, see [Set logging and notification preferences](#).

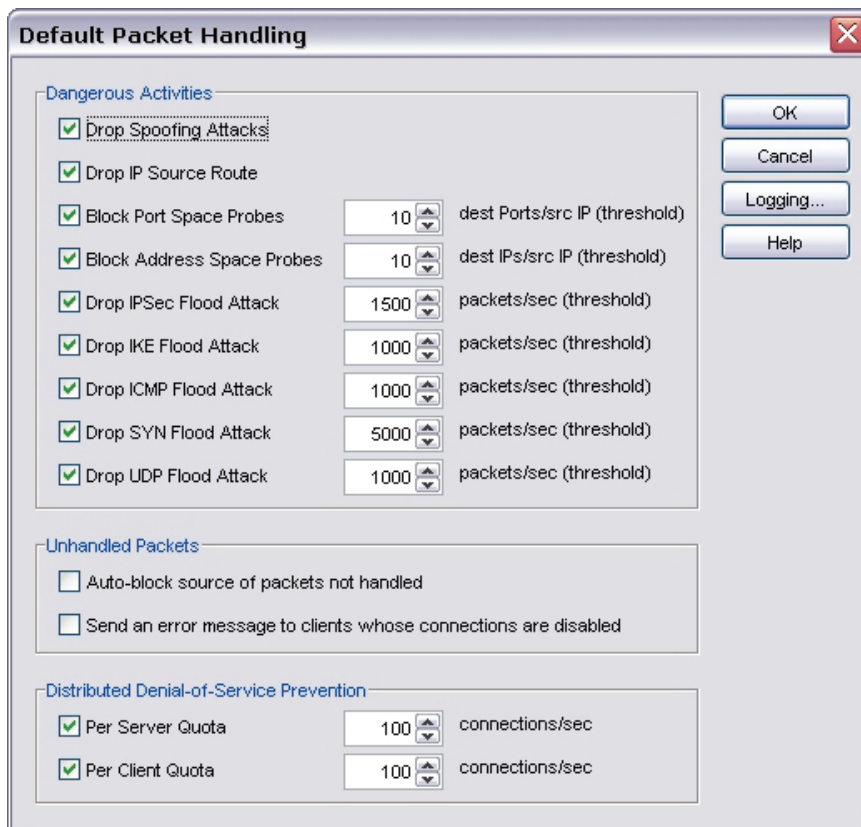
About spoofing attacks

One procedure that attackers use to get access to your network is to make an electronic false identity. With this IP spoofing procedure, the attacker sends a TCP/IP packet that uses a different IP address than the host that first sent it.

With anti-spoofing enabled, the Firebox checks to make sure that the source IP address of a packet is from a network on that interface.

The default configuration of the Firebox is to drop spoofing attacks. To disable or reenable this feature:

1. From Policy Manager, click .
Or, select **Setup > Default Threat Protection > Default Packet Handling**.
The Default Packet Handling dialog box appears.



Dangerous Activities		
<input checked="" type="checkbox"/> Drop Spoofing Attacks		
<input checked="" type="checkbox"/> Drop IP Source Route		
<input checked="" type="checkbox"/> Block Port Space Probes	10	dest Ports/src IP (threshold)
<input checked="" type="checkbox"/> Block Address Space Probes	10	dest IPs/src IP (threshold)
<input checked="" type="checkbox"/> Drop IPSec Flood Attack	1500	packets/sec (threshold)
<input checked="" type="checkbox"/> Drop IKE Flood Attack	1000	packets/sec (threshold)
<input checked="" type="checkbox"/> Drop ICMP Flood Attack	1000	packets/sec (threshold)
<input checked="" type="checkbox"/> Drop SYN Flood Attack	5000	packets/sec (threshold)
<input checked="" type="checkbox"/> Drop UDP Flood Attack	1000	packets/sec (threshold)

Unhandled Packets	
<input type="checkbox"/> Auto-block source of packets not handled	
<input type="checkbox"/> Send an error message to clients whose connections are disabled	

Distributed Denial-of-Service Prevention		
<input checked="" type="checkbox"/> Per Server Quota	100	connections/sec
<input checked="" type="checkbox"/> Per Client Quota	100	connections/sec

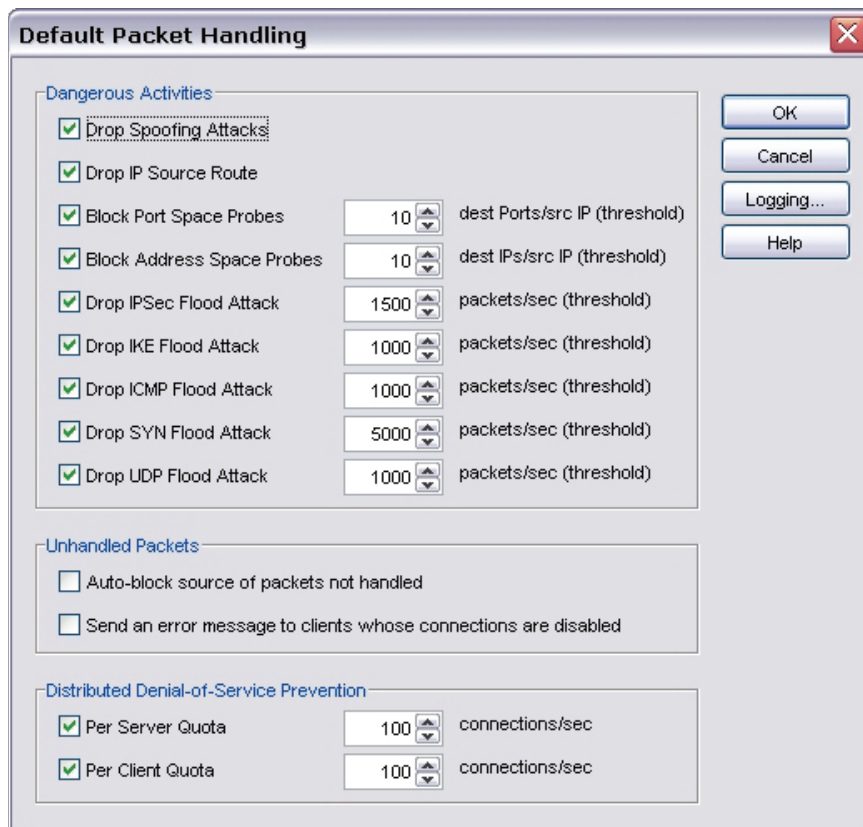
2. Select or clear the **Drop Spoofing Attacks** check box.

About IP source route attacks

Attackers use IP source route attacks to send an IP packet to find the route that the packet uses to go through the network. The attacker can then see the response to the packets and get information about the operating system of the target computer or network device.

The default configuration of the Firebox is to drop IP source route attacks. To disable or reenable this feature:

1. From Policy Manager, click .
Or, select **Setup > Default Threat Protection > Default Packet Handling**.
The Default Packet Handling dialog box appears.



2. Select or clear the **Drop IP Source Route** check box.

About port space and address space probes

Attackers frequently look for open ports as starting points to launch network attacks. A *port space probe* is TCP or UDP traffic that is sent by a host to a range of ports. These ports can be in sequence or random, from 0 to 65535. An *address space probe* is TCP or UDP traffic that is sent by a host to a range of network addresses. Port space probes examine a host to find the services that it uses. Address space probes examine a network to see which hosts are on that network.

For more information about ports, see [About ports](#).



The Firebox detects port and address space probes only on interfaces configured as type External.

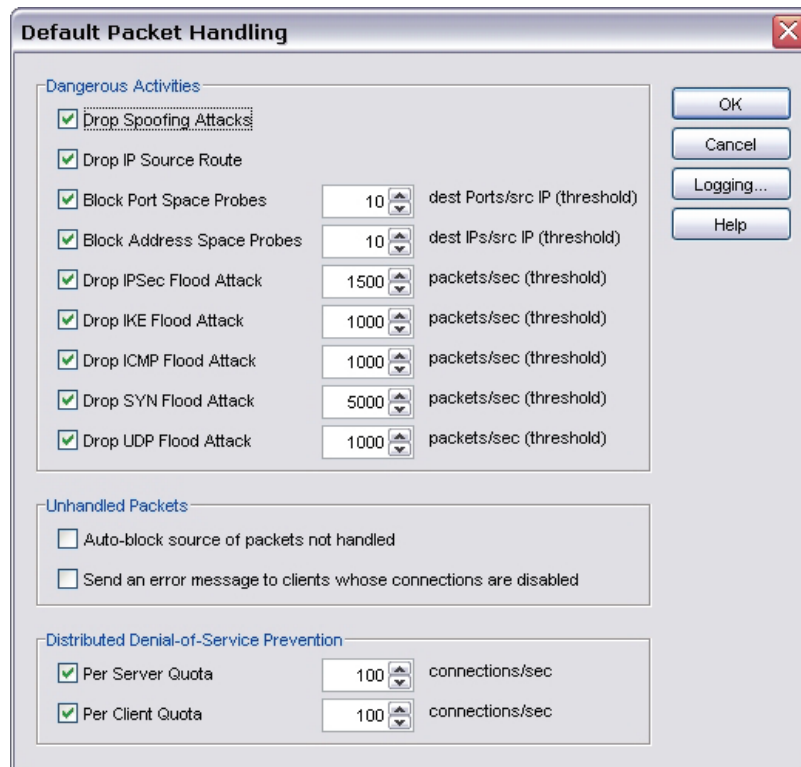
To protect against port space and address space probes

The default configuration of the Firebox is to block network probes. To disable or reenable this feature, or to change the maximum allowed number of address or port probes per second for each source IP address (the default value is 10):

1. From Policy Manager, click .

Or, select **Setup > Default Threat Protection > Default Packet Handling**.

The *Default Packet Handling* dialog box appears.



2. Select or clear the **Block Port Space Probes** and the **Block Address Space Probes** check boxes.

You then use the arrows to select the maximum allowed number of address or port probes per second for each source IP address. The default for each is 10 per second. This means that a source is blocked if it initiates connections to 10 different ports or hosts within one second.

To block attackers more quickly, you can set this threshold to a lower value. However, the Firebox could deny legitimate network traffic if the number is set too low. You are less likely to block legitimate network traffic if you use a higher number, but the Firebox must send TCP reset packets for each connection it drops. This uses bandwidth and resources on the Firebox and provides the attacker with information about your firewall.

How the Firebox identifies network probes

When the **Block Port Space Probes** and **Block Address Space Probes** check boxes are selected, all incoming traffic on any external interface is examined by the Firebox. You cannot disable these features for specified IP addresses or during different times.

An address space probe is identified when a computer on the external network sends a specified number of packets to different IP addresses assigned to the external interfaces of the Firebox. To identify a port space probe, your Firebox counts the number of packets sent from one IP address to external interface IP addresses. The addresses can include the external interface IP address and any secondary IP addresses configured on the external interface. If the number of packets sent to different IP addresses or destination ports in one second is larger than the number you select, the source IP address is added to the Blocked Sites list.

About flood attacks

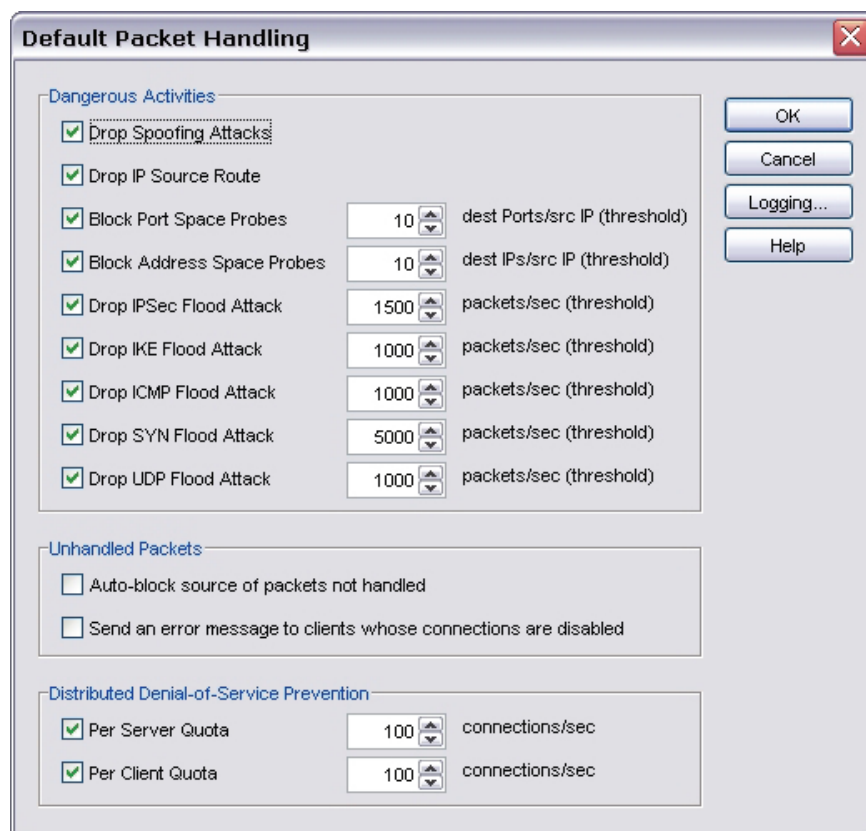
In a flood attack, attackers send a very high volume of traffic to a system so it cannot examine and allow permitted network traffic. For example, an ICMP flood attack occurs when a system receives sufficient ICMP ping commands that it uses all of its resources to send reply commands. The Firebox can protect against these types of flood attacks:

- IPSec flood attacks
- IKE flood attacks
- ICMP flood attacks
- SYN flood attacks
- UDP flood attacks

Flood attacks are also known as Denial of Service (DoS) attacks.

The default configuration of the Firebox is to block flood attacks. To disable or reenable this feature, or to change the maximum allowed number of packets each second:

1. From Policy Manager, click .
Or, select **Setup > Default Threat Protection > Default Packet Handling**.
The Default Packet Handling dialog box appears.



The image shows the 'Default Packet Handling' dialog box. It has a title bar with a close button (X). The dialog is divided into three sections: 'Dangerous Activities', 'Unhandled Packets', and 'Distributed Denial-of-Service Prevention'. On the right side, there are four buttons: 'OK', 'Cancel', 'Logging...', and 'Help'.

Dangerous Activities		
<input checked="" type="checkbox"/> Drop Spoofing Attacks		
<input checked="" type="checkbox"/> Drop IP Source Route		
<input checked="" type="checkbox"/> Block Port Space Probes	10	dest Ports/src IP (threshold)
<input checked="" type="checkbox"/> Block Address Space Probes	10	dest IPs/src IP (threshold)
<input checked="" type="checkbox"/> Drop IPSec Flood Attack	1500	packets/sec (threshold)
<input checked="" type="checkbox"/> Drop IKE Flood Attack	1000	packets/sec (threshold)
<input checked="" type="checkbox"/> Drop ICMP Flood Attack	1000	packets/sec (threshold)
<input checked="" type="checkbox"/> Drop SYN Flood Attack	5000	packets/sec (threshold)
<input checked="" type="checkbox"/> Drop UDP Flood Attack	1000	packets/sec (threshold)

Unhandled Packets	
<input type="checkbox"/> Auto-block source of packets not handled	
<input type="checkbox"/> Send an error message to clients whose connections are disabled	

Distributed Denial-of-Service Prevention		
<input checked="" type="checkbox"/> Per Server Quota	100	connections/sec
<input checked="" type="checkbox"/> Per Client Quota	100	connections/sec

2. Select or clear the check boxes for the flood attacks you want to prevent.

You then use the arrows to select the maximum allowed number of packets per second for each source IP address. If the setting is, for example, 1000, this means that the Firebox blocks a source if it receives more than 1000 packets per second from that source.

About the SYN flood attack setting

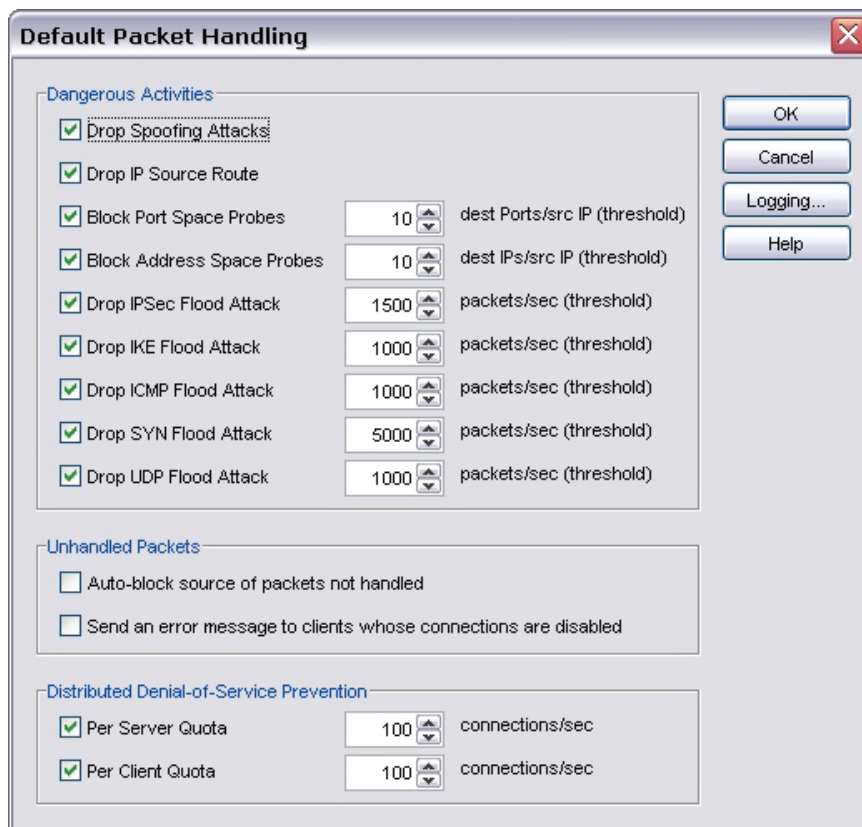
For SYN flood attacks, you set the threshold for the Firebox to report that a SYN flood attack may be taking place. But, no packets are dropped if only that number of packets is received. At twice the threshold, all SYN packets are dropped. At any level between the threshold you define and twice that level, if a packet's src_IP, dst_IP, and total_length are the same as the previous packet received, then it will always be dropped; otherwise 25 percent of the new packets received are dropped.

For example, suppose you define the threshold at 18 packets per second. When you receive that amount, the Firebox warns you that a SYN flood attack may be taking place but it drops no packets. If you receive 20 packets per second, the FB drops 25% of the packets (5 packets). If you receive 36 or more, the last 18 or more packets are dropped.

About unhandled packets

An unhandled packet is a packet that does not match any rule created in Policy Manager. The Firebox always denies unhandled packets, but you can take further actions to protect your network:

1. From Policy Manager, click .
Or, select **Setup > Default Threat Protection > Default Packet Handling**.
The Default Packet Handling dialog box appears.



2. Select or clear the check boxes for these options:
Auto-block source of packets not handled: Select to automatically block the source of unhandled packets. The Firebox adds the IP address that sent the packet to the temporary Blocked Sites list.
Send an error message to clients whose connections are disabled: Select to send a TCP reset or ICMP error back to the client when an unhandled packet is received by the Firebox.

See statistics on unhandled packets

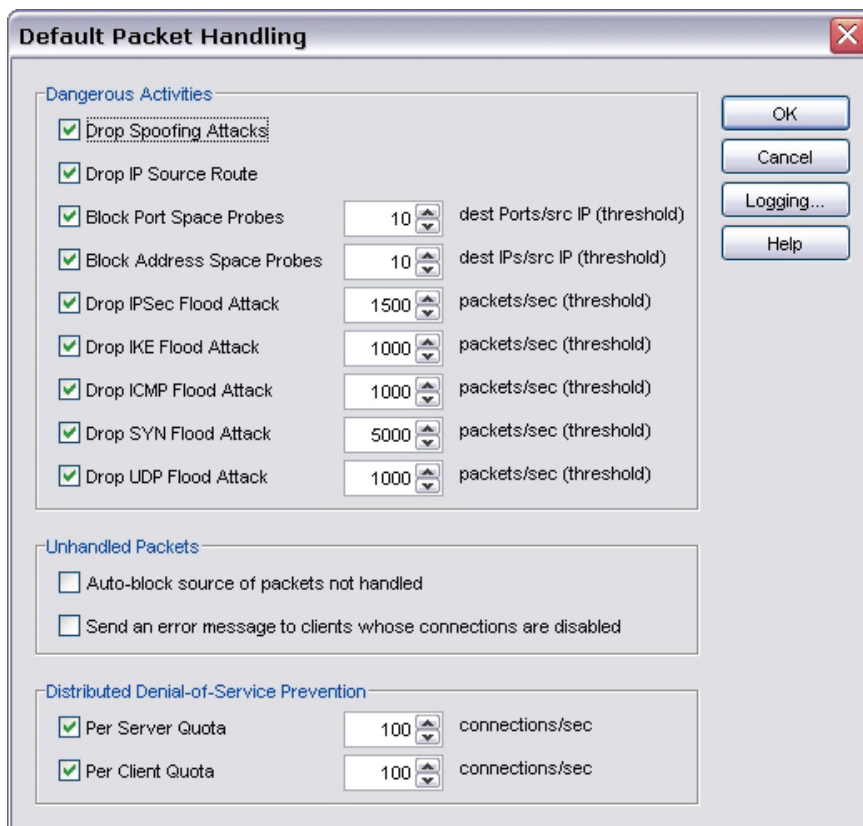
You can see statistics on unhandled packets through the Firebox on the [Service Watch tab](#) in Firebox System Manager. Use the **Show connections by** drop-down list to show connections by rule instead of policy.

About distributed denial-of-service attacks

Distributed Denial of Service (DDoS) attacks are very similar to flood attacks. In a DDoS, many different clients and servers send connections to one computer system to try to flood the system and to prevent legitimate users from using the targeted system.

The default configuration of the Firebox is to block Distributed Denial of Service (DDoS) attacks. To disable or reenable this feature, or to change the maximum allowed number of connections each second:

1. From Policy Manager, click .
Or, select **Setup > Default Threat Protection > Default Packet Handling**.
The Default Packet Handling dialog box appears.



Default Packet Handling

Dangerous Activities

<input checked="" type="checkbox"/> Drop Spoofing Attacks		
<input checked="" type="checkbox"/> Drop IP Source Route		
<input checked="" type="checkbox"/> Block Port Space Probes	10	dest Ports/src IP (threshold)
<input checked="" type="checkbox"/> Block Address Space Probes	10	dest IPs/src IP (threshold)
<input checked="" type="checkbox"/> Drop IPSec Flood Attack	1500	packets/sec (threshold)
<input checked="" type="checkbox"/> Drop IKE Flood Attack	1000	packets/sec (threshold)
<input checked="" type="checkbox"/> Drop ICMP Flood Attack	1000	packets/sec (threshold)
<input checked="" type="checkbox"/> Drop SYN Flood Attack	5000	packets/sec (threshold)
<input checked="" type="checkbox"/> Drop UDP Flood Attack	1000	packets/sec (threshold)

Unhandled Packets

☐ Auto-block source of packets not handled

☐ Send an error message to clients whose connections are disabled

Distributed Denial-of-Service Prevention

<input checked="" type="checkbox"/> Per Server Quota	100	connections/sec
<input checked="" type="checkbox"/> Per Client Quota	100	connections/sec

Buttons: OK, Cancel, Logging..., Help

2. Select or clear the check boxes for the attacks you want to prevent. Use the arrow keys to set the maximum allowed number of connections per second from a source IP address protected by the Firebox (**Per Client Quota**) or to a destination IP address protected by the Firebox (**Per Server Quota**). Connections that exceed this quota are dropped.

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

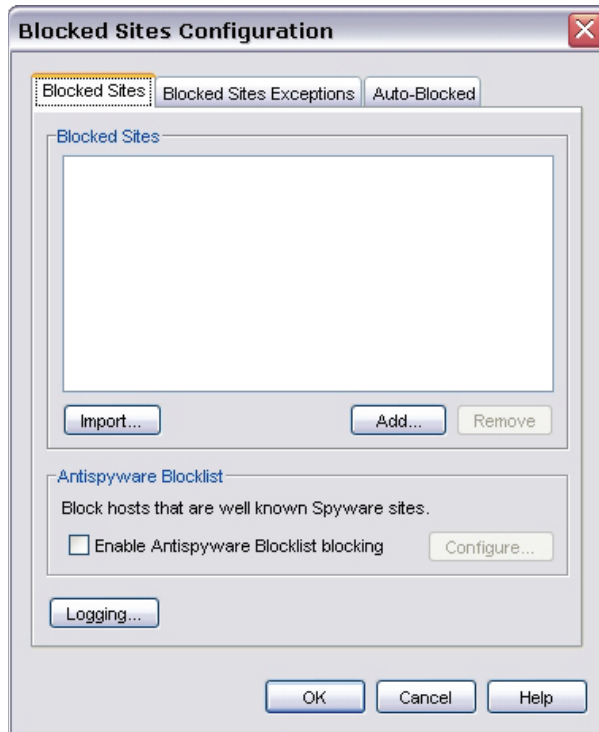
Packets from auto-blocked sites are denied for the amount of time you specify. The Firebox uses the packet handling rules that are specified for each policy to determine if a site should be blocked. For example, if you create a policy that denies all traffic on port 23 (Telnet), any IP address that attempts to send Telnet traffic using that port is automatically blocked for the amount of time you specify.

To automatically block sites that send denied traffic, see [Block sites temporarily with policy settings](#).

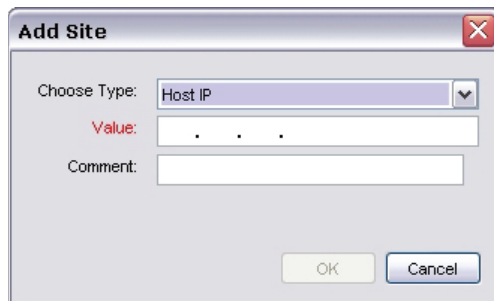
You can also automatically block sites that are the source of packets that do not match any rule created in Policy Manager. For more information, see [About unhandled packets](#).

Block a site permanently or block spyware sites

1. From Policy Manager, click .
Or, select **Setup > Default Threat Protection > Blocked Sites**.
The Blocked Sites Configuration dialog box appears.



2. Click **Add**.
The Add Site dialog box appears.



3. Use the **Choose Type** drop-down list to select the method you use to identify the blocked site. The selections are **Host IP**, **Network IP**, **Host Range**, or **Host Name (DNS lookup)**.
4. Type the value.
The value shows whether this is an IP address or a range of IP addresses. When you type an IP address, type all the numbers and the period. Do not use the tab or the arrow key. You cannot add internal IP or network addresses to the Blocked Sites list. If you must block an address range that includes one or more internal IP addresses, you must first add the internal IP addresses to the Blocked Sites Exceptions list. (To add exceptions, see [Create exceptions to the Blocked Sites list](#).)
5. (Optional) Type a comment to provide information on the site or why you want to block it.
6. Select **OK**.
The new site appears in the Blocked Sites list.

Configure logging for blocked sites

You can configure the Firebox to make a log entry when a host tries to use a blocked site. You can also set up notification for when a host tries to get access to a blocked site. To do this, click **Logging**. For more information about the parameters on this dialog box, see [Set logging and notification preferences](#).

Block spyware sites

You can block hosts that are known spyware sites by configuring categories of spyware to block. You must [activate Intrusion Prevention Service \(IPS\)](#) to use this feature.

1. From the **Blocked Sites Configuration** dialog box, select the **Enable Antispyware Blocklist blocking** check box. Click **Configure**.
2. Select or clear the following check boxes to enable or disable antispyware blocking for these categories. To enable or disable all categories, select or clear the **All Spyware Categories** check box:

Adware

A software application in which advertising banners are shown while the program is in operation. It sometimes includes code that records a user's personal information and sends it to third parties, without the user's authorization or knowledge.

Dialer

A software application that can hijack a user's modem and dial toll numbers that get access to inappropriate web sites.

Downloader

A program that gets and installs other files. Most are configured to get files from a designated web or FTP site.

Hijacker

A type of malware program that changes your computer's browser settings and redirects you to web sites that you did not plan to browse to.

Trackware

Any software that uses a computer's Internet connection to send personal information without the user's permission.

Use an external list of blocked sites

If you manage several Fireboxes and want to block the same sites for each of them, you can list the sites to block in an external file and import the file into each Firebox. This file must be a text (.txt) file. The IP addresses in the text file must be separated by spaces or line breaks. Use slash notation to specify networks. To indicate a range of addresses, separate the start and end addresses with a hyphen. An example text import file might look like this:

```
2.2.2.2 5.5.5.0/24
3.3.3.3-3.3.3.8
6.6.6.6 7.7.7.7
```

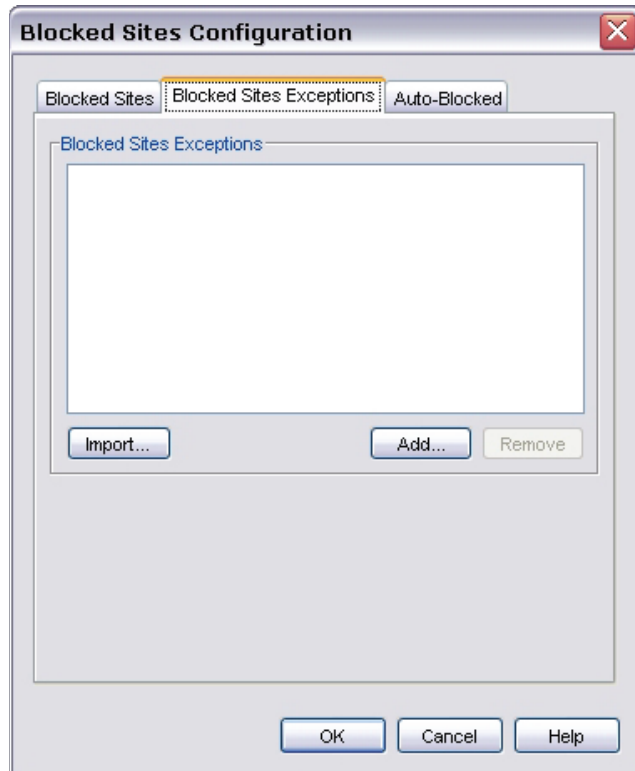
To import the file into the current Firebox:

1. In the **Blocked Sites Configuration** dialog box, click **Import**.
2. Find the file. Double-click it, or select it and click **Open**.
The sites in the file appear in the Blocked Sites list.

Create exceptions to the Blocked Sites list

A host defined as a blocked sites exception does not appear in the Blocked Sites list. The automatic rules do not apply for this host.

1. From Policy Manager, select **Setup > Default Threat Protection > Blocked Sites**. Click the **Blocked Sites Exceptions** tab.



2. Click **Add**.
3. Use the **Choose Type** drop-down list to select a member type. The selections are **Host IP**, **Network IP**, **Host Range**, or **Host Name (DNS lookup)**.
4. Type the member value.
The member type shows whether this is an IP address or a range of IP addresses. When you type an IP address, type all the numbers and the period. Do not use the TAB or the arrow key.
5. Click **OK**.

Use an external list of blocked sites exceptions

If you manage several Fireboxes and want to use the same blocked sites exceptions for each of them, you can list the exceptions in an external file and import the file into each Firebox. The procedure is the same as the one for blocked sites, as described in [Use an external list of blocked sites](#).

Block sites temporarily with policy settings

You can use the policy configuration to block sites that try to use a denied service:

1. From Policy Manager, double-click the policy icon.
The Edit Policy Properties dialog box appears.
2. On the **Policy** tab, make sure you set the **Connections Are** drop-down list to **Denied** or **Denied (send reset)**.
3. On the **Properties** tab, select the check box **Automatically block sites that attempt to connect**. IP addresses from the denied packets are added to the Temporary Blocked Sites list for 20 minutes (by default). You can change this time interval on the **Auto-Blocked** tab in the **Blocked Sites Configuration** dialog box.
4. You can use the Temporary Blocked Sites list with log messages to help you make decisions about which IP addresses to block permanently. In the policy definition, click the **Properties** tab, click the **Logging** button and [Set logging and notification preferences](#).

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 of the policy definitions you create in Policy Manager. 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.



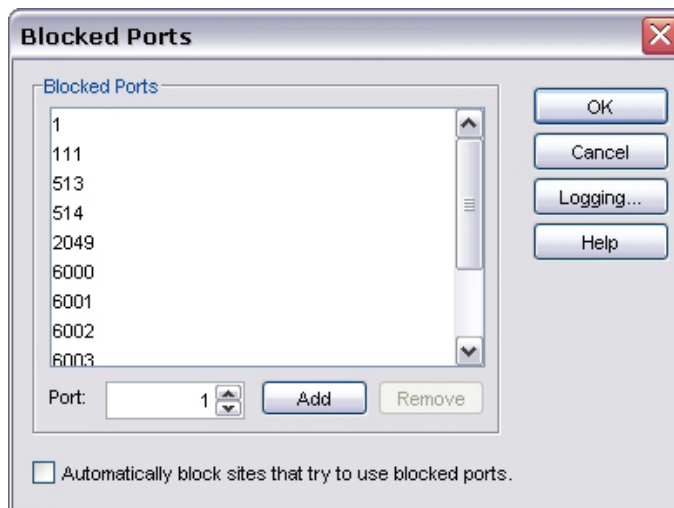
If you must allow traffic through for the types of software applications that use recommended blocked ports, we recommend that you allow the traffic only through an IPSec VPN tunnel or use ssh to get access to the port.

Block a port



Be very careful if you block port numbers higher than 1023. Clients frequently use these source port numbers.

1. From Policy Manager, click .
Or, select **Setup > Default Threat Protection > Blocked Ports**.
The Blocked Ports dialog box appears.
2. Type the port number. Click **Add**.
The new port number appears in the Blocked Ports list.



Block IP addresses that try to use blocked ports

You can configure the Firebox to automatically block an external host that tries to get access to a blocked port. In the **Blocked Ports** dialog box, select the **Automatically block sites that try to use blocked ports** check box.

Set logging and notification for blocked ports

You can configure the Firebox to make a log entry when a host tries to use a blocked port. You can also set up notification for when a host tries to get access to a blocked port. To do this, click **Logging**. For more information about the parameters on this dialog box, see [Set logging and notification preferences](#).

14 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 the Firebox with the Quick Setup Wizard, the wizard adds only four basic policies (TCP/UDP outgoing, FTP packet filter (not the FTP proxy), ping, and WatchGuard). If you have more software applications and network traffic for the Firebox to examine, you must:

- Configure the policies on the Firebox 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.

About Policy Manager

Policy Manager for Fireware or Fireware Pro is a WatchGuard software tool that lets you make, change, and save configuration files. When you use the Policy Manager user interface on your computer screen, you see a version of your configuration file that is easy to examine and change.

To open Policy Manager, see [Open Policy Manager](#).

Policy Manager window

Policy Manager has two tabs. The **Firewall** tab shows policies that are used for general firewall traffic on the Firebox. The **Firewall** tab also shows BOVPN policies so you can see the order in which the Firebox examines network traffic and applies a policy rule. (To change the order, see [About policy precedence](#).) The **Mobile VPN with IPSec** tab shows policies that are used with Mobile VPN with IPSec tunnels.

The Policy Manager user interface can show either icons that represent each policy in your configuration (Large Icons view, which is the default view), or a list of the policies (Details view). To switch between these two views, see [Change the Policy Manager view](#).

Policy icons

The Policy Manager window contains icons for the policies that are defined on the Firebox. You can double-click them if you want to edit the properties for that policy. The appearance of the icons shows their status and type:

- Enabled policies that allow traffic appear with a green bar on top with a check mark.
- Enabled policies that deny traffic have a red bar on top with an X.
- Disabled policies have a black bar.
- An icon that contains a shield symbol on the left side is a proxy policy. The others are packet filter policies.

The names of policies appear in color based on policy type:


- Managed policies appear in gray with a white background.
- BOVPN policies (such as BOVPN-allow.out) appear in green with a white background.
- Mixed BOVPN and firewall policies (such as Ping or Any-PPTP) appear in blue with a white background.
- All other policies appear in black with a white background.

To change these default colors, see [Change colors used for Policy Manager text](#).

To find a specific policy in Policy Manager, see [Find a policy by address, port, or protocol](#).

Open Policy Manager

To open Policy Manager, from the WatchGuard System Manager window:

- Select the Firebox whose Policy Manager you want to open and click .
- or
- Select **Tools > Policy Manager**.

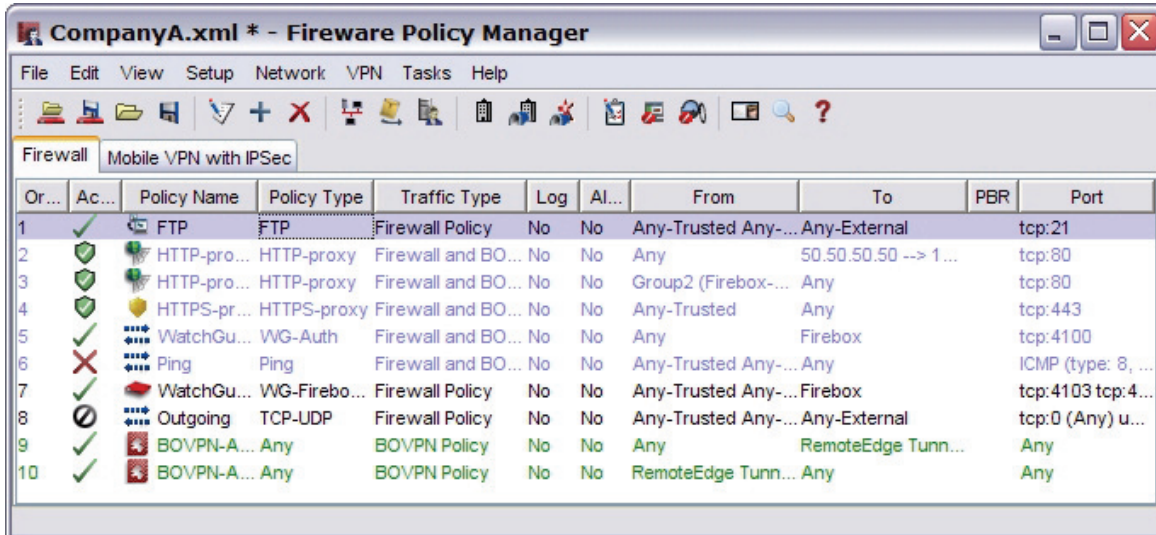
If the Firebox you select is a managed device, Policy Manager puts a lock on the device in WatchGuard System Manager to prevent simultaneous changes made to its definition in WatchGuard System Manager. The lock is released when you close Policy Manager or if you open Policy Manager for a different device.

Change the Policy Manager view



Large Icons View

Policy Manager has two views: Large Icons and Details. The default Large Icons view shows each policy as an icon. To change to the Details view, select **Details** from the **View** menu. In the Details view, each policy is a row of information divided among several columns. You can see configuration information, including source and destination, and logging and notification parameters.



The screenshot shows the 'CompanyA.xml * - Fireware Policy Manager' window. The 'Firewall' tab is selected, and the 'Mobile VPN with IPSec' sub-tab is active. The table below represents the data shown in the screenshot.

Or...	Ac...	Policy Name	Policy Type	Traffic Type	Log	Al...	From	To	PBR	Port
1	✓	FTP	FTP	Firewall Policy	No	No	Any-Trusted Any-...	Any-External		tcp:21
2	✓	HTTP-pro...	HTTP-proxy	Firewall and BO...	No	No	Any	50.50.50.50 --> 1...		tcp:80
3	✓	HTTP-pro...	HTTP-proxy	Firewall and BO...	No	No	Group2 (Firebox-...	Any		tcp:80
4	✓	HTTPS-pr...	HTTPS-proxy	Firewall and BO...	No	No	Any-Trusted	Any		tcp:443
5	✓	WatchGu...	WG-Auth	Firewall and BO...	No	No	Any	Firebox		tcp:4100
6	✗	Ping	Ping	Firewall and BO...	No	No	Any-Trusted Any-...	Any		ICMP (type: 8, ...
7	✓	WatchGu...	WG-Firebo...	Firewall Policy	No	No	Any-Trusted Any-...	Firebox		tcp:4103 tcp:4...
8	○	Outgoing	TCP-UDP	Firewall Policy	No	No	Any-Trusted Any-...	Any-External		tcp:0 (Any) u...
9	✓	BOVPN-A...	Any	BOVPN Policy	No	No	Any	RemoteEdge Tunn...		Any
10	✓	BOVPN-A...	Any	BOVPN Policy	No	No	RemoteEdge Tunn...	Any		Any

Details View

The following information appears for each policy:

Order

Order in which the policies are sorted, and traffic flows through the policies. Policy Manager automatically sorts policies from the most specific to the most general. If you want to switch to manual-order mode, select **View > Auto-order mode** so that the check mark disappears. Then, select the policy whose order you want to change and drag it to its new location. (For more information on policy precedence, see [About policy precedence](#).)

Action

The action taken by the policy for traffic that matches the specification. The symbol in this field also indicates whether the policy is a packet filter policy or a proxy policy.

Green check mark = policy is a packet filter policy and traffic is allowed.

Red X = policy is a packet filter policy and traffic is denied.

Circle with line = policy is a packet filter policy and the action for traffic is not configured.

Green shield with check mark = policy is a proxy policy and traffic is allowed.

Red shield with X = policy is a proxy policy and traffic is denied.

Gray shield = policy is a proxy policy and the action for traffic is not configured.

Policy Name

Name of the policy, as defined in the **Name** field in the **New/Edit Policy Properties** dialog box. (For more information, see [Add a policy from the list of templates](#).)

Policy Type

Packet filter policies are listed according to policy name. Proxy policies are listed according to proxy name followed by -proxy.

Traffic Type

Type of traffic the policy examines: firewall or VPN.

Log

Whether logging is enabled for the policy.

Alarm

Whether alarms are configured for the policy.

From

Addresses from which traffic for this policy applies (source addresses).

To

Addresses to which traffic for this policy applies (destination addresses).

PBR

Indicates whether the policy uses policy-based routing. If it does, and failover is not enabled, the interface number appears. If policy-based routing and failover are enabled, a list of interface numbers appear, with the primary interface listed first. For information on policy-based routing, see [Configure policy-based routing](#).

Port

Protocols and ports used by the policy.

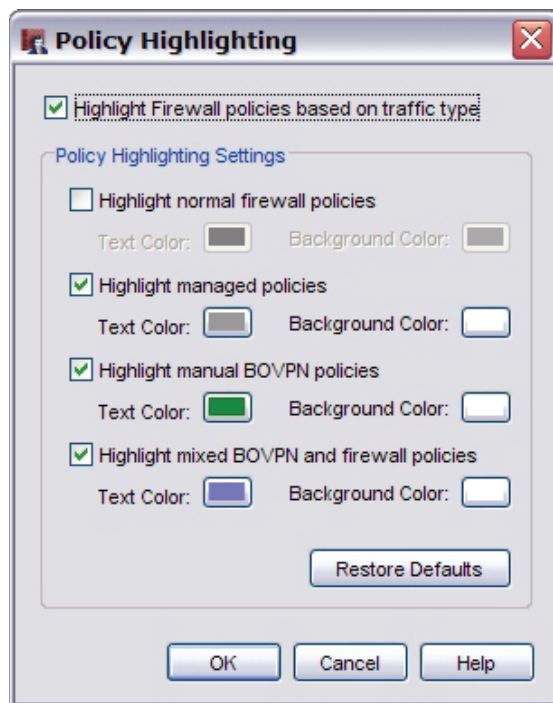
Change colors used for Policy Manager text

The default setup for Policy Manager is for the names of policies (or the entire row in Details view) to appear highlighted in color based on traffic type:

- Managed policies appear in gray with a white background.
- BOVPN policies (such as BOVPN-allow.out) appear in green with a white background.
- Mixed BOVPN and firewall policies (such as Ping or Any-PPTP) appear in blue with a white background.
- All other policies (normal policies) are not highlighted. They appear in black.

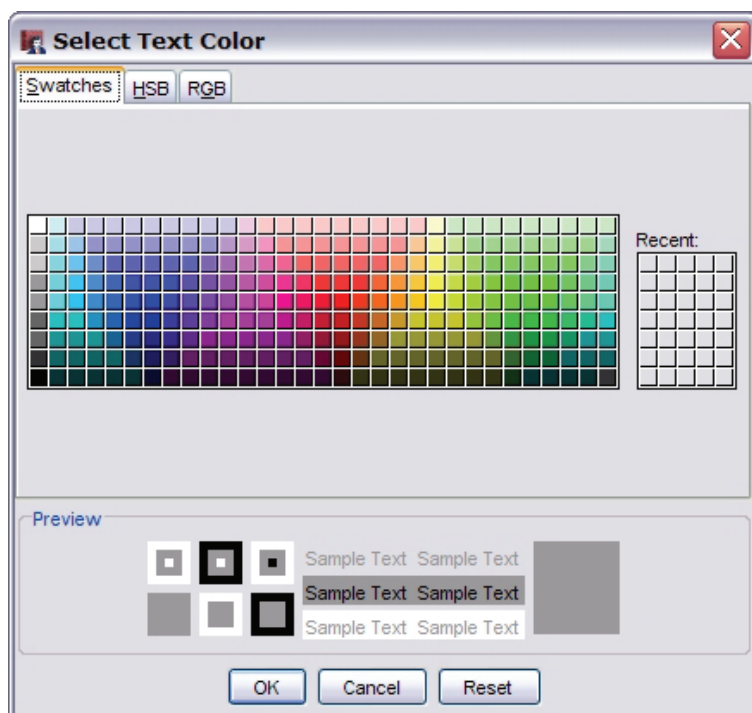
You can use default colors or colors that you select. You can also disable policy highlighting.

1. From Policy Manager, select **View > Policy Highlighting**.
The *Policy Highlighting* dialog box appears.



2. To turn policy highlighting off or on, clear or select the **Highlight Firewall policies based on traffic type** check box.

3. To select different colors for the text or background of the policy names for normal, managed, BOVPN, or mixed policies, click the block adjacent to **Text Color** or **Background Color**.
The Select Text Color or Select Background Color dialog box appears.

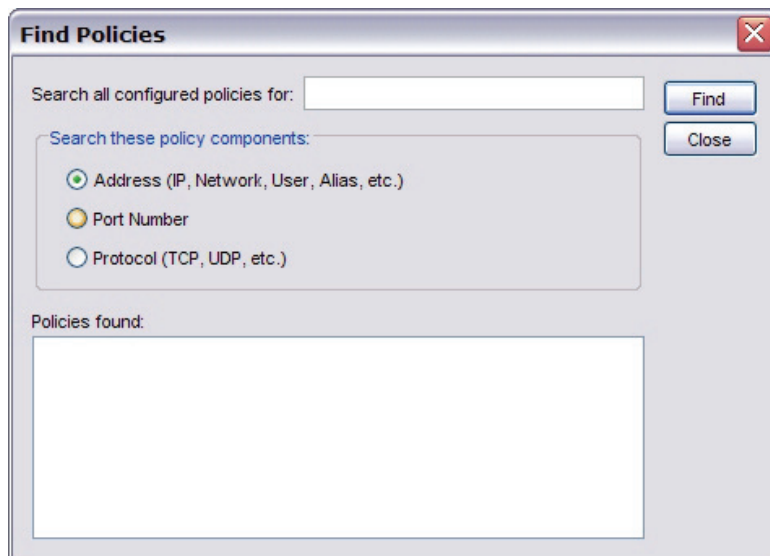


4. Use one of the three tabs, **Swatches**, **HSB**, or **RGB** to specify the color you want:
 - Swatches: Click one of the small swatches of the available colors.
 - HSB: Select the **H** (hue), **S** (saturation), or **B** (brightness) radio button and then either use the slider or type numbers into the adjacent fields.
 - RGB: Use the **Red**, **Green**, or **Blue** sliders or type numbers into the adjacent fields.
When you specify a color, a sample of what it will look like appears in the **Sample** block at the bottom of the dialog box. When you are satisfied with the color, click **OK**.
5. Click **OK** on the **Policy Highlighting** dialog box for the changes to take effect.

Find a policy by address, port, or protocol

1. From Policy Manager, select **Edit > Find**.

The Find Policies dialog box appears.



2. Select the **Address**, **Port Number**, or **Protocol** radio button to specify the policy component you are searching for.
3. Next to **Search all configured policies for**, type the string to search for. For address and protocol searches, Policy Manager performs a partial string search. You can type only a partial string, and Policy Manager will show all policies that contain the string.
4. Click **Find**.
Policy Manager displays policies that match the criteria in the Policies found box.
5. To edit a policy that is returned for a search, double-click its name.

Add policies to your configuration

To add a policy, you choose from the list of policy templates in Policy Manager. A policy template contains the policy name, a short description of the policy, and the protocol/port used by the policy.

- To see the list of templates to choose from, see [See the list of policy templates](#).
- To add one of the policies in the list to your configuration, see [Add a policy from the list of templates](#).
- To see or modify the definition of a policy template, see [See template details and modify policy templates](#).
- If you manage several Fireboxes and have custom policies for them, you can use the policy import/export function to copy policies from one Firebox to another. For more information, see [Import and export custom policy templates](#).

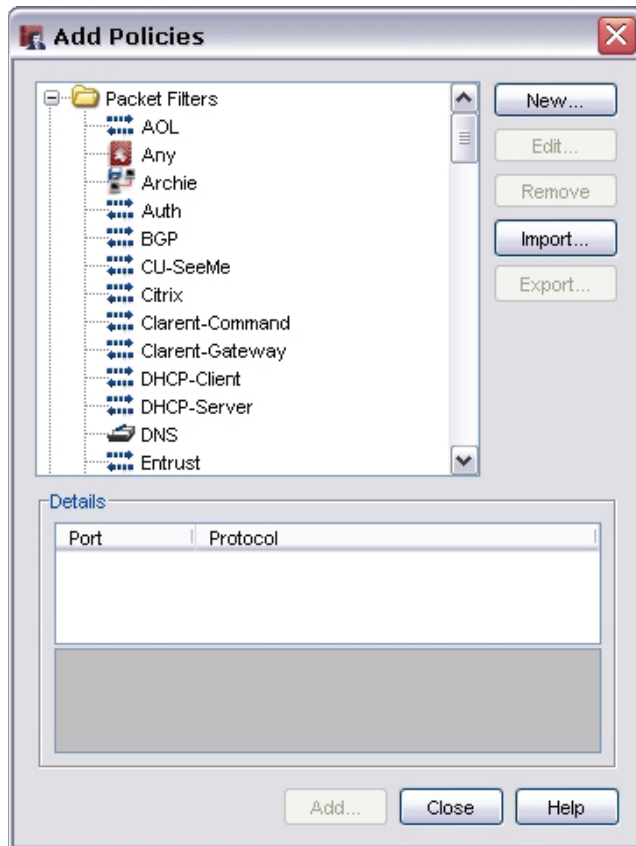
After you add a policy to your configuration, you define rules to:

- Set allowed traffic sources and destinations
- Make filter rules
- Enable or disable the policy
- Configure properties such as Traffic Management, NAT, schedules, and logging

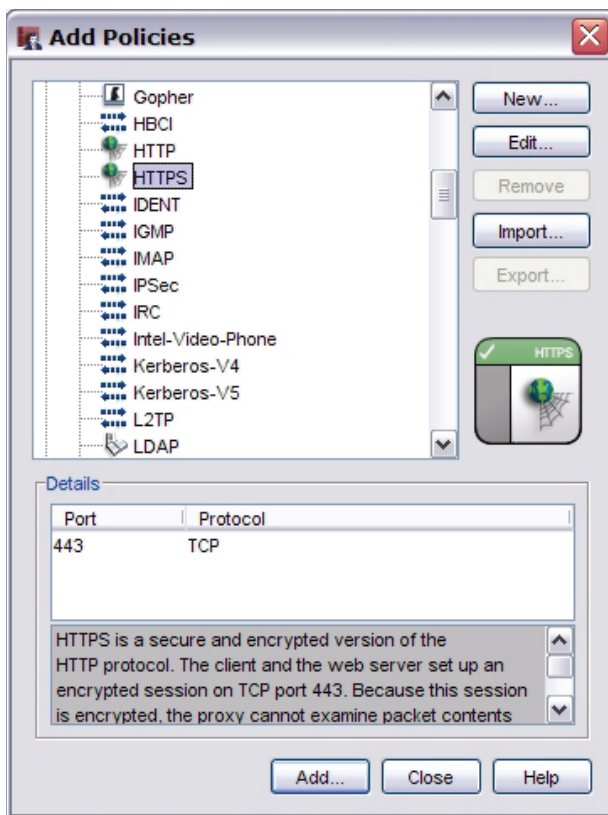
For information on the options available for defining policy properties, see [About policy properties](#).

See the list of policy templates

1. In Policy Manager, click the plus (+) sign on the Policy Manager toolbar.
You can also select Edit > Add Policies. The Add Policies dialog box appears.
2. Click the plus (+) sign on the left side of the folder to expand the **Packet Filters** or **Proxies** folders.
A list of templates for packet filters or proxies appears.



To see basic information about a policy template, select it. The policy icon appears in the area below the buttons on the right side of the dialog box. Also, the Details box shows the basic information about the policy.



Add a policy from the list of templates

1. If you have not already done so, from the **Add Policies** dialog box, expand the **Packet Filters** or **Proxies** folders.
A list of templates for packet filters or proxies appears.
2. Select the name of the policy you want to add. Click **Add**.
The New Policy Properties dialog box appears.

New Policy Properties

Name: TFTP-proxy ☒ Enable

Policy Properties Advanced

TFTP-proxy connections are...

Allowed

From

Any-Trusted

Add... Remove

To

Any-External

Add... Remove

Select the method to route outbound non-IPSec traffic:

☐ Use policy-based routing External 50

☐ Failover Configure...

OK Cancel Help

3. You can change the name of the policy here. This information appears in the Policy Manager Details view. To change the name, type a new name in the **Name** text box.
4. Set the access rules for the policy, as described in [Set access rules for a policy](#).
5. Click **OK** to close the **Properties** dialog box.
You can add more than one policy while the Policies dialog box is open.
6. Click **Close**.
The new policy appears in Policy Manager.

Add more than one policy of the same type

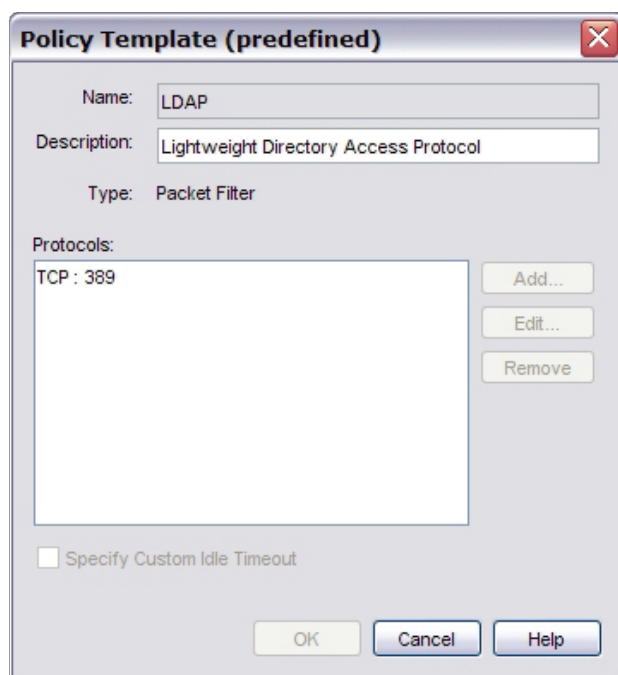
If your security policy requires it, you can add the same policy more than one time. For example, you can set a limit on web access for most users, while you give full web access to your management team. To do this, you make two different policies with different properties:

1. Add the first policy.
2. Change the name of the policy to a name that matches your security policy and add the related information.
In this example, you can name the first policy `restricted_web_access`.
3. Click **OK**. The **New Policy Properties** dialog box for the policy appears. The default policy settings are appropriate for most installations. However, you can modify them to meet your particular business needs, or if you want to include special policy properties such as Traffic Management actions and operating schedules. For more information on policy properties, see [About policy properties](#).
4. Add the second policy.
5. Click **OK**. The **New Policy Properties** dialog box for the policy appears. To change default policy properties, see [About policy properties](#).

See template details and modify policy templates

To see a policy template, select it on the **Add Policies** dialog box and click **Edit**. You normally do not need to see the actual template because relevant information from the template appears in the Details box when you select the policy template on the **Add Policies** dialog box.

With pre-defined policies (those listed under Packet Filters and Proxies in the **Add Policies** dialog box), you can edit only the **Description** field on the policy template. You also cannot delete pre-defined policies. You can, however, perform both of these operations on custom policy templates. For more information on custom policies, see [About custom policies](#).



Disable a policy

To disable a policy, you can right-click it in the Policy Manager window and select **Disable Policy**. When a policy is disabled, the menu choice changes to **Enable Policy**, which you can use to reenable the policy.

You can also clear the **Enable** check box at the top of the **Edit Policy Properties** dialog box to disable a policy. If you want to reenable the policy, select the **Enable** check box.

Delete a policy

As your security policy changes, you sometimes have to remove one or more policies. To remove a policy, you first remove it from Policy Manager. Then you save the new configuration to the Firebox.

1. From Policy Manager, click the policy.
2. In Policy Manager, click the **X** button on the Policy Manager toolbar. You can also select Edit > Delete Policy.
3. When asked to confirm, click **Yes**.
4. Save the configuration to the Firebox and start the Firebox again. Select **File > Save > To Firebox**. Type the configuration passphrase. Select the **Save to Firebox** check box. Click **Save**.

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.

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.

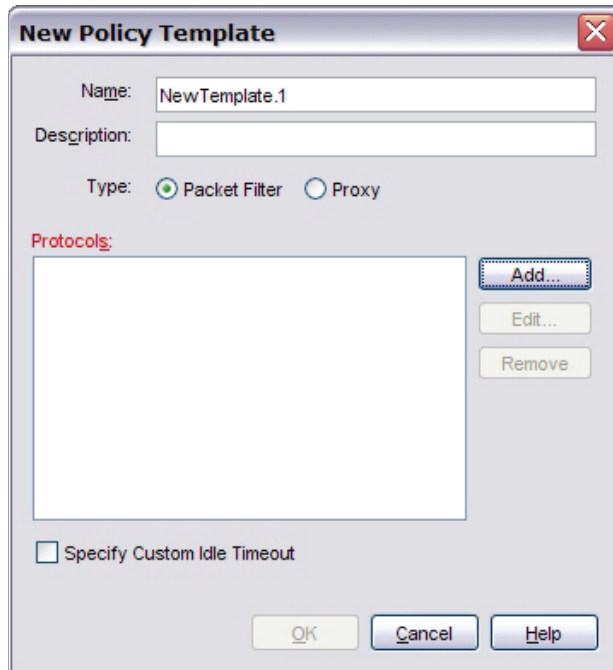
To begin to create a custom policy, see [Create a custom policy template](#). Or, start with an existing custom template. You use the same procedure to add a custom policy to Policy Manager as you would a pre-defined policy, as described in [Add a policy from the list of templates](#).

Create or edit a custom policy template

The first step when you create a new policy is to make a template for it. The template is added to the **Custom** folder in the **Add Policies** dialog box. You can then add the policy and configure it as you would a pre-defined policy.

You can also use this procedure to edit an existing policy template. In step 2, click the **Edit** button.

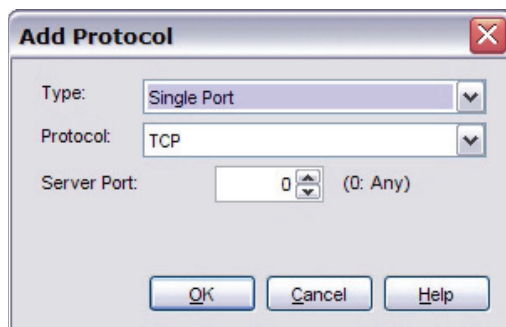
1. In Policy Manager, click the plus (+) sign on the Policy Manager toolbar.
You can also select Edit > Add Policies. The Add Policies dialog box appears.
2. Click **New**.
The New Policy Template dialog box appears.



The **New Policy Template** dialog box is shown. It has a title bar with a close button (X). The fields include:

- Name:** A text box containing "NewTemplate.1".
- Description:** An empty text box.
- Type:** Two radio buttons: "Packet Filter" (selected) and "Proxy".
- Protocols:** A large empty list box. To its right are three buttons: "Add..." (highlighted), "Edit...", and "Remove".
- Specify Custom Idle Timeout:** An unchecked checkbox.
- At the bottom are three buttons: "OK", "Cancel", and "Help".

3. In the **Name** text box, type the name of the custom policy. The name appears in Policy Manager as the policy type. A unique name helps you to find the policy when you want to change or remove it. This name must not be the same as any name in the list in the **Add Policy** dialog box.
4. In the **Description** text box, type a description of the policy.
This appears in the Details section when you click the policy name in the list of User Filters.
5. Select the type of policy: **Packet Filter** or **Proxy**.
6. To add protocols for this policy, click **Add**.
The Add Protocol dialog box appears.



The **Add Protocol** dialog box is shown. It has a title bar with a close button (X). The fields include:

- Type:** A drop-down menu showing "Single Port".
- Protocol:** A drop-down menu showing "TCP".
- Server Port:** A text box with "0" and a spin button, followed by "(0: Any)".
- At the bottom are three buttons: "OK", "Cancel", and "Help".

7. From the **Type** drop-down list, select **Single Port** or **Port Range**.

8. From the **Protocol** drop-down list, select the protocol for this new policy. For more information about network protocols, see the chapter about services and protocols in the Reference Guide. When you select **Single Port**, you can select:

- TCP
- UDP
- GRE
- AH
- ESP
- ICMP
- IGMP
- OSPF
- IP
- Any

When you select **Port Range**, you can select:

- TCP
- UDP

When you add an IGMP policy to your Fireware configuration, Fireware does not pass IGMP multicast traffic through the Firebox or between Firebox interfaces. It passes IGMP multicast traffic only between an interface and the Firebox. When you select **Port Range**, you can select **TCP** or **UDP**.

9. From the **Server Port** drop-down list, select the port for this new policy. If you selected **Port Range**, select a starting server port and an ending server port.
10. Click **OK**.
Policy Manager adds the values to the **New Policy Template** dialog box. Make sure that the name, information, and configuration of this policy are correct. If necessary, click **Add** to configure more ports for this policy. Repeat steps 6 – 10 until you configure all ports for the policy.
11. Click **OK**.
The Add Policy dialog box appears with the new policy in the Custom folder.
12. You can now use the custom policy template to add a custom policy to your configuration. Use the same procedure as you would for a predefined template (described in [Add a policy from the list of templates](#)). The only difference is that, in Step 1, the policy appears in the Custom folder instead of the Packet Filters or Proxies folders.

Import and export custom policy templates

If you manage several Fireboxes and have custom policies for them, you can use the policy import/export function to save time. You can define the templates on one Firebox, export them to an ASCII file, and then import them to another Firebox.

The Firebox where you created the policies must run the same version of WSM as the version of Policy Manager you use to import the policies. You cannot import a template from a previous version into the current version.

1. On the first Firebox, define custom policy templates for the policies you need.
2. Click **Export**.
You do not need to select the custom policies. The Export function automatically exports all custom policies regardless of which policy is actually selected.
3. In the **Save** dialog box, select where you want to save the policy templates file. Type a name for the file and click **Save**.
The default location is My Documents > My WatchGuard.
4. From Policy Manager on a different Firebox, on the **Add Policies** dialog box, click **Import**.
5. Find the file you created in step 3 and click **Open**.
6. If custom policy templates are already defined in the current Policy Manager, you are asked whether you want to replace the existing templates or append the imported templates to the existing templates. Click **Replace** or **Append**.
If you click **Replace**, the existing templates are deleted and replaced with the new templates.
If you click **Append**, both the existing and the imported templates are listed in alphabetical order under **Custom**.

About policy properties

The Firebox includes a default definition for each policy included in the Firebox configuration. The default definition consists of settings that are appropriate for most installations. However, you can modify them to meet your particular business needs, or if you want to include special policy properties such as Traffic Management actions and operating schedules.

To set properties for a policy, double-click the policy icon or name in the Policy Manager window to open the **Edit Policy Properties** dialog box. Or, if you have just added a policy to your configuration, the **New Policy Properties** box automatically appears for you to set policy properties.

See the following topics for more information about the policy properties you can set:

Policy tab

For information on the **policy_name connections are** drop-down list and the **From** and **To** fields, see [Set access rules for a policy](#).

[Configure policy-based routing](#)

[Configure static NAT](#), or [About using static NAT route for a policy](#)

[Configure server load balancing](#)

Properties tab

[About proxy actions](#) (proxy policies only)


[Set logging and notification preferences](#)

[Block sites temporarily with policy settings](#)

[Set a custom idle timeout](#)

Proxy action settings (proxy policies only)

WatchGuard proxies have predefined rulesets that provide a good balance of security and accessibility for most installations. If a default ruleset does not meet all of your business needs, you can add, delete, or modify rules.

To modify the settings and rulesets for a proxy action, click the **View/Edit Proxy** icon  (the first icon to the right of the **Proxy action** drop-down list) and select a category of settings from the left side of the dialog box. For more information, see [About rules and rulesets](#) and the “About” topic for the specific policy type:

- [About the DNS proxy](#)
- [About the FTP proxy](#)
- [About the H.323 proxy](#)
- [About the HTTP proxy](#)
- [About the HTTPS proxy](#)
- [About the POP3 proxy](#)
- [About the SIP proxy](#)
- [About the SMTP proxy](#)
- [About the TCP-UDP proxy](#)
- [About the TFTP proxy](#)

Advanced tab

[Set an operating schedule](#)

[Apply Traffic Management actions to a policy](#)

[Set traffic priority in a policy](#)

[Set ICMP error handling](#)

[Apply NAT rules](#)

[Enable QoS Marking for a policy](#)

[Add a sticky connection duration to a policy](#)

Set access rules for a policy

You use the **Policy** tab of the **Edit Policy Properties** dialog box to configure access rules for a given policy.

The **policy_name connections are** field defines whether traffic that matches the rules in the proxy is allowed, or traffic that matches the rules is denied. You use these settings to configure how traffic is handled:

Allowed

The Firewall allows traffic that uses this policy if it matches the rules you set in the policy.

Denied

The Firewall denies all traffic that matches the rules in this policy. You can configure it to record a log message when a computer tries to use this policy. The policy can also automatically add a computer or network to the Blocked Sites list if it tries to start a connection with this policy (for more information, see [Block sites temporarily with policy settings](#)).

Denied (send reset)

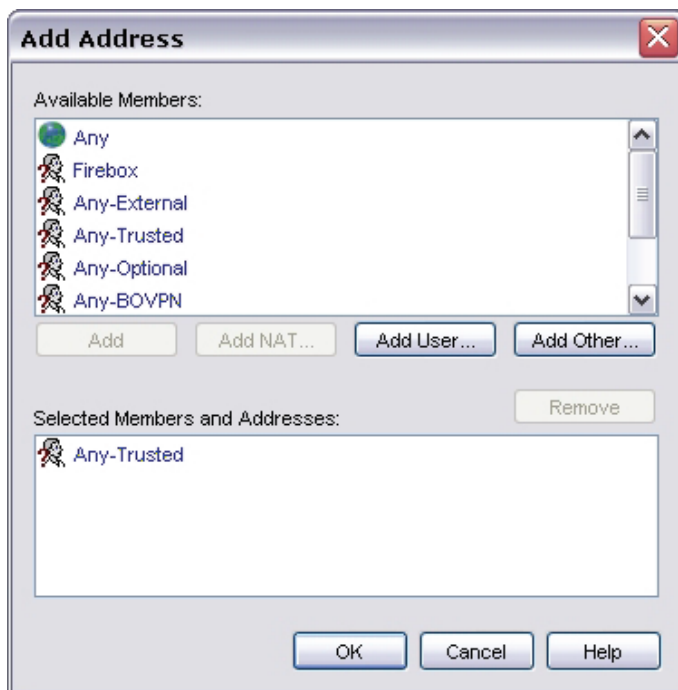
The Firebox denies all traffic that matches the rules in this policy. You can configure it to record a log message when a computer tries to use this policy. The policy can also automatically add a computer or network to the Blocked Sites list if it tries to start a connection with this policy (for more information, see [Block sites temporarily with policy settings](#)). The Firebox also sends a reset (RST) packet to tell the client that the session is refused and closed.

The **Policy** tab also includes:

- A **From** list (or source) that specifies who can send (or cannot send) network traffic with this policy.
- A **To** list (or destination) that specifies who the Firebox can route traffic to if the traffic matches (or does not match) the policy specifications.

For example, you could configure a ping packet filter to allow ping traffic from all computers on the external network to one web server on your optional network. Note, however, that the destination network is made vulnerable whenever you open it to connections over the port or ports that the policy controls. Make sure you use care when you configure your policies.

1. To add members to your access specifications, click **Add** for the **From** or the **To** member list.
The Add Address dialog box appears.



2. The **Available Members** list contains the aliases you can add to the **From** or **To** lists. Select an alias and click **Add**, or double-click an alias in this window.
If you want to add hosts, users, aliases or tunnels to the policy that do not appear in the **Available Members** list, see [Add new members for policy definitions](#).
3. Repeat the previous step to add other members and addresses. Your policy can have more than one object in the **From** or **To** field. Click **OK**.

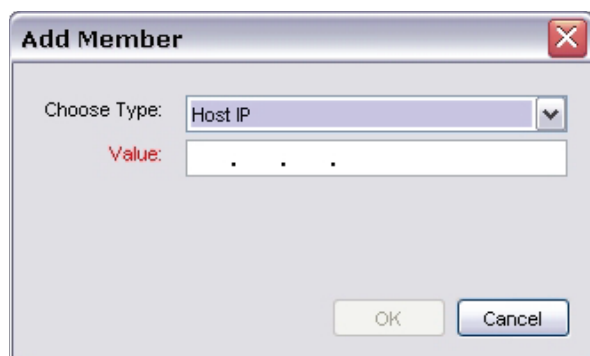
The source and destination can be a host IP address, host range, host name, network address, user name, alias, VPN tunnel, or any combination of those objects. For more information on the aliases that appear as options on the **From** and **To** list, see the topic [About aliases](#).

To create a new alias, see [Create an alias](#).

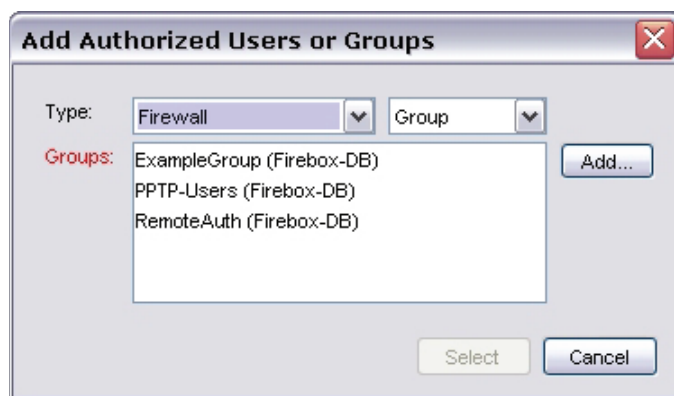
Add new members for policy definitions

1. If you want to add a user or group to the **Available Members** list, click **Add User**. If you want to add hosts, aliases, or tunnels to the **Available Members** list, click **Add Other**.
2. If you selected **Add Other**, the **Add Member** dialog box appears. From the **Choose Type** drop-down list, select the host range, host IP address, or network IP address to add. In the **Value** text box, type the correct network address, range, or IP address. Click **OK**.

The member or address appears in the Selected Members and Addresses list.

The 'Add Member' dialog box has a title bar with a close button. It contains a 'Choose Type' dropdown menu with 'Host IP' selected. Below it is a 'Value' text box with three dots. At the bottom are 'OK' and 'Cancel' buttons.

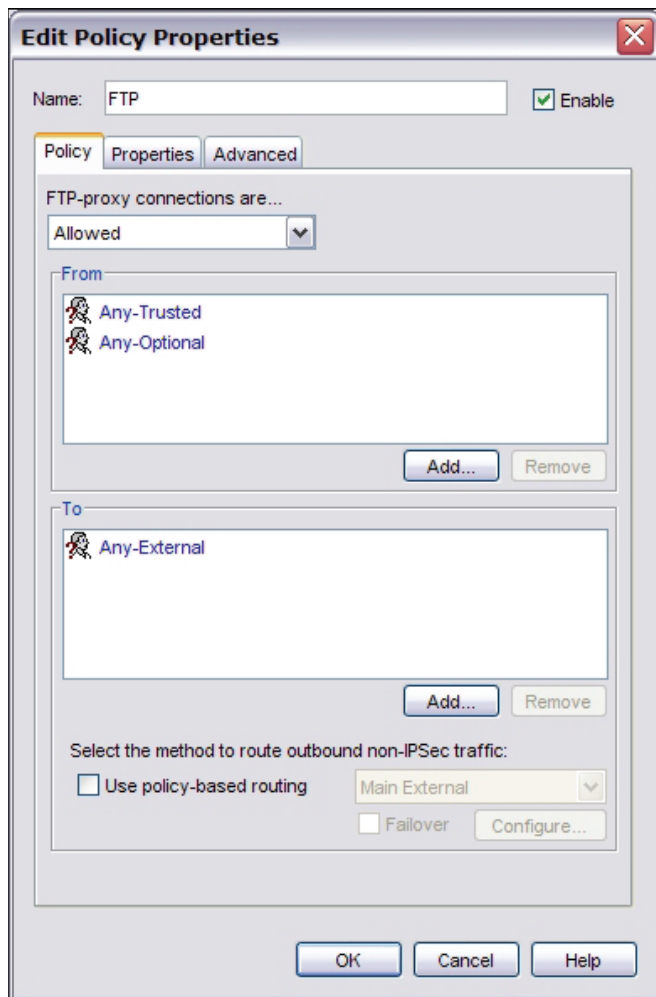
3. If you selected **Add User**, the **Add Authorized Users or Groups** dialog box appears. Select the type of user or group, select the authentication server, and whether you want to add a user or group. Click **OK**.

The 'Add Authorized Users or Groups' dialog box has a title bar with a close button. It contains two dropdown menus: 'Type' with 'Firewall' selected and 'Group' with a blank selection. Below these is a list box labeled 'Groups' containing 'ExampleGroup (Firebox-DB)', 'PPTP-Users (Firebox-DB)', and 'RemoteAuth (Firebox-DB)'. To the right of the list is an 'Add...' button. At the bottom are 'Select' and 'Cancel' buttons.

4. If the user or group you want to add does not appear in the list, it is not yet defined as an authorized user or group. To define a new authorized user or group, see [Use authorized users and groups in policies](#).

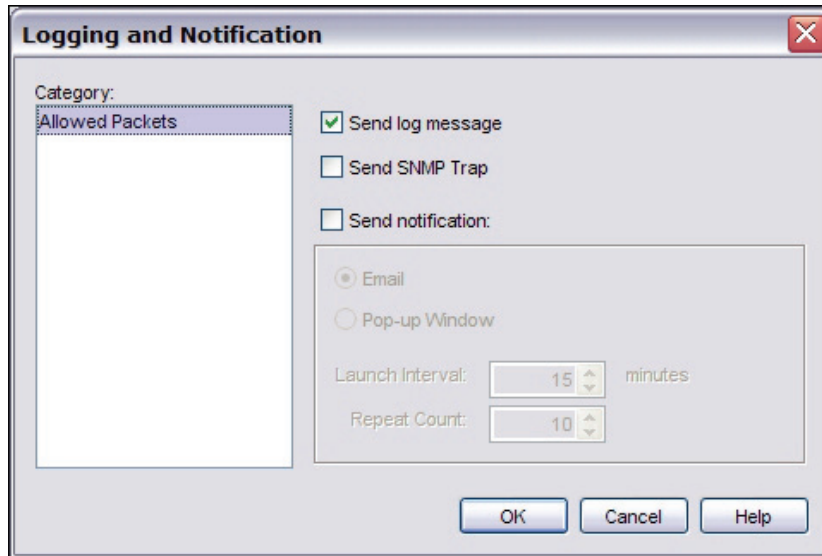
Configure logging and notification for a policy

1. From Policy Manager, [add a policy](#) or double-click a policy icon to edit an existing policy.
The Edit Policy Properties dialog box appears.



2. Click the **Properties** tab.

- Click **Logging**.
The *Logging and Notification* dialog box appears.



- Set the parameters to match your security policy.
For information on fields in the **Logging and Notification** dialog box, see [Set logging and notification preferences](#).

Block sites temporarily with policy settings

You can use the policy configuration to block sites that try to use a denied service:

- From Policy Manager, double-click the policy icon.
The *Edit Policy Properties* dialog box appears.
- On the **Policy** tab, make sure you set the **Connections Are** drop-down list to **Denied** or **Denied (send reset)**.
- On the **Properties** tab, select the check box **Automatically block sites that attempt to connect**. IP addresses from the denied packets are added to the Temporary Blocked Sites list for 20 minutes (by default). You can change this time interval on the **Auto-Blocked** tab in the **Blocked Sites Configuration** dialog box.
- You can use the Temporary Blocked Sites list with log messages to help you make decisions about which IP addresses to block permanently. In the policy definition, click the **Properties** tab, click the **Logging** button and [Set logging and notification preferences](#).

Set a custom idle timeout

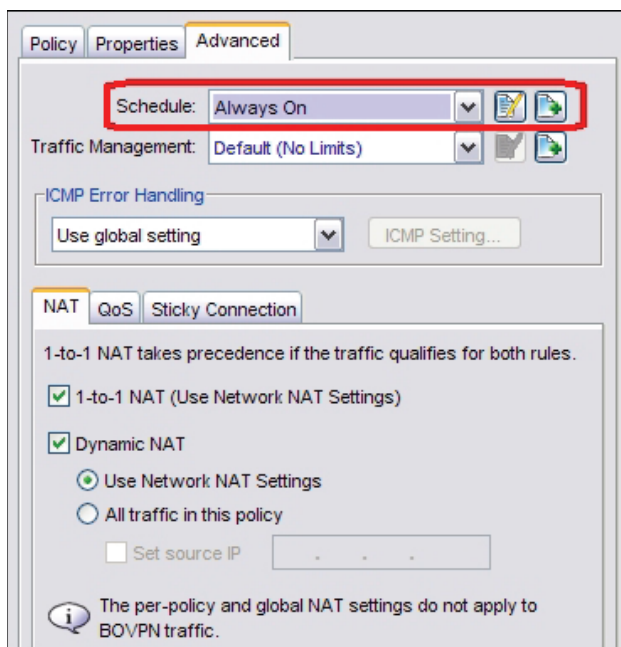
Idle timeout is the maximum length of time the user can stay authenticated when idle (not passing any traffic to the external network). If you set this field to zero (0) seconds, minutes, hours, or days, no idle timeout is used and the user can stay idle for any length of time.

Idle timeout is usually determined by the global authentication timeout described in [Set global authentication values](#), in the **Setup Firebox User** dialog box described in [Define a new user for Firebox authentication](#), or, for users authenticated by third-party servers, the timeouts set on those servers. (The timeouts for the Firebox and third-party servers override the global authentication timeouts.) You can set an idle timeout that applies only to a specific policy. This timeout overrides all other timeouts:

- On the **Properties** tab of the **Policy Properties** dialog box, click **Specify Custom Idle Timeout**.
- Click the arrows to set the number of seconds before timeout.

Set an operating schedule

You can set an operating schedule for the policy. You can use the schedule templates in the **Schedule** drop-down list or create a custom schedule. If you want to create a new schedule, see [Create schedules for Firebox actions](#).



Note that schedules can be shared by more than one policy.

Configure 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.

Policy-based routing can be used when you have more than one external interface and have configured your Firebox for multi-WAN. With policy-based routing, you can make sure that 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. For example, if you want email to be routed through a particular interface, you can use policy-based routing in the SMTP or POP3 proxy definition.

Policy-based routing takes precedence over other multi-WAN settings.

Policy-based routing, failover, and failback

When you use policy-based routing along with multi-WAN failover, you can specify whether traffic that matches the policy uses another external interface when failover occurs. The default is that the traffic is dropped until the interface is available again.

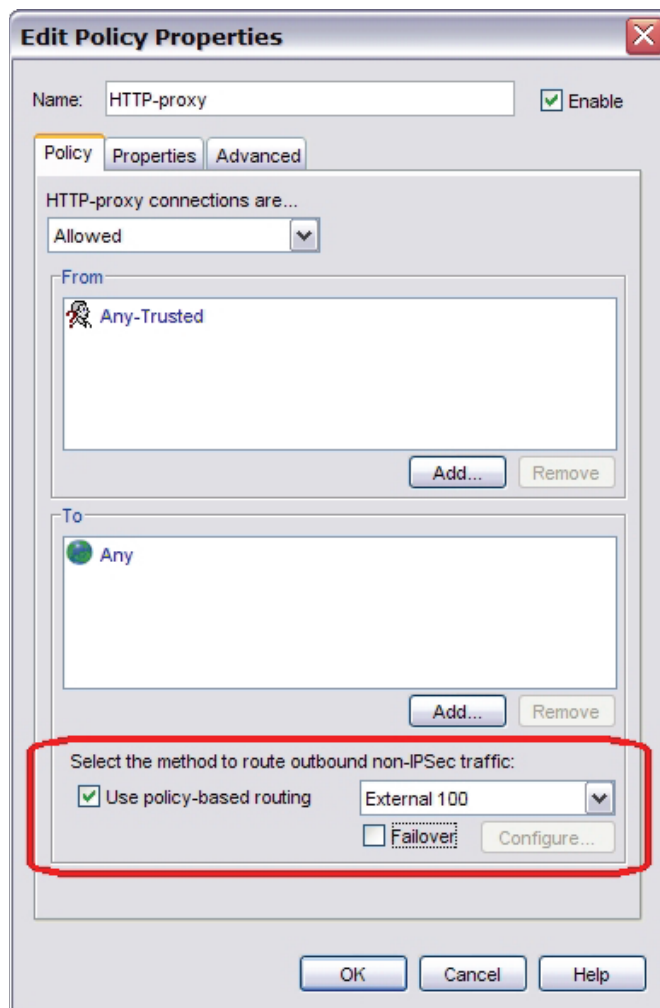
Also, failback settings (defined on the **Multi-WAN** tab of the **Network Configuration** dialog box) apply to policy-based routing. If a failover event occurs, and the original interface later becomes available, the Firebox can send active connections to the failover interface or it can fail back to the original interface. New connections are sent to the original interface.

Restrictions on policy-based routing

- Policy-based routing is available only if multi-WAN is enabled. If you enable multi-WAN, the **Edit Policy Properties** dialog box automatically includes fields for configuring policy-based routing. By default, policy-based routing is not enabled.
- Policy-based routing does not apply to IPSec traffic, or to traffic destined for the trusted or optional network (incoming traffic).

Add policy-based routing to a policy

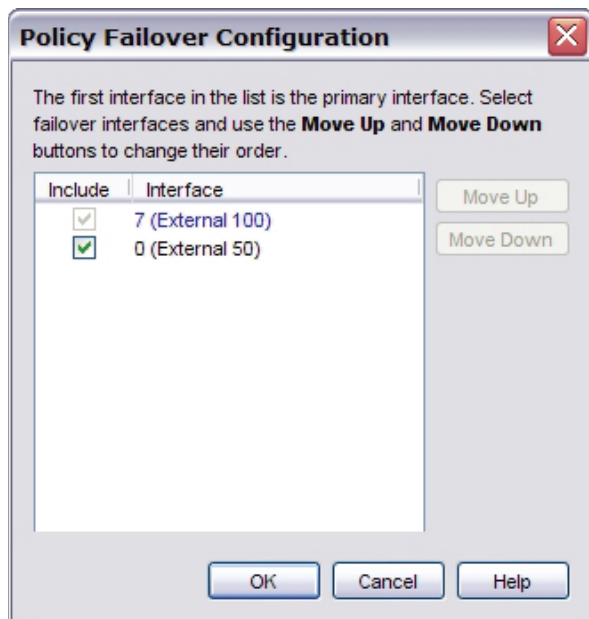
1. In Policy Manager, double-click the icon of the policy for which you want to define policy-based routing.
The Edit Policy Properties dialog box appears.
2. At the bottom of the **Edit Policy Properties** dialog box, select the **Use policy-based routing** check box to enable policy-based routing.



3. To specify the interface to send outbound traffic that matches the policy, select the interface name from the adjacent drop-down list. You must make sure that the interface you select is a member of the alias or network that you set in the **To** field of your policy.
4. (Optional) Configure policy-based routing with multi-WAN failover as described below.
5. Click **OK**.

Configure policy-based routing with failover

1. From the **Edit Policy Properties** dialog box, select **Failover** if you want to set the interface you specified for this policy as the primary interface and define other external interfaces as backup interfaces for all non-IPSec traffic.
If you do not select **Failover** and the interface you set for this policy is not active, traffic is dropped until link monitoring establishes that the interface is available again.
2. Click **Configure** to specify backup interfaces for this policy. If the primary interface you set for this policy is not active, traffic is sent to the backup interface or interfaces you specify here.
The Policy Failover Configuration dialog box appears.



3. In the **Include** column, select the check box for each interface you want to use in the failover configuration. Use the **Move Up** and **Move Down** buttons to set the order for failover. The first interface in the list is the primary interface.
4. When you have selected the interfaces you want to use and set the order you want, click **OK**.
5. Click **OK** to close the **Edit Policy Properties** dialog box.
6. [Save the configuration file.](#)

About using static NAT for a policy

Static NAT is also known as port forwarding. Static NAT is a port-to-host NAT. A host sends a packet from the external network to a specified public address and port. Static NAT changes this address to an address and port behind the firewall.

For more information on static NAT, and for information on how to use it, see [About static NAT](#).

Because of how static NAT operates, it is available only for policies that use a specified port, which includes TCP and UDP.

About using NAT with SMTP

To help fight spam, many servers that receive email do a reverse lookup of the source IP address the mail comes from. The receiving server does this to make sure that the sending server (the server sending the email) is an authorized mail server for that domain. Because of this, we recommend that you use the external IP address of your Firebox as the MX record for your domain. An MX, or Mail exchange, record is a type of DNS record that sets how email is routed through the Internet. MX records show the servers to send an email message to, and which server to send an email message to first, by priority.

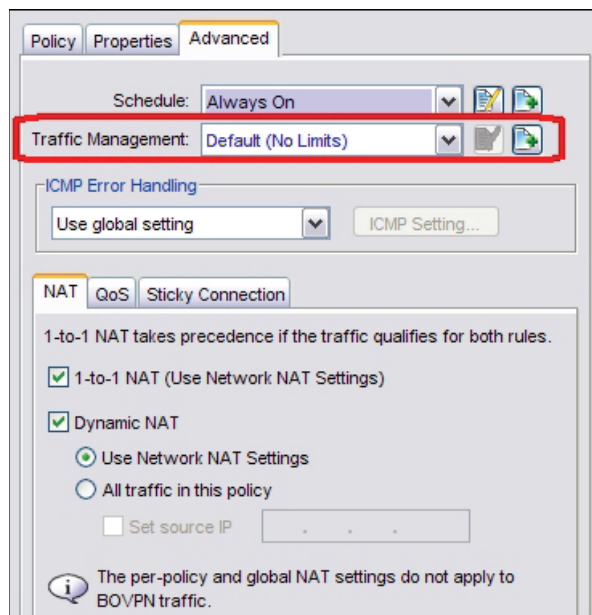
Usually, connections that start from a trusted or optional network and go to the Internet show the external IP address of the Firebox as the source IP address of the packets. If the Firebox external IP address is not your domain's MX record IP address, some remote servers reject email that you send. They do this because the SMTP session does not show your MX record as the source IP address for the connection. If your Firebox does not use your MX record IP address as the external interface IP address, you can use a 1-to-1 NAT mapping to make outgoing email connections show the correct source IP address. For more information, see [About 1-to-1 NAT](#).

To configure 1-to-1 NAT for a policy, see [Configure policy-based 1-to-1 NAT](#).

Apply a Traffic Management action to a policy

After you have created Traffic Management actions, or if actions have already been created on the Firebox, you can apply them to the policies you have configured in Policy Manager. To apply a Traffic Management action:

1. From Policy Manager, double-click the icon of the policy for which you want to guarantee a minimum bandwidth. Click the **Advanced** tab.
2. From the **Traffic Management** drop-down list, select a Traffic Management action to apply to the policy.



3. Click **OK** to close the **Edit Policy Properties** dialog box. Save your changes to the Firebox. You will get a warning message if the sum of all guaranteed bandwidths for an interface approaches or exceeds the bandwidth limit you set for the interface.
The new action appears in the Traffic Management Actions dialog box.

If you want to track the bandwidth being used by a policy, go to the **Service Watch** tab of Firebox System Manager and specify **Bandwidth** instead of **Connections**. For more information, see [Visual display of policy usage](#).

Use Traffic Management actions in a multi-WAN environment

When a Traffic Management action is applied on a multiple WAN policy with the multi-WAN feature set up in round-robin mode, the maximum bandwidth and connection rate settings in the Traffic Management action control the total throughput and connection rate across all interfaces. This includes all external interfaces that are configured to route traffic.

Apply a Traffic Management action to multiple policies

When the same Traffic Management action is applied to multiple policies, the connection rate, maximum bandwidth, and minimum bandwidth apply to all traffic that matches each policy. If two policies share an action that has a maximum bandwidth of 100 kbps, then all traffic that matches those policies will be limited to 100 kbps. Each policy will not get 100 kbps; they get 100 kbps combined.

If you have limited bandwidth on an interface used for several applications, each using unique ports, you might need all the high priority connections to share one Traffic Management action. If you have lots of bandwidth to spare, you could create separate Traffic Management actions for each application.

About server load balancing for a policy

If you have Fireware Pro, you can use the server load balancing feature to help you increase the scalability and performance of a high-traffic network with multiple public servers protected by your Firebox. With server load balancing, you can have the Firebox control the number of sessions initiated to as many as 10 servers for each firewall policy you configure. The Firebox controls the load based on the number of sessions in use on each server. For information on how to configure server load balancing, see [Configure server load balancing](#).

Set traffic priority for a policy

Traffic priority can be set at the interface level, but you can override this setting for individual policies:

1. To override the setting at the interface level, select the **Override per-interface settings** check box.
2. In the **Prioritize Traffic Based On** drop-down list, select either **QoS Marking** or **Custom Value**.
3. If you chose **Custom Value**, in the **Value** field, select a value from 0 (Best Effort) to 7 (highest priority).

Set ICMP error handling

You can set the ICMP error handling settings associated with the policy. These settings override the global ICMP error handling settings.

From the **ICMP Error Handling** drop-down list, select:

Use global setting

Use the global ICMP error handling setting set for the Firebox. For information on this global setting, see [Define Firebox global settings](#).

Specify setting

Configure a parameter that overrides the global setting. Click **ICMP Setting**. From the **ICMP Error Handling Settings** dialog box, select the check boxes to configure individual settings. For information on these settings, see [Define Firebox global settings](#).

Apply NAT rules

You can apply Network Address Translation (NAT) rules to a policy. From the **Advanced** tab of the **Edit Policy Properties** dialog box, select one of the following options:

1-to-1 NAT

With this type of NAT, the Firebox uses private and public IP ranges that you set, as described in [Use 1-to-1 NAT](#).

Dynamic NAT

With this type of NAT, the Firebox maps private IP addresses to public IP addresses. All policies have dynamic NAT enabled by default. Select **Use Network NAT Settings** if you want to use the dynamic NAT rules set for the Firebox. Select **All traffic in this policy** if you want to apply NAT to all traffic in this policy.

You can use the **Set Source IP** field to set a dynamic NAT source IP address for any policy that uses dynamic NAT. This makes sure that any traffic that uses this policy shows a specified address from your public or external IP address range as the source. You would most often do this to force outgoing SMTP traffic to show your domain's MX record address when the IP address on the Firebox's external interface is not the same as your MX record IP address.

1-to-1 NAT rules have higher precedence than dynamic NAT rules.

Use QoS Marking for a policy

QoS Marking creates different classes of service for different kinds of outbound network traffic. When you mark traffic, you change up to six bits on packet header fields defined for this purpose. QoS-capable external devices can make use of this marking and provide appropriate handling of a packet as it travels from one point to another in a network.

You can use QoS Marking on a per-interface or per-policy basis. When you define QoS Marking for an interface, packets leaving that interface are marked. QoS Marking for a policy marks traffic that uses the policy.

1. From the **Edit Policy Properties** dialog box, click the **Advanced** tab.
2. Midway down the dialog box, select the **QoS** tab.
3. Select the **Override per-interface settings** check box to make the QoS Marking for a policy override any QoS Marking set on an interface.

For information on how to use QoS Marking, see [About QoS Marking](#).

Add a sticky connection duration to a policy



*The **Sticky Connections** tab appears only if multi-WAN is enabled.*

The sticky connection setting for a policy overrides the global sticky connection setting, described in [About advanced multi-WAN settings](#).

1. From the **Advanced** tab of the **Policy Properties** dialog box, click the **Sticky Connection** tab.
2. Keep the **Override Multi-WAN sticky connection setting** check box clear if you want the sticky connection configured on the **Network > Configuration > Multi-WAN** tab to apply. Select this check box if you want to set a custom sticky connection for this policy.
3. If you want to set a custom sticky connection for this policy, select the **Enable sticky connection** check box.
4. Enter the amount of time to maintain the connection.

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.

Use automatic order

Unless you manually set precedence, the Firebox gives the highest precedence to the most specific policies and the lowest to the least specific. The Firebox examines specificity of the following criteria in this order. If it cannot determine the precedence from the first criterion, it moves to the second, and so on.

1. The specificity of the policy itself. For example, an Any policy is less specific than policies that allow only specific traffic.
2. Protocols set for the policy type. For example, a policy that specifies many ports for a given protocol is less specific than a policy with fewer ports.
3. Traffic rules of the **To** field. Most specific to least specific are: rules specifying IP address ranges, users, groups, interfaces.
4. Traffic rules of the **From** field. Most specific to least specific are: rules specifying IP address ranges, users, groups, interfaces.
5. Firewall action applied to the policies. Most specific to least specific is: Denied or Denied (send reset), Allowed (proxy policy), Allowed (packet filter policy).
6. Schedules applied to the policies. Most to least specific is: Always off, Sometimes on, Always on.
7. Alphanumeric sequence based on policy type.
8. Alphanumeric sequence based on policy name.

For details on each of these steps, see [About automatic policy order](#).

Set precedence manually

To switch to manual-order mode, select **View > Auto-Order Mode** so that the checkmark disappears. You are asked to confirm if you want to switch to manual-order mode. If you switch to manual-order mode, the Policy Manager window changes to the Details view. You cannot change the order of policies if you are in Large Icons view.

To change the order of a policy, select it and drag it to its new location.

About automatic policy order

The Firebox gives the highest precedence to the most specific policies and the lowest precedence to the least specific. The Firebox examines specificity of criteria in this order. If it cannot determine the precedence from the first criterion, it moves to the second, and so on:

1. Policy specificity.
2. Protocols set for the policy type.
3. Traffic rules of the **To** field.
4. Traffic rules of the **From** field.
5. Firewall action (Allowed, Denied, or Denied (send reset)) applied to the policies.
6. Schedules applied to the policies.
7. Alphanumeric sequence based on policy type
8. Alphanumeric sequence based on policy name.

The sections below give more details about what the Firebox does within these eight steps.

Policy specificity and protocols

The Firebox uses these criteria in sequence to compare two policies until it finds that the policies are equal or that one is more detailed than the other:

1. An Any policy always has the lowest precedence.
2. Check for the number of TCP 0 (any) or UDP 0 (any) protocols. The policy with the smaller number has higher precedence.
3. Check for the number of unique ports for TCP and UDP protocols. The policy with the smaller number has higher precedence.
4. Add up the unique TCP and UDP port numbers. The policy with the smaller number has higher precedence.
5. Score the protocols based on their IP protocol value. The policy with the smaller score has higher precedence.

If the Firebox cannot set the precedence when it compares the policy specificity and protocols, it examines traffic rules.

Traffic rules

The Firebox uses these criteria in sequence to compare the most general traffic rule of one policy with the most general traffic rule of a second policy. It assigns higher precedence to the policy with the most detailed traffic rule. The list of traffic rules from most detailed to the most general:

1. Host address
2. IP address range (smaller than the subnet being compared to)
3. Subnet
4. IP address range (larger than the subnet being compared to)
5. Authentication user name
6. Authentication group
7. Interface, Firebox
8. Any-External, Any-Trusted, Any-Optional
9. Any

For example, compare these two policies:

HTTP-1

From: Trusted, user1

HTTP-2

From: 10.0.0.1, Any-Trusted

Trusted is the most general entry for HTTP-1. Any-Trusted is the most general entry for HTTP-2. Because Trusted is within Any-Trusted, HTTP-1 is the more detailed traffic rule. This is correct despite the fact that HTTP-2 includes an IP address, because the Firebox compares the most general traffic rule of one policy to the most general traffic rule of the second policy to set precedence

If the Firebox cannot set the precedence when it compares the traffic rules, it examines the firewall actions.

Firewall actions

The Firebox compares the firewall actions of two policies to set precedence. Precedence of firewall actions from highest to lowest is:

1. Denied or Denied (send reset)
2. Allowed proxy policy
3. Allowed packet-filter policy

If the Firebox cannot set the precedence when it compares the firewall actions, it examines the schedules.

Schedules

The Firebox compares the schedules of two policies to set precedence. Precedence of schedules from highest to lowest is: 1—Always off. 2—Sometimes on. 3—Always on.

If the Firebox cannot set the precedence when it compares the schedules, it examines the policy types and names.

Policy types and names

If the two policies do not match any other precedence criteria, the Firebox sorts the policies in alphanumeric sequence. First, it uses the policy type. Then, it uses the policy name. Because no two policies can be the same type and have the same name, this is the last criteria for precedence.

15 Proxy Policies

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.

Types of proxies

Important concepts about proxies are:

- [About rules and rulesets](#)
- [About proxy actions](#)
- [About predefined and user-defined proxy actions](#)

About rules and rulesets

A major portion of the work you do to configure a proxy policy involves creating or modifying rules, which are sets of criteria to which the proxy compares traffic. A rule consists of a type of content, pattern, or expression, and the action the Firebox does when a component of the packet's content matches that content, pattern, or expression. Rules also include settings for when the Firebox sends alarms or if it sends events to the log file. A ruleset is a group of rules based on one feature of a proxy such as the content types or filenames of email attachments. The process to create and modify rules is consistent throughout all Fireware proxies.

The Firebox includes default sets of rules for each proxy policy included in the Firebox configuration. Separate sets of rules are provided for clients and servers—to protect both your trusted users and your public servers. You can use these rules without changing them, or you can customize them to meet your business needs.

About working with rules and rulesets

When you configure a proxy, you can see the rulesets for that proxy in the **Categories** list. The rulesets you see change when you change the proxy action on the **Properties** tab of a proxy configuration window. For example, the rules for the FTP-Client action have different settings than the rules for the FTP-Server action.

WatchGuard proxies have predefined rulesets that provide a good balance of security and accessibility for most installations. If a default ruleset does not meet all of your business needs, you can add, delete, or modify rules.

Simple and advanced views

You can see rules in proxy definitions in two ways. The simple view is used to configure wildcard pattern matching with simple regular expressions.

To see the advanced view of the current rules, click **Change View**. This view shows the action for each rule. It also has buttons you can use to edit, clone (use an existing rule definition to start a new one), delete, or reset rules. You use the advanced view to configure exact match and Perl-compatible regular expressions.

To go back to the simple view, click **Change View** again. Note that you cannot go back to simple view if the enabled rules have different action, alarm, or log settings. You must continue to use the advanced view. For example, if most rules are set to **Allow** but one is set to **Deny**, you must use the advanced view.

Add rules

You can use either the simple or advanced view of the ruleset to add rules. Use the simple view to configure wildcard pattern matching with simple regular expressions. Use the advanced view to configure exact match and Perl-compatible [regular expressions](#). Also, the advanced view shows the action for each rule and has buttons you can use to edit, clone (use an existing rule definition to start a new one), delete, or reset rules.

To switch from either view to the other, click **Change View**.

Add rules (simple view)

From the simple view, do these steps to add new rules:

1. In the **Pattern** text box, type a pattern that uses simple regular expression syntax.
*The wildcard for zero or more than one character is *. The wildcard for one character is ?.*
2. Click **Add**.
The new rule appears in the Rules box.
3. In the **Actions to take** section, the **If matched** drop-down list sets the action to do if the contents of a packet match one of the rules in the list. The **None matched** drop-down list sets the action to do if the contents of a packet do not match a rule in the list. Below is a list of all possible actions. Different actions appear for different proxies or for different features of a particular proxy. For example, the actions **Strip** and **Lock** apply only to signature-based intrusion prevention actions.

Allow

Allows the connection.

Deny

Denies a specific request but keeps the connection if possible. Sends a response to the client.

Drop

Denies the specific request and drops the connection. Does not send a response to the sender. The Firewall sends only a TCP reset packet to the client. The client's browser might display The connection was reset or The page cannot be displayed but the browser does not tell the user why.

Block

Denies the request, drops the connection, and blocks the site. For more information on blocked sites, see [About Blocked Sites](#).

All traffic from the site's IP address is denied for the amount of time specified in Policy Manager at **Setup > Default Threat Protection > Blocked Sites**, on the **Auto-Blocked** tab. Use this action only if you want to stop all traffic from the offender for this time.

Strip

Removes an attachment from a packet and discards it. The other parts of the packet are sent through the Firebox to its destination.

Lock

Locks an attachment, and wraps it so that it cannot be opened by the user. Only the administrator can unlock the file.

AV Scan

Scans the attachment for viruses. If you select this option, Gateway AntiVirus is enabled for the policy.

4. An alarm is a mechanism to tell users when a proxy rule applies to network traffic. Use the **Alarm** check box to configure an alarm for this event. To set the options for the alarm, select **Proxy Alarm** from the **Categories** list on the left side of a Proxy Configuration window. You can send an SNMP trap, send email, or open a pop-up window.
5. Use the **Log** check box to write a message to the traffic log for this event.

Add rules (advanced view)

You use the advanced view to configure exact match and Perl-compatible regular expressions. For more information about the use of regular expressions in proxy rules, see the product FAQs on the product support web site at <http://www.watchguard.com/support/faqs/fireware>.

1. In the **Proxy Action Configuration** dialog box, click **Add**.
The New <ruletype> Rule dialog box appears.

New Commands Rule

Rule Name:

Rule Settings

Pattern Match
 (*.?.[.]) Wildcards
 Use '%0x[hex-data]%' for binary data

Rule Actions

Action: ☐ Alarm ☒ Log

2. Configure the fields as follows:

Rule Name

Name of the rule. This field is blank if you are adding a rule, can be edited if you clone a rule, and cannot be changed if you are editing a rule

Rule Settings

To match the rule text exactly, select **Exact Match** from the drop-down list. To match a pattern of text using wildcard characters, select **Pattern Match**. To match a pattern of text with a regular expression, select **Regular Expression**.

For information on how to work with regular expressions, see [About regular expressions](#).

Rule Text

Type the text of the rule. If you selected Pattern Match as the rule setting, use an asterisk (*), a period (.), or a question mark (?) as wildcard characters.

Action, Alarm, Log

Set these fields as described in the section for simple rules, above.

Cut and paste rule definitions

You can copy and paste text in enterable fields from one proxy definition to another. For example, suppose you write a custom deny message for the POP3 proxy. You can select the deny message, copy it, and paste it into the **Deny Message** box for the SMTP proxy.

When you copy between proxy definitions, you must make sure the field you copy is compatible with the proxy you paste it into.

You can copy rulesets only between proxies or categories within these four groups. Other combinations are not compatible.

Content Types	Filenames	Addresses	Authentication
HTTP Content Types	FTP Download	SMTP Mail From	SMTP Authentication
SMTP Content Types	FTP Upload	SMTP Mail To	POP3 Authentication
POP3 Content Types	HTTP URL Paths		
	SMTP Filename		
	POP3 Filenames		

Change the order of rules

The order that rules are shown in the **Rules** list is the same as the order in which traffic is compared to the rules. The proxy compares traffic to the first rule in the list and continues in sequence from top to bottom. When traffic matches a rule, the Firebox performs the related action. It performs no other actions, even if the traffic matches a rule later in the list.

To change the sequence of rules, you must use the advanced view:

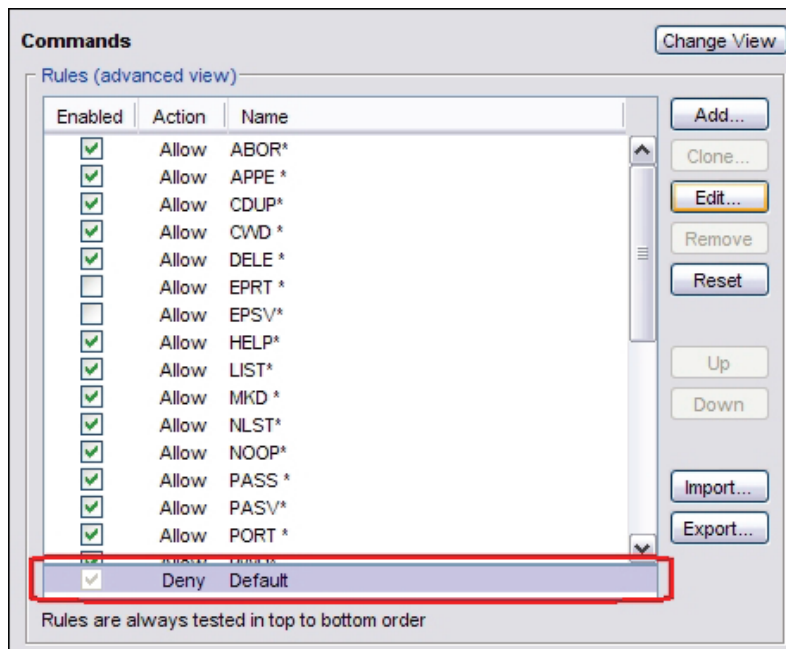
1. Click **Change View** to see the advanced view of rules.
2. Select the rule whose order you want to change. Click the **Up** or **Down** button to move the rule up or down in the list.

Modify the default rule

If traffic does not match any of the rules you have defined for a proxy category, the Firebox uses the default rule. This rule appears at the bottom of any list of rules when you use the advanced view.

To modify the default rule:

1. Select it and click **Edit**.
The Edit Default Rule dialog box appears.



2. You can change the action for the default rule, and whether the action triggers an alarm or a log message. You cannot change the name Default or the order of the rule. It must be the last rule in the list.
3. Click **OK**.

About regular expressions

A regular expression is a group of letters, numbers, and special characters used to match data. You can use Perl-compatible regular expressions (PCRE) in your Firebox configuration to match certain types of traffic in proxy actions. For example, you can use one regular expression to block connections to some web sites and allow connections to other web sites. You can also deny SMTP connections when the recipient is not a valid email address for your company. For example, if you want to block parts of a web site that violate your company's Internet use policy, you can do this if you use a regular expression in the URL Paths category of the HTTP proxy configuration.

General guidelines

- Regular expressions in Fireware are case-sensitive — When you create a regular expression, you must be careful to match the case of the letters in your regular expression to the letters of the text you want to match. You can change the regular expression to not be case-sensitive when you put the (?i) modifier at the start of a group.
- Regular expressions in Fireware are different from MS-DOS and Unix wildcard characters — When you change files using MS-DOS or the Windows Command Prompt, you can use ? or * to match one or more characters in a file name. These simple wildcard characters do not operate the same way in Fireware. See the subsequent sections for more information on how wildcard characters operate in Fireware.

How to build a regular expression

The most simple regular expression is made from the text you want to match. Letters, numbers, and other printable characters all match the same letter, number, or character that you type. A regular expression made from letters and numbers can match only a character sequence that includes all of those letters and numbers in order.

Example: `fat` matches `fat`, `fatuous`, and `infatuated`, as well as many other sequences.



Fireware accepts any character sequence that includes the regular expression. A regular expression frequently matches more than one sequence. If you use a regular expression as the source for a Deny rule, you can block some network traffic by accident. We recommend that you fully test your regular expressions before you save the configuration to your Firebox.

To match different sequences of characters at the same time, you must use a special character. The most common special character is the period (`.`), which is similar to a wildcard. When you put a period in a regular expression, it matches any character, space, or tab. The period does not match line breaks (`\r\n` or `\n`).

Example: `f.t` matches `foot`, `feet`, `f&#t`, `f -t`, and `f\t3t`.

To match a special character, such as the period, you must add a backslash (`\`) before the character. If you do not add a backslash to the special character, the rule may not operate correctly. It is not necessary to add a second backslash if the character usually has a backslash, such as `\t` (tab stop).

Example: `\$9\.` matches `$9.99`

You must add a backslash to each of these special characters to match the real character: `? . * | + $ \ ^ () [`

Hexadecimal characters

To match hexadecimal characters, use `\x` or `%0x%`. Hexadecimal characters are not affected by the case-insensitive modifier.

Example: `\x66` or `%0x66%` matches `f`, but cannot match `F`.

Repetition

To match a variable amount of characters, you must use a repetition modifier. You can apply the modifier to a single character, or a group of characters. There are four types of repetition modifiers:

- Numbers inside curly braces (such as `{2,4}`) match as few as the first number, or as many as the second number.
Example: `3{2,4}` matches `33`, `333`, or `3333`. It does not match `3` or `33333`.
- The question mark (`?`) matches zero or one occurrences of the preceding character, class, or group.
Example: `me?et` matches `met` and `meet`.
- The plus sign (`+`) matches one or more occurrences of the preceding character, class, or group.
Example: `me+t` matches `met`, `meet`, and `meeeeeeeeet`.
- The asterisk (`*`) matches zero or more occurrences of the preceding character, class, or group.
Example: `me*t` matches `mt`, `met`, `meet`, and `meeeeeeeeet`.

To apply modifiers to many characters at once, you must make a group. To group a sequence of characters, put parentheses around the sequence.

Example: `ba(na)*` matches `ba`, `bana`, `banana`, and `banananananana`.

Character classes

To match one character from a group, use square brackets instead of parentheses to create a character class. You can apply repetition modifiers to the character class. The order of the characters inside the class does not matter.

The only special characters inside a character class are the closing bracket (]), the backslash (\), the caret (^), and the hyphen (-).

To use a caret in the character class, do not make it the first character.

To use a hyphen in the character class, make it the first character.

Example: `gr[ae]y` matches gray and grey.

A negated character class matches everything but the specified characters. Type a caret (^) at the beginning of any character class to make it a negated character class.

Example: `[Qq][^u]` matches Qatar, but not question or Iraq.

Ranges

Character classes are often used with character ranges to select any letter or number. A range is two letters or numbers, separated by a hyphen (-), that mark the start and finish of a character group. Any character in the range can match. If you add a repetition modifier to a character class, the preceding class is repeated.

Example: `[1-3][0-9]{2}` matches 100 and 399, as well as any number in between.

Some ranges that are used frequently have a shorthand notation. You can use shorthand character classes inside or outside other character classes. A negated shorthand character class matches the opposite of what the shorthand character class matches. The table below includes several common shorthand character classes and their negated values.

Class	Equivalent to	Negated	Equivalent to
<code>\w</code>	Any letter or number [A-Za-z0-9]	<code>\W</code>	Not a letter or number
<code>\s</code>	Any whitespace character [\t\r\n]	<code>\S</code>	Not whitespace
<code>\d</code>	Any number [0-9]	<code>\D</code>	Not a number

Anchors

To match the beginning or end of a line, you must use an anchor. The caret (^) matches the beginning of a line, and the dollar sign (\$) matches the end of a line.

Example: `^am.*$` matches ampere if ampere is the only word on the line. It does not match dame.

You can use `\b` to match a word boundary, or `\B` to match any position that is not a word boundary.

There are three kinds of word boundaries:

- Before the first character in the character sequence, if the first character is a word character (`\w`)
- After the last character in the character sequence, if the last character is a word character (`\w`)
- Between a word character (`\w`) and a non-word character (`\W`)

Alternation

You can use alternation to match a single regular expression out of several possible regular expressions. The alternation operator in a regular expression is the pipe character (|). It is similar to the boolean operator OR.

Example: `m(oo|a|e)n` matches the first occurrence of moon, man, or men.

Common regular expressions

Match the PDF content type (MIME type)

`^%PDF-`

Match any valid IP address

`(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)`

Match most email addresses

`[A-Za-z0-9._-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,4}`

About proxy actions

A *proxy action* is a specific group of settings, sources, or destinations for a type of proxy. Because your configuration can include several instances of each proxy, you must link each instance to a specific proxy action. For each proxy, you typically have separate proxy actions for clients and servers. For example, you would use one proxy action for packets sent to a POP3 server protected by the Firebox and a different proxy action to apply to email messages retrieved by POP3 clients.

You can also have more than one proxy action for either clients or servers. For example, you might have one HTTP policy that controls HTTP traffic from a group of users with fewer privileges. This policy has the IP addresses of the less-privileged users' computers in the **From** field. A second HTTP policy controls traffic from a more privileged group, with those users' IP addresses in the **From** field. You assign one HTTP proxy action to the first policy and a different HTTP proxy action to the second policy. The proxy action you assign to the policy for the less privileged users has strict rules, designed to block more URLs and more content than the proxy action you apply to the policy for the more privileged users. You can create many proxy actions and use only some of them at a given time.

You can create more than one proxy action for each type of proxy, but you can assign only one proxy action to each proxy policy. For example, a POP3 proxy icon that appears in the Policy Manager main window is linked to only one proxy action; for example, a POP3-Client action. If you want to create a POP3 proxy for a POP3 server, or an additional policy for POP3 clients, you must add a new POP3 policy to Policy Manager.

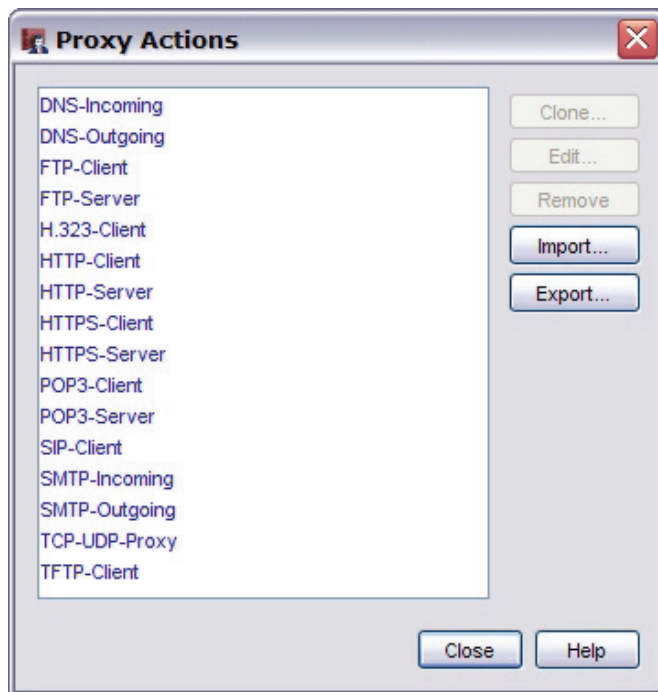
Set the proxy action in a proxy definition

On the **Properties** tab of the **Add/Edit Policy Properties** dialog box, use the **Proxy action** drop-down list to define the proxy action for a proxy policy definition.

Edit, delete, or clone proxy actions

You can also edit, delete, or clone (copy) an existing proxy action definition directly from the Policy Manager window:

1. Select **Tasks > Proxy Actions**.
2. From the **Proxy Actions** dialog box, select the proxy action you want to edit, delete, or clone. Click **Edit**, **Remove**, or **Clone**. You cannot delete predefined proxy actions, which appear in black. You can only delete user-defined proxy actions, which appear in blue.



If you want to edit or clone a proxy action, see the “About” topic for that proxy for more information on proxy action settings:

- [About the DNS proxy](#)
- [About the FTP proxy](#)
- [About the H.323 proxy](#)
- [About the HTTP proxy](#)
- [About the HTTPS proxy](#)
- [About the POP3 proxy](#)
- [About the SIP proxy](#)
- [About the SMTP proxy](#)
- [About the TCP-UDP proxy](#)
- [About the TFTP proxy](#)

Import or export proxy actions

If you manage several Fireboxes and have proxy actions defined for them, you can use the policy import/export function to save time. You can define the proxy actions on one Firebox, export them to an ASCII file, and then import them to another Firebox. For more information, see the procedure for policy templates: [Import and export custom policy templates](#).

About predefined and user-defined proxy actions

The Firebox has predefined client and server proxy actions for each proxy. These predefined actions are configured to balance the accessibility requirements of a typical company with the need to protect your computer assets from attacks. You cannot change the settings of predefined proxy actions. If you want to make changes to the configuration, you must clone (copy) the existing definition and save it as a user-defined proxy action.

For example, if you want to change a setting in the HTTP-Client proxy action, you must save it with a different name, such as HTTP-Client.1. Note that this is necessary only when you make changes to rulesets. If you make changes to general settings such as the allowed sources or destinations or NAT settings for a policy, you do not need to save it under a new name.

Add a proxy policy to your Firebox configuration

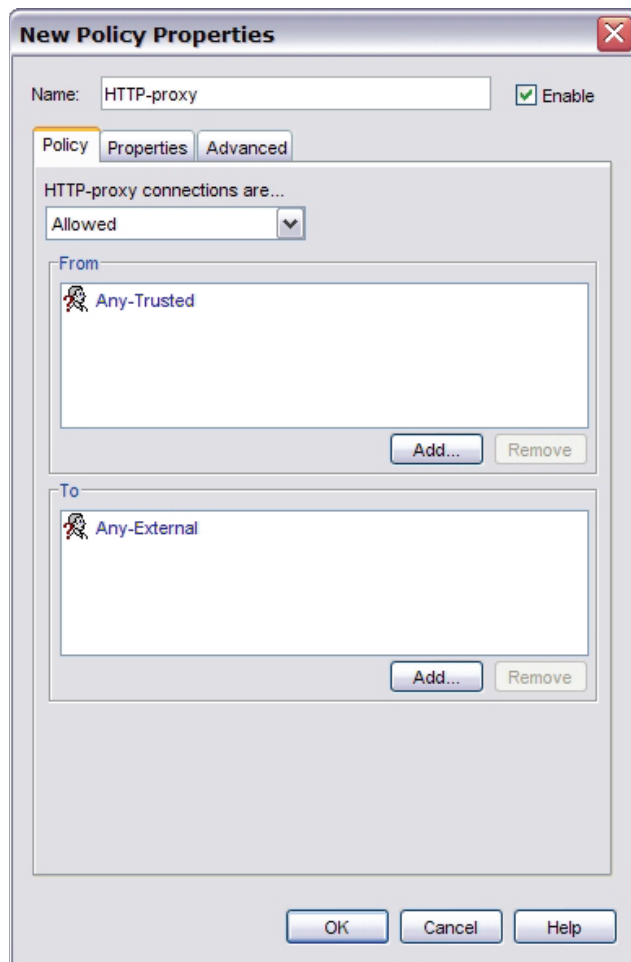
When you add a proxy policy to your Firebox configuration, you specify types of content that the proxy must look for as it filters traffic. If the content matches (or does not match) the criteria you set in the proxy definition, the proxy allows or denies the network traffic.

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.

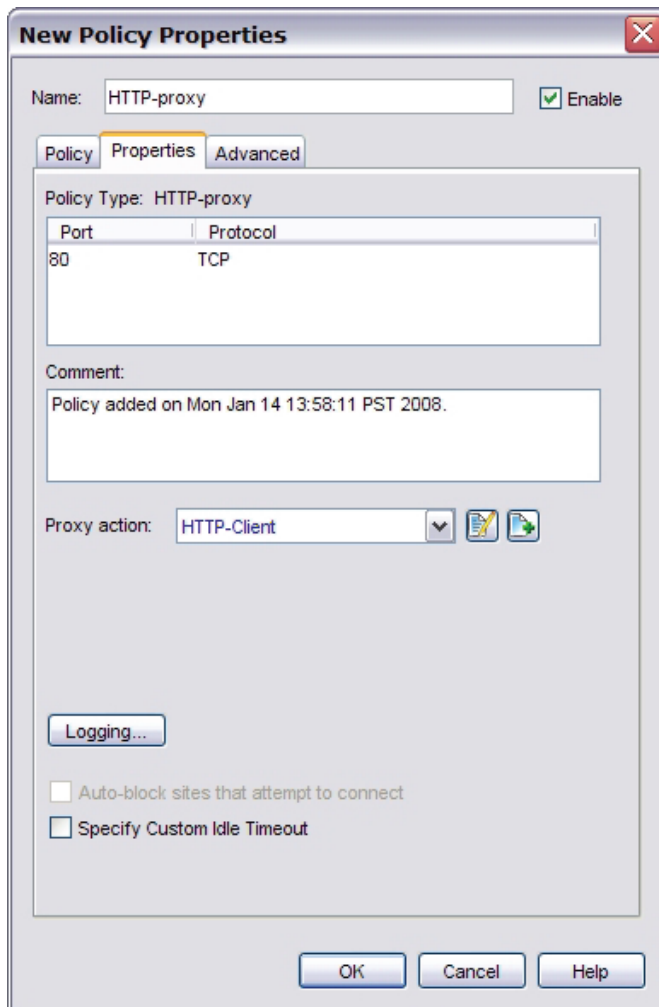
1. In Policy Manager, click the plus (+) sign on the Policy Manager toolbar.
Or select **Edit > Add Policies**.
The Add Policies dialog box appears.
2. Click the plus (+) sign on the left side of the folder to expand the **Proxies** folder.
A list of proxies appears.

3. Click the name of the proxy you want to add. Click **Add**.
The New Policy Properties dialog box appears.



4. If you choose, you can change the name of the proxy policy. To change the name, type a new name in the **Name** text box.

5. Click the **Properties** tab.
The New Policy Properties dialog box appears.



The image shows a Windows-style dialog box titled "New Policy Properties". It has a close button (X) in the top right corner. The dialog is divided into three tabs: "Policy", "Properties" (which is selected and highlighted with an orange border), and "Advanced".

At the top, there is a "Name:" text box containing "HTTP-proxy" and an "Enable" checkbox which is checked.

Below the tabs, the "Policy Type" is set to "HTTP-proxy". Underneath, there is a table with two columns: "Port" and "Protocol". The first row shows "80" in the Port column and "TCP" in the Protocol column.

Below the table is a "Comment:" text box containing the text "Policy added on Mon Jan 14 13:58:11 PST 2008."

Further down is a "Proxy action:" label followed by a dropdown menu showing "HTTP-Client" and two small icons (a document and a plus sign).

Below that is a "Logging..." button.

At the bottom of the main content area are two unchecked checkboxes: "Auto-block sites that attempt to connect" and "Specify Custom Idle Timeout".

At the very bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

To modify the default proxy policy definition to meet your business needs, see [About policy properties](#).

WatchGuard proxies have predefined rulesets that provide a good balance of security and accessibility for most installations. If a default ruleset does not meet all of your business needs, you can add, delete, or modify rules. For more information, see [About rules and rulesets](#).

About the DNS proxy

The Domain Name System (DNS) is a network system of servers that translates numeric IP addresses into readable, hierarchical Internet addresses, and vice versa. DNS allows your computer network to understand, for example, that you want to reach the server at 200.253.208.100 when you type into your browser a domain name such as www.watchguard.com. With Fireware, you have two methods to control DNS traffic through your firewall: the DNS packet filter and the DNS proxy policy. It is important to understand that the DNS proxy settings are useful only if the DNS request is routed through the firewall.

When you make a new configuration file, the file automatically includes an Outgoing packet filter policy that allows all TCP and UDP connections from your trusted and optional networks to external. This allows your users to connect to an external DNS server using the standard TCP 53 and UDP 53 ports. Because Outgoing is a packet filter, it is unable to protect against common UDP outgoing trojans, DNS exploits, and other problems that occur when you open all outgoing UDP traffic from your trusted networks. The DNS-Outgoing proxy action has features to protect your network from these threats. If you use external DNS servers for your network, the DNS-Outgoing ruleset offers additional ways to control the services available to your network community.

To add the DNS proxy to your Firebox configuration, see [Add a proxy to your Firebox configuration](#). Then, if you need to change the proxy definition to meet your business needs, you can use the **New/Edit Policy Properties** dialog box to modify the definition. The fields on this dialog box are divided into three tabs: **Policy**, **Properties**, and **Advanced**. In addition, the **Properties** tab contains an icon for you to configure the [proxy action](#).

Policy tab


- **DNS-proxy connections are:** Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)** and define who appears in the **From** and **To** list (on the **Policy** tab of the proxy definition). See [Set access rules for a policy](#).

Properties tab

- In the **Proxy action** drop-down list, select whether you want to define an action for a client or server. For information about proxy actions, see [About proxy actions](#).
- To define logging for a policy, click **Logging** and [Set logging and notification preferences](#).
- If you set the **DNS-proxy connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use DNS. See [Block sites temporarily with policy settings](#).
- If you want to use an idle timeout other than the one set by the Firebox or authentication server, [Set a custom idle timeout](#).

Proxy action settings

WatchGuard proxies have predefined rulesets that provide a good balance of security and accessibility for most installations. If a default ruleset does not meet all of your business needs, you can add, delete, or modify rules.

To modify the settings and rulesets for a proxy action, click the **View/Edit Proxy** icon  (the first icon to the right of the **Proxy action** drop-down list) and select a category of settings from the left side of the dialog box:

- [DNS proxy: General settings](#)
- [DNS proxy: OPcodes](#)
- [DNS proxy: Query types](#)
- [DNS proxy: Query names](#)
- [DNS proxy: Intrusion prevention](#)
- [Proxy and AV alarms](#). SNMP traps and notification are disabled by default.

Advanced tab

You can use several other options in your proxy definition:

- [Set an operating schedule](#)
- [Apply Traffic Management actions to a policy](#)
- [Set ICMP error handling](#)
- [Apply NAT rules](#) (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- [Enable QoS Marking for a policy](#)
- [Set traffic priority in a policy](#)
- [Add a sticky connection duration to a policy](#)

DNS proxy: General settings

On the **General** page (the page that first appears after you click the View/Edit Proxy icon) you can change the settings of two protocol anomaly detection rules. We recommend that you do not change the default settings.

General

Protocol Anomaly Detection Rules

Not of class Internet:	Deny	<input type="checkbox"/> Alarm	<input checked="" type="checkbox"/> Log
Badly formatted query:	Deny	<input type="checkbox"/> Alarm	<input checked="" type="checkbox"/> Log

☐ Turn on logging for reports

Not of class Internet

Select the action to do when the proxy examines DNS traffic that is not of the Internet (IN) class. The default action is to deny this traffic. We recommend that you do not change this default action.

Badly formatted query

Select the action when the proxy examines DNS traffic that does not use the correct format.

Alarm

An alarm is a mechanism to tell users when a proxy rule applies to network traffic. Select the **Alarm** check box to configure an alarm for this event. To set the options for the alarm, select **Proxy Alarm** from the **Categories** list on the left side of a Proxy Configuration window. You can send an SNMP trap, send email, or open a pop-up window.

Log

Select this check box to write a message to the traffic log for this event.

Turn on logging for reports

Creates a traffic log message for each transaction. This option creates a large log file, but this information is very important if your firewall is attacked. If you do not select this check box, you do not see detailed information about DNS proxied connections in reports.

If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#)). Enter a name for the new action and click **OK**.

DNS proxy: OPcodes

DNS OPcodes (operation codes) are commands given to the DNS server that tell it to do some action, such as a query (Query), an inverse query (IQuery), or a server status request (STATUS). They operate on items such as registers, values in memory, values stored on the stack, I/O ports, and the bus. If the default ruleset does not meet all of your business needs, you can add, delete, or modify rules. You can allow, deny, drop, or block specified DNS OPcodes.

1. From the **Categories** section, select **OPcodes**.
2. For the rules listed, select the **Enabled** check box to enable a rule. Clear the **Enabled** check box to disable a rule.



If you use Active Directory and your Active Directory configuration requires dynamic updates, you must allow DNS OPcodes in your DNS-Incoming proxy action rules. This is a security risk, but can be necessary for Active Directory to operate correctly.

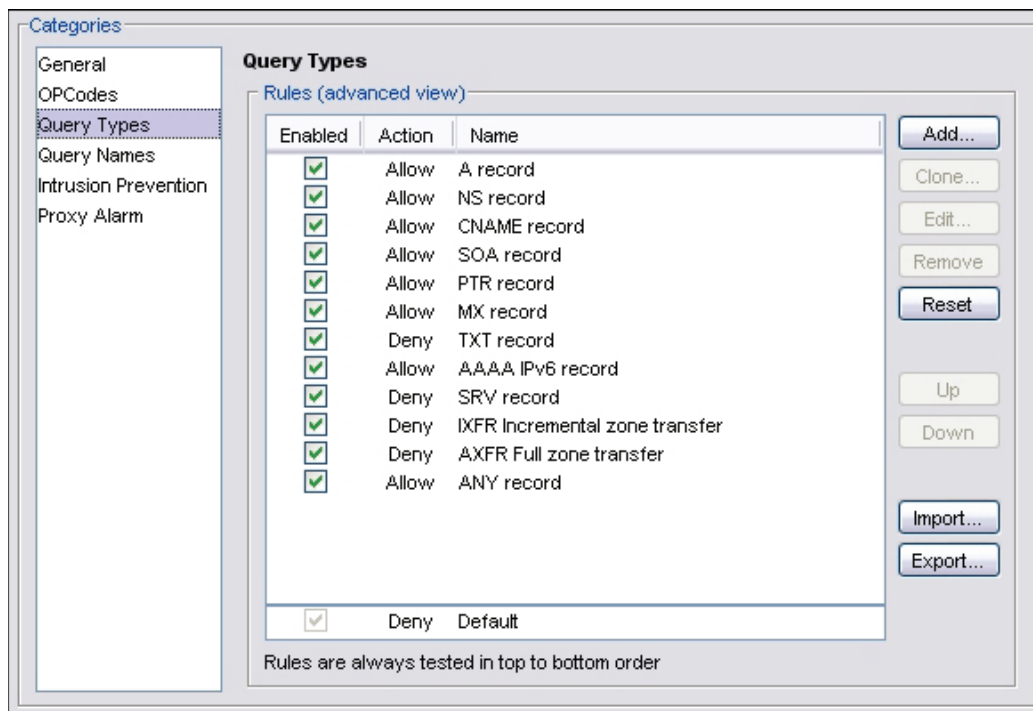
Adding a new OPcodes rule

1. Click **Add**.
The New OPcodes Rule dialog box appears.
2. Type a name for the rule.
Rules can have no more than 31 characters.
3. DNS OPcodes have an integer value. Use the arrows to set the OPCode value.
For more information on the integer values of DNS OPcodes, see RFC 1035.
4. Add, delete, or modify rules, as described in [About working with rules and rulesets](#).
5. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.
or
If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.
The New Policy Properties dialog box appears.

DNS proxy: Query types

A DNS query type can configure a resource record by type (such as a CNAME or TXT record) or as a custom type of query operation (such as an AXFR Full zone transfer). If the default Query Type ruleset does not meet all of your business needs, you can add, delete, or modify rules. You can allow, deny, drop, or block specified DNS query types.

1. From the **Categories** section, select **Query Types**.



2. To enable a rule, select the **Enabled** check box adjacent to the action and name of the rule.

Add a new query types rule

1. To add a new query types rule, click **Add**.
The New Query Types Rule dialog box appears.
2. Type a name for the rule.
Rules can have no more than 31 characters.
3. DNS query types have a resource record (RR) value. Use the arrows to set the value.
For more information on the values of DNS query types, see RFC 1035.
4. Add, delete, or modify rules, as described in [About rules and rulesets](#).
5. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.
or
If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.
The New Policy Properties dialog box appears.

DNS proxy: Query names

A DNS query name refers to a specified DNS domain name, shown as a fully qualified domain name (FQDN). If the default Query Name ruleset does not meet all of your business needs, you can add, delete, or modify rules.

1. From the **Categories** section, select **Query Names**.

2. To add more names, or to delete or modify them, see [About working with rules and rulesets](#).
3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

Intrusion prevention in proxy definitions

An *intrusion* is a direct attack on your computer. These attacks can cause damage to your network, get sensitive information, or use your computers to attack other networks.


To help protect your network from intrusions, you can purchase the optional Intrusion Prevention Service (IPS) for the Firebox. Intrusion Prevention Service operates with the SMTP, POP3, HTTP, FTP, DNS, and TCP-UDP proxies.

You can activate and configure IPS in two ways:

Run the Activate Intrusion Prevention wizard from the Tasks menu in Policy Manager

For more information, see [Activate Intrusion Prevention Service \(IPS\)](#).

Use the Intrusion Prevention ruleset in the proxy definition

1. [Get a feature key](#) for IPS from LiveSecurity Service and [add the feature key to the Firebox](#).
2. [Add a proxy policy to your Firebox configuration](#). Or, you can edit an existing proxy.
3. From the **Properties** tab of the **New/Edit Policy Properties** dialog box, click the **View/Edit Proxy** icon  (the first icon to the right of the **Proxy action** drop-down list).
4. Select the **Intrusion Prevention** category from the left side of the window. On the right side of the window, [set parameters for Intrusion Prevention Service \(IPS\)](#).

Proxy and AV alarms

An alarm is an event that triggers a *notification*, which is a mechanism to tell a network administrator about a condition in the network. In a proxy definition, an alarm might occur when traffic matches, or does not match, a rule in the proxy, and the **If matched** or **None matched** field under **Actions to take** in the ruleset definitions is set to an action other than **Allow**.

For example, the default definition of the FTP proxy has a rule that denies the download of files whose file types match any of these patterns: .cab, .com, .dll, .exe, and .zip. You can specify that an alarm is generated whenever the Firebox takes the **Deny** action because of this rule.

For each proxy, you can define what the Firebox does when an alarm occurs.

1. From the **Categories** section of the proxy definition, select **Proxy and AV Alarm**.
2. You can define the Firebox to send an SNMP trap, a notification to a network administrator, or both. The notification can either be an email to a network administrator or a pop-up window on the administrator's management station.
For more information on the Proxy and AV alarm fields, see [Set logging and notification preferences](#).
3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

Finish and save the configuration

1. When you are done with all changes for all categories of the proxy, click **OK** to close the **New Policy Properties** or **Edit Policy Properties** dialog box.
2. Save the configuration to the Firebox. To do this, select **File > Save > To Firebox**.
The Save dialog box appears with the default location for configuration files. You can change the name of the configuration file if you choose.
3. Click **Save**.
4. You are prompted for the configuration passphrase. Type it and click **OK**.

About MX (Mail eXchange) records

An MX (Mail eXchange) record is a type of DNS record that gives one or more host names of the email servers that are responsible for and authorized to receive email for a given domain. If the MX record has more than one host name, each name has a number that tells which is the most preferred host and which hosts to try next if the most preferred host is not available.

MX lookup

When an email server sends email, it first does a DNS query for the MX record of the recipient's domain. When it gets the response, the sending email server knows the host names of authorized mail exchangers for the recipient's domain. To get the IP addresses associated with the MX host names, a mail server does a second DNS lookup for the A record of the host name. The response gives the IP address associated with the host name. This lets the sending server know what IP address to connect to for message delivery.

Reverse MX lookup

Many anti-spam solutions, including those used by most major ISP networks and web mail providers such as AOL, MSN, and Yahoo!, use a reverse MX lookup procedure. Different variations of the reverse lookup are used, but the goals are the same: the receiving server wants to verify that the email it receives does not come from a spoofed or forged sending address, and that the sending server is an authorized mail exchanger for that domain.

To verify that the sending server is an authorized email server, the receiving email server tries to find an MX record that correlates to the sender's domain. If it cannot find one, it assumes that the email is spam and rejects it.

The domain name that the receiving server looks up can be any of these:

- Domain name in the email message's **From:** header
- Domain name in the email message's **Reply-To:** header
- Domain name the sending server uses as the FROM parameter of the MAIL command. (An SMTP command is different from an email header. The sending server sends the MAIL FROM: command to tell the receiving sender who the message is from.)
- Domain name returned from a DNS query of the connection's source IP address. The receiving server sometimes does a lookup for a PTR record associated with the IP address. A PTR DNS record is a record that maps an IP address to a domain name (instead of a normal A record, which maps a domain name to an IP address).

Before the receiving server continues the transaction, it makes a DNS query to see whether a valid MX record for the sender's domain exists. If the domain has no valid DNS MX record, then the sender is not valid and the receiving server rejects it as a spam source.

MX records and multi-WAN

Because outgoing connections from behind your Firebox can show different source IP addresses when your Firebox uses multi-WAN, you must make sure that your DNS records include MX records for each external IP address that can show as the source when you send email. If the list of host names in your domain's MX record does not include one for each external Firebox interface, it is possible that some remote email servers could drop your email messages.

For example, Company XYZ has a Firebox configured with multiple external interfaces. The Firebox uses the Failover multi-WAN method. Company XYZ's MX record includes only one host name. This host name has a DNS A record that resolves to the IP address of the Firebox's primary external interface.

When Company XYZ sends an email to test@yahoo.com, the email goes out through the primary external interface. The email request is received by one of Yahoo's many email servers. That email server does a reverse MX lookup to verify the identify of Company XYZ. The reverse MX lookup is successful, and the email is sent.

If a WAN failover event occurs at the Firebox, all outgoing connections from Company XYZ start to go out the secondary, backup external interface. In this case, when the Yahoo email server does a reverse MX lookup, it does not find an IP address in Company XYZ's MX and A records that matches, and it rejects the email. To solve this problem, make sure that:

- The MX record has multiple host names, at least one for each external Firebox interface.
- At least one host name in the MX record has a DNS A record that maps to the IP address assigned to each Firebox interface.

Add another host name to an MX record

MX records are stored as part of your domain's DNS records. For more information on setting up your MX records, contact your DNS host provider (if someone else hosts your domain's DNS service) or consult the documentation from the vendor of your DNS server software.

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 TCP/UDP proxy is available for protocols on non-standard ports. When FTP uses a port other than port 20, the TCP/UDP proxy relays the traffic to the FTP proxy. For information on the TCP/UDP proxy, see [About the TCP/UDP proxy](#).

To add the FTP proxy to your Firebox configuration, see [Add a proxy to your Firebox configuration](#). Then, if you need to change the proxy definition to meet your business needs, you can use the **New/Edit Policy Properties** dialog box to modify the definition. The fields on this dialog box are divided into three tabs: **Policy**, **Properties**, and **Advanced**. In addition, the **Properties** tab contains an icon for you to configure the [proxy action](#).

Policy tab


- **FTP-proxy connections are:** Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)** and define who appears in the **From** and **To** list (on the **Policy** tab of the proxy definition). See [Set access rules for a policy](#).
- **Use policy-based routing:** If you want to use policy-based routing in your proxy definition, see [Configure policy-based routing](#).

Properties tab

- In the **Proxy action** drop-down list, select whether you want to define an action for a client or server. For information about proxy actions, see [About proxy actions](#).
- To define logging for a policy, click **Logging** and [Set logging and notification preferences](#).
- If you set the **FTP-proxy connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use FTP. See [Block sites temporarily with policy settings](#).
- If you want to use an idle timeout other than the one set by the Firebox or authentication server, [Set a custom idle timeout](#).

Proxy action settings

WatchGuard proxies have predefined rulesets that provide a good balance of security and accessibility for most installations. If a default ruleset does not meet all of your business needs, you can add, delete, or modify rules.

To modify the settings and rulesets for a proxy action, click the **View/Edit Proxy** icon  (the first icon to the right of the **Proxy action** drop-down list) and select a category of settings from the left side of the dialog box:

- [FTP proxy: General settings](#)
- [FTP proxy: Commands](#). The default setting for the FTP-client proxy is to allow all commands. The default FTP-server proxy allows these commands:

ABOR*	HELP*	PASS*	REST*	STAT*	USER*
APPE*	LIST*	PASV*	RETR*	STOR*	XCUP*
CDUP*	MKD*	PORT*	RMD*	STOU*	XCWD*
CWD*	NLST*	PWD*	RNFR*	SYST*	XMKD*
DELE*	NOOP*	QUIT*	RNT0*	TYPE*	XRMD*
- [FTP proxy: Upload and download content](#). The default settings for the FTP-client proxy is to deny these files from being downloaded: .cab, .com., .dll, .exe., .zip. The FTP-server proxy allows all files. Both the client and server proxies allow all files to be uploaded.
- [FTP proxy: Antivirus responses](#). When Gateway AV is enabled for the FTP proxy, the default settings are to drop connections when a virus is detected or when a scan error occurs.
- [FTP proxy: Intrusion Protection](#). When Intrusion Prevention is enabled for the FTP proxy, the default setting is to deny traffic that matches an IPS signature.
- [Proxy and AV alarm](#). SNMP traps and notification are disabled by default.

Advanced tab

You can use several other options in your proxy definition:

- [Set an operating schedule](#)
- [Apply Traffic Management actions to a policy](#)
- [Set ICMP error handling](#)
- [Apply NAT rules](#) (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- [Enable QoS Marking for a policy](#)
- [Set traffic priority in a policy](#)
- [Add a sticky connection duration to a policy](#)

FTP proxy: General settings

On the **General** page (the page that first appears after you click the View/Edit Proxy icon), you can set basic FTP parameters including maximum user name length.

1. From the **Categories** section, select **General**.

FTP Proxy Action Configuration (predefined)

Name:

Description:

Categories

- General
- Commands
- Download
- Upload
- Antivirus
- Intrusion Prevention
- Proxy and AV Alarm

General

Limits

If any FTP connection parameter is greater than the values set below, the Firebox denies the connection.

<input checked="" type="checkbox"/> Set the maximum user name length to	<input type="text" value="64"/>	bytes	<input type="checkbox"/> Auto-block
<input checked="" type="checkbox"/> Set the maximum password length to	<input type="text" value="32"/>	bytes	<input type="checkbox"/> Auto-block
<input checked="" type="checkbox"/> Set the maximum file name length to	<input type="text" value="1024"/>	bytes	<input type="checkbox"/> Auto-block
<input checked="" type="checkbox"/> Set the maximum command line length to	<input type="text" value="1030"/>	bytes	<input type="checkbox"/> Auto-block
<input checked="" type="checkbox"/> Set the maximum number of failed logins per connection to	<input type="text" value="6"/>		<input type="checkbox"/> Auto-block

☐ Turn on logging for reports

OK Cancel Help

2. To set limits for FTP parameters, select the applicable check boxes. These settings help to protect your network from buffer overflow attacks. Use the arrows to change the limits:

Set the maximum user name length to

Sets a maximum length for user names on FTP sites.

Set the maximum password length to

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

Set the maximum file name length to

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

Set the maximum command line length to

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

Set the maximum number of failed logins per connection to

Allows you to limit the number of failed connection requests to your FTP site. This can protect your site against brute force attacks.

- For each setting, you can set or clear the **Auto-block** check box next to it. If someone tries to connect to an FTP site and exceeds a limit whose **Auto-block** check box is selected, the computer that sent the commands is added to the temporary Blocked Sites list.
- To create a log message for each transaction, select the **Turn on logging for reports** check box. You must select this option to get detailed reports on FTP traffic with WatchGuard Reports.
- If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

FTP proxy: Commands

FTP has a number of commands to manage files. You can configure rules to put limits on some FTP commands.

Use the FTP-Server proxy action to put limits on commands that can be used on an FTP server protected by the Firebox. The default configuration of the FTP-Server proxy blocks these commands:

ABOR*	HELP*	PASS*	REST*	STAT*	USER*
APPE*	LIST*	PASV*	RETR*	STOR*	XCUP*
CDUP*	MKD*	PORT*	RMD*	STOU*	XCWD*
CWD*	NLST*	PWD*	RNFR*	SYST*	XMKD*
DELE*	NOOP*	QUIT*	RNT0*	TYPE*	XRMD*

Use the FTP-Client proxy action to put limits on commands that users protected by the Firebox can use when they connect to external FTP servers. The default configuration of the FTP-Client is to allow all FTP commands.

If the default ruleset does not meet all of your business needs, you can add, delete, or modify rules. You usually should not block these commands, because they are necessary for the FTP protocol to work correctly.

Protocol command	Client Command	Description
USER	n/a	Sent with login name
PASS	n/a	Sent with password
PASV	pasv	Select passive mode for data transfer
SYST	syst	Print the server's operating system and version. FTP clients use this information to correctly interpret and show a display of server responses.

- From the **Categories** section, select **Commands**.
- Add, delete, or modify rules, as described in [About rules and rulesets](#).
- If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

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.

Use the FTP-Server proxy action to control rules for an FTP server protected by the Firebox. Use the FTP-Client proxy action to set rules for users connecting to external FTP servers.

1. From the **Categories** section, select **Upload** or **Download**.
2. Add, delete, or modify rules, as described in [About rules or rulesets](#).
3. If you want uploaded files to be scanned for viruses by Gateway AntiVirus, set one or more **Actions to take** fields to **AV Scan**.
4. If you want to change settings for one or more other categories in this proxy, go to the topics on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

Configure Gateway AntiVirus actions

When you enable Gateway AntiVirus, you must set the actions to be taken if a virus or error is found in an email message (SMTP or POP3 proxies), web page (HTTP proxy), or uploaded or downloaded file (FTP proxy). The options for antivirus actions are:

Allow

Allows the packet to go to the recipient, even if the content contains a virus.

Deny (FTP proxy only)

Deny the file and send a deny message.

Lock (SMTP and POP3 proxies only)

Locks the attachment. This is a good option for files that cannot be scanned by the Firebox. A file that is locked cannot be opened easily by the user. Only the administrator can unlock the file. The administrator can use a different antivirus tool to scan the file and examine the content of the attachment. For information on how to unlock a file locked by Gateway AntiVirus, see [Unlock a file locked by Gateway AntiVirus](#).

Quarantine (SMTP proxy only)

When you use the SMTP proxy with the spamBlocker security subscription, you can send email messages with viruses or possible viruses to the Quarantine Server. For more information on the Quarantine Server, see [About the Quarantine Server](#). For information on how to set up Gateway AntiVirus to work with the Quarantine Server, see [Configure Gateway AntiVirus to quarantine email](#).

Remove (SMTP and POP3 proxies only)

Removes the attachment and allows the message through to the recipient.

Drop (not supported in POP3 proxy)

Drops the packet and drops the connection. No information is sent to the source of the message.

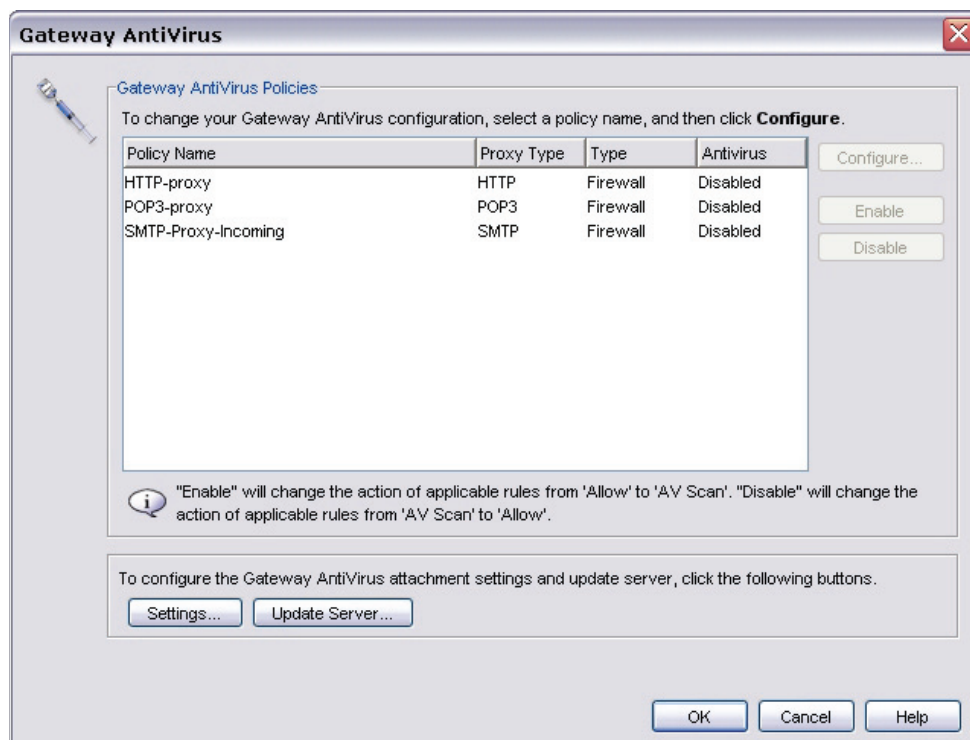
Block (not supported in POP3 proxy)

Blocks the packet, and adds the IP address of the sender to the Blocked Sites list.

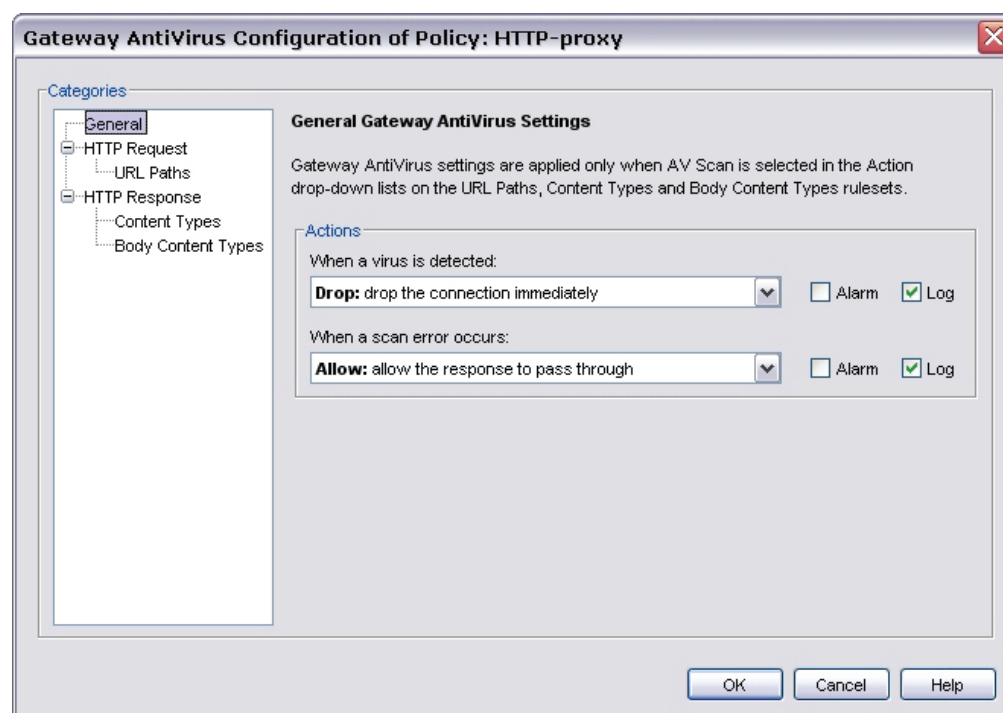


If you set the configuration to allow attachments, your configuration is less secure.

1. From Policy Manager, select **Tasks > Gateway AntiVirus > Configure**.
The Gateway AntiVirus dialog box appears, which lists the proxies that have already been created.



2. Select the policy you want to configure and click **Configure**.
The General Gateway Antivirus Settings page for that policy appears.
Or, instead of step 1 and 2, you can go to the same page from the proxy definition screens. From the **Categories** section in the proxy definition, select **AntiVirus**.



3. Set the action the Firebox takes if a virus is detected in an email message, file, or web page, in the **When a virus is detected** drop-down list. See the beginning of this section for a description of the proxy actions.
4. Set the action the Firebox takes when it cannot scan an object or an attachment in the **When a scan error occurs** drop-down list. Attachments that cannot be scanned include binhex-encoded messages, certain encrypted files, or files that use a type of compression that we do not support such as password-protected Zip files. See the beginning of this section for a description of the proxy actions.
5. (FTP proxy only) You can limit file scanning up to a specified kilobyte count. Any additional bytes in the file are not scanned. This allows the proxy to partially scan very large files without a large effect on performance. Enter the limit in the **Limit scanning to first** field.

Create alarms or log entries for antivirus actions

An alarm is a mechanism to tell users when a proxy rule applies to network traffic. Use the **Alarm** check box on the AntiVirus page of a proxy definition to create an alarm when the adjacent action occurs. If you do not want an alarm for the antivirus action, clear the **Alarm** check box for that action.

FTP Proxy Action Configuration (predefined)

Name:

Description:

Categories

- General
- Commands
- Download
- Upload
- Antivirus**
- Intrusion Prevention
- Proxy and AV Alarm

Antivirus

Gateway AntiVirus settings are applied only when the Action drop-down lists on the 'Upload' and 'Download' rulesets is set to 'AV Scan'.

Actions

When virus is detected:

Drop: drop the connection immediately ☐ Alarm ☒ Log

When a scan error occurs:

Drop: drop the connection immediately ☐ Alarm ☒ Log

File Scan

Use this setting to limit the number of bytes to scan at the start of each file. The Firebox does not scan data past this limit. This allows large files to pass with partial scanning.

☐ Limit scanning to first kilobyte(s)

To use the alarm feature successfully, you must also configure the type of alarm to use in each proxy policy. To configure the alarm type to use, use the Proxy and AV Alarms category for the proxy. For information about the settings for this category, see [Set logging and notification preferences](#).

If you want to record log messages for a proxy action, select the **Log** check box for the antivirus response. If you do not want to record log messages for an antivirus response, clear the **Log** check box.

Intrusion prevention in proxy definitions

An *intrusion* is a direct attack on your computer. These attacks can cause damage to your network, get sensitive information, or use your computers to attack other networks.


To help protect your network from intrusions, you can purchase the optional Intrusion Prevention Service (IPS) for the Firebox. Intrusion Prevention Service operates with the SMTP, POP3, HTTP, FTP, DNS, and TCP-UDP proxies.

You can activate and configure IPS in two ways:

Run the Activate Intrusion Prevention wizard from the Tasks menu in Policy Manager

For more information, see [Activate Intrusion Prevention Service \(IPS\)](#).

Use the Intrusion Prevention ruleset in the proxy definition

1. [Get a feature key](#) for IPS from LiveSecurity Service and [add the feature key to the Firebox](#).
2. [Add a proxy policy to your Firebox configuration](#). Or, you can edit an existing proxy.
3. From the **Properties** tab of the **New/Edit Policy Properties** dialog box, click the **View/Edit Proxy** icon  (the first icon to the right of the **Proxy action** drop-down list).
4. Select the **Intrusion Prevention** category from the left side of the window. On the right side of the window, [set parameters for Intrusion Prevention Service \(IPS\)](#).

Proxy and AV alarms

An alarm is an event that triggers a *notification*, which is a mechanism to tell a network administrator about a condition in the network. In a proxy definition, an alarm might occur when traffic matches, or does not match, a rule in the proxy, and the **If matched** or **None matched** field under **Actions to take** in the ruleset definitions is set to an action other than **Allow**.

For example, the default definition of the FTP proxy has a rule that denies the download of files whose file types match any of these patterns: .cab, .com, .dll, .exe, and .zip. You can specify that an alarm is generated whenever the Firebox takes the **Deny** action because of this rule.

For each proxy, you can define what the Firebox does when an alarm occurs.

1. From the **Categories** section of the proxy definition, select **Proxy and AV Alarm**.
2. You can define the Firebox to send an SNMP trap, a notification to a network administrator, or both. The notification can either be an email to a network administrator or a pop-up window on the administrator's management station.
For more information on the Proxy and AV alarm fields, see [Set logging and notification preferences](#).
3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.
or
If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.
The New Policy Properties dialog box appears.

Finish and save the configuration

1. When you are done with all changes for all categories of the proxy, click **OK** to close the **New Policy Properties** or **Edit Policy Properties** dialog box.
2. Save the configuration to the Firebox. To do this, select **File > Save > To Firebox**.
The Save dialog box appears with the default location for configuration files. You can change the name of the configuration file if you choose.
3. Click **Save**.
4. You are prompted for the configuration passphrase. Type it and click **OK**.

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 add the H.323 proxy to your Firebox configuration, see [Add a proxy to your Firebox configuration](#).

Configure the H.323 proxy action settings

The H.323 proxy has one ruleset, General, which has one setting:

Turn on logging for reports: Creates a traffic log message for each transaction. Logging for reports is enabled by default. This option may create a large log file, but this information is very important if your firewall is attacked. If you clear this check box, you do not see detailed information about H.323 proxied connections in WatchGuard Reports.

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.

The TCP/UDP proxy is available for protocols on non-standard ports. When HTTP uses a port other than port 80, the TCP/UDP proxy relays the traffic to the HTTP proxy. For information on the TCP/UDP proxy, see [About the TCP/UDP proxy](#).

To add the HTTP proxy to your Firebox configuration, see [Add a proxy to your Firebox configuration](#). Then, if you need to change the proxy definition to meet your business needs, you can use the **New/Edit Policy Properties** dialog box to modify the definition. The fields on this dialog box are divided into three tabs: **Policy**, **Properties**, and **Advanced**. In addition, the **Properties** tab contains an icon for you to configure the [proxy action](#).

HTTP and WebBlocker

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

Policy tab


- **HTTP-proxy connections are:** Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)** and define who appears in the **From** and **To** list (on the **Policy** tab of the proxy definition). See [Set access rules for a policy](#).
- **Use policy-based routing:** If you want to use policy-based routing in your proxy definition, see [Configure policy-based routing](#).

Properties tab

- In the **Proxy action** drop-down list, select whether you want to define an action for a client or server. For information about proxy actions, see [About proxy actions](#).
- To define logging for a policy, click **Logging** and [Set logging and notification preferences](#).
- If you set the **HTTP-proxy connections are** drop-down list (on the **Policy** tab) to Denied or Denied (send reset), you can block sites that try to use HTTP. See [Block sites temporarily with policy settings](#).
- If you want to use an idle timeout other than the one set by the Firebox or authentication server, [Set a custom idle timeout](#).

Proxy action settings

WatchGuard proxies have predefined rulesets that provide a good balance of security and accessibility for most installations. If a default ruleset does not meet all of your business needs, you can add, delete, or modify rules.

To modify the settings and rulesets for a proxy action, click the **View/Edit Proxy** icon  (the first icon to the right of the **Proxy action** drop-down list) and select a category of settings from the left side of the dialog box:

- [HTTP requests: General settings](#)
- [HTTP requests: Request methods](#)
- [HTTP requests: URL paths](#)
- [HTTP requests: Header fields](#)
- [HTTP requests: Authorization](#)
- [HTTP responses: General settings](#)
- [HTTP responses: Header fields](#)
- [HTTP responses: Content types](#)
- [HTTP responses: Cookies](#)
- [HTTP responses: Body content types](#)
- [HTTP proxy: Exceptions](#)
- [HTTP proxy: Antivirus responses](#)
- [HTTP proxy: Deny message](#)
- [HTTP proxy: Intrusion prevention](#)
- [Proxy and AV alarms](#)

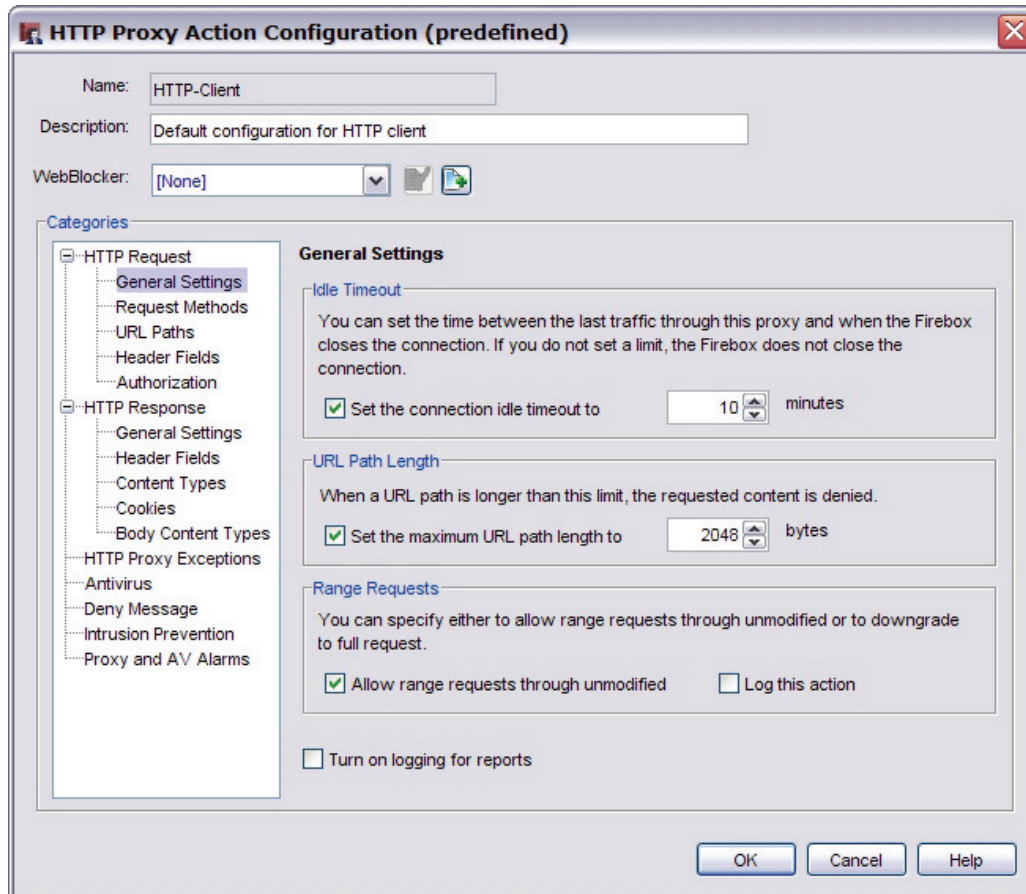
Advanced tab

You can use several other options in your proxy definition:

- [Set an operating schedule](#)
- [Apply Traffic Management actions to a policy](#)
- [Set ICMP error handling](#)
- [Apply NAT rules](#) (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- [Enable QoS Marking for a policy](#)
- [Set traffic priority in a policy](#)
- [Add a sticky connection duration to a policy](#)

HTTP requests: General settings

On the **General Settings** page (the page that first appears after you click the View/Edit Proxy icon), you can set basic HTTP parameters such as idle time out and URL length.



Set the connection idle timeout to

This setting closes the TCP socket used for an HTTP session after the specified amount of time has passed since the last packet that used the TCP socket. Because every open TCP session uses a small amount of memory on the Firebox, and because browsers and servers do not always close HTTP sessions cleanly, this option is used to control performance. In the adjacent field, enter the number of minutes before the proxy times out.

We recommend that you keep this check box selected to make sure that stale TCP connections are closed. This helps the Firebox save memory. You can lower the timeout to five minutes without problems.

Set the maximum URL path length to

Sets the maximum number of characters allowed in a URL. In this area of the proxy, URL includes anything in the web address after the top-level-domain, including the slash character, but not including the host name (the `www.mywatchguard.com` or the `mywatchguard.com` part of the web address). For example, the URL `www.mywatchguard.com/products` counts nine characters toward this limit because `/products` has nine characters. The default value of 2048 is usually enough for any URL requested by a computer behind your Firebox. A URL that is very long can indicate an attempt to compromise a web server.

We recommend that you leave this setting enabled with the default settings. This helps protect against infected web clients on the networks protected by the HTTP proxy.

Allow range requests through unmodified

Select to allow range requests through the Firebox. Range requests allow a client to request subsets of the bytes in a web resource instead of the full content. For example, if you want only some sections of a large Adobe file but not the whole file, the download occurs more quickly and prevents the download of unnecessary pages if you can request only what you need.

Range requests introduce security risks. Malicious content can hide anywhere in a file and a range request makes it possible for any content to be split across range boundaries. The proxy can fail to see a pattern it is looking for when the file spans two GET operations. If you have a subscription for Gateway AntiVirus (Gateway AV) or the signature-based Intrusion Prevention System (IPS), and you enable either of those security services, Fireware denies range requests regardless of whether this check box is selected.

We recommend that you keep this check box cleared if the rules you make in the Body Content Types section of the proxy are designed to identify byte signatures deep in a file instead of just in the file header.

Select **Log this action** if you want to add a traffic log message when the proxy takes the action indicated in the check box for range requests.

Turn on logging for reports

Creates a traffic log message for each transaction. This option creates a large log file, but this information is very important if your firewall is attacked. If you do not select this check box, you do not see detailed information about HTTP proxied connections in reports.

If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

HTTP requests: Request methods

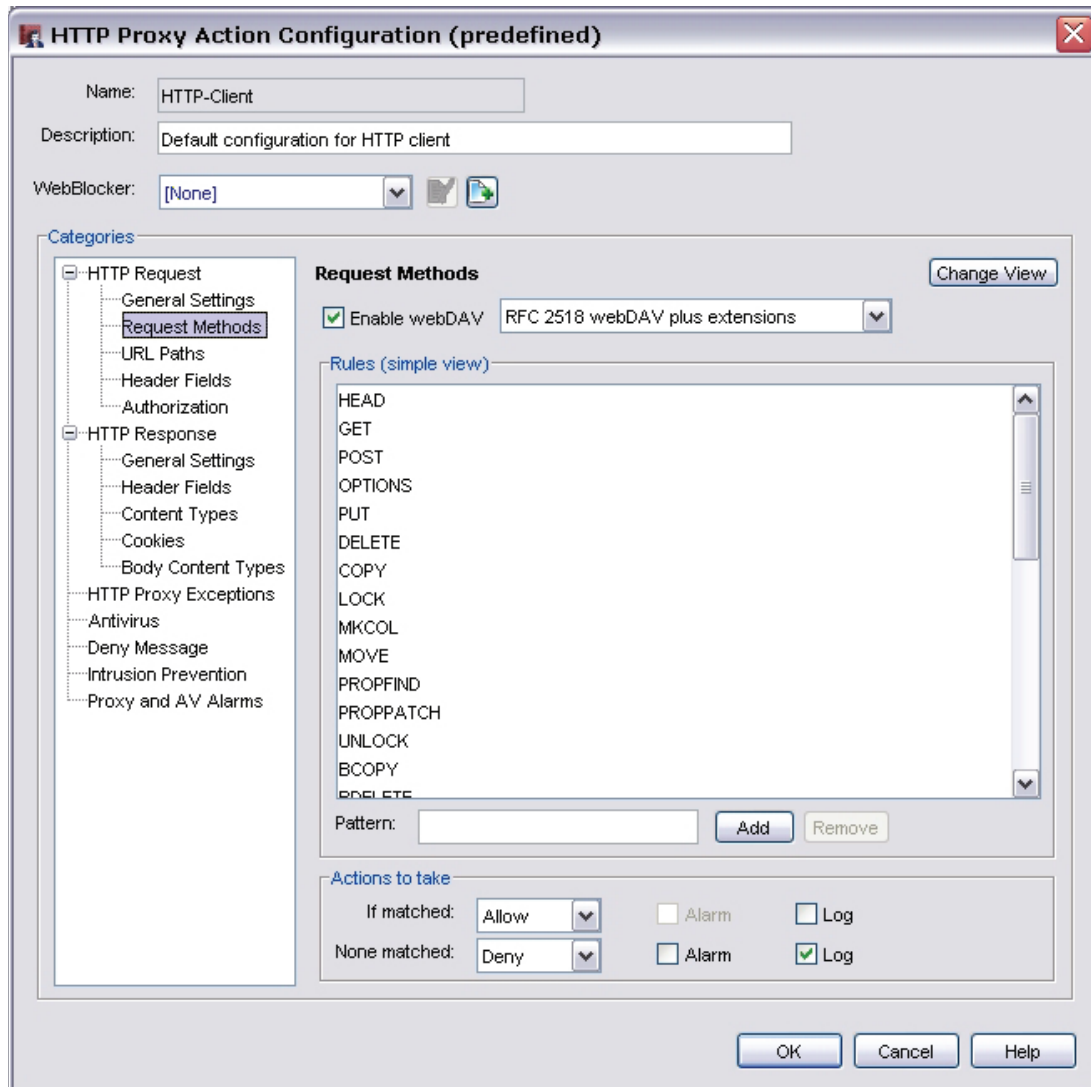
Most browser HTTP requests are in one of two categories: GET and POST operations. Browsers usually use GET operations to download objects such as a graphic, HTML data, or Flash data. More than one GET is usually sent by a client computer for each page, because web pages usually contain many different elements. The elements are put together to make a page that appears as one page to the end user.

Browsers usually use POST operations to send data to a web site. Many web pages get information from the end user such as location, email address, and name. If you disable the POST command, the Firebox denies all POST operations to web servers on the external network. This feature can prevent your users from sending information to a web site on the external network.

If webDAV extensions (described below) are not enabled, the HTTP proxy supports request methods: HEAD, GET, POST, OPTIONS, PUT, and DELETE. For HTTP-Server, the proxy supports these request methods by default: HEAD, GET, and POST. OPTIONS, PUT, and DELETE are added but are disabled by default.

1. From the **Categories** section, select **Request Methods**.
2. Web-based Distributed Authoring and Versioning (webDAV) is a set of HTTP extensions that allows users to edit and manage files on remote web servers. WebDAV is compatible with Outlook Web Access (OWA). Select the **Enable webDAV** check box if you want to allow your users to use these extension.

Many extensions to the base webDAV protocol are also available. If you enable webDAV, from the adjacent check box, select whether you want to enable only the extensions described in RFC 2518 or if you want to include an additional set of extensions to maximize interoperability.



3. Add, delete, or modify rules, as described in [About working with rules and rulesets](#).
4. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

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`



Usually, if you filter URLs with the HTTP request URL path ruleset, you must configure a complex pattern that uses full regular expression syntax from the advanced view of a ruleset. It is easier and gives better results to filter based on header or body content type than it is to filter by URL path.

1. From the **Categories** section, select **URL paths**.
2. Add, delete, or modify rules, as described in [About working with rules and rulesets](#).
3. If you want to change settings for one or more other categories in this proxy, go to the topic on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#). Enter a name for the new action and click **OK**.

HTTP requests: Header fields

This ruleset supplies content filtering for the full HTTP header. By default, the HTTP proxy uses exact matching rules to strip `Via` and `From` headers, and allows all other headers. This ruleset matches against the full header, not only the name. Thus, to match all values of a header, type the pattern: `[header name]:*`. To match only some values of a header, replace the asterisk (*) wildcard with a pattern. If your pattern does not start with an asterisk (*) wildcard, include one space between the colon and the pattern when typing in the **Pattern** text box. For example, type: `[header name]: [pattern]` and not `[header name]:[pattern]`.

Note that the default rules do not strip the `Referer` header, but do include a disabled rule to strip this header. To enable the rule, select **Change View**. Some web browsers and software applications must use the `Referer` header to operate correctly.

1. From the **Categories** section, select **Header Fields**.
2. Add, delete, or modify rules, as described in [About working with rules and rulesets](#).
3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

HTTP requests: Authorization

This rule sets the criteria for content filtering of HTTP Request Header authorization fields. When a web server starts a WWW-Authenticate challenge, it sends information about which authentication methods it can use. The proxy puts limits on the type of authentication sent in a request. It uses only the authentication methods that the web server accepts. With a default configuration, the Firebox allows Basic, Digest, NTLM, and Passport1.4 authentication, and strips all other authentication. If the default ruleset does not meet all of your business needs, you can add, delete, or modify rules:

1. From the **Categories** section, select **Authorization**.
2. Add, delete, or modify rules, as described in [About working with rules and rulesets](#).
3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. For more information on predefined user actions, see [About predefined and user-defined proxy actions](#). Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

HTTP responses: General settings

You use the General Settings fields to configure basic HTTP parameters such as idle time out and limits for line and total length.

1. From the **Categories** section, select **General Settings**.
2. To set limits for HTTP parameters, select the applicable check boxes. Use the arrows to set the limits:

Set the timeout to

Controls how long the Firebox HTTP proxy waits for the web server to send the web page. 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 continues to send the request 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.

Set the maximum URL length to

Controls the maximum allowed length of a line of characters in the HTTP response headers. Use this property to protect your computers from buffer overflow exploits. Because URLs for many commerce sites continue to increase in length over time, you may need to adjust this value in the future.

Set the maximum total length to

Controls the maximum length of the HTTP response headers. If the total header length is more than this limit, the HTTP response is denied.

3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

HTTP responses: Header fields

This ruleset controls which HTTP response header fields the Firebox allows. If the default ruleset does not meet all of your business needs, you can add, delete, or modify rules.

RFC 2616 describes many of the HTTP response headers that are allowed in the default configuration. For more information, see <http://www.ietf.org/rfc/rfc2616.txt>.

1. From the **Categories** section, select **Header Fields**.
2. Add, delete, or modify rules, as described in [About working with rules and rulesets](#).
3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

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/jpeg` 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. From the **Categories** section, select **Content Types**.
2. Add, delete, or modify rules, as described in [About working with rules and rulesets](#).
3. The HTTP proxy includes a list of commonly used content types that you may want to add to the ruleset. To add content types, click the **Predefined** button. The **Select Content Type** dialog box appears. Select the type or types you want to add, and click **OK**. The new types appear in the **Rules** box.
4. If you want to change settings for one or more other categories in this proxy, go to topic on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

Allow web sites with a missing content type

By default, the Firebox denies MIME content that has no specified content type. In most cases, we recommend that you keep this default setting. Sites that do not supply legitimate MIME types in their HTTP responses do not follow RFC recommendations and could pose a security risk. However, some organizations need their employees to get access to web sites that do not have a specified content type.

You must make sure that you change the proxy configuration of the correct policy or policies. You can apply the change to any policy that uses an HTTP client proxy action. This could be an HTTP proxy policy, the Outgoing policy (which also applies an HTTP client proxy action), or the TCP-UDP policy.

1. From the **Categories** section, select **Content Types**.
2. Click **Change View**.
3. From the **Rules** list, select the check box adjacent to the **Allow (none)** rule.

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 HTTP proxy gives you control of the cookies in HTTP responses. You can configure rules to strip cookies, based on your network requirements. The default rule for the HTTP-Server and HTTP-Client proxy action allows all cookies. If the default ruleset does not meet all of your business needs, you can add, delete, or modify rules.

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.

Change settings for cookies

1. From the **Categories** section on the left, select **Cookies**.
2. Add, delete, or modify rules, as described in [About working with rules and rulesets](#).
3. If you want to change settings for one or more other categories in this proxy, go to the topics on the next category you want to modify.
or
If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [Predefined and user-defined proxy actions](#). Enter a name for the new action and click **OK**.
The New Policy Properties dialog box appears.

HTTP responses: Body content types

This ruleset gives you control of the content in an HTTP response. The Firebox is configured to deny Java bytecodes, Zip archives, Windows EXE/DLL files, and Windows CAB files. The default proxy action for outgoing HTTP requests (HTTP-Client) allows all other response body content types. If the default ruleset does not meet all of your business needs, you can add, delete, or modify rules. We recommend that you examine the file types that are used in your organization and allow only those file types that are necessary for your network.

1. From the **Categories** section, select **Body Content Types**.
2. Add, delete, or modify rules, as described in [About working with rules and rulesets](#).
3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

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.

Proxy settings skipped

These settings are skipped:

- HTTP request: range requests, URL path length, all request methods, all URL paths, request headers*, authorization pattern matching
- HTTP response: response headers*, content types, cookies, body content types

* Request headers and response headers are parsed by the HTTP proxy even when the traffic matches the HTTP proxy exception. If a parsing error does not occur, all headers are allowed. Also, antivirus scanning, IPS scanning, and WebBlocker are not applied to traffic that matches an HTTP proxy exception.

Proxy settings not skipped

These settings are not skipped:

- HTTP request: Idle timeout
- HTTP response: Idle timeout, maximum line length limit, maximum total length limit

All transfer-encoding parsing is still applied to allow the proxy to determine the encoding type. The HTTP proxy denies all invalid or malformed transfer encoding.

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`.

1. From the **Categories** section, select **HTTP Proxy Exceptions**.
2. In the field to the left of the **Add** button, type the host name or host name pattern. Click **Add**. Repeat for additional exceptions you want to add.
3. If you want to add a traffic log message each time the HTTP proxy takes an action on a proxy exception, select the **Log each transaction that matches an HTTP proxy exception** check box.
4. If you want to change settings for one or more other categories in this proxy, go to the topic on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#). Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

Configure Gateway AntiVirus actions

When you enable Gateway AntiVirus, you must set the actions to be taken if a virus or error is found in an email message (SMTP or POP3 proxies), web page (HTTP proxy), or uploaded or downloaded file (FTP proxy). The options for antivirus actions are:

Allow

Allows the packet to go to the recipient, even if the content contains a virus.

Deny (FTP proxy only)

Deny the file and send a deny message.

Lock (SMTP and POP3 proxies only)

Locks the attachment. This is a good option for files that cannot be scanned by the Firebox. A file that is locked cannot be opened easily by the user. Only the administrator can unlock the file. The administrator can use a different antivirus tool to scan the file and examine the content of the attachment. For information on how to unlock a file locked by Gateway AntiVirus, see [Unlock a file locked by Gateway AntiVirus](#).

Quarantine (SMTP proxy only)

When you use the SMTP proxy with the spamBlocker security subscription, you can send email messages with viruses or possible viruses to the Quarantine Server. For more information on the Quarantine Server, see [About the Quarantine Server](#). For information on how to set up Gateway AntiVirus to work with the Quarantine Server, see [Configure Gateway AntiVirus to quarantine email](#).

Remove (SMTP and POP3 proxies only)

Removes the attachment and allows the message through to the recipient.

Drop (not supported in POP3 proxy)

Drops the packet and drops the connection. No information is sent to the source of the message.

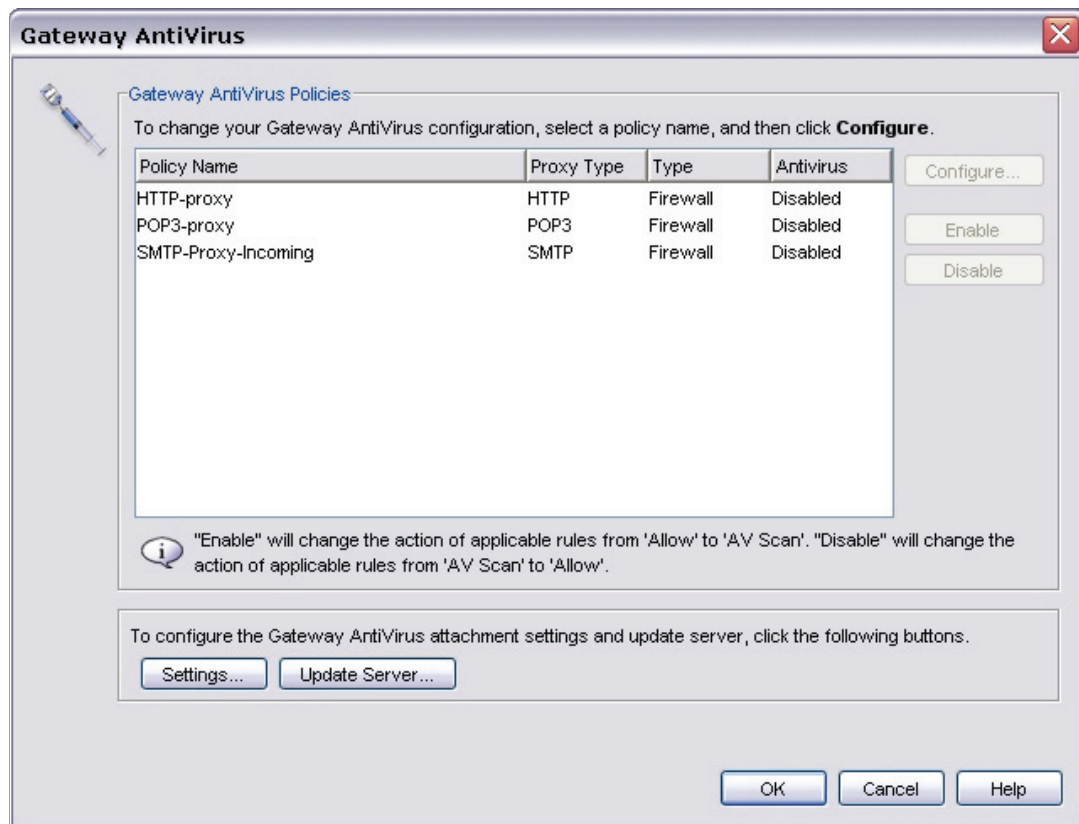
Block (not supported in POP3 proxy)

Blocks the packet, and adds the IP address of the sender to the Blocked Sites list.

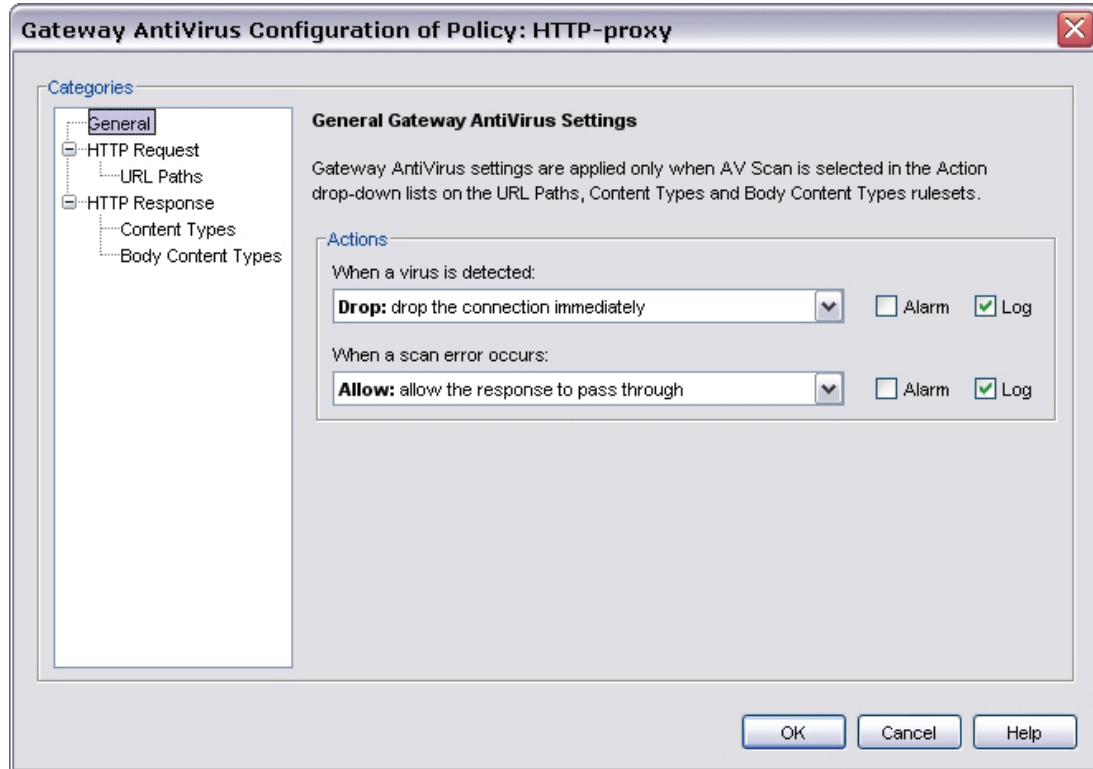


If you set the configuration to allow attachments, your configuration is less secure.

1. From Policy Manager, select **Tasks > Gateway AntiVirus > Configure**.
The Gateway AntiVirus dialog box appears, which lists the proxies that have already been created.



2. Select the policy you want to configure and click **Configure**.
The General Gateway Antivirus Settings page for that policy appears.
 Or, instead of step 1 and 2, you can go to the same page from the proxy definition screens. From the **Categories** section in the proxy definition, select **AntiVirus**.



3. Set the action the Firebox takes if a virus is detected in an email message, file, or web page, in the **When a virus is detected** drop-down list. See the beginning of this section for a description of the proxy actions.
4. Set the action the Firebox takes when it cannot scan an object or an attachment in the **When a scan error occurs** drop-down list. Attachments that cannot be scanned include binhex-encoded messages, certain encrypted files, or files that use a type of compression that we do not support such as password-protected Zip files. See the beginning of this section for a description of the proxy actions.
5. (FTP proxy only) You can limit file scanning up to a specified kilobyte count. Any additional bytes in the file are not scanned. This allows the proxy to partially scan very large files without a large effect on performance. Enter the limit in the **Limit scanning to first** field.

Create alarms or log entries for antivirus actions

An alarm is a mechanism to tell users when a proxy rule applies to network traffic. Use the **Alarm** check box on the AntiVirus page of a proxy definition to create an alarm when the adjacent action occurs. If you do not want an alarm for the antivirus action, clear the **Alarm** check box for that action.

FTP Proxy Action Configuration (predefined)

Name:

Description:

Categories

- General
- Commands
- Download
- Upload
- Antivirus**
- Intrusion Prevention
- Proxy and AV Alarm

Antivirus

Gateway AntiVirus settings are applied only when the Action drop-down lists on the 'Upload' and 'Download' rulesets is set to 'AV Scan'.

Actions

When virus is detected:

Drop: drop the connection immediately ☐ Alarm ☒ Log

When a scan error occurs:

Drop: drop the connection immediately ☐ Alarm ☒ Log

File Scan

Use this setting to limit the number of bytes to scan at the start of each file. The Firebox does not scan data past this limit. This allows large files to pass with partial scanning.

☐ Limit scanning to first kilobyte(s)

OK Cancel Help

To use the alarm feature successfully, you must also configure the type of alarm to use in each proxy policy. To configure the alarm type to use, use the Proxy and AV Alarms category for the proxy. For information about the settings for this category, see [Set logging and notification preferences](#).

If you want to record log messages for a proxy action, select the **Log** check box for the antivirus response. If you do not want to record log messages for an antivirus response, clear the **Log** check box.

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.

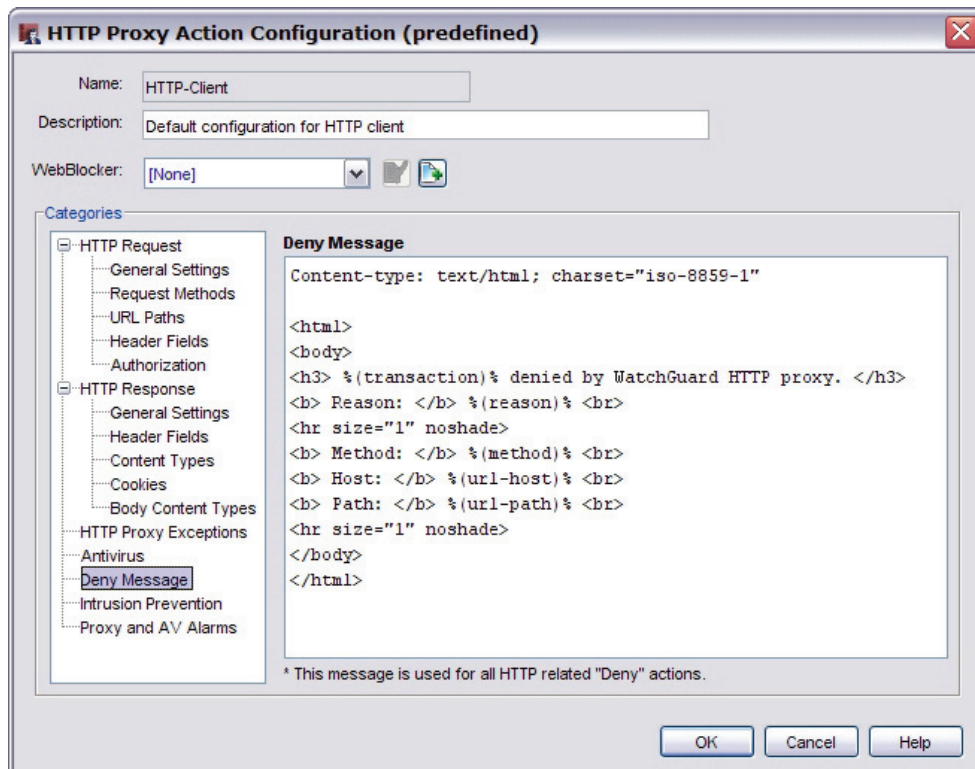
`%(url-host)%`

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.

1. From the **Categories** section, select **Deny Message**.



2. Type the deny message in the deny message box.
3. If you want to change settings for one or more other categories in this proxy, go to the topic on the next category you want to modify.
or
If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#). Enter a name for the new action and click **OK**.
The New Policy Properties dialog box appears.

Intrusion prevention in proxy definitions

An *intrusion* is a direct attack on your computer. These attacks can cause damage to your network, get sensitive information, or use your computers to attack other networks.


To help protect your network from intrusions, you can purchase the optional Intrusion Prevention Service (IPS) for the Firebox. Intrusion Prevention Service operates with the SMTP, POP3, HTTP, FTP, DNS, and TCP-UDP proxies.

You can activate and configure IPS in two ways:

Run the Activate Intrusion Prevention wizard from the Tasks menu in Policy Manager

For more information, see [Activate Intrusion Prevention Service \(IPS\)](#).

Use the Intrusion Prevention ruleset in the proxy definition

1. [Get a feature key](#) for IPS from LiveSecurity Service and [add the feature key to the Firebox](#).
2. [Add a proxy policy to your Firebox configuration](#). Or, you can edit an existing proxy.
3. From the **Properties** tab of the **New/Edit Policy Properties** dialog box, click the **View/Edit Proxy** icon  (the first icon to the right of the **Proxy action** drop-down list).
4. Select the **Intrusion Prevention** category from the left side of the window. On the right side of the window, [set parameters for Intrusion Prevention Service \(IPS\)](#).

Proxy and AV alarms

An alarm is an event that triggers a *notification*, which is a mechanism to tell a network administrator about a condition in the network. In a proxy definition, an alarm might occur when traffic matches, or does not match, a rule in the proxy, and the **If matched** or **None matched** field under **Actions to take** in the ruleset definitions is set to an action other than **Allow**.

For example, the default definition of the FTP proxy has a rule that denies the download of files whose file types match any of these patterns: .cab, .com, .dll, .exe, and .zip. You can specify that an alarm is generated whenever the Firebox takes the **Deny** action because of this rule.

For each proxy, you can define what the Firebox does when an alarm occurs.

1. From the **Categories** section of the proxy definition, select **Proxy and AV Alarm**.
2. You can define the Firebox to send an SNMP trap, a notification to a network administrator, or both. The notification can either be an email to a network administrator or a pop-up window on the administrator's management station.
For more information on the Proxy and AV alarm fields, see [Set logging and notification preferences](#).

3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

Allow Windows updates through the HTTP proxy

Windows Update servers identify the content they deliver to a computer as a generic binary stream (such as octet stream), which is blocked by the default HTTP proxy rules. To allow Windows updates through the HTTP proxy, you must edit your HTTP-Client proxy ruleset to add HTTP proxy exceptions for the Windows Update servers:

1. Make sure that your Firebox allows outgoing connections on port 443 and port 80. These are the ports that computers use to contact the Windows Update servers.
2. From the **Categories** section, select **HTTP Proxy Exceptions**.
3. In the field to the left of the **Add** button, type or paste each domain into the text box, and click **Add** after each one:
 windowsupdate.microsoft.com
 download.windowsupdate.com
 update.microsoft.com
 download.microsoft.com
 ntservicepack.microsoft.com
 wustat.windows.com
 v4.windowsupdate.microsoft.com
 v5.windowsupdate.microsoft.com
4. Click **OK** three times to close all proxy and policy dialog boxes. [Save the configuration file](#).

If you still cannot download Windows updates

If you have more than one HTTP proxy policy, make sure that you add the HTTP exceptions to the correct policy and proxy action.

Microsoft does not limit updates to only these domains. Examine your logs for denied traffic to a Microsoft-owned domain. If you do not have a Log Server, run Windows Update and monitor the [Firebox log messages \(Traffic Monitor\)](#). Look for any traffic denied by the HTTP proxy. The log line should include the domain. Add any new Microsoft domain to the HTTP proxy exceptions list, and then run Windows Update again.

Finish and save the configuration

1. When you are done with all changes for all categories of the proxy, click **OK** to close the **New Policy Properties** or **Edit Policy Properties** dialog box.
2. Save the configuration to the Firebox. To do this, select **File > Save > To Firebox**.
The Save dialog box appears with the default location for configuration files. You can change the name of the configuration file if you choose.
3. Click **Save**.
4. You are prompted for the configuration passphrase. Type it and click **OK**.

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.

When an HTTPS client or server uses a port other than port 443 in your organization, you can use the TCP/UDP proxy to relay the traffic to the HTTPS proxy. For information on the TCP/UDP proxy, see [About the TCP/UDP proxy](#).

To add the HTTPS proxy to your Firebox configuration, see [Add a proxy to your Firebox configuration](#). Then, if you need to change the proxy definition to meet your business needs, you can use the **New/Edit Policy Properties** dialog box to modify the definition. The fields on this dialog box are divided into three tabs: **Policy**, **Properties**, and **Advanced**. In addition, the **Properties** tab contains an icon for you to configure the [proxy action](#).

HTTPS and WebBlocker

You can use the HTTPS proxy with the WebBlocker security subscription. For more information, see [About WebBlocker](#). Note that you can use the [HTTPS proxy: Domain names](#) settings to filter sites prior to the sites being compared to the WebBlocker database.

Policy tab


- **HTTPS-proxy connections are:** Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)** and define who appears in the **From** and **To** list (on the **Policy** tab of the proxy definition). See [Set access rules for a policy](#).
- **Use policy-based routing:** If you want to use policy-based routing in your proxy definition, see [Configure policy-based routing](#).

Properties tab

- In the **Proxy action** drop-down list, select whether you want to define an action for a client or server. For information about proxy actions, see [About proxy actions](#).
- To define logging for a policy, click **Logging** and [Set logging and notification preferences](#).
- If you set the **HTTPS-proxy connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use HTTPS. See [Block sites temporarily with policy settings](#).
- If you want to use an idle timeout other than the one set by the Firebox or authentication server, [Set a custom idle timeout](#).

Proxy action settings

WatchGuard proxies have predefined rulesets that provide a good balance of security and accessibility for most installations. If a default ruleset does not meet all of your business needs, you can add, delete, or modify rules.

To modify the settings and rulesets for a proxy action, click the **View/Edit Proxy** icon  (the first icon to the right of the **Proxy action** drop-down list) and select a category of settings from the left side of the dialog box:

- [HTTPS proxy: General settings](#)
- [HTTPS proxy: Domain names](#)
- [Proxy and AV alarms](#)

Advanced tab

You can use several other options in your proxy definition:

- [Set an operating schedule](#)
- [Apply Traffic Management actions to a policy](#)
- [Set ICMP error handling](#)
- [Apply NAT rules](#) (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- [Enable QoS Marking for a policy](#)
- [Set traffic priority in a policy](#)
- [Add a sticky connection duration to a policy](#)

HTTPS Proxy: General settings

On the **General Settings** page (the page that first appears after you click the View/Edit Proxy icon), you can set idle timeout length and whether logging is enabled or disabled.

Set the connection idle timeout to

Select this check box to control how long the HTTPS proxy waits for the web client to make a request from the external web server after it starts a TCP/IP connection or after an earlier request, if one was made, for the same connection. If the time period exceeds this setting, the HTTPS proxy closes the connection. In the adjacent field, enter the number of minutes before the proxy times out.

Turn on logging for reports

Creates a traffic log message for each transaction. This option creates a large log file, but this information is very important if your firewall is attacked. If you do not select this check box, you do not see detailed information about HTTPS proxied connections in WatchGuard Reports.

If you want to change settings for one or more other categories in this proxy, go to the topic on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

HTTPS proxy: Domain names

You use domain names to filter content at an entire site. The difference between domain names and the URL path rules you use with the HTTP proxy is that domain names apply to all protocols and all client types. URL paths are used only for web connections.

For example, if you want to deny traffic from any site in the abc.com domain, you would add a Domain Name rule with the pattern *.abc.com.

1. From the **Categories** section, select **Domain Names**.
2. Add, delete, or modify rules, as described in [About working with rules and rulesets](#).
3. If you want to change settings for one or more other categories in this proxy, go to the topic on the next category you want to modify.
or
If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#). Enter a name for the new action and click **OK**.

Proxy and AV alarms

An alarm is an event that triggers a *notification*, which is a mechanism to tell a network administrator about a condition in the network. In a proxy definition, an alarm might occur when traffic matches, or does not match, a rule in the proxy, and the **If matched** or **None matched** field under **Actions to take** in the ruleset definitions is set to an action other than **Allow**.

For example, the default definition of the FTP proxy has a rule that denies the download of files whose file types match any of these patterns: .cab, .com, .dll, .exe, and .zip. You can specify that an alarm is generated whenever the Firebox takes the **Deny** action because of this rule.

For each proxy, you can define what the Firebox does when an alarm occurs.

1. From the **Categories** section of the proxy definition, select **Proxy and AV Alarm**.
2. You can define the Firebox to send an SNMP trap, a notification to a network administrator, or both. The notification can either be an email to a network administrator or a pop-up window on the administrator's management station.
For more information on the Proxy and AV alarm fields, see [Set logging and notification preferences](#).
3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.
or
If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.
The New Policy Properties dialog box appears.

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 add the POP3 proxy to your Firebox configuration, see [Add a proxy to your Firebox configuration](#). Then, if you need to change the proxy definition to meet your business needs, you can use the **New/Edit Policy Properties** dialog box to modify the definition. The fields on this dialog box are divided into three tabs: **Policy**, **Properties**, and **Advanced**. In addition, the **Properties** tab contains an icon for you to configure the [proxy action](#).

Policy tab


- **POP3-proxy connections are:** Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)** and define who appears in the **From** and **To** list (on the **Policy** tab of the proxy definition). See [Set access rules for a policy](#).
- **Use policy-based routing:** If you want to use policy-based routing in your proxy definition, see [Configure policy-based routing](#).

Properties tab

- In the **Proxy action** drop-down list, select whether you want to define an action for a client or server. For information about proxy actions, see [About proxy actions](#).
- To define logging for a policy, click **Logging** and [Set logging and notification preferences](#).
- If you set the **POP3-proxy connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use POP3. See [Block sites temporarily with policy settings](#).
- If you want to use an idle timeout other than the one set by the Firebox or authentication server, [Set a custom idle timeout](#).

Proxy action settings

WatchGuard proxies have predefined rulesets that provide a good balance of security and accessibility for most installations. If a default ruleset does not meet all of your business needs, you can add, delete, or modify rules.

To modify the settings and rulesets for a proxy action, click the **View/Edit Proxy** icon  (the first icon to the right of the **Proxy action** drop-down list) and select a category of settings from the left side of the dialog box:

- [POP3 proxy: General settings](#)
- [POP3 proxy: Authentication](#)
- [POP3 proxy: Content types](#)
- [POP3 proxy: File names](#)
- [POP3 proxy: Headers](#)
- [POP3 proxy: Antivirus responses](#)
- [POP3 proxy: Deny message](#)
- [POP3 proxy: Intrusion prevention](#)
- [POP3 proxy: spamBlocker](#)
- [Proxy and AV alarms](#)

Advanced tab

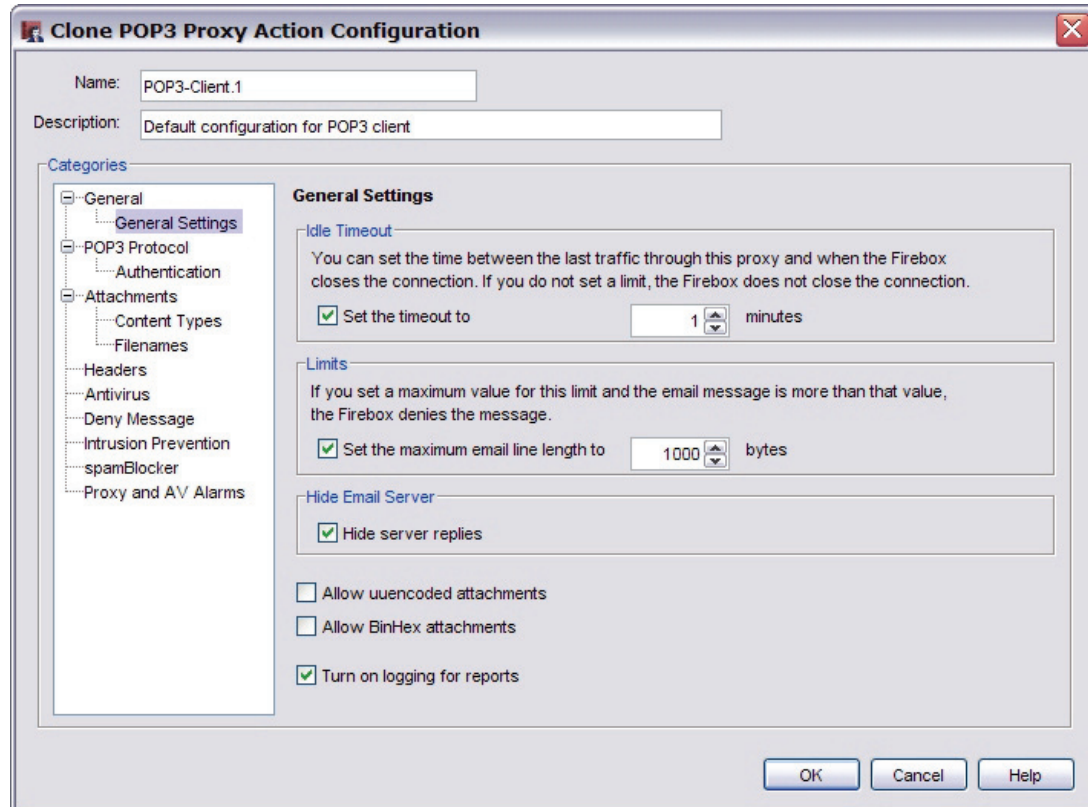
You can use several other options in your proxy definition:

- [Set an operating schedule](#)
- [Apply Traffic Management actions to a policy](#)
- [Set ICMP error handling](#)
- [Apply NAT rules](#) (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- [Enable QoS Marking for a policy](#)
- [Set traffic priority in a policy](#)
- [Add a sticky connection duration to a policy](#)

POP3 proxy: General settings

On the **General Settings** page (the page that first appears after you click the View/Edit Proxy icon), you can adjust time out and line length limits as well as other general parameters for the POP3 proxy:

1. If you are not already on this page, from the **Categories** section, select **General Settings**.



2. Change any of these settings to meet your business needs:

Set the timeout to

Use this setting to limit the number of minutes 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 POP3 server is slow or cannot be reached.

Set the maximum email line length to

Use this setting to prevent some types of buffer overflow attacks. Very long line lengths can cause buffer overflows on some email systems. Most email clients and systems send relatively short lines, but some web-based email systems send very long lines. However, it is unlikely that you will need to change this setting unless it prevents access to legitimate mail.

Hide server replies

Select this check box if you want to replace the POP3 greeting strings in email messages. These strings can be used by hackers to identify the POP3 server vendor and version.

Allow uuencoded attachments

Select this check box if you want the POP3 proxy to allow uuencoded attachments to email messages. Uuencode is an older program used to send binary files in ASCII text format over the Internet. UUencoded attachments can be security risks because they appear as ASCII text files but can actually contain executable files.

Allow BinHex attachments

Select this check box if you want the POP3 proxy to allow BinHex attachments to email messages. BinHex, which is short for binary-to-hexadecimal, is a utility that converts a file from binary format to ASCII.

Turn on logging for reports

Select this check box if you want the POP3 proxy to send a log message for each connection request through POP3. If you want to use WatchGuard Reports to create reports on POP3 traffic, you must select this check box.

3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

POP3 proxy: Authentication

A POP3 client must authenticate to a POP3 server before they exchange information. On the **Authentication** page, you can set the types of authentication for the proxy to allow and the action to take for types that do not match the criteria. If the default ruleset does not meet all of your business needs, you can add, delete, or modify rules:

1. From the **Categories** section, select **Authentication**.
2. Add, delete, or modify rules, as described in [About working with rules and rulesets](#).
3. After you are finished modifying the ruleset, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

4. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

POP3 Proxy Action Configuration (predefined)

Name: POP3-Client

Description: Default configuration for POP3 client

Categories

- General
 - General Settings
- POP3 Protocol
 - Authentication**
- Attachments
 - Content Types
 - Filenames
- Headers
- Antivirus
- Deny Message
- Intrusion Prevention
- spamBlocker
- Proxy and AV Alarms

Authentication Change View

Rules (simple view)

- DIGEST-MD5
- CRAM-MD5
- PLAIN
- NTLM
- LOGIN
- GSSAPI
- KERBEROS_V4

Pattern: Add Remove

Actions to take

If matched:	Allow	<input type="checkbox"/> Alarm	<input type="checkbox"/> Log
None matched:	Deny	<input type="checkbox"/> Alarm	<input checked="" type="checkbox"/> Log

POP3 proxy: 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. 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.

If the default ruleset does not meet all of your business needs, you can add, delete, or modify rules. On the **Content Types** page, you can set values for content filtering and the action to take for content types that do not match the criteria. For the POP3-server proxy action, you set values for incoming content filtering. For the POP3-client action, you set values for outgoing content filtering.

1. From the **Categories** section, select **Content Types**.
2. Select the **Enable content type auto detection** check box for the POP3 proxy to examine content to determine content type. Otherwise, the POP3 proxy uses the value stated in the email header, which clients sometimes set incorrectly.
As an example, an attached .pdf file might have a content type stated as application/octet-stream. If you enable content type auto detection, the POP3 proxy recognizes the .pdf file and uses the actual content type, application/pdf. If the proxy does not recognize the content type after it examines the content, it uses the value stated in the email header, as it would if content type auto detection were not enabled.
Because hackers often try to disguise executables files as other content types, we recommend that you enable content type auto detection to make your installation more secure.
3. Add, delete, or modify rules, as described in [About working with rules and rulesets](#).
4. 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. To allow any image format, you add image/* to the list.
5. Several predefined content types are available for you to add. Click the **Predefined** button to see a list of content types, along with short descriptions of the content types.
6. After you are finished with your changes to the ruleset, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

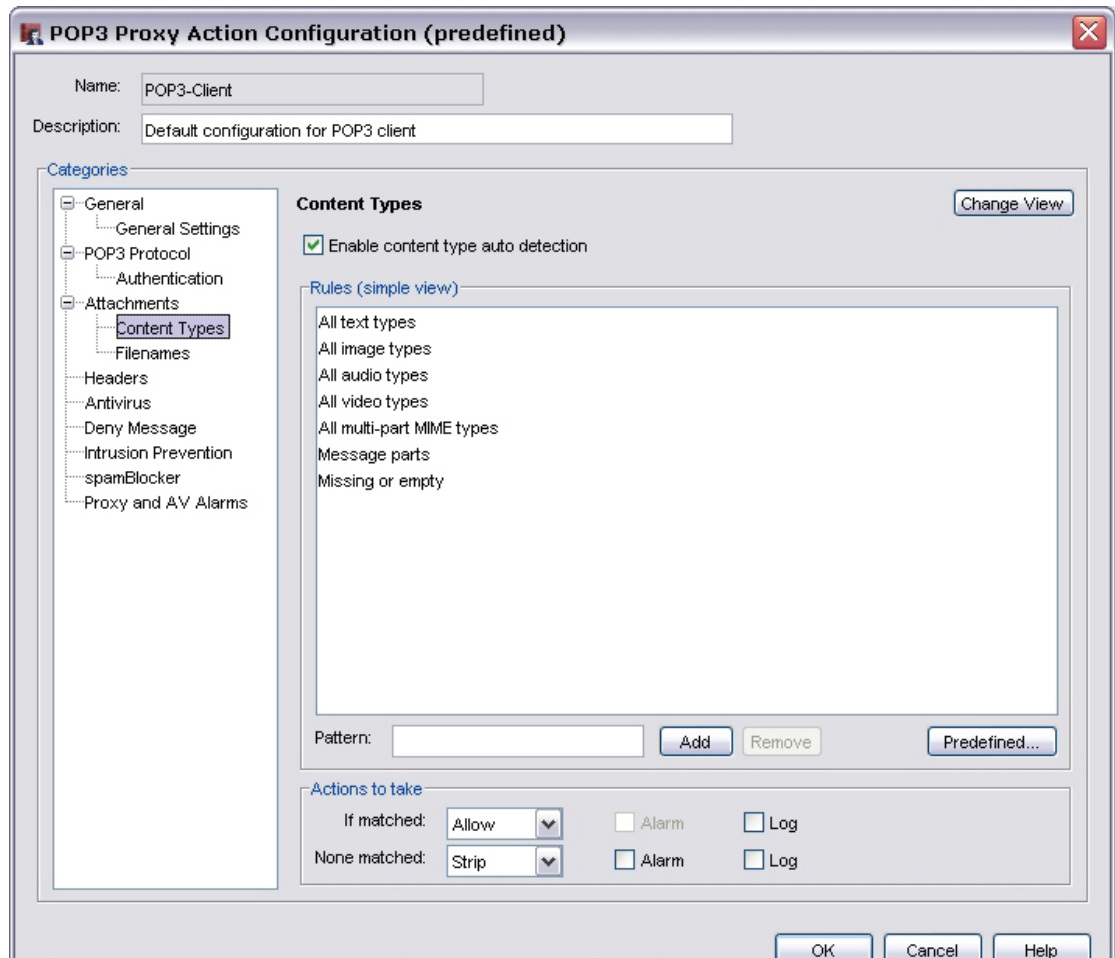
7. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions.](#))

Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.



POP3 proxy: File names

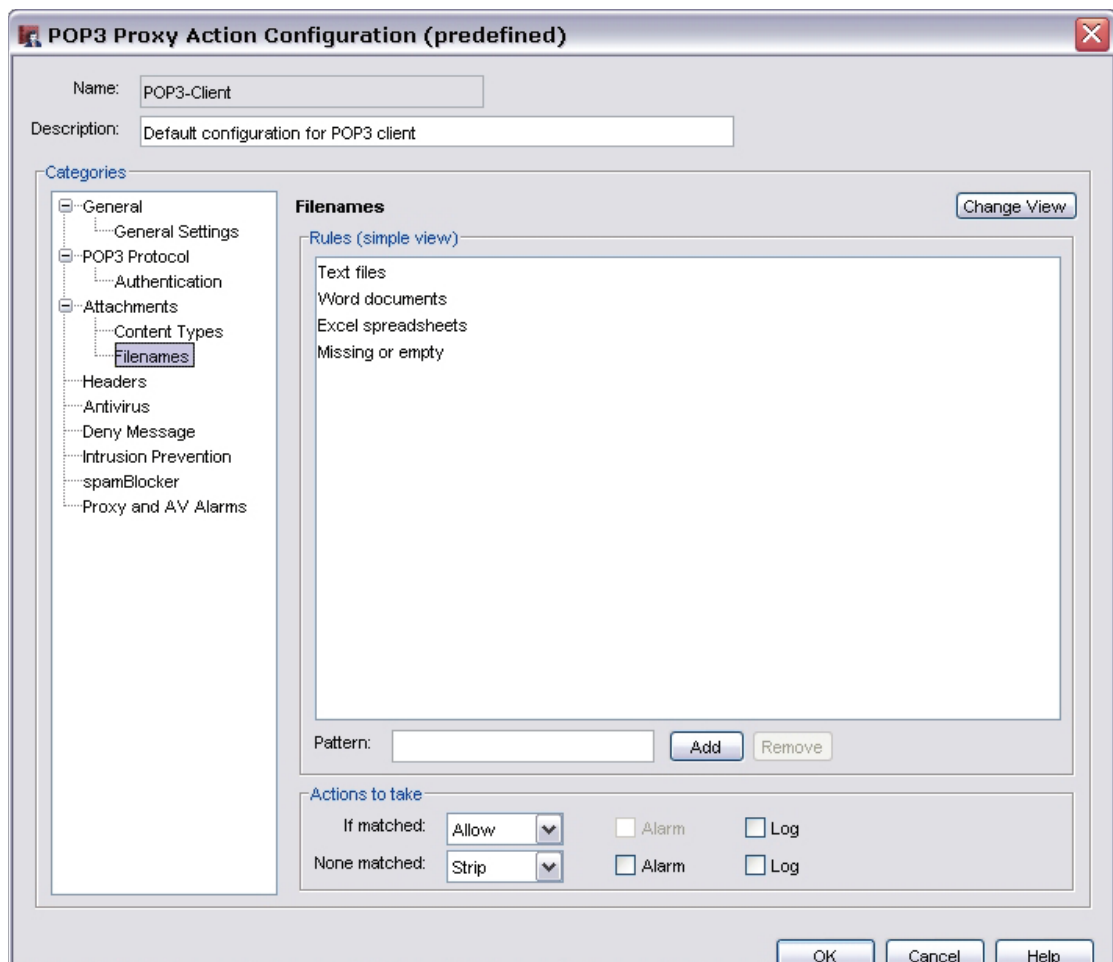
You use this ruleset in a POP3-server proxy action to put limits on file names for incoming email attachments. You use the ruleset for the POP3-client proxy action to put limits on file names for outgoing email attachments. If the default ruleset does not meet all of your business needs, you can add, delete, or modify rules.

1. From the **Categories** section, select **Filenames**.
2. Add, delete, or modify rules, as described in [About working with rules and rulesets](#).
3. After you are finished with your changes to the ruleset, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. Enter a name for the new action and click **OK**.
The New Policy Properties dialog box appears.
4. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.



POP3 proxy: Headers

The POP3 proxy examines email headers to find patterns common to forged email messages as well as those from legitimate senders. If the default ruleset does not meet all of your business needs, you can add, delete, or modify rules:

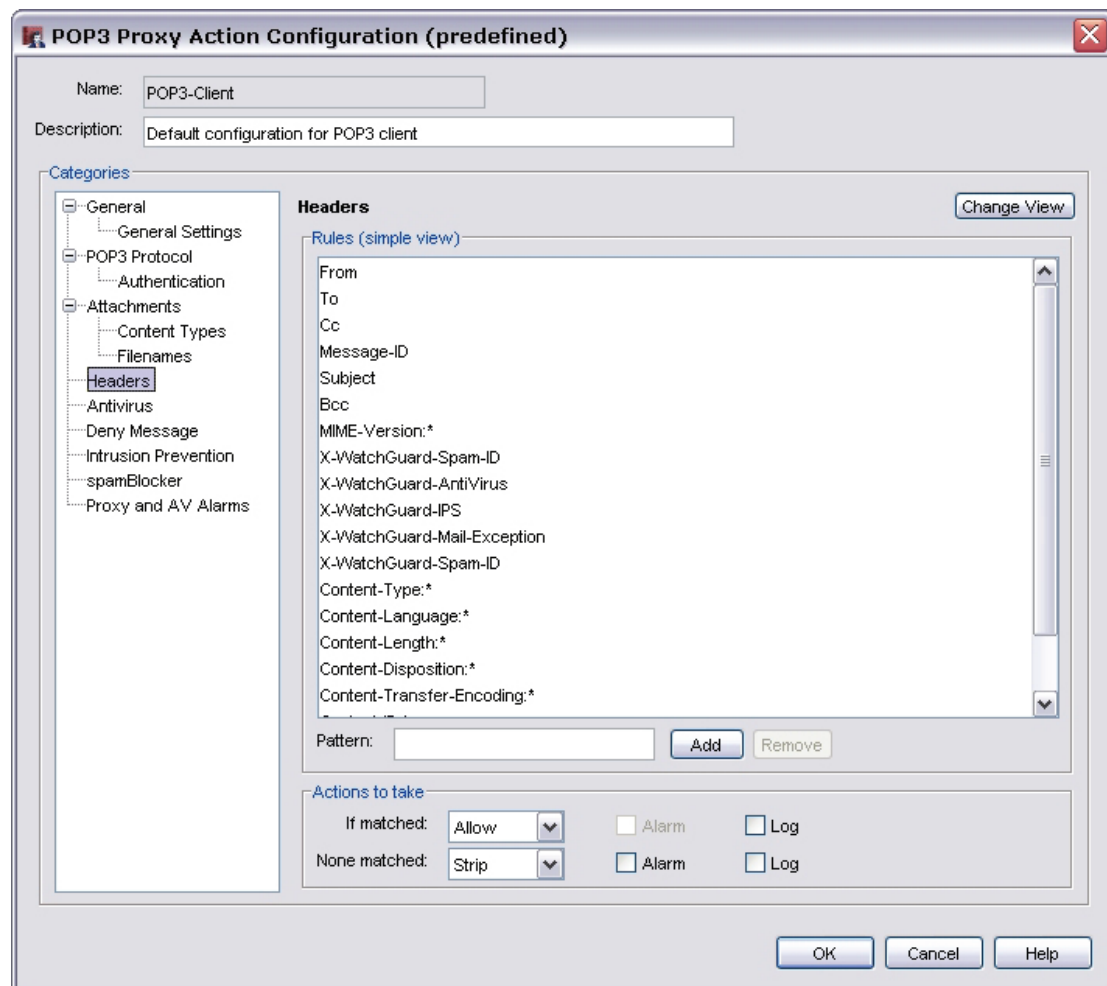
1. From the **Categories** section, select **Headers**.
2. Add, delete, or modify rules, as described in [About working with rules and rulesets](#).
3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

4. If you want to change settings for one or more other categories, go to the section in this document on that category.



Configure Gateway AntiVirus actions

When you enable Gateway AntiVirus, you must set the actions to be taken if a virus or error is found in an email message (SMTP or POP3 proxies), web page (HTTP proxy), or uploaded or downloaded file (FTP proxy). The options for antivirus actions are:

Allow

Allows the packet to go to the recipient, even if the content contains a virus.

Deny (FTP proxy only)

Deny the file and send a deny message.

Lock (SMTP and POP3 proxies only)

Locks the attachment. This is a good option for files that cannot be scanned by the Firebox. A file that is locked cannot be opened easily by the user. Only the administrator can unlock the file. The administrator can use a different antivirus tool to scan the file and examine the content of the attachment. For information on how to unlock a file locked by Gateway AntiVirus, see [Unlock a file locked by Gateway AntiVirus](#).

Quarantine (SMTP proxy only)

When you use the SMTP proxy with the spamBlocker security subscription, you can send email messages with viruses or possible viruses to the Quarantine Server. For more information on the Quarantine Server, see [About the Quarantine Server](#). For information on how to set up Gateway AntiVirus to work with the Quarantine Server, see [Configure Gateway AntiVirus to quarantine email](#).

Remove (SMTP and POP3 proxies only)

Removes the attachment and allows the message through to the recipient.

Drop (not supported in POP3 proxy)

Drops the packet and drops the connection. No information is sent to the source of the message.

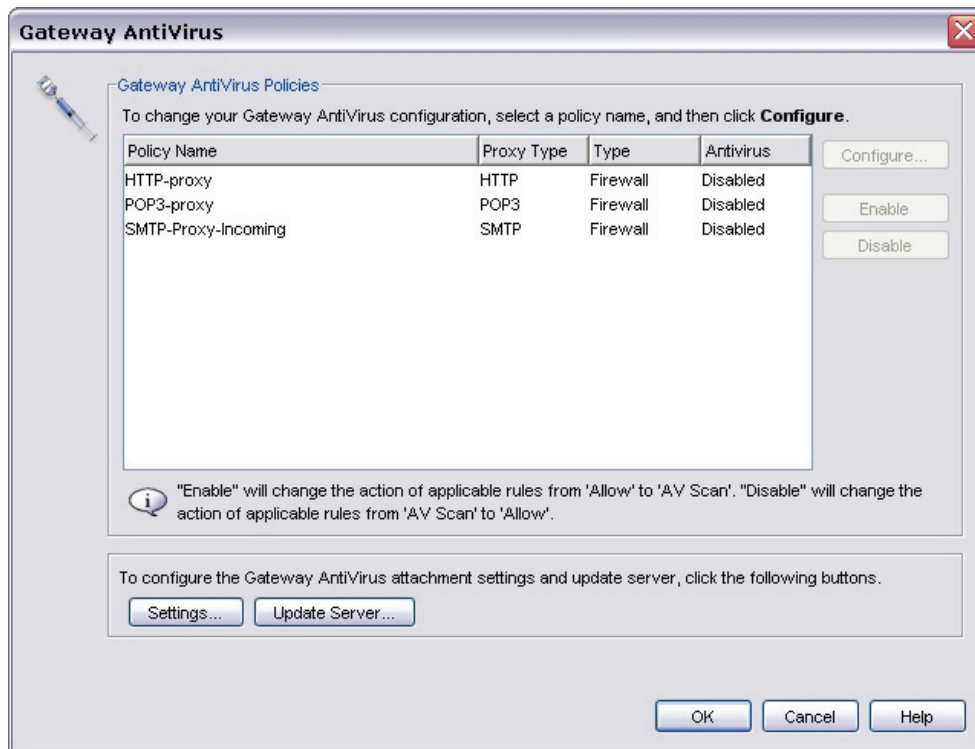
Block (not supported in POP3 proxy)

Blocks the packet, and adds the IP address of the sender to the Blocked Sites list.

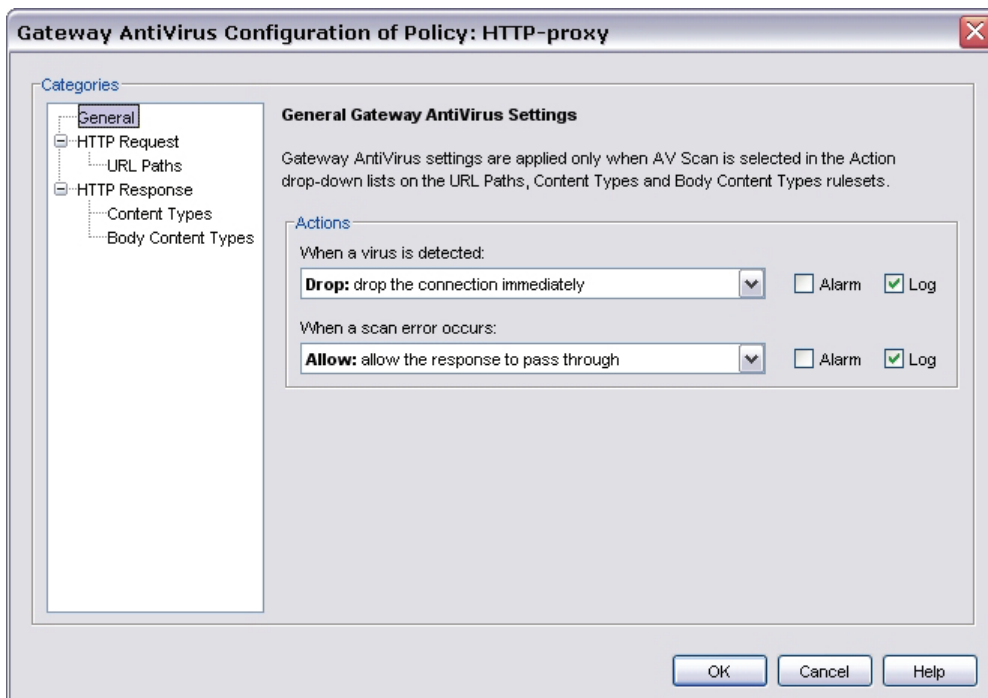


If you set the configuration to allow attachments, your configuration is less secure.

1. From Policy Manager, select **Tasks > Gateway AntiVirus > Configure**.
The Gateway AntiVirus dialog box appears, which lists the proxies that have already been created.



2. Select the policy you want to configure and click **Configure**.
The General Gateway Antivirus Settings page for that policy appears.
Or, instead of step 1 and 2, you can go to the same page from the proxy definition screens. From the **Categories** section in the proxy definition, select **AntiVirus**.



3. Set the action the Firebox takes if a virus is detected in an email message, file, or web page, in the **When a virus is detected** drop-down list. See the beginning of this section for a description of the proxy actions.
4. Set the action the Firebox takes when it cannot scan an object or an attachment in the **When a scan error occurs** drop-down list. Attachments that cannot be scanned include binhex-encoded messages, certain encrypted files, or files that use a type of compression that we do not support such as password-protected Zip files. See the beginning of this section for a description of the proxy actions.
5. (FTP proxy only) You can limit file scanning up to a specified kilobyte count. Any additional bytes in the file are not scanned. This allows the proxy to partially scan very large files without a large effect on performance. Enter the limit in the **Limit scanning to first** field.

Create alarms or log entries for antivirus actions

An alarm is a mechanism to tell users when a proxy rule applies to network traffic. Use the **Alarm** check box on the AntiVirus page of a proxy definition to create an alarm when the adjacent action occurs. If you do not want an alarm for the antivirus action, clear the **Alarm** check box for that action.

FTP Proxy Action Configuration (predefined)

Name:

Description:

Categories

- General
- Commands
- Download
- Upload
- Antivirus**
- Intrusion Prevention
- Proxy and AV Alarm

Antivirus

Gateway AntiVirus settings are applied only when the Action drop-down lists on the 'Upload' and 'Download' rulesets is set to 'AV Scan'.

Actions

When virus is detected:

☐ Alarm ☒ Log

When a scan error occurs:

☐ Alarm ☒ Log

File Scan

Use this setting to limit the number of bytes to scan at the start of each file. The Firebox does not scan data past this limit. This allows large files to pass with partial scanning.

☐ Limit scanning to first kilobyte(s)

OK Cancel Help

To use the alarm feature successfully, you must also configure the type of alarm to use in each proxy policy. To configure the alarm type to use, use the Proxy and AV Alarms category for the proxy. For information about the settings for this category, see [Set logging and notification preferences](#).

If you want to record log messages for a proxy action, select the **Log** check box for the antivirus response. If you do not want to record log messages for an antivirus response, clear the **Log** check box.

POP3 proxy: Deny message

The Firebox gives a default deny message that replaces denied content. You can replace that deny message with one that you write. The first line of the deny message is a section of the HTTP header. You must include an empty line between the first line and the body of the message.

1. From the **Categories** section, select **Deny Message**.
2. In the **Deny Message** block, you can write a custom plain text message with standard HTML that will appear in the recipient email when the proxy blocks that email. You can use these variables:

%(reason)%

Puts the cause for the Firebox to deny the content. *%(type)%* Puts the type of content that was denied.

%(filename)%

Puts the file name of the denied content.

%(virus)%

Puts the name or status of a virus, for Gateway AntiVirus users only.

%(action)%

Puts the name of the action taken: lock, strip, and so on.

%(recovery)%

Puts whether you can recover the attachment.

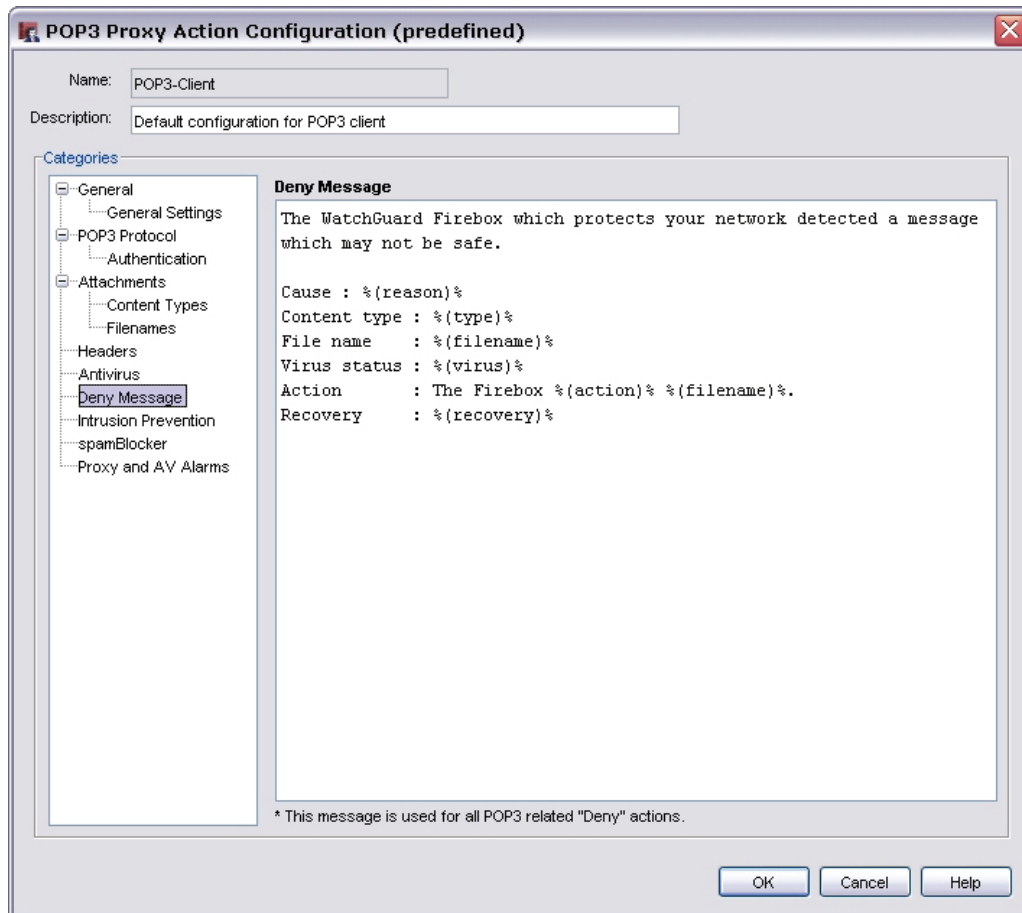
- If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions.](#))

Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.



Intrusion prevention in proxy definitions

An *intrusion* is a direct attack on your computer. These attacks can cause damage to your network, get sensitive information, or use your computers to attack other networks.


To help protect your network from intrusions, you can purchase the optional Intrusion Prevention Service (IPS) for the Firebox. Intrusion Prevention Service operates with the SMTP, POP3, HTTP, FTP, DNS, and TCP-UDP proxies.

You can activate and configure IPS in two ways:

Run the Activate Intrusion Prevention wizard from the Tasks menu in Policy Manager

For more information, see [Activate Intrusion Prevention Service \(IPS\).](#)

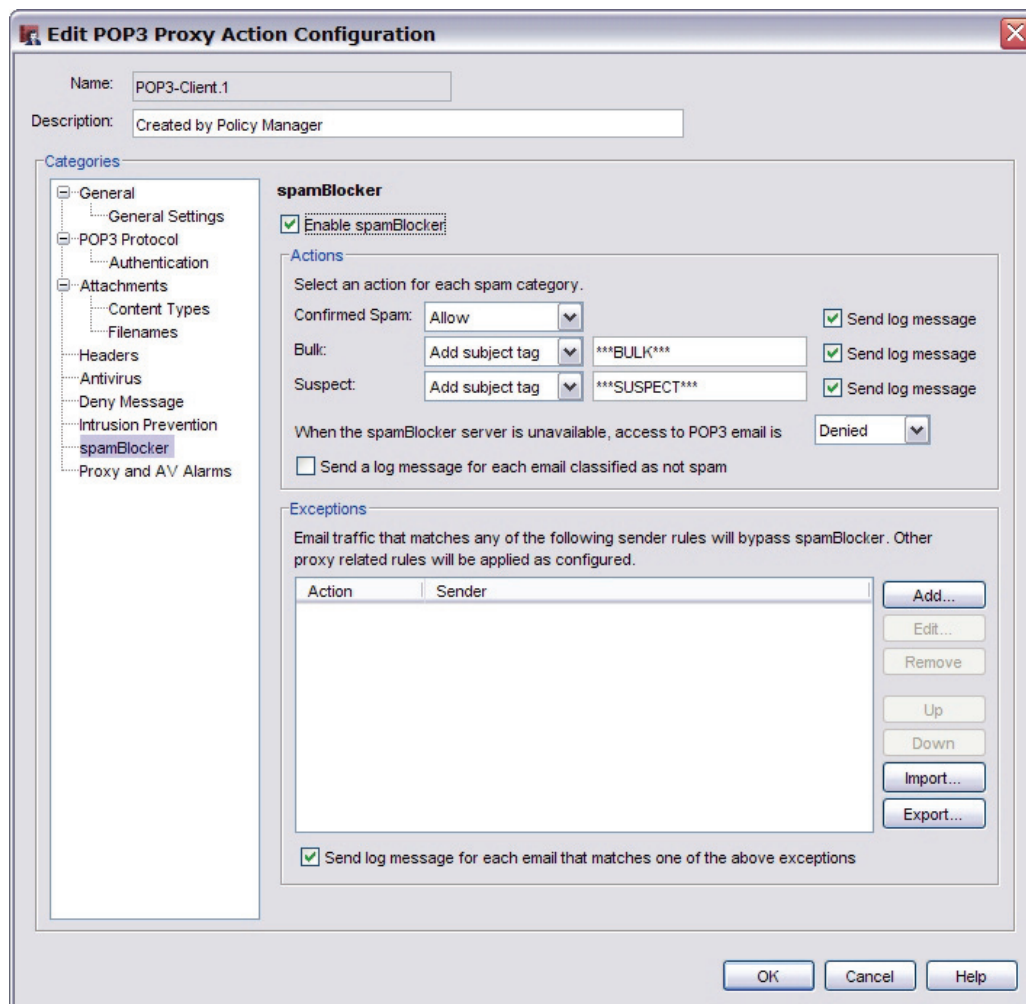
Use the Intrusion Prevention ruleset in the proxy definition

1. [Get a feature key](#) for IPS from LiveSecurity Service and [add the feature key to the Firebox](#).
2. [Add a proxy policy to your Firebox configuration](#). Or, you can edit an existing proxy.
3. From the **Properties** tab of the **New/Edit Policy Properties** dialog box, click the **View/Edit Proxy** icon  (the first icon to the right of the **Proxy action** drop-down list).
4. Select the **Intrusion Prevention** category from the left side of the window. On the right side of the window, [set parameters for Intrusion Prevention Service \(IPS\)](#).

POP3 proxy: 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 increases your capacity to catch spam at the edge of your network when it tries to come into your system. If you have purchased and enabled the spamBlocker feature, the fields in the spamBlocker category set the actions for email messages identified as spam.

Although you can use the proxy definition screens to activate and configure spamBlocker, it is easier to use the **Tasks** menu in Policy Manager to do this. For more information on how to do this, or to use the spamBlocker screens in the proxy definition, see [About spamBlocker](#).



Edit POP3 Proxy Action Configuration

Name: POP3-Client.1

Description: Created by Policy Manager

Categories

- General
 - General Settings
- POP3 Protocol
 - Authentication
- Attachments
 - Content Types
 - Filenames
- Headers
- Antivirus
- Deny Message
- Intrusion Prevention
- spamBlocker**
- Proxy and AV Alarms

spamBlocker

☒ **Enable spamBlocker**

Actions

Select an action for each spam category.

Confirmed Spam: Allow ☐ Send log message

Bulki: Add subject tag ***BULK*** ☒ Send log message

Suspect: Add subject tag ***SUSPECT*** ☒ Send log message

When the spamBlocker server is unavailable, access to POP3 email is Denied ☐ Send a log message for each email classified as not spam

Exceptions

Email traffic that matches any of the following sender rules will bypass spamBlocker. Other proxy related rules will be applied as configured.

Action	Sender

☒ Send log message for each email that matches one of the above exceptions

OK Cancel Help

Proxy and AV alarms

An alarm is an event that triggers a *notification*, which is a mechanism to tell a network administrator about a condition in the network. In a proxy definition, an alarm might occur when traffic matches, or does not match, a rule in the proxy, and the **If matched** or **None matched** field under **Actions to take** in the ruleset definitions is set to an action other than **Allow**.

For example, the default definition of the FTP proxy has a rule that denies the download of files whose file types match any of these patterns: .cab, .com, .dll, .exe, and .zip. You can specify that an alarm is generated whenever the Firebox takes the **Deny** action because of this rule.

For each proxy, you can define what the Firebox does when an alarm occurs.

1. From the **Categories** section of the proxy definition, select **Proxy and AV Alarm**.
2. You can define the Firebox to send an SNMP trap, a notification to a network administrator, or both. The notification can either be an email to a network administrator or a pop-up window on the administrator's management station.
For more information on the Proxy and AV alarm fields, see [Set logging and notification preferences](#).
3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

Finish and save the configuration

1. When you are done with all changes for all categories of the proxy, click **OK** to close the **New Policy Properties** or **Edit Policy Properties** dialog box.
2. Save the configuration to the Firebox. To do this, select **File > Save > To Firebox**.
The Save dialog box appears with the default location for configuration files. You can change the name of the configuration file if you choose.
3. Click **Save**.
4. You are prompted for the configuration passphrase. Type it and click **OK**.

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. The 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

To add the SIP proxy to your Firebox configuration, see [Add a proxy to your Firebox configuration](#).

Configure the SIP proxy action settings

The SIP proxy has one ruleset, General, which has one setting:

Turn on logging for reports: Creates a traffic log message for each transaction. Logging for reports is enabled by default. This option may create a large log file, but this information is very important if your firewall is attacked. If you clear this check box, you do not see detailed information about SIP proxied connections in WatchGuard Reports.

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.

When you use incoming static NAT with SMTP, you might see packets that come from the remote mail server being denied with destination port 113. In these cases, you can add an IDENT policy to Policy Manager. Configure IDENT to allow incoming connections to: **Firebox**. This enables outgoing mail messages from behind the Firebox to the few SMTP servers on the Internet that use IDENT.

The TCP/UDP proxy is available for protocols on non-standard ports. When SMTP uses a port other than port 25, the TCP/UDP proxy relays the traffic to the SMTP proxy. For information on the TCP/UDP proxy, see [About the TCP/UDP proxy](#).

To add the SMTP proxy to your Firebox configuration, see [Add a proxy to your Firebox configuration](#). Then, if you need to change the proxy definition to meet your business needs, you can use the **New/Edit Policy Properties** dialog box to modify the definition. The fields on this dialog box are divided into three tabs: **Policy**, **Properties**, and **Advanced**. In addition, the **Properties** tab contains an icon for you to configure the [proxy action](#).

Policy tab


- **SMTP-proxy connections are:** Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)** and define who appears in the **From** and **To** list (on the **Policy** tab of the proxy definition). See [Set access rules for a policy](#).

Properties tab

- In the **Proxy action** drop-down list, select whether you want to define an action for a client or server. For information about proxy actions, see [About proxy actions](#).
- To define logging for a policy, click **Logging** and [Set logging and notification preferences](#).
- If you set the **SMTP-proxy connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use SMTP. See [Block sites temporarily with policy settings](#).
- If you want to use an idle timeout other than the one set by the Firebox or authentication server, [Set a custom idle timeout](#).

Proxy action settings

WatchGuard proxies have predefined rulesets that provide a good balance of security and accessibility for most installations. If a default ruleset does not meet all of your business needs, you can add, delete, or modify rules.

To modify the settings and rulesets for a proxy action, click the **View/Edit Proxy** icon  (the first icon to the right of the **Proxy action** drop-down list) and select a category of settings from the left side of the dialog box:

- [SMTP proxy: General settings](#)
- [SMTP proxy: Greeting rules](#)
- [SMTP proxy: ESMTP settings](#)
- [SMTP proxy: Authentication](#)
- [SMTP proxy: Content types](#)
- [SMTP proxy: File names](#)
- [SMTP proxy: Mail From/Mail To](#)
- [SMTP proxy: Headers](#)
- [SMTP proxy: Antivirus responses](#)
- [SMTP proxy: Deny message](#)
- [SMTP proxy: Intrusion prevention](#)
- [SMTP proxy: spamBlocker](#)
- [Proxy and AV alarms](#)

Advanced tab

You can use several other options in your proxy definition:

- [Set an operating schedule](#)
- [Apply Traffic Management actions to a policy](#)
- [Set ICMP error handling](#)
- [Apply NAT rules](#) (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- [Enable QoS Marking for a policy](#)
- [Set traffic priority in a policy](#)
- [Add a sticky connection duration to a policy](#)

SMTP proxy: General settings

On the **General Settings** page (the page that first appears after you click the View/Edit Proxy icon), you can set basic SMTP proxy parameters such as idle timeout and message limits.

Clone SMTP Proxy Action Configuration

Name:

Description:

Categories

- General
 - General Settings
 - Greeting Rules
- ESMTP
 - ESMTP Settings
 - Authentication
- Attachments
 - Content Types
 - FileNames
- Address
 - Mail From
 - Rcpt To
- Headers
- Antivirus
- Deny Message
- Intrusion Prevention
- spamBlocker
- Proxy and AV Alarms

General Settings

Idle Timeout

You can set the time between the last traffic through this proxy and when the Firebox closes the connection. If you do not set a limit, the Firebox does not close the connection.

☒ Set the timeout to minutes

Limits

If you set a maximum value for one or more of these limits and the email message is more than that value, the Firebox denies the message.

☒ Set the maximum email recipients to

☐ Set the maximum address length to

☒ Set the maximum email size to kilobytes

☒ Set the maximum email line length to bytes

Hide Email Server

The Firebox can rewrite basic information about your email to help protect it from attack.

☐ Message ID

☒ Server Replies

☐ Rewrite Banner Domain:

☐ Rewrite HELO Domain:

☐ Allow uuencoded attachments

☐ Allow BinHex attachments

☒ Auto-block: source of invalid commands

☐ Turn on logging for reports

OK Cancel Help

Idle timeout

You can set the length of time an incoming SMTP connection can idle before the connection times out. The default value is 10 minutes.

Maximum email recipients

With the **Set the maximum email recipients to** check box, you can set the maximum number of email recipients to which a message can be sent. The Firebox counts and allows the specified number of addresses through, and then drops the other addresses. For example, if you set the value to 50 and there is a message for 52 addresses, the first 50 addresses get the email message. The last two addresses do not get a copy of the message. A distribution list appears as one SMTP email address (for example, support@watchguard.com). The Firebox counts this as one address. You can use this feature to decrease spam email because spam usually includes a large recipient list. Be careful when you do this because you can also deny legitimate email.

Maximum address length

With the **Set the maximum address length to** check box, you can set the maximum length of email addresses.

Maximum email size

With the **Set the maximum email size to** check box, you can set the maximum length of an incoming SMTP message. Most email is sent as 7-bit ASCII text. The exceptions are Binary MIME and 8-bit MIME. 8-bit MIME content (for example, MIME attachments) is encoded with standard algorithms (Base64 or quote-printable encoding) to enable them to be sent through 7-bit email systems. Encoding can increase the length of files by as much as one third. To allow messages as large as 10 KB, you must set this field to a minimum of 1334 bytes to make sure all email gets through.

Maximum email line length

With the **Set the maximum email line length to** check box, you can 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.

Hide Email Server

Select the **Message ID** and **Server Replies** check boxes to replace MIME boundary and SMTP greeting strings in email messages. These are used by hackers to identify the SMTP server vendor and version.

If you have an email server and use the SMTP-Incoming proxy action, you can have the SMTP proxy replace the domain shown in your SMTP server banner with a domain name you select. To do this, next to **Rewrite Banner Domain**, type the domain name you want to use in your banner in the text box that appears. For this to occur, you must also have the **Server Replies** check box selected.

If you use the SMTP-Outgoing proxy action, you can have the SMTP proxy replace the domain shown in the HELO or EHLO greetings. A HELO or EHLO greeting is the first part of an SMTP transaction, when your email server announces itself to a receiving email server. To do this, next to **Rewrite HELO Domain**, type the domain name you want to use in your HELO or EHLO greeting in the text box that appears.

Allow uuencoded attachments

Select this check box if you want the SMTP proxy to allow uuencoded attachments to email messages. Uuencode is an older program used to send binary files in ASCII text format over the Internet. UUencode attachments can be security risks because they appear as ASCII text files but can actually contain executables.

Allow BinHex attachments

Select this check box if you want the SMTP proxy to allow BinHex attachments to email messages. BinHex, which is short for binary-to-hexadecimal, is a utility that converts a file from binary format to ASCII.

Auto-block sources of invalid commands

Select this check box to add senders of invalid SMTP commands to the Blocked Sites list. Invalid SMTP commands often indicate an attack on your SMTP server.

Turn on logging for reports

Select to send a log message for each connection request through SMTP. For WatchGuard Reports to create accurate reports on SMTP traffic, you must select this check box.

If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [Predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

SMTP proxy: Greeting rules

The proxy examines the initial HELO/EHLO responses during the SMTP session initialization. The default rules for the SMTP-Incoming proxy action make sure that packets with greetings that are too long, or include characters that are not correct or expected, are denied. If the default ruleset does not meet all of your business needs, you can add, delete, or modify rules:

1. From the **Categories** section, select **Greeting Rules**.
2. Add, delete, or modify rules, as described in [About working with rules and rulesets](#).
3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify
or

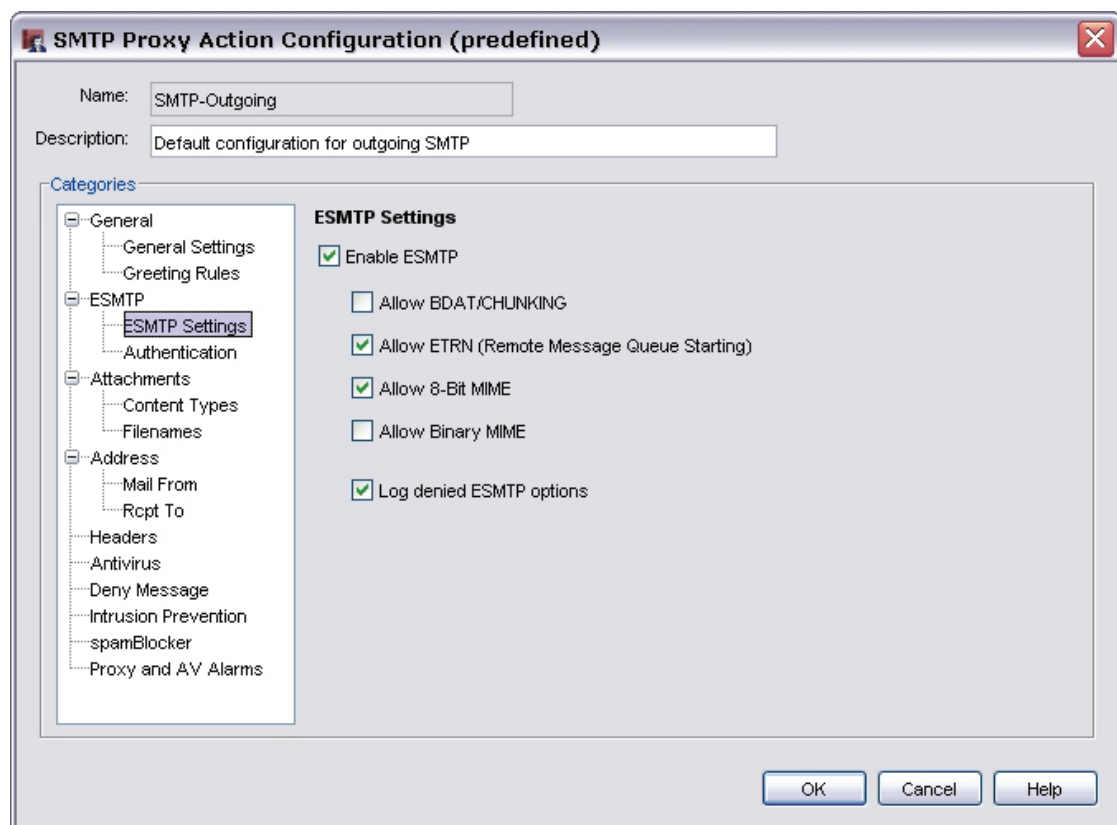
If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

SMTP proxy: ESMTP settings

You use the **ESMTP Settings** fields to set the filtering for ESMTP content. Although SMTP is widely accepted and widely used, some parts of the Internet community have found a need to extend SMTP to allow more functionality. ESMTP gives a method for functional extensions to SMTP, and for servers and clients who support extended features to be identified.

1. From the **Categories** section, select **ESMTP Settings**.



Enable ESMTP

Select to enable the fields below. If you clear this check box, all check boxes below are disabled. However, their settings are saved, and they are restored if this check box is selected again.

Allow BDAT/CHUNKING

Select to allow BDAT/CHUNKING. This enables large messages to be sent more easily through SMTP connections.

Allow ETRN (Remote Message Queue Starting)

This is an extension to SMTP that allows an SMTP client and server to interact to start the exchange of message queues for a given host.

Allow 8-Bit MIME

Select to allow 8-bit MIME, if the client and host give support to the extension. The 8-bit MIME extension allows a client and host to exchange messages made up of text that has octets which are not of the US-ASCII octet range (hex 00-7F, or 7-bit ASCII) that SMTP uses.

Allow Binary MIME

Select to allow the Binary MIME extension, if the sender and receiver accept it. Binary MIME prevents the overhead of base64 and quoted-printable encoding of binary objects sent that use the MIME message format with SMTP. We do not recommend you select this option as it can be a security risk.

Log denied ESMTP options

Select to log, or clear to disable, logging of unknown ESMTP options that are stripped by the SMTP proxy.

2. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

SMTP proxy: Authentication

This ruleset allows these ESMTP authentication types: DIGEST- MD5, CRAM-MD5, PLAIN, LOGIN, LOGIN (old style), NTLM, and GSSAPI. The default rule denies all other authentication types. The RFC that tells about the SMTP authentication extension is RFC 2554.

If the default ruleset does not meet all of your business needs, you can add, delete, or modify rules:

1. From the **Categories** section, select **Authentication**.
2. Add, delete, or modify rules, as described in [About working with rules and rulesets](#).
3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

SMTP proxy: Content types

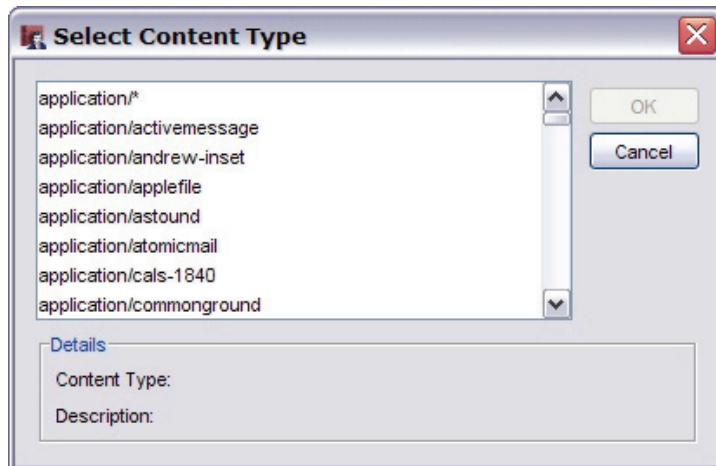
Certain kinds of content embedded in email can be a security threat to your network. Other kinds of content can decrease the productivity of your users. You use the ruleset for the SMTP-Incoming proxy action to set values for incoming SMTP content filtering. You use the ruleset for the SMTP-Outgoing proxy action to set values for outgoing SMTP content filtering. The SMTP proxy allows these content types: text/*, image/*, multipart/*, and message/* . If the default ruleset does not meet all of your business needs, you can add, delete, or modify rules:

1. From the **Categories** section, select **Content Types**.
Select the **Enable content type auto detection** check box for the SMTP proxy to examine content to determine content type. Otherwise, the SMTP proxy uses the value stated in the email header, which clients sometimes set incorrectly. As an example, an attached .pdf file might have a content type stated as application/octet-stream. If you enable content type auto detection, the SMTP proxy recognizes the .pdf file and uses the actual content type, application/pdf. If the proxy does not recognize the content type after it examines the content, it uses the value stated in the email header, as it would if content type auto detection were not enabled. Because hackers often try to disguise executable files as other content types, we recommend that you enable content type auto detection to make your installation more secure.
2. Add, delete, or modify rules, as described in [About rules and rulesets](#).
3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify
or
If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

Add common content types

1. For your convenience, the proxy definition lists several content types that you can easily add to the Content Type ruleset. To bring up the list of common content types, click the **Predefined** button.
The Select Content Type dialog box appears.



2. To add a content type to the ruleset, select it and click **OK**.
To select a range of content types, click the first in the range, press the Shift key, and click the last content type in the range.
To select multiple content types that are not in a range, hold down Ctrl as you select content types.

SMTP proxy: File names

You use the ruleset for the SMTP-Incoming proxy action to put limits on file names for incoming email attachments. You use the ruleset for the SMTP-Outgoing proxy action to put limits on file names for outgoing email attachments. If the default ruleset does not meet all of your business needs, you can add, delete, or modify rules:

1. From the **Categories** section, select **Filenames**.
2. Add, delete, or modify rules, as described in [About working with rules and rulesets](#).
3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

SMTP proxy: Mail From/Mail To

Use the **Mail From** ruleset to put limits on email and allow email into your network only from specified senders. The default configuration is to allow email from all senders. If the default ruleset does not meet all of your business needs, you can add, delete, or modify rules.

The **Mail To** ruleset can limit the email that goes out of your network to only specified recipients. The default configuration allows email to all recipients out of your network. On an SMTP-Incoming proxy action, you can use the Mail To ruleset to prevent people from using your email server for email relaying, as described in [Protect your SMTP server from email relaying](#).

You can also use the **Rewrite As** feature included in this rule configuration dialog box to have the Firebox change the From and To components of your email address to a different value. This feature is also known as SMTP masquerading.

There are two more options available in the **Mail From** and **Mail To** rulesets:

Block source-routed addresses

Select this check box to block a message when the sender address or recipient address contains source routes. A source route identifies the path a message must take when it goes from host to host. The route can identify which mail routers or backbone sites to use. For example, @backbone.com:freddyb@something.com means that the host named Backbone.com must be used as a relay host to deliver mail to freddyb@something.com. By default, this option is enabled for incoming SMTP packets and disabled for outgoing SMTP packets.

Block 8-bit characters

Select this check box to block a message that has 8-bit characters in the sender user name or recipient user name. This allows an accent on an alphabet character. By default, this option is enabled for incoming SMTP packets and disabled for outgoing SMTP packets.

1. From the **Categories** section, select **Mail From** or **Mail To**.
2. Add, delete, or modify rules, as described in [About working with rules and rulesets](#).
3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [Predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

SMTP proxy: Headers

Header rulesets allow you to set values for incoming or outgoing SMTP header filtering. If the default ruleset does not meet all of your business needs, you can add, delete, or modify rules:

1. From the **Categories** section, select **Headers**.
2. Add, delete, or modify rules, as described in [About working with rules and rulesets](#).
3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [Predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

Configure Gateway AntiVirus actions

When you enable Gateway AntiVirus, you must set the actions to be taken if a virus or error is found in an email message (SMTP or POP3 proxies), web page (HTTP proxy), or uploaded or downloaded file (FTP proxy). The options for antivirus actions are:

Allow

Allows the packet to go to the recipient, even if the content contains a virus.

Deny (FTP proxy only)

Deny the file and send a deny message.

Lock (SMTP and POP3 proxies only)

Locks the attachment. This is a good option for files that cannot be scanned by the Firebox. A file that is locked cannot be opened easily by the user. Only the administrator can unlock the file. The administrator can use a different antivirus tool to scan the file and examine the content of the attachment. For information on how to unlock a file locked by Gateway AntiVirus, see [Unlock a file locked by Gateway AntiVirus](#).

Quarantine (SMTP proxy only)

When you use the SMTP proxy with the spamBlocker security subscription, you can send email messages with viruses or possible viruses to the Quarantine Server. For more information on the Quarantine Server, see [About the Quarantine Server](#). For information on how to set up Gateway AntiVirus to work with the Quarantine Server, see [Configure Gateway AntiVirus to quarantine email](#).

Remove (SMTP and POP3 proxies only)

Removes the attachment and allows the message through to the recipient.

Drop (not supported in POP3 proxy)

Drops the packet and drops the connection. No information is sent to the source of the message.

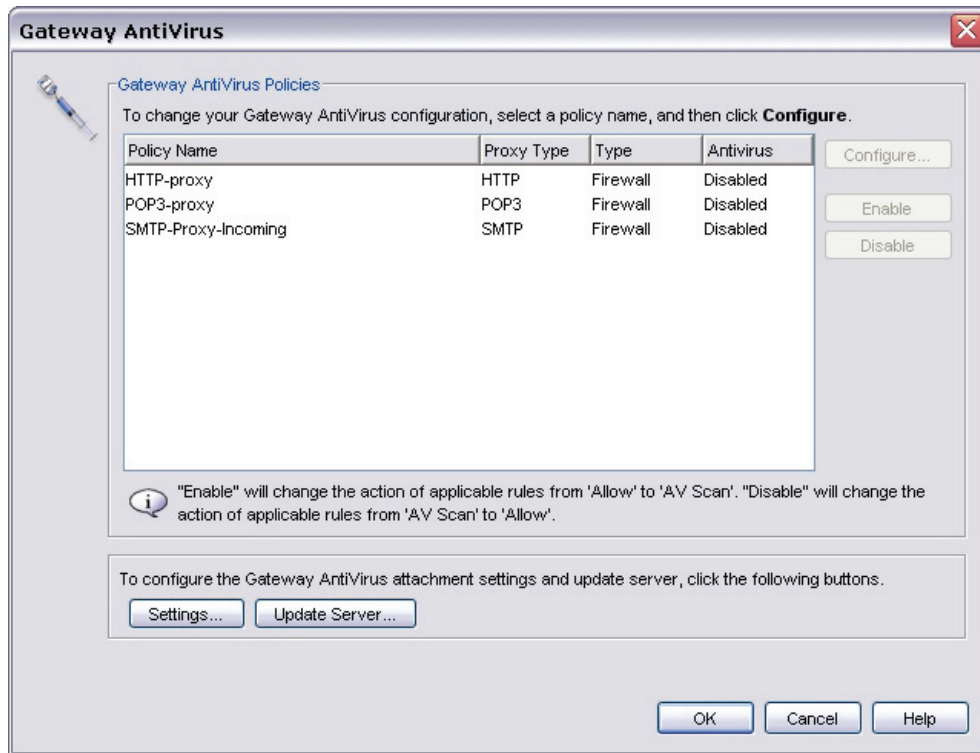
Block (not supported in POP3 proxy)

Blocks the packet, and adds the IP address of the sender to the Blocked Sites list.

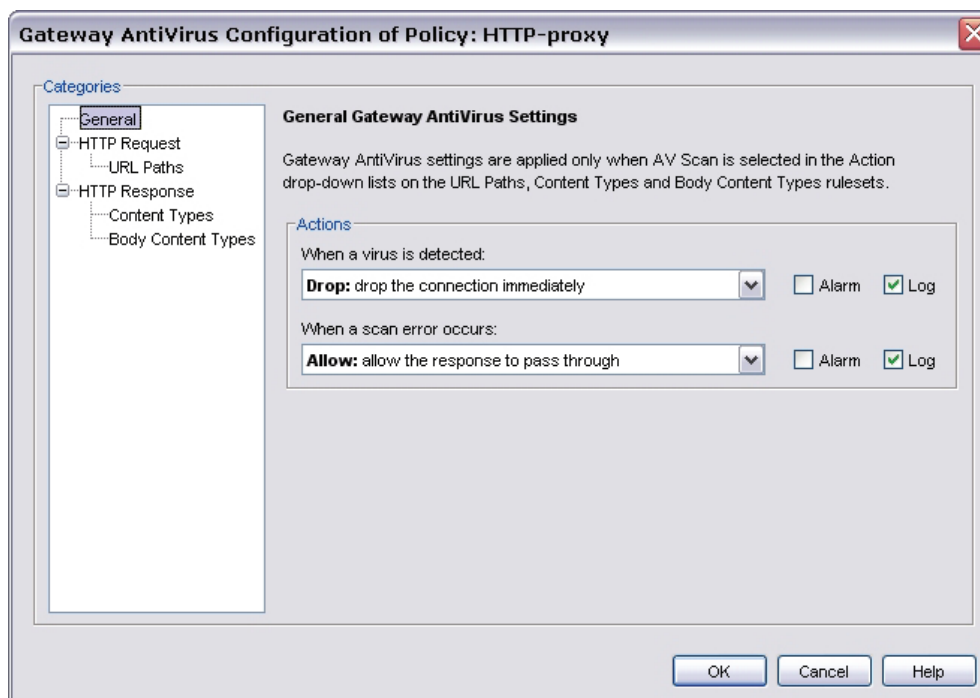


If you set the configuration to allow attachments, your configuration is less secure.

1. From Policy Manager, select **Tasks > Gateway AntiVirus > Configure**.
The Gateway AntiVirus dialog box appears, which lists the proxies that have already been created.



2. Select the policy you want to configure and click **Configure**.
The General Gateway Antivirus Settings page for that policy appears.
Or, instead of step 1 and 2, you can go to the same page from the proxy definition screens. From the **Categories** section in the proxy definition, select **AntiVirus**.



3. Set the action the Firebox takes if a virus is detected in an email message, file, or web page, in the **When a virus is detected** drop-down list. See the beginning of this section for a description of the proxy actions.
4. Set the action the Firebox takes when it cannot scan an object or an attachment in the **When a scan error occurs** drop-down list. Attachments that cannot be scanned include binhex-encoded messages, certain encrypted files, or files that use a type of compression that we do not support such as password-protected Zip files. See the beginning of this section for a description of the proxy actions.
5. (FTP proxy only) You can limit file scanning up to a specified kilobyte count. Any additional bytes in the file are not scanned. This allows the proxy to partially scan very large files without a large effect on performance. Enter the limit in the **Limit scanning to first** field.

Create alarms or log entries for antivirus actions

An alarm is a mechanism to tell users when a proxy rule applies to network traffic. Use the **Alarm** check box on the AntiVirus page of a proxy definition to create an alarm when the adjacent action occurs. If you do not want an alarm for the antivirus action, clear the **Alarm** check box for that action.

FTP Proxy Action Configuration (predefined)

Name:

Description:

Categories

- General
- Commands
- Download
- Upload
- Antivirus**
- Intrusion Prevention
- Proxy and AV Alarm

Antivirus

Gateway AntiVirus settings are applied only when the Action drop-down lists on the 'Upload' and 'Download' rulesets is set to 'AV Scan'.

Actions

When virus is detected:

☐ Alarm ☒ Log

When a scan error occurs:

☐ Alarm ☒ Log

File Scan

Use this setting to limit the number of bytes to scan at the start of each file. The Firebox does not scan data past this limit. This allows large files to pass with partial scanning.

☐ Limit scanning to first kilobyte(s)

OK Cancel Help

To use the alarm feature successfully, you must also configure the type of alarm to use in each proxy policy. To configure the alarm type to use, use the Proxy and AV Alarms category for the proxy. For information about the settings for this category, see [Set logging and notification preferences](#).

If you want to record log messages for a proxy action, select the **Log** check box for the antivirus response. If you do not want to record log messages for an antivirus response, clear the **Log** check box.

SMTP proxy: Deny message

The Firebox gives a default deny message that replaces denied content. You can replace that deny message with one that you write. The first line of the deny message is a section of the HTTP header. You must include an empty line between the first line and the body of the message.

1. From the **Categories** section, select **Deny Message**.
2. In the **Deny Message** block, you can write a custom plain text message with standard HTML that will appear in the recipient email when the proxy blocks that email. You can use these variables:

`%(reason)%`

Puts the cause for the Firebox to deny the content.

`%(type)%`

Puts the type of content that was denied.

`%(filename)%`

Puts the file name of the denied content.

`%(virus)%`

Puts the name or status of a virus, for Gateway AntiVirus users only.

`%(action)%`

Puts the name of the action taken: lock, strip, and so on.

`%(recovery)%`

Puts whether you can recover the attachment.

3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

Intrusion prevention in proxy definitions

An *intrusion* is a direct attack on your computer. These attacks can cause damage to your network, get sensitive information, or use your computers to attack other networks.


To help protect your network from intrusions, you can purchase the optional Intrusion Prevention Service (IPS) for the Firebox. Intrusion Prevention Service operates with the SMTP, POP3, HTTP, FTP, DNS, and TCP-UDP proxies.

You can activate and configure IPS in two ways:

Run the Activate Intrusion Prevention wizard from the Tasks menu in Policy Manager

For more information, see [Activate Intrusion Prevention Service \(IPS\)](#).

Use the Intrusion Prevention ruleset in the proxy definition

1. [Get a feature key](#) for IPS from LiveSecurity Service and [add the feature key to the Firebox](#).
2. [Add a proxy policy to your Firebox configuration](#). Or, you can edit an existing proxy.
3. From the **Properties** tab of the **New/Edit Policy Properties** dialog box, click the **View/Edit Proxy** icon  (the first icon to the right of the **Proxy action** drop-down list).
4. Select the **Intrusion Prevention** category from the left side of the window. On the right side of the window, [set parameters for Intrusion Prevention Service \(IPS\)](#).

SMTP proxy: 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 increases your capacity to catch spam at the edge of your network when it tries to come into your system. If you have purchased and enabled the spamBlocker feature, the fields in the spamBlocker category set the actions for email messages identified as spam.

Although you can use the proxy definition screens to activate and configure spamBlocker, it is easier to use the **Tasks** menu in Policy Manager to do this. For more information on how to do this, or to use the spamBlocker screens in the proxy definition, see the topic [About spamBlocker](#).

Proxy and AV alarms

An alarm is an event that triggers a *notification*, which is a mechanism to tell a network administrator about a condition in the network. In a proxy definition, an alarm might occur when traffic matches, or does not match, a rule in the proxy, and the **If matched** or **None matched** field under **Actions to take** in the ruleset definitions is set to an action other than **Allow**.

For example, the default definition of the FTP proxy has a rule that denies the download of files whose file types match any of these patterns: .cab, .com, .dll, .exe, and .zip. You can specify that an alarm is generated whenever the Firebox takes the **Deny** action because of this rule.

For each proxy, you can define what the Firebox does when an alarm occurs.


1. From the **Categories** section of the proxy definition, select **Proxy and AV Alarm**.
2. You can define the Firebox to send an SNMP trap, a notification to a network administrator, or both. The notification can either be an email to a network administrator or a pop-up window on the administrator's management station.
For more information on the Proxy and AV alarm fields, see [Set logging and notification preferences](#).
3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.
or
If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.
The New Policy Properties dialog box appears.

Protect your SMTP server from email relaying

Email relaying, also called “mail spamming” or open mail relay, is an intrusion in which a person uses your email server, address, and other resources to send large amounts of spam email. This can cause system crashes, equipment damage, and financial loss.

If you are not familiar with the issues involved with mail relaying, or are unsure whether your email server is vulnerable to mail relaying, we recommend you do research on your own email server and learn its potential vulnerabilities. The Firebox can give basic mail relay protection if you are unsure of how to configure your email server. However, you should work toward using your email server to prevent email relaying.

Before you start this procedure, you must know the names of all domains that your SMTP email server receives email for.

1. [Add an SMTP proxy policy to your Firebox configuration.](#)
2. Click the **View/Edit Proxy** icon  (the first icon to the right of the **Proxy action** drop-down list). *The SMTP Proxy Action Configuration dialog box appears.*
3. From the **Categories** list on the left, select **Addresses > Rcpt To**.
4. In the **Pattern** text box, type the asterisk character * followed by @your-domain-name. Click **Add**. Your rule appears in the list. Because of the wildcard * character, any email address that ends with @your-domain-name is allowed. If your email server accepts email for more than one domain, you can add more domains here. For example, if you add both *@watchguard.com and *@*.watchguard.com to the list, your email server will accept all email destined to the watchguard.com top-level domain and all email destined to sub-domains of watchguard.com such as rnd.watchguard.com.
5. Make sure the **None Matched** drop-down list in the **Actions to Take** block is set to **Deny**. This means that any email destined to an address other than the domains in the list will be denied.
6. Click **OK**. Edit the name of the new proxy action and click **OK**.
7. Click **OK** again to close the SMTP policy definition. Click **Close** and [save the configuration file](#).

Configure the SMTP proxy to quarantine email

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 filtered by spamBlocker.

To configure the SMTP proxy to quarantine email:

1. Add the SMTP proxy to your configuration and enable spamBlocker from the proxy definition. Or, enable spamBlocker and select to enable it for the SMTP proxy.
2. When you set the actions spamBlocker applies for different categories of email (as described in [Configure spamBlocker](#)), make sure you select the **Quarantine** action for at least one of the categories. When you select this action, you are prompted to configure the Quarantine Server if you have not already done so.

You can also select the **Quarantine** action for email messages identified by Virus Outbreak Detection as containing viruses. For more information, see [Configure Virus Outbreak Detection \(VOD\) actions](#).

Finish and save the configuration

1. When you are done with all changes for all categories of the proxy, click **OK** to close the **New Policy Properties** or **Edit Policy Properties** dialog box.
2. Save the configuration to the Firebox. To do this, select **File > Save > To Firebox**. *The Save dialog box appears with the default location for configuration files. You can change the name of the configuration file if you choose.*
3. Click **Save**.
4. You are prompted for the configuration passphrase. Type it and click **OK**.

About the TCP-UDP proxy

The TCP-UDP proxy is included for these protocols on non-standard ports: HTTP, HTTPS, SIP, and FTP. For these protocols, the TCP-UDP proxy relays the traffic to the correct proxies for the protocols or allows you to allow or deny traffic. For other protocols, you can select to allow or deny traffic.

To add the TCP-UDP proxy to your Firebox configuration, see [Add a proxy to your Firebox configuration](#). Then, if you need to change the proxy definition to meet your business needs, you can use the **New/Edit Policy Properties** dialog box to modify the definition. The fields on this dialog box are divided into three tabs: **Policy**, **Properties**, and **Advanced**. In addition, the **Properties** tab contains an icon for you to configure the [proxy action](#).

Policy tab


- **TCP-UDP-proxy connections are:** Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)** and define who appears in the **From** and **To** list (on the **Policy** tab of the proxy definition). See [Set access rules for a policy](#).
- **Use policy-based routing:** If you want to use policy-based routing in your proxy definition, see [Configure policy-based routing](#).

Properties tab

- In the **Proxy action** drop-down list, select whether you want to define an action for a client or server. For information about proxy actions, see [About proxy actions](#).
- To define logging for a policy, click **Logging** and [Set logging and notification preferences](#).
- If you set the **TCP-UDP-proxy connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use TCP-UDP. See [Block sites temporarily with policy settings](#).
- If you want to use an idle timeout other than the one set by the Firebox or authentication server, [Set a custom idle timeout](#).

Proxy action settings

WatchGuard proxies have predefined rulesets that provide a good balance of security and accessibility for most installations. If a default ruleset does not meet all of your business needs, you can add, delete, or modify rules.

To modify the settings and rulesets for a proxy action, click the **View/Edit Proxy** icon  (the first icon to the right of the **Proxy action** drop-down list) and select a category of settings from the left side of the dialog box:

- [TCP-UDP proxy: General settings](#)
- [TCP-UDP proxy: Application blocking](#)
- [TCP-UDP proxy: Intrusion prevention](#)
- [Proxy alarm](#). SNMP traps and notification are disabled by default.

Advanced tab

You can use several other options in your proxy definition:

- [Set an operating schedule](#)
- [Apply Traffic Management actions to a policy](#)
- [Set ICMP error handling](#)
- [Apply NAT rules](#) (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- [Enable QoS Marking for a policy](#)
- [Set traffic priority in a policy](#)
- [Add a sticky connection duration to a policy](#)

TCP-UDP proxy: General settings

On the **General** page (the page that first appears after you click the View/Edit Proxy icon), you set basic parameters for the TCP-UDP proxy.

HTTP

Select whether to allow or deny, or which HTTP proxy action to use for, TCP-UDP connections identified as HTTP traffic.

HTTPS

Select whether to allow or deny, or which HTTPS proxy action to use for, TCP-UDP connections identified as HTTPS traffic.

SIP

Select whether to allow or deny, or which SIP proxy action to use for, TCP-UDP connections identified as SIP traffic.

FTP

Select whether to allow or deny, or which FTP proxy action to use for, TCP-UDP connections identified as FTP traffic.

Other protocols

Select whether to allow or deny TCP-UDP connections identified as other protocols.

Turn on logging for reports

Creates a traffic log message for each transaction. This option creates a large log file, but this information is very important if your firewall is attacked. If you do not select this check box, you do not see detailed information about these proxy connections in WatchGuard Reports.

TCP-UDP proxy: Application blocking

You use this ruleset to define actions the Firebox takes when the TCP-UDP proxy detects Instant Messaging (IM) or Peer to Peer (P2P) services. The TCP-UDP proxy finds these IM services: AOL Instant Messenger (AIM), ICQ, IRC, MSN Messenger, and Yahoo! Messenger. It finds these types of P2P services: BitTorrent, eDonkey2000 (Ed2k), Gnutella, Kazaa, Napster, and Phatbot.

You do not need to purchase Intrusion Prevention Service to use the application blocking feature.

1. From the **Categories** section of the TCP-UDP proxy, select **Application Blocking**.
2. On the **IM** tab, use the drop-down list to select the Firebox action when it detects Instant Messaging (IM) use:
 - Allow*
Allows the packet to go to the recipient, even if the content matches a signature.
 - Deny*
Drops the packet and sends a TCP reset packet to the sender.
3. Use the check boxes to select individual IM applications whose traffic you want the Firebox to take the actions for. If you want to select all the IM applications, select **All Categories**. All the applications are then automatically selected. You can clear a check boxes any applications you do not want to restrict, if you choose.

4. To define actions for P2P applications, click the **P2P** tab. Use the information in steps 2 and 3, above, to set actions and categories.
5. Click **Logging and Notification** to configure logging and notification for IPS. For information on the dialog box that appears, see [Set logging and notification preferences](#).
6. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.
or
If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

Intrusion prevention in proxy definitions

An *intrusion* is a direct attack on your computer. These attacks can cause damage to your network, get sensitive information, or use your computers to attack other networks.


To help protect your network from intrusions, you can purchase the optional Intrusion Prevention Service (IPS) for the Firebox. Intrusion Prevention Service operates with the SMTP, POP3, HTTP, FTP, DNS, and TCP-UDP proxies.

You can activate and configure IPS in two ways:

Run the Activate Intrusion Prevention wizard from the Tasks menu in Policy Manager

For more information, see [Activate Intrusion Prevention Service \(IPS\)](#).

Use the Intrusion Prevention ruleset in the proxy definition

1. [Get a feature key](#) for IPS from LiveSecurity Service and [add the feature key to the Firebox](#).
2. [Add a proxy policy to your Firebox configuration](#). Or, you can edit an existing proxy.
3. From the **Properties** tab of the **New/Edit Policy Properties** dialog box, click the **View/Edit Proxy** icon  (the first icon to the right of the **Proxy action** drop-down list).
4. Select the **Intrusion Prevention** category from the left side of the window. On the right side of the window, [set parameters for Intrusion Prevention Service \(IPS\)](#).

Finish and save the configuration

1. When you are done with all changes for all categories of the proxy, click **OK** to close the **New Policy Properties** or **Edit Policy Properties** dialog box.
2. Save the configuration to the Firebox. To do this, select **File > Save > To Firebox**.
The Save dialog box appears with the default location for configuration files. You can change the name of the configuration file if you choose.
3. Click **Save**.
4. You are prompted for the configuration passphrase. Type it and click **OK**.

About the TFTP proxy

Trivial File Transfer Protocol (TFTP) is a simple form of FTP that uses very small amounts of memory. It is used to transfer small files between hosts on the same network. Some manufacturers use the TFTP protocol to send periodic updates to 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.

To add the TFTP proxy to your Firebox configuration, see [Add a proxy to your Firebox configuration](#). Then, if you need to change the proxy definition to meet your business needs, you can use the **New/Edit Policy Properties** dialog box to modify the definition. The fields on this dialog box are divided into three tabs: **Policy**, **Properties**, and **Advanced**. In addition, the **Properties** tab contains an icon for you to configure the [proxy action](#).

Policy tab

- **TFTP-proxy connections are:** Specify whether connections are **Allowed**, **Denied**, or **Denied (send reset)** and define who appears in the **From** and **To** list (on the **Policy** tab of the proxy definition). See [Set access rules for a policy](#).
- **Use policy-based routing:** If you want to use policy-based routing in your proxy definition, see [Configure policy-based routing](#).


Properties tab

In the **Proxy action** drop-down list, select whether you want to define an action for a client or server. The TFTP proxy has only one predefined proxy action: TFTP-Client. For information about proxy actions, see [About proxy actions](#).

- To define logging for a policy, click **Logging** and [Set logging and notification preferences](#).
- If you set the **TFTP-proxy connections are** drop-down list (on the **Policy** tab) to **Denied** or **Denied (send reset)**, you can block sites that try to use TFTP. See [Block sites temporarily with policy settings](#).
- If you want to use an idle timeout other than the one set by the Firebox or authentication server, [Set a custom idle timeout](#).

Proxy action settings

WatchGuard proxies have predefined rulesets that provide a good balance of security and accessibility for most installations. If a default ruleset does not meet all of your business needs, you can add, delete, or modify rules.

To modify the settings and rulesets for a proxy action, click the **View/Edit Proxy** icon  (the first icon to the right of the **Proxy action** drop-down list) and select a category of settings from the left side of the dialog box:

- [TFTP proxy: General settings](#)
- [TFTP proxy: Upload and download content](#)
- [Proxy and AV alarms](#). SNMP traps and notification are disabled by default.

Advanced tab

You can use several other options in your proxy definition:

- [Set an operating schedule](#)
- [Apply Traffic Management actions to a policy](#)
- [Set ICMP error handling](#)
- [Apply NAT rules](#) (Both 1-to-1 NAT and dynamic NAT are enabled by default in all policies.)
- [Enable QoS Marking for a policy](#)
- [Set traffic priority in a policy](#)
- [Add a sticky connection duration to a policy](#)

TFTP proxy: General settings

On the **General** page (the page that first appears after you click the View/Edit Proxy icon), you can set basic TFTP parameters.

1. From the **Categories** section, select **General**.
2. To create a log message for each transaction, select the **Turn on logging for reports** check box. You must select this option to get detailed reports on TFTP traffic with WatchGuard Reports.
3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

TFTP proxy: Upload and download content

You can control the type of files that the TFTP 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 TFTP server, you could add *.wma to the proxy definition and specify that these files are denied. Use the asterisk (*) as a wild card.

The TFTP proxy has only one predefined proxy action: TFTP-Client. Use the TFTP-Client proxy action to set rules for users connecting to external TFTP servers.

1. From the **Categories** section, select **Upload** or **Download**.
2. Add, delete, or modify rules, as described in [About rules or rulesets](#).
3. If you want to change settings for one or more other categories in this proxy, go to the topics on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

Proxy and AV alarms

An alarm is an event that triggers a *notification*, which is a mechanism to tell a network administrator about a condition in the network. In a proxy definition, an alarm might occur when traffic matches, or does not match, a rule in the proxy, and the **If matched** or **None matched** field under **Actions to take** in the ruleset definitions is set to an action other than **Allow**.

For example, the default definition of the FTP proxy has a rule that denies the download of files whose file types match any of these patterns: .cab, .com, .dll, .exe, and .zip. You can specify that an alarm is generated whenever the Firebox takes the **Deny** action because of this rule.

For each proxy, you can define what the Firebox does when an alarm occurs.

1. From the **Categories** section of the proxy definition, select **Proxy and AV Alarm**.
2. You can define the Firebox to send an SNMP trap, a notification to a network administrator, or both. The notification can either be an email to a network administrator or a pop-up window on the administrator's management station.
For more information on the Proxy and AV alarm fields, see [Set logging and notification preferences](#).
3. If you want to change settings for one or more other categories in this proxy, go to the section in this document on the next category you want to modify.

or

If you are finished with your changes to this proxy definition, click **OK**. If the proxy action you have modified is a predefined one, you must clone (copy) your settings to a new action. (For more information on predefined user actions, see [About predefined and user-defined proxy actions](#).) Enter a name for the new action and click **OK**.

The New Policy Properties dialog box appears.

About import and export functions for proxies

WatchGuard proxies support several import and export functions:

[About predefined and user-defined proxy actions](#): If you manage several Fireboxes and have user-defined proxy actions for them, you can define custom proxy actions on one Firebox, export them to an ASCII file, and then import them to another Firebox.

[Import and export rulesets](#): If you want to copy rulesets between or within proxies, you can define the rules once for one proxy or category, export them to an XML file, and then import them to a new proxy or category.

Import and export user-defined proxy actions

If you manage several Fireboxes and have user-defined proxy actions for them, you can use the policy action import/export function to save time. You can define custom proxy actions on one Firebox, export them to an ASCII file, and then import them to another Firebox.

The Firebox for which you created the policies must run the same version of WSM as the version of Policy Manager you use to import the proxy actions. You cannot import a proxy action from an old version into the current version.

1. On the first Firebox, create the user-defined proxy actions that you need.
2. From the **Proxy Actions** dialog box, click **Export**. You do not need to select the user-defined actions. The Export function automatically exports all custom actions regardless of which proxy action is actually selected.
3. In the **Save** dialog box, select where you want to save the proxy actions file. Type a name for the file and click **Save**.
The default location is My Documents > My WatchGuard.
4. From Policy Manager on a different Firebox, from the **Proxy Actions** dialog box, click **Import**.
5. Find the file you created in step 3 and click **Open**.
6. If user-defined proxy actions are already defined in the current Policy Manager, you are asked whether you want to replace the existing actions or append the imported actions to the existing ones. Click **Replace** or **Append**.
If you click **Replace**, the existing user-defined proxy actions are deleted and replaced with the new actions.
If you click **Append**, both the existing and the imported actions are listed in on the dialog box.

Import and export rulesets

If you want to copy rulesets between or within proxies, you can define the rules once for one proxy or category, export them to an XML file, and then import them to a new proxy or category. For example, you can export the Content Types ruleset of an HTTP proxy action, and then import it to the Content Types ruleset of an SMTP proxy action. Or, you can export the SMTP Mail From ruleset to the SMTP Mail To ruleset.

You can copy rulesets only between proxies or categories within these four groups. Other combinations are not compatible.

Content Types	Filenames	Addresses	Authentication
HTTP Content Types	FTP Download	SMTP Mail From	SMTP Authentication
SMTP Content Types	FTP Upload	SMTP Mail To	POP3 Authentication
POP3 Content Types	HTTP URL Paths		
	SMTP Filename		
	POP3 Filenames		

1. Create the rulesets that you need for one proxy or category.
2. If necessary, click **Change View** to see the advanced view of the ruleset. Click **Export**.
3. In the **Save** dialog box, select where you want to save the XML file. Type a name for the file and click **Save**.
The default location is My Documents > My WatchGuard.
4. From the new proxy or category, click **Import**.
5. Find the file you created in step 2 and click **Open**.
6. If rules are already defined in the new category or proxy, you are asked whether you want to clear the old ruleset first.
If you click **Yes**, the existing rules are deleted and replaced with the new ones.
If you click **No**, both the existing and the imported rules are included in the ruleset.

16 WatchGuard Reports

About the Report Server

The Report Server consolidates data collected by your Log Servers from your Firebox devices and then generates reports from that data. After the data is on the Report Server, you can use Report Manager to see the available reports.

For more information about the Report Manager, see [About the Report Manager](#).

For more information about the available reports, see [Predefined Reports List](#).

Set up the Report Server

You can use WatchGuard System Manager installation program to install the Report Server on the computer you are using as a management station, or you can install the Report Server software on a different computer. You can also add additional Report Servers for backup.

If you install the Report Server on a computer with a firewall other than Windows Firewall, you must open the ports necessary for the servers to connect through the firewall. Windows Firewall users do not have to modify their firewall configuration. For more information, see [Install WatchGuard Servers on computers with desktop firewalls](#).

About passphrases

All WatchGuard servers share the same master passphrase and server management passphrase. If you set up another server first, you do not have to set the passphrase again when you set up the Report Server.



If you have already run the Report Server Setup Wizard, the wizard sets up the Report Server with no input required.


Install the Report Server

You can install the Report Server on your management station or on another computer.

Run the WatchGuard System Manager installation program, and select only the Report Server component.

Run the setup wizard

If you run the Report Server Setup Wizard from a remote desktop connection to a Windows 2000 or Windows 2003 Server Terminal Services session, the PostgreSQL database fails to install if you do not open the remote desktop session as a console or remote administration session, and configure Terminal services to run in Remote Administration Mode.

1. Right-click  in the system tray and select **Setup Wizard**.
The Report Server Setup Wizard appears.
2. If you have already set up a WatchGuard server, the Report Server Setup Wizard shows only a screen that tells you the wizard is configuring your server.
If you have not yet run a server setup wizard, the Report Server Setup Wizard shows these screens:
 - Create a master passphrase
The master passphrase encrypts all Management 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.
3. Click through the wizard and add the information it asks for.




Select the **Data directory path** carefully. After you have installed the database you cannot change the directory location through the Report Server user interface.

To modify the default settings of the Report Server to best meet the needs of your installation, see [Configure the Report Server](#).

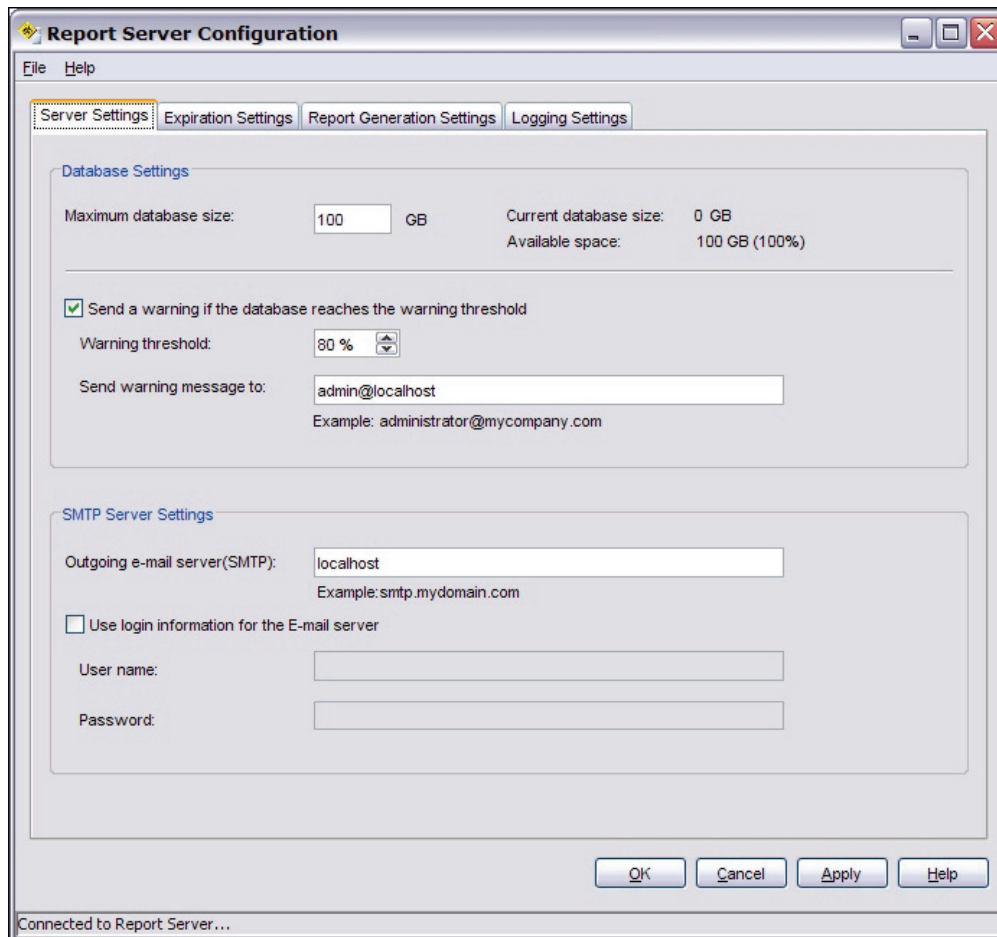
Configure the Report Server

If you have not yet set up the Report Server, you cannot configure it yet. [Set up the Report Server](#), and then follow these steps to configure the server.

1. Right-click  in the system tray and select **Configure**. Type the server management passphrase.
The Report Server Configuration dialog box appears.
2. If necessary, change the default settings as appropriate for your network. When you are finished, click **OK**.

Server settings

You can configure settings for your Report Server database and SMTP server.



Database settings

Maximum database size

Type the maximum size for the Report Server database.

The dialog box displays the current size of the database and the number of GB currently available.

Send a warning if the database reaches the warning threshold

If you want to receive a warning message when the database is near its limit, select this check box.

Warning threshold

To specify when the database sends you a threshold warning message, press the up or down arrows.

Send warning message

Type the email address where you want to send the threshold warning message.

For example, if you select to receive a warning message, use the default warning threshold of 90%, and use the default maximum database size of 10000 MB, the Report Server sends the warning message when 9000 MB have been used and only 1000 MB are available.



*When the Report Server database is regularly purged, and the number of records sent to the server remains fairly constant, space freed by the purge process is simply reused by subsequent reports. However, if the purge interval (defined in the **Retain log messages for** field on the **Expiration settings** tab of the **Report Server Configuration** dialog box) is reduced, or debug logging is disabled after being used for a period of time, we recommend you use the vacuumdb command-line utility to [Reclaim free space from the Report Server database](#).*

SMTP server settings

Outgoing email server (SMTP)

Type the address of the outgoing SMTP email server.

Use login information for the email server

If your email server requires authentication, select this check box.

User name

Type the user name for the email server.

Password

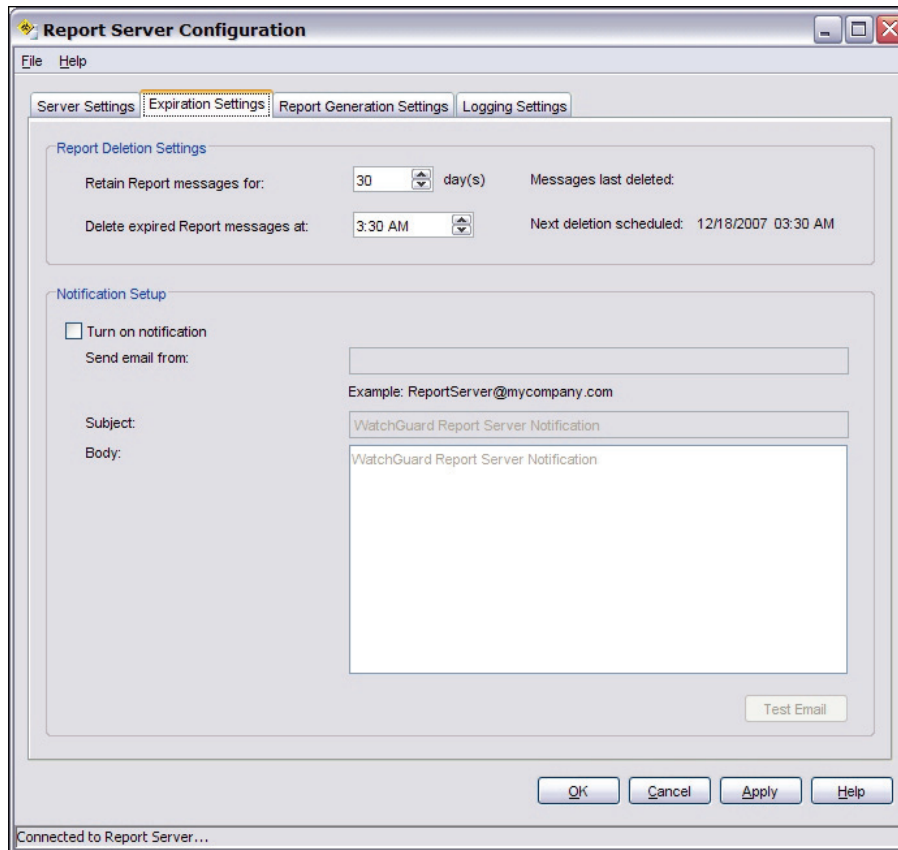
Type the password for the email server.



If the user name and password are not required for your SMTP server, you can leave the fields blank.

Expiration settings

You can configure report deletion and notification setup settings for your Report Server.



Report deletion settings

Retain Report messages for

To specify the number of days messages remain on the Report Server, press the up or down arrows.
The dialog box shows the date messages were last deleted.

Delete expired Report messages at

To set the time of day the expired messages are deleted, press the up or down arrows.
The dialog box shows the date and time of the next scheduled deletion.

Notification setup

Turn on notification

Select this check box to enable email notifications.

Send email from

Type the full email address of the account you want to send notifications from.

Subject

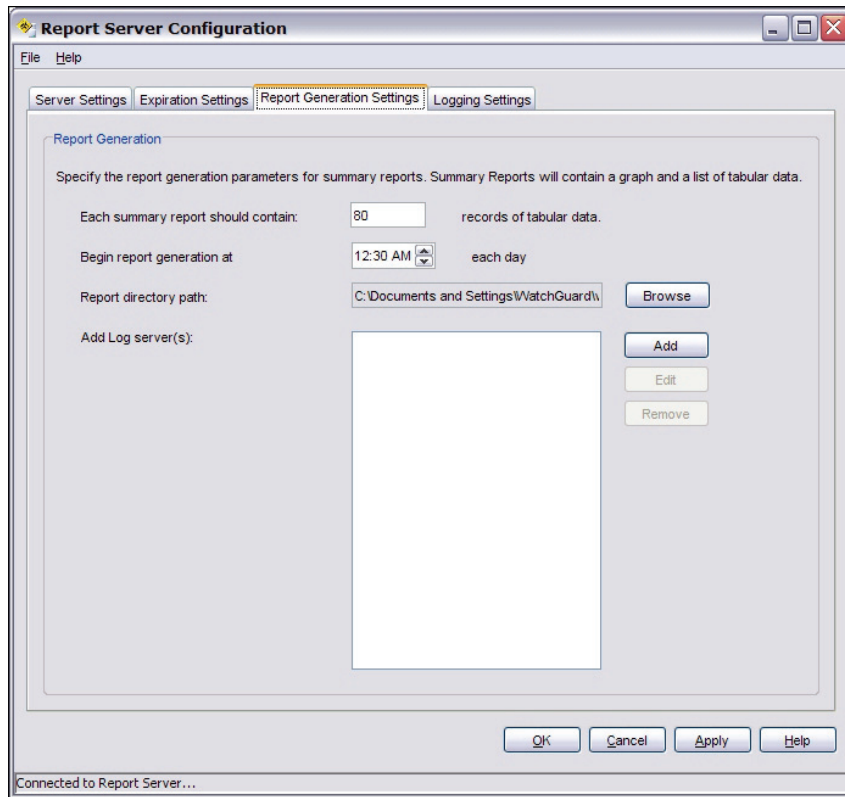
Type the subject line you want users to see when they receive a notification email.

Body

Type the message you want users to see. You can use plain text or HTML when typing the message body.

Report generation settings

You can configure report generation settings for your Report Server.
These selections apply only to summary report data.



Each summary report should contain

Type the number of records you want to appear in summary reports.
This setting applies to Summary reports only.

Begin generating weekly reports at

To set the day you want the report to be generated, click the drop-down list and select a day.
To set the time of day you want the report to begin, press the up or down arrows.

Select report type

To specify the reports to include in the list, select the check box next to each of the reports you want to see when reports are generated.

Run Now

Click this button to immediately generate all selected reports.

After you click **Run Now**, a Report Generation message appears to indicate that the report generation is in process and may take a few minutes to complete. When the report generation is complete, another Report Generation message appears to indicate the report is ready. Click **Run Now** again to see the report.



Because the log server and the Report Server logs are not always synchronized, it may take up to 15 minutes for the reports to generate.

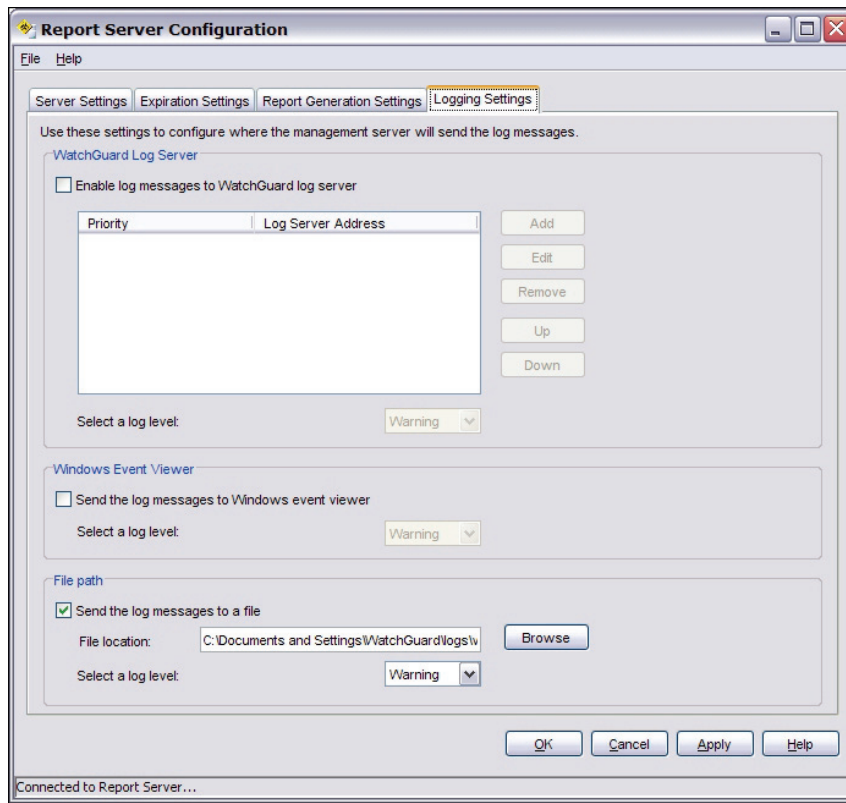
Add Log server(s)

The Report Server can collect data from more than one Log Server. Click **Add** to add a log server to the list. Type the IP address and the passphrase for the Log Server.

Report directory path

Specify the directory for report files.

Logging settings



Enable log messages to WatchGuard log server

Select this check box to enable the Log Server to collect log data from your Firebox devices.

Select a log level

If you selected the **Enable log messages to WatchGuard log server** check box, you can select the level that is assigned to log messages.

- Error
- Information
- Warning
- Debug

Send the log messages to Windows event viewer

Select this check box to enable Log Server to send messages to event viewer.

Select a log level

If you selected the **Send the log messages to Windows event viewer** check box, you can select the level that is assigned to log messages:

- Error
- Information
- Warning
- Debug

Send the log messages to a file

This check box is selected by default. You can clear this check box to discard log messages.

File location

If you selected the **Send the log messages to a file** check box, you can select the location where log messages will be stored.

Select a log level

If you selected the **Send the log messages to a file** check box, you can select the level that is assigned to log messages:

- Error
- Information
- Warning
- Debug

Reclaim free space from the Report Server database

When the Report Server database is regularly purged, and the number of records sent to the server remains fairly constant, space freed by the purge process is simply reused by subsequent reports. However, if the purge interval (defined in the **Retain log messages for** field on the [Expiration settings tab of the Report Server Configuration dialog box](#)) is reduced, or debug logging is disabled after being used for a period of time, we recommend you use the vacuumdb command-line utility. This utility reduces the physical file size of the database by marking for reuse the objects that were purged.

The vacuumdb utility can also be used to [Reclaim free space from the Log Server database](#).


To run the vacuumdb utility:

1. Stop the Report Server.
2. From the command line, run:
`C:\Program Files\WatchGuard\wsm10.0\postgresql\bin\vacuumdb -v -f -d wgrep -U wguser.`
(You can omit the `-v` option to disable verbose output.)
3. When prompted, enter the server management passphrase.


Depending on the size of the database, the operation can take from a few minutes to several hours to run. After the command finishes, restart the Report Server.

Start or stop the Report Server

You can start or stop the Report Server service at any time without disconnecting from your Report Server.

To start service, right-click  in your system tray and select **Start Service**.
Or you can select **File > Start Server** in the Report Server Configuration dialog box.

The system tray icon changes to .

To stop service, right-click  in your system tray and select **Stop Service**.
Or you can select **File > Stop Server** in the Report Server Configuration dialog box.

The system tray icon changes to .

About the Report Manager

You can use Report Manager to review the data collected from your Log Servers for all your Firebox devices. From Report Manager, you can see the available WatchGuard Reports for one Firebox, or a selection of your Firebox devices.

WatchGuard Reports are summaries of the log data that you have selected to collect from the Firebox log files. Report Manager consolidates the log data into a variety of predefined reports so you can quickly and easily locate and review Firebox actions and events. For more information about predefined reports, see [Predefined Reports list](#).

With the advanced features of Report Manager, you can:

- [Set Report options](#) such as background color, maximum number of records per file, and the directory in which to store reports.
- [Select report parameters](#) such as date ranges for reports and groups of Fireboxes you want to create reports for.
- [Change the Report type](#) from HTML to PDF or back.
- [Email, print, or save a Report](#)



To use WatchGuard Reports, you must have Internet Explorer 6.0 or higher installed.


Report Manager toolbar

The Report Manager toolbar includes icons to help you navigate the interface.

Icon	Name	Action
	Connect to Report Server	Connect to a Report Server.
	Email report	Open an email message with the selected report format attached.
	Print report	Open the print dialog box to select print parameters.
	Save as	Save the report as a PDF, HTML, or CSV file.
	Show report in HTML	Show the report in HTML format.
	Show report in PDF	Show the report in PDF format.
	Back	Go back one page.
	Forward	Go forward to the previously selected page.
	Refresh	Refresh the current view.
	Stop	Stop the current action.
	Options	Open the Options dialog box to set Report Manager options.
	Help	Open Report Manager Help.

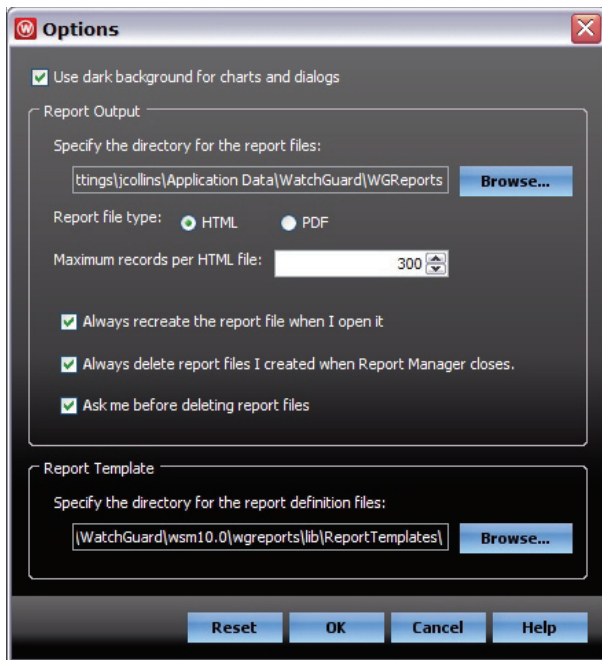
Set report options

You can change the default settings for report output and the default report template.

From the Report Manager toolbar, click .

Or select **View > Options**.

The Options dialog box appears.



Use dark background for charts and dialogs

This option is selected by default. Clear this check box to use a light background in all charts and dialog boxes.

Specify the directory for the report files

Each time you look at a report, Report Manager puts the report file on your local hard drive. You can specify the folder where the file is located.

Report file type

Select the default view for report output. Report Manager automatically displays reports in this format.

Maximum records per HTML file

Click the up or down arrow to set the maximum number of records to include in each HTML file.

Always recreate the report file when I open it

Clear this check box to enable Report Manager to open existing versions of the selected reports. Large reports might take a long time to generate. Clear this option to decrease the time it takes to see a report. Information included in previously created reports might not be the most recent data.

Select this option if you want Report Manager to always create a new report. This option might take longer, but it will provide the most recent data.

Always delete report files I created when Report Manager closes

To leave report files on your hard drive, clear this check box.

Ask me before deleting report files

If you want Report Manager to delete report files without notifying you, clear this check box.

Specify the directory for the report definition files

Select the directory where report definition files are saved.

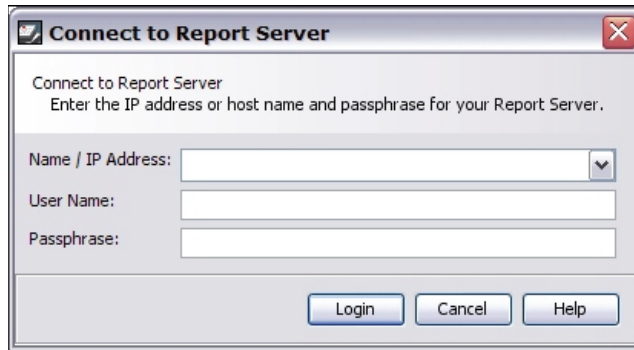
Open Report Manager

Open Report Manager from the main WatchGuard System Manager (WSM) interface.

1. From the WSM toolbar, click .

Or, select **Tools > Logs > Report Manager**.

WatchGuard Report Manager and the Connect to Report Server dialog box appear.



2. Type the IP address, user name, and passphrase for your Report Server.

All WatchGuard servers share the same master passphrase.

3. Click **Login**.

Report Manager connects to the report server and data appears in the left WatchGuard Reports navigation window.

The first time you connect to a Report Server, an **Accept Certificate** dialog box appears. You must accept the certificate to continue.

Connect to a different Report Server

To connect to a different Report Server while Report Manager is open, you must first disconnect from the current Report Server.

Select **File > Disconnect**.

Predefined Reports list

Report Manager includes predefined reports that you can select to show the data your Firebox has collected.

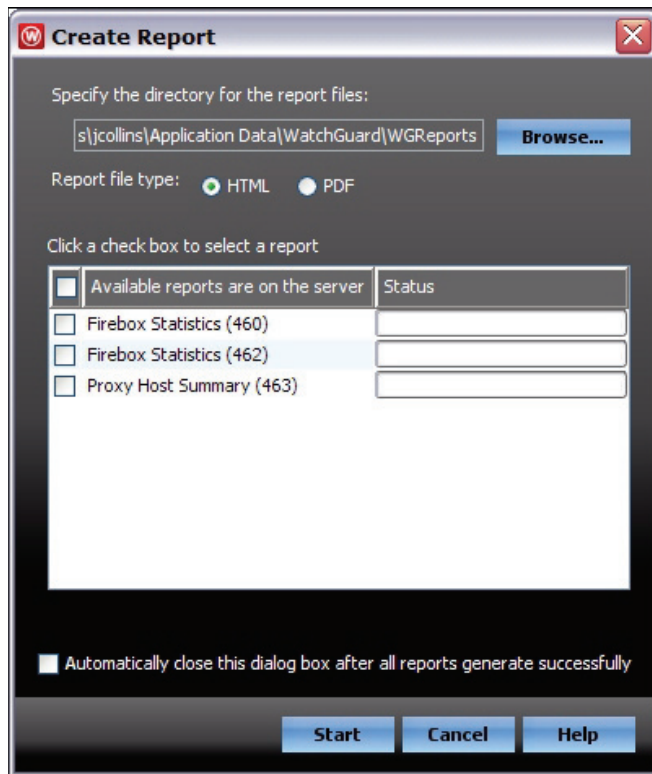
Report Type	Report Name	Description
Web Traffic Summary	Web activity trend	Trends, active clients, most popular domains, WebBlocker information, and web sites blocked by proxy rules. Charts are included for the more detailed reports. You can click a chart to show the detailed report.
	Web trend summary	Hourly trend data
	Most active clients	Top 50 clients by the number of web connections
	Most popular domains	Top 50 web sites visited by clients
	WebBlocker service	Statistics and web sites blocked by WebBlocker service
	URL details by time	All URLs in chronological order
	URL details by client	All URLs in order by client
	URL details by domain	All URLs in order by domain
Intrusion Prevention Summary	Web activity audit	Includes allowed websites for HTTP connections, if you enable the audit flag for HTTP in Policy Manager.
	Intrusion Prevention Summary	All intrusion prevention actions
	Detail by protocol	Prevention summary details by protocol
	Detail by severity	Prevention summary details by severity
	Detail by source IP	Prevention summary details by source IP
AntiVirus Summary	Detail by signature	Prevention summary details by signature
	AntiVirus summary	AntiVirus action summary
	Detail by protocol	AntiVirus action details by protocol
	Detail by host (HTTP)	AntiVirus action details by host
	Detail by virus	AntiVirus action details by virus
spamBlocker Summary	Detail by email sender	AntiVirus action details by email sender Available for SMTP or POP3
	spamBlocker summary	Statistics by spam type, action, and top spam senders and recipients
	spamBlocker by sender	Statistics by sender
Proxy Summaries	Host summary	Proxy action summary
SMTP Proxy Summary	SMTP server summary	SMTP server activity summary (for internal and external email accounts)
	SMTP email summary	SMTP email activity summary (for internal and external servers)
	SMTP proxy detail	SMTP proxy action records by time

Report Type	Report Name	Description
POP3 Proxy	Email account summary	Internal and external email accounts
	Email server summary	Internal and external servers
	POP3 detail	All records by time
Packet-Filtered Summary	Host summary	Summary of all packet-filter data
Firebox Statistics	Firebox statistics	Firebox bandwidth statistics for all interfaces
	External interface bandwidth	Firebox bandwidth statistics summary (for external interfaces) The data sampling interval is based on the report time range. The minimum interval is 1 minute. The published report samples data every 10 minutes.
	VPN tunnel bandwidth	VPN tunnel traffic summary
Exceptions	Denied packet summary	Log summary for all denied packets
	Denied incoming packets detail	Detailed log for each incoming action
	Denied outgoing packet detail	Detailed log for each outgoing action
Management Server Audit	Alarms	All alarm records
	Server audit summary	Server audit details summary
	Server audit detail	All server audit details
Management Reports	Server Authentication Report	All server authentication failures
	Boxes Under Management Report	Summary of details for all Firebox devices connected to the Management Server.

Select reports to generate

You can select which types of reports to include when you generate WatchGuard Reports.

1. Select **Edit > Create reports**.
The Create Report dialog box appears.



2. Select a **Report file type**.
3. Click a check box in the report list to select the reports you want to generate. To select all reports in the list, click the **Available reports are on the server** check box.
4. Click **Start**.
Report Manager generates the selected reports.

Create Report dialog box settings

Specify the directory for the report files

Select the directory where report files are saved.

Report file type

Select the default view for report output. Report Manager automatically displays reports in this format.

Automatically close this dialog box after all reports generate successfully.

Clear this check box if you want the **Create Report** dialog box to remain open after all the reports have successfully generated.

Select report parameters

After you connect to your Report Server, you can use Report Manager to review the log data. To show reports, you must first select the Firebox devices and date range to include in the report.

You can choose to include one Firebox or a group of Firebox devices in your report.

1. Select a Firebox to report on from the **Select device** drop-down list.
For instructions to create a group of Firebox devices, see the subsequent section.
2. Select a date range for the report from the **Select range** drop-down list.
For instructions to select to show reports for specific date and time ranges, see Specify a date range.

Create device groups

You can select to show reports for multiple Firebox devices in one list. You cannot change a device group after it is created. If you want to change a group, you must define a new group.

1. Select **Define a group** in the **Select device** drop-down list.
Or, select **Edit > Define a group**.
The Create a group dialog box appears.
2. Type a name in the **Group name** field for the list of Firebox devices.
3. Select the check box for each Firebox you want to include in the group in the **Available devices** list.
To select all the listed devices, select the **Device Name** check box.
4. Click **OK**.
The group name appears in the Select device field and the available report data appears in the WatchGuard Reports list.



Device groups cannot be saved from session to session. When you close Report Manager, all device groups disappear.

Specify a date range

To refine your report data, you can select to show reports for specific date and time ranges in one report list.

1. Select **Specify a range** in the **Select range** drop-down list.
Or, select **Edit > Specify a range**.
The Specify a range dialog box appears.
2. Select a start date and time in the **Start** section.
3. Select an end date and time in the **End** section.
4. Click **OK**.
The range appears in the Select device field.



Specified date ranges cannot be saved from session to session. When you close Report Manager, all specified ranges disappear.



Show a report

After you have selected your report parameters, and selected which reports to generate, you can show your reports.

For more information about report parameter selection, see [Select report parameters](#).



For more information about selecting which reports to generate, see [Select reports to generate](#).

Reports are grouped by date and then by report type for all selected devices.

- To see a report, click a report name in the **WatchGuard Reports** list in the left navigation pane.
The Progress dialog box appears and then the selected report appears on the right.
- For reports that include links to device data, click a link to see the data.
The device data appears.
- To stop generating a report, click .
- To refresh the selected report, click .
Or select **Edit > Update report list**.

Find a report in the list

You can use the **Find** field to find a specific report in the list.

1. Select a section of the reports to include in the search.
For example, to search all of the displayed reports, click WatchGuard Reports at the top of the list.
2. In the **Find** field at the bottom of Report Manager, type a phrase to find within the listed reports.
3. Click .
Or, press **Enter** on your keyboard.
If the phrase is included in the displayed reports, the first instance of the report in the list is highlighted, and the report appears.
4. Click  again to search for more reports in the list.
If the phrase is not included in the displayed reports, "Phrase not found" appears below the Find field.

Find details in a report

You can use the Windows search feature to find details in a report.

1. Select a report in the **WatchGuard Reports** list.
The report data appears.
2. Press **Ctrl + f** on your keyboard.
The Find dialog box appears.
3. Type a phrase to search on in the **Find** field.
4. Click **Find**.

Change the report type

You can show your report in HTML or PDF format.

- To see the report in HTML format, click .
- To see the report in PDF format, click .

Email, print, or save a report

After you have selected a report, you can email, print, or save it directly from Report Manager.

Send a report in email

Click .

Or, select **File > Send to**.

If the report is in HTML format, an email message opens with a link to the HTML file.

If the report is in PDF format, an email message opens with the selected file type attached.

Print a report

Click .

Or, select **File > Print**.

*If the report is in HTML format, the **Print** dialog box appears. Select your print parameters and click **Print**.*

If the report is in PDF format, the report appears in a separate window. Print from that application window.

Save a report

Click .

Or, select **File > Save as**.

The Save dialog box appears.

Select a location, filename, and file type. Click **Save**.

17 Management Server Setup and Administration

About the WatchGuard Management Server

The WatchGuard Management Server allows you to centrally manage multiple Firebox devices and VPN tunnels of a distributed enterprise from one easy-to-use management interface. You can manage different types of Firebox devices: Firebox X Core, Firebox X Peak, Firebox III, Firebox X Edge, and SOHO 6.

The workstation that is configured as the Management Server also operates as a CA. The CA gives certificates to managed Firebox clients when they contact the Management Server to receive configuration updates.

Install the Management Server

When you run the Setup program to install the WatchGuard System Manager software, you are asked which client and server components you want to install. Under the **Server Components** section, make sure you select **Management Server**.

If you have already run the WatchGuard System Manager Installation and did not install the Management Server, you can run the installer again. Select the **Management Server** check box. Do not select the check box for components you have already installed.

You do not have to install the Management Server on the computer you are using as the management station. You can install it on a different computer that uses the Windows operating system. We recommend that you install the Management Server software on a computer with a static IP address that is behind a Firebox with a static external IP address. Otherwise, the Management Server may not operate correctly.

About WatchGuard Server passphrases

The five WatchGuard System Manager Servers (Management Server, Log Server, Quarantine Server, Report Server, and WebBlocker Server) use passphrases to protect sensitive information and to secure data with client systems. The first time you run the Setup Wizard to configure any one of the servers, you create two passphrases that you will need to use with all five servers:

- Master passphrase
- Management Server passphrase

Master passphrase

The first passphrase that you set with the Setup Wizard is the master passphrase. The master passphrase is used to encrypt the Management Server passphrase. This prevents a person with access to the hard drive or its archived contents from getting the passphrases and using them to access other sensitive data on the hard drive.

The master passphrase is not used frequently. You use the master passphrase when you:

- Migrate the Management Server data to a new system
- Restore a lost or corrupt master key file
- Change the master passphrase

Make sure that the master passphrase and the Management Server passphrase are not the same. We recommend that you write the master passphrase down and lock it in a secure location.

Server management passphrase

The second passphrase that the Setup Wizard prompts for is the server management passphrase. This passphrase is used frequently by the administrator. You use this passphrase to connect all WatchGuard System Manager servers.

Password and key files

The Management Server passphrase and all the automatically created passphrases are kept in a passphrase file. The passphrase data in this file is protected by the master passphrase. The master passphrase is not kept on the hard drive. An encryption key is created from the master passphrase.

The default locations for the passphrase file and encryption key are:

- C:\Documents and Settings\WatchGuard\wgauth\wgauth.ini
- C:\Documents and Settings\WatchGuard\wgauth\wgauth.key

These files are used by the Management Server software and must not be modified directly.

Microsoft SysKey utility

The passphrase file is protected by the master key. This key is protected by an encryption key, which is protected by the Windows system key.

Windows operating systems use a system key to protect the Security Accounts Management (SAM) database. This is a database of the Windows accounts and passwords on the computer. By default, the system key data is hidden in the registry. The system is protected, and the system key is created from the registry during the startup procedure. If you want a more secure system, you can remove the system key data from the registry so that this sensitive data is not on the system at all.

You can use the SysKey utility to:

- Move the system key to a floppy disk
- Make the administrator type a password at start time
- Move the system key from the floppy disk to the system

If you move the startup key to a floppy disk, then that disk must be inserted in the drive for the system to start. If you make the administrator type a startup password, the administrator must type the password each time the system starts.

To configure SysKey options, click **Start > Run**, type `syskey`, and click **OK**.

Set up the Management Server

The Management Server Setup Wizard creates a new Management Server on your workstation. If you used earlier versions of WatchGuard System Manager and VPN Manager, you can also use the Wizard to migrate a DVCP Server that is installed on a Firebox to a new Management Server on a workstation. To move a Management Server off a Firebox, see the *WFS to Fireware Pro Migration Guide*.



The Quarantine Server, the Report Server, the Log Server, and the WatchGuard Management Server share the same master passphrase and server management passphrase. If you set up one of the other servers first, you do not have to set the passphrases again when you set up the Management Server.

To successfully set up a new Management Server:

1. Right-click the Management Server icon (second from the left) in the WatchGuard toolbar on the Windows taskbar.



You do not see this icon if you have not installed the Management Server.

For installation information, see [About the WatchGuard Management Server](#).

2. Select **Start Service**.
3. The Management Server Setup Wizard starts. Click **Next**.
4. If you have not yet run the Setup Wizard for another WSM server, you are asked to enter a master passphrase. This passphrase is necessary to control access to the WatchGuard management station. Type a passphrase that has a minimum of eight characters and then type it again to confirm. Click **Next**. For more information on the master passphrase, see [About WatchGuard Server passphrases](#). *Make sure you keep this passphrase in a safe place.*
5. If you have not yet run the Setup Wizard for another WSM server, you are asked to enter a server management passphrase. You use this passphrase when you configure and monitor the WatchGuard Management Server. Use a passphrase that has a minimum of eight characters and then type it again to confirm. Click **Next**. For more information on the server management passphrase, see [About WatchGuard Server passphrases](#).
6. If you have a gateway Firebox for the Management Server, type the external IP address and passphrases for the Firebox. We recommend that you use a gateway Firebox to protect the Management Server from the Internet. When you add an IP address, the Wizard does three things:
 - o The Wizard uses this IP address to configure the gateway Firebox to allow connections to the Management Server. If you do not type an IP address here, you must configure any firewall between the Management Server and the Internet to allow connections to the Management Server on TCP ports 4110, 4112, and 4113.
 - o If you have an earlier version of WatchGuard System Manager, and have a Firebox configured as a DVCP server, the Wizard gets the DVCP server information from the gateway Firebox and moves these settings to your Management Server. For more information, see the *Migration Guide*.
 - o The Wizard sets the IP address for the Certificate Revocation List (CRL). The devices you add as managed clients use this IP address to connect to the Management Server. This IP address must be the public IP address your Management Server shows to the Internet. If you do not type an IP address here, the Wizard uses the current IP address on your Management Server computer for the CRL IP address. If this is not the IP address your computer shows to the Internet because it is behind a device that does network address translation (NAT), you must edit the CRL and type the public IP address your Management Server uses. For more information, see [Change the Management Server Configuration](#).

7. Type the license key for the Management Server. Click **Next**.
To find the license key, see [Find your Management Server license key](#).
8. Type the name of your organization. Click **Next**.
This name is used for the certificate authority on the Management Server.
9. An information screen that shows the information for your server appears. Click **Next**.
The Wizard configures the server.
10. Click **Finish**.



When an interface whose IP address is bound to the Management Server goes down and then restarts, we recommend that you restart the Management Server.

Find your Management Server license key

WatchGuard System Manager for most Firebox X Core and Peak appliances includes a license key that allows you to manage up to four devices. The only exceptions are the Firebox X 500 and Firebox X 550e. If you have a VPN Manager license key from a previous Firebox purchase, you can use the VPN Manager license key for the WatchGuard Management Server. If you do not have either a WatchGuard System Manager license key that includes the ability to manage more than one Firebox or a VPN Manager license key, you must purchase one from a WatchGuard reseller to use the WatchGuard Management Server.

To find your WatchGuard System Manager or VPN Manager license key:

1. On the LiveSecurity web site, go to the Manage Products area of the LiveSecurity web site:
<https://www.watchguard.com/archive/manageproducts.asp>.
You must log in with your LiveSecurity credentials if you are not already logged in.
2. Scroll to the bottom of the page.
3. Click the **View Details** link adjacent to **WatchGuard System Manager** or **VPN Manager**.
4. Use one of these keys when you run the Management Server Setup Wizard to set up your Management Server.

The license key has this format:

WSMMGR-X-000392-YYYYYYYY

or

VPNMGR-X-024535-YYYYYYYY

The X shows how many devices you can manage with each key. The y characters are a string of alphanumeric characters.

If more than one license key is listed, you can use any of them.

Configure the certificate authority on the Management Server

You can configure the certificate authority (CA) on the WatchGuard Management Server.

Set properties for the certificate authority

Usually, Firebox administrators do not change the properties of the CA certificate. If you must change these settings:

1. From the computer configured as the Management Server, right-click the Management Server icon in the WatchGuard toolbar and select **Configure**.
2. Click the **Certificates** tab.

The screenshot shows the 'Management Server Configuration' dialog box with the 'Certificates' tab selected. The dialog has a menu bar with 'File' and 'Help'. Below the menu bar are two tabs: 'Certificates' (active) and 'Management'. The main content area is divided into three sections: 'Certificate Authority', 'Client', and 'Certificate Revocation List'. The 'Certificate Authority' section has fields for 'Common Name' (WatchGuard Certificate Authority), 'Organization' (My Watchguard), 'Certificate Lifetime' (1000 Days), and 'Key Bits' (2048). The 'Client' section has fields for 'Certificate Lifetime' (365 Days) and 'Key Bits' (1024). The 'Certificate Revocation List' section has a 'Distribution IP Address' field (50.50.50.50) with 'Add...' and 'Remove' buttons, and a 'Publication Interval' field (720 Hours). At the bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons. A status bar at the very bottom says 'Connected to Management Server...'.

3. In the **Common Name** field, type the name you want to appear in the CA certificate.
4. In the **Organization** field, type an organization name for the CA certificate.
5. In the **Certificate Lifetime** field, type the number of days after which the CA certificate will expire. A longer certificate lifetime could give an attacker more time to attack it.
6. From the **Key Bits** drop-down list, select the strength to apply to the certificate. The higher the number in the **Key Bits** setting, the stronger the cryptography that protects the key.

Set properties for client certificates

1. In the **Client** section of the dialog box, in the **Certificate Lifetime** field, type the number of days after which the client certificate will expire.
A longer certificate lifetime could give an attacker more time to attack it.
2. From the **Key Bits** drop-down list, select the strength to apply to the certificate.
The higher the number of the **Key Bits** setting, the stronger the cryptography that protects the key.

Set properties for the Certification Revocation List (CRL)

1. In the **Certificate Revocation List** section of the dialog box, the **Distribution IP Address** box contains a list of IP addresses. You can select an address from the list, or click **Add** to add a new address.
You can also select an address and click **Remove** if you no longer need it.
By default, the distribution IP address is the address of the gateway Firebox. This is also the IP address the remote managed Firebox clients use to connect to the Management Server. If the external IP address of your Firebox changes, you must change this value.
2. Type the **Publication Interval** for the CRL in hours. This is the period after which the CRL is automatically published.
The default setting is zero (0), which means that the CRL is published every 720 hours (30 days). The CRL is also updated after a certificate is revoked.

Send diagnostic log messages for the certification authority

To have the Management Server send diagnostic log messages to the Windows Event Viewer, select the **Debug CA Service log messages** check box.

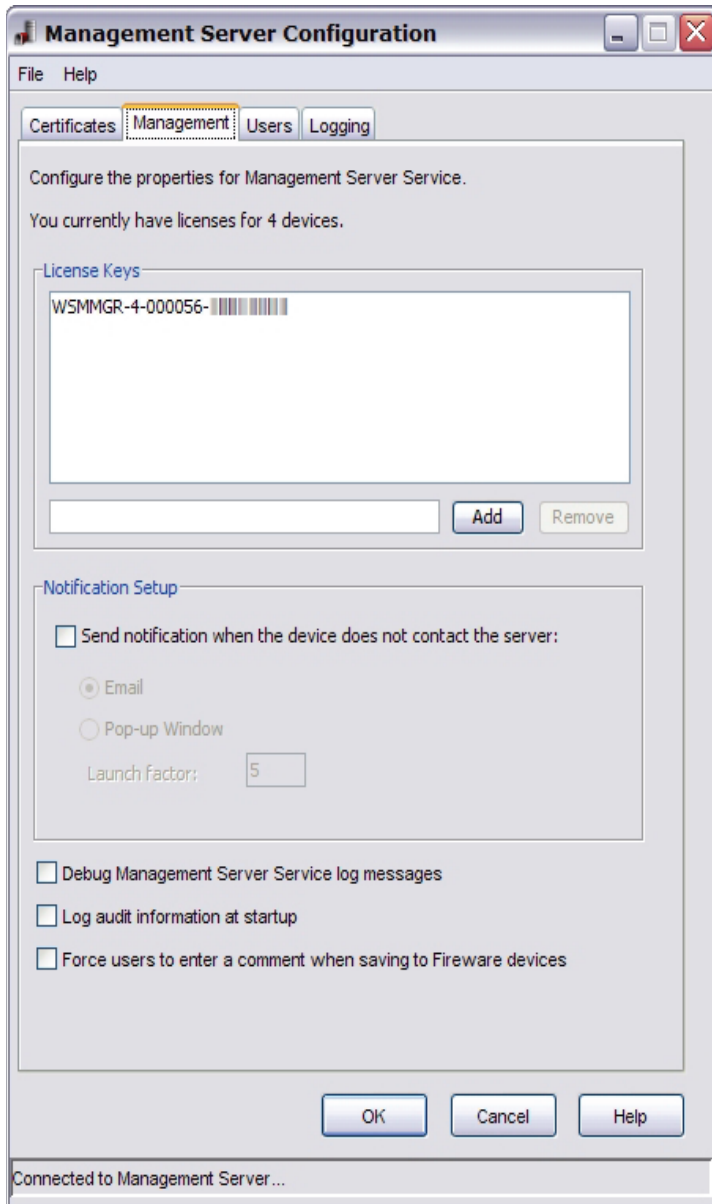
To see the log messages, open the Windows Event Viewer:

1. From the Windows desktop, select **Start > Run**.
2. Type `eventvwr`.
The log messages appear in the **Application** section of the Event Viewer.

Change the Management Server configuration

The Management Server Setup Wizard configures your Management Server. It is not usually necessary to change the properties of your Management Server configuration after you use the wizard. If you must change the Management Server configuration, you can access the configuration properties on the Management Server itself.

From the computer configured as a Management Server, right-click the Management Server icon in the WatchGuard toolbar and select **Configure**. The **Management Server Configuration** dialog box appears.



Add or remove a Management Server license

To add a Management Server license:

1. Click the **Management** tab.
2. Type or paste the Management Server license key into the **License Key** field.
3. Click **Add**.

To remove a Management Server license:

1. Click the **Management** tab.
2. Select the license to remove, and click **Remove**.

When you finish the configuration, click **OK**.

For more information on Management Server license keys, see the Management Server section of the Firewall FAQs at: www.watchguard.com/support/faqs/fireware/.

Configure notification

You can have the Firebox send a notification when the device fails to contact the server.

For information on the fields in this dialog box, see [Set logging and notification preferences](#).

Control logging and configuration change settings

You can set several global configuration parameters to control the log messages sent from the Management Server to the Log Server.

Debug Management Server Service log messages

Select this check box to have the Management Server send diagnostic log messages to the Windows Event Viewer. You can also control Management Server logging on the **Logging** tab.

To see the diagnostic log messages, open the Windows Event Viewer.

1. From the Windows desktop, select **Start > Run**.
2. Type `eventvwr`.

The log messages appear in the **Application** section of the Event Viewer.

Log audit information at startup

Select this check box if you want the Management Server to log information on managed devices, VPN resources, VPN firewall policy templates, security or Edge centralized management templates, and managed VPN tunnels when it starts up. You must select this check box to get accurate information in Report Manager for managed Firebox devices.

Force users to enter a comment when saving to Firewall devices

Select this check box to require users to type a comment before they save changes to a Firebox from Policy Manager for a managed Firebox device.

Update the Management Server with new gateway address

When you first use the Management Server Setup Wizard on your Management Server, you identify the IP address of your gateway Firebox that protects the Management Server from the Internet. This same IP address is used as the Certificate Revocation List (CRL) Distribution IP address. If you want to change the IP address on your gateway Firebox, you must first update the CRL Distribution IP address on your Management Server and update all managed devices with this information. If you do not do this, you will lose the connection to each of your managed devices.



If you have managed Branch Office VPN tunnels configured on your Management Server and the gateway Firebox is the endpoint in any of these tunnels, you must remove those VPN tunnels before you start this procedure. When you are done with this procedure, you must create the VPN tunnels again.

To change the IP address on your gateway Firebox IP, you must update your Management Server configuration, update each managed device, and edit the WG-Mgmt-Server policy NAT configuration:

1. On your Management Server, right-click on the Management Server icon on your WatchGuard desktop toolbar and select **Configure**.
2. Change the **Distribution IP Address** to the new IP address you will give to your gateway Firebox. Click **OK**.
3. On your management station, connect to your Management Server.
4. Select the **Device Management** tab.
5. Right-click on a managed Firebox and select **Update Device**.
6. Below **Update Client Settings**, make sure that the **Reset Server Configuration** and **Expire Lease** check boxes are selected. Make sure the **Issue/Reissue Firebox's IPsec Certificate and CA's Certificate** check box also is selected.
7. Repeat steps 3–6 for each device managed by your Management Server.
8. Open the configuration of the gateway Firebox in Policy Manager.
9. Select **Network > Configuration** and change the IP address of the external interface of the Firebox to the new IP address.
10. Double-click the WG-Mgmt-Server policy.
When you configure a managed Firebox client, you give the managed Firebox the IP address of the gateway Firebox. The managed Firebox uses this IP address to find the Management Server. The WG-Mgmt-Server policy on the gateway Firebox sets up a NAT policy to make sure that any connection from a managed Firebox client to the Management Server is sent correctly through the external interface of the Firebox.
11. Select the NAT entry in the **To** dialog box of the WG-Mgmt-Server policy and click **Remove**.
12. Below the **To** dialog box, click **Add**.
The Add Address dialog box appears.
13. Click **Add NAT**.
The Add Static NAT dialog box appears.
14. From the **External IP Address** drop-down list, select the new IP address for your gateway Firebox. In the **Internal IP Address text** box, type the IP address of your Management Server. Click **OK**.
15. [Save the configuration file.](#)

When the Firebox restarts, connections between the Management Server and the managed Firebox clients start again. You can now re-create any BOVPN tunnels for which the gateway Firebox is a VPN endpoint.

Change the IP address of a Management Server

To change the IP address on your Management Server, you must edit the WG-Mgmt-Server policy NAT configuration.

If the Management Server has a public IP address, change the CRL Distribution IP address. You must then update all managed devices with the new Management Server configuration information:

1. From Policy Manager, open the configuration of the gateway Firebox that protects your Management Server from the Internet.
2. Double-click the WG-Mgmt-Server policy.
When you configure a managed Firebox client, you give the managed Firebox the IP address of the gateway Firebox. The managed Firebox uses this IP address to find the Management Server. The WG-Mgmt-Server policy on the gateway Firebox sets up a NAT policy to make sure that any connection from a managed Firebox client to the Management Server is sent correctly through the external interface of the Firebox.
3. Select the NAT entry in the **To** dialog box of the WG-Mgmt-Server policy and click **Remove**.
4. Below the **To** dialog box, click **Add**.
The Add Address dialog box appears.



If your Management Server has a public IP address, stop here. Skip ahead to the next section.

5. Click **Add NAT**.
The Add Static NAT dialog box appears.
6. From the **External IP Address** drop-down list, make sure the IP address for your gateway Firebox is selected. In the **Internal IP Address text** box, type the new IP address of your Management Server. Click **OK**.
7. [Save the configuration file](#).

If your Management Server is configured with a public IP address

1. Click **Add Other**.
The Add Member dialog box appears.
2. From the **Choose Type** drop-down list, select **Host IP**.
3. Type the new public IP on the Management Server. Click **OK**.
4. [Save the configuration file](#).

Update the Certificate Revocation List (CRL) distribution IP address

The CRL Distribution IP address is the IP address that the Management Server gives to the managed client devices. The managed client devices use this IP address to check in to the Management Server. If the Management Server is configured with a private IP address and it is behind the Gateway Firebox, the CRL Distribution IP address should be the IP address on the external interface of the Gateway Firebox.



Use this procedure only if your Management Server is configured with a public IP address.

1. From the Management Server computer, right-click the Management Server icon in the WatchGuard toolbar and select **Configure**. Type the Management Server passphrase.
The Management Server Configuration dialog box appears.
2. Select an address from the **Distribution IP Address** drop-down list, or click **Add** to add a new address.
3. Click **OK**. The change is applied to the Management Server.

Update managed Firebox clients

You must update all managed client devices to finish the IP address change.

1. From WatchGuard System Manager on your management station, connect to your Management Server. Select the **Device Management** tab.
2. Right-click on a managed Firebox and select **Update Device**.
3. Below **Update Client Settings**, make sure that the **Reset Server Configuration** and **Expire Lease** check boxes are selected.
4. Repeat steps 1–3 for each device connected to the Management Server.

Define user accounts for the Management Server

You can define accounts on the Management Server to enable multiple users to access the server simultaneously.

A default admin account is created for you when you install the Management Server software. The passphrase for this account is the same as the management server passphrase.

1. From the computer configured as a Management Server, right-click the Management Server icon in the WatchGuard toolbar and select **Configure**.
The Management Server Configuration dialog box appears.
2. Click the **Users** tab.
3. To add an account, click **Add**.
4. Enter the username and password for the user in the **Add User** dialog box.
5. Select either the **Admin Privileges**, **Read-Write Privileges**, or **Read-Only Privileges** radio button to define the level of privilege for the user. Click **OK**.

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**.
For more information about how to use the **Add Event Processor** dialog box that appears, see [Add a Log Server](#).
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.

Back up or restore the Management Server configuration

The Management Server contains the configuration information for all managed Firebox X Edge and VPN tunnels. It is a good idea to create regular and frequent backup files for the Management Server and keep them in a safe place. You can use this backup file to restore the Management Server in case of hardware failure. You can also use this backup file if you want to move the Management Server to a new computer. To use the backup file after it is created, you must know the master key. The master key is set when you first configure the Management Server.

1. From your Windows toolbar, right-click the Management Server icon and select **Stop Service**.
2. From your Windows toolbar, right-click the Management Server icon and select **Backup/Restore**. The Management Server Backup/Restore Wizard starts. Use the onscreen instructions to create a backup file or restore a Management Server configuration from a backup file.
3. When the procedure is complete, right-click the Management Server icon on your Windows toolbar and select **Start Service**.

Back up the Management Server for troubleshooting

Use the **File > Export to File** option to create a plain-text version of your Management Server configuration, which includes all information about managed devices and templates. This should be used only when you troubleshoot an issue with Technical Support.


Move the WatchGuard Management Server to a new computer

To move the Management Server to a new computer, you must know the master key. You must also make sure that the new Management Server is given the same IP address as the former Management Server.

1. Use the Management Server Backup/Restore Wizard to create a backup file of your current Management Server configuration.
2. Use the WatchGuard System Manager installation file and install the Management Server software on the new Management Server.
3. Run the Restore wizard and select the backed-up file.
4. From the Windows toolbar, right-click the Management Server icon and select **Start Service**.

Connect to a Management Server

To connect to a Management Server from WSM:

1. Click .
Or, select **File > Connect to Server**.
Or, right-click anywhere in the WatchGuard System Manager window and select **Connect to > Server**.



2. From the **Management Server** drop-down list, select a server by its host name or IP address. You can also type the IP address or host name if necessary. When you type an IP address, type all the numbers and the periods. Do not use the TAB or arrow keys.
3. Type or select your username for your user account on the Management Server.
4. Type the passphrase for your user account. If you are using the default admin account, the passphrase is the server management passphrase.
5. If necessary, change the value in the **Timeout** field. This value sets the time (in seconds) that WatchGuard System Manager listens for data from the Management Server before it sends a message that it cannot connect.
If you have a slow network or Internet connection to the device, you can increase the timeout value. If you decrease the value, it decreases the time you must wait for a timeout message if you try to connect to a Management Server that is not available.
6. Click **Login**.
The server appears in the WatchGuard System Manager window.



In some previous versions of WatchGuard security products, the WatchGuard Management Server was called the DVCP Server.

Disconnecting from the Management Server

Select the Management Server in the WSM tree view. Click .
Or, click on the Management Server name and select **File > Disconnect**.

18

Devices and VPNs in WatchGuard System Manager

Use the WatchGuard System Manager window

The WatchGuard System Manager window has menus and icons you can use to start other tools.

The window also has two tabs that you can use to monitor and manage your Firebox devices and environment: **Device Status** and **Device Management**.

Device status

Information about a device you connect to appears in the WatchGuard System Manager **Device Status** tab. The information that appears includes the status, IP address, and MAC address for each Ethernet interface, and the installed certificates. It also includes the status of all virtual private network (VPN) tunnels that are configured in WSM.

Expanded information for each Firebox includes the IP address and subnet mask of each Firebox interface. It also includes:

- IP address and netmask of the default gateway (for external interfaces only).
- Media Access Control (MAC) address of the interface.
- Number of packets sent and received on each interface since the last Firebox restart.

Each device can be in one of four possible states, as indicated by the appearance of the device in the window:

- Normal icon: Usual operation. The device is successfully sending data to WatchGuard System Manager.
- Yellow question mark: The device has a dynamic IP address and has not yet contacted the Management Server.
- Red exclamation point and gray icon: WatchGuard System Manager cannot make a network connection to the device at this time.
- No exclamation point and gray icon: The device is being contacted for the first time or has not been contacted yet.

The **Device Status** tab also includes information on Branch Office VPN tunnels and Mobile VPN tunnels.

Device management: General navigation



You see the **Device Management** tab only when you [connect to a Management Server](#).

The **Device Management** tab has a navigation pane on the left and an information pane on the right. The navigation pane shows the connected WatchGuard Management Servers and their devices, managed VPNs, VPN Firewall policy templates, security templates, Firebox X Edge configuration templates, and scheduled firmware updates. If you expand a device listing, you see [VPN resources](#) (networks) behind the device.

The information pane shows more detailed information for any item you select in the navigation pane.

If you click the Management Server in the navigation pane, you use the information pane to see or change the following information about the Management Server:

- User name and IP address
- [Aliases for Edge devices](#)
- Server licenses
- Customers. You can change the Contact List, as described in [Set device management properties](#).
- Monitored [Report Servers](#)
- List of managed devices, [VPN tunnels](#), and [Edge Configuration Templates](#)
- WatchGuard Alerts: Recent [LiveSecurity Broadcasts](#) that are information alerts. If you click an alert, you must log into LiveSecurity Service to see the full text of the alert.
- [Start Firebox and Edge tools](#)
- [See and delete firmware updates](#)

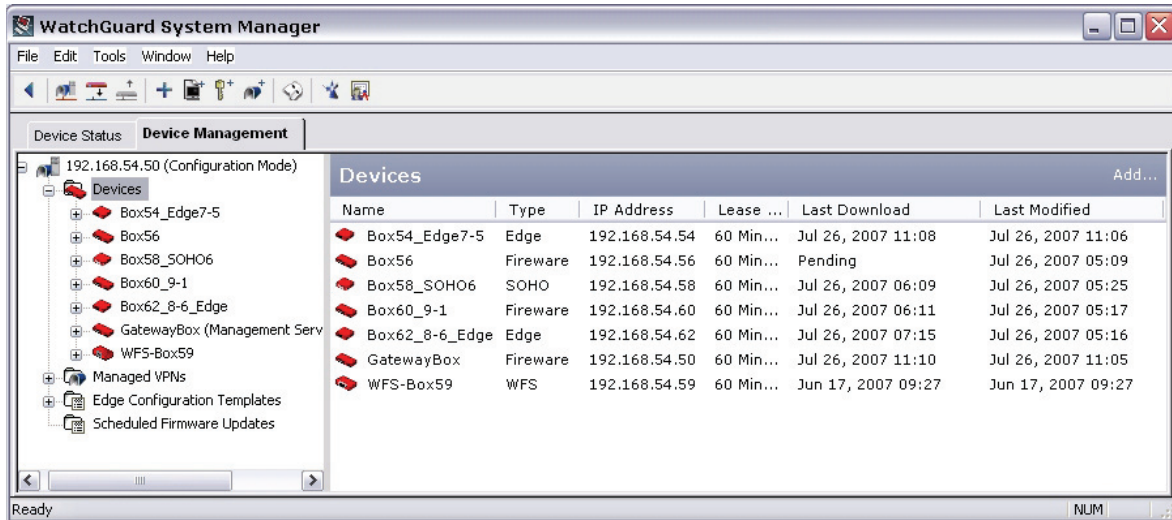
If you click the Devices heading in the navigation pane, you see a [list of managed devices](#) for the server.

If you click a device in the navigation pane, you see the [device management page for the device](#).

If you click a managed VPN in the navigation pane, you see the VPN properties dialog box and VPN settings. You can also add a tunnel from this section, or add a VPN resource.

See information on managed devices

When you select the folders under **Devices**, on the left side of the **Device Management** tab in WSM, you can see a list of devices and the following information for each one.



Name

The name of the managed Firebox.

Type

The type of device or appliance software installed on the managed Firebox.

IP Address

The IP address used to identify the Firebox. If the Firebox has not reported into the server, the field shows **n/a**.

Lease Time

The Management Server lease time is the time interval at which the managed client contacts the Management Server for updates. The default is 60 minutes. The lease time is configured as part of the Device Properties, on the **Connection Settings** tab.

For more information, see [Set device management properties](#).

Last Download

The time of the most recent update of the managed device from the Management Server. The field can also show **Never** if it has never been updated, or **Pending** if an update is in progress.

Last Modified

The time of the most recent configuration file change on the managed Firebox. The field can also show **Never** if it has never been updated, or **Pending** if an update is in progress.

Go to the device management page for a device

You can use the device management page to configure management settings on the device.

1. Expand **Devices** on the left side of the WatchGuard System Manager **Device Management** tab.
A list of managed devices appears.
2. Select a device. The management page for the device appears on the right side of the WatchGuard System Manager window.

From the device management page you can:

- See if another Management Server user account has locked the device definition by opening it in Policy Manager. This alert will appear at the top of the page. You cannot make changes to the device definition until this user unlocks the device (closes Policy Manager or opens it for another device),
- See general device information
- See VPN tunnels the device participates in; add edit or remove tunnels. For more information on using this section of the page, see [VPN tunnels](#).
- VPN resources for the device; add edit or remove resources
- Launch tools you can use to monitor, define, or manage the device

About preparing devices for management

After you have set up and configured the Management Server, you can use it to manage multiple Firebox devices. To manage a Firebox with the Management Server, you must:

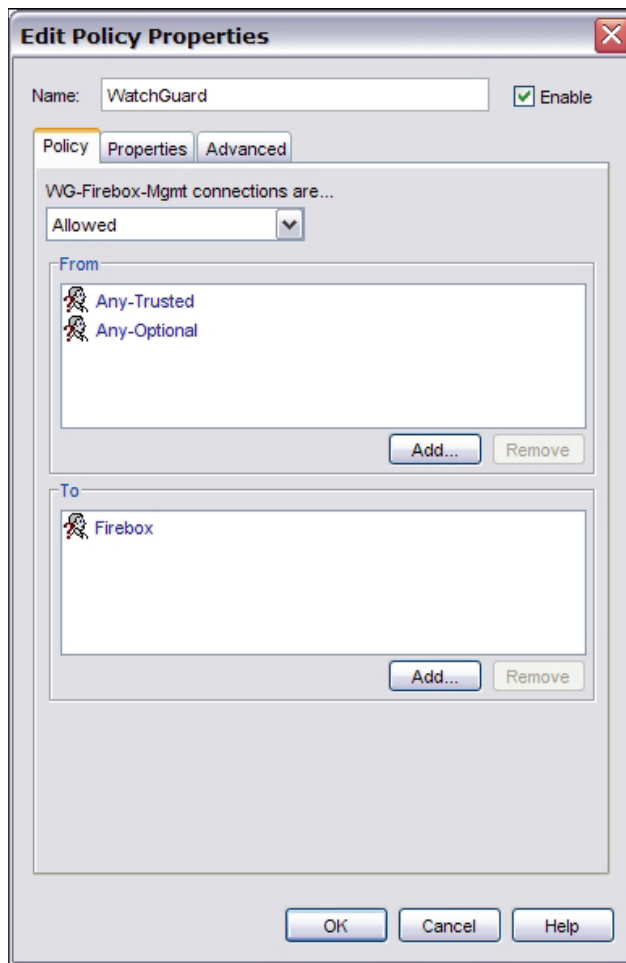
- Make sure the Firebox allows management connections from the Management Server.
- For any Firebox that has a dynamic external IP address, manually enable the Firebox as a managed client.
- Add the Firebox to the Management Server configuration.

The procedures you use are different if you use different Firebox appliance software or a different Firebox model. The instructions can also be different if the managed Firebox client has a dynamic IP address. Make sure you go to the topic that matches your Firebox model and configuration:

- [Configure a Firebox running Fireware as a managed client](#)
- [Configure a Firebox III or Firebox X Core running WFS as a managed client](#)
- [About configuring Edges and SOHOs as managed clients](#)

Configure a Firebox running Firewall as a managed client

1. Open Policy Manager for the Firebox you want to enable as a managed client.
2. Double-click the **WatchGuard** policy to open it for editing.
The Edit Policy Properties dialog box for the WatchGuard policy appears.



3. Make sure the **WG-Firebox-Mgmt connections are** drop-down list is set to **Allowed**.
4. Below the **From** dialog box, click **Add**. Click **Add Other**.
5. Make sure the **Choose Type** drop-down list is set to **Host IP**. In the **Value** field, type the IP address of the external interface of the gateway Firebox or where the computer runs WSM.
If you do not have a gateway Firebox that protects the Management Server from the Internet, type the static IP address of your Management Server.
6. Click **OK**. Click **OK** again.

7. Make sure the **To** dialog box includes an entry of either **Firebox** or **Any**.



If the Firebox you want to manage has a static IP address on its external interface, or if it is dynamic and you know the current IP address, you can stop here. Save the configuration to this Firebox. You can now add the device to your Management Server configuration as described in [Add managed devices to the Management Server](#). When you add this Firebox to the Management Server configuration, the Management Server automatically connects to the static IP address and configures the Firebox as a managed Firebox client. If the Firebox you want to manage has a dynamic IP address and you do not know the current IP address, go on to step 8.

8. From Policy Manager, select **VPN > Managed Client**.
The *Managed Client Setup* dialog box appears.

Managed Client Setup

To configure this Firebox as a managed client, enable the client and configure the Management Server and settings below.

☒ Enable this Firebox as a Managed Client

Client Name:

Management Server:

Shared Secret:

Confirm:

Management Server CA Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDTsTCCApmgAwIBAgIJAPQP9B1DnCrnMAOGCSqG
BAMTGVdhhdGNoR3VhcmQgU2VydM VyIFJvb3QgQ0Ex
cmQwHhcNMjE0MjE0MjE0ODQzWhcNMjE0MjE0MjE0
YXRjaEd1YXJkIFN1cnZ1ciBSb290IENBMjE0MjE0
IjANBgkqhkiG9w0BAQEFAAOCQA8AMIIBCgKCAQEA
0o162zpqvfDMJ8Eco155PowGcIE0G74KUqLFclAf
ooouZq2ZArSMeBkr2uRwhiKCIAlDYL3pZ2p0v6f2
/7UzHKayW5qyZk0+a02b1hHiGTyQLLOojyPAnSQ
-----
```

☐ Enable diagnostic logs

9. To set up a Firebox as a managed device, select the **Enable this Firebox as a Managed Client** check box.
10. In the **Client Name** field, type the name you want to give the Firebox when you add it to the Management Server configuration. This name is case-sensitive and must match the name you use when you add the device to the Management Server configuration.
11. To enable the managed client to send log messages to the Log Server, select the **Enable diagnostic logs** check box. (We recommend this option only to perform troubleshooting.)

12. In the **Management Server** address box, select the IP address of the Management Server if it has a public IP address. Or, select the public IP address of the Firebox that protects the Management Server. If you need to add an address, click **Add**.
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. When you use the Management Server Setup Wizard, the wizard adds a WG-Mgmt-Server policy to your configuration to handle these connections. If you did not use the Management Server Setup Wizard on the Management Server, or, if you skipped the Gateway Firebox step in the wizard, you must manually add the WG-Mgmt-Server policy to the configuration of your gateway Firebox.
13. In the **Shared Secret** box, type the shared secret. Type it again to confirm. The shared secret you type here must match the shared secret you type when you add the Firebox to the Management Server configuration.
14. Click the **Import** button and import the CA-Admin.pem file as your certificate. This file is in \My Documents\My WatchGuard\certs\[firebox_ip].
15. Click **OK**.

When you save the configuration to the Firebox, the Firebox is enabled as a managed client. The managed Firebox client tries to connect to the IP address of the Management Server on TCP port 4110. Management connections are allowed from the Management Server to this managed Firebox client.

You can now add the device to your Management Server configuration as described in [Add managed devices to the Management Server](#).

Configure a Firebox III or Firebox X Core running WFS as a managed client

1. Open Policy Manager for the Firebox you want to enable as a managed client.
2. Double-click the **WatchGuard** service to open it for editing.
The Edit Service Properties dialog box for the WatchGuard policy appears.
3. On the **Incoming** tab, make sure that incoming WatchGuard connections are set to **Enabled and Allowed**.
4. Below the **From** dialog box, click **Add**. Click **Add Other**.
5. Make sure the **Choose Type** drop-down list is set to **Host IP Address**. In the **Value** field, type the IP address of the external interface of the gateway Firebox that protects the Management Server from the Internet.
If you do not have a gateway Firebox that protects the Management Server from the Internet, type the static IP address of your Management Server.
6. Click **OK**. Click **OK** again.
7. Make sure the **To** dialog box includes an entry of either **Firebox** or **Any**.



If the Firebox you want to manage has a static IP address on its external interface, you can stop here. Save the configuration to this Firebox. You can now add the device to your Management Server configuration. When you add this Firebox to the Management Server configuration, the Management Server automatically connects to the static IP address and configures the Firebox as a managed Firebox client. If the Firebox you want to manage has a dynamic IP address, go on to step 8.

8. From Policy Manager, select **Network > DVCP Client**.
9. Select the **Enable this Firebox as a DVCP Client** check box.

10. In the **Firebox Name** field, type the name of the Firebox.

The Firebox name is case-sensitive. The name you type here must match the name you type when you add this Firebox to the Management Server configuration.

11. To send log messages for the managed client, select the **Enable debug log messages for the DVCP Client** check box. (WatchGuard recommends this option only when troubleshooting.)
12. Click **Add** to add the Management Server the Firebox connects to.
13. In the **DVCP Server** address box, type the IP address of the Management Server if it has a public IP address. Or, type the public IP address of the Firebox that protects the Management Server.
14. Type the **Shared Secret** to use to connect to the Firebox. The shared secret you type here must match the shared secret you type when you add this device to the Management Server configuration. A Firebox can be a client of only one 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. The Firebox protecting the Management Server is configured to do this when you run the Management Server Setup Wizard.

If you did not use the Management Server Setup Wizard on the Management Server, or, if you skipped the *Gateway Firebox* step in the wizard, configure the gateway Firebox to forward TCP ports 4110, 4112, and 4113 to the private IP address of the Management Server. Click **OK**.

When you save the configuration to the Firebox, the Firebox is enabled as a managed client. The managed Firebox client tries to connect to the IP address of the Management Server on TCP port 4110. Management connections are allowed from the Management Server to this managed Firebox client.

You can now add the device to your Management Server configuration as described in [Add managed devices to the Management Server](#).

About configuring Edges and SOHOs as managed clients

You can use the WatchGuard Management Server to configure and manage many Firebox X Edge and SOHO devices. For Firebox X Edge devices, you can enable centralized management with WatchGuard System Manager, which means you can manage policies, updates, and VPNs for many Edge devices from one location. For both Edge and SOHO devices, you can use them as endpoints for managed BOVPN tunnels.

Each Firebox X Edge and SOHO must be configured for management by the Management Server. Then you **Insert** or **Add** the devices to the Management Server.

You can **Import** one or more Firebox X Edge devices that have already been configured with the Quick Setup Wizard into the Management Server. This is the fastest procedure to provision and add a group of Firebox X Edge devices to the Management Server.

You can **Add** a Firebox X Edge device that is already configured or installed using the Add Device Wizard. You must configure values to identify the device to the Management Server. You can add only one device at a time.

- For a new or factory default Firebox X Edge device, configure the device with the procedure [Prepare a new or factory default Firebox X Edge for management](#). Then, import the device with the procedure [Import Firebox X Edge devices into a Management Server](#).
- For a Firebox X Edge that is already installed, configure the device for management with the procedure [Prepare an installed Firebox X Edge for management](#). Then, add the device to the Management Server with the procedure [Add managed devices to the Management Server](#).

You can now add the device to your Management Server configuration as described in [Add managed devices to the Management Server](#).



Use the WG-SmallOffice-Mgmt packet filter to allow connections between the Management Server and the managed Firebox X Edge devices. If you have another firewall, make sure that you have a policy to allow traffic from managed Edge devices on TCP port 4109.

Prepare a new Firebox X Edge for management

To prepare a new or factory default Firebox X Edge for management with the Management Server, you must be able to physically connect the Firebox X Edge to an Ethernet interface on your computer.

To prepare the Firebox X Edge:

1. On the computer that runs WatchGuard System Manager, change the IP address to 192.168.111.x/24.
2. Start WatchGuard System Manager and select **Tools > Quick Setup Wizard**.
The Quick Setup Wizard starts.
3. Read the Welcome page and click **Next**.
4. Select **Firebox X Edge** as the type of Firebox and click **Next**.
5. Connect the network interface on your computer to any LAN port on the Firebox X Edge, and click **Next**.
Use one of the green Ethernet cables included with the Firebox X Edge. (If no green cable is included with your Firebox X Edge, try the red cable.)
6. Use the instructions on the subsequent page of the wizard to start the Firebox X Edge in safe mode.
7. Use the instructions on the wizard page, and click **Next**.
8. Use the instructions on the **Wait for the Firebox** and **The Wizard found this Firebox** pages. Click **Next** after each page.
9. Accept the License Agreement and click **Next**.

10. Configure the external (WAN 1) interface of the Firebox X Edge. Select **DHCP**, **PPPoE**, or **Static IP addressing**, and click **Next**. (For detailed information on how to configure the Edge interfaces, see the *Firebox X Edge User Guide*.)
11. Click **Next** after you configure the interface.
12. Configure the Edge internal interface and click **Next**.
13. Create a status passphrase and a configuration passphrase for your Edge and click **Next**.
You must type each passphrase two times. This is the passphrase that is used by WatchGuard System Manager to connect to and configure the device.
14. Type a user name and passphrase for the device, and click **Next**.
You must type the passphrase two times. This is the user name and passphrase that you can use to connect to and configure the device with a web browser.
15. Select the time zone settings and click **Next**.
16. Configure the Management Server settings. Type the IP address of the gateway Firebox that protects the Management Server, the name to identify the Firebox in the Management Server interface, and the shared key. Click **Next**.
The shared key is used by the Management Server to create VPN tunnels between Fireboxes. You do not have to remember this key.
17. Review the configuration for the Edge and click **Next**.
18. To set up another Edge, select the check box. Click **Finish**.
If you select this check box, the Quick Setup Wizard populates the fields with the same values as this configuration, so you can easily set up similar Edge devices.
You can now add the device to your Management Server configuration as described in [Add managed devices to the Management Server](#).

Import Firebox X Edge devices into a Management Server

Firebox X Edge devices that are configured with the Quick Setup Wizard can be imported into the Management Server. You must connect from the computer from which you ran the Quick Setup Wizard. Also, you must connect to the same Management Server that you connected to when you ran the Quick Setup Wizard to configure the first device.

1. Start WatchGuard System Manager, and connect to the Management Server for which you configured Edge devices.
2. Select **File > Import Device**.
The WatchGuard System Manager dialog box appears.
3. Select the check boxes in front of each Edge device you want to import. Click **Import**.

The Firebox X Edge devices are imported into the Management Server. The devices appear in the **Imported Devices** folder for the Management Server.

Prepare an installed Firebox X Edge for management

1. To connect to the Firebox X Edge System Status page, type `https://` in the browser address bar, and the IP address of the Edge trusted interface.
The default URL is: `https://192.168.111.1`
2. From the navigation bar, select **Administration > WSM Access**.
The WatchGuard Management 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 the **Use Centralized Management** check box if you are using 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 in the correct fields.
7. Type a configuration passphrase for your Firebox X Edge and then type it again to confirm in the correct fields.
These passphrases must match the passphrases you use when you add the device to the Management Server or the connection will fail.



If the Firebox X Edge you want to manage has a static IP address on its external interface, you can stop here. Save the configuration to this Firebox. You can now add the device to your Management Server configuration. When you add this Edge to the Management Server configuration, the Management Server automatically connects to the static IP address and configures the Edge as a managed Firebox client. If the Edge you want to manage has a dynamic IP address, go on to step 8.

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 necessary for this to occur.
9. Type the **Client Name** to identify the Edge in the Management Server configuration.
This name is case-sensitive and must match the name you use for the Edge when you add it to 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. You must get the shared key from your Management Server administrator.
11. Click **Submit** to save this configuration to the Edge.
When you save the configuration to the Edge, the Edge is enabled as a managed client. The managed Firebox client tries to connect to the IP address of the Management Server. Management connections are allowed from the Management Server to this managed Firebox client.

You can now add the device to your Management Server configuration as described in [Add managed devices to the Management Server](#).

Configure a Firebox SOHO 6 as a managed client

1. Start your web browser. Type the IP address of the SOHO 6.
2. If the SOHO 6 must have a login and passphrase, type the login and passphrase.
3. Below Administration, click **VPN Manager Access**.
The VPN Manager Access page appears.

4. In the left navigation pane below VPN, click **Managed VPN**. Select the **Enable VPN Manager Access** check box.
5. Type the status passphrase for VPN Manager access. Type the status passphrase again to confirm the passphrase.

6. Type the configuration passphrase for VPN Manager access. Type the configuration passphrase again to confirm the passphrase.



*If the Firebox SOHO you want to manage has a static IP address on its external interface, you can stop here. Click **Submit** to save your configuration to the SOHO. You can now add the device to your Management Server configuration. When you add this SOHO to the Management Server configuration, the Management Server automatically connects to the static IP address and configures the SOHO as a managed Firebox client.
If the SOHO you want to manage has a dynamic IP address, go on to step 7.*

7. Select the **Enable Managed VPN** check box.
8. From the **Configuration Mode** drop-down list, select **SOHO**.
9. In the **DVCP 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 necessary for this to occur.
10. Type the **Client Name** to give your Firebox SOHO.
This name is case-sensitive and must match the name you use for the device when you add it to the Management Server configuration.
11. In the **Shared Key** field, type the key used to encrypt the connection between the Management Server and the Firebox SOHO. This shared key must be the same on the SOHO and the Management Server.
You must get the shared key from your Management Server administrator.
12. Click **Submit**.
When you save the configuration to the Firebox SOHO, the SOHO is enabled as a managed client. The managed SOHO client tries to connect to the IP address of the Management Server. Management connections are allowed from the Management Server to this managed SOHO client.

You can now add the device to your Management Server configuration as described in the [Add managed devices to the Management Server](#).

Add managed devices to the Management Server

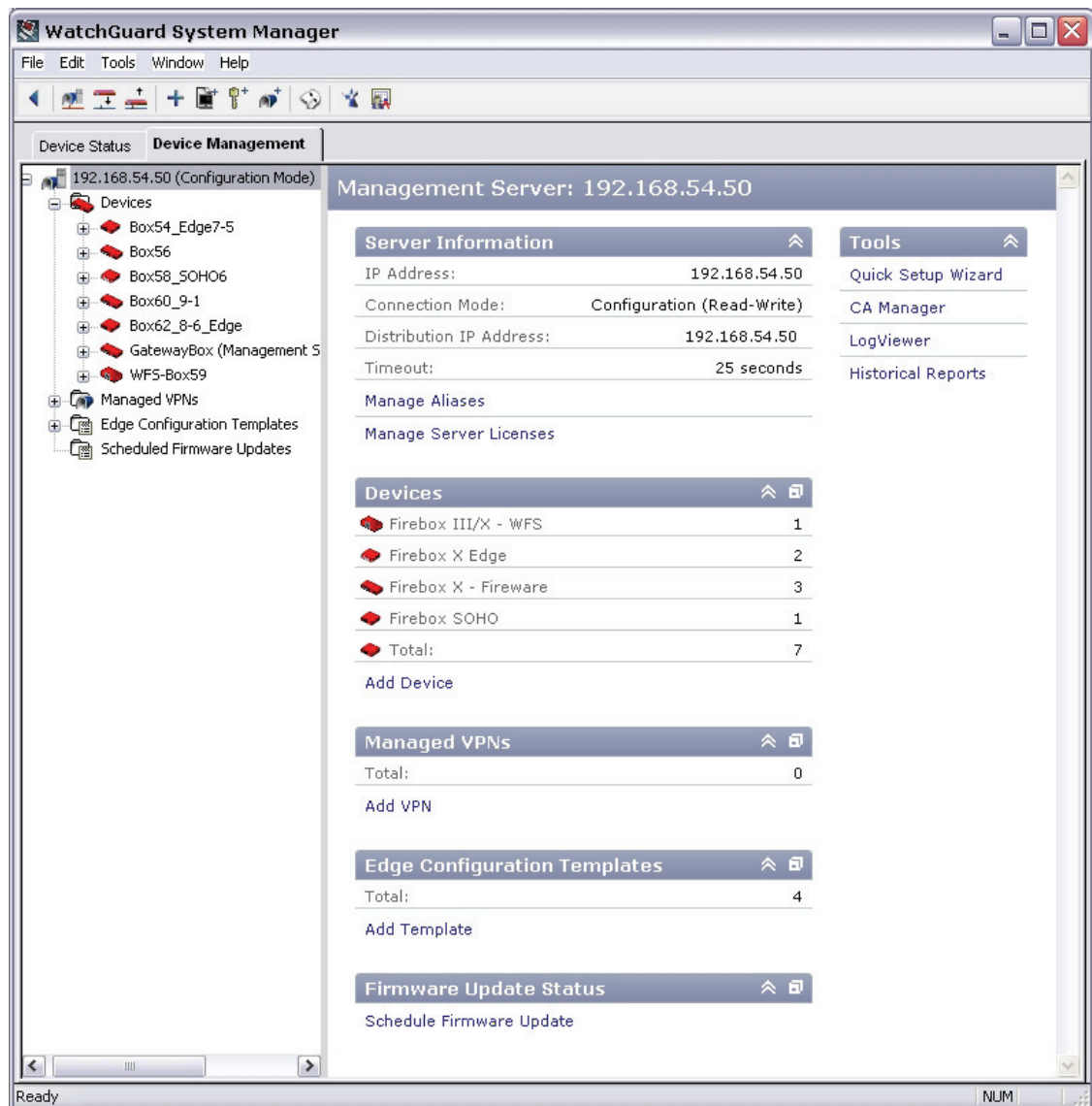
You can use the Management Server to manage Firebox devices, including Firebox III and Firebox X Core devices that use WFS appliance software, Firebox X devices that use Firewall appliance software, Firebox X Edge devices, and Firebox SOHO devices.

A device with a dynamic IP address must also be configured as a managed client from Policy Manager for the device. See the previous sections for these instructions.

If your device has multiple external interfaces, do not change the interface configuration after you add the device to the Management Server.

1. In WatchGuard System Manager, connect to the Management Server.
2. Select **File > Connect to Server**.
Or, select the **Device Status** tab.
Or, right-click anywhere in the window and select **Connect to > Server**.
3. Type or select the IP address of the Management Server, type the configuration passphrase, and click **Login**.
4. Click the **Device Management** tab.

5. Select the Management Server from the list at the left of the window.
The Management Server page appears.



6. Under **Devices**, in the folder that corresponds to the device type you want to add, select **Edit > Insert Device**, or right-click in the left frame of this window and select **Insert Device**.
The Add Device Wizard starts.

7. Click **Next** to see the first configuration screen.

8. If the device is either static or dynamic and you know the device's IP address, type it (or the host name) along with the status and configuration passphrase. If the device has a dynamic IP address but does not use the Dynamic DNS service, type a unique name for the device. The name you type here must match the name you enter in Policy Manager for that device (if the device is a Firebox III, Firebox X Core, or Firebox X Peak). If the device is a Firebox X Edge, this name must match the name you give the device when you enable it as a managed client with the web configuration manager. If you do not know the device's IP address, click the appropriate radio button. At any time after you complete the wizard, you can manually configure the device for management. When the device is configured for management, it will contact the Management Server.
9. Click **Next**.
The wizard performs a device discovery.
10. Enter a name for the device, if you want to use a name other than the default name. Type the shared secret. The name and shared secret must match the name you give the device when you enable it as a managed client. From the **Device Type** drop-down list, select the device type. Click **Next**.
11. Type the device's status and configuration passphrases. Click **Next**.
12. Specify authentication for the device. Click **Next**.
13. Click **Next**.
The Configure the Device screen appears.
14. Click **Next** to configure the device with the new management settings and add it to the Management Server. If the device is already managed by another server, or configured for management by this server, a warning dialog box appears.
15. Click **Yes** to continue.
16. Click **Close** to close the Add Device Wizard.



If traffic is very heavy, the Add Device Wizard cannot connect because of SSL timeout. Try again later when the system has less load.

Set device management properties

You configure three categories of Firebox management properties: connection settings, IPSec tunnel preferences, and contact information.

Connection settings

1. On the [device management page for a device](#), under **Device Information**, click **Configure**.
The Device Properties dialog box appears.

Device Properties

Connection Settings | IPSec Tunnel Preferences | Contact Information

A managed device can participate in VPNs as defined by the list of tunnels. WatchGuard System Manager can also provide real-time status of all configured devices.

Display Name: GatewayBox

Firebox Type: Firebox X with Fireware

☐ Device has dynamic external IP address (DHCP, PPPoE)

Hostname/IP Address: 192.168.54.50
10.0.44.1
10.0.55.1

Status Passphrase:

Configuration Passphrase:

Shared Secret: dEE^327@w~(MMhq(u{#9cmE~eX5L+

Lease Time: 60 minutes

OK Cancel Help

2. In the **Display Name** field, type the name for the device that will appear in WSM.
3. From the **Firebox Type** drop-down list, select the device hardware and, if applicable, the appliance software installed on it.
4. If the device has a static IP address, from the **Hostname/IP Address** box, select or type the entry for your device. This box contains the external IP addresses of all devices managed by the Management Server.

5. If the device has a dynamic IP address, select the **Device has dynamic external IP address** check box. In the **Client Name** field, enter the name of the device. (For information on how to set up a device manually for management, see [About preparing devices for management](#)).

Device Properties

Connection Settings | IPsec Tunnel Preferences | Contact Information

A managed device can participate in VPNs as defined by the list of tunnels. WatchGuard System Manager can also provide real-time status of all configured devices.

Display Name:

Firebox Type:

☒ Device has dynamic external IP address (DHCP, PPPoE)

Client Name:

Status Passphrase:

Configuration Passphrase:

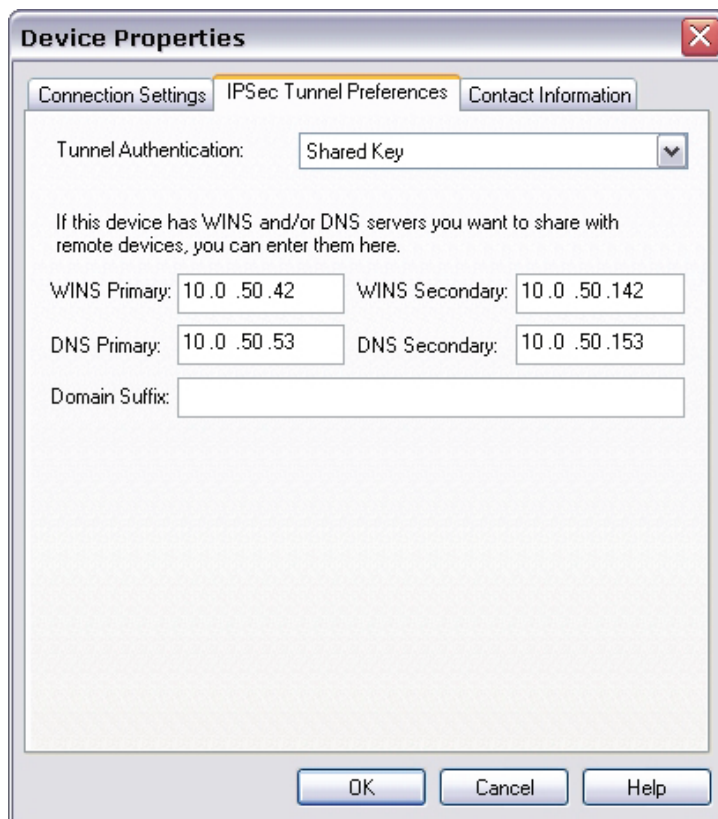
Shared Secret:

Lease Time: minutes

6. Type the status and configuration passphrases for the Firebox.
7. In the **Shared Secret** field, type the shared secret between the device and the Management Server.
8. Use the arrow buttons next to **Lease Time** to change the Management Server lease time. This is the time interval at which the managed client contacts the Management Server for updates. The default is 60 minutes.

IPSec tunnel preferences

1. On the **Device Properties** dialog box, click the **IPSec Tunnel Preferences** tab.

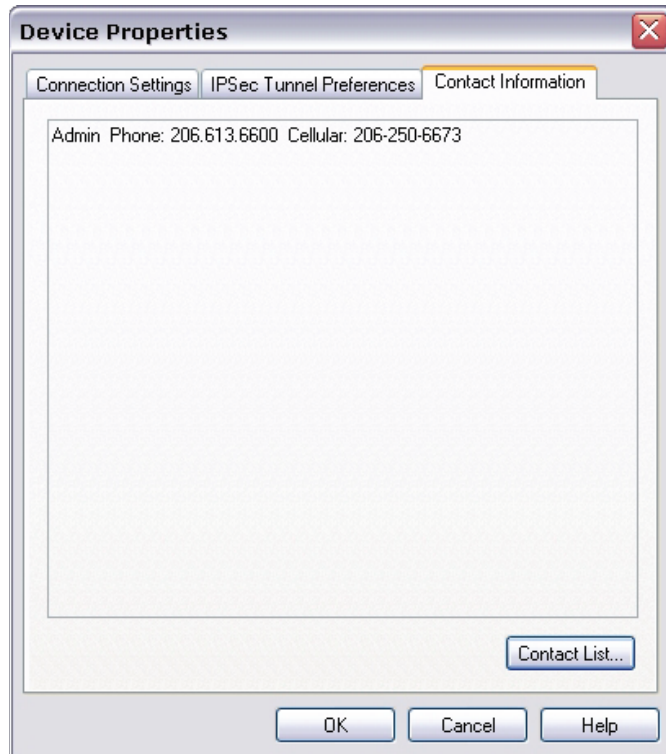


The screenshot shows the 'Device Properties' dialog box with the 'IPSec Tunnel Preferences' tab selected. The 'Tunnel Authentication' dropdown is set to 'Shared Key'. Below this, a text box explains: 'If this device has WINS and/or DNS servers you want to share with remote devices, you can enter them here.' There are four text input fields: 'WINS Primary' (10.0.50.42), 'WINS Secondary' (10.0.50.142), 'DNS Primary' (10.0.50.53), and 'DNS Secondary' (10.0.50.153). A 'Domain Suffix' text box is empty. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

2. (Does not appear for Edge) From the **Tunnel Authentication** drop-down list, select either **Shared Key** or **IPSec Firebox Certificate**. The second option uses the certificate for the Firebox. For more information about certificates, see [Use a certificate for BOVPN tunnel authentication](#).
3. Type the primary and secondary addresses for the WINS and DNS servers if you want your managed client to get its WINS and DNS settings through the IPSec BOVPN tunnel. Otherwise, you can leave these fields blank. You can also type a domain suffix in the **Domain Name** text box for a DHCP client to use with unqualified names such as *kunstler_mail*.

Contact information

1. On the **Device Properties** dialog box, select the **Contact Information** tab.
A list of contact information for remote devices appears.



2. To add to the contact list or edit an existing entry, click **Contact List**.
The contact list appears.
3. Click **Add** or select an entry you want to edit or delete.
The Contact Information dialog box appears.

 The screenshot shows the 'Contact Information' dialog box. It contains several input fields for contact details:

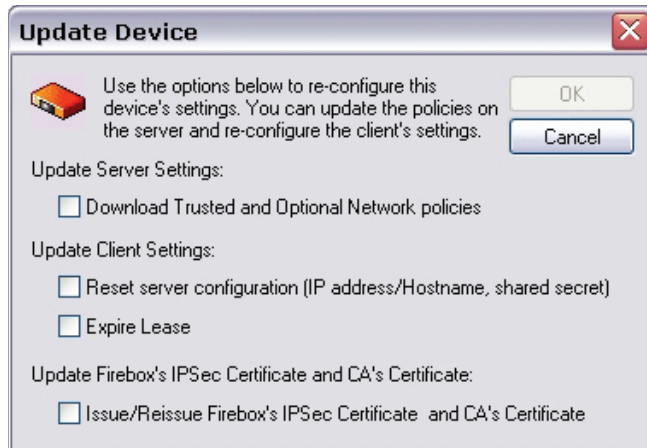
- Name:** Admin
- Phone:** 206.613.6600
- Cellular:** 206-250-6673
- Pager:** (empty)
- Fax:** (empty)
- E-mail:** admin@mywatchguard.com
- Web:** www.mywatchguard.com
- Address:** 505 Fifth Avenue South, Suite 500, Seattle, WA 98104, United States
- Notes:** (empty text area)

 On the right side of the dialog, there are three buttons: 'OK', 'Cancel', and 'Help'.

4. Make any necessary changes and click **OK**.

Update a device

1. On the device management page, click **Update Device**.
The Update Device dialog box appears.



2. Select the **Download Trusted and Optional Network Policies** check box to download the policies on the managed device to the Management Server for the trusted and optional networks. We recommend you do this to make sure you have the latest policies when you edit the device configuration and have not connected to the device in a long time.
3. If the device does not receive the update, refresh the Management Server configuration: select the **Reset Server Configuration** check box to refresh the Management Server IP address, hostname, shared secret, and lease time on the device. If you have made any changes to the device properties, make sure you select this check box.
4. Select the **Expire Lease** check box to expire the Management Server lease for the managed client and download any VPN or configuration changes.
5. (Does not appear for Edge) Select the **Issue/Reissue Firebox's IPSec Certificate and CA's Certificate** check box to issue or reissue the IPSec certificate for the Firebox and the Certificate Authority's certificate.
6. Click **OK**.

Remove a device

To remove a device so that it is no longer managed by the Management Server and no longer appears on the Management Server window:

1. On the left side of the Management Server window, click the icon for the device you want to remove and select **Edit > Remove**.
2. On the confirmation dialog box, click **Yes**.
3. Go to Policy Manager for that device, select **VPN > Managed Client**, and clear the **Enable this Firebox as a Managed Client** check box.

Start Firebox and Edge tools

The **Device Management** tab allows you to start other tools for device configuration and monitoring.

For Firebox devices, you can start:

- Policy Manager
- Firebox System Manager
- HostWatch
- Ping

For Edge devices, you can start:

- Edge Web Manager (Firebox X Edge only). Use Internet Explorer 6.0 or later. This link provides secure web access to the device's web user interface without the need to open any ports on the device.
- Policy Manager (SOHO 6 only)
- Firebox System Manager
- HostWatch
- Ping

VPN tunnels

You can see all tunnels that include the device in the Tunnels section. You can also add a VPN tunnel in this section.

1. On the Firebox X Edge or SOHO management page, find the VPN Tunnels section. This section shows all tunnels in which this device is a VPN endpoint.



2. Click **Add** to add a new VPN tunnel.
The Add VPN wizard starts. Configure the VPN to match your requirements.

For more information about the Add VPN wizard, see [Make managed tunnels between devices](#).

Add a VPN resource

For a VPN, you can configure (and put a limit to) the networks that have access through the tunnel. You can make a VPN between hosts or networks. To configure the networks that are available through a given VPN device, you define VPN resources.

The **Device Management** tab lists VPN resources currently defined. To add more VPN resources, see [Add VPN resources](#).

Configure network settings (Edge devices only)

With WatchGuard Management Server, you can configure the network settings for a group of Firebox X Edge devices. You can use WatchGuard System Manager to configure the unique network settings for each Firebox X Edge. Note that this procedure loads the current network settings for the Edge and enables central management of the device.



All Firebox X Edge network settings can be configured with the Edge web interface. For detailed information on these configuration options, see the Firebox X Edge help or documentation.

1. Select the **Device Management** tab on WatchGuard System Manager.
2. Under **Devices**, expand the **Edge appliances** folder and select a Firebox X Edge device.
The Edge configuration appears in the right pane.
3. Below **Network Settings**, click **Configure**.
The Network Settings dialog box appears.
4. To configure network settings, click each category of settings in the left pane of the dialog box and provide information in the fields that appear. For information on these fields and how to configure them, see the Firebox X Edge documentation.

Use the Firebox X Edge policy section



*The management page for a SOHO 6 does not have the **Policy** section.*

This section shows the Edge Configuration Template to which this Firebox X Edge is subscribed. If no template has been applied, you can drag the device to one of the Edge Configuration Templates. You can use the **Configure** link in this section to configure an existing Edge Configuration Template. For information about Edge Configuration Templates, see [Create and apply Edge Configuration Templates](#).

19 Firebox X Edge Centralized Management

About Edge centralized management

You can configure a Firebox X Edge for *centralized management*, which means that you can use WatchGuard System Manager to manage and configure Edge devices instead of using the configuration pages of the individual Edges. WatchGuard System Manager includes a number of features specifically for centralized management of Firebox X Edge devices. You can easily manage many Edge devices, make changes to the security policy for more than one Edge device at one time, and still have individual control over the configuration of each Edge. With a Management Server, you can also:

- Manage Firebox X Edge firmware updates. These updates can be scheduled and installed by the Management Server.
- Create Edge Configuration Templates, which are collections of configuration settings. for a group of Firebox X Edge devices. You create a configuration template on the Management Server, and install (subscribe) it on many Firebox X Edge devices. If you make a change to the configuration, the configuration is automatically updated on all subscribed Firebox X Edge devices.
- Use aliases to define a common destination for policy configuration on individual Firebox X Edge devices.

You can also manage Firebox SOHO 6 and SOHO 5 devices from WatchGuard System Manager, although you cannot configure them for centralized management. You cannot create Configuration Templates for the Firebox SOHO.



This section of topics describes how to use WatchGuard System Manager to manage Firebox X Edge devices, but it does not describe individual Edge configuration settings. For detailed information on configuring the Firebox X Edge, see the Firebox X Edge documentation.

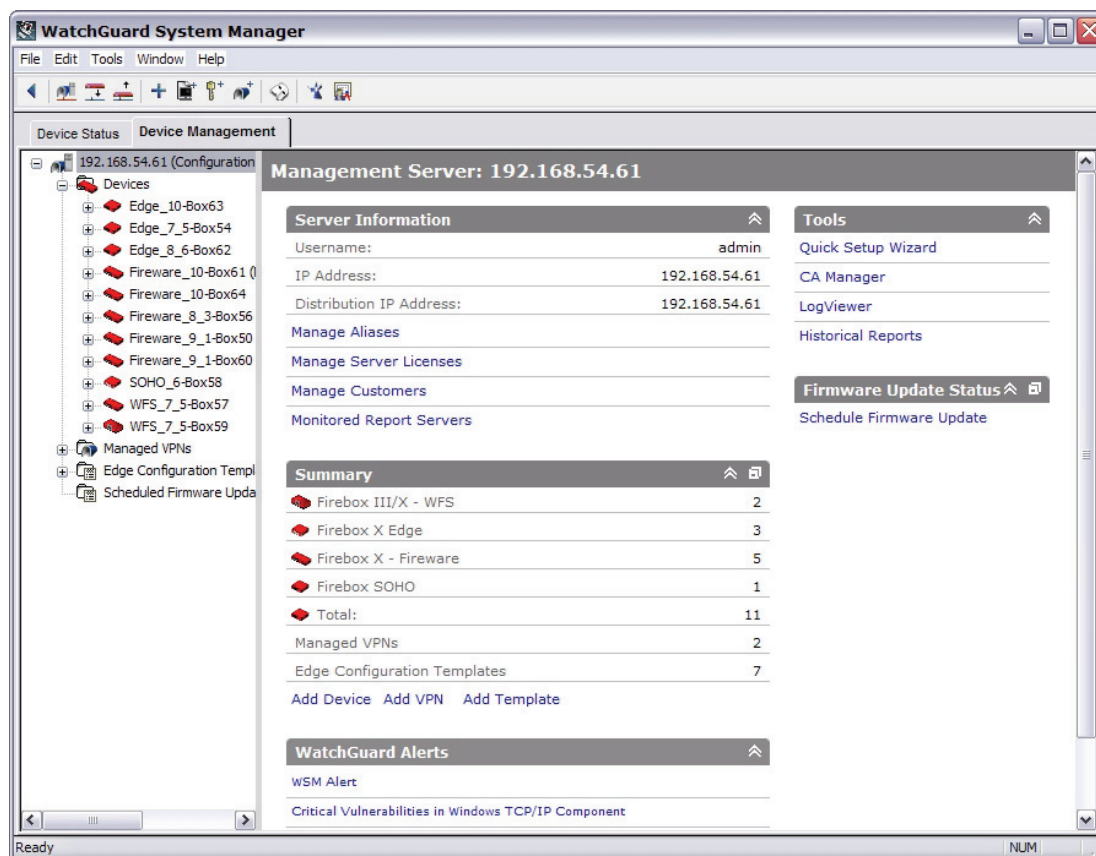
Schedule Firebox X Edge firmware updates

Firmware updates for Firebox X Edge devices must be installed on the Management Server. You can then use a single operation to update firmware on groups of Edge devices, either immediately or on a schedule.

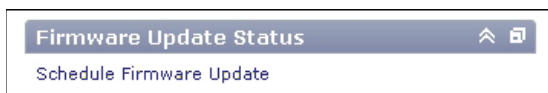
Current status of firmware updates appear on the **Device Management** tab, in the **Firmware Update Status** section.

You get firmware updates from LiveSecurity. You can download Edge firmware updates whenever you update the WSM software.

1. In the **Device Management** tab in WatchGuard System Manager, select the Management Server.
The Management Server settings page appears.



2. Look to the right for the **Firmware Update Status** section.
If any firmware updates are scheduled, they are shown here.



3. Click **Schedule Firmware Update**.
The Update Firmware wizard starts.
4. Read the Welcome screen and click **Next**.

5. Select the device type from the list and click **Next**.



In this version of WatchGuard System Manager, the only device types you can select are Firebox X Edge and Firebox X Edge e-Series.

6. Select the check box in front of each Firebox X Edge that you want to update. Click **Next**.
7. Select the firmware version to use. Click **Next**.
The Select the Time and Date page appears.

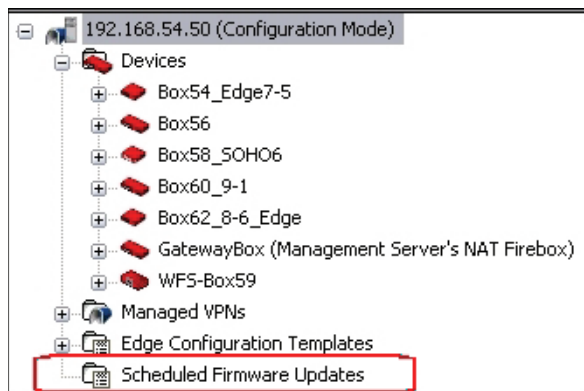


8. To update firmware immediately, select **Update firmware immediately**. To schedule the update for a time in the future, select **Schedule firmware update**.
9. If you selected **Schedule firmware update**, select the date from the **Date** field, and set the time in the **Time** field.
10. Click **Next**.
11. Click **Next**. Click **Close**.

The Firmware is updated if you selected Update firmware immediately, or scheduled if you selected Schedule firmware update.

See and delete firmware updates

1. On the **Device Management** tab, click **Scheduled Firmware Updates**.
The Scheduled Firmware Updates page appears.



Scheduled Firmware Updates						Add...
Task ID	Device	Type	Update Version	Scheduled Update Time	Status	
task_1001	Box54_Edge7-5	Firebox X Edge	7.5	Jul 28, 04:43:28 PM	Scheduled	

2. All scheduled firmware updates are shown. Firmware updates are shown separately for each device, even if more than one device is included in the same firmware update. For this reason, when you select a device, all devices included in that scheduled firmware update are also selected.
 - To delete a scheduled firmware update, right-click a device and select **Remove Scheduled Update**.
All devices in that firmware update task are removed from the schedule.
 - To cancel a scheduled firmware update, right-click a device and select **Cancel Scheduled Update**.
The task stays in the schedule, but its status changes to Cancelled.
 - To add a scheduled firmware update, click **Add**. Or, right-click and select **Add Scheduled Update**.
The Update Firmware wizard starts.

Create and apply Edge Configuration Templates

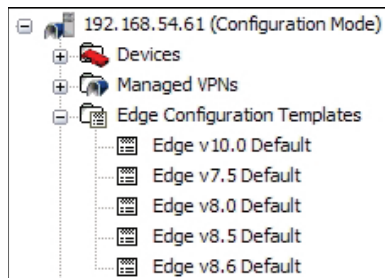
An Edge Configuration Template is a collection of configuration settings that multiple Edge devices can use. When you use Firebox X Edge devices with the WatchGuard Management Server, you can create Edge Configuration Templates on the Management Server. You can then apply those Edge Configuration Templates to Edge devices. With Edge Configuration Templates, you can easily configure standard firewall filters, change the Blocked Sites list, change your WebBlocker configuration, or change other policy settings for one or many managed Edge devices.

Edge Configuration Templates have the following restrictions:

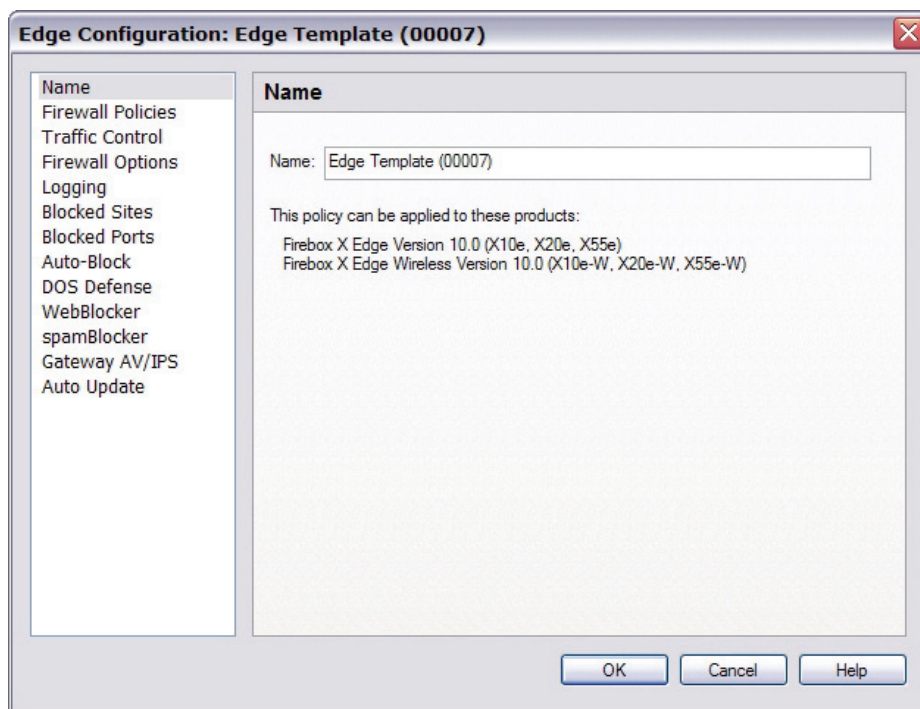
- Edge Configuration Templates can be used with the Firebox X Edge only.
- Each Edge can have only one Edge Configuration Template.
- An Edge must have firmware version 7.5 or later to use Edge Configuration Templates. You must use separate templates for Edges that run firmware versions 7.5, 8.0, 8.5, 8.6, or 10.0.

You can make changes to an Edge Configuration Template or to the list of devices to which the policy has been applied at any time. The Management Server automatically makes the changes.

1. Start WatchGuard System Manager and connect to the Management Server.
2. Click the **Device Management** tab.
You can expand the list of Edge Configuration Templates to see any Edge Configuration Templates that have been created. If you have not created any Edge Configuration Templates, this list is empty.
3. Right-click the Edge Configuration Templates heading.



4. Select **Insert Edge Configuration Template**.
The Product Version dialog box appears.
5. Select the product line and version from the drop-down list. Click **OK**.
The Edge Configuration: Edge Template window appears.



6. Type a name for the template.
7. To configure the policy, click each category of settings in the left pane of the dialog box and type information in the fields that appear. The categories listed depend on which version of the Edge you are defining the template for.
For information on the fields that appear, see the Firebox X Edge e-Series User Guide.
8. Click **OK** to close the Edge Configuration Template.
The template is saved to the Management Server, and an update is sent to all Firebox X Edge devices to which this template is applied.

Add a pre-defined policy with the Add Policy wizard

1. From the **Device Management** tab, on the left side of the screen, right-click **Edge Configuration Templates** and select **Insert Edge Configuration Template**.
The Product Version dialog box appears.
2. Select the product line and version from the drop-down list. Click **OK**.
The Edge Configuration Edge Template appears.
3. On the left side of the template, select **Firewall Policies** and click **Add**. The Add Policy wizard starts.
4. The Welcome page appears. Click **Next**.
The Select a policy type page appears.



5. To use a pre-defined policy, select **Choose a pre-defined policy from this list** and select the policy to use from the list.
6. Click **Next**.
7. If you use a pre-defined policy, select the traffic direction.
8. Select to deny or allow traffic for this policy and direction. The **From** and **To** boxes define the sources and destinations the policy. If you need to add a new resource, click **Add** beneath the **From** or **To** boxes and add the required information.

Add a custom policy with the Add Policy wizard

1. Start the Add Policy wizard. To do this, on the Firewall Policies page, click **Add** in the **Edge Configuration** dialog box.
2. The Welcome page appears. Click **Next**.



3. To create and use a custom policy, select **Create and use a new custom policy**.
4. Click **Next**.
The Specify Protocols page appears.
5. Type a name for the protocol.
6. To add a protocol, click **Add**.
The Add protocol dialog box appears.
7. Select to filter the TCP, UDP, or IP protocol.
8. Select one port or a range.
9. Type the port number or numbers, or the IP protocol number. Click **OK** to add the protocol.
10. Click **Add** to add another protocol. Click **Next** when all the protocols for this policy are added.
11. Select the traffic direction. Select **Incoming**, **Outgoing**, or **Optional**.
12. Select **Allow** or **Deny** for the filter action.
If the action is **Allow**, add the **From and To** destinations as required.
13. Click **Next**.
14. Click **Finish** to finish the wizard and return to the **Edge Configuration** dialog box.

Clone an Edge Configuration Template

To clone (copy) a template is useful when you have devices that use similar configurations, with slight variations. You can make one Edge Configuration Template, and then clone that policy for each variation, and make changes to those cloned templates.

1. Expand **Edge Configuration Templates** in the Device Management pane.
2. Right-click the Edge Configuration Template to be cloned, and select **Clone**.
A copy of the Edge Configuration Template appears in the list of Edge Configuration Templates.
3. Edit the cloned policy.

Apply Edge Configuration Templates to devices

You can apply an Edge Configuration Template to any number of Firebox X Edge devices. You cannot apply more than one Edge Configuration Template to the same Edge.

Applying the template using drag-and-drop

You can add an Edge Configuration Template to a Firebox X Edge device by drag-and-drop. Click the Edge device in the Devices list. Drag the Edge over the Edge Configuration Template in the Edge Configuration Templates list, and drop it on the policy. You can also drag a template and drop it on a device. The policy is added to the Edge.

If you have a folder of devices, you can drag the folder over the Edge Configuration Template to apply the Edge Configuration Template to all Edge devices in the folder. All other devices are skipped.

Applying the policy to devices in the device list

1. In the WatchGuard System Manager **Device Management** tab, expand the list of Edge Configuration Templates.
2. Select the template to add to a device.

The template appears in the right frame of the window.

Edge Configuration: Edge v10.0 Default

Firewall Policies

Action	Direction	Policy Name	From	To	Port	Log
✓ Allow	Optional	Outgoing	Any	Any	any:0	Disabled
✓ Allow	Outgoing	Outgoing	Any	Any	any	Disabled

[Configure](#)

Firewall Options

PING requests from External Network:	Do Not Respond
PING requests from Trusted Network:	Respond
PING requests from Optional Network:	Do Not Respond
FTP access from Trusted Network:	Allowed
Log All Allowed Outbound Access:	Disabled

[Configure](#)

Logging

WatchGuard Logging:	Disabled
Primary Log Server:	n/a
System:	Disabled

About

This configuration template is compatible with Firebox X Edge v10.0: (X10e, X20e, X55e, X10e-W, X20e-W, X55e-W)

Devices

[Configure](#)

Blocked Sites

There are no blocked sites.

[Configure](#)

- Click the **Configure** link below the **Devices** section.
The Manage Device List appears.



- Click **Add**.
The Select Devices dialog box appears.
- Select one or more devices from the list.
- Click **OK**. Click **OK** again.
The managed devices you select are subscribed to the Edge Configuration Template.

Remove an Edge from the device list

- To remove an Edge from the device list, in the WatchGuard System Manager **Device Management** tab, expand the list of Edge Configuration Templates.
- Click the **Configure** link below the **Devices** section.
The Manage Device List appears.
- Select the device you want to delete and click **Remove**.
The device is removed from the list, and from centralized management by WSM.

About aliases and Edge devices

Aliases are used with managed Firebox X Edge devices to define a common destination for policy configuration on the Management Server. For example, with aliases, you can create an Edge Configuration Template for a mail server, and define that policy to operate with your mail server. Because the mail server can have a different IP address on each Firebox X Edge network, you create an alias on the Management Server called MailServer. When you create the Edge Configuration Template for the mail server, you use this alias as the destination. Then you define that alias as either the source or destination, depending on the direction of the policy. In this example you can configure an incoming SMTP Allow policy with MailServer as the destination.

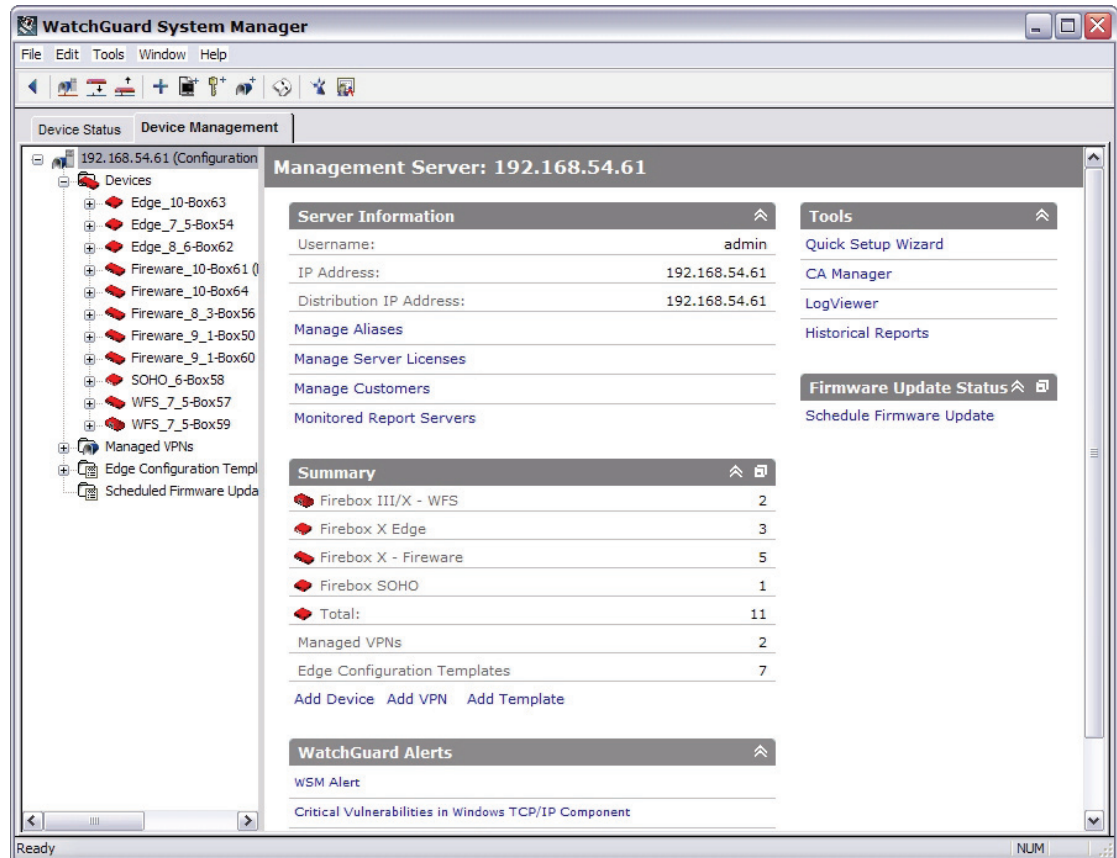
To make the Edge Configuration Template operate correctly on Edge devices that use the policy, you configure the MailServer alias in the Network Settings for each Firebox X Edge device.

Alias configuration is done in two steps:

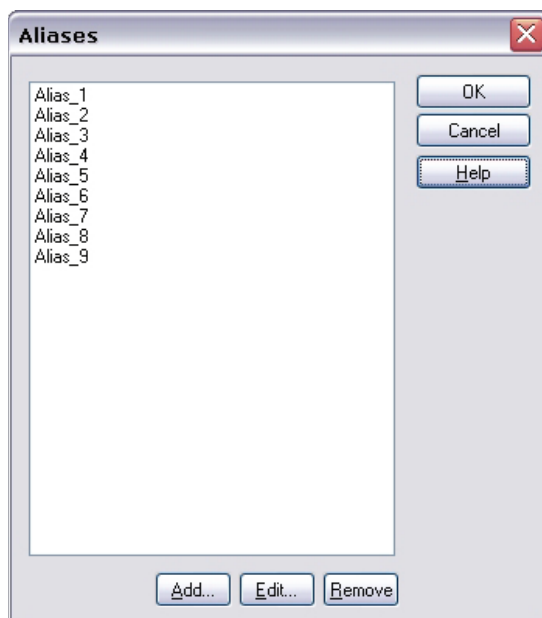
- [Give names to aliases](#)
- [Define aliases on a Firebox X Edge](#)

Give names to aliases

1. In the **Device Management** tab in WatchGuard System Manager, select the Management Server.
The Management Server settings page appears.



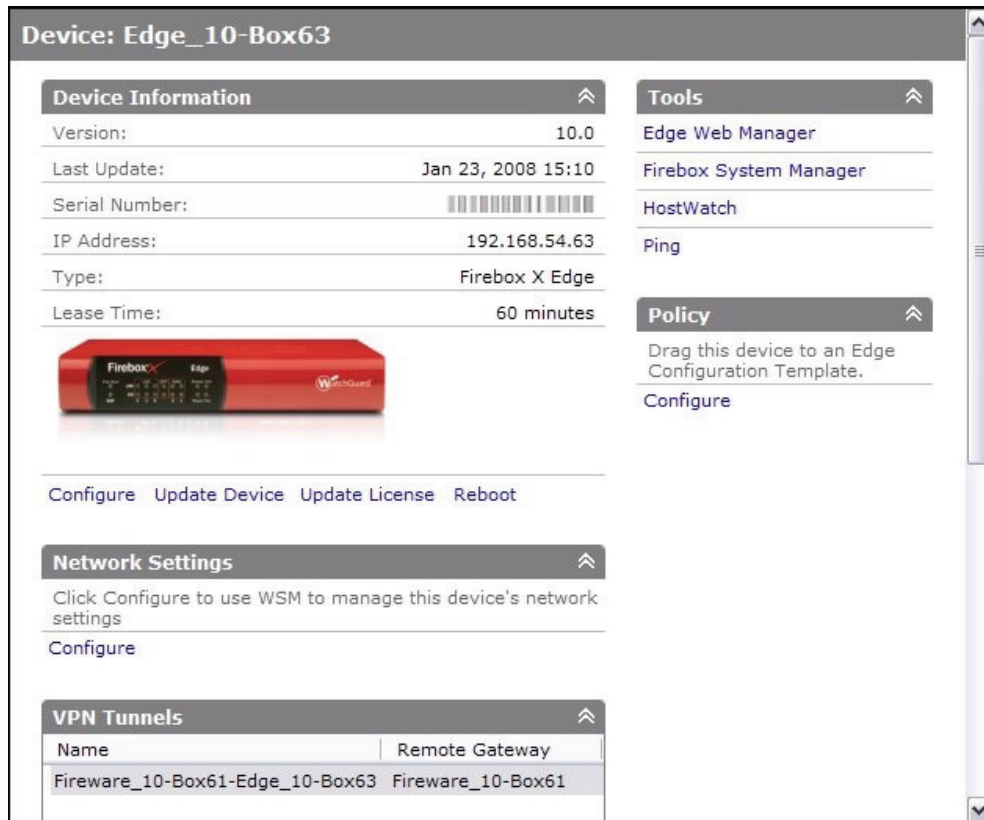
2. Click **Manage Aliases**.
The Aliases dialog box appears.



3. Select an alias and click **Edit** to edit the name.
4. Type a name for the alias and click **OK**.
5. Repeat this procedure for all aliases that you must define.
6. Click **OK** when all aliases are configured.

Define aliases on a Firebox X Edge

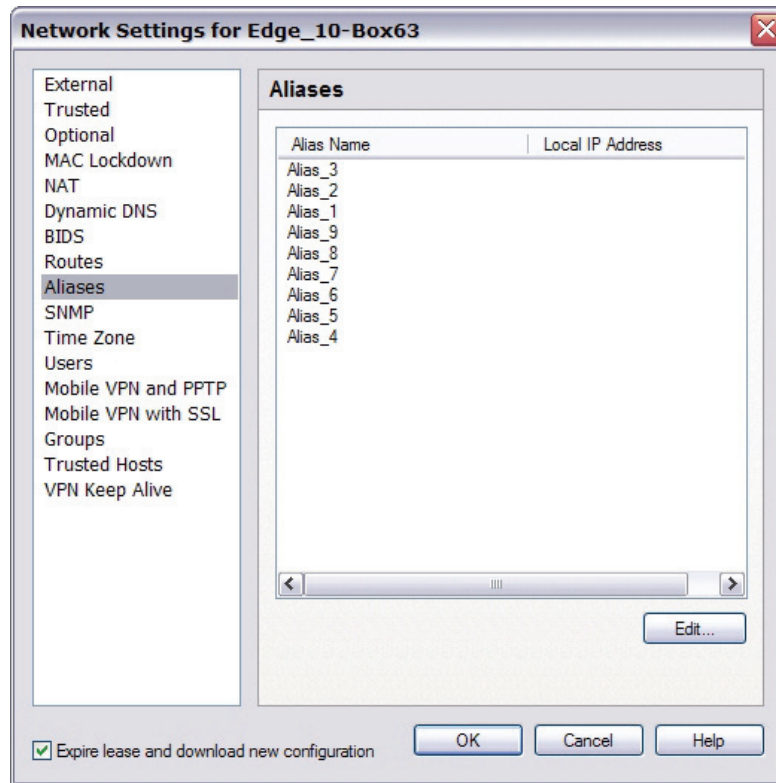
1. In the **Device Management** tab in WatchGuard System Manager, select a Firebox X Edge.
The Management Server settings page appears.



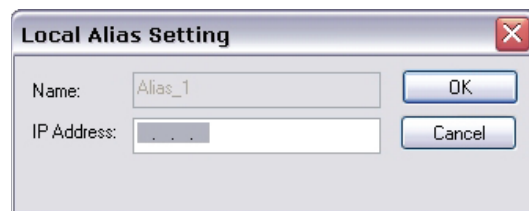
2. Click **Configure** under the **Network Settings** section.
The Network Settings dialog box appears.

3. Click **Aliases**.

The aliases appear. The aliases you named on the Management Server appear with those names in this dialog box.

4. Select an alias to define and click **Edit**.

The *Local Alias Setting* dialog box appears.

5. Type the IP address for the local alias on the network of this Firebox X Edge. Click **OK**.

6. Repeat the procedure for each alias to define.

7. Click **OK** when you have defined all aliases that you need.

20 Managed BOVPN Tunnels

About managed BOVPN tunnels

A VPN (Virtual Private Network) creates secure connections between computers or networks in different locations. Each 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 (BOVPN) 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 provides confidential connections between these offices, which streamlines communication, reduces the cost of dedicated lines, and retains security at each end.

With WatchGuard System Manager, you can quickly and easily make in minutes IPsec tunnels that use authentication and encryption. You can be sure that these tunnels operate with other tunnels and security policies. These tunnels are called *managed BOVPN tunnels*. Another type of tunnel is a *manual BOVPN tunnel*, which is a BOVPN tunnel that you use dialog boxes to define. For information on this type of tunnel, see [About manual BOVPN tunnels](#).

How to create a managed BOVPN tunnel

The basic procedure for creating a manual tunnel between devices is a very easy one that uses a drag-and-drop procedure and a simple wizard, as described in [Make managed tunnels between devices](#).

However, you must make sure you have done these procedures before you create managed tunnels:

1. Configure a WatchGuard Management Server and certificate authority as described in [Set up the Management Server](#) and [Configure the certificate authority on the Management Server](#).
2. Add the Fireboxes or Firebox X Edge devices that will be the tunnel endpoints to the Management Server, as described in [Add managed devices to the Management Server](#). If any of these devices are dynamic devices, they must be configured as managed clients, as described in [About preparing devices for management](#). Because WSM cannot initiate contact to dynamic devices, it does not automatically update the resources. You must then either download the current resources for the dynamic device or add the networks behind the dynamic device as VPN resources, as described in [Add VPN resources](#).

Tunnel options

You can use several options to customize managed VPN tunnels:

- If the trusted network behind one of the devices has many routed or secondary networks that you want to allow through the tunnel, you add them manually as VPN resources for the device, as described in [Add VPN resources](#).
- If you want to restrict the types of traffic you allow through the managed BOVPN, or if you want to restrict the types of traffic that send log messages to the Log Server, you must use a VPN Firewall policy template. Or, you can use one that is already defined on your Management Server. For more information, see [Add VPN Firewall policy templates](#).
- The wizard you use to create managed BOVPN tunnels allows you to choose from several settings for the available encryption types. These settings are appropriate for most tunnels. However, if your network has special requirements, you can create your own settings, as described in [Add security templates](#).

VPN Failover

VPN Failover, described in [Configure VPN Failover](#), is supported with managed BOVPN tunnels. If you have multi-WAN configured and you create managed tunnels, WSM automatically sets up gateway pairs that include the external interfaces of both ends of your tunnel. No other configuration is necessary.

Global VPN settings

Global VPN settings on your Firebox apply to all manual BOVPN tunnels, managed tunnels, and Mobile VPN tunnels. You can use these settings to:

- Enable IPSec pass-through.
- Clear or maintain the settings of packets with Type of Service (TOS) bits set.
- Use an LDAP server to verify certificates.
- Make the Firebox to send a notification when a BOVPN tunnel is down (BOVPN tunnels only).

To change these settings, from Policy Manager, select **VPN > VPN Settings**. For more information on these settings, see [About global VPN settings](#).

BOVPN tunnel status

You can use Firebox System Manager to see the current status of BOVPN tunnels. This information also appears on the **Device Status** tab of WatchGuard System Manager. For more information, see [VPN tunnel status and security services](#).

Rekey BOVPN tunnels

You can use Firebox System Manager to immediately generate new keys for BOVPN tunnels instead of waiting for them to expire. For more information, see [Rekey BOVPN tunnels](#).

Add VPN resources

A VPN resource is a network that is allowed to connect through a given VPN tunnel. If a VPN endpoint device has a static IP address, all trusted networks behind the device are automatically allowed to connect. The Management Server creates a default VPN resource for the device that includes all trusted networks.

However, if the trusted network behind a device has many routed or secondary networks that you want to allow through the tunnel, you add them manually as VPN resources for the device. If an endpoint device has a dynamic IP address, you must either get its current resources, as described below, or add any networks behind that device as VPN resources. The Management Server does not automatically create VPN resources for them.

Get the current resources from a device

If an endpoint device has a dynamic IP address, get the policies that already apply to the networks behind the device. Or, you can skip this procedure and add the networks as VPN resources instead.

1. In WatchGuard System Manager on the **Device Management** tab, select a managed device, and then select **Edit > Update Device**.


The Update Device dialog box appears.



2. Select the **Download Trusted and Optional Network policies** check box.
3. Click **OK**.

Create a new VPN resource

To make a VPN resource, on the **Device Management** tab:

1. Select the device for which you want to configure a VPN resource and click . Or, right-click the device and select **Insert VPN Resource**. The VPN Resource dialog box for that device appears.



2. In the **Policy Name** box, type a name for the policy. This name will appear in the Device Management window and in the Add VPN Wizard.
3. If you want to create a VPN resource for a Firebox X Core, Firebox X Peak, or WFS device, the **Disposition** field appears. From the **Disposition** drop-down list, select one of the following options:

secure

Encrypt traffic to and from this resource. This is the most commonly used option.

bypass

Sends the traffic in cleartext. You might use this option if one Firebox is in drop-in mode and the tunnel routes traffic to the drop-in network. In this case, the drop-in IP address must be bypassed but not blocked or the tunnel cannot negotiate.

block

Do not allow the traffic through the VPN. You might use this option to exclude one or more IP addresses from using a VPN that allows a full subnet, but only when given a higher precedence than the full subnet.

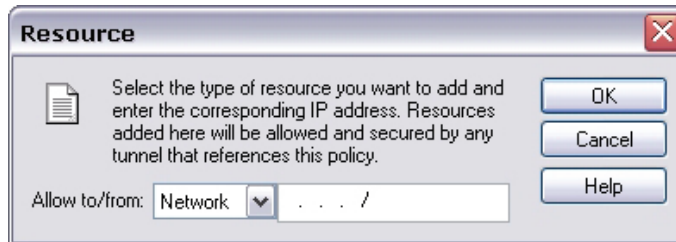


*If you want to create a VPN resource for a Firebox X Edge, the **Disposition** field does not appear because only the **secure** option is supported.*

4. Add, edit, or delete resources. Click **Add** to add an IP address or a network address. Click **Edit** to edit a resource that you have selected in the list. Select a resource in the **Resources** list and click **Remove** to delete a resource.
5. Click **OK**.

Add a host or network

1. From the **VPN Resource** dialog box, click **Add**.
The Resource dialog box appears.



2. From the **Allow to/from** drop-down list, select the resource type, and then type the IP address or network address in the adjacent address box.
3. Click **OK**.

Add VPN Firewall policy templates

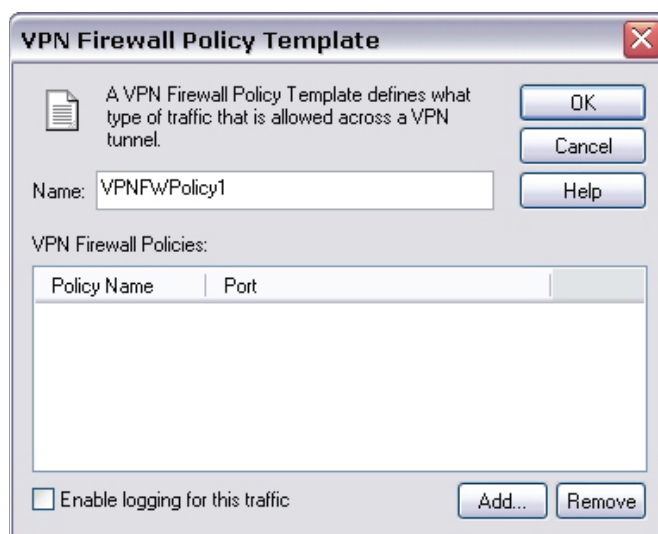
You use VPN Firewall Policy templates to create a set of one or more bidirectional firewall policies that restrict the type the traffic allowed across a VPN. Note that Policy Templates do not support proxy policies. If you use the default Any VPN firewall policy, a log message is generated for all traffic through the managed VPN tunnel. If you want to control what traffic is recorded in the logs, you must create your own VPN firewall policy template and use the **Enable logging for this traffic** check box. You cannot turn off logging for the default Any VPN firewall policy or change it in any way.

1. On the left side (tree view) of the **Device Management** tab, expand **Managed VPNs**, and click **VPN Firewall Policy Templates**.

A list of currently defined policy templates, if any, appears on the right side of the screen

2. In the upper-right corner of the screen, click **Add**.

The VPN Firewall Policy Template dialog box appears.



3. In the **Name** field, type a name for the Policy Template. This name will appear in the Device Management tree view and in the Add VPN wizard.

4. To add a policy to the template, click **Add**.
The Add Policy wizard starts.
5. Select from a list of pre-defined policies or create a custom policy. If you select to create a custom policy, use the wizard's next screen to type a name and select a port and protocol for the policy.
6. After you add the policy, you can repeat the procedure to add additional policies, if needed. Click **OK** when you are done.

Add Security Templates

A Security Template is a set of configuration information to be used when you create tunnels. When you use Security Templates, you do not need to individually create settings each time you create a tunnel. These templates include Phase 1 and Phase 2 settings. For more information on these settings, see [Configure mode and transforms \(Phase 1 settings\)](#) and [Configure Phase 2 settings](#).

Default Security Templates are supplied for the available encryption types. You can use these settings to create secure tunnels that work correctly for most networks. However, if your network has special requirements, you can modify the existing templates or make new templates. To make a Security Template:

1. On the **Device Management** tab, right-click in the window, and select **Insert Security Template** or click the Insert Security Template icon.



The Security Template dialog box appears.



2. In the **Template Name** box, type a name for the template. This name will appear in the Device Management tree view and in the Add VPN wizard.

- Click the **Phase 1 Settings** tab.

The screenshot shows the 'Security Template Properties' dialog box with the 'Phase 1 Settings' tab selected. The 'Name' tab is also visible. The 'IKE Keep-alive' checkbox is checked. The 'Message Interval' is set to 30 seconds, and the 'Max Failures' is set to 5. The 'Transform Settings' section is expanded, showing 'Authentication' set to SHA1-HMAC, 'Encryption' set to DES-CBC, and 'Key Group' set to Diffie-Hellman Group 1. The 'SA Lifetime' is set to 0 kilobytes and 24 hours. The 'OK', 'Cancel', and 'Help' buttons are at the bottom.

- To have the Firebox send messages to its IKE peer to keep the VPN tunnel open, select the **IKE Keep-alive** check box. To set the **Message Interval**, type the number of seconds or use the value control to select the number of seconds you want.
- To set the maximum number of times the Firebox tries to send an IKE keep-alive message before it tries to negotiate Phase 1 again, type the number you want in the **Max failures** box.
- From the **Authentication** and **Encryption** drop-down lists, select the authentication method and encryption method.
- From the **Key Group** drop-down list, select the Diffie-Hellman group you want. Diffie-Hellman groups determine the strength of the master key used in the key exchange process. The higher the group number, the greater the security but the more time is required to make the keys. For more information, see [About Diffie-Hellman groups](#).
- To change the SA (security association) life, type a number in the **SA Life** fields to define the amount of time or traffic that must pass before the SA expires. Enter a zero for no limit.

- Click the **Phase 2 Settings** tab.

The image shows a 'Security Template Properties' dialog box with three tabs: 'Name', 'Phase 1 Settings', and 'Phase 2 Settings'. The 'Phase 2 Settings' tab is selected. Inside the dialog, there is a section for 'ESP (Encapsulating Security Payload)' with two drop-down menus: 'Authentication' set to 'SHA1-HMAC' and 'Encryption' set to '3DES-CBC'. Below these, there is a checked checkbox for 'Force key expiration:'. Under this checkbox, there are two rows of settings: 'every 128000 kilobytes' and 'every 8 hours'. At the bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons.


- From the **Authentication** drop-down list, select the authentication method for Phase 2.
- From the **Encryption** drop-down list, select the encryption method.
- To force the key to expire, select the **Force Key Expiration** check box. In the fields below, enter a quantity of time and a number of bytes after which the key expires.
If **Force Key Expiration** is disabled, or if it is enabled and both the time and kilobytes are set to zero, the Firebox tries to use the key expiration time set for the peer. If this is also disabled or zero, the Firebox uses a key expiration time of 8 hours. You can set the time up to one year.
- Click **OK**.

Make managed tunnels between devices

You configure a tunnel with the Add VPN Wizard.

Dynamic Fireboxes and Firebox X Edge devices must have networks that are configured before you can use this procedure. You must also get the policies from any new dynamic devices before you configure tunnels. See [Add VPN resources](#).

On the **Device Management** tab:

1. On one of the tunnel endpoints, click the device name. Drag-and-drop the name to the device name at the other tunnel endpoint.
The Add VPN wizard starts.
Or, from the **Device Management** tab, select **Edit > Create a new VPN** or click the Create New VPN icon.

The Add VPN wizard starts.
2. Click **Next**.
3. If you used the drag-and-drop procedure in Step 1, the screen shows the two endpoint devices you selected with drag-and-drop, and the VPN resource that the tunnel uses. If you did not use drag-and-drop, select the endpoints from the drop-down list.
4. From the drop-down list, select a VPN resource for each device. (For more information on VPN resources, see the description at the beginning of [Add VPN resources](#)). Click **Next**.
Select **Hub Network** to make a null-route VPN tunnel to force all traffic through a VPN. Use this setting as the VPN resource for the device that hosts the null-route VPN. The remote device then sends all traffic through the VPN to the device that has **Hub Network** as the local resource.
5. Select the Security Template applicable for the type of security and type of authentication to use for this tunnel. For more information on Security Templates, see [Add Security Templates](#). Use the check boxes to specify the DNS and WINS servers you want to use. Click **Next**.
6. Select the VPN Firewall Policy Template applicable for the type of traffic you want to allow through this tunnel. If no VPN Firewall Policy Templates have been defined, the default Any policy applies to the tunnel. For more information on VPN Firewall Policy Templates, see [Add VPN Firewall policy templates](#).
7. Click **Next**.
The wizard shows the configuration.
8. Select the **Restart devices now to download VPN configuration** check box. Click **Finish** to start the devices again and deploy the VPN tunnel.

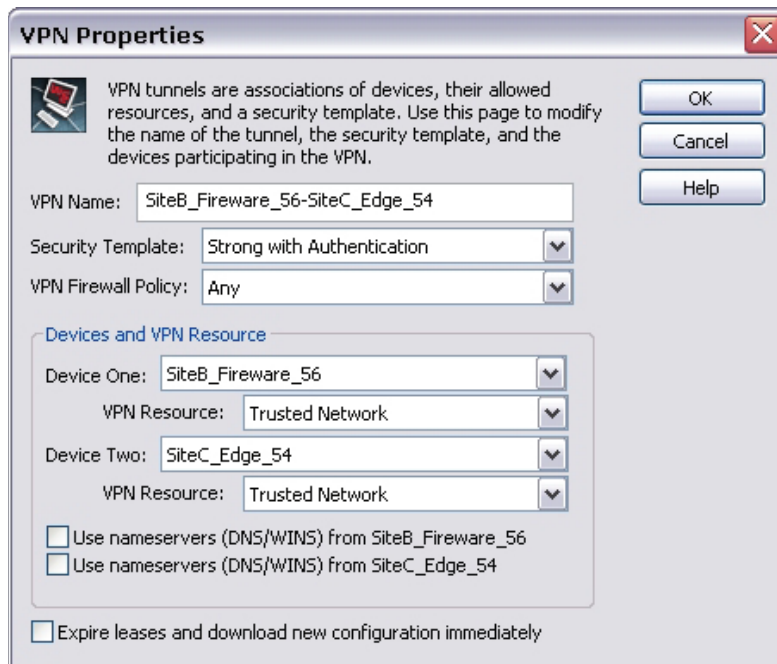
Edit a tunnel definition

You can see all your tunnels on the **Device Management** tab of WatchGuard System Manager (WSM). WSM lets you change the tunnel name, Security Template, endpoints, and the policy you use.

If you want to change the Policy Template or the Security Template for the tunnel, you can drag-and-drop the template name from the tree view at the left side of the **Device Management** tab to the VPN name in the tree view. The new template is applied. For other changes, or to use a dialog box to change a template:

1. On the **Device Management** tab, expand the tree to see the device to change and its policy.
2. Select the tunnel you want to change.
3. Right-click and select **Properties**.
The VPN Properties dialog box appears.
4. Make the changes you want to the tunnel. The fields on this dialog box are explained in previous sections.
5. Click **OK** to save the changes.

When the tunnel is renegotiated, the changes are applied.



The screenshot shows the "VPN Properties" dialog box. It has a title bar with a close button (X). Inside, there's a small icon of a laptop and a text box explaining that VPN tunnels are associations of devices, resources, and a security template. To the right of this text are three buttons: "OK", "Cancel", and "Help". Below the text, there are three input fields: "VPN Name" (containing "SiteB_Fireware_56-SiteC_Edge_54"), "Security Template" (a dropdown menu showing "Strong with Authentication"), and "VPN Firewall Policy" (a dropdown menu showing "Any"). Below these is a section titled "Devices and VPN Resource" in blue. It contains four input fields: "Device One" (containing "SiteB_Fireware_56"), "VPN Resource" (containing "Trusted Network"), "Device Two" (containing "SiteC_Edge_54"), and "VPN Resource" (containing "Trusted Network"). At the bottom, there are two checkboxes: "Use nameservers (DNS/WINS) from SiteB_Fireware_56" and "Use nameservers (DNS/WINS) from SiteC_Edge_54", both of which are unchecked. At the very bottom, there is another unchecked checkbox labeled "Expire leases and download new configuration immediately".

Remove tunnels and devices

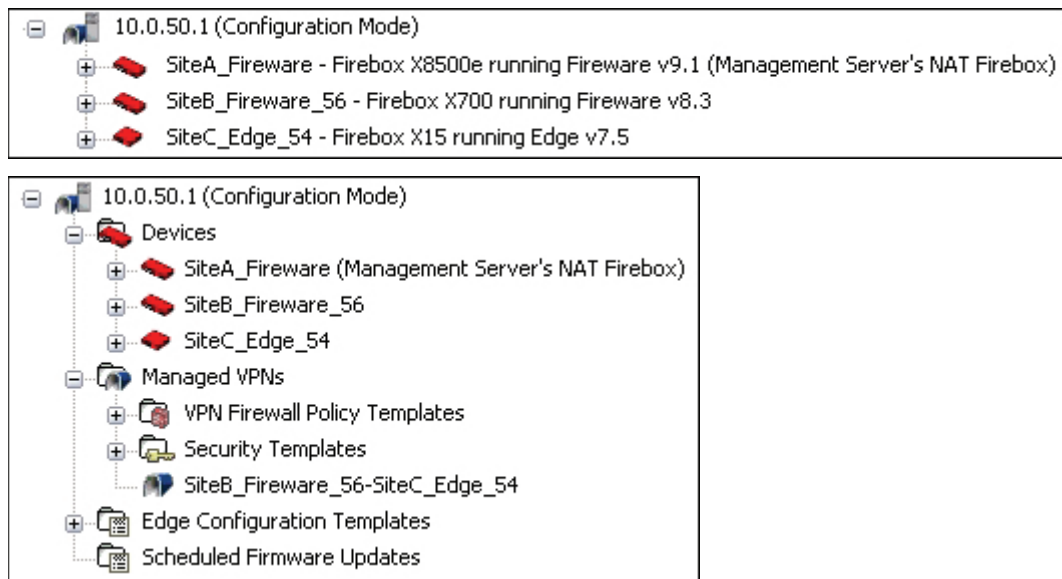
To remove a device from WatchGuard System Manager (WSM), you must first remove the tunnels for which that device is an endpoint.

Removing a tunnel

1. From WSM, click the **Device Management** tab.
2. Expand the **Managed VPNs** folder to show the tunnel you want to remove.
3. Right-click the tunnel.
4. Select **Remove**. Click **Yes** to confirm.
5. You may have to restart the devices that use the tunnel you want to remove. Click **Yes**.

Removing a device

1. From System Manager, click the **Device Status** or **Device Management** tab.




2. If you use the **Device Management** tab, expand the **Devices** folder to show the device to remove.
3. Right-click the device.
4. Select **Remove**. Click **Yes**.

VPN tunnel status and security services

The front panel of Firebox System Manager includes statistics about current VPN tunnels.

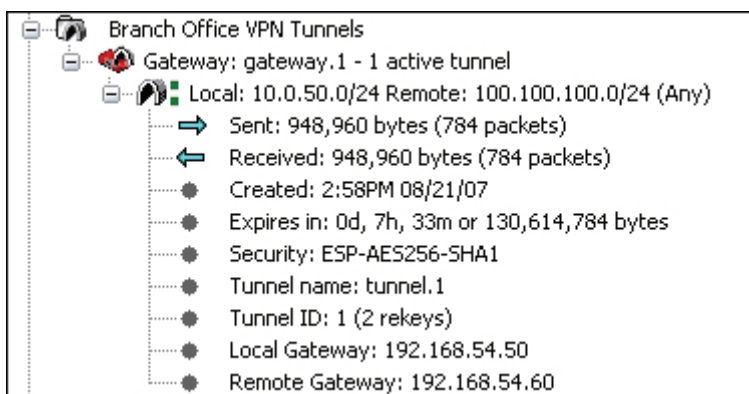
To open Firebox System Manager:

1. From WatchGuard System Manager, select the **Device Status** tab.
2. Select the Firebox to examine with Firebox System Manager.
3. Click .

Or, select **Tools > Firebox System Manager**.

Firebox System Manager appears. It may take a moment to connect to the Firebox to get information about the status and configuration.

Below the Firebox Status section on the right side of the screen is a section on BOVPN tunnels. Firebox System Manager shows the current tunnel status and gateway information for each VPN tunnel as well as data sent and received, creation and expiration information, type of authentication and encryption, and number of rekeys.



Each BOVPN tunnel is shown in one of three states:

Active

The BOVPN tunnel is operational and passing traffic.

Inactive

The BOVPN tunnel has been created, but no tunnel negotiation has occurred. No traffic has been sent through the VPN tunnel.

Expired

The BOVPN tunnel was active, but is no longer active because the tunnel has no traffic or because the link between the gateways is lost.

This information also appears on the **Device Status** tab in WatchGuard System Manager.

Mobile VPN tunnel status

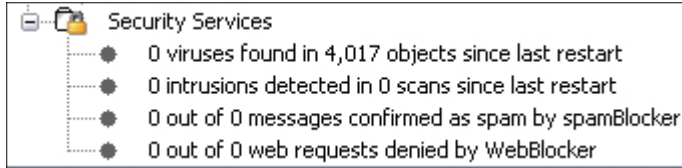
Firebox System Manager shows the user name, IP address information, and the quantity of sent and received packets for the three types of Mobile VPN Tunnels:

- Mobile VPN with IPSec
- Mobile VPN with SSL
- Mobile VPN with PPTP

To log off Mobile VPN users, right-click a user and select **Logoff selected user**.

Security Services status

Below Security Services, Firebox System Manager shows the number of viruses found, the number of intrusions, the number of email messages confirmed as spam, and the number of web requests denied by WebBlocker since the last restart.



21 Manual BOVPN Tunnels

About manual BOVPN tunnels

A *VPN (Virtual Private Network)* creates secure connections between computers or networks in different locations. Each 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 (BOVPN) 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 provides confidential connections between these offices, which streamlines communication, reduces the cost of dedicated lines, and retains security at each end.

Manual BOVPN tunnels are those created with dialog boxes, which provide many options for customizing tunnel definitions. Another type of tunnel is a *managed BOVPN tunnel*, which is a BOVPN tunnel that you create with a drag-and-drop procedure, a wizard, and the use of templates. For information on this type of tunnel, see [About managed BOVPN tunnels](#).

How to create a manual BOVPN tunnel

The basic procedure for creating a manual tunnel requires these steps:

1. [Configure gateways](#) — connection points on both the local and remote sides of the tunnel.
2. [Make tunnels between gateway endpoints](#) — configure routes for the tunnel, specify how the devices control security, and make a policy for the tunnel.

Other options you can use for BOVPN tunnels are described in the sections below.

Custom tunnel policies

The Firebox automatically adds new VPN tunnels to the BOVPN-Allow.in and BOVPN-Allow.out policies. This allows all traffic to use the tunnel. You can choose to not use this policy and instead create a custom VPN policy to allow specified policy types through the tunnel. For more information, see [Define a custom tunnel policy](#).

One-way tunnels

[Set up outgoing dynamic NAT through a BOVPN tunnel](#) if you want to keep the VPN tunnel open in one direction only. This can be helpful when you make a tunnel to a remote site where all VPN traffic comes from one public IP address.

VPN Failover

VPN tunnels automatically fail over to the backup WAN interface during a WAN failover. For more information on VPN Failover, see [Configure VPN Failover](#).

You can configure BOVPN tunnels such that they fail over to a backup peer endpoint if the primary endpoint becomes unavailable. To do this, you must define at least one backup endpoint, as described in [Configure VPN Failover](#).

Global VPN settings

Global VPN settings on your Firebox apply to all manual BOVPN tunnels, managed tunnels, and Mobile VPN tunnels. You can use these settings to:

- Enable IPsec pass-through.
- Clear or maintain the settings of packets with Type of Service (TOS) bits set.
- Use an LDAP server to verify certificates
- Make the Firebox send a notification when a BOVPN tunnel is down (BOVPN tunnels only).

To change these settings, from Policy Manager, select **VPN > VPN Settings**. For more information on these settings, see [About global VPN settings](#).

BOVPN tunnel status

You can use Firebox System Manager to see the current status of BOVPN tunnels. This information also appears on the **Device Status** tab of WatchGuard System Manager. For more information, see [VPN tunnel status and security services](#).

Rekey BOVPN tunnels

You can use Firebox System Manager to immediately generate new keys for BOVPN tunnels instead of waiting for them to expire. For more information, see [Rekey BOVPN tunnels](#).

Configure gateways

A gateway is a connection point for one or more tunnels. To create a tunnel, you must set up gateways on both the local and remote devices. To configure these gateways, you specify:

- Credential method—either pre-shared keys or an IPsec Firebox certificate. For information about using certificates for BOVPN authentication, see [Use a certificate for BOVPN tunnel authentication](#).
- Location of local and remote gateway endpoints, either by IP address or domain information.
- Settings for Phase 1 of the Internet Key Exchange (IKE) negotiation. This phase defines the security association—protocols and settings that the gateway endpoints will use to communicate—to protect data that is passed during the negotiation.

1. From Policy Manager, click **VPN > Branch Office Gateways**.
The Gateways dialog box appears.



- To add a gateway, click **Add**.
The New Gateway dialog box appears.

New Gateway

Gateway Name: SiteB

General Settings | Phase1 Settings

Credential Method

☒ Use Pre-Shared Key
☐ Use IPsec Firebox Certificate

Select the certificate to be used for the Gateway.

Id	Certificate Name	Algorithm

Gateway Endpoints

Local Gateway			Remote Gateway	
Type	ID	Interface	IP Address	Type
IP Address	50.50.50.50	External	23.23.23.23	IP Address

Buttons: Add..., Edit..., Delete, Move up, Move down

Buttons: OK, Cancel, Help

- In the **Gateway Name** text box, type a name to identify this gateway in Policy Manager for this Firebox.
- BOVPN tunnels are normally started automatically when the Firebox starts. If you do not want the tunnels that use this gateway to start automatically, clear the **Start Phase1 tunnel when Firebox starts** check box at the bottom of the screen. When this check box is cleared, tunnels start only when traffic is ready to be sent through them.
- You can now [Define the credential method](#) or [Define gateway endpoints](#).

Edit and delete gateways

To change the definition of a gateway, select **VPN > Branch Office Gateways**. Or, right-click on a tunnel icon in the **BOVPN** tab of Policy Manager, and select **Gateway Property**.

- Select the gateway you want and click **Edit**.
The Edit Gateway dialog box appears.
- Make the changes and click **OK**.

To delete a gateway, select the gateway and click **Remove**. You can also select multiple gateways and click **Remove** to delete them all at once.

Define the credential method

From the **New Gateway** dialog box, select either **Use Pre-Shared Key** or **Use IPSec Firebox Certificate** to identify the authentication procedure to use.

If you selected Pre-Shared Key

Type or paste the shared key. You must use the same shared key on the remote device. This shared key must use only standard ASCII characters.

If you selected Use IPSec Firebox Certificate

The table below the radio button shows current certificates on the Firebox. Select the certificate to be used for the gateway.

If you use a certificate for BOVPN authentication:

- The certificate must be recognized as an IPSec-type certificate by Firebox System Manager. To verify, Start Firebox System Manager, select **View > Certificates**, and make sure the **Type** column in the **Certificates** dialog box that appears says "IPSec" or "IPSec/Web."
- Make sure certificates for the devices at each gateway endpoint use the same algorithm. Either both must use DSS or both must use RSA. The algorithm for certificates appears in the table in the New Gateway dialog box and in the **Certificates** dialog box in Firebox System Manager.
- You must start the certificate authority on the Management Server if you select certificate-based authentication. For information on this, see [Configure the certificate authority on the Management Server](#).
- You must use the WatchGuard Log Server for log messages.

After you define the credential method, you can [define gateway endpoints](#) for the tunnel.

Define gateway endpoints

A set of gateway endpoints is known as a *gateway pair*.

1. In the Gateway Endpoints section of the **New Gateway** dialog box, click **Add**.
The *New Gateway Endpoints Settings* dialog box appears.

2. Specify the location of the local gateway.

If you want to use the IP address

- o Select the **By IP Address** radio button.
- o Select the address from the **IP address** drop-down list. All configured Firebox IP addresses appear in the list.
- o In the **External Interface** field, select whether to use the backup or main external interface. Click **OK**.

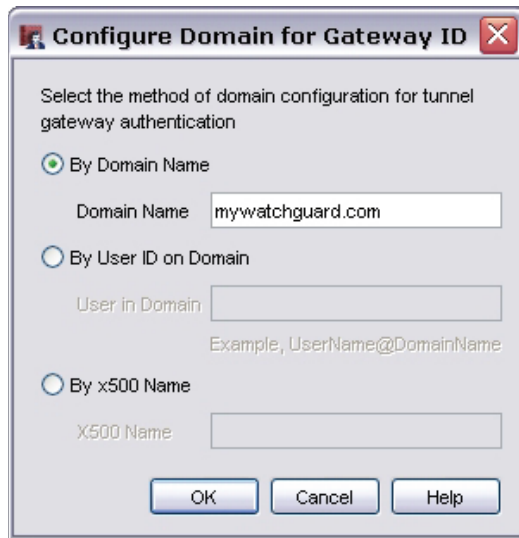
If you want to use domain information

- o Select the **By Domain Information** radio button. Click **Configure**.
- o In the **Configure Domain for Gateway ID** dialog box that appears, select either **By Domain Name**, **By User ID on Domain**, or **By X500 Name** to specify the method of domain configuration and external interfaces for tunnel gateway authentication.
- o Type either the domain name, user and domain name (UserName@DomainName), or x500 name according to which radio button you selected in the previous step. Click **OK**.



The X500 option is available only if you have Fireware Pro installed on your Firebox.

3. In the **External Interface** field, select whether to use the backup or main external interface. Click **OK**.



4. Specify the way the remote gateway obtains an IP address.

If it has a static IP address

- Select the **Static IP address** radio button
- Select the address from the **IP address** drop-down list or type it into the field.

If it has a dynamic IP address:

- Select the **Dynamic IP address** radio button.

5. Specify the remote gateway location for tunnel authentication.

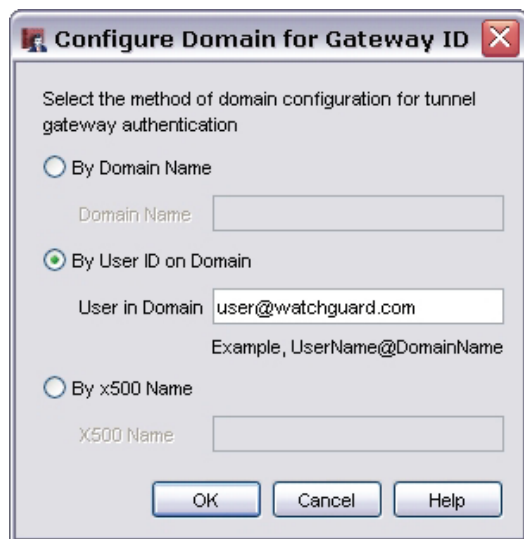
If you want to use the IP address

- Select the **By IP Address** radio button
- Select the address from the **IP address** drop-down list. All configured Firebox IP addresses appear in the list.

If you want to use domain information

- Make sure the Firebox is configured with DNS servers that can resolve the domain name.
- Select the **By Domain Information** radio button. Click **Configure**.

- From the **Configure Domain for Gateway ID** dialog box that appears, select either **By Domain Name**, **By User ID on Domain**, or **By X500 Name** to specify the method of domain configuration and external interfaces for tunnel gateway authentication.
- Type either the domain name, user and domain name (UserName@DomainName), or x500 name according to which radio button you selected in the previous step. Click **OK**.



*If the remote VPN endpoint uses DHCP or PPPoE to get its external IP address, set the ID type of the remote gateway to **Domain Name**. Set the peer name field to the fully qualified domain name of the remote VPN endpoint. The Firebox uses the IP address and domain name to find the VPN endpoint. Make sure the DNS server used by the Firebox can identify the name.*

6. Click **OK** to close the **New Gateway Endpoints Settings** dialog box.
The New Gateway dialog box appears. The gateway pair you defined appears in the list of gateway endpoints.
7. Go to [Configure mode and transforms \(Phase 1 settings\)](#) if you want to use Phase 1 settings other than the default values. Otherwise, click **OK**.

Configure mode and transforms (Phase 1 settings)

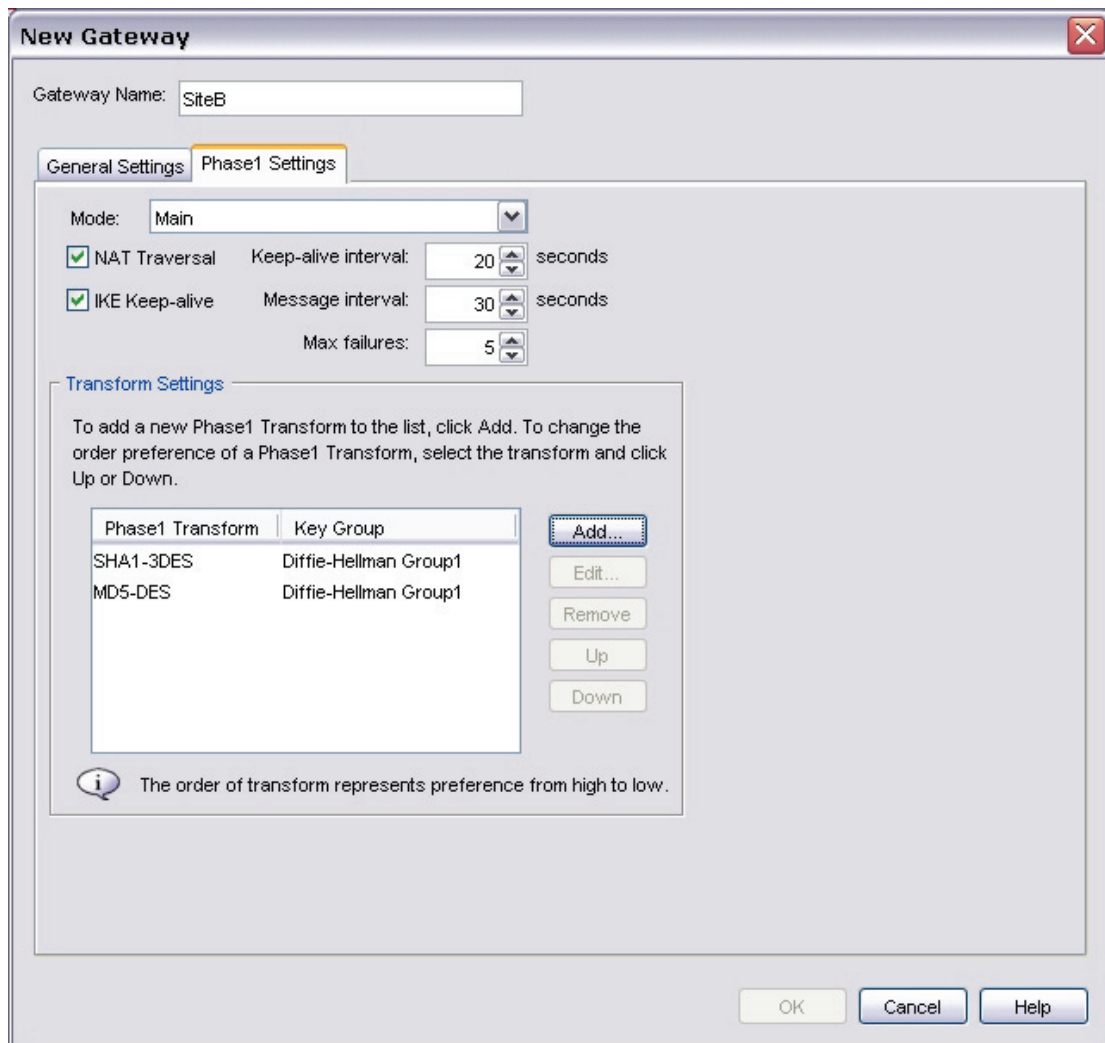
Phase 1 of establishing an IPSec connection is where the two peers make a secure, authenticated channel they can use to communicate. This is known as the ISAKMP Security Association (SA).

A Phase 1 exchange can use either *Main Mode* or *Aggressive Mode*. The mode determines the type and number of message exchanges that take place during this phase.

A transform is a set of security protocols and algorithms to protect data. During IKE negotiation, the peers make an agreement to use a certain transform.

You can define a tunnel such that it offers a peer more than one transform for negotiation, see [Add a Phase 1 transform](#).

1. On the **New Gateway** dialog box, select the **Phase1 Settings** tab.



New Gateway

Gateway Name: SiteB

General Settings | **Phase1 Settings**

Mode: Main

☒ NAT Traversal Keep-alive interval: 20 seconds

☒ IKE Keep-alive Message interval: 30 seconds

Max failures: 5

Transform Settings

To add a new Phase1 Transform to the list, click Add. To change the order preference of a Phase1 Transform, select the transform and click Up or Down.

Phase1 Transform	Key Group
SHA1-3DES	Diffie-Hellman Group1
MD5-DES	Diffie-Hellman Group1

Add... Edit... Remove Up Down

i The order of transform represents preference from high to low.

OK Cancel Help

2. From the **Mode** drop-down list, select **Main**, **Aggressive**, or **Main fallback to Aggressive**.

Main Mode

More secure; Uses three separate message exchanges (total of six messages). The first two negotiate policy; the next two exchange Diffie-Hellman data, and the last two authenticate the Diffie-Hellman exchange. Main Mode supports Diffie-Hellman groups 1, 2, and 5. This mode also enables you to use multiple transforms, as described in [Add a Phase 1 transform](#).

Aggressive Mode

Quicker because it uses only three messages, which exchange [Diffie-Hellman](#) data and identify the two VPN endpoints. The latter makes Aggressive Mode less secure.

Main fallback to aggressive

The Firebox attempts Phase 1 exchange with Main Mode. If the negotiation fails, it uses Aggressive Mode.

3. If you want to build a BOVPN tunnel between the Firebox and another device that is behind a NAT device, select the **NAT Traversal** check box. NAT Traversal, or UDP Encapsulation, allows traffic to get to the correct destinations.
4. To have the Firebox send messages to its IKE peer to keep the VPN tunnel open, select the **IKE Keep-alive** check box. To set the **Message Interval**, type the number of seconds or use the value control to select the number of seconds you want.
5. To set the maximum number of times the Firebox tries to send an IKE keep-alive message before it tries to negotiate Phase 1 again, type the number you want in the **Max failures** box.
6. Use the **Dead Peer Detection** check box to enable or disable traffic-based dead peer detection. When you enable dead peer detection, the Firebox queries a peer only if no traffic is received from the peer for a defined length of time and a packet is waiting to be sent to the peer. This method of finding dead IPSec peers is more scalable than IKE keep-alive messages.
If you want to change the Firebox defaults, enter the amount of time, in seconds, in the **Traffic idle timeout** field before the query is sent. In the **Max retries** field, enter the number of times the peer is queried before the peer is declared dead.
7. The Firebox contains one default transform set, which appears in the **Transform Settings** list. This transform specifies SHA1 authentication, 3DES encryption, and the Diffie-Hellman group 1.
You can either:
 - Use this default setting.
 - Remove it and replace it with a new one.
 - Add an additional setting, as explained in [Add a Phase 1 transform](#).

Add a Phase 1 transform

You can define a tunnel such that it offers a peer more than one transform for negotiation. For example, one transform might bundle SHA1-DES-DF1 ([authentication method]-[encryption method]-[key group]) and a second transform might consist of MD5-3DES-DF2, with the SHA1-DES-DF1 transform having a higher priority than MD5-3DES-DF2. When traffic passes through the tunnel, the security association can use either SHA1-DES-DF1 (first priority) or MD5-3DES-DF2 (second priority) depending on which of the transforms match the peer's transform.

You can include a maximum of nine transforms. You must specify Main Mode in step 2 of the previous procedure to use multiple transforms.

1. From the **Phase 1 Settings** tab of the **New Gateway** dialog box, find the **Transform Settings** box in the lower portion of the dialog box. Click **Add**.
The Phase1 Transform dialog box appears.
2. From the **Authentication** drop-down list, select **SHA1** or **MD5** as the type of authentication.
3. From the **Encryption** drop-down list, select **AES (128-bit)**, **AES (192-bit)**, **AES (256-bit)**, **DES**, or **3DES** as the type of encryption.
4. To change the SA (security association) life, type a number in the **SA Life** field, and select **Hour** or **Minute** from the drop-down list.
5. From the **Key Group** drop-down list, select the Diffie-Hellman group you want. WatchGuard supports groups 1, 2, and 5.
Diffie-Hellman groups determine the strength of the master key used in the key exchange process. The higher the group number, the greater the security but the more time is required to make the keys. For more information, see [About Diffie-Hellman groups](#).
6. You can add up to nine transforms. You can select a transform and select the **Up** or **Down** key to change the priority of transforms.
7. Click **OK**.

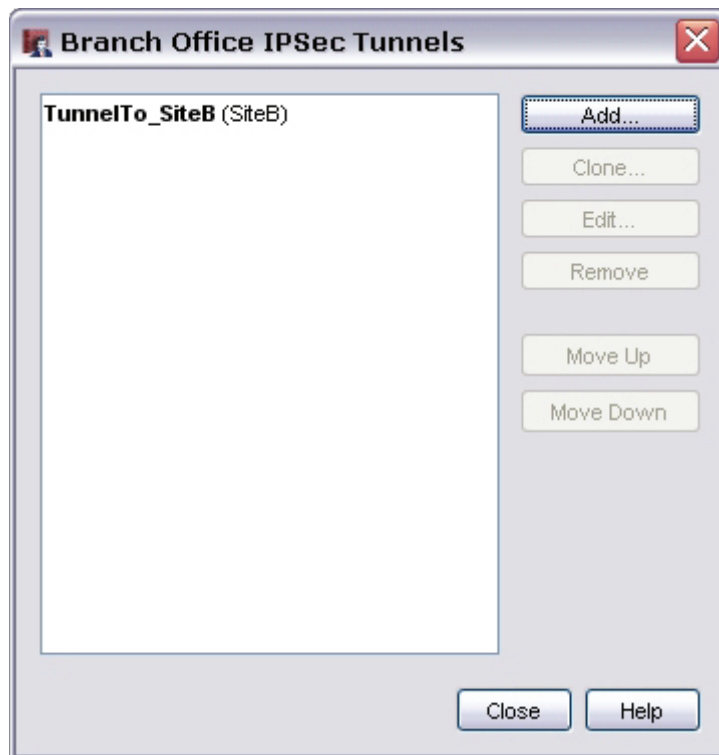
Make tunnels between gateway endpoints

After you define gateway endpoints, you can make tunnels between them. To make a tunnel, do the following:

- [Define a tunnel](#)
- [Configure Phase 2 settings](#) for the Internet Key Exchange (IKE) negotiation. This phase sets up security associations for the encryption of data packets.

Define a tunnel

1. From Policy Manager, select **VPN > Branch Office Tunnels**.
The Branch Office IPsec Tunnels dialog box appears.






2. Click **Add**.

The New Tunnel dialog box appears.

New Tunnel

Tunnel Name:




Gateway:   

Addresses | Phase2 Settings



Addresses

Configure tunnel routes for the tunnel.

Local	Dir	Remote
10.0.1.0/24	<==>	192.168.111.0/24

☒ Add this tunnel to the BOVPN-Allow policies

3. In the **Tunnel Name** box, type a name for the tunnel.
Make sure the name is unique among tunnel names as well as all Mobile VPN group names and interface names.
4. From the **Gateway** list, select the gateway for this tunnel to use.
If you want to edit existing gateways, select the name and click the **Edit** button.
Follow the procedures described in [Configure gateways](#). 
If you want to add a new gateway, click the **New** button.
Follow the procedure described in [Configure gateways](#). 
5. Select the **Add this tunnel to the BOVPN-Allow policies** check box at the bottom of the dialog box if you want to add the tunnel to the BOVPN-Allow.in and BOVPN-Allow.out policies. These policies allow all traffic that matches the tunnel's routes. If you want to restrict traffic through the tunnel, clear this check box and use the BOVPN Policy wizard as described in [Define a custom tunnel policy](#) to create policies for types of traffic that you want to allow through the tunnel.

You can now [Add routes for a tunnel](#) or [Configure Phase 2 settings](#).

Edit and delete a tunnel

To change a tunnel, select **VPN > Branch Office Tunnels**. Or, right-click on a tunnel icon in the **Branch Office VPN** tab of Policy Manager, and select **Tunnel Property**.

1. Select the tunnel and click **Edit**.
The Edit Tunnel dialog box appears.
2. Make the changes and click **OK**.

To delete a tunnel from the **Branch Office IPSec Tunnels** dialog box, select the tunnel and click **Remove**. You can also select multiple tunnels and click **Remove** to delete them all at once.

Add routes for a tunnel

1. On the **New Tunnel** dialog box, click **Add**.
The Tunnel Route Settings dialog box appears.

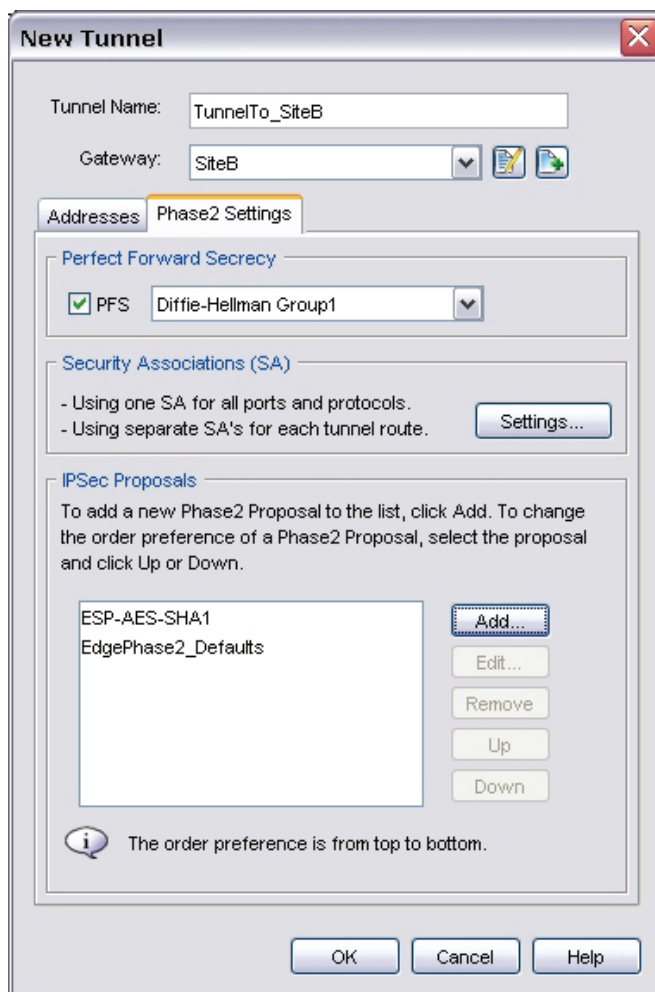
2. From the **Local** drop-down list, select the local address you want.
You can also click the button adjacent to the **Local** drop-down list to enter a host IP address, network address, a range of host IP addresses, or a DNS name.
3. In the **Remote** box, type the remote network address.
You can also click the adjacent button to enter a host IP address, network address, a range of host IP addresses, or a DNS name.
4. From the **Direction** drop-down list, select the direction for the tunnel. The tunnel direction determines which endpoint of the VPN tunnel can start a VPN connection through the tunnel.
5. You can enable 1-to-1 NAT and dynamic NAT for the tunnel, depending on the address types and tunnel direction you select for the tunnel. Select the **1:1 NAT** check box or the **DNAT** check box.
6. If you selected the **1:1 NAT** check box, click the adjacent button to enter the address you want to change. You can specify a host IP address, network address, a range of host IP addresses, or a DNS name.
If you want to use dynamic NAT, you must set a unidirectional tunnel from LAN1 to LAN2 where you want all LAN1 servers to connect to LAN2 servers but appear as only one IP address on LAN2. For information on how to do this, see [Set up outgoing dynamic NAT through a BOVPN tunnel](#).
7. Click **OK**.

Configure Phase 2 settings

Phase 2 settings include settings for a security association (SA), which defines how data packets are secured when they are passed between two endpoints. The SA keeps all information necessary for the Firebox to know what it should do with the traffic between the endpoints. Parameters in the SA can include:

- Encryption and authentication algorithms used.
- Lifetime of the SA (in seconds or number of bytes, or both).
- IP address of the device for which the SA is established (the device that handles IPSec encryption and decryption on the other side of the VPN, not the computer behind it that sends or receives traffic).
- Source and destination IP addresses of traffic to which the SA applies
- Direction of traffic to which the SA applies (there is one SA for each direction of traffic, incoming and outgoing).

1. From the **New Tunnel** dialog box, click the **Phase2 Settings** tab.



2. Select the **PFS** check box if you want to enable Perfect Forward Secrecy (PFS). If you enable PFS, select the Diffie-Hellman group.

Perfect Forward Secrecy gives more protection to keys that are created in a session. Keys made with PFS are not made from a previous key. If a previous key is compromised after a session, your new session keys are secure. Diffie-Hellman Group 1 uses a 768-bit group to create the new key exchange, Diffie-Hellman Group 2 uses a 1024-bit group, and Diffie-Hellman Group 5 uses a 1536-bit group. For more information, see [About Diffie-Hellman groups](#).

3. To set advanced SA parameters, such as specifying that all ports/protocols will use the same SA, click **Settings**. For information on the fields used to set advanced SA parameters, see [Use advanced Security Association \(SA\) settings](#).
4. The Firebox contains one default proposal, which appears in the **IPSec Proposals** list. This proposal specifies the ESP data protection method, AES encryption, and SHA1 authentication. You can either:
 - o Use this default proposal.
 - o Remove it and replace it with a new one.
 - o Add an additional proposal, as explained in [Add a Phase 2 proposal](#).

If you plan to use the IPSec pass-through feature, you must use a proposal that specifies ESP (Encapsulating Security Payload) as the proposal method. IPSec pass-through supports ESP but not AH. For more information on IPSec pass-through, see [About global VPN settings](#).

Use advanced Security Association (SA) settings

1. From the **Phase2 Settings** tab of the **New Tunnel** dialog box, click **Settings**.
The Advanced SA Settings dialog box appears.
2. Define addressing and service usage for the SA:

Create one SA that includes all tunnel routes

This check box controls whether or not a unique SA is created for each Local/Remote address pair in your VPN tunnel definition. We recommend you keep this check box cleared. Most IPSec devices create an SA for each Local/Remote address pair. This is compliant with the RFC and increases Firebox interoperability with other vendors' IPSec devices, but can affect your BOVPN license count as each SA is equal to one BOVPN tunnel. Select this check box only if you know that the other VPN endpoint can put all Local/Remote address pairs into one SA. If you want to use Any as the source address, destination address, or both, select **Use Any for source address in selector** or **Use Any for destination address in selector**.

Create one SA that includes all ports and protocols

This check box specifies, when selected, that all ports/protocols will use the same SA. If you clear this check box, one SA will be created for each unique port/protocol pair. We recommend you keep this check box selected because many IPSec devices cannot make an SA that includes port and protocol information. This is compliant with the RFC and increases Firebox interoperability with other vendors' IPSec devices. You can still filter the traffic that the Firebox allows to go through the VPN tunnel with the firewall policies on your Firebox. The Firebox sends traffic to the IPSec module only if there is a firewall policy to allow the traffic. Even if an SA is for all ports and protocols, your firewall policies control what is allowed in and out of your network. Clear this check box only if you know that the other VPN endpoint can make an SA that can select traffic by port or protocol. If you do this, you must control what port is used by each SA in your firewall policies.

Add a Phase 2 proposal

You can define a tunnel such that it offers a peer more than one proposal for Phase 2 of the IKE. For example, you might specify ESP-3DES-SHA1 in one proposal, and ESP-DES-MD5 for second proposal. When traffic passes through the tunnel, the security association can use either ESP-3DES-SHA1 (first priority) or ESP-DES-MD5 (second priority) depending on which of the proposals match the peer's transform.

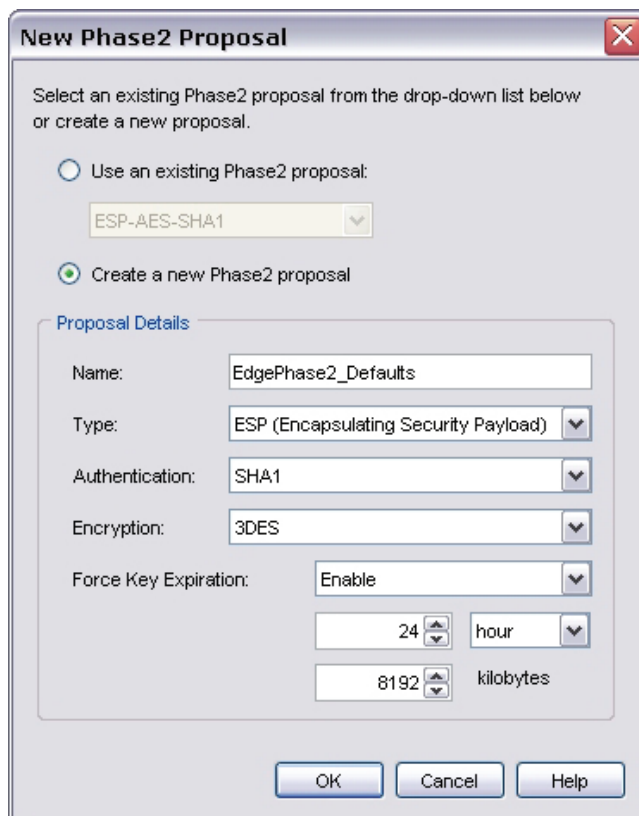
You can include a maximum of nine proposals.

1. To add a new proposal, from the **Phase2 Settings** tab of the **New Tunnel** dialog box, in the **IPSec Proposals** section, click the **Add** button.

Or,

From Policy Manager, select **VPN > Phase2 Proposals**. From the **Phase2 Proposals** dialog box, click **Add**.

The New Phase2 Proposal dialog box appears.



The dialog box is titled "New Phase2 Proposal" and contains the following elements:

- Instructions:** "Select an existing Phase2 proposal from the drop-down list below or create a new proposal."
- Radio Buttons:**
 - ☐ Use an existing Phase2 proposal: Below this is a drop-down menu showing "ESP-AES-SHA1".
 - ☒ Create a new Phase2 proposal
- Proposal Details Section:**
 - Name:** EdgePhase2_Defaults
 - Type:** ESP (Encapsulating Security Payload)
 - Authentication:** SHA1
 - Encryption:** 3DES
 - Force Key Expiration:** Enable
 - 24 hour
 - 8192 kilobytes
- Buttons:** OK, Cancel, Help

Add an existing proposal

1. Select the **Use an existing Phase 2 proposal** check box.
2. From the drop-down list, select the proposal you want to add. Click **OK**.

Create a new proposal

1. From the **New Phase2 Proposal** dialog box, select the **Create a new Phase 2 proposal** check box.
or
From Policy Manager, select **VPN > Phase2 Proposals**. The **Phase2 Proposals** dialog box appears.
Click **Add**.
2. Type a name for the new proposal. If you opened the dialog box from **VPN > Phase 2 Proposals**, an optional **Description** field appears.
From the **Type** drop-down list, select **ESP** or **AH** as the proposal method.
We recommend that you use ESP (Encapsulating Security Payload). The differences between ESP and AH (Authentication Header) are:
 - o ESP is authentication with encryption.
 - o AH is authentication only. ESP authentication does not include the protection of the IP header, while AH does.
 - o IPSec pass-through supports ESP but not AH. If you plan to use the IPSec pass-through feature, you must specify ESP as the proposal method. For more information on IPSec pass-through, see [About global VPN settings](#).
3. From the **Authentication** drop-down list, select **SHA1**, **MD5**, or **None** for the authentication method.
4. (If you selected **ESP** from the **Type** drop-down list) From the Encryption drop-down list, select the encryption method.
The options are DES, 3DES, and AES 128, 192, or 256 bit, which appear in the list from the most simple and least secure to most complex and most secure.
5. To make the gateway endpoints generate and exchange new keys after a quantity of time or amount of traffic passes, select the **Force Key Expiration** check box. In the fields below, enter a quantity of time and a number of bytes after which the key expires.
If Force Key Expiration is disabled, or if it is enabled and both the time and kBytes are set to zero, the Firebox tries to use the key expiration time set for the peer. If this is also disabled or zero, the Firebox uses a key expiration time of 8 hours.
You can set the time up to one year.
6. Click **OK**.

Edit or clone a proposal

To clone a proposal is to copy an existing proposal to a new name and make changes. You must do this if you want to edit a predefined proposal because you can edit only user-defined proposals.

1. From Policy Manager, select **VPN > Phase2 Proposals**.
The Phase2 Proposals dialog box appears.
2. Select a proposal and click **Edit** or **Clone**.
3. Make changes to the fields as described in the **Create a new proposal** section of this topic. Click **OK**.

Change order of tunnels

Order of tunnels is particularly important when more than one tunnel uses the same routes or when the routes overlap. A tunnel higher in the list of tunnels on the **Branch Office IPSec Tunnels** dialog box takes precedence over a tunnel below it when traffic matches tunnel routes of multiple tunnels.

You can change the order in which the Firebox attempts connections:

1. From Policy Manager, select **VPN > Branch Office Tunnels**.
The Branch Office IPSec Tunnels dialog box appears.
2. Select a tunnel and click **Move Up** or **Move Down** to move it up or down in the list.

Define a custom tunnel policy

Tunnel policies are sets of rules that apply to tunnel connections.

By default, a new VPN tunnel is automatically added to the BOVPN-Allow.in and BOVPN-Allow.out policies, which allow all traffic to use the tunnel. You can configure the tunnel such that it is not added to this policy. See [Define a tunnel](#) to make sure you clear the **Add this tunnel to the BOVPN-Allow policies** check box. Then, create a custom VPN policy to allow specified policy types. You can also keep the default setting of adding the tunnel to BOVPN-Allow.in and BOVPN-Allow.out and then add other policies for other types of traffic, such as HTTP proxy.

1. From Policy Manager, select **VPN > Create BOVPN Policy**.
The BOVPN Policy Wizard starts.
2. Click through the wizard and add the information it asks for. The wizard has these screens:

Choose a name for the policies

The name is prepended to .in and .out to create the firewall policy names for incoming and outgoing tunnels, respectively. For example, if you use williams as the name base, the wizard creates the policies williams.in and williams.out.

Select the policy type

Specify the traffic type allowed to pass through the BOVPN tunnel.

Select the BOVPN tunnels

Select the BOVPN tunnels to which the policies created by this wizard will apply.

Create an alias for the tunnels

(Optional) As with the policy name, the name you specify is prepended to .in and .out to create the alias names for incoming and outgoing tunnels, respectively. You can use these aliases in other policies as well.

You should consider creating an alias when you create policies for many BOVPN tunnels. Include those tunnels in the alias. You can then modify the alias as you add or remove tunnels instead of regenerating the policy. For information on how to create an alias, see [Create an alias](#).

The BOVPN Policy Wizard has completed successfully

The final screen tells you which policies and aliases were created by the wizard.

Set up outgoing dynamic NAT through a BOVPN tunnel

You can use dynamic NAT through BOVPN tunnels. Dynamic NAT acts as unidirectional NAT, and keeps the VPN tunnel open in one direction only. This can be helpful when you make a BOVPN to a remote site where all VPN traffic comes from one public IP address.

For example, suppose you want to create a BOVPN tunnel to a business partner so you can get access to their database server, but you do not want this company to get access to any of your resources. Your business partner wants to allow you access, but only from a single IP address so they can monitor the connection.

You must have the external IP address and the trusted network address of each VPN endpoint to do this procedure. If you enable dynamic NAT through a BOVPN tunnel, you cannot use the VPN Failover feature for that VPN tunnel.

1. From Policy Manager at your site, select **VPN > Branch Office Tunnels**. Select **Add** to add a new BOVPN tunnel.
2. Give the BOVPN tunnel a name.
3. Select the New Gateway icon (button at the far right of the **Gateway** field).
The New Gateway dialog box appears.

New Gateway

Gateway Name: SiteB

General Settings | Phase1 Settings

Mode: Main

☒ NAT Traversal Keep-alive interval: 20 seconds

☒ IKE Keep-alive Message interval: 30 seconds

Max failures: 5

Transform Settings

To add a new Phase1 Transform to the list, click Add. To change the order preference of a Phase1 Transform, select the transform and click Up or Down.

Phase1 Transform	Key Group
SHA1-3DES	Diffie-Hellman Group1
MD5-DES	Diffie-Hellman Group1

The order of transform represents preference from high to low.

4. Create a new gateway, as described in [Configure gateways](#).
5. Click **OK** to return to the **New Tunnel** dialog box.
6. On the **Addresses** tab, click **Add**. Use the procedure that starts with "From the Local drop-down list" at [Add routes for a tunnel](#) to add a new tunnel route. Make sure you select the **DNAT** check box.
7. Click **OK**. Save these changes to the Firebox.
8. From Policy Manager at the remote site, select **VPN > Branch Office Tunnels**. Select **Add** to add a new BOVPN tunnel.
9. Do steps 2 – 7 at the remote site, but do not select the **DNAT** check box.

When the Firebox at the remote site restarts, the two Firebox devices negotiate a VPN tunnel. Your Firebox applies dynamic NAT to all traffic destined for the trusted network of the remote site. When this traffic reaches the remote site, it arrives as traffic that originated on your external interface.

Define a route for all Internet-bound traffic

When you enable remote users to access the Internet through a VPN tunnel, the most secure setup 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 a hub route or 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. When you use default-route VPN, a dynamic NAT policy must include the outgoing traffic from the remote network. This allows remote users to browse the Internet when they send all traffic to the Firebox.

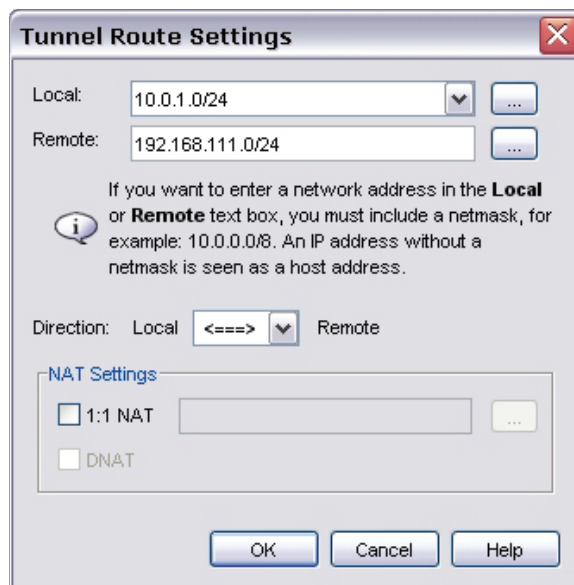
When you define a default route through a BOVPN tunnel, you must do two things:

- Configure the remote Firebox (whose traffic you want to send through the tunnel) to send all traffic from its own network address to 0.0.0.0/0.
- Add a route on the central Firebox from 0.0.0.0/0 to the network address of the remote Firebox.

Before you begin the procedures in this topic, you must have already created a manual branch office VPN between the central and remote Fireboxes. For information on how to do this, see [About manual BOVPN tunnels](#).

Configure the remote Firebox

1. From Policy Manager, open the configuration file on the remote Firebox.
2. Select **VPN > Branch Office Tunnels**. Find the name of the tunnel to the central Firebox and click **Edit**. *The Edit Tunnels dialog box appears.*
3. Click **Add**. *The Tunnel Route Settings dialog box appears.*



4. From the **Local** drop-down list, select or type the trusted network address of the remote Firebox. the local address you want.
5. In the **Remote** box, type 0.0.0.0/0. Click OK. [Save the configuration file](#).

If the remote Firebox is an Edge device

1. Connect to the System Status page of the remote Edge.
From the navigation bar, select **VPN > Manual VPN**.
The Manual VPN page appears.
2. Find the name of the tunnel to the central Firebox and click **Edit**.
The EditGateway page appears.
3. Look below the Phase 2 Settings for the **Local Network** and **Remote Network** text boxes. In the **Local Network** text box, type the trusted network address for the remote Edge.
In the **Remote Network** text box, type 0.0.0.0/0. Click **Add**.
4. Click **Submit** to save your changes.

Phase 2 Settings

Authentication Algorithm SHA1-HMAC

Encryption Algorithm 3DES-CBC

☐ Enable TOS for IPSEC

☐ Enable Perfect Forward Secrecy

Key expires in 8192 kilobytes

Key expires in 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

Remove

Local Network 0.0.0.0/0

Remote Network 0.0.0.0/0 Add

Add a dynamic NAT entry on the central Firebox

To allow a computer with a private IP address to access the Internet through the Firebox, you must configure the Firebox to use dynamic NAT. With dynamic NAT, the Firebox replaces the private IP address included in a packet sent from a computer protected by the Firebox with the public IP address of the Firebox itself. By default, dynamic NAT is enabled and active for the three RFC-approved private network addresses:

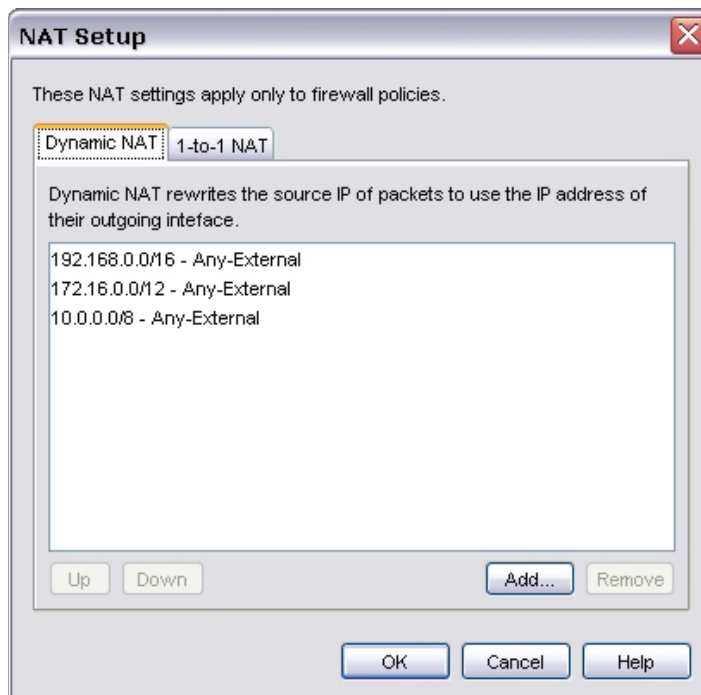
192.168.0.0/16 - Any-External

172.16.0.0/12 - Any-External

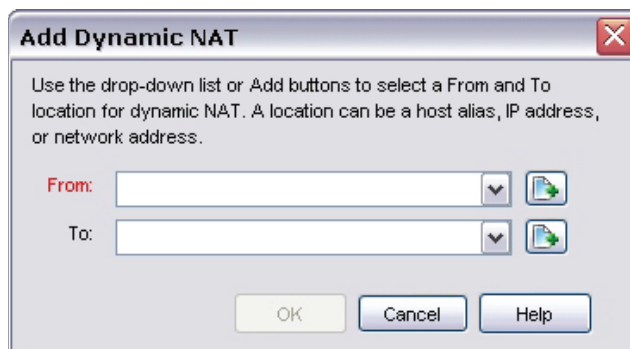
10.0.0.0/8 - Any-External


When you set up a default route through a branch office VPN tunnel to another Firebox, you must add a dynamic NAT entry for the subnet behind the remote Firebox if it does not match the three networks shown above.

1. From Policy Manager, select **Network > NAT**.
The NAT Setup dialog box appears.



2. On the **Dynamic NAT** tab of the **NAT Setup** dialog box, click **Add**.
The Add Dynamic NAT dialog box appears.



3. Click  next to the **From** drop-down list.

4. From the **Choose Type** drop-down list, select **Network IP**. Type the network IP address of the network behind the remote Firebox in the **Value** field. Click **OK**.
5. From the **To** drop-down list, select **Any-External**.
6. Click **OK** to close the **Add Dynamic NAT** dialog box.
7. Click **OK**. [Save the configuration file](#) to the central Firebox.

Configure VPN Failover



This topic applies only to manual VPN tunnels. If you have multi-WAN configured and you create managed tunnels, WSM automatically sets up gateway pairs that include the external interfaces of both ends of your tunnel. No other configuration is necessary.

Failover is an important function of networks that need a high degree of availability.

When you have multi-WAN failover configured, VPN tunnels automatically fail over to a backup external interface if a failure occurs. You can also configure VPN tunnels to fail over to a backup endpoint if the primary endpoint becomes unavailable.

VPN Failover occurs when one of these two events occur:

- A physical link is down. The Firebox monitors the status of the VPN gateway and the devices identified in the multi-WAN link monitor configuration. If the physical link is down, VPN failover occurs.
- The Firebox detects the VPN peer is not active.

When failover occurs, IKE continues to send Phase 1 keep-alive packets to the peer. When it gets a response, IKE triggers failback to the primary VPN gateway.

When a failover event occurs, most new and existing connections failover automatically. For example, if you start an FTP PUT command and the primary VPN path goes down, the existing FTP connection continues on the backup VPN path. The connection is not lost, but there is some delay. Note that VPN Failover can occur only if:

- Fireboxes at each tunnel endpoint have Fireware v10 installed.
- Multi-WAN failover is configured, as described in [About using multiple external interfaces](#).
- The interfaces of your Firebox are listed as gateway pairs on the remote Firebox. If you have already configured multi-WAN failover, your VPN tunnels will automatically fail over to the backup interface.

VPN Failover does not occur for BOVPN tunnels with dynamic NAT enabled as part of their tunnel configuration. For non-NAT BOVPN tunnels, VPN Failover occurs and the BOVPN session continues.

With Mobile VPN tunnels, the session does not continue. You must authenticate your Mobile VPN client again to make a new Mobile VPN tunnel.

Define multiple gateway pairs



If you have multi-WAN configured and you create managed tunnels, WSM automatically sets up gateway pairs that include the external interfaces of both ends of your tunnel. No other configuration is necessary.

To configure manual BOVPN tunnels to fail over to a backup endpoint, you must define more than one set of local and remote endpoints (gateway pairs) for each gateway. For complete failover functionality for a VPN configuration, you must define gateway pairs for each combination of external interfaces on each side of the tunnel. For example, suppose your primary local endpoint is 205.122.1.1/24 with a backup of 205.122.2.1/24. Your primary remote endpoint is 50.50.1.1/24 with a backup of 50.50.2.1/24. For complete VPN Failover, you would need to define these four gateway pairs:

205.122.1.1 - 50.50.1.1

205.122.1.1 - 50.50.2.1

205.122.2.1 - 50.50.1.1

205.122.2.1 - 50.50.2.1

1. Select **VPN > Branch Office Gateways**. Click **Add** to add a new gateway. Give the gateway a name and define the credential method, as described in [Configure gateways](#).
2. In the Gateway Endpoints section of the **New Gateway** dialog box, click **Add**.
The New Gateway Endpoints Settings dialog box appears.

New Gateway Endpoints Settings - MultipleGate...

A tunnel needs authentication on each side of the tunnel. Provide the configuration details for the gateway endpoints below.

Local Gateway

Specify the gateway ID for tunnel authentication.

☒ By IP Address

IP address: 205.122.1.1

☐ By Domain Information [Configure...](#)

External Interface: External

Remote Gateway

Specify the remote gateway IP address for a tunnel.

☒ Static IP address

IP Address: 50.50.1.1

☐ Dynamic IP address

Specify the gateway ID for tunnel authentication.

☒ By IP Address

IP address: 50.50.1.1

☐ By Domain Information [Configure...](#)

OK Cancel Help

3. Specify the location of the local and remote gateways. Select the external interface name that matches the local gateway IP address or domain name you add.
You can add both a gateway IP address and gateway ID for the remote gateway. This can be necessary if the remote gateway is behind a NAT device and requires more information to authenticate to the network behind the NAT device.
4. Click **OK** to close the **New Gateway Endpoints Settings** dialog box.
The New Gateway dialog box appears. The gateway pair you defined appears in the list of gateway endpoints.
5. Repeat this procedure to define additional gateway pairs. You can add up to nine gateway pairs. You can select a pair and select the **Up** or **Down** key to change the order in which the Firebox attempts connections.
6. Click **OK**.

Force a BOVPN tunnel rekey

Normally, the gateway endpoints must generate and exchange new keys after a quantity of time or amount of traffic passes, as defined in **Force Key Expiration** field in the **Phase2 Proposals** dialog box. You might sometimes, particularly when you troubleshoot tunnels, want to immediately generate new keys instead of waiting for them to expire.

To rekey one BOVPN tunnel

You can rekey a tunnel either from the front panel of Firebox System Manager or from the **Device Status** tab of WatchGuard System Manager. Under the **Branch Office VPN Tunnels** heading, select the tunnel you want to rekey. Right-click and select *Rekey Selected BOVPN Tunnel*. When prompted, type the configuration passphrase for the Firebox to which Firebox System Manager is connected.

To rekey all BOVPN tunnels

From Firebox System Manager, right-click anywhere on the front panel of the window. Select **Rekey All BOVPN Tunnels**. When prompted, type the configuration passphrase for the Firebox to which Firebox System Manager is connected.

or

From Firebox System Manager, select **Tools > Rekey All BOVPN Tunnels**. When prompted, type the configuration passphrase for the Firebox to which Firebox System Manager is connected.


or

From the **Device Status** tab of WatchGuard System Manager, right-click the **Branch Office VPN Tunnels** heading or any tunnel below the heading. Select **Rekey All BOVPN Tunnels**.

VPN tunnel status and security services

The front panel of Firebox System Manager includes statistics about current VPN tunnels.

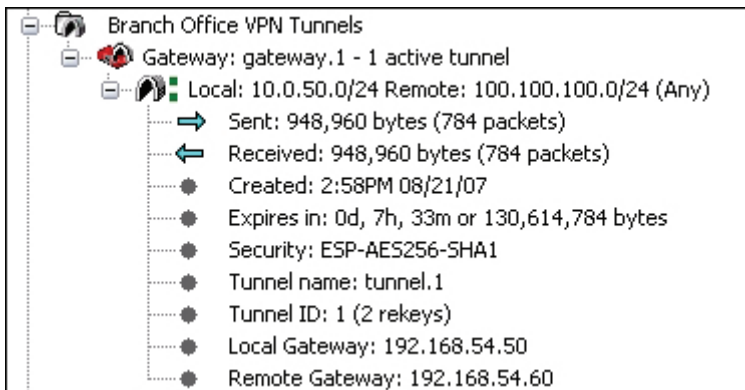
To open Firebox System Manager:

1. From WatchGuard System Manager, select the **Device Status** tab.
2. Select the Firebox to examine with Firebox System Manager.
3. Click .

Or, select **Tools > Firebox System Manager**.

Firebox System Manager appears. It may take a moment to connect to the Firebox to get information about the status and configuration.

Below the Firebox Status section on the right side of the screen is a section on BOVPN tunnels. Firebox System Manager shows the current tunnel status and gateway information for each VPN tunnel as well as data sent and received, creation and expiration information, type of authentication and encryption, and number of rekeys.



Each BOVPN tunnel is shown in one of three states:

Active

The BOVPN tunnel is operational and passing traffic.

Inactive

The BOVPN tunnel has been created, but no tunnel negotiation has occurred. No traffic has been sent through the VPN tunnel.

Expired

The BOVPN tunnel was active, but is no longer active because the tunnel has no traffic or because the link between the gateways is lost.

This information also appears on the **Device Status** tab in WatchGuard System Manager.

Mobile VPN tunnel status

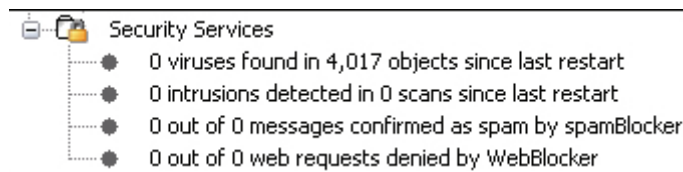
Firebox System Manager shows the user name, IP address information, and the quantity of sent and received packets for the three types of Mobile VPN Tunnels:

- Mobile VPN with IPSec
- Mobile VPN with SSL
- Mobile VPN with PPTP

To log off Mobile VPN users, right-click a user and select **Logoff selected user**.

Security Services status

Below Security Services, Firebox System Manager shows the number of viruses found, the number of intrusions, the number of email messages confirmed as spam, and the number of web requests denied by WebBlocker since the last restart.



22

Certificates and the Certificate Authority

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.

In WatchGuard System Manager, the workstation that is configured as the Management Server also operates as a CA. The CA gives certificates to managed Firebox clients when they contact the Management Server to receive configuration updates.

To configure the certificate authority on the Management Server, see [Configure the certificate authority on the Management Server](#).

Certificate lifetimes and CRLs

Each certificate has a lifetime set when it is created. When the end date and time set for the certificate lifetime is reached, the certificate expires and can no longer be used. Sometimes, certificates are revoked before their lifetime expiration. The Firebox keeps a current list of these revoked certificates, called the Certificate Revocation List (CRL). The CRL is published to each Firebox when the Firebox connects to the Management Server.

Create a certificate with FSM or the Management Server

If you have not prepared a certificate, you can create a certificate signing request (CSR) using Firebox System Manager (FSM). You can also create a new certificate for a Mobile VPN using the built-in Certificate Authority (CA) Manager on your Management Server.

Create a certificate with FSM

1. From Firebox System Manager, select **View > Certificates**.
2. Click **Create Request**.
The Certificate Request Wizard starts.
3. Click **Next**.
4. Enter your name, your department, the name of your company, and the city, state or province, and country you are working in. These entries are used to create the subject name.




The Certificate Request Wizard dialog box is shown. It has a title bar with the text "Certificate Request Wizard" and a close button. The main area has a header "Configure the fields for the subject name." with the WatchGuard logo. Below this, a message states: "The information here will be used to generate the subject name." There are six input fields: "Name:" with "John Smith" and "(required)" label; "Department Name:" with "Technical Support"; "Company Name:" with "MyWatchguard" and "(required)" label; "City/Location:" with "Seattle"; "State/Province:" with "WA"; and "Country:" with "US" and "(required)" label. At the bottom are three buttons: "< Back", "Next >", and "Cancel".

5. Click **Next**.
The wizard creates a subject name based on what you entered in the previous screen.

6. Enter the appropriate information in the **DNS name**, **IP address**, and **user domain name** fields. Click **Next**.

Certificate Request Wizard

Configure the remaining domain information. 

Subject Name: (required)

DNS Name: (required)

IP Address:


User Domain Name:

< Back Next > Cancel

- By default, the certificate uses RSA encryption, 512-bit key length, and both encryption and signatures for keys. Make any changes you want to these settings. Click **Next**.
- After you type the configuration passphrase, click **OK** to see the finished CSR.

9. Click **Copy** to copy the Certificate Signing Request to the Windows clipboard. You must send this CSR to a certificate authority for signature before you can use it with your Firebox. Click **Next**.
10. On the last screen of the wizard, you can:
 - Click **Import Now** to import a certificate.
The Import Certificate/CRL dialog box appears.
For information on how to use this dialog box, see [Import a certificate](#).
or
 - Click **Finish** to close the wizard.

Create a certificate with CA Manager

1. From WatchGuard System Manager, connect to the Management Server.
You must type the configuration passphrase to connect.
2. Click the **Device Management** tab for the Management Server.
3. Click .
Or, select **Tools > CA Manager**.
4. Click **Generate a New Certificate**.
5. Type the subject's common name, password, and certificate lifetime.
 - o For Mobile VPN users, the common name must agree with the user name of the remote user.
 - o For Firebox users, the common name must agree with the Firebox identifying information (normally, its IP address).
 - o For a generic certificate, the common name is the name of the user.
6. If this certificate is for Mobile VPN users only, type the subject's organizational unit. The organizational unit must appear in this format:
GW:<vpn gateway name>
If you do not know the VPN gateway name, use the value of config.watchguard.id in the configuration file of the gateway Firebox.
7. To download the certificate after it is generated, select the **Download Cert** check box.
8. Click **Generate**.

Create a certificate with Microsoft CA

Although you can easily [Create a certificate with FSM or the Management Server](#), you can also create a certificate yourself using the Microsoft Certificate Authority (CA).

Each certificate signing request (CSR) must be signed by a certificate authority (CA) before it can be used for authentication. When you do this procedure yourself, you act as the CA and digitally sign your own request. For compatibility reasons, however, we recommend that you instead send your CSR to a widely known CA, such as Verisign or GeoTrust. Because the root certificates for these organizations are installed by default with most major Internet browsers, you do not have to distribute the root certificates yourself.

You can use Windows Server 2003 to complete a CSR.

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. Click **Submit a certificate**.
5. Paste the contents of your CSR file into the **Saved Request** text box. Click **OK**.
6. Close your web browser.

Issue the certificate

1. Connect to the server where the Certification Authority is installed, if necessary.
2. Select **Start > 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

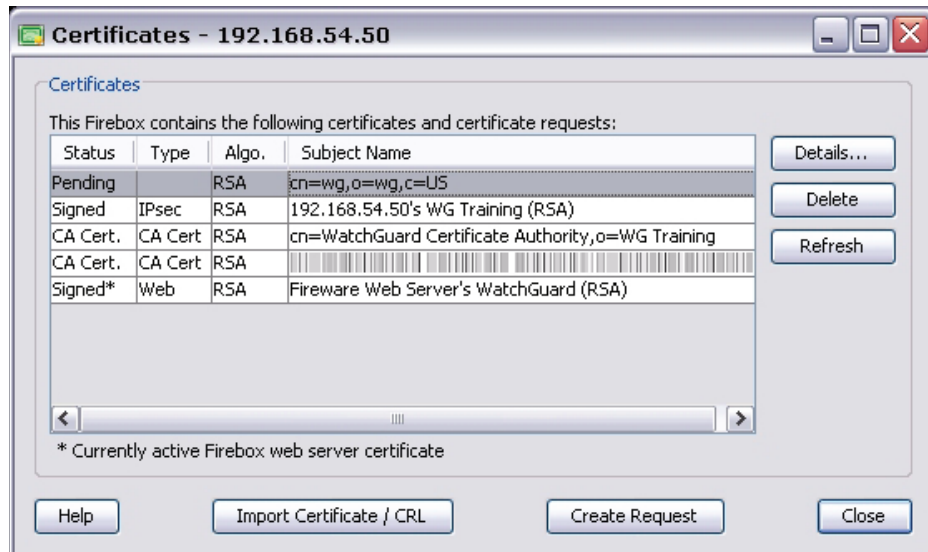
1. Open your web browser. In the location or address bar, type the IP address of the server where the certification authority is installed, followed by `certsrv`.
Example: `http://10.0.2.80/certsrv`
2. Click the **View the status of a pending certificate request** link.
3. Click the certificate request with the time and date you submitted.
4. Select the **Base 64 encoded** radio button to choose the PKCS10 or PKCS7 format.
5. Click **Download certificate** to save the certificate on your hard drive.

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 to install it.

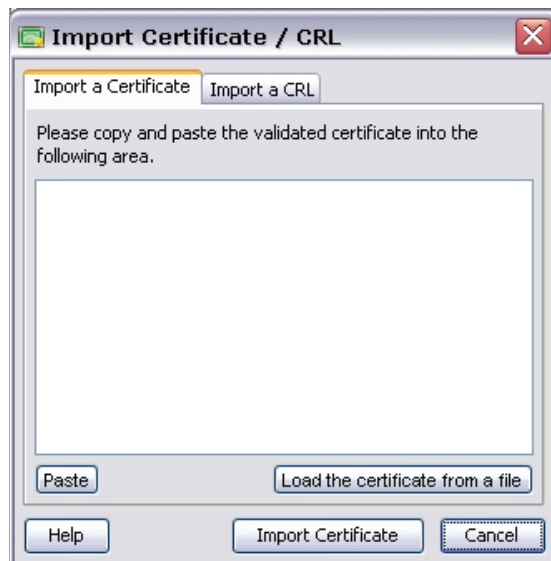
Import a certificate

You must import certificates before you can use them for local Firebox or VPN authentication. You can use Firebox System Manager to import CA root certificates, certificates in PEM format that include a private key, or a certificate that matches the private key used to create the last certificate signing request (CSR).

1. From Firebox System Manager, select **View > Certificates**.



2. Click **Import Certificate/CRL**.
3. Click the **Import a Certificate** tab.



4. Paste the contents of the certificate into the text box, or click **Load the certificate from a file** to browse to a certificate file.
5. Click **Import Certificate**.
Your certificate must be in Base64 format.
6. Type the Firebox configuration (read/write) passphrase.

Use certificates for authentication

You can use certificates for:

- [Mobile VPN with IPsec tunnel authentication](#)
- [BOVPN tunnel authentication](#)



Third-party or self-signed certificates cannot be used for Mobile VPN authentication.

You can also [Configure the web server certificate for Firebox authentication](#). The web server certificate is the certificate that the Firebox uses for HTTPS connections.

When you perform any of these procedures, we recommend that you [Connect to a Firebox](#) so Policy Manager can download the list of currently installed certificates. If you save changes from a local configuration file and the new settings do not match the certificates on the Firebox, your Firebox may not operate correctly.

Use certificates for Mobile VPN with IPsec tunnel authentication

When a Mobile VPN tunnel is created, the IPsec protocol checks the identity of each endpoint using a pre-shared key (PSK). This key can be a passphrase known by both endpoints, or a certificate from the Management Server. The Firebox must be a managed client to use a certificate for Mobile VPN authentication.

To use certificates for a new Mobile VPN with IPsec tunnel:

1. In Policy Manager, select **VPN > Mobile VPN > IPsec**.
2. Click the **Add** button.
3. On the third screen of the wizard, select the **Use an RSA certificate issued by your WatchGuard Management Server** radio button.
4. Type the IP address and administration passphrase of your Management Server.
5. Finish the wizard.

To change an existing Mobile VPN tunnel to use certificates for authentication:

1. In Policy Manager, select **VPN > Mobile VPN > IPsec**.
2. Select the Mobile VPN tunnel you want to change. Click **Edit**.
3. Click the **IPsec Tunnel** tab.
4. Select the **Use a certificate** radio button.
5. Type the **IP address** of the Management Server. If necessary, adjust the connection timeout.
6. Click **OK**.

When you use certificates, you must give each Mobile VPN user three files:

- The end-user profile (.wgx)
- The client certificate (.p12)
- The CA root certificate (.pem)

When an Mobile VPN user opens the .wgx file, the root and client certificates contained in the cacert.pem and the .p12 files are automatically loaded. For more information on Mobile VPN with IPsec, see [About the Mobile VPN with IPsec client](#).

Use a certificate for BOVPN tunnel authentication

When a BOVPN tunnel is created, the IPSec protocol checks the identity of each endpoint using either a pre-shared key (PSK) or a certificate imported and stored on the Management Server.

To use a certificate for BOVPN tunnel authentication:

1. In Policy Manager, select **VPN > Branch Office Gateways**.
2. Click the **Add** button to create a new gateway, or select an existing gateway and click **Edit**.
3. Select the **Use IPSec Firebox Certificate** radio button.
4. Click the certificate you want to use.
5. Set other parameters as necessary. Click **OK**.

If you use a certificate for BOVPN authentication:

- The certificate must be recognized as an IPSec-type certificate by Firebox System Manager. To verify, [Start Firebox System Manager](#), select **View > Certificates**, and make sure the **Type** column in the **Certificates** dialog box that appears says "IPSec" or "IPSec/Web."
- Make sure certificates for the devices at each gateway endpoint use the same algorithm. Both endpoints must use either DSS or RSA. The algorithm for certificates appears in the table in the New Gateway dialog box and in the **Certificates** dialog box in Firebox System Manager.
- You must start the certificate authority on the Management Server if you select certificate-based authentication. For more information on this, see [Configure the certificate authority on the Management Server](#).
- You must use the WatchGuard Log Server for log messages.

Configure the web server certificate for Firebox authentication

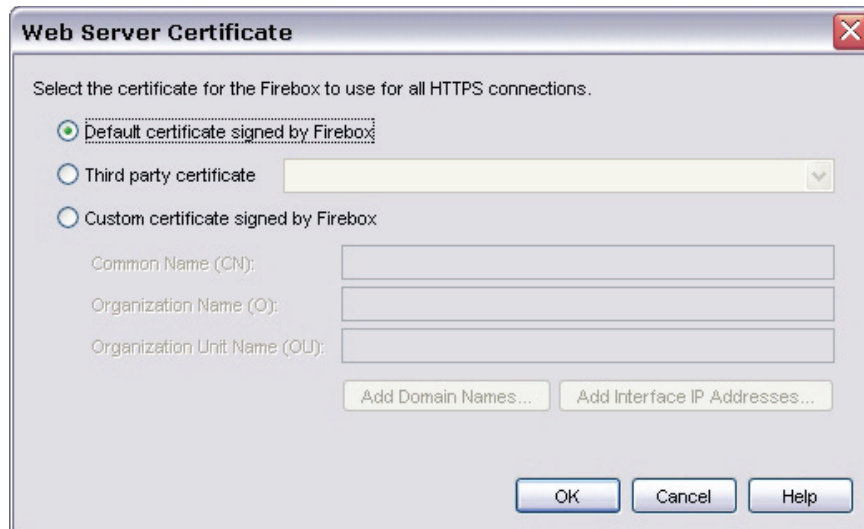
When users connect to the Firebox with a web browser, they often see a security warning. This warning occurs because the default certificate does not match the IP address or domain name used for authentication. To remove this warning, you can use a third-party certificate, or create a custom certificate that matches the IP or domain name.

To see the current web server certificate:

From Firebox System Manager, select **View > Certificates**. The web server certificate is the one in the table that is marked with an asterisk.

To configure the web server certificate for Firebox authentication:

1. From Policy Manager, select **Setup > Authentication > Web Server Certificate**.



Web Server Certificate

Select the certificate for the Firebox to use for all HTTPS connections.


☒ **Default certificate signed by Firebox**
☐ **Third party certificate**
☐ **Custom certificate signed by Firebox**

Common Name (CN):
 Organization Name (O):
 Organization Unit Name (OU):

Add Domain Names...
Add Interface IP Addresses...

OK Cancel Help

2. To use the default certificate, select the **Default certificate signed by Firebox** radio button. Skip to step 7.
3. To use a certificate you have previously imported, select the **Third-party certificate** radio button. Select a certificate from the drop-down list. Skip to step 7.
This certificate must be recognized as a Web-type certificate by Firebox System Manager.
4. If you want to create a custom certificate signed by the Firebox, select the **Custom certificate signed by Firebox** radio button.
5. Click the **Add Domain Names** button, or the **Add Interface IP Addresses** button.




Add Domain Names

You can add domain names to include in the certificate here. Domain names you add here will appear in the certificate as additional *subject alt name* fields.

Add Remove

OK Cancel Help



Add Interface IP Addresses

The certificate automatically includes all **Trusted** interface IP addresses. You can add the IP addresses of other interfaces to include in the certificate here.

Add Remove

OK Cancel Help

6. Type a domain name or IP address of an interface on your Firebox in the field at the bottom of the dialog box. Click **Add**. When you have added all the domain names you want, click **OK**.
7. Click **OK** to save your changes.

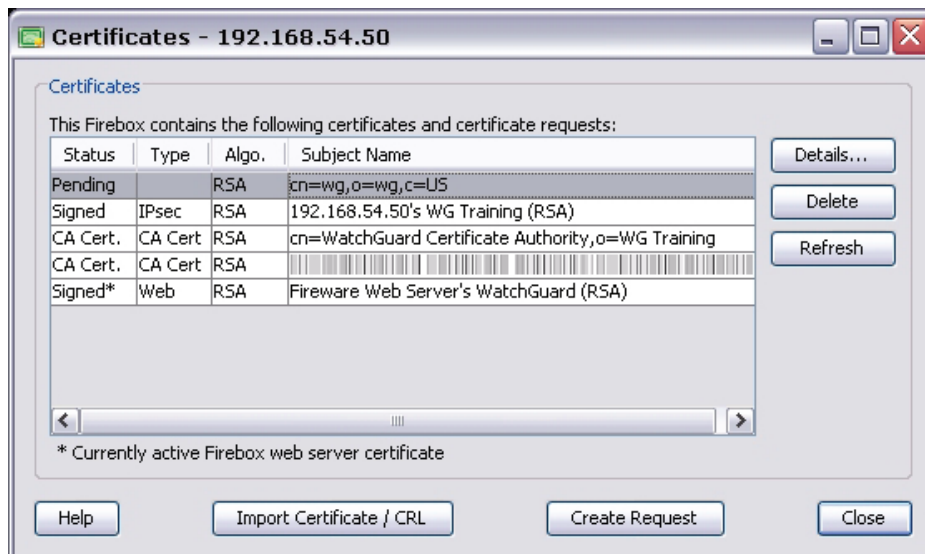
See and manage Firebox certificates

You can do the following from Firebox System Manager:

- See a list of the current Firebox certificates and details on any of them.
- Remove a certificate from the Firebox.
- Make a certificate request.
- Import a third-party CA certificate and store it in the certificate trust list.

See current certificates

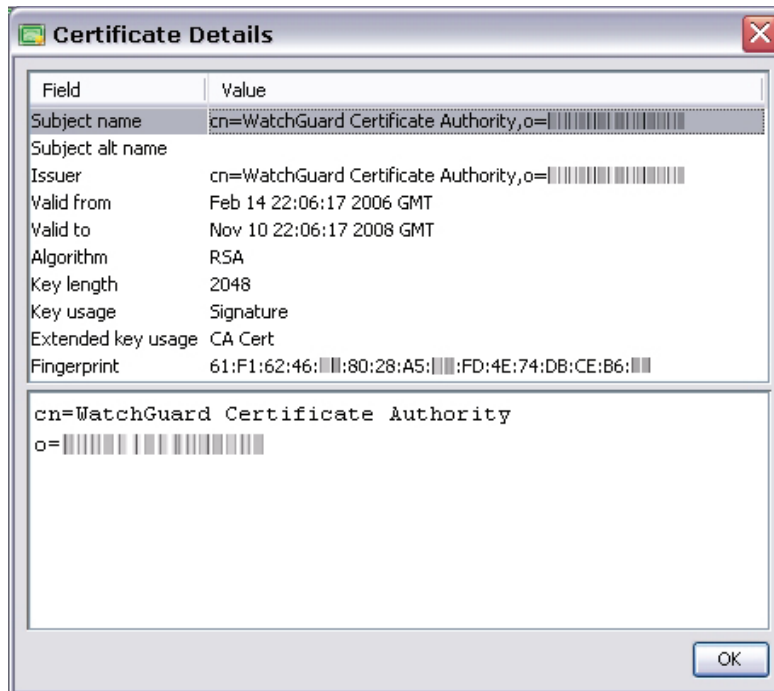
To see the current list of certificates, from Firebox System Manager, select **View > Certificates**.



In this window, you can see a list of all certificates and certificate signing requests (CSRs). The list includes this information:

- The status and type of the certificate. The certificate marked with an asterisk is the currently active Firebox web server certificate.
For more information on options for the web server certificate, see [Firebox authentication](#).
- The algorithm used by the certificate.
- The subject name or identifier of the certificate.

To see additional information on a certificate in the list, select the certificate and click **Details**.



The **Certificate Details** window includes information about which CA signed the certificate and the certificate fingerprint. Use this information to troubleshoot or uniquely identify certificates.

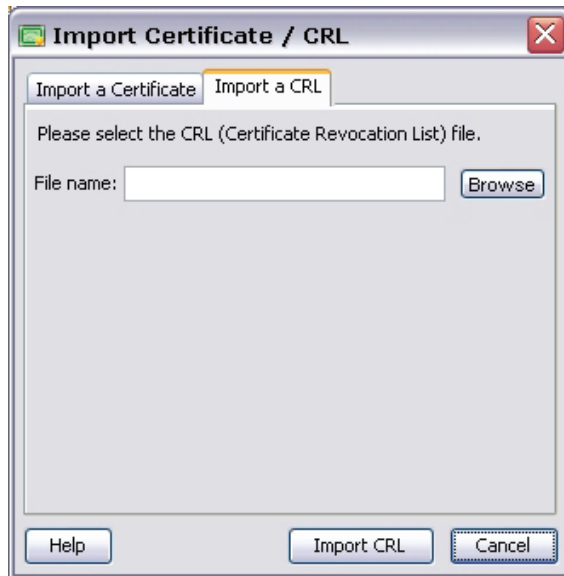
Delete a certificate

To remove a certificate from the Firebox, select the certificate in the **Certificates** dialog box and click **Delete**. You must provide the Firebox configuration (read/write) passphrase to remove a certificate. Certificates you delete can no longer be used for authentication.

Import a CRL from a file

You can import a certificate revocation list (CRL) from a file on your local computer. This is useful when you must restore a Firebox from a backup.

1. From Firebox System Manager, select **View > Certificates**.
2. From the **Certificate** dialog box, click **Import Certificate/CRL**.
3. Click the **Import a CRL** tab. Click **Browse** to find the file.



4. Click **Import CRL**.
The Import CRL dialog box appears.
5. Type the configuration passphrase and click **OK**.
The CRL you specified is appended to the CRL on your Firebox.

Retrieve the CRL from an LDAP server

You can retrieve a CRL from an LDAP server if you have access to the server. You must have LDAP account information provided by a third-party CA service.

1. From Policy Manager, select **VPN > VPN Settings**.

The VPN Settings dialog box appears.




2. Select the **Enable LDAP server for certificate verification** check box.
3. Enter the name or address of the LDAP server.
4. (Optional) Enter the port number.
5. Click **OK**.

Your Firebox checks the CRL stored on the LDAP server when tunnel authentication is requested.

See and manage Management Server certificates

You can manage, and see a list of, certificates on the Management Server. You usually use the web-based CA Manager to use this. You can also perform some of these functions from the WatchGuard System Manager window.

Use the web-based CA Manager

1. From WatchGuard System Manager, connect to the Management Server.
You must type the configuration passphrase to connect.
2. Click the **Device Management** tab for the Management Server.
3. Click .
Or, select **Tools > CA Manager**.

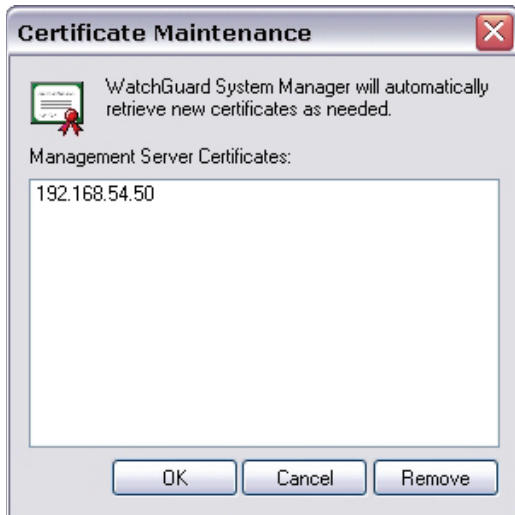
The web-based CA Manager has several web pages you can use to manage certificates:

- **Certificate Authority CA Certificate:** Shows the CA (root) certificate. You can save the certificate to a file, or copy its contents to the Windows clipboard.
- **Management Server CA Certificate:** Shows the Management Server CA certificate. You can save the certificate to a file, or copy its contents to the Windows clipboard.
- **Generate a New Certificate:** Use this option to create a new certificate, as described in the “Create a certificate with CA Manager” section of [Create a certificate with FSM or the Management Server](#).
- **Find and Manage Certificates:** On this page, you can search for certificates by serial number, common name, or organizational unit. You can then view details for, revoke, reinstate, or destroy the certificates returned in the search results.
- **List and Manage Certificates:** To see the full certificate, click its number in the **Serial** column. This page shows detailed information about the certificate, such as its signature algorithm and issuer.
 - *To change the status of one or more certificates,* select the check box adjacent to each certificate. At the bottom of the page, select an action from the drop-down list and click **Go**.
 - *When you revoke a certificate,* it is added to the Certificate Revocation List (CRL) and cannot be used for authentication.
 - *When you reinstate a certificate,* it is removed from the CRL and can be used again. If you remove or destroy a certificate, it is not added to the CRL, but it cannot be used for authentication. The CRL is published to each Firebox when the Firebox connects to the Management Server.
- **Upload Certificate Request:** Use this page to sign a certificate request from a different device. Type in the common name and organizational unit used in the certificate, and then click **Browse** to find the CSR (Certificate Signing Request) file. When you are finished, click **Upload**.
- **Publish a Certificate Revocation List (CRL):** This option publishes the CRL to each Firebox connected to the Management Server. Any VPN tunnels that use newly expired certificates stop operating when the Firebox receives the new list.

Manage certificates with WSM

You can use WSM to see certificates used by the Management Server and delete those that are no longer needed.

From WSM, select **File > Certificates**.



The **Certificate Maintenance** dialog box shows a list of the certificates used by WatchGuard System Manager. WatchGuard automatically gets the certificates it needs.

To remove a certificate, select it and click **Remove**. If the certificate is currently used by the Management Server, you must first disconnect from the server before you delete the certificate.



When you delete a Management Server certificate, you do not delete certificates in Microsoft Internet Explorer.

23 Mobile VPN with PPTP

About Mobile VPN with PPTP

Mobile Virtual Private Networking (Mobile VPN) with Point-to-Point Tunneling Protocol (PPTP) makes a secure connection between a remote computer and the network resources behind the Firebox. It supports as many as 50 users at the same time for each Firebox. Mobile VPN with PPTP users can authenticate to the Firebox, or to a RADIUS or VACMAN Middleware authentication server. To use Mobile VPN with PPTP you must configure the Firebox and the remote client computers of the remote users.

Mobile VPN with PPTP connections

When you activate Mobile VPN with PPTP on your Firebox, users included in the Mobile VPN with PPTP group can use the PPTP feature included in their computer operating system to make a PPTP connection to the Firebox.

Because the Firebox allows the PPTP connection from any Firebox user that gives the correct credentials, it is important that you make a policy for PPTP sessions that includes only users you want to allow to send traffic over the PPTP session. You can also add a group or individual user to a policy that restricts access to resources behind the Firebox. The Firebox creates a pre-configured group called *PPTP-Users* for this purpose.

To configure a Mobile VPN with PPTP connection:

1. From Policy Manager select **VPN > Mobile VPN > PPTP**.
2. Select **Activate Mobile VPN with PPTP**.
3. Clear the **Use Radius authentication to authenticate Mobile VPN with PPTP users** check box, to allow the Firebox to authenticate the PPTP session.
The Firebox checks to see whether the user name and password the user enters into the VPN connection box matches the user name and password in the Firebox User database that is a member of the PPTP-Users group.
If the credentials supplied by the user match an account in the Firebox User database, the user is authenticated for a PPTP session.
4. Create a policy that allows traffic only from or to a list of Firebox user names, or a list of Firebox groups.
The Firebox does not look at this policy unless traffic comes from or goes to the authenticated user's virtual IP address.

Client requirements

Before you configure a Firebox to use Mobile VPN with PPTP, make sure you have this information:

- The IP addresses for the remote client to use for Mobile VPN with PPTP sessions. For Mobile VPN with PPTP tunnels, the Firebox gives each remote user a virtual IP address. **These IP addresses cannot be addresses that the network behind the Firebox uses.** The safest procedure to give addresses for Mobile VPN users is to install a placeholder secondary network. Then, select an IP address from that network range. For example, create a new subnet as a secondary network on your trusted network 10.10.0.0/24. Select the IP addresses in this subnet for your range of PPTP addresses.
- The IP addresses of the DNS and WINS servers that resolve host names to IP addresses.
- The user names and passphrases of users that are allowed to connect to the Firebox with Mobile VPN with PPTP.

Encryption levels

For Mobile VPN with PPTP, you can select to use 128-bit encryption or 40-bit encryption. U.S. domestic versions of Windows XP have 128-bit encryption enabled. You can get a strong encryption patch from Microsoft for other versions of Windows. The Firebox always tries to use 128-bit encryption first. It uses 40-bit encryption (if enabled) if the client cannot use the 128-bit encrypted connection.

For information on how to enable the drop from 128-bit to 40-bit, see [Enable Mobile VPN with PPTP](#).

If you do not live in the U.S. and you want to have strong encryption allowed on your LiveSecurity Service account, send an email message to supportid@watchguard.com and include in it:

- Your LiveSecurity Service key number
- Date of purchase
- Name of your company
- Company mailing address
- Telephone number and name
- Email address

If you live in the U.S. and are not already using WSM with strong encryption, you must download the strong encryption software from your Software Downloads page in the LiveSecurity Service web site. Go to www.watchguard.com, click **Support**, log in to your LiveSecurity Service account, and then click **Software Downloads**. Download WatchGuard System Manager with Strong Encryption.

Uninstall WatchGuard System Manager before you install the WatchGuard System Manager with Strong Encryption software.



To keep your current Firebox configuration, do not use the Quick Setup Wizard when you install the new software. Open WatchGuard System Manager, connect to the Firebox, and save your configuration file. Configurations with a different encryption version are compatible.

Configure WINS and DNS servers

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 Firebox must have access to these servers.

1. From Policy Manager, select **Network > Configuration**. Click the **WINS/DNS** tab.
The information for the WINS and DNS servers appears.
2. In the IP address text boxes, type the addresses for the WINS and DNS servers. You can type up to three addresses for DNS servers, and two addresses for WINS servers. Type a domain name for the DNS server.

The screenshot shows the 'Network Configuration' dialog box with the 'WINS/DNS' tab selected. The dialog has a title bar with a close button. Below the title bar are five tabs: 'Interfaces', 'VLAN', 'WINS/DNS' (which is highlighted with a dotted border), 'Dynamic DNS', and 'Multi-WAN'. The main content area is divided into two sections. The first section is titled 'DNS (Domain Name System) Servers' and contains a 'Domain Name:' text box and three 'DNS Servers:' text boxes, each with a placeholder '. . .' for an IP address. The second section is titled 'WINS (Windows Internet Naming Service) Servers' and contains two 'WINS Servers:' text boxes, each with a placeholder '. . .' for an IP address. At the bottom right of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

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. When you use default-route VPN, a dynamic NAT policy must include the outgoing traffic from the remote network. This allows remote users to browse the Internet when they send all traffic to the Firebox.



*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

In Windows Vista, XP and 2000 the default setting for a PPTP connection is a default-route. The Firebox must be configured to dynamically NAT the traffic from a PPTP user and any policy that manages traffic going out to the Internet from behind the Firebox must be configured to allow the PPTP user traffic.

- Make sure that the IP addresses you have added to the PPTP address pool are included in your dynamic NAT configuration on the Firebox. To make sure, from Policy Manager, select **Network > NAT**.
- Edit your policy configuration to allow connections from PPTP-Users through the external interface. For example, if you use WebBlocker to control web access, add PPTP-Users to the proxy policy that is configured to with WebBlocker enabled.

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.

Configure the Firebox for Mobile VPN with PPTP

1. From Policy Manager, click **VPN > Mobile VPN > PPTP**.
The *Mobile VPN with PPTP* dialog box appears.

Mobile VPN with PPTP Configuration

When you activate Mobile VPN with PPTP, a "PPTP-Users" user group and a "WatchGuard PPTP" policy are created to allow PPTP connections from the Internet to your external interface.

☒ Activate Mobile VPN with PPTP

☐ Use Radius authentication to authenticate Mobile VPN with PPTP users

Encryption Settings

☒ Require 128-bit encryption

☐ Allow drop from 128-bit to 40-bit encryption

☐ Do not require encryption

Other Settings

Maximum Transmission Unit (MTU): 1300 bytes

Maximum Receive Unit (MRU): 1300 bytes

Session Timeout: 12 hours

Idle Timeout: 15 minutes

IP Address Pool:

10.0.2.17-10.0.2.27

Add... Remove

You can configure only 50 Mobile VPN with PPTP users. You have 39 remaining.

OK Cancel Help

2. Select the **Activate Mobile VPN with PPTP** check box. This allows PPTP remote users to be configured and automatically creates a WatchGuard PPTP policy to allow PPTP traffic to the Firebox. We recommend that you do not change the default properties of the WatchGuard PPTP policy.

Enable RADIUS or VASCO authentication

Mobile VPN with extended authentication lets users authenticate to a RADIUS or VACMAN Middleware server as an alternative to the Firebox. The instructions to use a VACMAN Middleware server are identical to the instructions to use a RADIUS server.

1. Select the **Use RADIUS Authentication to authenticate Mobile VPN with PPTP users** check box. If you do not select this check box, the Firebox database is used to authenticate users.
2. Configure the RADIUS server in the **Authentication Servers** dialog box, as described in [Configure RADIUS server authentication](#).
Configure the VASCO server in the **Authentication Servers** dialog box, as described in [Configure VASCO server authentication](#).
3. On the RADIUS server, create a PPTP-Users group and add names or groups of PPTP users.



To establish the PPTP connection the user must be a member of a group named PPTP-Users. Once the user is authenticated, the Firebox keeps a list of all groups that a user is a member of. Use any of the groups in a policy to control traffic from the user.

Set encryption for PPTP tunnels

U.S. domestic versions of Windows XP have 128-bit encryption enabled. You can get a strong encryption patch from Microsoft for other versions of Windows.

- Select **Require 128-bit encryption** if you want to require 128-bit encryption for all PPTP tunnels. We recommend that you use 128-bit encryption for VPN.
- Select **Allow Drop from 128-bit to 40-bit** to allow the tunnels to drop from 128-bit to 40-bit encryption for connections that are less reliable. The Firebox 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.
- Select **Do not require encryption** to allow traffic that is not encrypted through the VPN.

MTU and MRU

The Maximum Transmission Unit (MTU) or Maximum Receive Unit (MRU) sizes are sent to the client as part of the PPTP parameters to use during the PPTP session. Do not change MTU or MRU values unless you know it will fix a problem you are experiencing. Incorrect MTU or MRU values will cause traffic through the PPTP VPN to fail.

Define timeout settings for PPTP tunnels

You can define two timeout settings for PPTP tunnels:

Session Timeout

Maximum length of time the user can send traffic to the external network. If you set this field to zero (0) seconds, minutes, hours, or days, no session timeout is used and the user can stay connected for any length of time.

Idle Timeout

Maximum length of time the user can stay authenticated when idle (not passing any traffic to the external network interface). If you set this field to zero (0) seconds, minutes, hours, or days, no idle timeout is used and the user can stay idle for any length of time.

If you do not define these timeout settings, the global settings for the Firebox are used, as described in [Define Firebox global settings](#).

Make outbound PPTP connections from behind a Firebox

If necessary, you can make a PPTP connection to a Firebox from behind a different Firebox. For example, a remote user goes to a customer office that has a Firebox. The user can make PPTP connections to their network with PPTP. For the local Firebox to correctly allow the outgoing PPTP connection, add the PPTP policy and allow traffic from the network the user is on, to Any-External. To add a policy, see [Add policies to your configuration](#).

Add IP addresses for Mobile VPN sessions

Mobile VPN with PPTP supports as many as 50 users at the same time. The Firebox gives an open IP address to each incoming Mobile VPN user from a group of available addresses. This goes on until all the addresses are in use. After a user closes a session, the address is put back in the available group. The subsequent user who logs in gets this address.

You must configure two or more IP addresses for PPTP to operate correctly.

From the **Mobile VPN with PPTP Configuration** dialog box:

1. Click **Add**.

The Add Address dialog box appears.

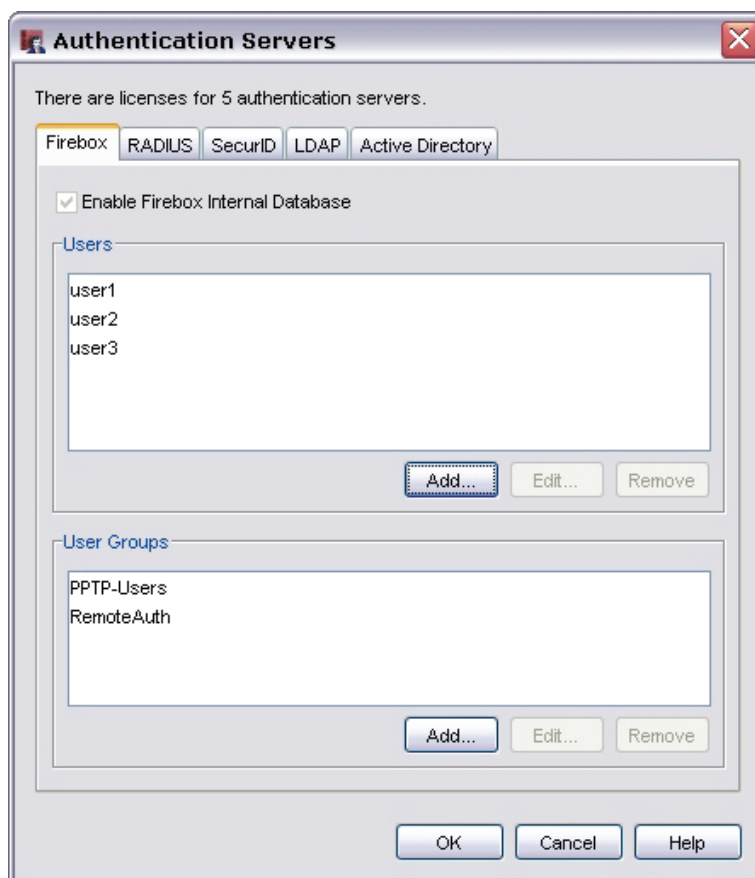
2. From the **Choose Type** drop-down list, select **Host IP** (for a single IP address) or **Host Range** (for a range of IP addresses).
You can configure 50 addresses. If you select **Host IP**, you must add at least two IP addresses. If you select **Host Range** and add a range of IP addresses that is larger than 50 addresses, Mobile VPN with PPTP uses the first 50 addresses in the range.
3. In the **Value** text box, type the host IP address. If you selected **Host Range**, type the first and last IP address in the range. Click **OK**.
Type IP addresses that are not in use that the Firebox can give to clients during Mobile VPN with PPTP sessions. The IP address appears in the list of addresses available to remote clients.
4. Repeat steps 1–3 to configure all the addresses for use with Mobile VPN with PPTP.

Add new users to the PPTP_Users group

To create a PPTP VPN tunnel with the Firebox, mobile users type their user names and passphrases to authenticate. WatchGuard System Manager software uses this information to authenticate the user to the Firebox.

When you enable PPTP in your Firebox configuration, a default user group is created automatically. This user group is called PPTP_Users. You see this group name when you create a new user or add user names to policies. For more information on Firebox groups, see [Configure the Firebox as an authentication server](#).

1. From Policy Manager, click **Setup > Authentication > Authentication Servers**.
The Authentication Servers dialog box appears.
2. Click the **Firebox** tab.



3. To add a new user, click the **Add** button below the **Users** list.
The Setup Firebox User dialog box appears.

4. Type a user name and passphrase for the new user. Type the passphrase again to confirm it.
A description is not required. We recommend that you do not change the default values for Session Timeout and Idle Timeout.
5. Use the horizontal arrows in the group section to put the new user in the PPTP-Users group.
6. To close the **Setup Firebox User** dialog box, click **OK**.
7. To close the **Authentication Servers** dialog box, click **OK**.
You can use the users and groups to configure policies. See the subsequent section.

Configure policies to allow Mobile VPN with PPTP traffic

Mobile VPN with PPTP users have no access privileges through a Firebox by default. You must add user names or the full PPTP-Users group as sources and definitions in individual policy definitions to give remote users access to specified network resources. See [Use authorized users and groups in policies](#)

To use WebBlocker to control the access of remote users, add PPTP users or groups to a proxy policy that controls WebBlocker.



If you assign addresses from a trusted network to PPTP users, the traffic from the PPTP user will not be considered trusted. All Mobile VPN with PPTP traffic is untrusted by default. Regardless of assigned IP address, policies must be created to allow PPTP users access to network resources.

Prepare client computers

You must first prepare each computer that you use as a Mobile VPN with PPTP remote host with Internet access. Then, follow these procedures using the instructions in the subsequent sections:

- Install the necessary version of Microsoft Dial-Up Networking and the necessary service packs
- Prepare the operating system for VPN connections
- Install a VPN adapter (not necessary for all operating systems)

Prepare a Windows NT or 2000 client computer: Install MSDUN and service packs

It can be necessary to install these options for the correct configuration of Mobile VPN with PPTP on Windows NT and 2000:

- MSDUN (Microsoft Dial-Up Networking) upgrades
- Other extensions
- Service packs

For Mobile VPN with PPTP, you must have these upgrades installed:

Encryption	Platform	Application
Base	Windows NT	40-bit SP4
Strong	Windows NT	128-bit SP4
Base	Windows 2000	40-bit SP2*
Strong	Windows 2000	128-bit SP2 *

*40-bit encryption is the default for Windows 2000. If you upgrade from Windows 98, with strong encryption, Windows 2000 will automatically set strong encryption for the new installation.

To install these upgrades or service packs, go to the Microsoft Download Center web site at:

<http://www.microsoft.com/downloads/>

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. The user name and password refers to one of the users you added to the PPTP-Users group (see [Add new users to the PPTP-Users authentication group](#)).

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. This information was given when you added the user to PPTP-Users.
For more information about the user name and passphrase, see [Add new users to the PPTP_Users group](#).
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. This information was given when you added the user to PPTP-Users.
For more information about the user name and passphrase, see [Add new users to the PPTP_Users group](#).
4. Click **Connect**.

24 Mobile VPN with IPSec

About a Mobile VPN with IPSec configuration for your Firebox

WatchGuard Mobile VPN with IPSec is a client 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.

These topics include instructions to help you configure a Mobile VPN tunnel between the WatchGuard Mobile VPN with IPSec client and a Firebox X Core or Firebox X Peak device running Fireware.

Configure a Mobile VPN with IPSec connection

You can configure the Firebox to host Mobile VPN with IPSec sessions. From Policy Manager, select **VPN > Mobile VPN > IPSec**.

For more information about the Mobile VPN with IPSec client, see [About the Mobile VPN with IPSec client](#).

For more information about installing the Mobile VPN with IPSec client, see [Install the Mobile VPN with IPSec client software](#).

You create the Mobile VPN group using the Add Mobile VPN with IPSec wizard.

When the wizard is finished, Policy Manager does two things:

- Makes a client configuration profile (called a .wgx file) and puts it on the management station computer that created the Mobile VPN account. The user must have this .wgx file to configure the Mobile VPN client computer.
- Automatically adds an Any policy to the **Mobile VPN** tab that allows traffic to pass to and from the authenticated Mobile VPN user.

When the user's computer is correctly configured, the user makes the Mobile VPN connection. If the user name and password the user enters into the Mobile VPN authentication dialog box match an entry in the Firebox User database, and if the user is in the Mobile VPN group you create, the Mobile VPN session is authenticated. Policy Manager automatically makes a policy that allows any traffic from the authenticated user. To restrict the ports the Mobile VPN client can access, delete the Any policy and add policies for those ports to the **Mobile VPN with IPSec** tab.

To learn how to add policies, see [About Policy Manager](#).

Client requirements

Before you begin, make sure you understand the client requirements:

- Because strict export restrictions are put on exported high encryption software, WatchGuard System Manager is available with two encryption levels. You must make sure you download and use WatchGuard System Manager with strong encryption when you use Mobile VPN with IPSec, because the IPSec standard requires a minimum of 56-bit (medium) encryption.
- You can install the Mobile VPN with IPSec client software on any computer running:
 - 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.

Options for Internet access through a Mobile VPN 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. When you use default-route VPN, a dynamic NAT policy must include the outgoing traffic from the remote network. This allows remote users to browse the Internet when they send all traffic to the Firebox.

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.

About Mobile VPN client configuration files

With Mobile VPN with IPSec, the network security administrator controls end-user profiles. Policy Manager is used to set the name of the end user and create a client configuration file, or profile, with the file extension .wgx. The .wgx 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 Firebox. 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 .wgx file is imported on the remote client, this key is used to decrypt the file for the client software to use.

After you use the Add Mobile User VPN wizard, you can create or re-create a .wgx file at any time.

If you want to lock the profiles for mobile users by making them read-only, see [Lock down an end-user profile](#).

Configure the Firebox for Mobile VPN

You can enable Mobile VPN with IPSec for an existing group of users or you can create a new user group. The users in the group can authenticate either to the local Firebox authentication server, or to a third-party authentication server included in your Firebox configuration.

For more information about adding users to a group for local Firebox authentication, see [Add users to a Firebox Mobile VPN group](#). If you use a third-party authentication server, follow the instructions provided in that vendor's documentation.

1. From Policy Manager, select **VPN > Mobile VPN > IPSec**.
The Mobile VPN with IPSec Configuration dialog box appears.



2. Click **Add**.

The *Add Mobile User VPN with IPSec Wizard* appears.



3. Click **Next**.

4. **Select a user authentication server** screen:

- Select an authentication server from the **Authentication Server** drop-down list. You can authenticate users with the internal Firebox database (Firebox-DB) or with a RADIUS, VASCO, SecurID, LDAP, or Active Directory server. Make sure that this method of authentication is enabled in Policy Manager (select **Setup > Authentication > Authentication Servers**).
- Type a group name in the **Group Name** field. You can type the name of an existing Mobile VPN group, or enter a group name for a new Mobile VPN group. Make sure the name is unique among VPN group names as well as all interface and tunnel names. For more information about VPN groups, see [Authentication types](#).



5. Click **Next**.
6. **Select a tunnel authentication method** screen:
 - Select **Use this passphrase**.
 - Type and confirm a passphrase.

When your remote users import their Mobile VPN connection profile, they will need this passphrase. In the Mobile VPN Configuration Assistant, this passphrase is known as the pre-shared key or shared secret.

7. Click **Next**.
8. **Direct the flow of Internet traffic** screen:

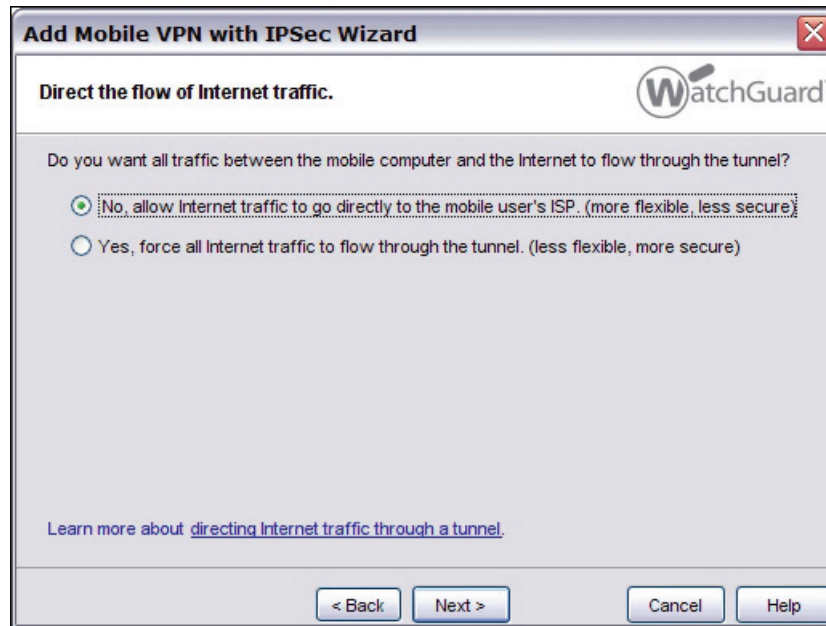
Select an option for Internet traffic.

 - **No, allow Internet traffic to go directly to the mobile user's ISP.**
(Split tunneling)

- **Yes, force all Internet traffic to flow through the tunnel.**

(Default-route VPN)

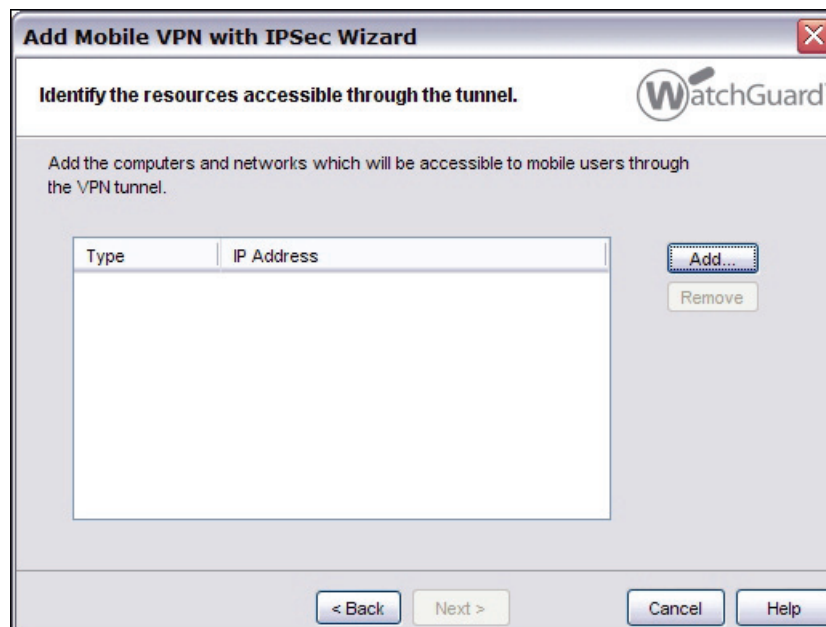
For more information about split tunneling and default-route VPN, see [Access the Internet through a Mobile VPN tunnel](#).



9. Click **Next**.

10. **Identify the resources accessible through the tunnel** screen:

- Click **Add** to specify the host or network IP addresses that users can connect to through the VPN tunnel.



11. Click **Next**.

12. **Create the virtual IP address pool** screen:

- Click **Add** to add one IP address or an IP address range.
To add more virtual IP addresses, repeat this step.



Mobile VPN users will be assigned one of these IP addresses when they connect to your network. The number of IP addresses should be the same as the number of Mobile VPN users. If High Availability is configured, you must add two virtual IP addresses for each Mobile VPN user. The IP addresses cannot be used for anything else on your network.

13. Click **Next**.

14. Click **Finish**.

The Mobile VPN with IPSec Configuration dialog box appears with the new group you created at the bottom of the user group list.

15. Click **OK** to close.

The Mobile VPN client profile is saved in Documents and Settings\All Users\ Shared WatchGuard\muvpn\ip_address\config_name\wgx\config_name.wgx.

Configure the external authentication server

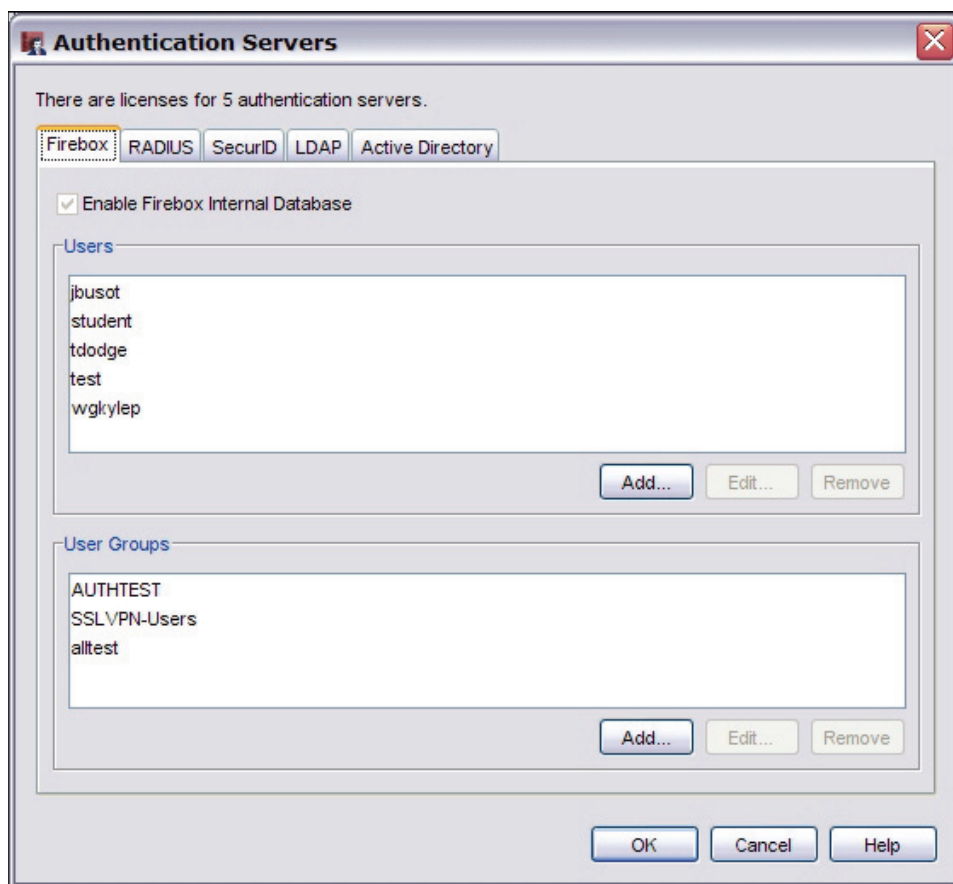
If you create a Mobile VPN user group that authenticates to a third-party server, make sure you create a group on the server that has the same name as the Mobile VPN group name entered in the wizard. For RADIUS, VASCO, or SecurID, make sure that the RADIUS server sends a Filter-Id attribute (RADIUS attribute #11) when a user successfully authenticates, to tell the Firebox what group the user belongs to. The value for the Filter-Id attribute must match the name of the Mobile VPN group as it appears in Policy Manager. All Mobile VPN users that authenticate to the server must belong to this group.

Add users to a Firebox Mobile VPN group

To create an Mobile VPN tunnel with the Firebox, remote users type their user name and password to authenticate. WatchGuard System Manager software uses this information to authenticate the user to the Firebox.

To authenticate, users must be part of the group entered in the Add Mobile User VPN Wizard. If you use Firebox authentication, use the instructions below. If you use a third-party authentication server, use the instructions provided in your vendor documentation. For more information on Firebox groups, see [Authentication types](#).

1. From Policy Manager, select **Setup > Authentication > Authentication Servers**.
The Authentication Servers dialog box appears.



2. Select the **Firebox** tab.

- To add a new user, click the **Add** button below the **Users** list.
The Setup Firebox User dialog box appears.

Setup Firebox User

User Information

Name:

Description:

Passphrase:

Confirm:

Session Timeout: hours

Idle Timeout: minutes

Firebox Authentication Groups

Member:

Available:

- AUTHTEST
- SSLVPN-Users
- alltest

<< >>

OK Cancel Help

- Type a user name and passphrase for the new user. Type the passphrase again to confirm it.
Description is not required. Do not change the values for Session Timeout and Idle Timeout unless the change is necessary.
- In the **Firebox Authentication Groups** window click the horizontal arrows to make the new user a member of the group you created in the wizard.
- Click **OK**.
The new user appears in the Users list in the Authentication Servers dialog box. The dialog box stays open for you to add more users if you choose.
- To close the **Authentication Servers** dialog box, click **OK**.

Modify an existing Mobile VPN profile

After you use the Mobile User VPN wizard to create a new .wgx file, you can edit the profile to:

- Change the shared key
- Add access to more hosts or networks
- Restrict access to a single destination port, source port, or protocol
- Change the Phase 1 or Phase 2 settings.

1. From Policy Manager, select **VPN > Mobile VPN > IPSec**.

The Mobile VPN with IPSec Configuration dialog box appears.



2. Select the user name or group from the list that you want to change.

3. Click **Edit**.

The *Edit Mobile VPN with IPSec* dialog box appears.

Edit Mobile VPN with IPSec

Group Name:

General | IPsec Tunnel | Resources

Authentication Server

Passphrase

Used to encrypt the Mobile VPN with IPSec end-user profile for this group.

Passphrase:

Confirm:

Firebox IP Addresses

Mobile VPN with IPSec clients will connect to one of these External IP addresses or domains.

Primary:

Backup:

Timeouts

When you use the Firebox as your authentication server, you set the timeout in each Firebox User account.

Session: minutes

Idle: minutes

4. Use the following fields on the **General** tab to edit the group profile:*Authentication Server*

Select the authentication server to use for this Mobile VPN group. To configure your authentication server, select **Setup > Authentication > Authentication Servers** from the menu bar in Policy Manager.

Passphrase

Type a passphrase to encrypt the Mobile VPN profile (.wgx file) that you distribute to users in this group.

Confirm

Type the passphrase again.

Primary

Select or type the primary external IP address to which Mobile VPN users in this group can connect.

Backup

Select or type a backup external IP address to which Mobile VPN users in this group can connect. This backup IP address is optional. If you add a backup IP address, make sure it is an IP address assigned to a Firebox external interface.

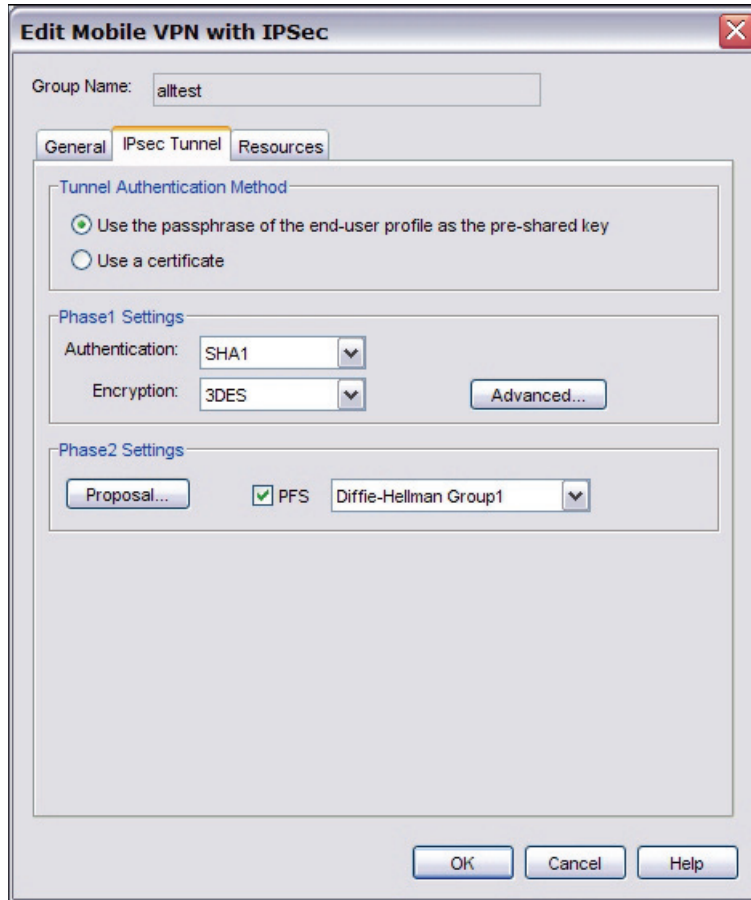
Session

Select the maximum time in minutes that a Mobile VPN session can be active.

Idle

Select the time in minutes before the Firebox closes an idle Mobile VPN session. The session and idle timeout values are the default timeouts if the authentication server does not return specific timeout values. If you use the Firebox as the authentication server, the timeouts for the Mobile VPN group are always ignored because you set timeouts in the individual Firebox user accounts. The session and idle timeouts cannot be longer than the value in the **SA Life** field. To set this field, from the **IPSec Tunnel** tab of the **Edit MUVPN Extended Authentication Group** dialog box, click **Advanced**. The default value is 8 hours.

- Click the **IPSec Tunnel** tab.



- Use the following fields on the **IPSec tunnel** tab to edit settings:

Use the passphrase of the end-user profile as the pre-shared key

Select this setting to use the passphrase of the end-user profile as the pre-shared key for tunnel authentication. You must use the same shared key on the remote device, and this shared key can use only standard ASCII characters.

Use a certificate

Select this setting to use a certificate for tunnel authentication. You must start the WatchGuard Certificate Authority if you select certificate-based authentication. You must also use the WatchGuard Log Server for log messages and the Firebox must be a managed client of a WatchGuard Management Server. The WatchGuard Certificate Authority is installed by default as part of the Management Server installation.

CA IP address

(This field appears only if you select to use a certificate) Type the IP address for the certificate authority (CA).

Timeout

(This field appears only if you select to use a certificate) Type the time in seconds before the certificate authority request times out.

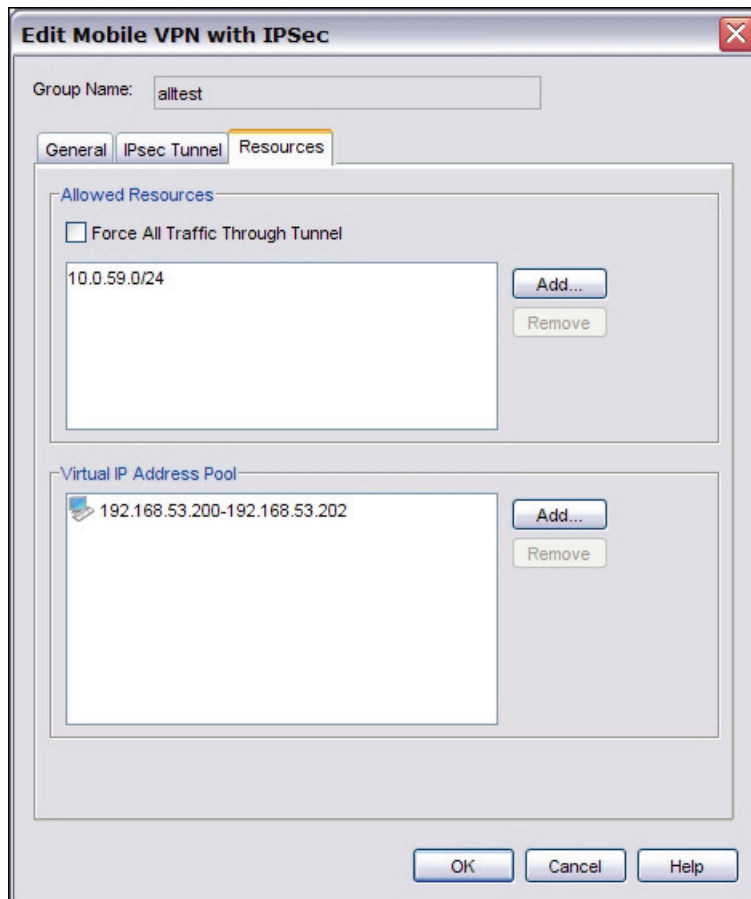
Phase1 Settings

Select the authentication and encryption methods for the Mobile VPN tunnel. These settings must be the same for both VPN endpoints. To configure advanced settings, such as NAT Traversal or the key group, click the **Advanced** button, and see the procedure described in [Define advanced Phase 1 settings](#).

Phase2 Settings

Select the proposal and key expiration settings for the Mobile VPN tunnel. You can also enable Perfect Forward Secrecy (PFS) or set the Diffie-Hellman group. To change other proposal settings, click the **Proposal** button, and see the procedure described in [Define advanced Phase 2 settings](#).

- Click the **Resources** tab.



- Use the following fields to add and remove allowed network resources and virtual IP addresses:

Allowed Resources list

This list shows the resources that users in the Mobile VPN authentication group can get access to on the network. Click **Add** to add an IP address or IP address range to the network resources list. Click **Remove** to clear the selected IP address or IP address range from the network resources list.

Force All Traffic Through Tunnel

Select this check box to send all Mobile VPN user Internet traffic through the VPN tunnel. When this is selected, Mobile VPN user Internet traffic is sent through the VPN, but web sites can be slower for those users. If this is not selected, Mobile VPN user Internet traffic is not sent safely, but users can browse the Internet more quickly.

Virtual IP Address Pool

This list shows the internal IP addresses that are used by Mobile VPN users over the tunnel. These addresses are used only when they are needed. Click **Add** to add an IP address or IP address range to the virtual IP address pool. Click **Remove** to clear the selected IP address or IP address range from the virtual IP address pool.

- Click **OK**.

The Edit Mobile VPN with IPSec dialog box appears.



End-user profiles (.wgx) for the profile you edited are automatically regenerated. You must distribute new end-user profiles to the affected users and groups.*

Define advanced Phase 1 settings

You can define the advanced Phase 1 settings for your Mobile VPN user profile.

- From the **IPSec Tunnel** tab of the **Edit Mobile VPN with IPSec** dialog box, select **Advanced**.
The Phase1 Advanced Settings dialog box appears.

The image shows the 'Phase1 Advanced Settings' dialog box. It contains the following fields and options:

- SA Life:** 8 (spin box) hour (dropdown)
- Key Group:** Diffie-Hellman Group1 (dropdown)
- ☒ **NAT Traversal**
 - Keep-alive interval:** 20 (spin box) seconds
- ☒ **IKE Keep-alive**
 - Message interval:** 20 (spin box) seconds
 - Max failures:** 2 (spin box)
- ☒ **Dead Peer Detection (RFC3706)**
 - Traffic idle timeout:** 90 (spin box) seconds
 - Max retries:** 5 (spin box)

At the bottom are buttons for **OK**, **Cancel**, and **Help**.

- Configure the setting options for your profile.
For more information about the available options, see Setting Options below.
- Click **OK**.

Setting Options

SA Life

Select a SA (security association) lifetime duration and select **Hour** or **Minute** from the drop-down list.

Key Group

Select the Diffie-Hellman group you want. WatchGuard supports groups 1, 2, and 5. Diffie-Hellman groups determine the strength of the master key used in the key exchange process. Higher group numbers have greater security, but more time is required to make the keys.

NAT Traversal

Select this check box to build a Mobile VPN tunnel between the Firebox and another device that is behind a NAT device. NAT Traversal, or UDP Encapsulation, allows traffic to route to the correct destinations.

IKE Keep-alive

You must select this check box to enable the Firebox to send messages to its IKE peer to keep the VPN tunnel open. If you disable the IKE Keep-alive feature, the Mobile VPN client will not be able to connect to the Firebox.

Keep-alive interval

Select the number of seconds for the keep-alive interval.

Message interval

Select the number of seconds for the keep-alive message interval.

Max failures

Set the maximum number of times the Firebox sends an IKE keep-alive message before it tries to negotiate Phase 1 again.

Dead Peer Detection

Select this check box to enable Dead Peer Detection (DPD). DPD is based on RFC 3706 and uses IPSec traffic patterns to determine if a connection is live before a packet is sent. When you select DPD, an are-you-there message is sent to the peer when no traffic has been received from the peer within the selected time period. If DPD determines a peer detection is dead, additional connection attempts are not made.

Traffic Idle Timeout

Set the number of seconds the Firebox waits before it sends an are-you-there message.

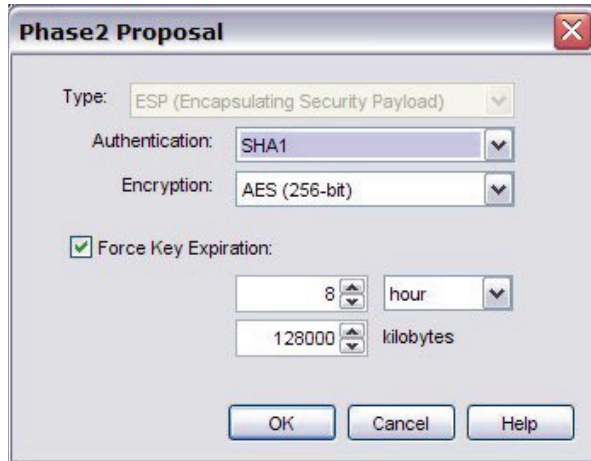
Max retries

Set the maximum number of times the Firebox sends an are-you-there message to a peer before it determines the peer connection is dead.

Define advanced Phase 2 settings

You can define the advanced Phase 2 settings for your Mobile VPN user profile.

1. From the **IPSec Tunnel** tab of the **Edit Mobile VPN with IPSec** dialog box, select **Proposal**.
The Phase2 Proposal dialog box appears.



2. Configure the setting options for your profile.
For more information about the available options, see Setting Options below.
3. Click **OK**.

Setting Options

Type

ESP or **AH** are the two proposal method options. Only ESP is supported at this time.

Authentication

Select **SHA1** or **MD5** for the authentication method from the drop-down list.

Encryption

Select an encryption method from the drop-down list. The options are listed from the most simple and least secure, to the most complex and most secure.

- None
- DES
- 3DES
- AES (128 bit)
- AES (192 bit)
- AES (256 bit)

Force Key Expiration

Select this check box to generate the gateway endpoints and exchange new keys after a quantity of time or amount of traffic passes through the gateway.

In the fields below **Force Key Expiration**, select a quantity of time and a number of bytes after which the key expires.

If **Force Key Expiration** is disabled, or if it is enabled and both the time and kBytes are set to zero, the Firebox tries to use the key expiration time set for the peer. If this is also disabled or zero, the Firebox uses a key expiration time of 8 hours. You can set the time up to one year.

Route Internet access through Mobile VPN tunnels

You can give remote users access to the Internet through a Mobile VPN tunnel when you use the **Add Mobile VPN with IPSec Wizard** and select the **Yes, force all Internet traffic to flow through the tunnel** option on the Direct the flow of Internet traffic screen. This ensures all Internet traffic travels through the Firebox VPN tunnel (direct-route VPN), which is a more secure option than to allow Internet traffic to go around the VPN tunnel (split tunnel VPN). This option adds Any-External as an allowed resource, which means that traffic destined to go out any external interface is allowed.

For more information about direct-route VPN and split tunnel VPN, see [Access the Internet through a Mobile VPN tunnel](#).

Configure WINS and DNS servers

Mobile VPN clients rely on shared Windows Internet Name Server (WINS) and Domain Name System (DNS) server addresses. DNS translates host names into IP addresses. WINS resolves NetBIOS names to IP addresses. These servers must be accessible from the Firebox trusted interface.

Make sure you use only an internal DNS server. Do not use external DNS servers.

1. From Policy Manager, select **Network > Configuration**.
The Network Configuration dialog box appears.
2. Select the **WINS/DNS** tab.
The information for the WINS and DNS servers appears.

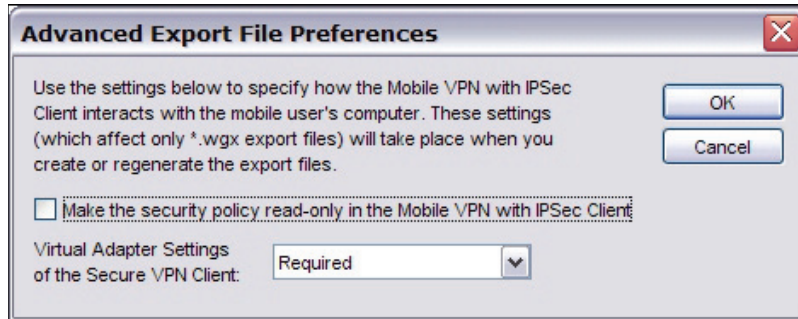
The screenshot shows the 'Network Configuration' dialog box with the 'WINS/DNS' tab selected. The dialog has a title bar with a close button. Below the title bar are five tabs: 'Interfaces', 'VLAN', 'WINS/DNS' (which is highlighted), 'Dynamic DNS', and 'Multi-WAN'. The main area of the dialog is divided into two sections. The first section is titled 'DNS (Domain Name System) Servers' and contains a 'Domain Name:' text box and a 'DNS Servers:' text box. The 'DNS Servers' box contains two lines of IP addresses: '192.168.130.131' and '192.168.130.245', followed by a line with three dots. The second section is titled 'WINS (Windows Internet Naming Service) Servers' and contains a 'WINS Servers:' text box with two lines of IP addresses, each followed by three dots. At the bottom right of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

3. Type a domain name for the DNS server.
4. In the **DNS Servers** and **WINS Servers** text boxes, type the addresses for the WINS and DNS servers.
5. Click **OK**.

Lock down an end-user profile

You can use the advanced settings to lock down the end-user profile so that users can see some settings but not change them, and hide other settings so that users cannot change them. We recommend that you lock down all profiles so that users cannot make changes to their profile.

1. From Policy Manager, select **VPN > Mobile VPN > IPSec**.
The Mobile VPN with IPSec Configuration dialog box appears.
2. Click **Advanced**.
The Advanced Export File Preferences dialog box appears.



3. To give mobile users only read-only access to their profiles, select the **Make the security policy read-only in the MUVPN Client** check box.
4. Select a **Virtual Adapter Settings of the Secure VPN Client** option from the drop-down list: **Disabled, Preferred, Required**.



The Mobile VPN client always uses a virtual adapter, so you should not change the virtual adapter settings on this dialog box. The Mobile VPN client does not operate without a virtual adapter.

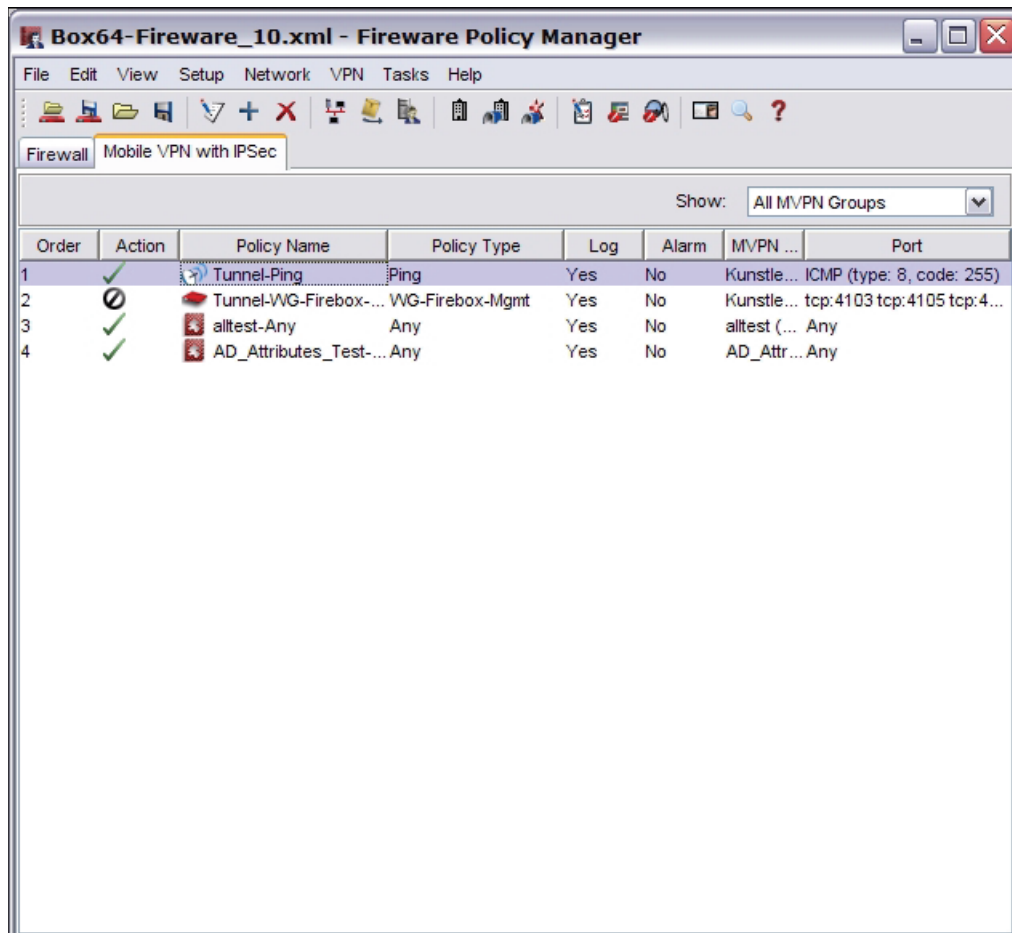
5. Click **OK**.

Configure policies to filter Mobile VPN traffic

In a default configuration, Mobile VPN with IPSec users have full access privileges through a Firebox, with the Any policy. To put limits on Mobile VPN users, you must add policies to the **Mobile VPN with IPSec** tab in Policy Manager.

Add individual policies

1. In Policy Manager, click the **Mobile VPN with IPsec** tab.



2. From the **Show** drop-down list, select the name of the Mobile VPN group for which you are adding a policy. You must select a group before you add a policy.
3. Add, edit, and delete policies as described in [About policies](#). Make sure you save your configuration file to the Firebox after you make these changes.

Change the view

You can choose to see the policy list as large icons or as a detailed list.

- To see large icons and no details, select **View > Large Icons**.
- To see more information in a detailed list, select **View > Details**.

Under **MVPN Group**, Policy Manager displays the authentication server, in parentheses, for the Mobile VPN group.

Use the Any policy

The Any policy is added to all Mobile VPN user groups by default. The Any policy allows traffic on all ports and protocols between the Mobile VPN user and the Remote Networks available through the Mobile VPN tunnel. If you want to restrict traffic for Mobile VPN users to a more limited group or ports and protocols, the Any policy on the Mobile User VPN can be deleted and replaced with policies specified by the administrator.

For more information about adding policies, see [Add policies to your configuration](#).

Re-creating end-user profiles

The WatchGuard Mobile VPN with IPSec configuration gives you the ability to re-create end-user profiles for your existing Mobile VPN users. Use this procedure to create new end-user profiles with the same settings for the current MUVPN users.

Mobile VPN configuration files, or profiles, are located in Documents and Settings\All Users\ Shared Watchguard\muvpn\ip_address\config_name\wgx\config_name.wgx. If the tunnel is authenticated with certificates, the certificates are also created.

To create new end-user profiles for current Mobile VPN users, on the Policy Manager **Mobile User VPN** tab, select the Mobile VPN group and click **Generate**.

You can now distribute these end-user profiles as necessary.

Save the profile to a Firebox

To activate a new Mobile VPN user profile, you must save the configuration file to the Firebox.

From Policy Manager, click .

Or, select **File > Save > To Firebox**.

Distribute the software and profiles

WatchGuard recommends distributing end-user profiles by encrypted email or with 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.
- The end-user profile
This file contains the group name, shared key, and settings that enable a remote computer to connect securely over the Internet to a protected, private computer network. The end-user profile has the file name **groupname.wgx**.
- Two certificate files—if you are authenticating with certificates
These are the .p12 file, which is an encrypted file containing the certificate; and cacert.pem, which contains the root (CA) certificate.
- User documentation
Documentation to help the remote user install the Mobile VPN client and import the Mobile VPN configuration file can be found in the [About Mobile VPN client configuration files](#) topics.
- 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 during the creation of the file in Policy Manager.



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.

Additional Mobile VPN topics

This section describes special topics for Mobile VPN with IPSec.

Making outbound IPSec connections from behind a Firebox

A user might have to make IPSec connections to a Firebox from behind another Firebox. For example, if a mobile employee travels to a customer site that has a Firebox, that user can make IPSec connections to their network using IPSec. For the local Firebox to correctly handle the outgoing IPSec connection, you must set up an IPSec policy that includes the IPSec packet filter. For information on enabling policies, see [About policies](#).

Because the IPSec policy enables a tunnel to the IPSec server and does not complete any security checks at the firewall, add to this policy only the users that you trust.

Terminate IPSec connections

To fully stop VPN connections, the Firebox must be restarted. Removing the IPSec policy does not stop current connections.

Global VPN settings

Global VPN settings on your Firebox apply to all manual BOVPN tunnels, managed tunnels, and Mobile VPN tunnels. You can use these settings to:

- Enable IPSec pass-through.
- Clear or maintain the settings of packets with Type of Service (TOS) bits set.
- Use an LDAP server to verify certificates.

To change these settings, from Policy Manager, select **VPN > VPN Settings**. For more information on these settings, see [About Global VPN settings](#).

See the number of Mobile VPN licenses

You can see the number of Mobile VPN licenses that are installed from Policy Manager.

1. Select **Setup > Feature Keys**.
The Firebox Feature Key dialog box appears.
2. Scroll down to **Mobile User VPN Users** in the **Features** column, and look at the number in the **Capacity** column. This is the number of installed Mobile VPN licenses.

Purchase additional Mobile VPN licenses

WatchGuard Mobile VPN with IPSec is an optional feature. Each Firebox X device includes a number of Mobile VPN licenses. You can purchase more licenses for Mobile VPN.

Licenses are available through your local reseller or at:

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

Add feature keys

For information on adding feature keys, see [About feature keys](#).

Mobile VPN and VPN failover

You can configure VPN tunnels to fail over to a backup endpoint if the primary endpoint becomes unavailable. For more information on VPN failover, see [Configure VPN failover](#).

If VPN failover is configured and failover occurs, Mobile VPN sessions do not continue. You must authenticate your Mobile VPN client again to make a new Mobile VPN tunnel.

To configure VPN failover for Mobile VPN tunnels:

1. From Policy Manager, select **VPN > Mobile VPN > IPSec**.
The Mobile VPN with IPSec Configuration dialog box appears.
2. Select a mobile user group from the list and click **Edit**.
The Edit Mobile VPN with IPSec dialog box appears.
3. Select the **General** tab.
4. Type a backup WAN interface IP address in the **Backup** field in the **Firebox IP Addresses** box.
You can specify only one backup interface for tunnels to fail over to, even if you have additional WAN interfaces.

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.

Install the Mobile VPN with IPSec client software

The installation process consists of two parts: installing the client software on the remote computer and importing the end-user profile into the client. Before you start the installation, make sure you have the following installation components, which you should get from your network administrator:

- The Mobile VPN installation file
- An end-user profile, with a file extension of .wgx
- Shared Key
- A .p12 certificate file (if you are connecting to a Firebox X Core or Peak and use certificates to authenticate)
- User name and password (if you are connecting to a Firebox X Core or Peak and use Extended Authentication)



Write the shared key down and keep it in a secure location. You must use it during the final steps of the installation procedure.

To install the client:

1. Copy the Mobile VPN .zip file to the remote computer and extract the contents of the file.
2. Copy the end-user profile (the .wgx file) to the root directory on the remote (client or user) computer. *If you use certificates to authenticate, copy the .p12 file to the root directory as well.*
3. Run the Mobile VPN executable file by double-clicking the .exe file you extracted in step 1. This starts the WatchGuard Mobile VPN Installation wizard. You must restart your computer when the installation wizard completes.

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**.



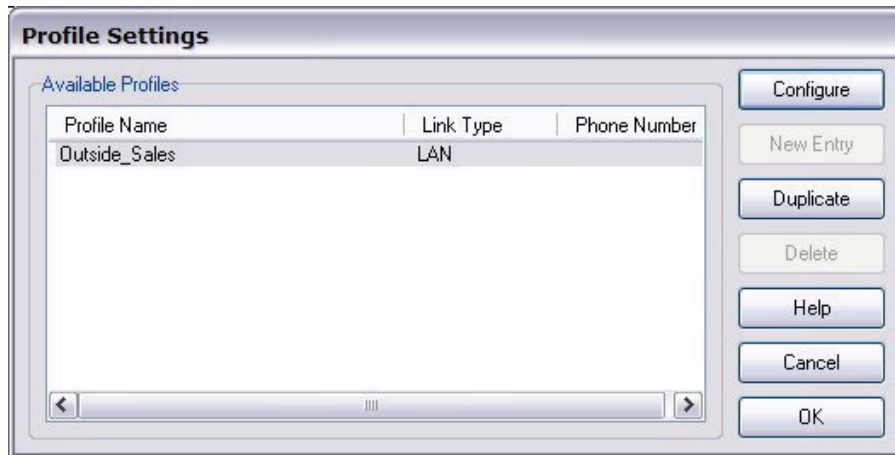
Disconnect the Mobile VPN client

From the Mobile VPN Monitor, click **Disconnect**.

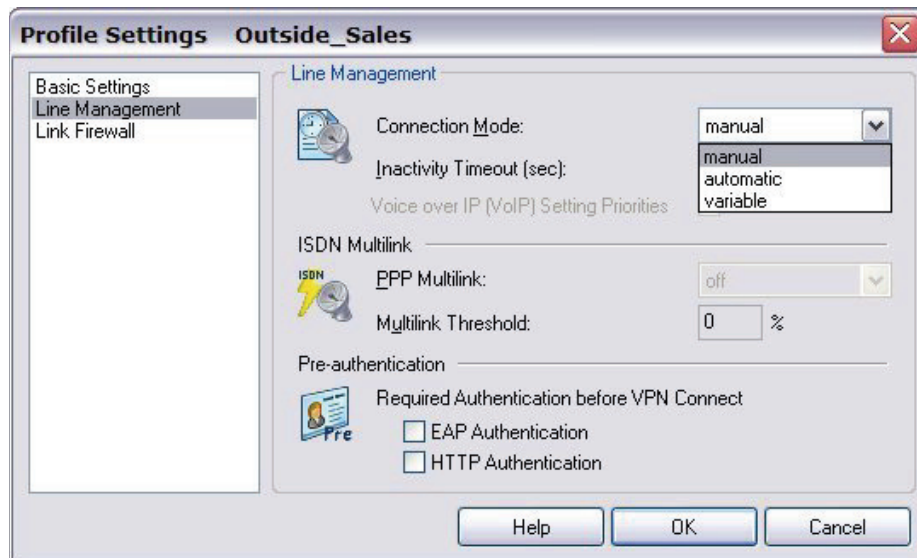
Control connection behavior

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

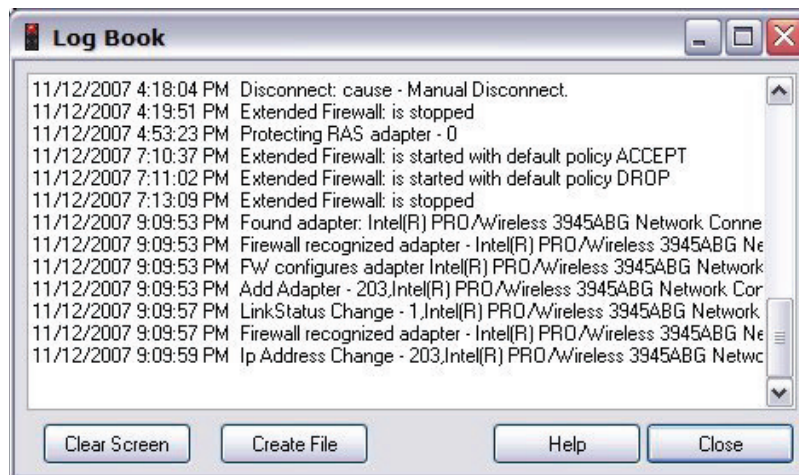
The Mobile User VPN icon appears in the Windows desktop system tray to show the status of the full featured desktop firewall, the link firewall, and the VPN network. You can right-click the icon to easily connect and disconnect your Mobile VPN and see which profile is in use.

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

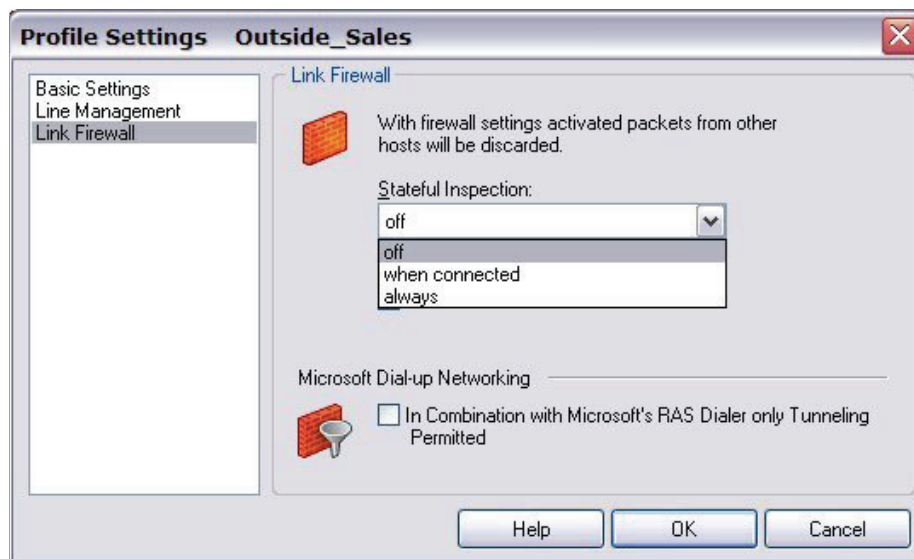
This full-featured firewall can control connections to and from your computer. You can define friendly networks and set access rules separately for friendly and unknown networks.

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

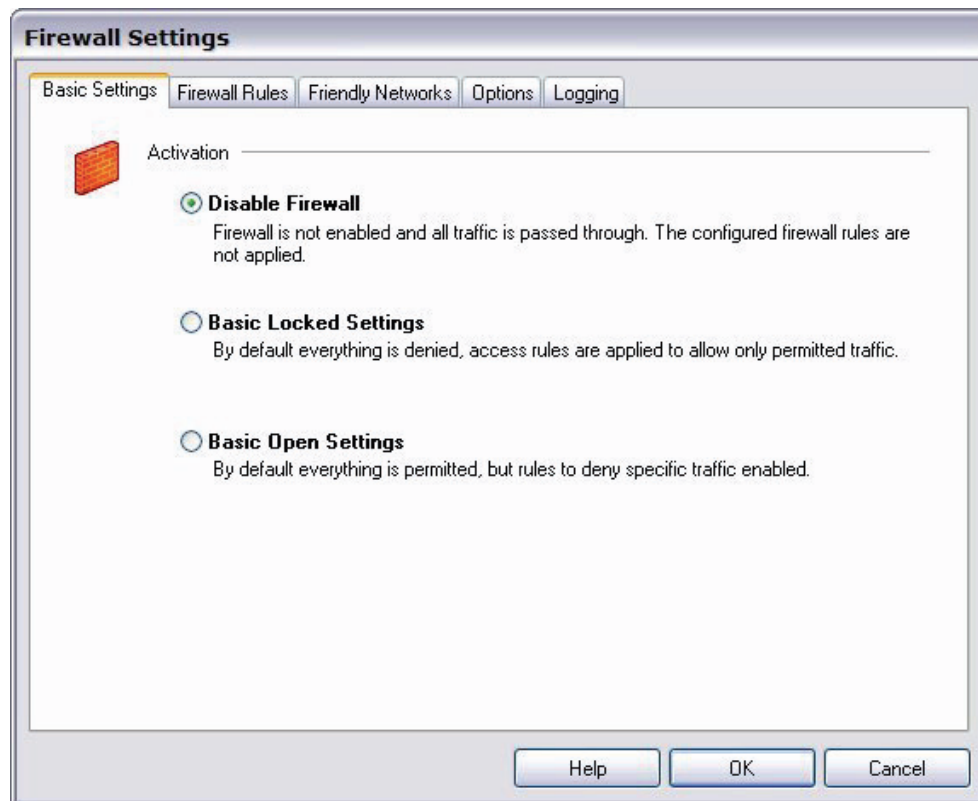
Any network specified in the firewall as a known network.

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:
 - **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.
 - **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.

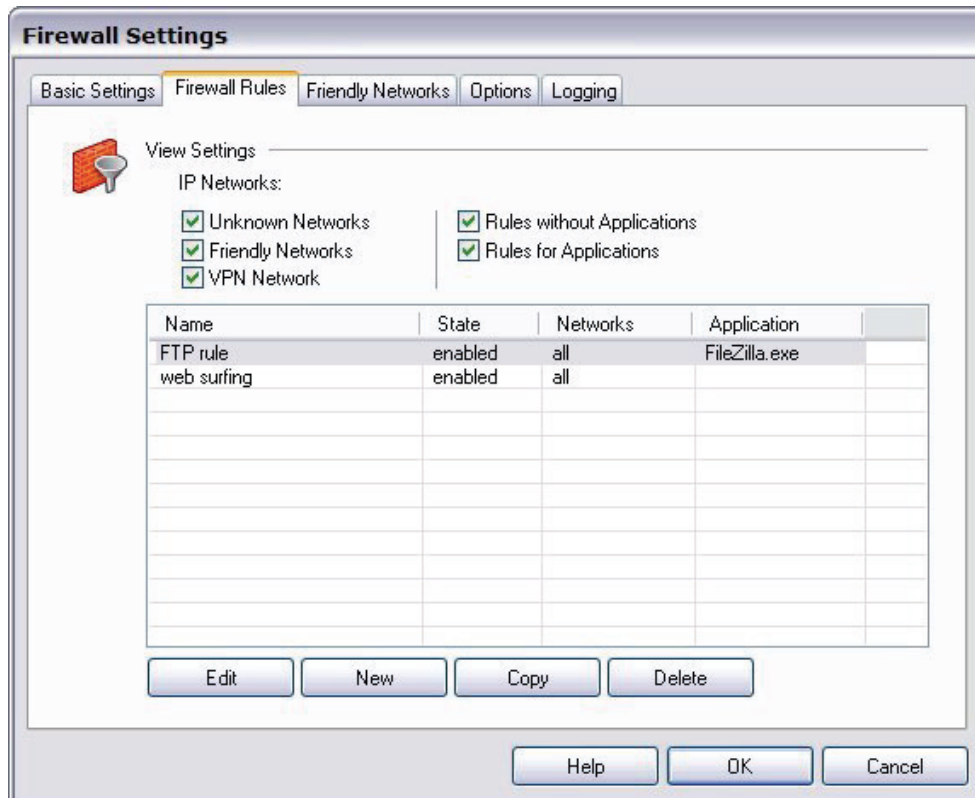
1. From the **Firewall Settings** dialog box, click the **Friendly Networks** tab.
2. Click **New** to add a new friendly network.

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

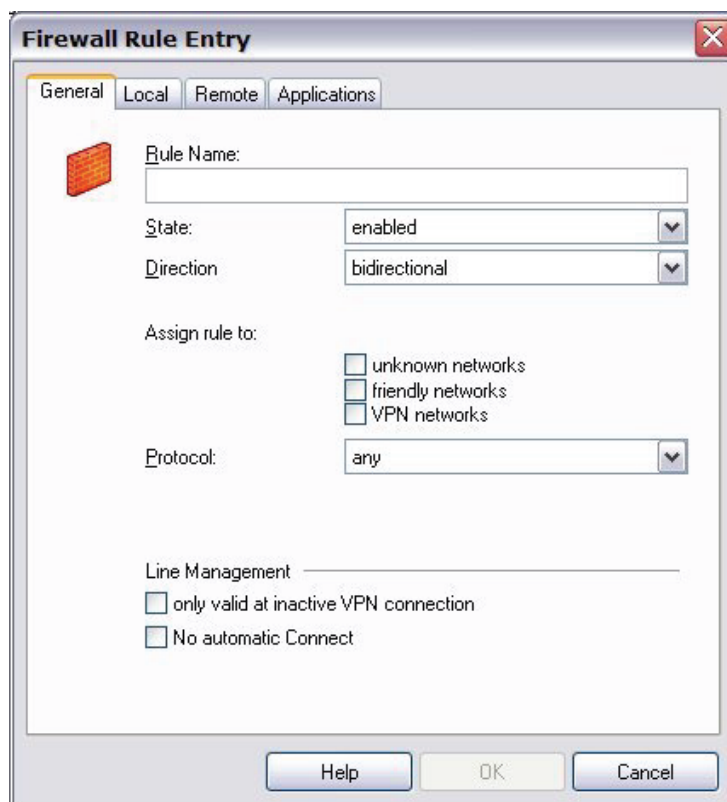
To apply the rule to traffic that comes from your computer, select **outgoing**. To apply the rule to traffic that is sent to your computer, select **incoming**. To apply the rule to all traffic, select **bidirectional**.

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.



The screenshot shows the 'Firewall Rule Entry' dialog box with the 'General' tab selected. The dialog has four sub-tabs: 'General', 'Local', 'Remote', and 'Applications'. The 'General' tab contains the following fields and options:

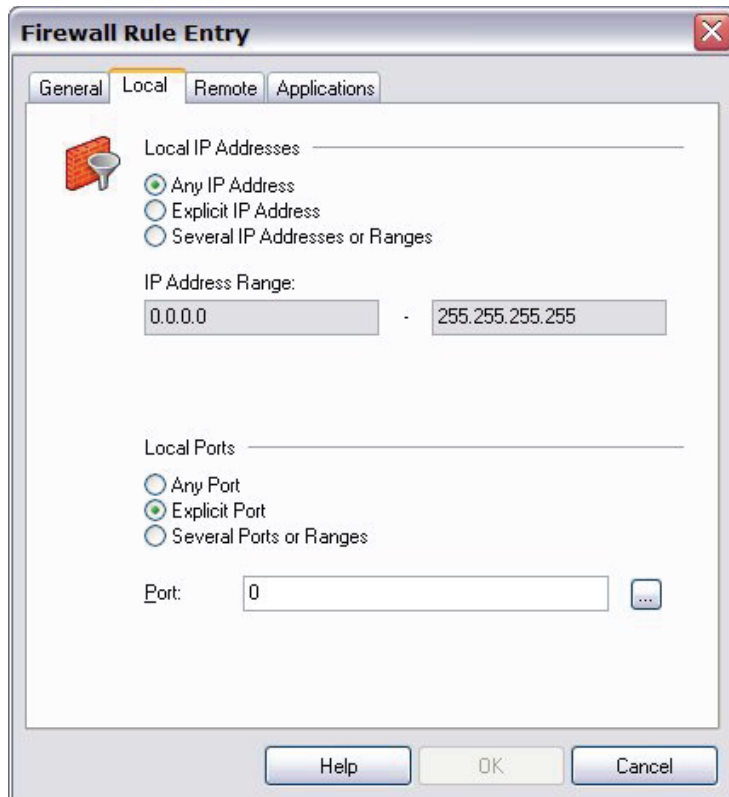
- Rule Name:** A text input field.
- State:** A dropdown menu currently set to 'enabled'.
- Direction:** A dropdown menu currently set to 'bidirectional'.
- Assign rule to:** Three checkboxes: 'unknown networks' (unchecked), 'friendly networks' (unchecked), and 'VPN networks' (unchecked).
- Protocol:** A dropdown menu currently set to 'any'.
- Line Management:** Two checkboxes: 'only valid at inactive VPN connection' (unchecked) and 'No automatic Connect' (unchecked).

At the bottom of the dialog are three buttons: 'Help', 'OK', and 'Cancel'.

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.



The screenshot shows the 'Firewall Rule Entry' dialog box with the 'Local' tab selected. The 'Local IP Addresses' section has three radio buttons: 'Any IP Address' (selected), 'Explicit IP Address', and 'Several IP Addresses or Ranges'. Below this is an 'IP Address Range' field with '0.0.0.0' and '255.255.255.255' entered. The 'Local Ports' section has three radio buttons: 'Any Port', 'Explicit Port' (selected), and 'Several Ports or Ranges'. Below this is a 'Port' field with '0' entered. At the bottom are 'Help', 'OK', and 'Cancel' buttons.

Firewall Rule Entry

General Local Remote Applications

Local IP Addresses

☒ Any IP Address
☐ Explicit IP Address
☐ Several IP Addresses or Ranges

IP Address Range:
0.0.0.0 - 255.255.255.255

Local Ports

☐ Any Port
☒ Explicit Port
☐ Several Ports or Ranges

Port: 0

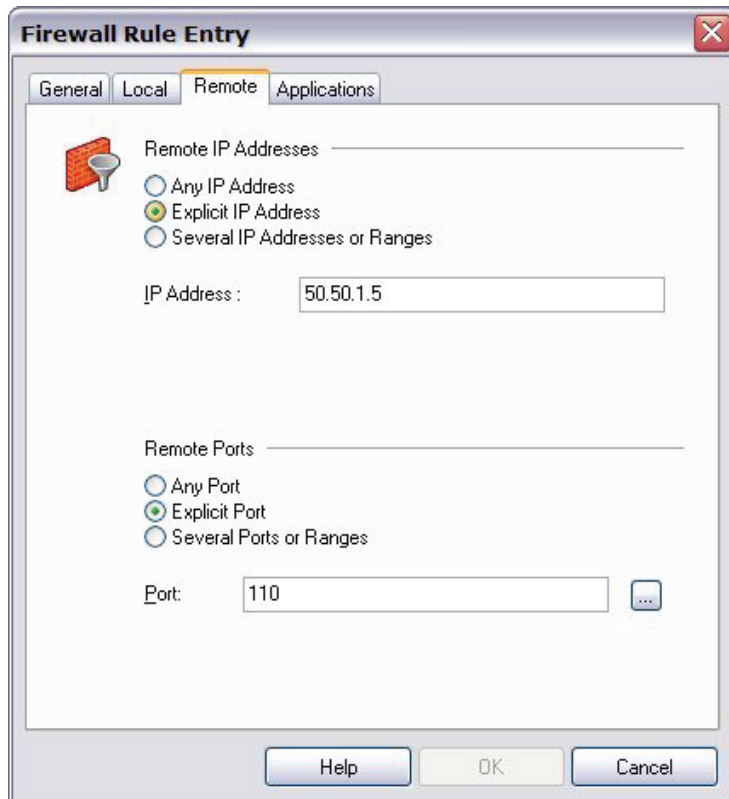
Help OK Cancel

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.

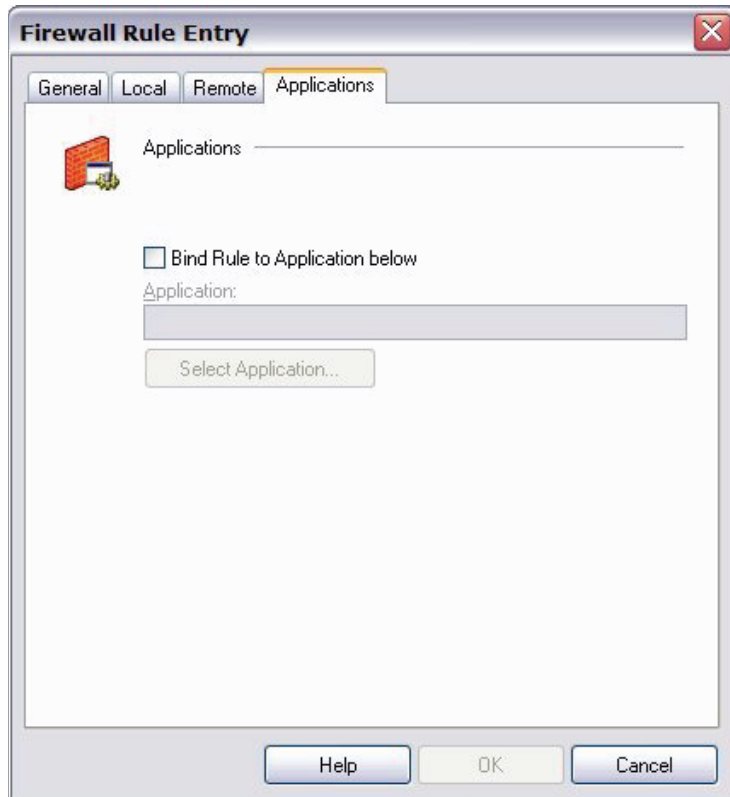
If you select the **Explicit IP Address** radio button, make sure you specify an IP address. The IP address must not be set to 0.0.0.0.



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**.

25 Mobile VPN with SSL

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.

Options for Internet access through a Mobile VPN 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. When you use default-route VPN, a dynamic NAT policy must include the outgoing traffic from the remote network. This allows remote users to browse the Internet when they send all traffic to the Firebox.

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.

Configure the Firebox for Mobile VPN with SSL

1. From Policy Manager, select **VPN > Mobile VPN > SSL**.
The *Mobile VPN with SSL Configuration* dialog box appears.

2. Select the **Activate Mobile VPN with SSL** check box.
3. Select an authentication server from the **Authentication Server** drop-down list. You can authenticate users with the internal Firebox database (Firebox-DB) or with a RADIUS, VACMAN Middleware, SecurID, LDAP, or Active Directory server.
Make sure that the method of authentication is enabled in Policy Manager (select **Setup > Authentication > Authentication Servers**).
4. From the **Primary** drop-down list, select the Firebox IP address that Mobile VPN with SSL users will connect to. This list is populated with all public IP addresses on the Firebox.
5. If your Firebox has more than one WAN connection, select a different public IP address from the **Backup** drop-down list. The Mobile VPN with SSL client will connect to the backup IP address when it is unable to establish a connection with the primary IP address.

6. Direct the flow of Internet traffic on the client computer using the **Allowed Resources** area.
 - Select **Force all client traffic through tunnel** to send all private network and Internet traffic through the tunnel. If you choose this option, more processing power and bandwidth on the Firebox is used, but the configuration is more secure. All other resources, defined below, allow Internet traffic between the Mobile VPN client and the Internet to use the ISP of the client.
 - Select **Allow access to networks connected through Trusted, Optional and VLANs** to give the client access to all network resources connected to the Firebox.
 - Select **Specify allowed resources** to restrict access to specific subnets and IP addresses, Type the IP address of a resource in slash notation and click **Add**.
7. By default the **Enter a subnet to be used as a virtual address pool** field has a subnet that matches the maximum number of licensed Mobile VPN with SSL clients and is not in use by any network connected to your Firebox. Keep this subnet or enter your own. IP addresses from the subnet are assigned to Mobile VPN with SSL connections.
8. Click **OK**. [Save the configuration file](#).

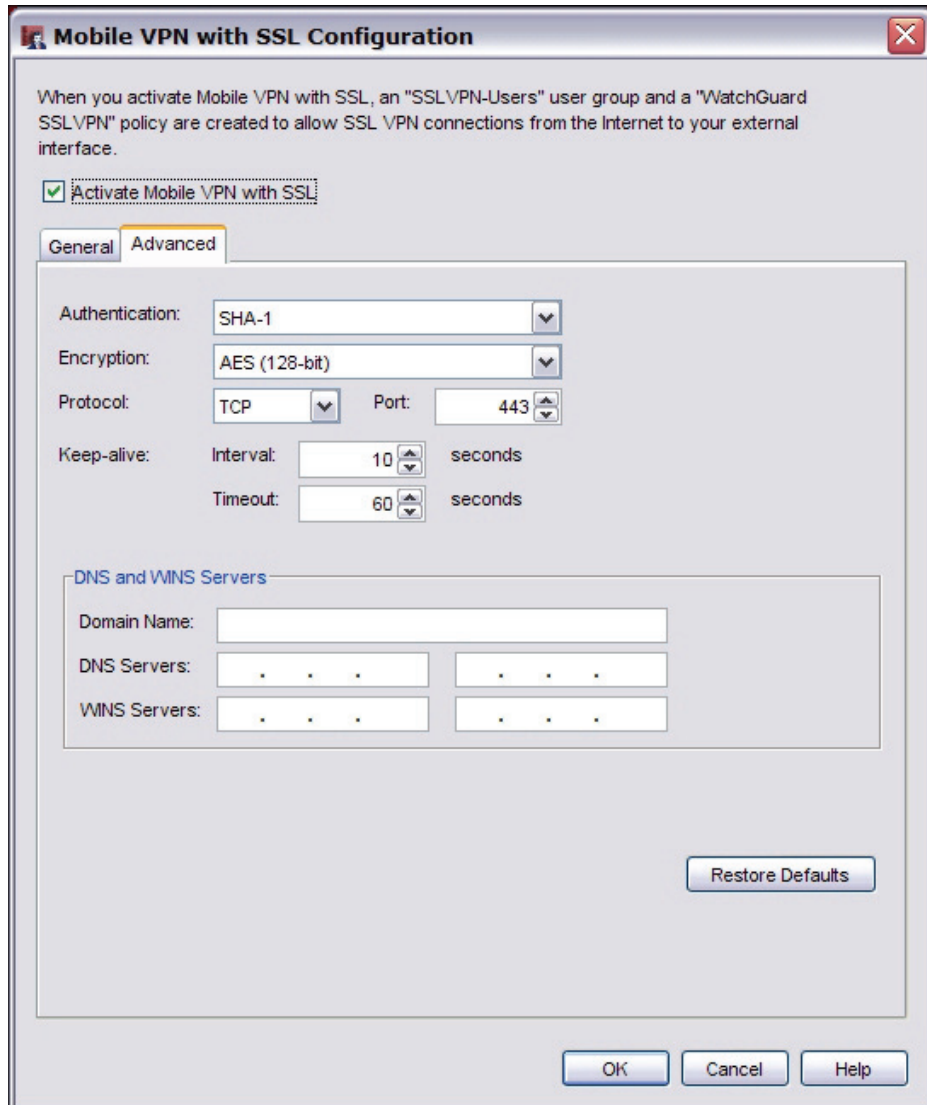
After the changes have been saved to the Firebox, you must [Add remote users to authentication groups](#) before they can download and install the software. Any future changes made to the settings will automatically be given to clients the next time they connect using Mobile VPN with SSL.

Define advanced settings for Mobile VPN with SSL

Mobile VPN with SSL operates correctly with the default **Advanced** settings. If necessary, you can edit the settings to meet your security needs and to work with the network behind the Firebox.

1. From Policy Manager, select **VPN > Mobile VPN > SSL**.

The Mobile VPN with SSL Configuration dialog box appears.



Mobile VPN with SSL Configuration

When you activate Mobile VPN with SSL, an "SSLVPN-Users" user group and a "WatchGuard SSLVPN" policy are created to allow SSL VPN connections from the Internet to your external interface.

☒ **Activate Mobile VPN with SSL**

General **Advanced**

Authentication: SHA-1

Encryption: AES (128-bit)

Protocol: TCP Port: 443

Keep-alive: Interval: 10 seconds
Timeout: 60 seconds

DNS and WINS Servers

Domain Name:

DNS Servers:

WINS Servers:

Restore Defaults

OK Cancel Help

2. Click the **Advanced** tab.
The fields on this tab are described below.

Authentication

This is the authentication method used to establish the connection. The options are **MD5**, **SHA**, or **SHA-1**.

Encryption

This is the algorithm that is used to encrypt the traffic. The options are **Blowfish**, **DES**, **3DES**, or **AES (128 bit)**, **AES (192 bit)**, or **AES (256 bit)**. The algorithms are shown in order from weakest to strongest, with the exception of Blowfish, which uses a 128 bit key for strong encryption.



For best performance with a high level of encryption, we recommend that you choose MD authentication with Blowfish encryption.

Protocol and Port

The default protocol and port for Mobile VPN with SSL are TCP 443. This is the standard protocol and port for HTTPS traffic. If the Firebox has a policy for TCP 443 you cannot use this port and protocol for Mobile VPN with SSL. For example, you cannot use TCP 443 for Mobile VPN if the Firebox has a web server behind it that uses HTTPS or an Exchange server with OWA and you use static NAT. You must change the port and protocol that SSL VPN uses or use a secondary external IP address in your HTTPS policy.

Use these guidelines to choose a different port and protocol:

- UDP is better than TCP.
- Use a standard protocol and port. Many hotels and wireless access points restrict outgoing traffic. TCP 443, TCP 80, TCP 53 and UDP 53 are usually allowed.



With any port and protocol selected, the traffic is always be SSL encrypted.

Keep-alive

The **Keep Alive** interval controls how often the Firebox 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.

The timeout setting defines how long the Firebox waits for a response. If there is no response before the timeout value, the tunnel is dropped and the client must reconnect.

DNS and WINS Servers Field

If you want the Mobile VPN with SSL clients to use a domain DNS or WINS server behind the Firebox instead of the servers configured on their computer, type the Domain Name and IP addresses of the DNS and WINS server.

Restore Defaults Button

Click the **Restore Defaults** button to reset the **Advanced** tab settings to their default values. All DNS and WINS server information on the **Advanced** tab is deleted.

Add remote users to authentication groups

After you [Configure the Firebox for Mobile VPN with SSL](#), a group named SSLVPN-Users is automatically created. To allow users access to your local network through a Mobile VPN with SSL tunnel, you must add them to the SSLVPN-Users group, whether you are using the Firebox or a third party as an authentication server.

If you use the Firebox as an authentication server

Use the procedure described in [Define a new user for Firebox authentication](#) to add remote users to the SSLVPN-Users group.

If you use a third-party authentication server

On any third-party authentication server, the user must be a member of a group named SSLVPN-Users. Use the instructions provided in that vendor's documentation to add users to the SSLVPN-Users group.

Distribute the client software

After you enable Mobile VPN with SSL for a user or group, your users can download the Mobile VPN client software from your Firebox. To get the software, users must connect to the Firebox with a web browser.

Each user must type:

`https://IP address of a Firebox interface:4100/sslvpn.html`

or

`https://Host name of the Firebox:4100/sslvpn.html`

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](#).

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/sslvpn.html`

or

`https://Host name of the Firebox:4100/sslvpn.html`

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.

Install the 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.

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

After you have installed the Mobile VPN with SSL client, you can connect to your Firebox.

Windows Vista and Windows XP




1. Use one of these three methods to start the client software:
 - o Select **Start > All Programs > WatchGuard > Mobile VPN with SSL client > Mobile VPN with SSL client**.
 - o Double-click the Mobile VPN with SSL client icon on the desktop.
 - o 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**.

Mac OS X

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.

26 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.


To install WebBlocker, you must have a WebBlocker license key and register it on the LiveSecurity web site. After you register the license key, LiveSecurity gives you a new feature key. For information on working with feature keys, see [About feature keys](#).

Get started with WebBlocker

Use this procedure to start WebBlocker on your Firebox., Before you begin:

- Make sure you have installed the WebBlocker Server software on your management station. You usually do this when you select to install server components during the initial setup for WatchGuard System Manager. If you did not do this, rerun the setup procedure as described in [Set up the management station](#), but select only the WebBlocker Server component. (Operating systems that are supported for the WebBlocker Server are Windows 2000, Windows 2003, and Windows XP.)
- [Get a feature key](#) for WebBlocker, and then [import the feature key to the Firebox](#).

Download the WebBlocker database

1. Right-click  in the system tray at the bottom of the screen. (The WebBlocker Server icon is the one on the far right.)
2. Select **Get Full Database**.

The Download WebBlocker Database dialog box appears.



3. If you want to use a folder other than the default **C:\Documents and Settings\WatchGuard\wbserver\db** as the destination folder for the database, click **Browse** and select a new folder.
You cannot save the WebBlocker database to a root directory, such as c:\.
4. Select **Download** to download the new database.



The WebBlocker database has more than 220 MB of data. Your connection speed sets the download speed, and the download can be more than 30 minutes. Make sure the hard disk drive has a minimum of 250 MB of free space.

You can use this procedure to download a new version of the database at any time. We recommend you use Windows Task Scheduler to set up regular, automatic database downloads. For more information, see [Keep the WebBlocker database updated](#).

Run the Activate WebBlocker Wizard

1. If you have not done so already, [open Policy Manager](#).
2. Select **Tasks > WebBlocker > Activate**.
The Activate WebBlocker Wizard starts.
3. Click **Next**.
4. Click through the wizard and add the information it asks for. The wizard has three screens, as described below.

Select policies for WebBlocker

This screen does not appear if you have not yet defined any HTTP or HTTPS proxy policies. In this case, the wizard will create a default HTTP proxy policy for you.

If HTTP or HTTPS proxy policies are already created on your Firebox, this screen shows them in a list. From the list, select the proxy policies you want to enable WebBlocker for. If you do not select any policies, a new HTTP proxy policy is created with a WebBlocker action.

Identify the WebBlocker Servers

You must configure a minimum of one WebBlocker Server. To add a WebBlocker Server, click **Add**. Next to **Server IP**, type the IP address of the WebBlocker Server. If necessary, change the port number.

You can add more than one WebBlocker Server so the Firebox can fail over to a backup server if it cannot connect to the primary server.

The first server in the list is the primary server. To move a server higher in the list, select it and click **Move Up**. To move it lower, select it and click **Move Down**.

To add a WebBlocker Server after you complete the wizard, go to **Setup > Actions > WebBlocker**. Click **Add**, and click the **Servers** tab.

Select categories to block

Select the check box adjacent to the categories of web sites you want to block. Only the **Other** category is enabled by default. For more information on WebBlocker categories, see [About WebBlocker categories](#).

To read a description of the category, click on it. The description appears in the box at the bottom of the screen.

If you want to block access to web sites that match any category, select **Deny All Categories**.

To stop users from going to anonymizer web sites to try to avoid WebBlocker, select to block the **Proxies & Translators** category.


Use exception rules to restrict web site access

You can also choose to not use the categories at all and instead use exception rules only to restrict web site access. To do this, do not select any categories. Make sure you select the **Deny website access** radio button, as described in the [About allowing sites to bypass WebBlocker](#).

Keep the WebBlocker database updated

You can update the WebBlocker database at any time. Use the download procedure you used when you first started WebBlocker, as described in [Get started with WebBlocker](#).

Get an incremental update

To get an incremental update of the WebBlocker database, you must first stop the WebBlocker Server service. To stop the service, right-click  in the system tray at the bottom of the screen and select **Stop Service**. Then, right-click again and select **Get Incremental Update**.


Automate WebBlocker database downloads

The best procedure to keep your WebBlocker database updated is to use Windows Task Scheduler. You can use Windows Task Scheduler to schedule the updatedb.bat process, which is created automatically for you in your WSM10/bin directory.

1. Open **Scheduled Tasks**. To open the Task Scheduler using Windows XP, click **Start**, click **All Programs**, point to **Accessories**, point to **System Tools**, and then click **Scheduled Tasks**.
2. Click **Add Scheduled Task**.
3. The Scheduled Tasks wizard starts. Click **Next**.
4. The screen shows a list of programs. Click **Browse**.
5. Go to C:\Program Files\WatchGuard\wsm10.0\bin. Select **updatedb.bat**.

6. Select the time interval at which to do this task. We recommend that you update your database each day. You can update less frequently if you have low bandwidth. Click **Next**.
7. Type the time and frequency to start the procedure. Because you must stop the WebBlocker Server to do the update, we recommend that you schedule updates outside your usual hours of operation.
8. Select a start date. Click **Next**.
9. Type the user name and the password to use this procedure. Make sure that this user has access to the necessary files. Click **Next**.
10. Click **Finish**.

See database status

Right-click  in the system tray at the bottom of the screen and select **Show Database Status**.

About WebBlocker categories

The WebBlocker database contains nine category groups, with 54 website categories.

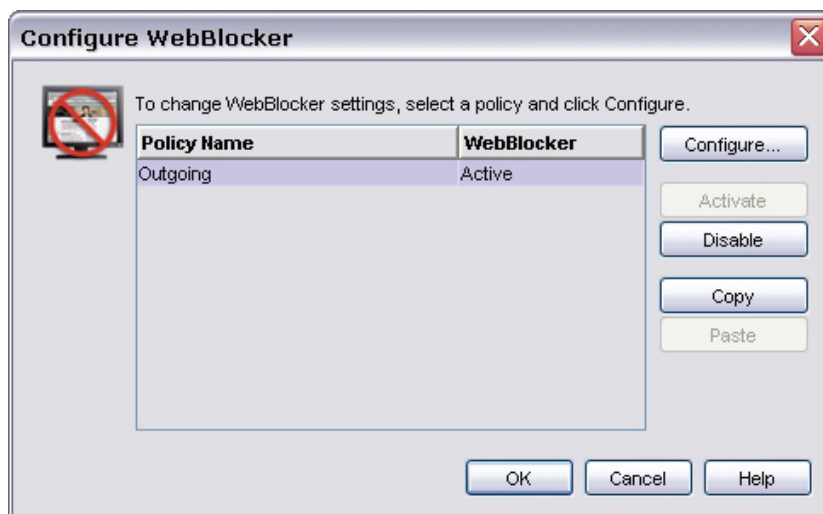
A web site is added to a category when the contents of the web site meet the correct criteria. Web sites that give opinions or educational material about the subject matter of the category are not included. For example, the **Illegal Drugs** category denies sites that tell how to use marijuana. They 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 Firefox X Edge software update. The **Uncategorized** category includes sites that do not meet the criteria for any other category.

Configure WebBlocker

After you use the Activate WebBlocker Wizard to activate WebBlocker and create a basic configuration, you can configure more WebBlocker settings.

1. From Policy Manager, select **Tasks > WebBlocker > Configure**.
The Configure WebBlocker dialog box appears and shows any HTTP or HTTPS policies that were already created.



2. Select the policy you want to configure and click **Configure**.
The WebBlocker Configuration dialog box for that policy appears.



The **WebBlocker Configuration** dialog box includes tabs to you can use to:

- [Add new servers or change their order](#)
- [Change categories to block](#)
- [Add exceptions](#)
- [Define advanced WebBlocker options](#)
- [Define WebBlocker alarms](#)

Add new servers or change their order

You can add up to five WebBlocker Servers. If the Firebox cannot connect to the first server in the list, it tries to connect to the next one in the list. The first server in the list is the primary server.

Add a server

1. On the **Servers** tab of the **WebBlocker Configuration** dialog box, click **Add**.
The *Add WebBlocker Server* dialog box appears.
2. Next to **Server IP**, type the IP address of the WebBlocker Server. If necessary, change the port number. Click **OK**.

Change order of servers

1. You can change the order of the servers to define the order in which the Firebox fails over to backup servers. To move a server higher in the list, select it and click **Move Up**. To move it lower, select it and click **Move Down**.
2. Click **OK**.

For information on server timeout settings, see [Define advanced WebBlocker options](#).

Change categories to block

When you used the Activate WebBlocker wizard, you selected categories of web sites you want to block. Click the **Categories** tab on the **WebBlocker Configuration** dialog box to make changes to your original configuration.

This dialog box is very similar to the wizard screen described in [Get started with WebBlocker](#). The main difference is that the categories are grouped under headings. For example, the Shopping heading includes Advertisements, Food & Drink, Motor Vehicles, Real Estate, and Shopping. If you want to select all the sites under the Shopping heading, you can select the check box next to Shopping. All the sites under it are automatically selected. If you want to select only one or a few categories under Shopping but not all of them, clear the **Shopping** check box and select only the categories you want to restrict.

For information on WebBlocker categories, see [About WebBlocker categories](#).

Send an alarm when a site is denied

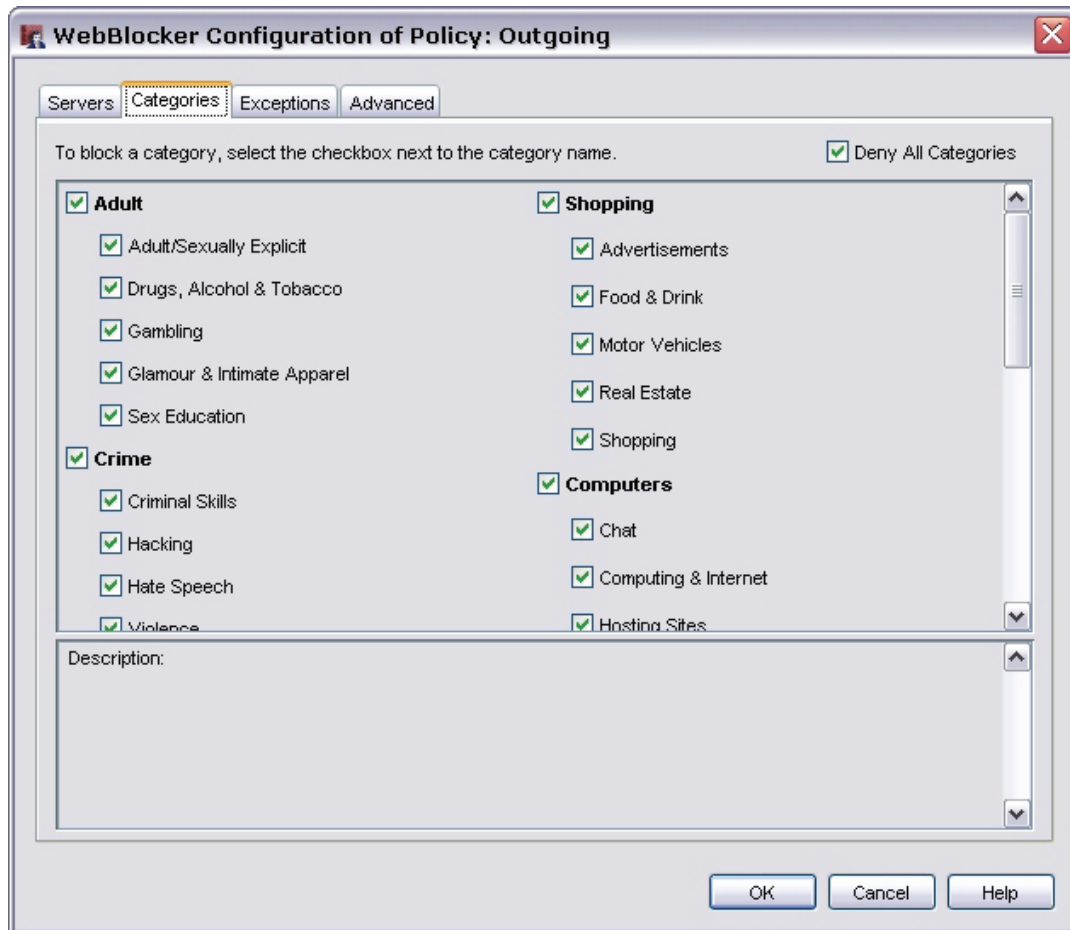
You can define WebBlocker to send an alarm if a user tries to go to a site and is denied. In the **Actions to Take** section at the bottom of the dialog box, select **Alarm if denied**.

To set parameters for the alarms, click the **Alarm** tab.

For information on the fields in this dialog box, see [Set logging and notification preferences](#).

Log WebBlocker actions

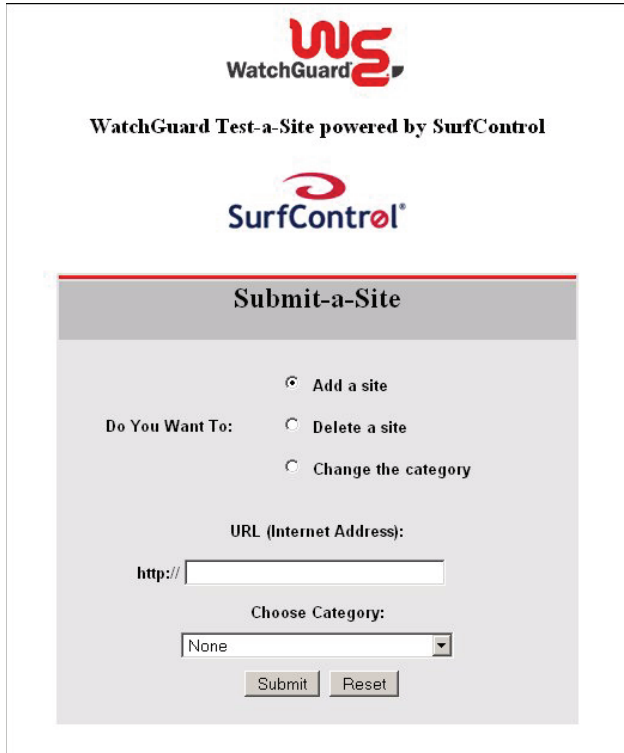
You can define WebBlocker to send a message to the log if a user tries to go to a site and is denied. In the **Actions to Take** section at the bottom of the dialog box, select **Log this action**.



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.



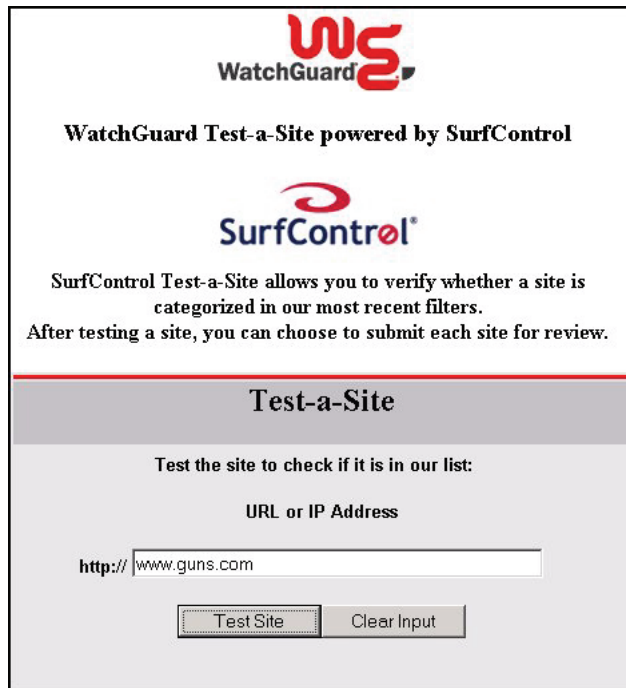
The screenshot shows a web page titled "WatchGuard Test-a-Site powered by SurfControl". At the top is the WatchGuard logo, followed by the text "WatchGuard Test-a-Site powered by SurfControl" and the SurfControl logo. Below this is a form titled "Submit-a-Site". The form has a section "Do You Want To:" with three radio button options: "Add a site" (which is selected), "Delete a site", and "Change the category". Below this is a text input field labeled "URL (Internet Address):" with the text "http://" followed by a white input box. Below the URL field is a dropdown menu labeled "Choose Category:" with "None" selected. At the bottom of the form are two buttons: "Submit" and "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**.

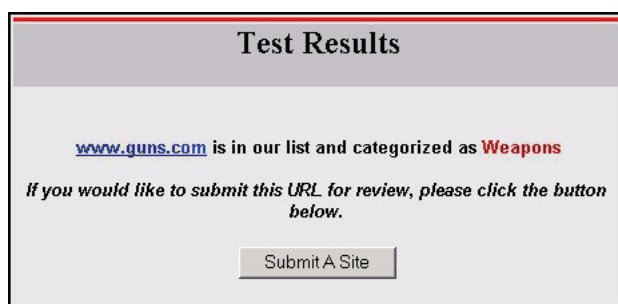
See whether a site is categorized

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.



Define advanced WebBlocker options

To configure advanced WebBlocker options, click the **Advanced** tab.

The screenshot shows the 'Edit WebBlocker Configuration' dialog box with the 'Advanced' tab selected. The dialog has a title bar with a close button. Below the title bar, there are fields for 'Name' (set to 'newWebBlocker.1') and 'Description' (set to 'Default configuration for WebBlocker'). Below these fields are five tabs: 'Servers', 'Categories', 'Exceptions', 'Advanced' (selected), and 'Alarm'. The 'Advanced' tab contains two main sections: 'Cache size' and 'Server timeout'. The 'Cache size' section has a text box with '100' and 'entries' next to it. The 'Server timeout' section has a text box with '5' and 'seconds' next to it. Below the 'Server timeout' section, there are two sets of radio buttons and checkboxes. The first set has 'Allow the user to view the website' selected. The second set has 'Deny access to the website' selected. There are also checkboxes for 'Alarm' and 'Log this action' in both sets. At the bottom right of the dialog, there are buttons for 'OK', 'Cancel', 'Help', and 'Restore Defaults'.

Cache size

Change this setting to improve WebBlocker performance.

Cache Size

Use the arrows to change the number of entries in the cache or type in a number.

Server timeout

If your Firebox cannot connect to the WebBlocker server in

Set the number of seconds to try to connect to the server before the Firebox times out.

Alarm

Select to send an alarm when the Firebox cannot connect to the WebBlocker Server and times out. To set parameters for the alarms, click the **Alarm** tab. For information on the **Alarm** tab fields, see [Set logging and notification preferences](#).

Log this action

Select to send a message to the log if the Firebox times out.

Allow the user to view the website

Select if you want to allow the user to see the web site if the Firebox times out and does not connect to the WebBlocker Server.

Deny access to the website

Select to deny access if the Firebox times out.

Alarm

Select to send an alarm when the Firebox times out and access to a site is denied. To set parameters for the alarms, click the **Alarm** tab. For information on the **Alarm** tab fields, see [Set logging and notification preferences](#).

Log this action

Select to send a message to the log if the Firebox times out and access to a site is denied.

The Firebox attempts to reach the WebBlocker Server even when it is unavailable. If you allow web traffic when the server is unavailable, each user who sends a web request must wait the amount of time in the above field to try to connect to the WebBlocker Server and time out. After this number of seconds, the Firebox allows access to the web site. When the Firebox can connect to the WebBlocker Server again, it will start to apply WebBlocker rules again.

To add or delete servers, or to change their order of priority, see [Add new servers or change their order](#).

Define WebBlocker alarms

To configure notification parameters for WebBlocker alarms, click the **Alarm** tab.

You can send an alarm when the Firebox cannot connect to the WebBlocker Server and times out, or when the Firebox times out and access to a site is denied. For information on the **Alarm** tab fields, see [Set logging and notification preferences](#).

To change server timeout settings, see [Define advanced WebBlocker options](#).

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 exceptions](#).

Define the action for sites that do not match exceptions

In the **Use category list** section below the list of exception rules, you can configure the action to occur if the URL does not match the exceptions you configure. The default setting is that the **Use the WebBlocker category list to determine accessibility** radio button is selected, and WebBlocker compares sites against the categories you selected on the **Categories** tab to determine accessibility.

You can also choose to not use the categories at all and instead use exception rules only to restrict web site access. To do this, click the **Deny website access** radio button.

Alarm

Select to send an alarm when the Firebox denies a WebBlocker exception. To set parameters for the alarms, click the **Alarm** tab. For information on the **Alarm** tab fields, see [Set logging and notification preferences](#).

Log this action

Select to send a message to the log when the Firebox denies a WebBlocker exception.

Components of exception rules

Exception rules are based on IP addresses or a pattern based on IP addresses. You can have the Firebox block a URL with an exact match. Usually, it is more convenient to have the Firebox look for URL patterns. The URL patterns do not include the leading "http://". To match a URL path on all web sites, the pattern must have a trailing /*.

The host in the URL can be the host name specified in the HTTP request, or the IP address of the server.

Network addresses are not supported at this time, though you can use subnets in a pattern (for example, 10.0.0.*).

For servers on port 80, do not include the port. For servers on ports other than 80, add :port, for example: 10.0.0.1:8080. You can also use a wildcard for the port—for example, 10.0.0.1:*—but this does not apply to port 80.

Exceptions with part of a URL

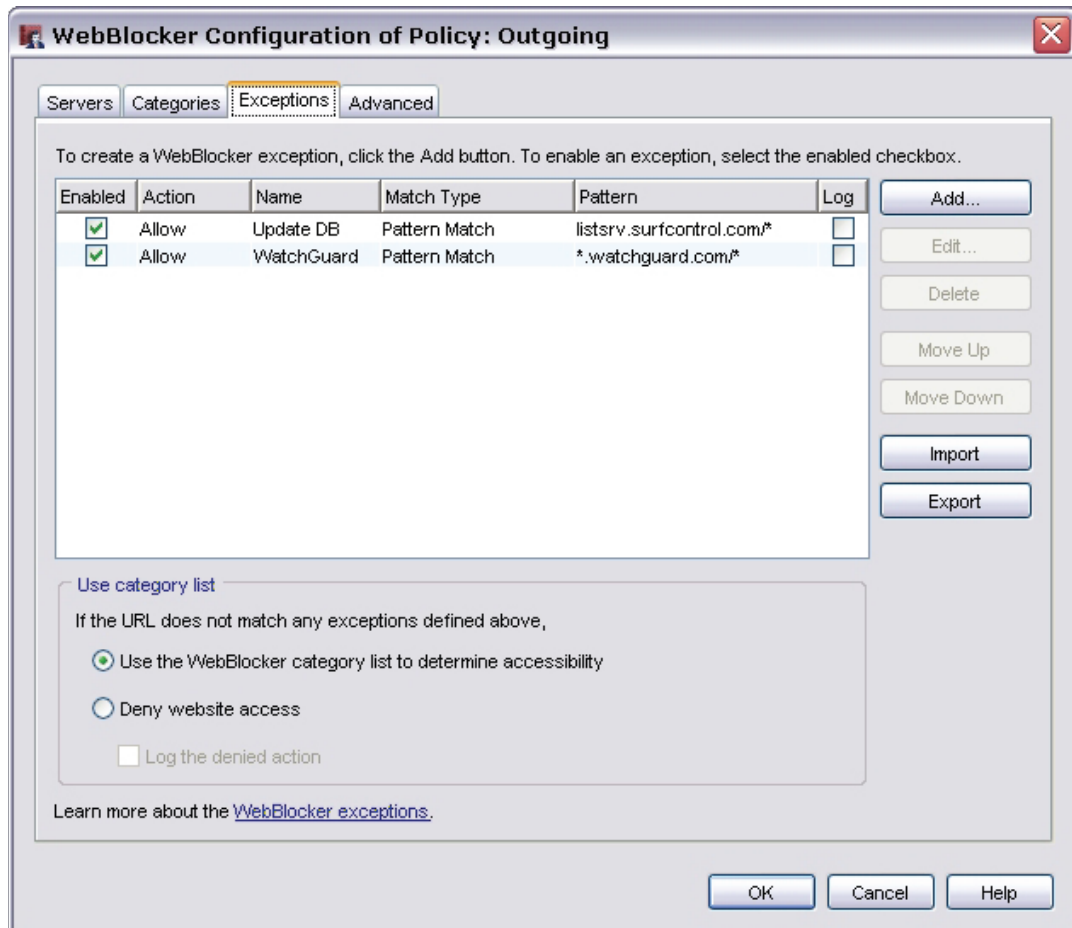
You can create WebBlocker exceptions with the use of any part of a URL. You can set a port number, path name, or string that must be blocked for a special web site. For example, if it is necessary to block only www.sharedspace.com/~dave because it has inappropriate photographs, you type www.sharedspace.com/~dave/*. This gives the users the ability to browse to www.sharedspace.com/~julia, which could contain content you want your users to see.

To block URLs that contain the word sex in the path, you can type `*/sex*`. To block URLs that contain sex in the path or the host name, type `*sex*`.

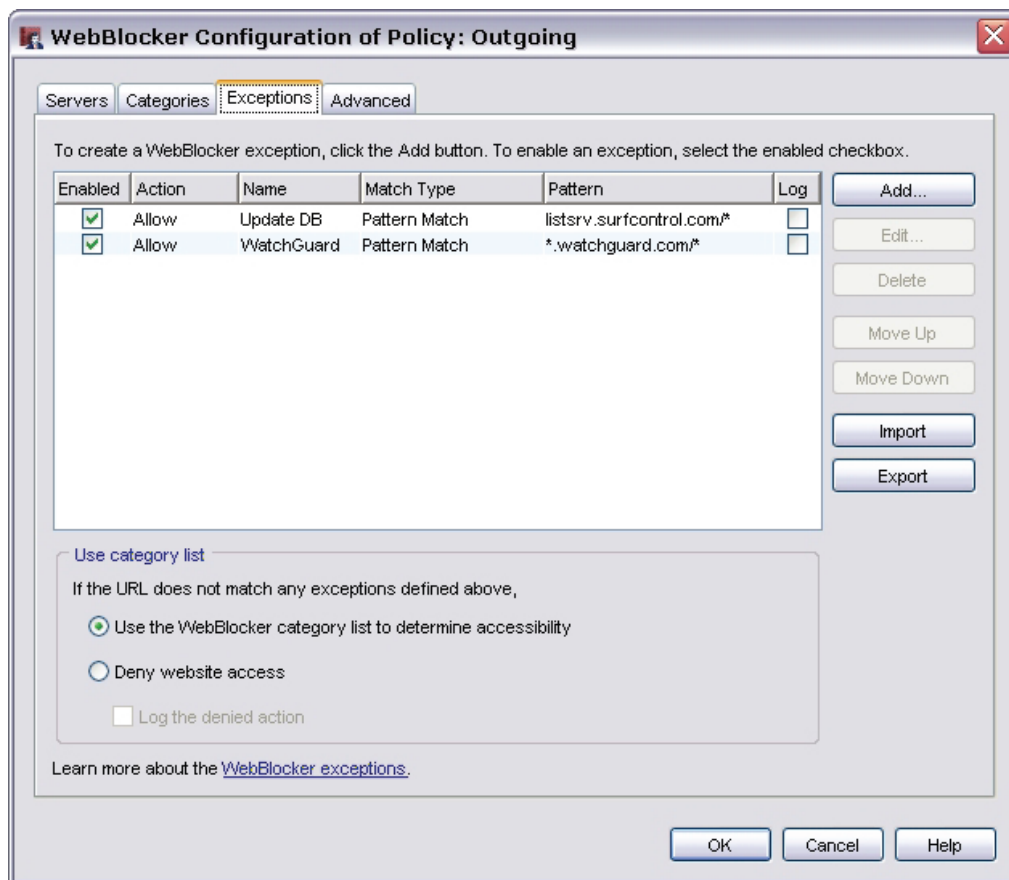
You can block ports in an URL. For example, look at the URL `http://www.hackerz.com/warez/index.html:8080`. This URL has the browser use the HTTP protocol on TCP port 8080 instead of the default method that uses TCP 80. You can block the port by matching `*8080`.

Add exceptions

1. To create exceptions to the WebBlocker categories, click the **Exceptions** tab.



- Click **Add** to add a new exception rule.
The New WebBlocker Exception dialog box appears.



- In the **Match Type** field, select one of these options:

Pattern match

Pattern matches match a pattern in the URL or address, for example pattern in www.pattern.com. Be sure to drop the leading http:// and include /* at the end. Use the wildcard symbol, *, to match any character. You can use more than one wildcard in one pattern. For example, the pattern www.somesite.com/* will match all URL paths on the www.somesite.com web site. To enter a network address, use a pattern match that ends in a wildcard. For example, to match all the web sites at 1.1.1.1 on port 8080, set the directory to *.

Exact match

Exact matches match an exact URL or IP address, character by character. You cannot use wildcards, and you must type each character exactly as you want it to be matched. For example, if you enter an exception to allow www.yahoo.com as an exact match only, and a user types www.yahoo.com/news, the request is denied.

Regular expression

Regular expression matches use a Perl-compatible regular expression to make a match. For example, \.[onc][eor][gtm] matches .org, .net, .com, or any other three-letter combination of one letter from each bracket, in order. Be sure to drop the leading http:// Supports wild cards used in shell script. For example, the expression (www)?\.watchguard\.[com|org|net] will match URL paths including www.watchguard.com, www.watchguard.net, and www.watchguard.org. The expression 1.1.1.[1-9] will match all IP addresses from 1.1.1.1 to 1.1.1.9. For help on how to use regular expressions, see [About regular expressions](#).

4. In the **Type** field, enter the web site type: **URL** or **Host IP Address**.
5. If you chose **URL** in the previous field, enter the pattern, value, or expression, depending on the value in the **Match Type** field.
If you chose **Host IP Address** in the previous field, enter the address, port, and directory to be matched.
6. Click **OK** to close the **New WebBlocker Expression** dialog box.
7. Click the **Action** column to get access to the **Action** drop-down list. Select to have WebBlocker allow or deny the exception.
8. Type a name for the exception in the **Name** text box. The default name is `WB Rule [number]`.

You can use any of these options for WebBlocker exceptions:

- You can use the drop-down lists for the **Match Type** and **Pattern** fields if you want to change the settings you made in the **New WebBlocker Exception** dialog box.
- Click the **Log** check box if you want a log message when an action is taken on a WebBlocker exception.
- To disable a exception but keep it in your configuration for possible use at a later time, clear the **Enabled** check box.
- In the **Use category list** section below the list of exception rules, you can configure the action to occur if the URL does not match the exceptions you configure. The default setting is that the **Use the WebBlocker category list to determine accessibility** radio button is selected, and WebBlocker compares sites against the categories you selected on the **Categories** tab to determine accessibility.
- You can also choose to not use the categories at all and instead use exception rules only to restrict web site access. To do this, click the **Deny website access** radio button.

Change the order of exception rules

The order that the exception rules are listed in the dialog box shows the order in which sites are compared to the rules. WebBlocker compares messages to the first rule in the list and continues in sequence from top to bottom. When a messages matches a rule, WebBlocker performs the related action. It performs no other actions, even if a site 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.

Import or export WebBlocker exception rules

If you manage several Fireboxes or use WebBlocker with more than one proxy definition, you can import and export exception rules between them. This saves time because you must define the rules only once.

You can transfer exception rules between proxies or Fireboxes in two ways. You can write an ASCII file that defines the rules and import it to other Fireboxes or proxies. Or, you can use the WebBlocker user interface to define the exception rules, export the file to an ASCII file, and import that file into another Firebox configuration file or proxy definition.

Write rulesets in an ASCII file

You can write rules in a normal ASCII file that uses the standard UTF-8 character set.

You must include only one rule per line. The syntax for rules is:

*[rule_name, action, **enabled|disabled**, **log|no log**, match_type,] pattern_value*

where:

rule_name is the name of the rule as it appears in the exception list. The default is **WB Rule n**.

action = **Allow** or **Deny**. The default action is **Allow**.

enabled|disabled = Whether the rule is currently enabled or disabled. The default is **enabled**.

log|no log = Specifies whether you want a log message when the action is taken. The default is **no log**.

match_type = Specifies the type of match: exact match, regular expression or pattern match. The default is **pattern match**.

value = value to be matched.

The fields enclosed in brackets are optional. If you omit them, the default values are used.

To add comments to a file, precede the comment with a number sign (#). Make sure the comment is on its own line.

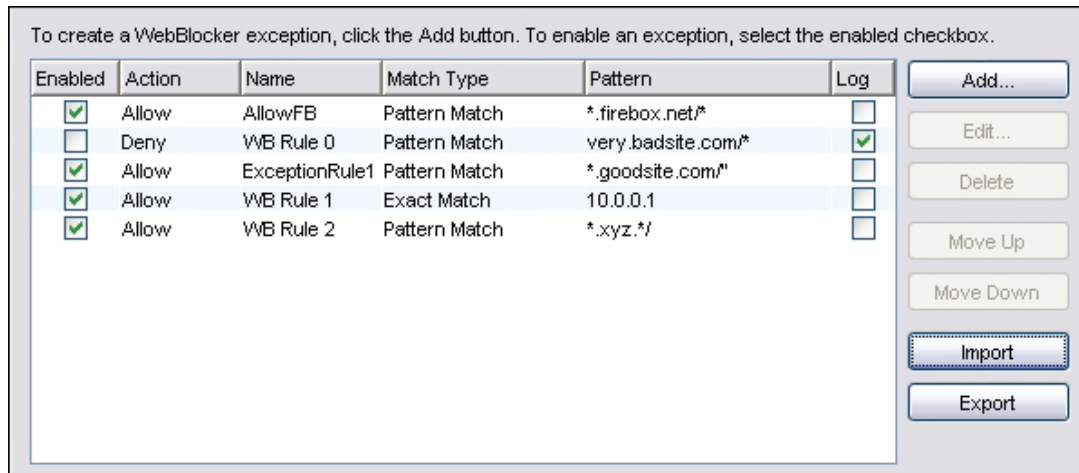
Below is an example exceptions file.

```
#
# Here are five exception rules
#
AllowFB, allow, enabled, No Log, *.firebox.net/*
deny, disabled, Log, very.badsite.com/*
ExceptionRule1, *.goodsite.com/"
exact match, 10.0.0.1
*.xyz.*/*
```

The next section, Import an ASCII exceptions file, shows how the above file would look if imported into WebBlocker.

Import an ASCII exceptions file

1. From the **Exceptions** tab of the **WebBlocker Configuration** dialog box, click **Import**.
2. Find the ASCII file and click **Open**.
3. If exceptions are already defined in WebBlocker, you are asked whether you want to replace the existing rules or append the imported rules to the list of existing rules. Click **Replace** or **Append**. If you click **Append**, the imported rules appear in the **Exceptions** block beneath any existing rules. If you want to change the order of the exception rules, see [Change the order of exception rules](#). If the example file in the previous section is imported into WebBlocker, it appears like this.



Export rules to an ASCII file

When you export exception rules from a proxy definition, the Firebox saves the current rules to an ASCII text file in the format described for spamBlocker in [Import and export exception rules](#).

1. From the **Exceptions** tab of the **WebBlocker Configuration** dialog box, define exceptions as described in [Add exceptions](#).
2. Click **Export**.
3. In the **Open** dialog box, select where you want to save the exceptions file and click **Save**. You can now open another HTTP proxy definition in the same or in a different Firebox configuration file and import the exceptions file.

Use WebBlocker actions in proxy definitions

The basic configuration you created with **Tasks > WebBlocker > Configure** is a WebBlocker action—a set of WebBlocker settings—that you can apply to an HTTP or HTTPS proxy definition. You can define additional WebBlocker actions if you want to apply different settings to different proxies.

Define additional WebBlocker actions

1. From Policy Manager, select **Setup > Actions > WebBlocker**.
The WebBlocker Configurations dialog box appears.



2. Click **Add**. Or if you want to define a new action based on an existing one, select that action and click **Clone**.
3. Configure the WebBlocker action as described in [Configure WebBlocker](#).

Add WebBlocker actions to a policy

1. Double-click the HTTP policy icon to open the **Edit Policy Properties** dialog box.
2. Select the **Properties** tab.
3. Click the **View/Edit Proxy** icon.
The HTTP Proxy Action Configuration dialog box appears.
4. From the **WebBlocker** drop-down list, select the WebBlocker action you want to apply.

Schedule WebBlocker actions

You can set an operating schedule for the policy. You can use the predefined settings in the drop-down list or create custom schedules. You use these time periods to set rules for when to block different web sites. For example, you can block sports web sites during usual business hours of operation, but allow users to browse at lunch time, evenings, and weekends.

To set a schedule for a policy:

1. Open the policy to edit it, and click the **Advanced** tab.
2. Select a schedule from the drop-down list, or click the New/Clone icon to make a new schedule.
For more information, see [Create schedules for Firebox actions](#).
3. Configure an HTTP policy that uses the schedule.

You can also configure two HTTP or HTTPS policies, but create a schedule for only one of them. Each policy uses one of the proxy actions. Each of these proxy actions points to one of at least two WebBlocker actions.

Renew security subscriptions

The WatchGuard security subscriptions (Gateway AntiVirus, Intrusion Prevention Service, WebBlocker, and spamBlocker) need regular updates to operate effectively.

The Firebox gives reminders to renew your subscriptions. When you save changes to a configuration file, WatchGuard System Manager tells you if a subscription will expire 60 days before, 30 days before, 15 days before, and the day before the expiration date.

When your subscriptions expire, you cannot save any changes to your configuration until you either renew or disable the expired subscription.



*If your site uses WebBlocker, you must renew or disable the WebBlocker subscription as soon as it expires to prevent an interruption in web browsing. WebBlocker has a default setting that blocks all traffic when the connections to the server time out. When your WebBlocker expires, it no longer contacts the server. This appears to the Firebox as a server timeout. All HTTP traffic is blocked unless this default was changed before expiration. To change this setting, go to the **Advanced** tab of the **WebBlocker Configuration** dialog box and select the **Allow the user to view the website** option.*

1. From Policy Manager, click **File > Save > To Firebox**.
You see a message that tells you to update your feature key.
2. Click **OK**.
The Feature Key Compliance dialog box appears.



3. Select the expired subscription.
4. If you already have the new feature key, click Add Feature Key. Paste in your new feature key. You cannot right-click to paste. You must use CTRL-V or click **Paste**.
If you do not already have your new feature key, you must click **Disable** even if you plan to renew later. You do not lose your settings if you disable the subscription. If you renew your subscription at a later time, you can reactivate the settings and save them to the Firebox.
5. Click **OK**.

Renew subscriptions from Firebox System Manager

On the front panel of Firebox System Manager, if a subscription will expire soon, a warning appears and the **Renew Now** button is visible in the upper-right corner of the window. Click it to go to the LiveSecurity Service web site where you can renew the subscription.

27 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 [Enable and set parameters for Virus Outbreak Detection \(VOD\)](#).

You can see statistics on current spamBlocker activity on the Firebox, as described in [spamBlocker statistics](#).

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.
- DNS configured on the Firebox that will apply spamBlocker rules. From Policy Manager, select **Network > Configuration**. Click the **WINS/DNS** tab and type the IP addresses of the DNS servers your Firebox uses to resolve host names.
- Connection to the Internet

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 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.

Drop (SMTP only)

Drop the connection immediately. The Firebox does not give any error messages to the sending server. The **Drop** 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 Spam** 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 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.

Activate spamBlocker

You use a wizard to enable the spamBlocker feature in the SMTP proxy, the POP3 proxy, or both. You can also use this wizard to add a new SMTP proxy or POP3 proxy to your Firebox configuration with spamBlocker enabled.

1. Make sure you have met all requirements for spamBlocker, as described in [spamBlocker requirements](#).
2. Import the feature key for spamBlocker to the Firebox, as described in [import a feature key to the Firebox](#).
3. From WatchGuard System Manager, select the Firebox that will use spamBlocker.
4. Click the Policy Manager icon .
Or select **Tools > Policy Manager**.
5. From Policy Manager, select **Tasks > spamBlocker > Activate**.
The Activate spamBlocker wizard starts.



6. Click through the wizard and add the information it asks for. The wizard has either one or two screens depending on how your Firebox is currently configured.

Apply spamBlocker settings to your policies

This screen appears if you already have one or more SMTP or POP3 policies defined on your Firebox. From the list, select the proxy policies for which you want to enable spamBlocker. The **Select** check box is dimmed for any policies that already have spamBlocker enabled.

Create new proxy policies

This screen appears if your Firebox does not yet have policies created for either SMTP or POP3, or if your Firebox has either SMTP or POP3 but not both. The wizard will create one or both of these policies for you. For either policy, you must have at least one external interface with a static IP address.

- To create a POP3 policy, select the **POP3** check box.
- To create an SMTP policy, select the **Incoming SMTP** check box. Type the email server IP address.
- The SMTP policy created by this wizard contains Any-External for the **From** field and a static NAT entry for the **To** field. The static NAT entry uses the first static external IP address configured on the Firebox. It enables static NAT for the email server IP address you enter in the wizard. If this default static NAT SMTP policy is not the best choice for your organization, you can use Policy Manager to create an SMTP policy before you use the wizard.
For information on how to add a policy to Policy Manager, see [Add a policy from the list of templates](#).

After the wizard is finished, you can click the check box at the bottom of the screen to begin to configure spamBlocker, as described in [Configure spamBlocker](#).

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.

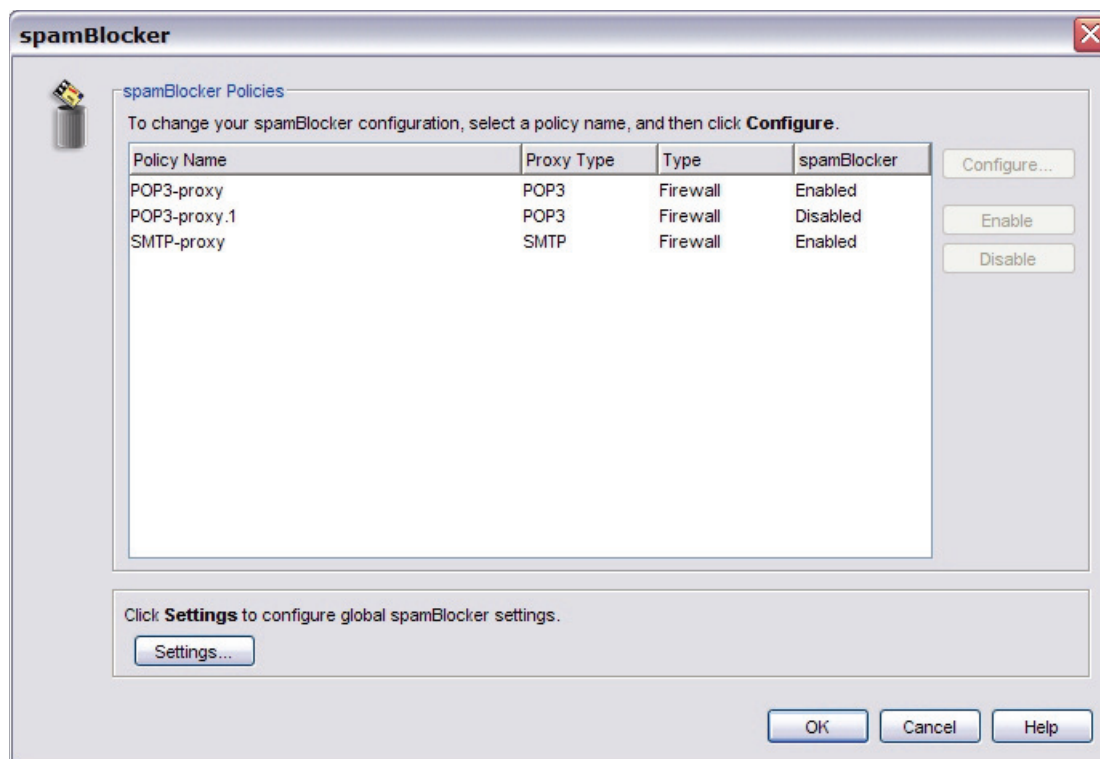
If you want to use more than one proxy service with spamBlocker, your network must use one of these configurations:

- 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.

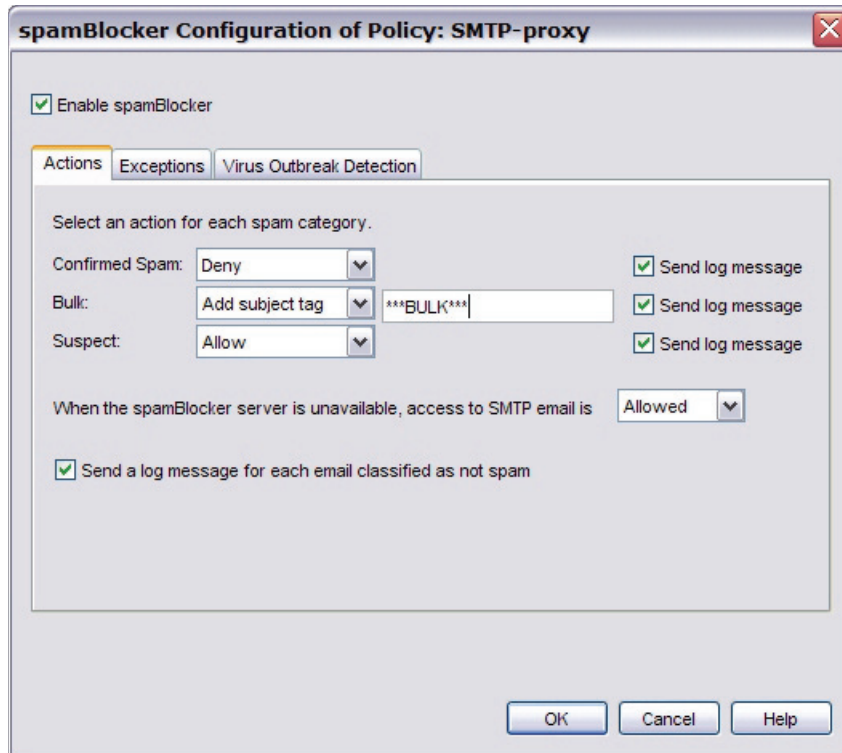
Configure spamBlocker

After you use the Activate spamBlocker Wizard to activate spamBlocker, you can set other configuration parameters.

1. If you did not click the check box in the last screen of the Activate spamBlocker Wizard to configure spamBlocker, you can do this from Policy Manager. Select **Tasks > spamBlocker > Configure**.
The spamBlocker dialog box appears with a list of the SMTP and POP3 proxies on your Firebox and whether spamBlocker is enabled for each one.



2. Select the policy you want to configure and click **Configure**.
The spamBlocker Configuration page for that policy appears.



The image shows a dialog box titled "spamBlocker Configuration of Policy: SMTP-proxy". It has a close button (X) in the top right corner. Inside the dialog, there is a checkbox labeled "Enable spamBlocker" which is checked. Below this are three tabs: "Actions", "Exceptions", and "Virus Outbreak Detection". The "Actions" tab is selected. The main area of the dialog is titled "Select an action for each spam category." and contains three rows of configuration options:

- Confirmed Spam:** A dropdown menu set to "Deny", a "Send log message" checkbox (checked), and a "Send log message" checkbox (checked).
- Bulk:** A dropdown menu set to "Add subject tag", a text box containing "***BULK***", a "Send log message" checkbox (checked), and a "Send log message" checkbox (checked).
- Suspect:** A dropdown menu set to "Allow", a "Send log message" checkbox (checked), and a "Send log message" checkbox (checked).

Below these rows is a section titled "When the spamBlocker server is unavailable, access to SMTP email is" with a dropdown menu set to "Allowed". At the bottom of the dialog is a checkbox labeled "Send a log message for each email classified as not spam" which is checked. At the very bottom are three buttons: "OK", "Cancel", and "Help".

3. Set the actions spamBlocker applies for each category of email in the drop-down lists next to **Confirmed spam**, **Bulk**, and **Suspect**. If you select **Add subject tag** for any category, you change the default tag that appears in the text box to the right of the drop-down list. For more information on spamBlocker tags, see [spamBlocker actions, tags, and categories](#).
4. If you want to send a log message each time spamBlocker takes an action, select the **Send log message** check box for the action. If you do not want to record log messages for an action, clear this check box.
5. The **When the spamBlocker server is unavailable, access to POP3/SMTP email is** dialog box specifies how the Firebox handles incoming email when the spamBlocker server is down. We recommend you use the default **Allowed** action.
If you configure spamBlocker to deny POP3 or 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 Firebox can connect to the spamBlocker server, until the request is dropped because the proxy times out, or until you cancel the request.
If you set this option to **Denied** with the SMTP proxy, the Firebox sends this 450 SMTP message to the sending email server: Mailbox is temporarily unavailable.
6. The **Send log message for each email classified as not spam** check box specifies whether a message is added to the log if an email message is scanned by spamBlocker but is not designated as Confirmed Spam, Bulk, or Suspect. Select this check box if you want to add a message to the log in this situation.
7. (Optional) Add spamBlocker exception rules, as described in [About spamBlocker exceptions](#).

8. Configure Virus Outbreak Detection actions, as described in [Configure Virus Outbreak Detection \(VOD\) actions](#).
9. Click **OK**.



If you have any perimeter firewall between the Firebox that uses spamBlocker and the Internet, it must not block HTTP traffic. The HTTP protocol is used to send requests from the Firebox to the spamBlocker server.

You can define global spamBlocker settings, which apply to spamBlocker regardless of which proxy you use. For more information, see [Set global spamBlocker parameters](#).

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 add an exception rule, see [Add spamBlocker exception rules](#).

To change the order of the rules listed in the dialog box, see [Change the order of exceptions](#).

You can also add exception rules by writing them in an ASCII file and importing them into your Firebox configuration. See [About importing and exporting exception rules](#).

Add spamBlocker exception rules

1. From the **Configure spamBlocker** dialog box, click the **Exceptions** tab.
2. Click **Add**.

The Add Exception Rule dialog box appears.



3. Select a rule action: **Allow**, **Add subject tag**, **Quarantine**, **Deny**, or **Drop**. (Remember that the POP3 proxy supports only the **Allow** and **Add subject tag** actions in spamBlocker.)
4. Type a sender, recipient, or both. You can type the full email name or use wildcards. 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.

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.

Import and export exception rules

If you manage several Fireboxes or use spamBlocker with more than one proxy definition, you can import and export exception rules between them. This saves time because you must define the rules only once.

You can transfer exception rules between proxies or Fireboxes in two ways.

- You can write an ASCII file that defines the rules and import it to other Fireboxes or proxies.
- You can use the spamBlocker user interface to define the exception rules, export the file to an ASCII file, and import that file into another Firebox configuration file or proxy definition.

Write rulesets in an ASCII file

You can write rules in a normal ASCII file that uses the standard UTF-8 character set. You must include only one rule per line. The syntax for rules is:

[action, <tag>,) sender [, recipient]

where:

action = Allow, Add subject tag <tag>, Quarantine, Deny, or Drop. (Quarantine, Deny, and Drop are not supported by the POP3 proxy.) The default action is Allow.

tag = The identifier you want to add to the email messages. The identifier must be enclosed in angle brackets.

sender = Email address (abc@mywatchguard.com) or pattern (*@firebox.net). The default is all senders.

recipient = Email address (abc@mywatchguard.com) or pattern (*@firebox.net). The default is all recipients.

The fields enclosed in brackets are optional. If you omit them, the default values are used.

To add comments to a file, precede the comment with a number sign (#). Make sure the comment is on its own line.

Here is an example of a spamBlocker exception rules file:

```
# allow all email from firebox.net *@firebox.net
# use **SPAM** tag on all email from xyz.com Add subject tag, <**SPAM**>, *@xyz.com
# deny all email from unknown.com to abc@mywatchguard.com Deny, *@unknown.com,
abc@mywatchguard.com
```

Import an ASCII exceptions file

1. From the **Exceptions** block of the **spamBlocker Configuration** dialog box, click **Import**.
2. Find the ASCII file and click **Open**.
3. If exceptions are already defined in spamBlocker, you are asked whether you want to replace the existing rules or append the imported rules to the list of existing rules. Click **Replace** or **Append**. If you click **Append**, the imported rules appear in the **Exceptions** block under any existing rules. If you want to change the order of the exception rules, see [Change the order of exception rules](#).



*If you import a rule with the **Deny** exception into the POP3 proxy, you will get an error message.*

Export rules to an ASCII file

When you export exception rules from a proxy definition, the Firebox saves the current rules to an ASCII text file.

1. From the **Exceptions** block of the **spamBlocker Configuration** dialog box, define exceptions as described in [Add spamBlocker exception rules](#).
2. Click **Export**.
3. In the **Open** dialog box, select where you want to save the exceptions file and click **Save**. You can now open another SMTP or POP3 proxy definition in the same or in a different Firebox configuration file and import the exceptions file.

Log exceptions

Select the **Send log message for each email that matches one of the above exceptions** check box if you want a message written to the log each time an email message matches an exception rule.

Configure Virus Outbreak Detection (VOD) actions

Virus Outbreak Detection (VOD) is a technology that uses traffic analysis technology to identify email virus outbreaks worldwide within minutes and then provides protection against those viruses. Provided by Commtouch, an industry leader in email spam and virus protection, VOD is incorporated into the spamBlocker security subscription.

To configure Virus Outbreak Detection actions:

1. Make sure Virus Outbreak Detection is enabled:
 - On the **spamBlocker Settings** dialog box, select the **Virus Outbreak Detection** tab.
 - Select the **Enable Virus Outbreak Detection (VOD)** check box.
For more information, see [Enable and set parameters for Virus Outbreak Detection \(VOD\)](#).
2. From the **Configure spamBlocker** dialog box, click the **Virus Outbreak Detection** tab.
3. Set the action the Firebox takes if VOD detects a virus in an email message from the **When a virus is detected** drop-down list.
4. Set the action the Firebox takes when VOD cannot scan an email message or attachment from the **When a scan error occurs** drop-down list.
Attachments that cannot be scanned include binhex-encoded messages, certain encrypted files, or files that use a type of compression that we do not support such as password-protected Zip files.

The SMTP proxy supports the **Allow**, **Lock**, **Remove**, **Quarantine**, **Drop**, and **Block** actions. The POP3 proxy supports only the **Allow**, **Lock**, and **Remove** actions.

For more information on these actions, see [spamBlocker actions, tags, and categories](#).

Configure spamBlocker to quarantine email

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 filtered by spamBlocker.

To configure spamBlocker to quarantine email:

1. When you run the Activate spamBlocker Wizard (as described in [Activate spamBlocker](#)), you must make sure you use spamBlocker with the SMTP proxy. The POP3 proxy does not support the Quarantine Server.
2. When you set the actions spamBlocker applies for different categories of email (as described in [Configure spamBlocker](#)), make sure you select the Quarantine action for at least one of the categories. When you select this action, you are prompted to configure the Quarantine Server if you have not already done so.

You can also select the **Quarantine** action for email messages identified by Virus Outbreak Detection as containing viruses. For more information, see [Configure Virus Outbreak Detection \(VOD\) actions](#).

Set global spamBlocker parameters

You can use global spamBlocker settings to optimize spamBlocker for your own installation. Because most of these parameters affect the amount of memory that spamBlocker uses on the Firebox, you must balance good spamBlocker performance with the needs of other Firebox functionality.

1. From the **spamBlocker** dialog box, click **Settings**.
The *spamBlocker Settings* dialog box appears.

2. spamBlocker creates a connection for each message it processes. This connection includes information about the message that is used to generate its spam score. spamBlocker sets a default maximum number of connections that can be simultaneously buffered according to your Firebox appliance model. You can use the **Maximum number of connections** field to increase or decrease this value. If the amount of traffic handled by your proxy policies is low, you can increase the number of supported connections for spamBlocker without affecting performance. If you have memory problems related to your use of proxies on the Firebox, you might want to decrease the value in this field.
3. Use the **Maximum file size to scan** field to set the number of bytes of an email message to be passed to spamBlocker to be scanned. Usually, 20–40K is enough for spamBlocker to correctly detect spam. However, if image-based spam is a problem for your organization, you can increase the maximum file size to block more image-based spam.

4. In the **Cache size** field, enter the number of entries spamBlocker caches locally for messages that have been categorized as spam and bulk. A local cache can improve performance because network traffic to Commtouch is not required. Usually, you do not have to change this value.
You can set the **Cache size** field to 0 to force all email to be sent to Commtouch. This is generally used only for troubleshooting.
5. Clear the **Enabled** check box next to **Proactive Patterns** if you want to disable the Commtouch CT Engine Proactive Patterns feature. This feature is automatically enabled on e-Series and Firebox X Peak models. It requires large amounts of disk space while the local database is updated. If you have limited memory or processor resources, consider disabling this feature.
6. The **Connection string override** text box is used only when you must troubleshoot a spamBlocker problem with a technical support representative. Do not change this value unless you are asked to give additional debug information for a technical support problem.
7. (Optional) You can use the tabs on the **spamBlocker Settings** dialog box to define several optional parameters for spamBlocker:
 - [Use an HTTP proxy server for spamBlocker](#)
 - [Use trusted email forwarders to improve spam score accuracy](#)
 - [Enable and set parameters for Virus Outbreak Detection \(VOD\)](#)
8. Click **OK**.

If you want to restore the default spamBlocker settings at any time, you can click **Restore Defaults**.

Use an HTTP proxy server for spamBlocker

On the **HTTP Proxy Server** tab, select the **Contact the spamBlocker server using an HTTP proxy server** check box if spamBlocker must use an HTTP proxy server to connect to the CommTouch server through the Internet.

Use the remaining fields in this dialog box to set up parameters for the proxy server, which include the address of the proxy server, the port the Firebox must use to contact the proxy server, and authentication credentials for the Firebox to use for proxy server connections (if required by the proxy server).

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.

1. From the **spamBlocker Settings** dialog box, click the **Trusted Email Forwarders** tab.
2. Type a host or domain name in the text field at the bottom of the dialog box and click **Add**.
If you add a domain name, make sure you add a leading period (.) to the name, as in `.firebox.net`.
3. (Optional) Repeat step 2 to add more trusted email forwarders.
4. Click **OK**.

Enable and set parameters for Virus Outbreak Detection (VOD)

Virus Outbreak Detection (VOD) is a technology that identifies email virus outbreaks worldwide within minutes and then provides protection against those viruses. Provided by Commtouch, an industry leader in email spam and virus protection, VOD catches viruses even faster than signature-based systems.

To enable and configure VOD:

1. On the **spamBlocker Settings** dialog box, select the **Virus Outbreak Detection** tab.
2. Select the **Enable Virus Outbreak Detection (VOD)** check box.
3. By default, VOD scans inbound email messages up to a 40 kilobyte limit. You can increase or decrease this limit with the arrows next to **VOD maximum file size to scan**. VOD uses the larger of the values set for VOD or spamBlocker. If the global spamBlocker value of the **Maximum file size to scan** field set on the spamBlocker Settings dialog box (as described in [Set global spamBlocker parameters](#)) is greater than the **VOD maximum file size to scan** value, VOD uses the global spamBlocker value.

In the proxy definitions for spamBlocker, you can set the actions for spamBlocker to take when a virus is found, as described in [Configure Virus Outbreak Detection \(VOD\) actions](#).

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 (Confirmed Spam, Bulk) 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
reportso@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/VK03E51A==

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](#).

spamBlocker statistics

The **Security Services** tab of Firebox System Manager includes current Firebox statistics about spamBlocker:

1. [Start Firebox System Manager](#).
2. Click the **Security Services** tab.

The following information appears:

- Number of messages since last restart that are identified as confirmed spam, bulk email, suspected spam, or not spam.
- Number of messages since last restart that are blocked, tagged, or sent to the Quarantine Server.
- Number of messages since last restart that are blocked or allowed because of a spamBlocker exceptions list that you create (exceptions that you create to deny additional sites are sometimes known as a blacklist; exceptions that you create to allow additional sites are sometimes known as a whitelist).

If you reboot the Firebox, all counters reset to zero.

Renew security subscriptions

The WatchGuard security subscriptions (Gateway AntiVirus, Intrusion Prevention Service, WebBlocker, and spamBlocker) need regular updates to operate effectively.

The Firebox gives reminders to renew your subscriptions. When you save changes to a configuration file, WatchGuard System Manager tells you if a subscription will expire 60 days before, 30 days before, 15 days before, and the day before the expiration date.

When your subscriptions expire, you cannot save any changes to your configuration until you either renew or disable the expired subscription.



*If your site uses WebBlocker, you must renew or disable the WebBlocker subscription as soon as it expires to prevent an interruption in web browsing. WebBlocker has a default setting that blocks all traffic when the connections to the server time out. When your WebBlocker expires, it no longer contacts the server. This appears to the Firebox as a server timeout. All HTTP traffic is blocked unless this default was changed before expiration. To change this setting, go to the **Advanced** tab of the **WebBlocker Configuration** dialog box and select the **Allow the user to view the website** option.*

1. From Policy Manager, click **File > Save > To Firebox**.
You see a message that tells you to update your feature key.
2. Click **OK**.
The Feature Key Compliance dialog box appears.



3. Select the expired subscription.
4. If you already have the new feature key, click Add Feature Key. Paste in your new feature key. You cannot right-click to paste. You must use CTRL-V or click **Paste**.
If you do not already have your new feature key, you must click **Disable** even if you plan to renew later. You do not lose your settings if you disable the subscription. If you renew your subscription at a later time, you can reactivate the settings and save them to the Firebox.
5. Click **OK**.

Renew subscriptions from Firebox System Manager

On the front panel of Firebox System Manager, if a subscription will expire soon, a warning appears and the **Renew Now** button is visible in the upper-right corner of the window. Click it to go to the LiveSecurity Service web site where you can renew the subscription.

28 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.

Start the Quarantine Server

To start the Quarantine Server, you must:

- [Install the Quarantine Server component](#)
- [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 WatchGuard System Manager Installation and did not install the Quarantine Server, you can run the installer again. Select the check box next to Quarantine Server. Do not select the check box for components you have already installed.

After you install the Quarantine Server, run the Quarantine Server Setup Wizard.

Run the Setup Wizard



The Quarantine Server, the Report Server, the Log Server, and the WatchGuard Management Server share the same master passphrase and server management passphrase. If you set up one of the other servers first, you do not have to set the passphrases again when you set up the Quarantine Server. If you have already run the Setup Wizard for one of these other servers, and then you run the Quarantine Server Setup Wizard, the wizard sets up the Quarantine Server with no input required.

Right-click the Quarantine Server icon (middle icon) in the System Tray and select **Start Service**.
The Quarantine Server Setup Wizard starts.

If you have already set up a Server

If you have already run the Management Server Setup Wizard or Report Server Setup Wizard, the Quarantine Server Setup Wizard shows only a screen that tells you the wizard is configuring your server. The last step you need to do to set up the Quarantine Server is to tell the Firebox where the Quarantine Server is located. The Firebox will send email messages to this location to be quarantined. For information on how to do this, see [Define the server location](#).

If you have not set up a Server

If you have not yet run the Management Server Setup Wizard or Report Server Setup Wizard, the Quarantine Server Setup Wizard shows the screens listed below.

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

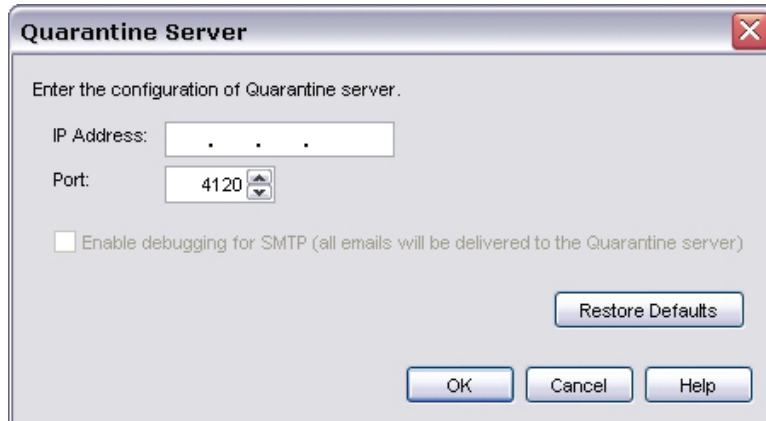
You can now define the server location, as described in [Define the server location](#).

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.

1. From Policy Manager, select **Tasks > Quarantine Server**.

The Quarantine Server dialog box appears.



The image shows a Windows-style dialog box titled "Quarantine Server". Inside the dialog, there is a text prompt: "Enter the configuration of Quarantine server." Below this, there are two input fields: "IP Address:" followed by a text box containing three dots, and "Port:" followed by a spinner box showing the value "4120". Below these fields is a checkbox labeled "Enable debugging for SMTP (all emails will be delivered to the Quarantine server)". At the bottom right of the dialog is a button labeled "Restore Defaults". At the very bottom are three buttons: "OK", "Cancel", and "Help".


2. Type the IP address for the Quarantine Server. We do not recommend that you change the Quarantine Server port unless you are working with a technical support representative to troubleshoot a specific problem.
3. To send all email messages that spamBlocker or Gateway AntiVirus handles to the Quarantine Server, select the **Enable debugging for SMTP** check box. If an email message is not handled by spamBlocker because it matches a spamBlocker exception, it is not sent to the Quarantine Server.
4. If you want to cancel the changes you made in this dialog box and return to the default entries, click the **Restore Defaults** button.

Configure the Quarantine Server

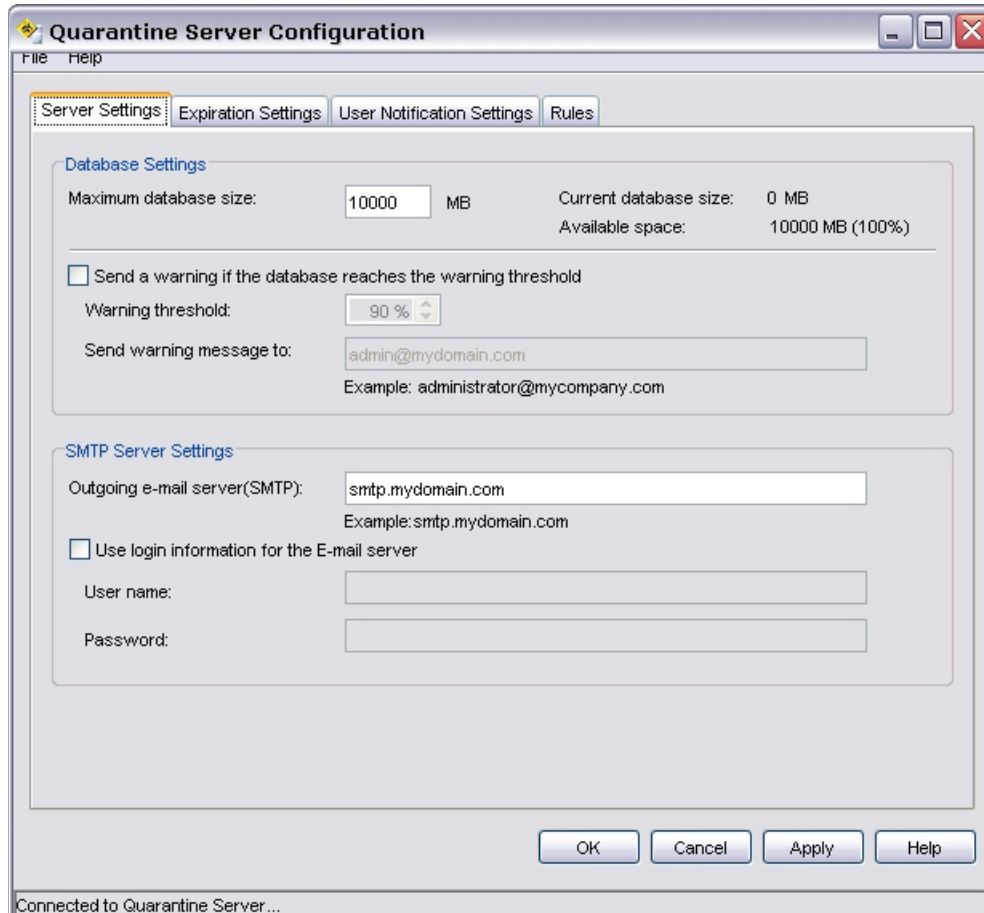
When you configure the Quarantine Server, you have these options:

- [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.



Quarantine Server Configuration

File Help

Server Settings | Expiration Settings | User Notification Settings | Rules

Database Settings

Maximum database size: 10000 MB Current database size: 0 MB
Available space: 10000 MB (100%)

☐ Send a warning if the database reaches the warning threshold

Warning threshold: 90 %

Send warning message to: admin@mydomain.com
Example: administrator@mycompany.com

SMTP Server Settings

Outgoing e-mail server(SMTP): smtp.mydomain.com
Example: smtp.mydomain.com

☐ Use login information for the E-mail server

User name:


Password:

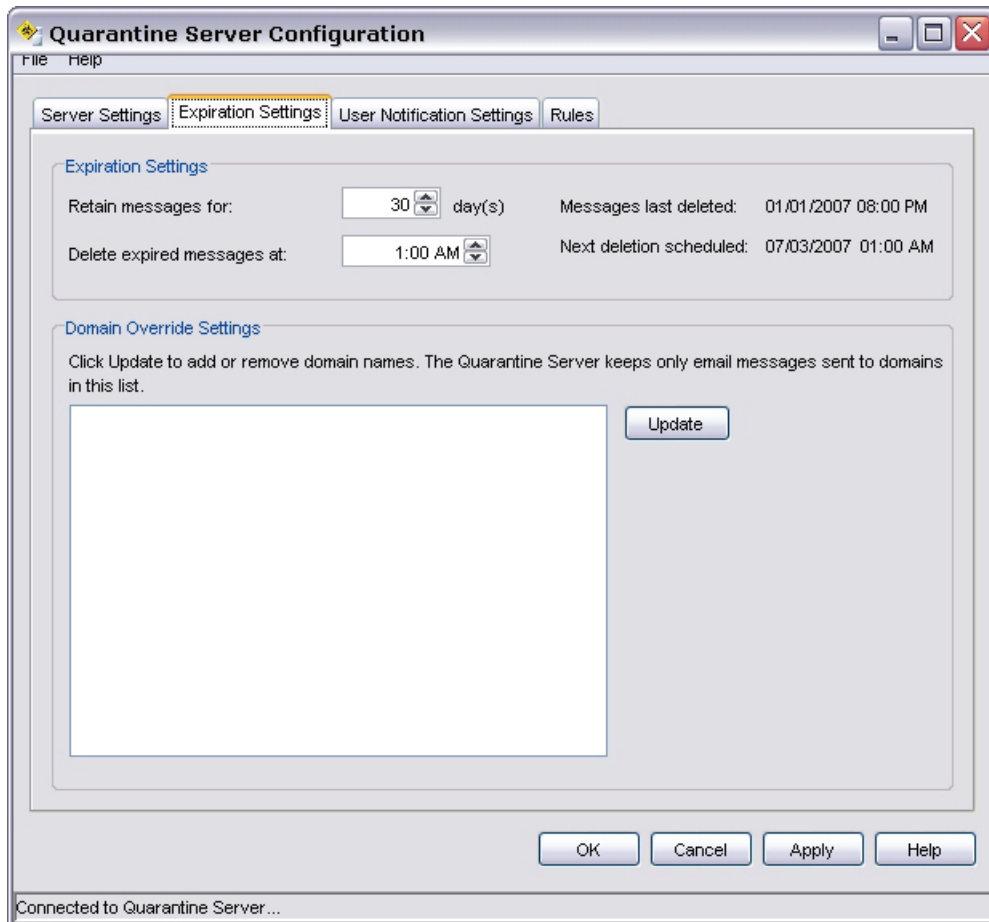
OK Cancel Apply Help

Connected to Quarantine Server...

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** 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.

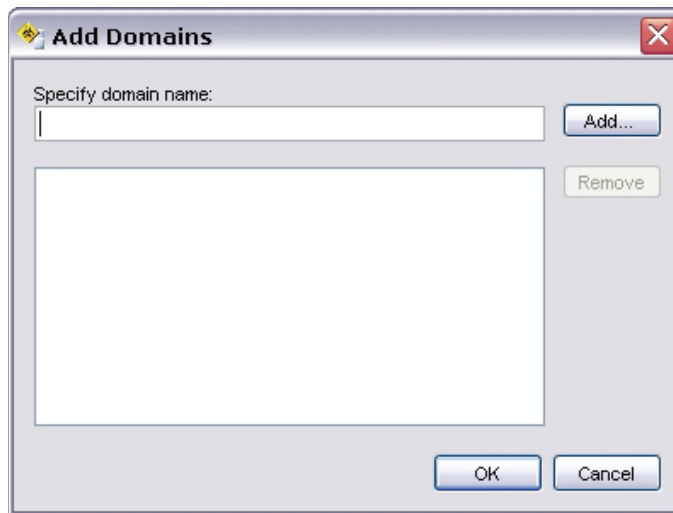


3. In the **Retain messages for** field, specify the number of days to maintain messages on the Quarantine Server.
4. In the **Delete expired messages at** field, enter the time of day to delete expired messages after the period of time in the previous field.

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.

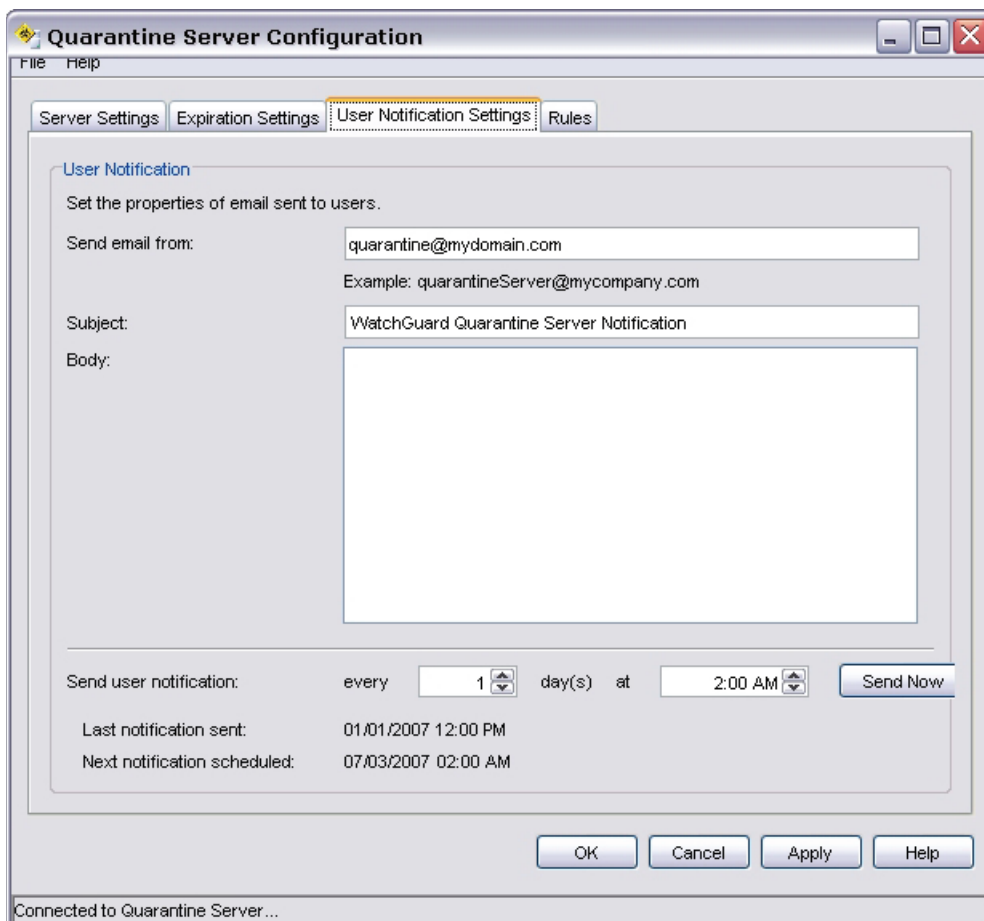


2. To add a domain, type it in the top field and click **Add**.
3. To remove a domain, select it from the list and click **Remove**.

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.



The screenshot shows the 'Quarantine Server Configuration' dialog box with the 'User Notification Settings' tab selected. The dialog has a menu bar with 'File' and 'Help'. Below the menu bar are four tabs: 'Server Settings', 'Expiration Settings', 'User Notification Settings' (which is highlighted), and 'Rules'. The 'User Notification' section contains the text 'Set the properties of email sent to users.' and four input fields: 'Send email from:' (containing 'quarantine@mydomain.com'), 'Subject:' (containing 'WatchGuard Quarantine Server Notification'), and 'Body:' (an empty text area). Below these fields is a section for scheduling notifications, including a 'Send user notification:' checkbox, a frequency selector (set to 'every 1 day(s) at 2:00 AM'), and a 'Send Now' button. At the bottom, there are buttons for 'OK', 'Cancel', 'Apply', and 'Help'. A status bar at the very bottom indicates 'Connected to Quarantine Server...'.

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**.
For more information about how to use the Add Event Processor dialog box that appears, see [Add a Log Server](#).
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

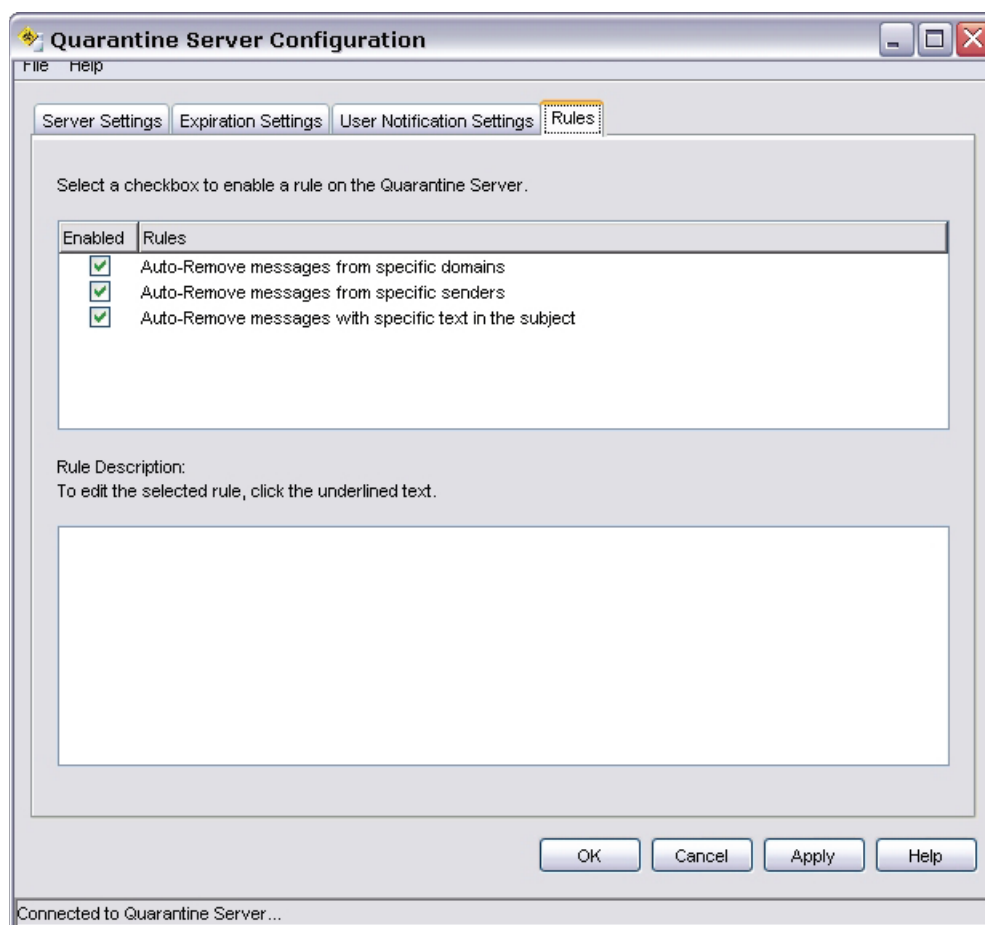
You set up rules to automatically remove certain messages if they come from a specific domain or sender, or if they contain specific text strings in the subject line.

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.

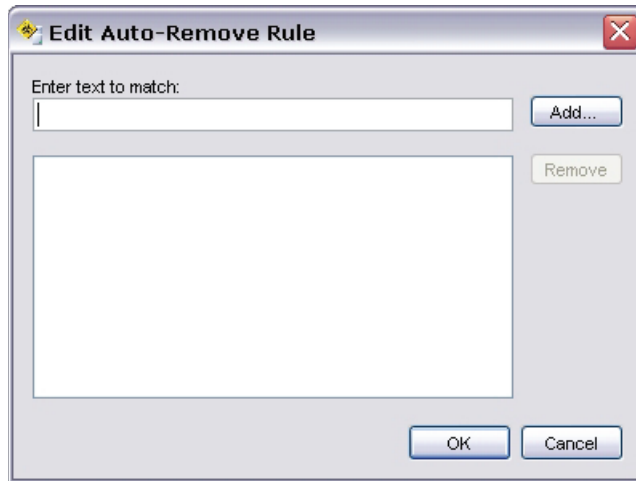
The Quarantine Server Configuration dialog box appears.

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

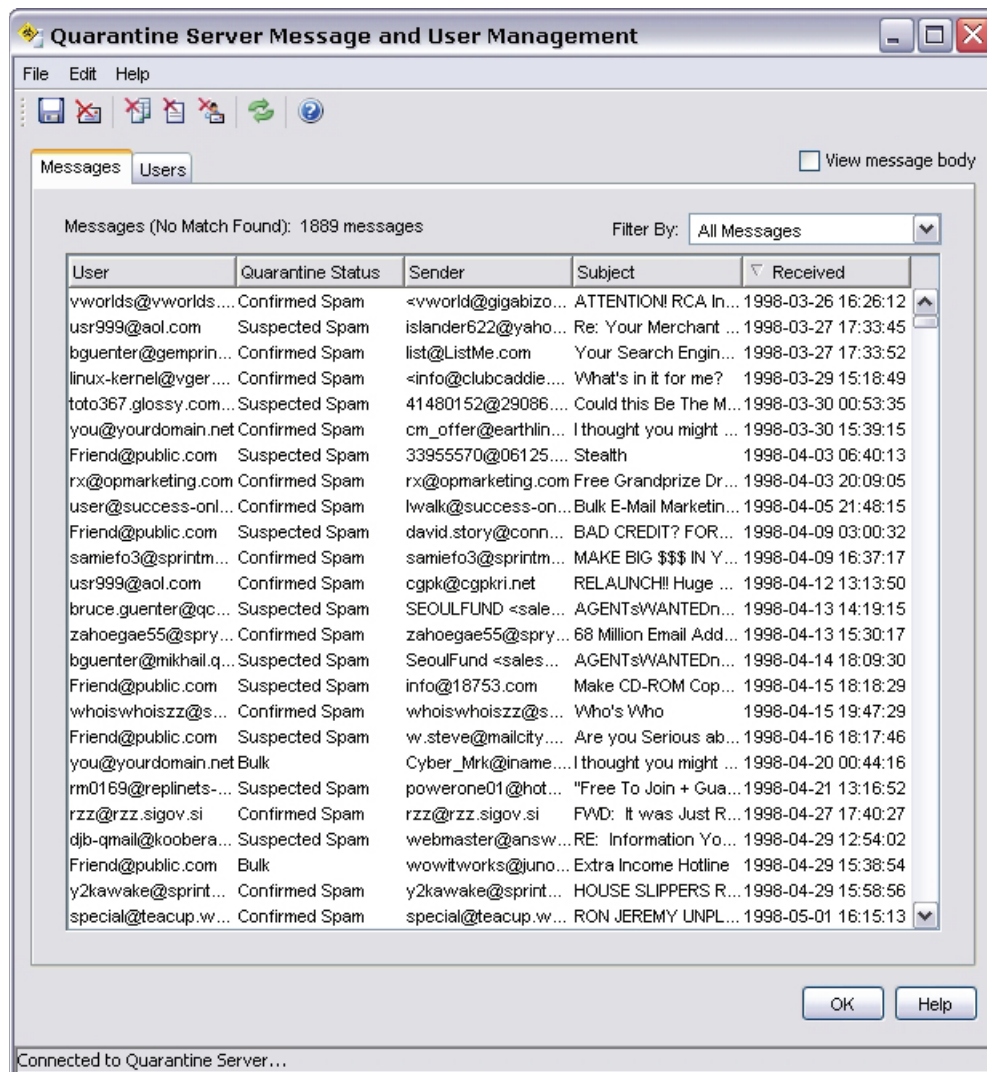
You can see all messages on the Quarantine Server in a dialog box. You can sort messages by user, quarantine status, sender, subject, and date/time received.



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.
 - To select a range of messages, click the first in the range, press the **Shift** key, and click the last message in the range.
 - To select multiple messages that are not in a range, hold down **Ctrl** as you select messages.
 - 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

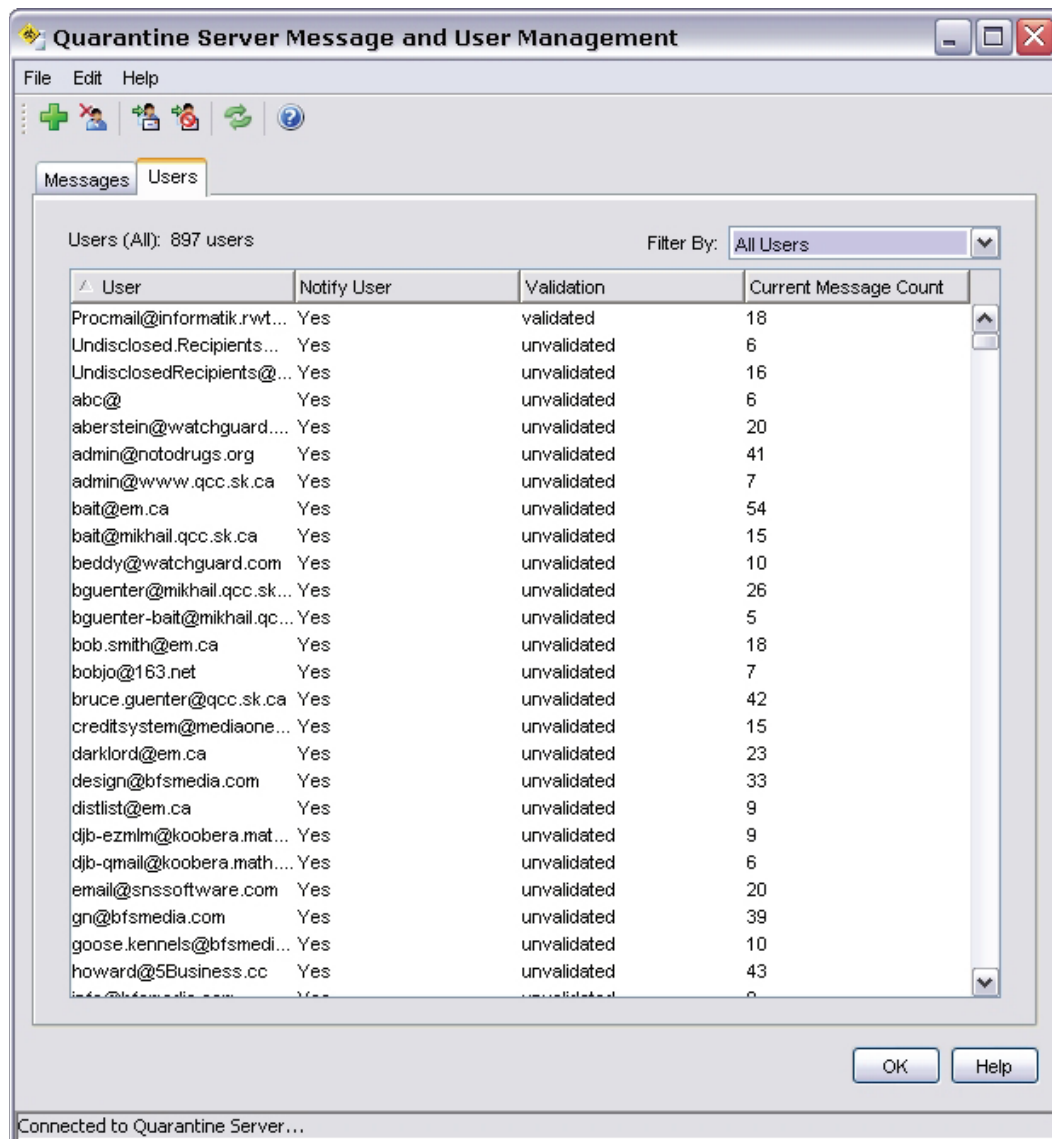
You can specify to automatically delete all future email messages from a particular domain or sender, or that contain certain text in the subject line. All subsequent email to any user with this characteristic is automatically deleted before it is sent to the Quarantine Server.

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.
 - To select a range of messages, click the first in the range, press the **Shift** key, and click the last message in the range.
 - To select multiple messages that are not in a range, hold down **Ctrl** as you select messages.
 - To select all messages, select **Edit > Select All**. Or, right-click any message and select **Select All**.
2. Choose the appropriate options for deletion.
 - 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.
 - You can also use the equivalent icons to select these options.

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**.

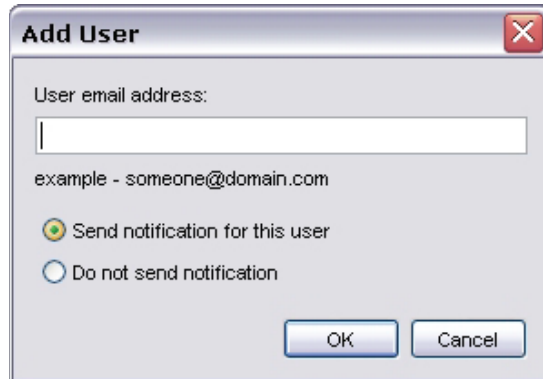


Add users

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**.

29 Signature-Based Security Services

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 can see statistics on current Gateway AntiVirus and Intrusion Prevention Service activity on the Firebox, as described in [Gateway AntiVirus statistics](#) and [Intrusion Prevention Service statistics](#).

Install and upgrade Gateway AV/IPS

To install either Gateway AntiVirus or Intrusion Prevention Service, you must [get a feature key](#) from LiveSecurity Service and [import a feature key to the Firebox](#).

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 [Configure the Gateway AV/IPS update server](#). You can also [See status and update signatures or engine manually](#).

About Gateway AntiVirus/Intrusion Prevention and proxy policies

Gateway AV can work with the WatchGuard SMTP, POP3, HTTP, FTP, and TCP-UDP proxies. Intrusion Prevention can work with those proxies in addition to the DNS proxy. When you enable Gateway AV or Intrusion Prevention, these proxies look at various types of traffic and perform an action that you specify, such as dropping the connection or blocking the packet and adding its source address to the Blocked Sites list.

Gateway AV and IPS scan different types of traffic according to which proxy or proxies you use the feature with:

- SMTP or POP3 proxy: Gateway AV/IPS looks for viruses and intrusions encoded with frequently used email attachment methods. You can also use Gateway AV and the SMTP proxy to send virus-infected email to the Quarantine Server. For more information, see [About the Quarantine Server](#) and [Configure Gateway AntiVirus to quarantine email](#).
- HTTP proxy: Gateway AV/IPS looks for viruses and intrusions in web pages that users try to download.
- TCP-UDP proxy: This proxy scans traffic on dynamic ports. It recognizes traffic for several different types of proxies, including HTTP and FTP. The TCP-UDP proxy then sends traffic to the appropriate proxy to scan for viruses or intrusions. You can also use the TCP-UDP proxy to block Instant Messaging (IM) or Peer to Peer (P2P) services. For more information, see [TCP-UDP proxy: Application blocking](#).
- FTP proxy: Gateway AV/IPS looks for viruses and intrusions in uploaded or downloaded files.
- DNS proxy: Gateway AV/IPS looks for viruses and intrusions in DNS packets.

Each proxy that uses Gateway AV/IPS is configured with options that are special to that proxy. For example, if you use Gateway AntiVirus with the FTP proxy, you can limit file scanning up to a specified kilobyte count.



*Signatures for Gateway AV are not automatically updated by default. To make sure Gateway AV has current signatures, either enable automatic updates for the Gateway AV server, (as described in [Configure the Gateway AV/IPS update server](#)) or use the **Security Services** tab of Firebox System Manager to manually update the signatures. For more information, see [Security services](#).*

Activate Gateway AntiVirus


You can activate Gateway AntiVirus in two ways: with the Activate Gateway AntiVirus wizard or through the definitions of proxies you want to use with the feature.

When you use the Activate Gateway AntiVirus wizard, you can create proxies in one step and enable Gateway AntiVirus for several proxies at the same time. If you plan to use Gateway AntiVirus for more than one proxy, you may save time if you use the wizard.

For more information, see:

- [Activate Gateway AntiVirus with a wizard from Policy Manager](#)
- [Activate Gateway AntiVirus wizard from proxy definitions](#)

Activate Gateway AV with a wizard

1. From WatchGuard System Manager, select the Firebox on which you want to use Gateway AntiVirus.
2. Click .
Or, select **Tools > Policy Manager**.
3. From Policy Manager, select **Tasks > Gateway AntiVirus > Activate**.
The Activate Gateway AntiVirus wizard starts.



4. Click **Next**.
5. Complete the wizard. The wizard shows different screens depending on whether you already have proxy policies in your configuration. If you do not, the wizard helps you create one or more proxy policies. The wizard has some or all of following screens depending on your current configuration.

Apply Gateway AntiVirus settings to your policies

This screen includes a list of proxy policies that are already on your Firebox. From the list, select the proxy policies for which you want to enable Gateway AntiVirus. The **Select** check boxes for any policies that are disabled or that have Gateway AntiVirus already enabled appear dimmed.

You can also automatically enable Gateway AntiVirus for the SMTP, POP3, HTTP, FTP, or TCP proxies if you change settings in the proxy definition, as described in [Activate Gateway AV from proxy definitions](#).

Select	Policy Name	Proxy Type	Type	Antivirus
<input type="checkbox"/>	HTTP-proxy-Out	HTTP	Firewall	Enabled
<input checked="" type="checkbox"/>	POP3-proxy	POP3	Firewall	Disabled
<input type="checkbox"/>	SMTP-proxy	SMTP	Firewall	Enabled

Create new proxy policies

This screen appears if your Firebox does not yet have policies created for Incoming SMTP, POP3, TCP, FTP, or HTTP Client.

To create a policy, select the corresponding check box. If you select SMTP, enter the mail server IP address.

If you select to create an SMTP policy, the wizard creates a default SMTP policy, which is a static NAT policy. To create this default SMTP policy, you must have at least one external interface with a static IP address or PPPoE. Only one policy is created even if you have more than one external interface. The **To** field of the policy is a static NAT entry (the static IP address of the first external interface to the specified mail service IP address). If this default policy does not meet your requirements, you can create an SMTP policy in Policy Manager before you run this wizard.



Activate Gateway AV from proxy definitions

You can activate Gateway AntiVirus from proxy definitions instead of the Activate Gateway AntiVirus wizard.

1. Add an SMTP, POP3, HTTP, FTP, or TCP-UDP proxy you want to use with Gateway AntiVirus.
For information on how to add policies, see [Add a proxy policy to your Firebox configuration](#).
For information on special procedures for defining proxies, see [About adding and configuring proxy policies](#).
2. Gateway AV can scan traffic that matches rules in several categories for each proxy. For example, for the SMTP and POP3 proxies, Gateway AV can scan traffic that matches rules in the Content Types and File Names categories. From the **Categories** list on the left side of the Proxy Configuration window, click one of the following categories.

FTP Proxy	SMTP Proxy	POP3 Proxy	HTTP Proxy	TCP-UDP Proxy (HTTP/SMTP traffic on dynamic ports)
Download	Content Types	Content Types	Requests: URL Paths	Request: URL Paths
Upload	File names	File names	Responses: Content Types, Body Content Types	Responses: Content Types, Body Content Types

3. Select **AV Scan** from the **If matched** or **None matched** drop-down lists if you want traffic that matches, or does not match, a given rule to be scanned for viruses. (For information on how to configure rules in a proxy definition, see [Add rules](#).)

Content Types Change View

Rules (simple view)

- text/*
- image/*
- application/pdf
- application/x-javascript
- application/x-shockwave-flash
- application/*xml*
- application/x-httpd-*
- httpd/*
- (none)

Pattern: Add Remove Predefined...

Actions to take

If matched: AV Scan Alarm Log

None matched: Deny Alarm ☒ Log

Gateway AntiVirus is automatically activated and enabled for the proxy. To use Gateway AntiVirus with other proxies, you must repeat this procedure for each one.

Configure Gateway AntiVirus actions

When you enable Gateway AntiVirus, you must set the actions to be taken if a virus or error is found in an email message (SMTP or POP3 proxies), web page (HTTP proxy), or uploaded or downloaded file (FTP proxy). The options for antivirus actions are:

Allow

Allows the packet to go to the recipient, even if the content contains a virus.

Deny (FTP proxy only)

Deny the file and send a deny message.

Lock (SMTP and POP3 proxies only)

Locks the attachment. This is a good option for files that cannot be scanned by the Firebox. A file that is locked cannot be opened easily by the user. Only the administrator can unlock the file. The administrator can use a different antivirus tool to scan the file and examine the content of the attachment. For information on how to unlock a file locked by Gateway AntiVirus, see [Unlock a file locked by Gateway AntiVirus](#).

Quarantine (SMTP proxy only)

When you use the SMTP proxy with the spamBlocker security subscription, you can send email messages with viruses or possible viruses to the Quarantine Server. For more information on the Quarantine Server, see [About the Quarantine Server](#). For information on how to set up Gateway AntiVirus to work with the Quarantine Server, see [Configure Gateway AntiVirus to quarantine email](#).

Remove (SMTP and POP3 proxies only)

Removes the attachment and allows the message through to the recipient.

Drop (not supported in POP3 proxy)

Drops the packet and drops the connection. No information is sent to the source of the message.

Block (not supported in POP3 proxy)

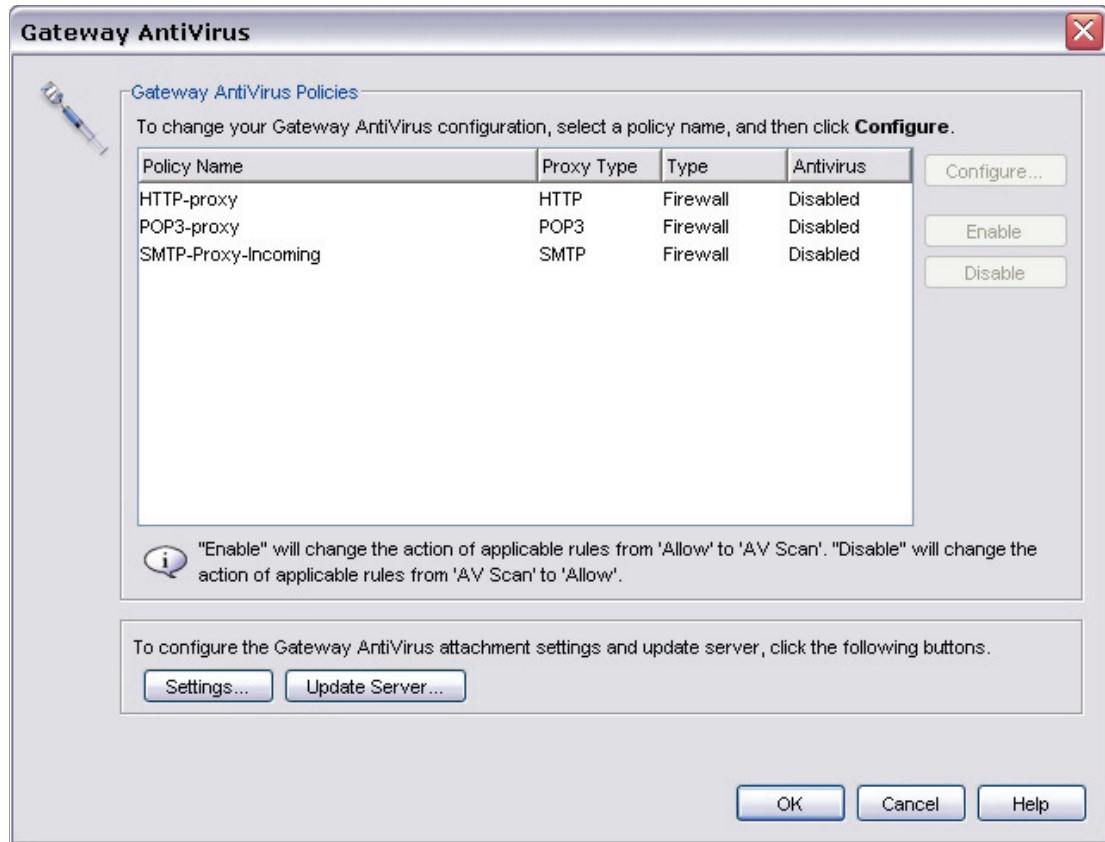
Blocks the packet, and adds the IP address of the sender to the Blocked Sites list.



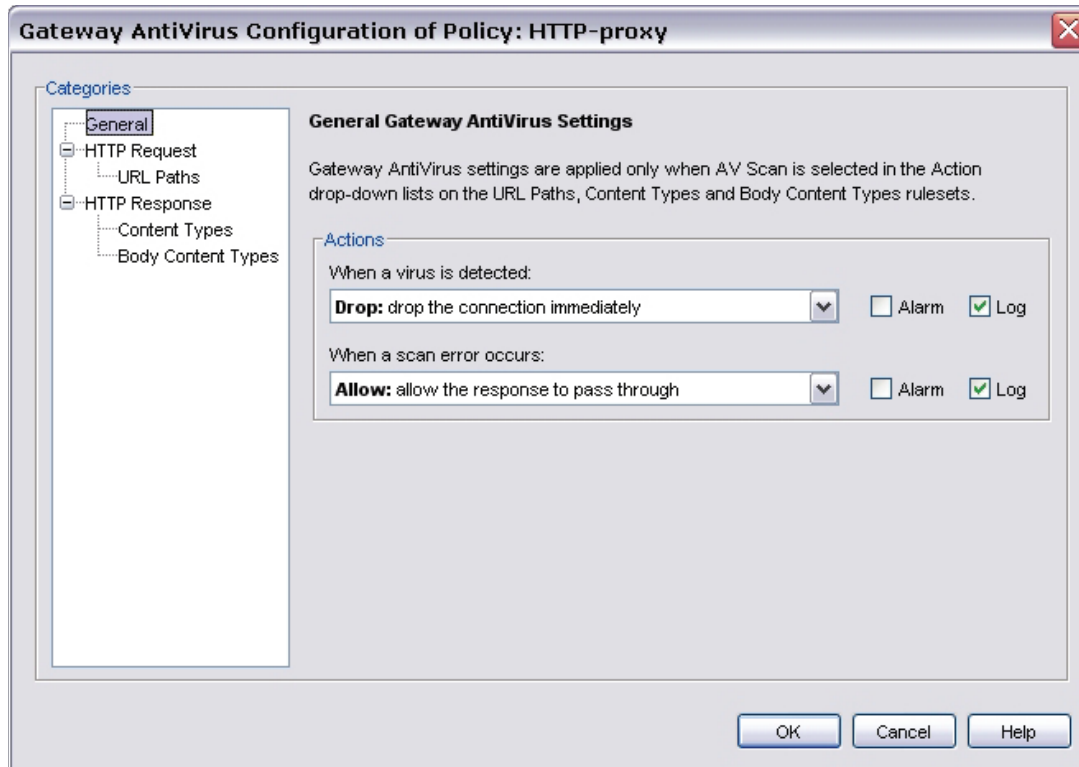
If you set the configuration to allow attachments, your configuration is less secure.

1. From Policy Manager, select **Tasks > Gateway AntiVirus > Configure**.

The Gateway AntiVirus dialog box appears, which lists the proxies that have already been created.



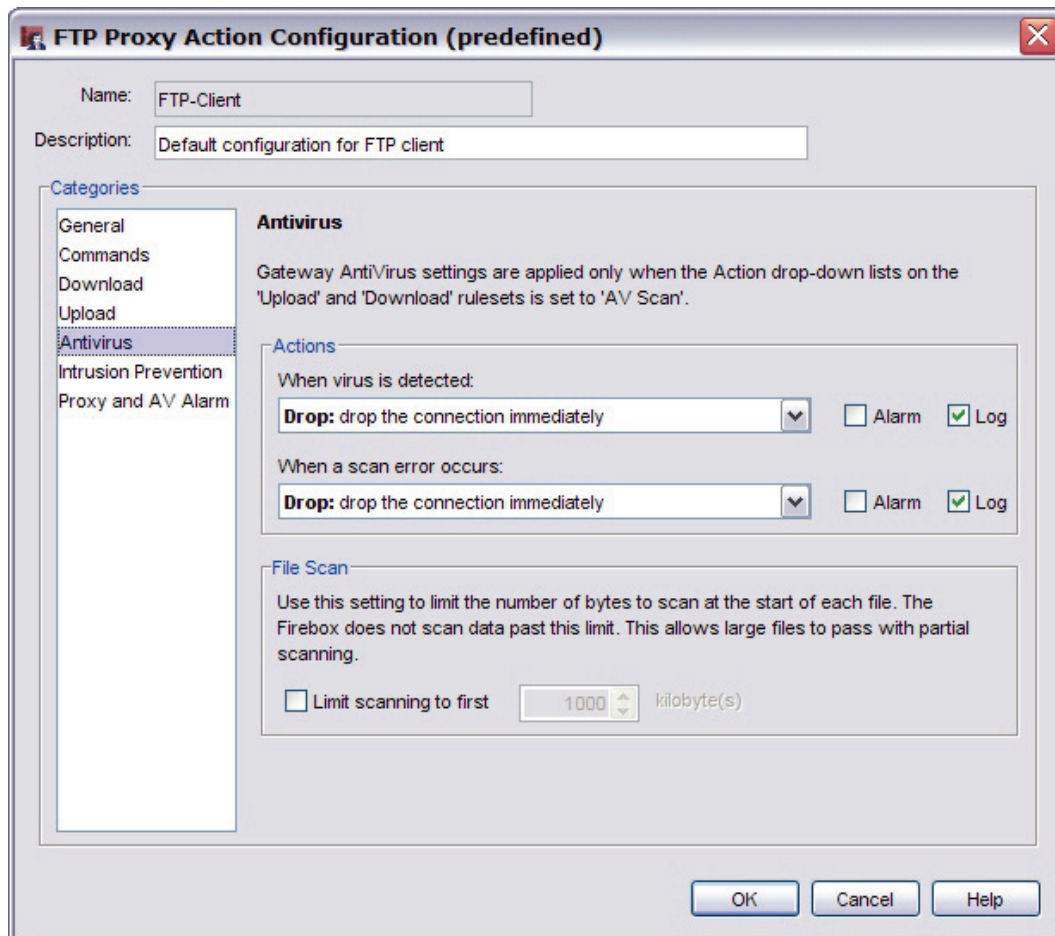
2. Select the policy you want to configure and click **Configure**.
The General Gateway AntiVirus Settings page for that policy appears.
 Or, instead of step 1 and 2, you can go to the same page from the proxy definition screens. From the **Categories** section in the proxy definition, select **AntiVirus**.



3. Set the action the Firebox takes if a virus is detected in an email message, file, or web page, in the **When a virus is detected** drop-down list. See the beginning of this section for a description of the proxy actions.
4. Set the action the Firebox takes when it cannot scan an object or an attachment in the **When a scan error occurs** drop-down list. Attachments that cannot be scanned include binhex-encoded messages, certain encrypted files, or files that use a type of compression that we do not support such as password-protected Zip files. See the beginning of this section for a description of the proxy actions.
5. (FTP proxy only) You can limit file scanning up to a specified kilobyte count. Any additional bytes in the file are not scanned. This allows the proxy to partially scan very large files without a large effect on performance. Enter the limit in the **Limit scanning to first** field.

Create alarms or log entries for antivirus actions

An alarm is a mechanism to tell users when a proxy rule applies to network traffic. Use the **Alarm** check box on the AntiVirus page of a proxy definition to create an alarm when the adjacent action occurs. If you do not want an alarm for the antivirus action, clear the **Alarm** check box for that action.



To use the alarm feature successfully, you must also configure the type of alarm to use in each proxy policy. To configure the alarm type to use, use the Proxy and AV Alarms category for the proxy. For information about the settings for this category, see [Set logging and notification preferences](#).

If you want to record log messages for a proxy action, select the **Log** check box for the antivirus response. If you do not want to record log messages for an antivirus response, clear the **Log** check box.

Unlock a file locked by Gateway AntiVirus

WatchGuard System Manager provides an executable file to unlock attachments locked by Gateway AntiVirus:

C:\Program Files\WatchGuard\wsm10.0\bin\unlock.exe

To open a locked file:

1. Open a command prompt.
2. Type: **Unlock** <path to locked file>

Configure Gateway AntiVirus to quarantine email

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 filtered by spamBlocker.

To configure Gateway AntiVirus to quarantine email:

1. When you run the Activate Gateway AntiVirus Wizard (as described in [Activate Gateway AntiVirus](#)), you must make sure you use Gateway AntiVirus with the SMTP proxy. The POP3 proxy does not support the Quarantine Server.
2. When you set the actions spamBlocker applies for different categories of email (as described in [Configure spamBlocker](#)), make sure you select the **Quarantine** action for at least one of the categories. When you select this action, you are prompted to configure the Quarantine Server if you have not already done so.

You can also select the **Quarantine** action for email messages identified by Virus Outbreak Detection as containing viruses. For more information, see [Configure Virus Outbreak Detection \(VOD\) actions](#).

Activate Intrusion Prevention Service (IPS)

Hackers use many methods to attack computers on the Internet. The function of these attacks is to cause damage to your network, get sensitive information, or use your computers to attack other networks. These attacks are known as *intrusions*.

You use the Firebox Intrusion Prevention Service (IPS) with the WatchGuard proxies to find and stop intrusions. IPS examines DNS, FTP, HTTP, POP3, and SMTP traffic. It uses the TCP/UDP proxy for HTTP and FTP on non-standard ports.



Because the TCP-UDP proxy has an additional set of options for IPS, you cannot use this procedure for that proxy. To use IPS with the TCP-UDP proxy, see [Activate and configure Intrusion Prevention Service for TCP-UDP](#). You can also use the TCP-UDP proxy to detect, and then allow or deny Instant Messaging (IM) or Peer to Peer (P2P) services. However, this feature is part of the base product. You do not need to purchase Intrusion Prevention Service to use it. For more information, see [TCP-UDP proxy: Application blocking](#).

Before you use IPS in a proxy policy, you must activate the feature and create a basic configuration. You can either run the Activate Intrusion Prevention wizard or use the Intrusion Prevention ruleset in the proxy definition, as described in [Intrusion prevention in proxy definitions](#). We recommend you use the wizard. To run the Activate Intrusion Prevention wizard:

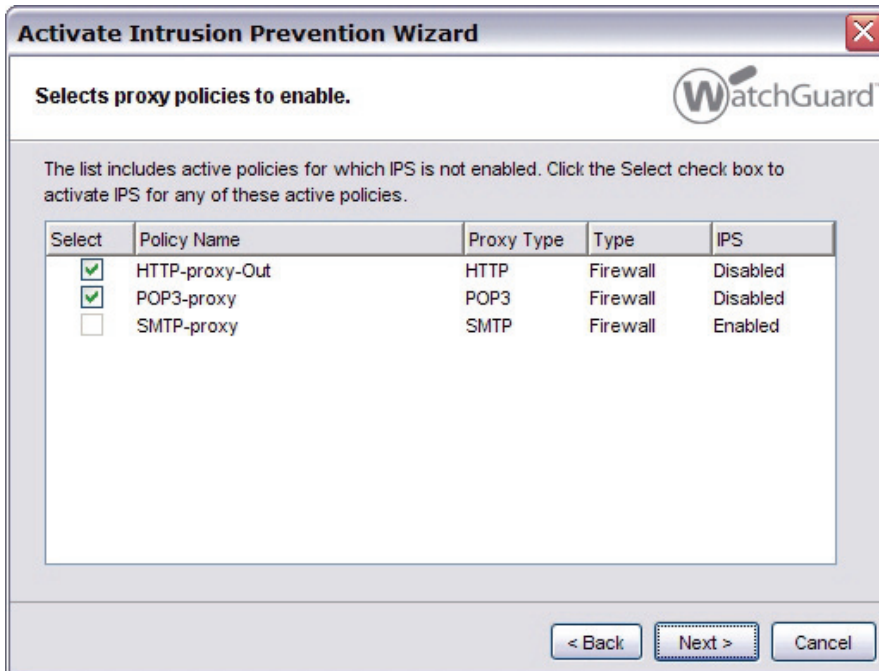
1. [Get a feature key](#) for IPS from LiveSecurity Service and [import a feature key to the Firebox](#).
2. From WatchGuard System Manager, select the Firebox that will use IPS, and [open Policy Manager](#).
3. From Policy Manager, select **Tasks > Intrusion Prevention > Activate**.
The Activate Intrusion Prevention wizard starts.



4. Click **Next**.
5. Click through the wizard and add the information it asks for. The wizard shows different screens depending on whether you already have proxy policies in your configuration. If you do not, the wizard helps you create a proxy policy. You can then use the wizard again to configure IPS, or see the instructions in the subsequent section. The wizard has the following screens.

Select proxy policies to enable

This screen shows a list of proxy policies that are already defined on your Firebox. From the list, select the proxy policies you want to enable IPS for. The **Select** check boxes for any policies that are disabled or that have Gateway AntiVirus already enabled appear dimmed.



Select	Policy Name	Proxy Type	Type	IPS
<input checked="" type="checkbox"/>	HTTP-proxy-Out	HTTP	Firewall	Disabled
<input checked="" type="checkbox"/>	POP3-proxy	POP3	Firewall	Disabled
<input type="checkbox"/>	SMTP-proxy	SMTP	Firewall	Enabled

Create new proxy policies

This screen shows the proxy types whose corresponding policies do not currently exist. If, for example, you have already created an SMTP policy, it does not appear in the list.

To create a policy, select the corresponding check box. If you select SMTP, enter the mail server IP address. This wizard creates a default SMTP policy, which is a static NAT policy. To create this default SMTP policy, you must have at least one external interface with a static IP address or PPPoE.

Only one policy is created even if you have more than one external interface. The **To** field of the policy is a static NAT entry (the static IP address of the first external interface to the specified mail service IP address). If this default policy does not meet your requirements, you can create an SMTP policy in Policy Manager before you run this wizard.



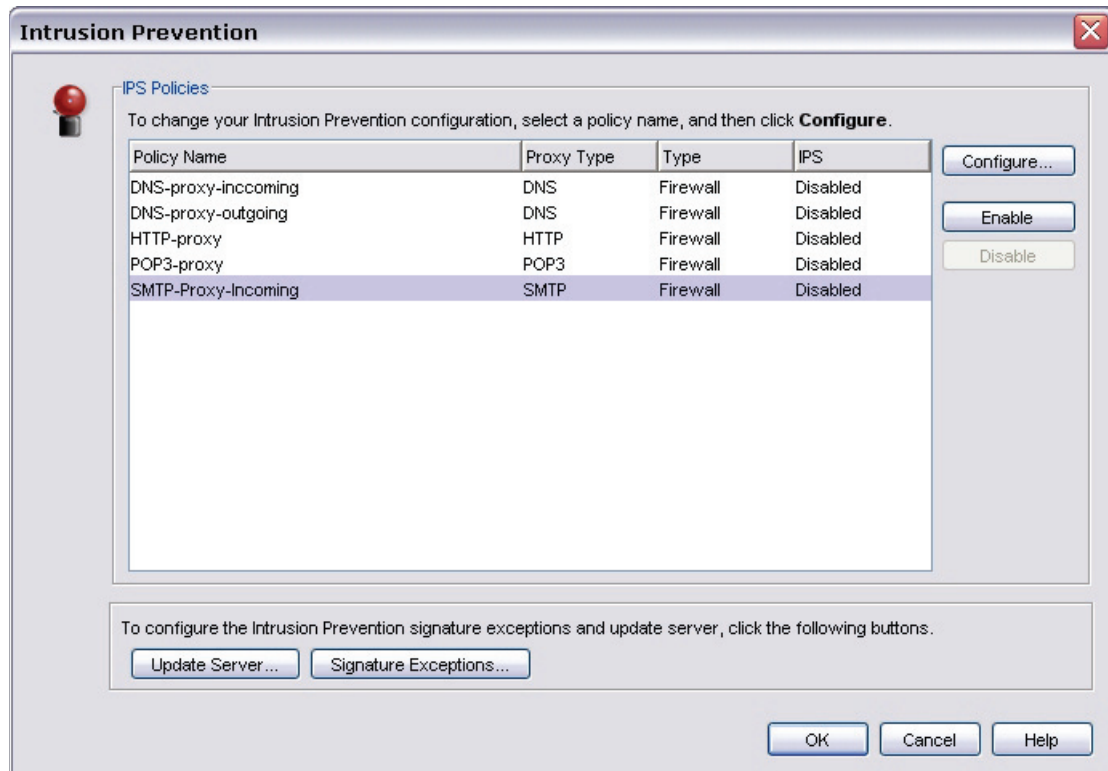
When the wizard is complete, you can [configure Intrusion Prevention Service \(IPS\)](#) for any proxies you have selected to use with it.

Configure Intrusion Prevention Service (IPS)

After you use the Activate Intrusion Prevention wizard to activate IPS and create a basic configuration, you can further refine the configuration.

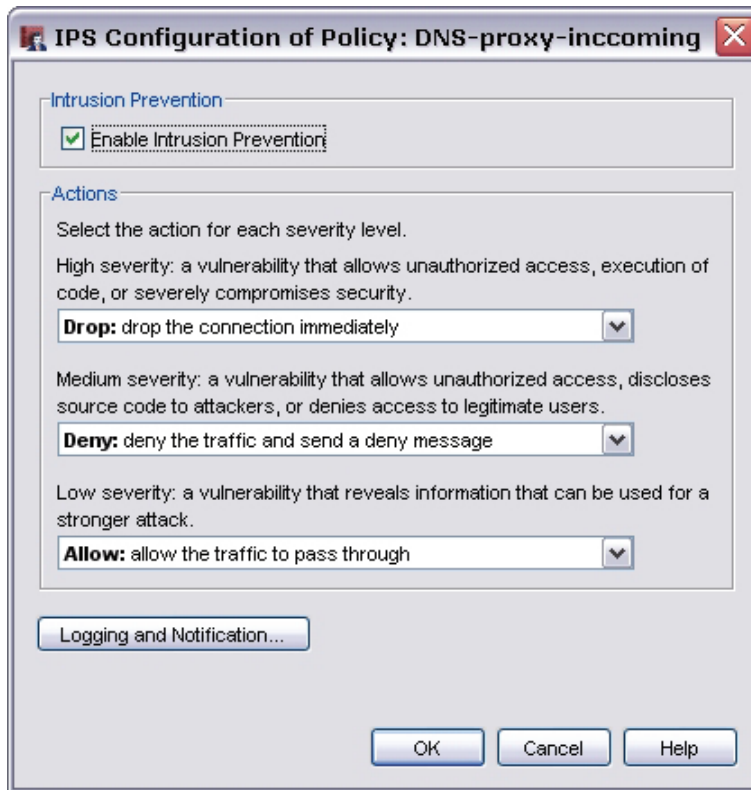
If you enabled IPS from a proxy definition, as described in [Proxy ruleset: Intrusion prevention](#), you do not need to use this procedure. You already configured the service when you used the proxy definition window to enable IPS. However, you can use this procedure to make changes to the IPS configuration at any time.

1. From Policy Manager, select **Tasks > Intrusion Prevention > Configure**.
The Intrusion Prevention dialog box appears, which lists the policies that have already been created.



2. Select the policy you want to configure and click **Configure**.
The IPS Configuration dialog box for that policy appears.

3. Select the **Enable Intrusion Prevention** check box.



4. [Set parameters for Intrusion Prevention Service \(IPS\).](#)

Set parameters for Intrusion Prevention Service (IPS)

1. Select the **Enable Intrusion Prevention** check box.

The screenshot shows a configuration window for the Intrusion Prevention Service (IPS). At the top, the 'Enable Intrusion Prevention' checkbox is checked. Below it, the 'Protection type' is set to 'Client' in a dropdown menu. A section titled 'Spyware Protection' contains a checked 'Enable Spyware protection' checkbox. Another section titled 'Actions' has a dropdown menu set to 'Deny: deny the transaction and send a deny message'. At the bottom left is a button labeled 'Logging and Notification...'. At the bottom right are three buttons: 'OK', 'Cancel', and 'Help'.

In the **Protection type** drop-down list, select **Client** or **Server**. Different signature sets are for client and server endpoints.

2. (HTTP and TCP-UDP proxies only) If you selected **Client** in the previous field, you can use the **Enable spyware protection** check box to enable or disable spyware protection.
3. Select one of the following actions:
 - **Allow**: Allow the transaction, even if the content matches a signature. If you allow attachments, your configuration is less secure.
 - **Deny**: Deny the transaction and send a deny message to the sender. (This option is not supported in the TCP-UDP proxy.)
 - **Drop**: Drop the connection to stop the message and drop the connection. No information is sent to the source of the message.
 - **Block**: Drop the connection and add the IP address of the sender to the Blocked Sites list. (This option is not supported in the TCP-UDP proxy.)
4. Click **Logging and Notification** to configure logging and notification for IPS. For information on the dialog box that appears, see [Set logging and notification preferences](#).

Configure signature exceptions

Each signature used by IPS has a unique ID number. You can find the ID number for a signature using the Firebox System Manager tool. Open Firebox System Manager and select the **Show Signatures** option on the **Security Services** tab. If you have a signature that you want the IPS service to ignore, you can add it as an exception.

1. From the **Intrusion Prevention** dialog box, click **Signature Exceptions**.
The Signature ID Exceptions dialog box appears.



2. Type or use the value control button to enter the signature that you want to disable. Click **Add**.

Copy IPS settings to other policies

After configuring IPS for one proxy, you can copy the same configuration to other proxies. However, you can copy IPS settings only between policies with compatible IPS configurations:


- Between FTP, DNS, POP3, and SMTP policies
- Between multiple TCP policies
- Between multiple HTTP policies

To copy IPS settings:

1. From the **Intrusion Prevention** dialog box, select the proxy whose configuration you want to copy, right-click, and select **Copy IPS Configuration**.
2. From the same dialog box, select the proxy or proxies you want to copy the configuration to, right-click, and select **Paste IPS Configuration**.

Activate and configure Intrusion Prevention Service for TCP-UDP

Because you can set more parameters for IPS with the TCP-UDP proxy than for other proxies, you cannot use the Activate IPS Wizard to enable or configure IPS for TCP-UDP.

1. If you have not yet added the TCP proxy to your Firebox configuration, [open Policy Manager](#), click the plus (+) sign on the Policy Manager toolbar, expand the **Proxies** folder, and double-click **TCP-proxy**.
2. In the New Policy Properties dialog box, select the Properties tab, and click .
3. From the **Categories** section, select **Intrusion Prevention**.
4. [Set parameters for Intrusion Prevention Service \(IPS\)](#).
5. To configure the TCP-UDP proxy to block Instant Messaging (IM) or Peer to Peer (P2P) services, see [TCP-UDP proxy: Application blocking](#).

Update Gateway AntiVirus/IPS and see status

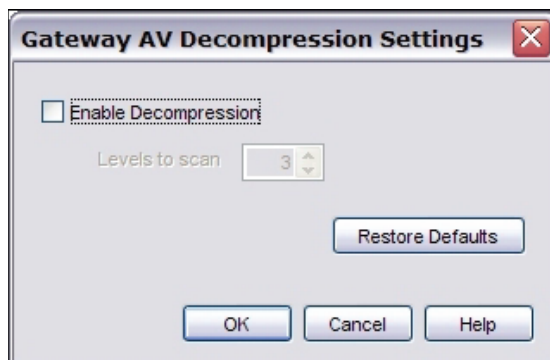
The Firebox uses several settings for the Gateway AntiVirus engine regardless of which proxy it is configured to work with. For more information, see [Configure Gateway AntiVirus engine settings](#).

It is important to update the signatures for Gateway AntiVirus/Intrusion Prevention Service. The signatures for these services are not automatically updated by default. You can update the signatures in two ways:

- [Configure the Gateway AV/IPS update server](#) to enable automatic updates
- Update the signatures manually in Firebox System Manager, as described in [See status and update signatures or engine manually](#).

Configure Gateway AV engine settings

1. From Policy Manager, select **Tasks > Gateway AntiVirus > Configure**.
The Gateway AntiVirus dialog box appears.
2. From the **Gateway AntiVirus** dialog box, click **Settings**.
The Gateway AV Decompression Settings dialog box appears.



3. To scan inside compressed attachments, select the **Enable Decompression** check box. Select or type the number of compression levels to scan. We recommend that you keep the default setting of three levels, unless your organization must use a larger value. If you specify a larger number, your Firebox could send traffic too slowly. Gateway AntiVirus supports up to six levels.
If Gateway AntiVirus detects that the archive depth is greater than the value set in this field, it will generate a scan error for the content.
Compressed attachments that cannot be scanned include encrypted files or files that use a type of compression that we do not support such as password-protected Zip files. To set the action for the Firebox when it finds a message it cannot scan, select an action for **When a scan error occurs** in the **General** category of the policy configuration.
4. Click **Restore Defaults** if you want to reset the user interface to default settings.
5. Click **OK**.

Configure the Gateway AV/IPS update server

Gateway AV and IPS use the same update server.

1. From Policy Manager, select **Tasks > Gateway AntiVirus > Configure**.
2. From the **Gateway AntiVirus** dialog box, click **Update Server**.
The Update Server dialog box appears

Update Server

Automatic Update

☒ Enable automatic update Interval: hour(s)

☐ IPS Signatures

☐ GAV Signatures

☐ GAV Engine

Server

Type the URL for the GAV/IPS update server.

HTTP Proxy Server

☐ Contact the GAV/IPS update server using an HTTP proxy server

Server address: . . .

Server port:

Server authentication:

User name:

User domain:

Password:

3. Automatic updates for Gateway AV/IPS are not enabled by default. To enable automatic updates for the server, select the **Enable automatic update** check box. Enter the number of hours between automatic updates in the **Interval** drop-down list.
 - If you want the Firebox to download a new set of Gateway AV signatures at this interval, select the **Gateway AV Signatures** check box.
 - If you want the Firebox to download a new set of IPS signatures at this interval, select the **IPS Signatures** check box.
 - If you want to check for updates to the Gateway AV engine at this interval, select the **Gateway AV Engine** check box.
4. Do not change the URL of the update server for Gateway AV or IPS unless you are told to do so by WatchGuard. If you change the URL accidentally or incorrectly, click **Restore Defaults** to return to the default setting.
5. Click **OK**.

Connect to the update server through an HTTP proxy server

If your Firebox must connect through an HTTP proxy to get to the Gateway AV/IPS update server, you must add information about the HTTP proxy server to your Gateway AV/IPS configuration.

1. From the **Gateway AntiVirus** or **Intrusion Prevention** dialog box, click **Update Server**.
2. Select the **Contact the Gateway AV/IPS update server using an HTTP proxy server** check box.
3. From the **Server address** drop-down list, select whether you identify your HTTP proxy server by host name or IP address. Type the host name or IP address in the adjacent field.
4. Most HTTP proxy servers receive requests on port 8080. If your HTTP proxy uses a different port, enter it in the **Server port** field.
5. From the **Server authentication** drop-down list, select the type of authentication your HTTP proxy server uses. Select **NoAuth** if your HTTP proxy does not require authentication. If your HTTP proxy server requires **NTLM** or **Basic** authentication, enter your user name, user domain, and password in the correct fields.

See status and update signatures or engine manually

Security services can be configured to update signatures and the engine automatically, as described in [Configure the Gateway AV/IPS update server](#). You can also update signatures or the engine manually. If the signatures or engine on the Firebox are not current, you are not protected from the latest viruses and intrusions.

You can see the status and get updates for Gateway AV/IPS on the **Security Services** tab in Firebox System Manager.

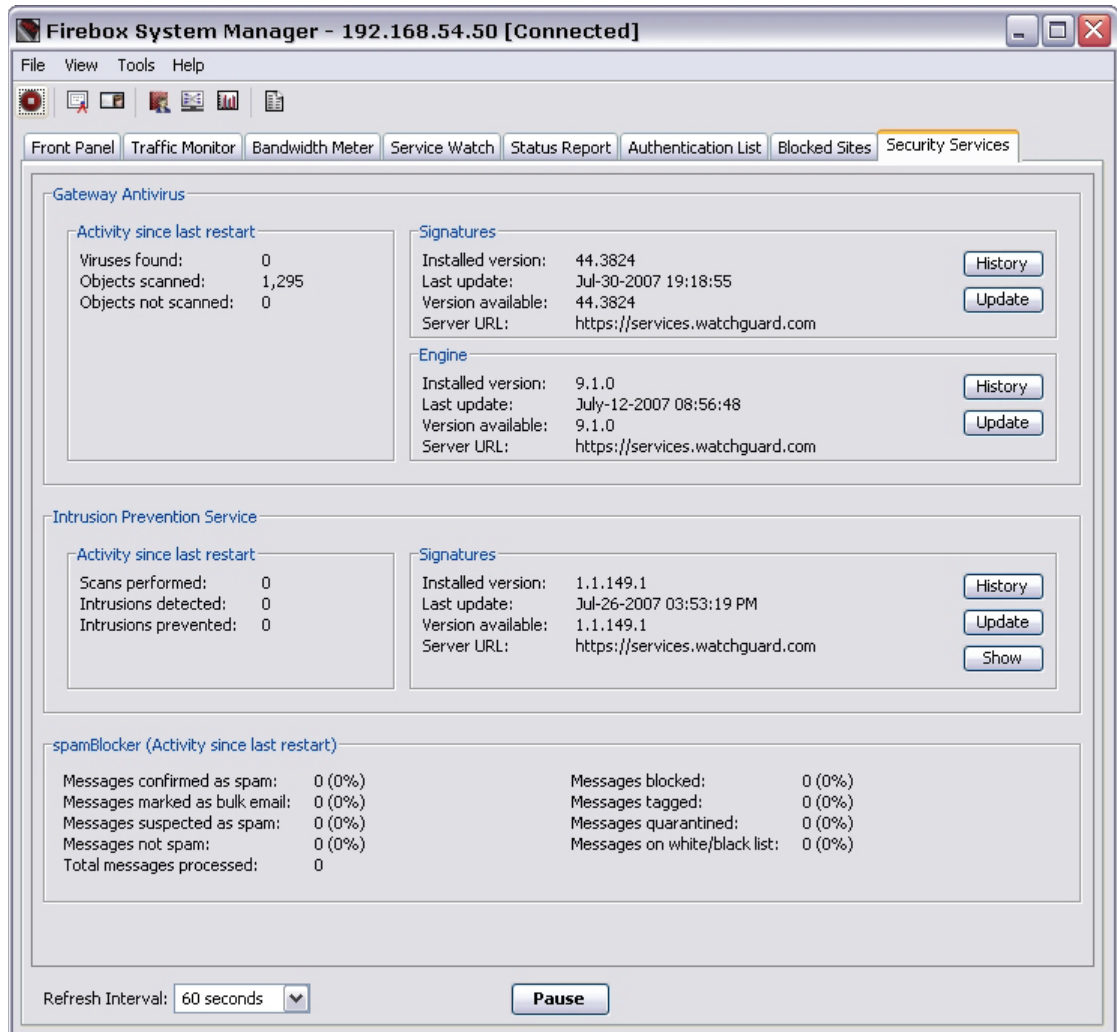
See service status

The **Security Services** tab in Firebox System Manager shows you whether protection is active. You can also see information about the signature versions.

To see service status:

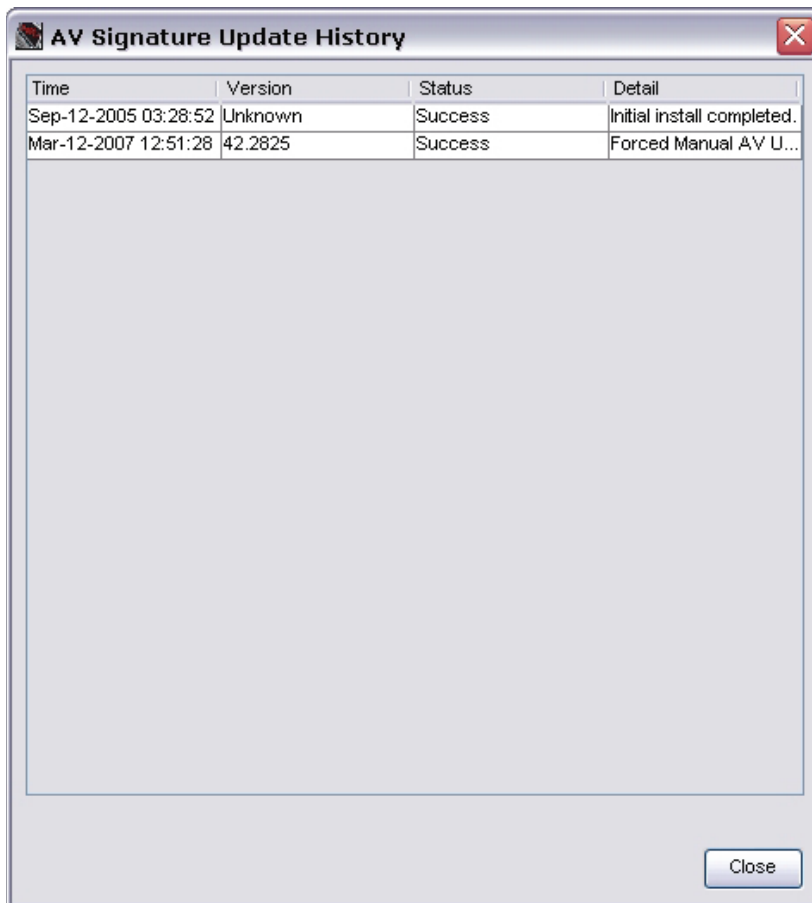
1. [Start Firebox System Manager](#).
2. Click the **Security Services** tab.

The window shows the status for the installed security services. Licenses for these features must be installed to see status information.



See the update history

From the **Security Services** tab, click **History** to see a list of updates of services and engines.

A screenshot of a Windows-style window titled "AV Signature Update History". The window has a standard title bar with a close button (X) in the top right corner. Inside the window, there is a table with four columns: "Time", "Version", "Status", and "Detail". The table contains two rows of data. Below the table, there is a large, empty rectangular area, likely for additional details or logs. At the bottom right of the window, there is a "Close" button.

Time	Version	Status	Detail
Sep-12-2005 03:28:52	Unknown	Success	Initial install completed.
Mar-12-2007 12:51:28	42.2825	Success	Forced Manual AV U...

Update services manually

From the **Security Services** tab, click **Update** for the service you want to update. You must type your configuration passphrase.

The Firebox downloads the most recent available signature update or the most recent available engine for Gateway AntiVirus or Intrusion Protection Service.

Renew security subscriptions

The WatchGuard security subscriptions (Gateway AntiVirus, Intrusion Prevention Service, WebBlocker, and spamBlocker) need regular updates to operate effectively.

The Firebox gives reminders to renew your subscriptions. When you save changes to a configuration file, WatchGuard System Manager tells you if a subscription will expire 60 days before, 30 days before, 15 days before, and the day before the expiration date.

When your subscriptions expire, you cannot save any changes to your configuration until you either renew or disable the expired subscription.



*If your site uses WebBlocker, you must renew or disable the WebBlocker subscription as soon as it expires to prevent an interruption in web browsing. WebBlocker has a default setting that blocks all traffic when the connections to the server time out. When your WebBlocker expires, it no longer contacts the server. This appears to the Firebox as a server timeout. All HTTP traffic is blocked unless this default was changed before expiration. To change this setting, go to the **Advanced** tab of the **WebBlocker Configuration** dialog box and select the **Allow the user to view the website** option.*

1. From Policy Manager, click **File > Save > To Firebox**.
You see a message that tells you to update your feature key.
2. Click **OK**.
The Feature Key Compliance dialog box appears.



3. Select the expired subscription.
4. If you already have the new feature key, click Add Feature Key. Paste in your new feature key. You cannot right-click to paste. You must use CTRL-V or click **Paste**.
If you do not already have your new feature key, you must click **Disable** even if you plan to renew later. You do not lose your settings if you disable the subscription. If you renew your subscription at a later time, you can reactivate the settings and save them to the Firebox.
5. Click **OK**.

Renew subscriptions from Firebox System Manager

On the front panel of Firebox System Manager, if a subscription will expire soon, a warning appears and the **Renew Now** button is visible in the upper-right corner of the window. Click it to go to the LiveSecurity Service web site where you can renew the subscription.

30 Dynamic Routing

About dynamic routing



The OSPF and BGP dynamic routing protocols are available only in Fireware Pro. Only Routing Information Protocol (RIP) is available with Fireware.

A routing protocol is the language a router speaks with other routers to share information about the status of network routing tables. With static routing, routing tables are set and do not change. If a router on the remote path fails, a packet cannot get to its destination.

Dynamic routing lets routing tables in routers change as the routes change. If the best path to a destination cannot be used, dynamic routing protocols change routing tables when necessary to keep your network traffic moving. Fireware Pro supports RIP v1 and v2, OSPF, and BGP v4 dynamic routing protocols. Fireware supports only RIP v1 and v2.

About routing daemon configuration files

To use any of the dynamic routing protocols with Fireware, you must import or type a dynamic routing configuration file for the routing daemon you choose. This configuration file includes information such as a password and log file name. To see sample configuration files for each of the routing protocols, see these topics:\

- [Sample RIP routing configuration file](#)
- [Sample OSPF routing configuration file](#)
- [Sample BGP routing configuration file](#)

Notes about configuration files:

- The ! and the # characters are comment characters. If the first character of the word is one of the comment characters, then the rest of the line is interpreted as a comment. If the comment character is not the first character of the word, it is interpreted as a command.
- Usually, you can use the word no at the beginning of the line to disable a command. For example: no network 10.0.0.0/24 area 0.0.0.0 disables the backbone area on the specified network.

About Routing Information Protocol (RIP)



Support for this protocol is available in both Fireware and Fireware Pro.

RIP (Routing Information Protocol) is used to manage router information in a self-contained network, such as a corporate LAN or a private WAN. With RIP, a gateway host sends its routing table to the closest router each 30 seconds. This router, in turn, sends the contents of its routing tables to neighboring routers.

RIP is best for small networks. This is because the transmission of the full routing table each 30 seconds can put a large traffic load on the network, and because RIP tables are limited to 15 hops. OSPF is a better alternative for larger networks.

There are two versions of RIP. RIP v1 uses a UDP broadcast over port 520 to send updates to routing tables. RIP v2 uses multicast to send routing table updates.

Routing Information Protocol (RIP) commands

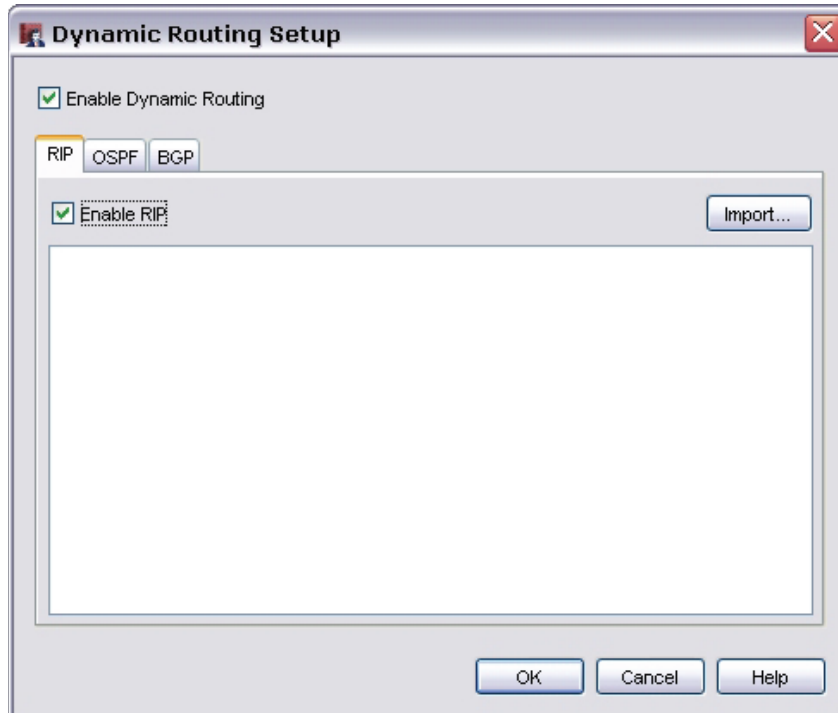
To create or modify a routing configuration file, here is a catalog of supported routing commands for RIP v1 and RIP v2. If you use RIP v2, you must include the subnet mask with any command that uses a network IP address or RIP v2 will not operate. The sections must appear in the configuration file in the same order they appear in this table.

Section	Command	Description
Set simple password or MD5 authentication on an interface		
	interface eth [N]	Begin section to set
		authentication type for interface
	ip rip authentication string [PASSWORD]	Set RIP authentication password
	key chain [KEY-CHAIN]	Set MD5 key chain name
	key [INTEGER]	Set MD5 key number
	key-string [AUTH-KEY]	Set MD5 authentication key
	ip rip authentication mode md5	Use MD5 authentication
	ip rip authentication mode key-chain [KEY-CHAIN]	Set MD5 authentication key-chain
Configure RIP routing daemon		
	router rip	Enable RIP daemon
	version [1/2]	Set RIP version to 1 or 2 (default version 2)
	ip rip send version [1/2]	Set RIP to send version 1 or 2
	ip rip receive version [1/2]	Set RIP to receive version 1 or 2
	no ip split-horizon	Disable split-horizon; enabled by default

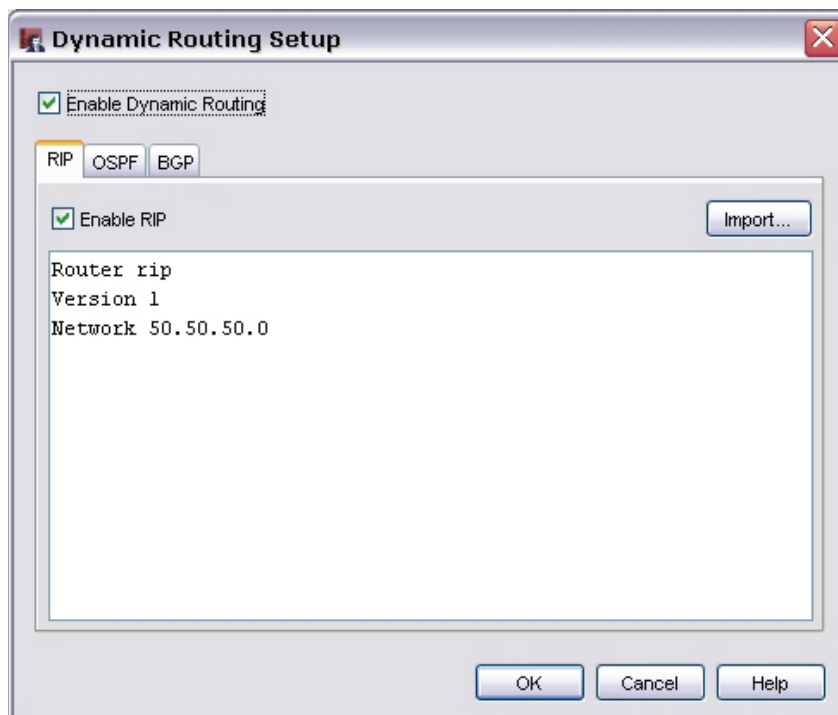
Section	Command	Description
Configure interfaces and networks		
	no network eth[N]	
	passive-interface eth[N]	
	passive-interface default	
	network [A.B.C.D/M]	
	neighbor [A.B.C.D/M]	
Distribute routes to RIP peers and inject OSPF or BGP routes to RIP routing table		
	default-information originate	Share route of last resort (default route) with RIP peers
	redistribute kernel	Redistribute firewall static routes to RIP peers
	redistribute connected	Redistribute routes from all interfaces to RIP peers
	redistribute connected route-map [MAPNAME]	Redistribute routes from all interfaces to RIP peers, with a route map filter (mapname)
	redistribute ospf	redistribute routes from OSPF to RIP
	redistribute ospf route-map [MAPNAME]	Redistribute routes from OSPF to RIP, with a route map filter (mapname)
	redistribute bgp	Redistribute routes from BGP to RIP
	redistribute bgp route-map [MAPNAME]	Redistribute routes from BGP to RIP, with a route map filter (mapname)
Configure route redistribution filters with route maps and access lists		
	access-list [PERMIT DENY] [LISTNAME] [A,B,C,D/M ANY]	Create an access list to allow or deny redistribution of only one IP address or for all IP addresses
	route-map [MAPNAME] permit [N]	Create a route map with a name and allow with a priority of N
	match ip address [LISTNAME]	

Configure the Firebox to use RIP v1

1. From Policy Manager, select **Network > Dynamic Routing**.
The Dynamic Routing Setup dialog box appears.



2. Click **Enable Dynamic Routing** and **Enable RIP**.
3. Click **Import** to import a routing daemon configuration file, or type your configuration file in the text box. Click **OK**. For more information see [About routing daemon configuration files](#).



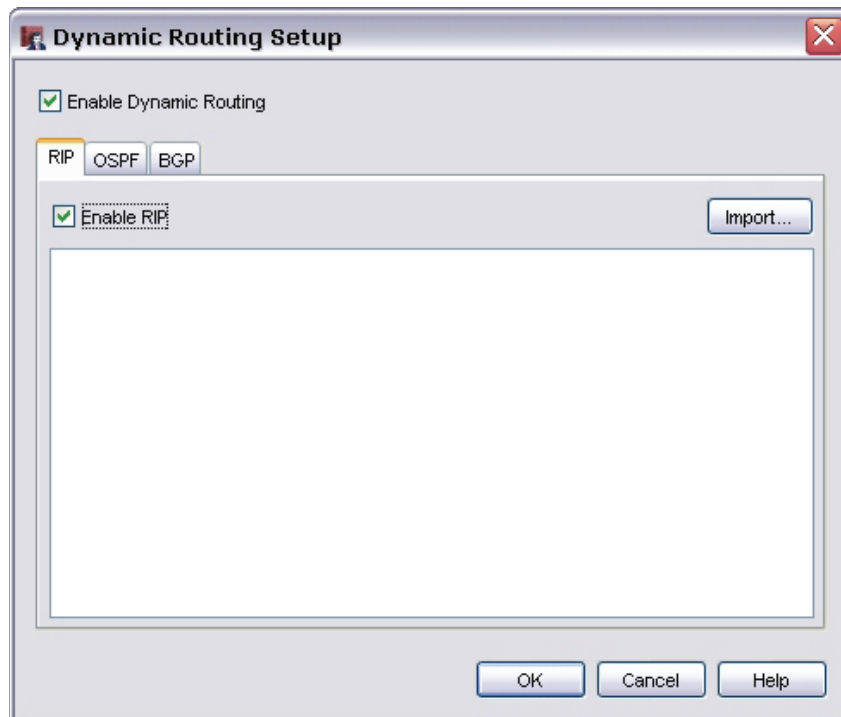
Allow RIP v1 traffic through the Firebox

You must add and configure a policy to allow RIP broadcasts from the router to the network broadcast IP address. You must also add the IP address of the Firebox interface to the **To** field.

1. From Policy Manager, select **Edit > Add Policies**. From the list of packet filters, select **RIP**. Click **Add**.
2. In the **New Policy Properties** dialog box, configure the policy to allow traffic from the IP or network address of the router that uses RIP to the Firebox interface it connects to. You must also add the network broadcast IP address. (For information on how to set the source and destination addresses for a policy, see [Set access rules for a policy](#).) Click **OK**.
3. Finally, you must set up the router for the Firebox to talk to. After it is configured, look at the dynamic routing section of the [Firebox Status Report](#) to verify that the Firebox and the router are sending updates to each other. You can then add authentication and restrict the RIP policy to listen only on the correct interfaces.

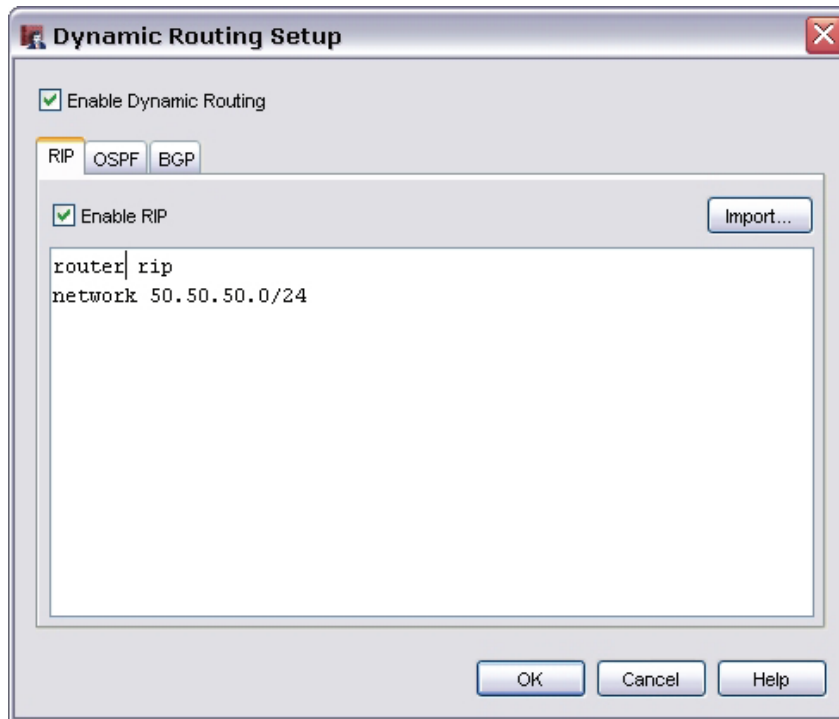
Configure the Firebox to use RIP v2

1. In Policy Manager, select **Network > Dynamic Routing**.
The Dynamic Routing Setup dialog box appears.



2. Click **Enable Dynamic Routing** and **Enable RIP**.

3. Click **Import** to import a routing daemon configuration file, or type your configuration parameters in the text box. Click **OK**.



Allow RIP v2 traffic through the Firebox

You must add and configure a policy to allow RIP v2 multicasts from the routers that have RIP v2 enabled to the reserved multicast IP address for RIP v2.

1. From Policy Manager, select **Edit > Add Policies**. From the list of packet filters, select **RIP**. Click **Add**. *The New Policy Properties dialog box appears for RIP.*
2. In the **New Policy Properties** dialog box, configure the policy to allow traffic from the IP or network address of the router that uses RIP to the multicast address 224.0.0.9. (For information on how to set the source and destination addresses for a policy, see [Set access rules for a policy](#).) Click **OK**.
3. Finally, you must set up the router for the Firebox to talk to. After it is configured, look at the dynamic routing section of the [Firebox Status Report](#) to verify that the Firebox and the router are sending updates to each other. You can then add authentication and restrict the RIP policy to listen only on the correct interfaces.

Sample RIP routing configuration file

To use any of the dynamic routing protocols with Fireware, you must import or type a configuration file for the dynamic routing daemon. This topic includes a sample configuration file for the RIP routing daemon. If you want to use this configuration file as a base for your own configuration file, copy the text into an application such as Notepad or Wordpad and save it with a new name. You can then edit the parameters to meet your own business requirements.

Optional commands are commented with the ! character. To enable a command, delete the ! and modify variables as necessary.

!! SECTION 1: Configure MD5 authentication keychains.

! Set MD5 authentication key chain name (KEYCHAIN), key number (1),

```
! and authentication key string (AUTHKEY).
! key chain KEYCHAIN
! key 1 ! key-string AUTHKEY
!! SECTION 2: Configure interface properties.
! Set authentication for interface (eth1).
! interface eth1
!
! Set RIP simple authentication password (SHAREDKEY).
! ip rip authentication string SHAREDKEY
!
! Set RIP MD5 authentication and MD5 keychain (KEYCHAIN).
! ip rip authentication mode md5
! ip rip authentication key-chain KEYCHAIN
!
!! SECTION 3: Configure global RIP daemon properties.
! Enable RIP daemon. Must be enabled for all RIP configurations. router rip
!
! Set RIP version to 1; default is version 2.
! version 1
!
! Set RIP to send or received to version 1; default is version 2.
! ip rip send version 1
! ip rip receive version 1
!
! Disable split-horizon to prevent routing loop. Default is enabled.
! no ip split-horizon
!! SECTION 4: Configure interfaces and networks.
! Disable RIP send and receive on interface (eth0).
! no network eth0
!
! Set RIP to receive-only on interface (eth2).
! passive-interface eth2
!
! Set RIP to receive-only on all interfaces.
! passive-interface default
```

```
!  
! Enable RIP broadcast (version 1) or multicast (version 2) on  
! network (192.168.253.0/24). !network 192.168.253.0/24  
!  
! Set unicast routing table updates to neighbor (192.168.253.254).  
! neighbor 192.168.253.254  
!! SECTION 5: Redistribute RIP routes to peers and inject OSPF or BGP  
!! routes to RIP routing table.  
! Share route of last resort (default route) from kernel routing table  
! with RIP peers.  
! default-information originate  
!  
! Redistribute firewall static routes to RIP peers.  
! redistribute kernel  
!  
! Set route maps (MAPNAME) to restrict route redistribution in Section 6.  
! Redistribute routes from all interfaces to RIP peers or with a route map  
! filter (MAPNAME).  
! redistribute connected  
! redistribute connected route-map MAPNAME  
!  
! Redistribute routes from OSPF to RIP or with a route map filter (MAPNAME).  
! redistribute ospf !redistribute ospf route-map MAPNAME  
!  
! Redistribute routes from BGP to RIP or with a route map filter (MAPNAME).  
! redistribute bgp !redistribute bgp route-map MAPNAME  
!! SECTION 6: Configure route redistribution filters with route maps and  
!! access lists.  
! Create an access list to only allow redistribution of 172.16.30.0/24.  
! access-list LISTNAME permit 172.16.30.0/24  
! access-list LISTNAME deny any  
!  
! Create a route map with name MAPNAME and allow with a priority of 10.  
! route-map MAPNAME permit 10  
! match ip address LISTNAME
```


About Open Shortest Path First (OSPF) Protocol



Support for this protocol is available only in Fireware Pro.

OSPF (Open Shortest Path First) is an interior router protocol used in larger networks. With OSPF, a router that sees a change to its routing table or that detects a change in the network immediately sends a multicast update to all other routers in the network. OSPF is different from RIP because:

- OSPF sends only the part of the routing table that has changed in its transmission. RIP sends the full routing table each time.
- OSPF sends a multicast only when its information has changed. RIP sends the routing table every 30 seconds.

Also, note the following about OSPF:

- If you have more than one OSPF area, one area must be area 0.0.0.0 (the backbone area).
- All areas must be adjacent to the backbone area. If they are not, you must configure a virtual link to the backbone area.

OSPF commands

To create or modify a routing configuration file, here is a catalog of supported routing commands. The sections must appear in the configuration file in the same order they appear in this table. You can also use the sample OSPF configuration file found in the Dynamic Routing section of the Fireware FAQs at

<http://www.watchguard.com/support/faqs/fireware/>

Section	Command	Description
Configure Interface		
	ip ospf authentication-key [PASSWORD]	Set OSPF authentication password
	interface eth[N]	Begin section to set properties for interface
	ip ospf message-digest-key [KEY-ID] md5 [KEY]	Set MD5 authentication key ID and key
	ip ospf cost [1-65535]	Set link cost for the interface (see OSPF Interface Cost table below)
	ip ospf hello-interval [1-65535]	Set interval to send hello packets; default is 10 seconds
	ip ospf dead-interval [1-65535]	Set interval after last hello from a neighbor before declaring it down; default is 40 seconds
	ip ospf retransmit-interval [1-65535]	Set interval between link-state advertisements (LSA) retransmissions; default is 5 seconds
	ip ospf transmit-delay [1-3600]	Set time required to send LSA update; default is 1 second
	ip ospf priority [0-255]	Set route priority; high value increases eligibility to become the designated router (DR)

Section	Command	Description
Configure OSPF Routing Daemon		
	router ospf	Enable OSPF daemon
	ospf router-id [A.B.C.D]	set router ID for OSPF manually; router will determine its own ID if not set
	ospf rfc 1583compatibility	Enable RFC 1583 compatibility (can lead to routing loops)
	ospf abr-type [cisco ibm shortcut standard]	More information about this command can be found in draft-ietf-abr-o5.txt
	passive-interface eth[N]	Disable OSPF announcement on interface eth[N]
	auto-cost reference bandwidth[0-429495]	Set global cost (see OSPF cost table below); do not use with "ip ospf [COST]" command
	timers spf [0-4294967295][0-4294967295]	Set OSPF schedule delay and hold time
Enable OSPF on a Network		
*The "area" variable can be typed in two formats: [W.X.Y.Z]; or as an integer [Z].		
	network [A.B.C.D/M] area [Z]	Announce OSPF on network A.B.C.D/M for area 0.0.0.Z
Configure Properties for Backbone area or Other Areas		
The "area" variable can be typed in two formats: [W.X.Y.Z]; or as an integer [Z].		
	area [Z] range [A.B.C.D/M]	Create area 0.0.0.Z and set a classful network for the area (range and interface network and mask setting should match)
	area [Z] virtual-link [W.X.Y.Z]	Set virtual link neighbor for area 0.0.0.Z
	area [Z] stub	Set area 0.0.0.Z as a stub
	area [Z] stub no-summary	
	area [Z] authentication	Enable simple password authentication for area 0.0.0.Z
	area [Z] authentication message-digest	Enable MD5 authentication for area 0.0.0.Z

Section	Command	Description
Redistribute OSPF Routes		
	default-information originate	Share route of last resort (default route) with OSPF
	default-information originate metrics [0-16777214]	Share route of last resort (default route) with OSPF, and add a metric used to generate the default route
	default-information originate always	Always share the route of last resort (default route)
	default-information originate always metrics [0-16777214]	Always share the route of last resort (default route), and add a metric used to generate the default route
	redistribute connected	Redistribute routes from all interfaces to OSPF
	redistribute connected metrics	Redistribute routes from all interfaces to OSPF, and a metric used for the action
Configure Route Redistribution with Access Lists and Route Maps		
	access-list [LISTNAME] permit [A.B.C.D/M]	Create an access list to allow distribution of A.B.C.D/M
	access-lists [LISTNAME] deny any	Restrict distribution of any route map not specified above
	route-map [MAPNAME] permit [N]	Create a route map with name [MAPNAME] and allow with a priority of [N]
	match ip address [LISTNAME]	

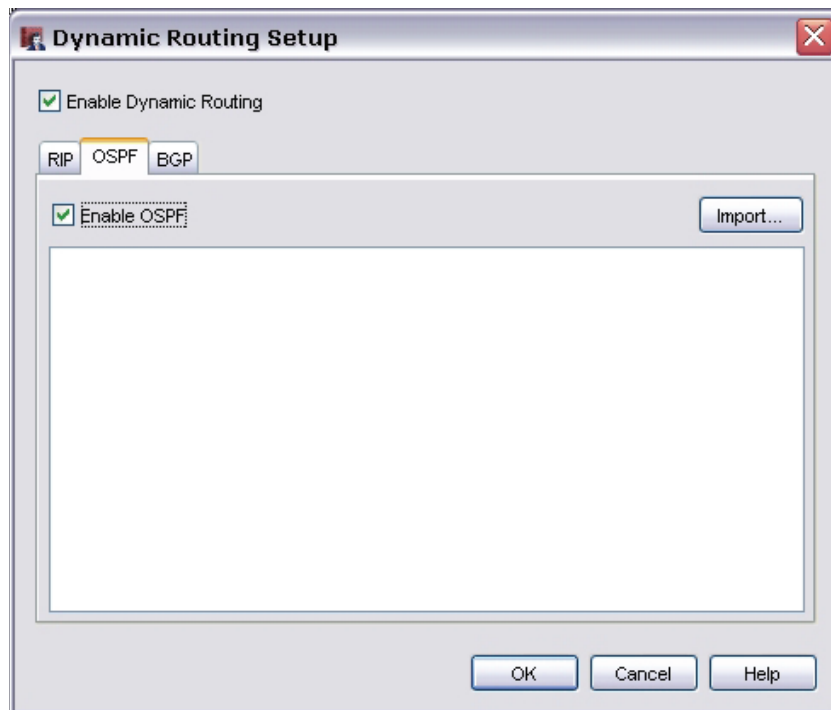
OSPF Interface Cost table

The OSPF protocol finds the most efficient route between two points. To do this, it looks at factors such as interface link speed, the number of hops between points, and other metrics. By default, OSPF uses the actual link speed of a device to calculate the total cost of a route. You can set the interface cost manually to help maximize efficiency if, for example, your gigabyte-based firewall is connected to a 100M router. Use the numbers in the OSPF Interface Cost table to manually set the interface cost to a value different than the actual interface cost.

Interface Type	Bandwidth in bit/second	Bandwidth in bytes/second	OSPF Interface Cost
Ethernet	1G	100M	1
Ethernet	100M	100M	10
Ethernet	10M	1m	100
Modem	2M	200K	500
Modem	1M	100K	1000
Modem	500K	50K	2000
Modem	250K	25K	4000
Modem	125K	12500	8000
Modem	62500	6250q	16000
Serial	115200	91=216	10850
Serial	57600	4608	21700
Serial	38400	3072	32550
Serial	19200	1636	61120
Serial	9600	768	65535

Configure the Firebox to use OSPF

1. From Policy Manager, select **Network > Dynamic Routing**.
The Dynamic Routing Setup dialog box appears.

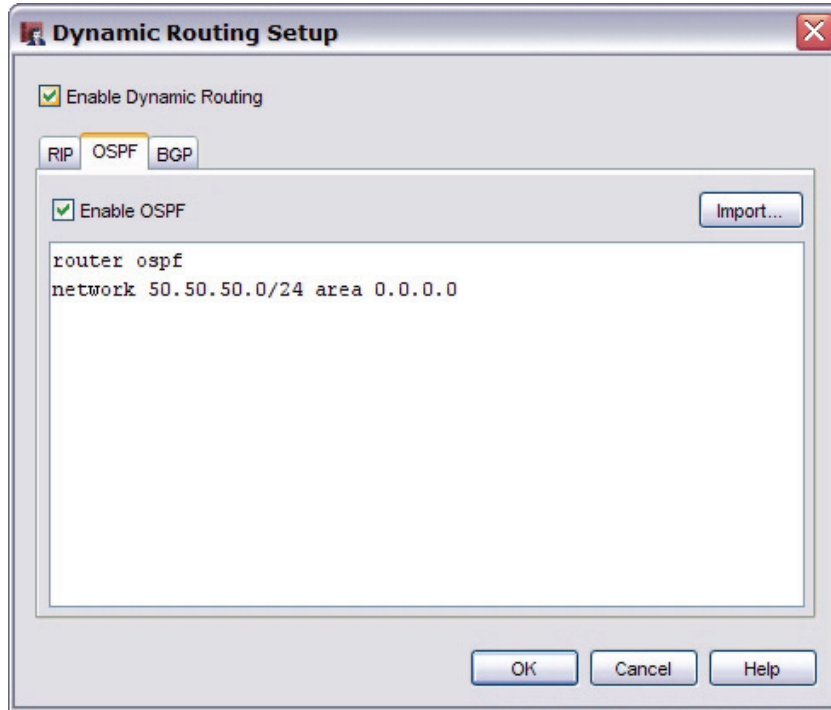


2. Click the **OSPF** tab.
3. Click **Enable Dynamic Routing** and **Enable OSPF**.

- Click **Import** to import a routing daemon configuration file, or type your configuration parameters in the text box. Click **OK**. For more information, see [About routing daemon configuration files](#). To get started, you need only two commands in your OSPF configuration file. These two commands, in this order, will start the OSPF process:

```
router ospf
```

```
network <network IP address of the interface you want the process to listen on and distribute through the protocol> area <area ID in x.x.x.x format, such as 0.0.0.0>
```



Allow OSPF traffic through the Firebox

You must add and configure a policy to allow OSPF multicasts from the routers that have OSPF enabled to the reserved multicast addresses for OSPF.

- From Policy Manager, select **Edit > Add Policies**. From the list of packet filters, select **OSPF**. Click **Add**. The *New Policy Properties* dialog box appears for OSPF.
- In the **New Policy Properties** dialog box, configure the policy to allow traffic from the IP or network address of the router using OSPF to the IP addresses 224.0.0.5 and 224.0.0.6. (For information on how to set the source and destination addresses for a policy, see [Set access rules for a policy](#).) Click **OK**.
- Finally, you must set up the router for the Firebox to talk to. After it is configured, look at the dynamic routing section of the [Firebox Status Report](#) to verify that the Firebox and the router are sending updates to each other. You can then add authentication and restrict the OSPF policy to listen only on the correct interfaces.

Sample OSPF routing configuration file

To use any of the dynamic routing protocols with Fireware, you must import or type a configuration file for the dynamic routing daemon. This topic includes a sample configuration file for the OSPF routing daemon. If you want to use this configuration file as a base for your own configuration file, copy the text into an application such as Notepad or Wordpad and save it with a new name. You can then edit the parameters to meet your own business requirements.

Optional commands are commented with the ! character. To enable a command, delete the ! and modify variables as necessary.

!! SECTION 1: Configure interface properties.

! Set properties for interface eth1.

! interface eth1

!

! Set simple authentication password (SHAREDKEY).

! ip ospf authentication-key SHAREDKEY

!

! Set MD5 authentication key ID (10) and MD5 authentication key (AUTHKEY).

! ip ospf message-digest-key 10 md5 AUTHKEY

!

! Set link cost to 1000 (1-65535) on interface eth1.

! for OSPF link cost table. !ip ospf cost 1000

!

! Set hello interval to 5 seconds (1-65535); default is 10 seconds.

! ip ospf hello-interval 5

!

! Set dead-interval to 15 seconds (1-65535); default is 40 seconds.

! ip ospf dead-interval 15

!

! Set interval between link-state advertisements (LSA) retransmissions

! to 10 seconds (1-65535); default is 5 seconds.

! ip ospf retransmit-interval 10

!

! Set LSA update interval to 3 seconds (1-3600); default is 1 second.

! ip ospf transmit-delay 3

!

! Set high priority (0-255) to increase eligibility to become the

! designated router (DR).

! ip ospf priority 255

```
!! SECTION 2: Start OSPF and set daemon properties.
! Enable OSPF daemon. Must be enabled for all OSPF configurations. router ospf
!
! Set the router ID manually to 100.100.100.20. If not set, the firewall will
! set its own ID based on an interface IP address.
! ospf router-id 100.100.100.20
!
! Enable RFC 1583 compatibility (increases probability of routing loops).
! ospf rfc1583compatibility
!
! Set area border router (ABR) type to cisco, ibm, shortcut, or standard.
! More information about ABR types is in draft-ietf-ospf-abr-alt-05.txt.
! ospf abr-type cisco
!
! Disable OSPF announcement on interface eth0.
! passive interface eth0
!
! Set global cost to 1000 (0-429495).
! auto-cost reference bandwidth 1000
!
! Set SPF schedule delay to 25 (0-4294967295) seconds and hold time to
! 20 (0-4294967295) seconds; default is 5 and 10 seconds. !timers spf 25 20
!! SECTION 3: Set network and area properties. Set areas with W.X.Y.Z
!! or Z notation.
! Announce OSPF on network 192.168.253.0/24 network for area 0.0.0.0.
! network 192.168.253.0/24 area 0.0.0.0
!
! Create area 0.0.0.1 and set a classful network range (172.16.254.0/24)
! for the area (range and interface network settings must match).
! area 0.0.0.1 range 172.16.254.0/24
!
! Set virtual link neighbor (172.16.254.1) for area 0.0.0.1.
! area 0.0.0.1 virtual-link 172.16.254.1
!
! Set area 0.0.0.1 as a stub on all routers in area 0.0.0.1.
```



```
! area 0.0.0.1 stub
!
! area 0.0.0.2 stub no-summary
!
! Enable simple password authentication for area 0.0.0.0.
! area 0.0.0.0 authentication
!
! Enable MD5 authentication for area 0.0.0.1.
! area 0.0.0.1 authentication message-digest
!! SECTION 4: Redistribute OSPF routes
! Share route of last resort (default route) from kernel routing table
! with OSPF peers.
! default-information originate
!
! Redistribute static routes to OSPF.
! redistribute kernel
!
! Redistribute routes from all interfaces to OSPF.
! redistribute connected
! redistribute connected route-map
!! Redistribute routes from RIP and BGP to OSPF.
! redistribute rip !redistribute bgp
!! SECTION 5: Configure route redistribution filters with access lists
!! and route maps.
! Create an access list to only allow redistribution of 10.0.2.0/24.
! access-list LISTNAME permit 10.0.2.0/24
! access-list LISTNAME deny any
!
! Create a route map with name MAPNAME and allow with a
priority of 10 (1-199).
! route-map MAPNAME permit 10
! match ip address LISTNAME
```

About Border Gateway Protocol (BGP)



Support for this protocol is available only in Fireware Pro.

Border Gateway Protocol (BGP) is a scalable dynamic routing protocol used on the Internet by groups of routers to share routing information. BGP uses route parameters or attributes to define routing policies and create a stable routing environment. This protocol allows you to advertise more than one path to and from the Internet to your network and resources, which gives you redundant paths and can increase your uptime.

Hosts that use BGP use TCP to send updated routing table information when one host finds a change. The host sends only the part of the routing table that has the change. BGP uses classless interdomain routing (CIDR) to reduce the size of the Internet routing tables. The size of the BGP routing table in Fireware Pro is set at 32K.

The size of the typical WatchGuard customer wide area network (WAN) is best suited for OSPF dynamic routing. A WAN can also use external border gateway protocol (EBGP) when more than one gateway to the Internet is available. EBGP allows you to take full advantage of the redundancy possible with a multi-homed network.

To participate in EBGP with an ISP you must have an autonomous system number (ASN). You must get an ASN from one of the regional registries in the table below. After you are assigned your own ASN, you must contact each ISP to get their ASNs and other necessary information.

Region	Registry Name	Web Site
North America	RIN	www.arin.net
Europe	RIPE NCC	www.ripe.net
Asia Pacific	APNIC	www.apnic.net
Latin America	LACNIC	www.lacnic.net
Africa	AfriNIC	www.afrinic.net

BGP commands

To create or modify a routing configuration file, here is a catalog of supported routing commands. The sections must appear in the configuration file in the same order they appear in this table.

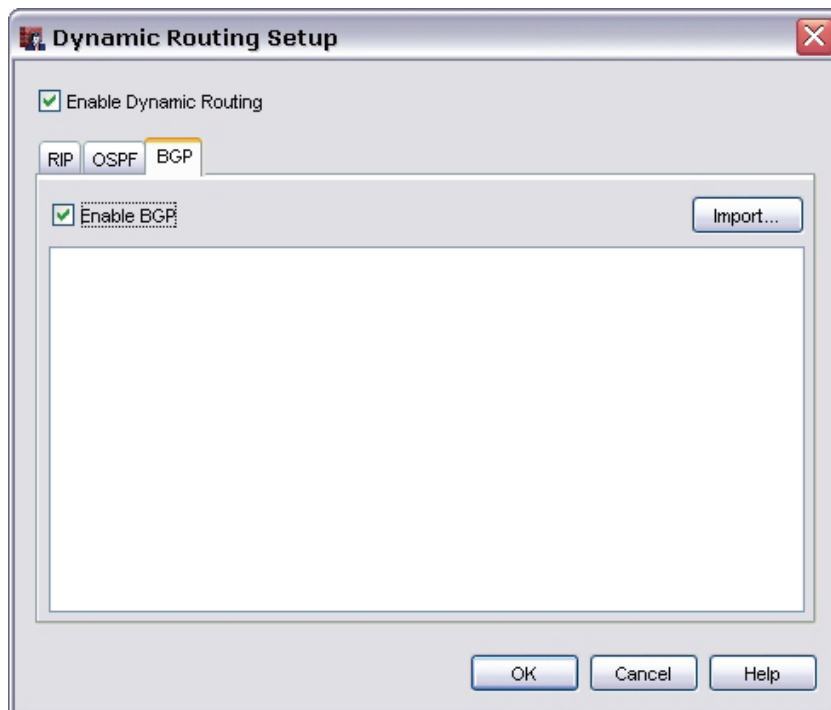
Do not use BGP configuration parameters that you do not get from your ISP.

Section	Command	Description
Configure BGP Routing Daemon		
	router bgp [ASN]	Enable BGP daemon and set autonomous system number (ASN); this is supplied by your ISP
	network [A.B.C.D/M]	Announce BGP on network A.B.C.D/M
	no network [A.B.C.D/M]	Disable BGP announcements on network A.B.C.D/M
Set Neighbor Properties		
	neighbor [A.B.C.D] remote-as [ASN]	Set neighbor as a member of remote ASN
	neighbor [A.B.C.D] ebgp-multihop	Set neighbor on another network using EBGp multi-hop
	neighbor [A.B.C.D] version 4+	Set BGP version (4, 4+, 4-) for communication with neighbor; default is 4
	neighbor [A.B.C.D] update-source [WORD]	Set the BGP session to use a specific interface for TCP connections
	neighbor [A.B.C.D] default-originate	Announce default route to BGP neighbor [A,B,C,D]
	neighbor [A.B.C.D] port 189	Set custom TCP port to communicate with BGP neighbor [A,B,C,D]
	neighbor [A.B.C.D] send-community	Set peer send-community
	neighbor [A.B.C.D] weight 1000	Set a default weight for neighbor's [A.B.C.D] routes
	neighbor [A.B.C.D] maximum-prefix [NUMBER]	Set maximum number of prefixes allowed from this neighbor
Community Lists		
	ip community-list [<1-99> <100-199>] permit AA:NN	Specify community to accept autonomous system number and network number separated by a colon

Section	Command	Description
Peer Filtering		
	neighbor [A.B.C.D] distribute-list [LISTNAME] [IN OUT]	Set distribute list and direction for peer
	neighbor [A.B.C.D] prefix-list [LISTNAME] [IN OUT]	To apply a prefix list to be matched to incoming advertisements or outgoing advertisements to that neighbor
	neighbor [A.B.C.D] filter-list [LISTNAME] [IN OUT]	To match an autonomous system path access list to incoming routes or outgoing routes
	neighbor [A.B.C.D] route-map [MAPNAME] [IN OUT]	To apply a route map to incoming or outgoing routes
Redistribute Routes to BGP		
	redistribute kernel	Redistribute static routes to BGP
	redistribute rip	Redistribute RIP routes to BGP
	redistribute ospf	Redistribute OSPF routes to BGP
Route Reflection		
	bgp cluster-id A.B.C.D	To configure the cluster ID if the BGP cluster has more than one route reflector
	neighbor [W.X.Y.Z] route-reflector-client	To configure the router as a BGP route reflector and configure the specified neighbor as its client
Access Lists and IP Prefix Lists		
	ip prefix-lists PRELIST permit A.B.C.D/E	Set prefix list
	access-list NAME [deny allow] A.B.C.D/E	Set access list
	route-map [MAPNAME] permit [N]	In conjunction with the "match" and "set" commands, this defines the conditions and actions for redistributing routes
	match ip address prefix-list [LISTNAME]	Matches the specified access-list
	set community [A:B]	Set the BGP community attribute
	match community [N]	Matches the specified community_list
	set local-preference [N]	Set the preference value for the autonomous system path

Configure the Firebox to use BGP

1. From Policy Manager, select **Network > Dynamic Routing**.
The Dynamic Routing Setup dialog box appears.



2. Click the **BGP** tab.
3. Click **Enable Dynamic Routing** and **Enable BGP**.

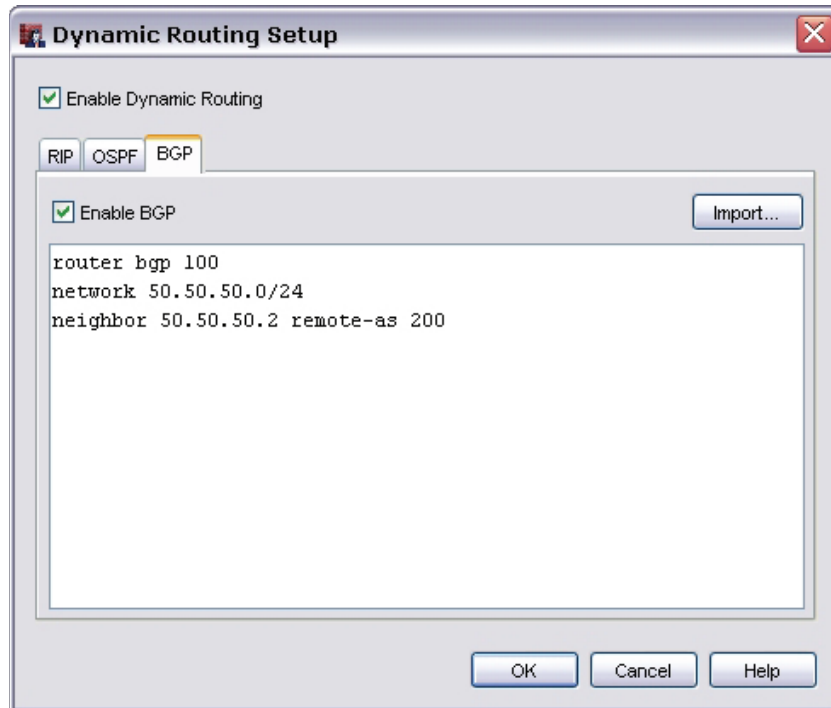
- Click **Import** to import a routing daemon configuration file, or type your configuration parameters in the text box. For more information, see [About routing daemon configuration files](#). To get started, you need only three commands in your BGP configuration file. These three commands, in this order, start the BGP process:

router BGP: BGP autonomous system number supplied by your ISP

network: network IP address that you want to advertise a route to from the Internet

neighbor: IP address of neighboring BGP router> remote-as <BGP autonomous number

With these three commands, you set up a peer relationship with the ISP and create a route for a network to the Internet.



- Click **Select a BGP Configuration** file. Click **OK**.

Allow BGP traffic through the Firebox

You must add and configure a policy to allow BGP traffic to the Firebox from the approved networks. These networks must be the same networks you defined in your BGP configuration file.

- From Policy Manager, select **Edit > Add Policies**. From the list of packet filters, select **BGP**. Click **Add**. *The New Policy Properties dialog box appears for BGP.*
- In the **New Policy Properties** dialog box, configure the policy to allow traffic from the IP or network address of the router using BGP to the Firebox interface it connects to. (For information on how to set the source and destination addresses for a policy, see [Set access rules for a policy](#).) Click **OK**.
- Finally, you must set up the router for the Firebox to talk to. After it is configured, look at the dynamic routing section of the [Firebox Status Report](#) to verify that the Firebox and the router are sending updates to each other. You can then add authentication and restrict the BGP policy to listen only on the correct interfaces.

Sample BGP routing configuration file

To use any of the dynamic routing protocols with Fireware, you must import or type a configuration file for the dynamic routing daemon. This topic includes a sample configuration file for the BGP routing daemon. If you want to use this configuration file as a base for your own configuration file, copy the text into an application such as Notepad or Wordpad and save it with a new name. You can then edit the parameters to meet your own business requirements.

Optional commands are commented with the ! character. To enable a command, delete the ! and modify variables as necessary.

```
!! SECTION 1: Start BGP daemon and announce network blocks to BGP
neighbors
! Enable BGP and set local ASN to 100 router bgp 100
! Announce local network 64.74.30.0/24 to all neighbors defined in
section 2
! network 64.74.30.0/24
!! SECTION 2: Neighbor properties
! Set neighbor (64.74.30.1) as member of remote ASN (200)
! neighbor 64.74.30.1 remote-as 200
! Set neighbor (208.146.43.1) on another network using EBGP multi-hop
! neighbor 208.146.43.1 remote-as 300
! neighbor 208.146.43.1 ebgp-multihop
! Set BGP version (4, 4+, 4-) for communication with a neighbor;
default is 4
! neighbor 64.74.30.1 version 4+
! Announce default route to BGP neighbor (64.74.30.1)
! neighbor 64.74.30.1 default-originate
! Set custom TCP port 189 to communicate with BGP neighbor
(64.74.30.1). Default port is TCP 179
! neighbor 64.74.30.1 port 189
! Set peer send-community
! neighbor 64.74.30.1 send-community
! Set a default weight for neighbor's (64.74.30.1) routes
! neighbor 64.74.30.1 weight 1000
! Set maximum number of prefixes allowed from this neighbor
! neighbor 64.74.30.1 maximum-prefix NUMBER
!! SECTION 3: Set community lists
! ip community-list 70 permit 7000:80
!! SECTION 4: Announcement filtering
! Set distribute list and direction for peer
! neighbor 64.74.30.1 distribute-list LISTNAME [in|out]
! To apply a prefix list to be matched to incoming or outgoing
advertisements to that neighbor
! neighbor 64.74.30.1 prefix-list LISTNAME [in|out]
! To match an autonomous system path access list to incoming or
outgoing routes
```

```
! neighbor 64.74.30.1 filter-list LISTNAME [in|out]
! To apply a route map to incoming or outgoing routes
! neighbor 64.74.30.1 route-map MAPNAME [in|out]
!! SECTION 5: Redistribute routes to BGP
! Redistribute static routes to BGP
! Redistribute kernel
! Redistribute rip routes to BGP
! Redistribute rip
! Redistribute ospf routes to BGP
! Redistribute ospf
!! SECTION 6: Route reflection
! Set cluster ID and firewall as a client of route reflector server
51.210.0.254
! bgp cluster-id A.B.C.D
! neighbor 51.210.0.254 route-reflector-client
!! SECTION 7: Access lists and IP prefix lists
! Set prefix list
! ip prefix-list PRELIST permit 10.0.0.0/8
! Set access list!access-list NAME deny 64.74.30.128/25
! access-list NAME permit 64.74.30.0/25
! Create a route map with name MAPNAME and allow with a priority of 10
! route-map MAPNAME permit 10
! match ip address prefix-list LISTNAME
! set community 7000:80
```


31 Traffic Management and Quality of Service

About Traffic Management and QoS



To use the features described in this chapter, you must have Fireware Pro installed on your Firebox.

In a large network with many computers, the volume of data that moves through the firewall can be very large. A network administrator can use Traffic Management and Quality of Service (QoS) actions to prevent data loss for important business applications and to make sure mission-critical applications take priority over other traffic.

Traffic Management and QoS provide a number of benefits. You can:

- Guarantee or limit bandwidth
- Control the rate at which the Firebox sends packets to the network
- Prioritize when to send packets to the network

To apply traffic management to policies, you define a Traffic Management action, which is a collection of settings that you can apply to one or more policy definitions. This way you do not need to configure the traffic management settings separately in each policy. You can define additional Traffic Management actions if you want to apply different settings to different policies.

Guarantee bandwidth

Bandwidth reservation prevents connection timeouts. A traffic management queue with reserved bandwidth and low priority can give bandwidth to real-time applications with higher priority when necessary without disconnecting. Other traffic management queues can take advantage of unused reserved bandwidth when it becomes available.

For example, suppose your company has an FTP server on the external network and you want to guarantee that FTP always has at least 200 Kilobytes per second through the external interface. You might also consider setting a minimum bandwidth from the trusted interface to make sure that the connection has end-to-end guaranteed bandwidth. To do this, you would create a Traffic Management action that defines a minimum of 200 kbps for FTP traffic on the external interface. You would then create an FTP policy and apply the Traffic Management action. This will allow ftp put at 200 kbps. If you want to allow ftp get at 200 kbps, you must configure the FTP traffic on the trusted interface to also have a minimum of 200 kbps.

As another example, suppose your company uses multimedia materials (streaming media) for training external customers. This streaming media uses RTSP over port 554. You have frequent FTP uploads from the trusted to external interface, and you do not want these uploads to compete with your customers receiving streaming media. You would apply a Traffic Management action to the external interface for the streaming media port to guarantee sufficient bandwidth.

Restrict bandwidth

The guaranteed bandwidth setting works with another setting configured for each external interface, **Outgoing Interface Bandwidth**, to make sure you do not guarantee more bandwidth than actually exists. This setting also helps you make sure the sum of guaranteed bandwidth settings does not fill the link such that non-guaranteed traffic cannot pass. For example, suppose the link is 1 Mbps and you try to use a Traffic Management action that guarantees 973 Kbps (0.95 Mbps) to the FTP policy on that link. With these settings, the FTP traffic could prevent other types of traffic from using the interface. If you try to configure the Firebox this way, Policy Manager warns you that you are approaching the Outgoing Interface Bandwidth setting for that interface.

QoS Marking

QoS Marking creates different classes of service for different kinds of outbound network traffic. When you mark traffic, you change up to six bits on packet header fields defined for this purpose. QoS-capable external devices can make use of this marking and provide appropriate handling of a packet as it travels from one point to another in a network.

You can use QoS Marking on a per-interface or per-policy basis. When you define QoS Marking for an interface, packets leaving that interface are marked. QoS Marking for a policy marks traffic that uses the policy.

Traffic priority

You can assign different levels of priority either to policies or for traffic from a particular interface. Traffic prioritization at the firewall allows you to manage multiple class of service (CoS) queues and reserve the highest priority for real-time or streaming data. A policy with high priority can take bandwidth away from existing low priority connections when the link is congested and traffic is competing for bandwidth.

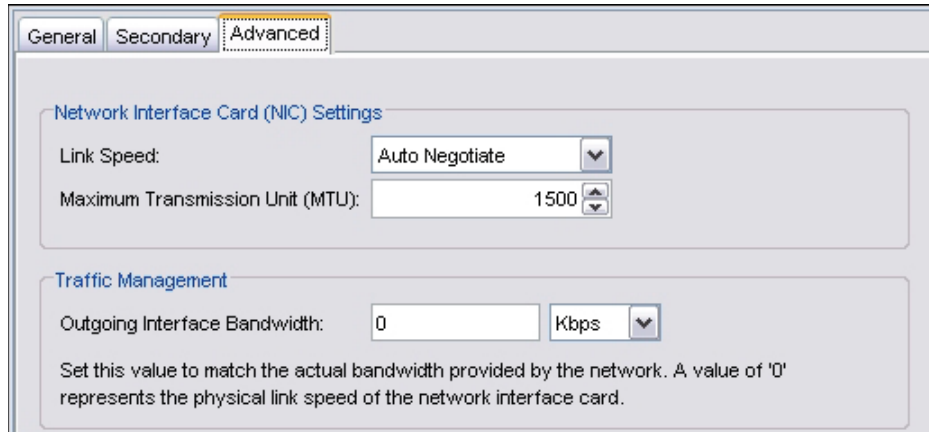
Set Outgoing Interface Bandwidth

Before you use Traffic Management features, you must give each interface a bandwidth limit, known as Outgoing Interface Bandwidth, for traffic sent from that interface to the network segment to which it is connected. After you set this limit, Firewall will refuse packets that exceed the limit. Also, Policy Manager gives a warning if you allocate too much bandwidth as you create or adjust traffic management actions.

If you keep the Outgoing Interface Bandwidth setting for any interface at its default value of 0, it is set to the auto-negotiated link speed for that interface.

1. From Policy Manager, select **Setup > Global Settings**.
The Global Settings dialog box appears.
2. At the bottom of the dialog box, make sure the **Disable all traffic management and QoS features** check box is cleared. If it is not, clear it.
3. Click **OK**.
You might want to disable these features at a later time if you do performance testing or network debugging.
4. From Policy Manager, select **Network > Configuration**.
The Network Configuration dialog box appears.

5. Select the interface for which you want to set bandwidth limits and click **Configure**.
The Interface Settings dialog box appears.
6. Click the **Advanced** tab.



The screenshot shows the 'Advanced' tab of the 'Interface Settings' dialog box. It contains two main sections: 'Network Interface Card (NIC) Settings' and 'Traffic Management'. In the NIC settings, 'Link Speed' is set to 'Auto Negotiate' and 'Maximum Transmission Unit (MTU)' is set to '1500'. In the Traffic Management section, 'Outgoing Interface Bandwidth' is set to '0' Kbps. A note below this field states: 'Set this value to match the actual bandwidth provided by the network. A value of '0' represents the physical link speed of the network interface card.'

7. In the **Outgoing Interface Bandwidth** field, enter the amount of bandwidth provided by the network. Use your Internet connection upload speed (in Kbps rather than KBps) as the limit for external interfaces. Set your LAN interface bandwidth based on the minimum link speed supported by your LAN infrastructure.

Define a Traffic Management action

Traffic Management actions can enforce an absolute maximum connection rate and bandwidth for groups of policies. Traffic Management actions can also guarantee minimum bandwidth for groups of policies per interface. This allows you to control how much bandwidth is reserved for connections from trusted to external independently from those between trusted and optional where more bandwidth might be available.

Determine available bandwidth

Before you begin, you must determine the available bandwidth of the interface used for the policy or policies you want to guarantee bandwidth. For external interfaces, you can contact your ISP to verify the service level agreement for bandwidth. You can then use a speed test with online tools to verify this value (do an Internet search for speed test). Note, however, that these tools can produce different values depending on a number of variables. For other interfaces, you can assume the link speed on the Firebox interface is the theoretical maximum bandwidth for that network. You must also consider both sending and receiving needs of an interface and set the threshold value based on these needs. If your ISP is asymmetric, use the uplink bandwidth as the threshold value.

Determine sum of bandwidth

You must also determine the sum of the bandwidth you want to guarantee for all policies on a given interface. On a 1500 Kbps external interface, you might want to, for example, reserve 600 Kbps for all the guaranteed bandwidth and use the remaining 900 Kbps for all other traffic.

All policies that use a given Traffic Management action share its connection rate and bandwidth settings. When they are created, policies automatically belong to the default Traffic Management action, which enforces no restrictions or reservations. If you create a Traffic Management action to set a maximum bandwidth of 10 Mbps and apply it to an FTP and an HTTP policy, all connections handled by those policies must share 10Mbps. If you later apply the same Traffic Management action to a Citrix policy, all three must share 10 Mbps. This logic applies to connection rate limits and guaranteed minimum bandwidth as well. Unused guaranteed bandwidth reserved by one Traffic Management action can be used by others.

1. From Policy Manager, select **Setup > Actions > Traffic Management** and click **Add**.
or

From Policy Manager, double-click the icon of the policy for which you want to guarantee a minimum bandwidth. Click the **Advanced** tab. Click the New/Clone Traffic Management icon to the far right of **Traffic Management**.

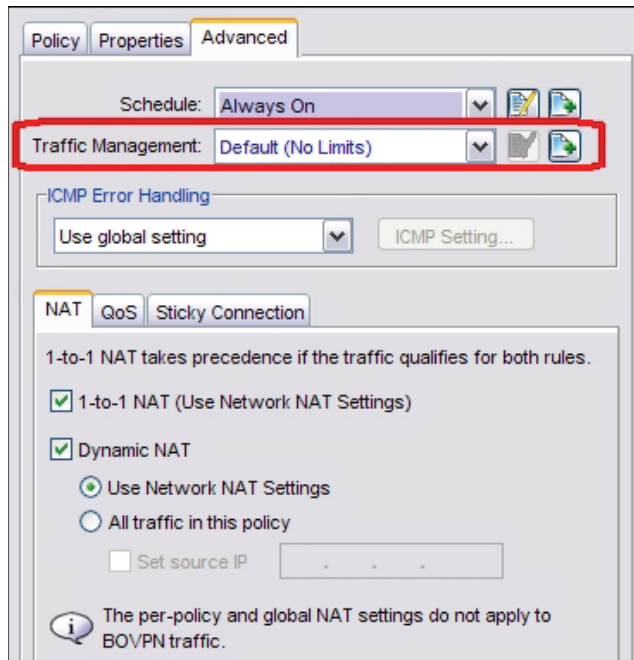
The New Traffic Management Action Configuration dialog box appears.

2. In the **Guaranteed Minimum Bandwidth** box, click **Add**.
3. Under **Outgoing Interface**, select the interface for which you want to set a minimum bandwidth.
4. Under **Minimum Bandwidth**, set the minimum Kilobytes per second through that interface. Click **OK**.
5. If you started defining the traffic action from a policy definition, the new traffic action now appears in **Traffic Management** on the **Advanced** tab. If you started defining the traffic actions from selecting **Setup > Actions > Traffic Management**, you must [Apply a Traffic Management action to a policy](#) for it to take effect on your network.

Apply a Traffic Management action to a policy

After you have created Traffic Management actions, or if actions have already been created on the Firebox, you can apply them to the policies you have configured in Policy Manager. To apply a Traffic Management action:

1. From Policy Manager, double-click the icon of the policy for which you want to guarantee a minimum bandwidth. Click the **Advanced** tab.
2. From the **Traffic Management** drop-down list, select a Traffic Management action to apply to the policy.



3. Click **OK** to close the **Edit Policy Properties** dialog box. Save your changes to the Firebox. You will get a warning message if the sum of all guaranteed bandwidths for an interface approaches or exceeds the bandwidth limit you set for the interface.
The new action appears in the Traffic Management Actions dialog box.

If you want to track the bandwidth being used by a policy, go to the **Service Watch** tab of Firebox System Manager and specify **Bandwidth** instead of **Connections**. For more information, see [Visual display of policy usage](#).

Use Traffic Management actions in a multi-WAN environment

When a Traffic Management action is applied on a multiple WAN policy with the multi-WAN feature set up in round-robin mode, the maximum bandwidth and connection rate settings in the Traffic Management action control the total throughput and connection rate across all interfaces. This includes all external interfaces that are configured to route traffic.

Apply a Traffic Management action to multiple policies

When the same Traffic Management action is applied to multiple policies, the connection rate, maximum bandwidth, and minimum bandwidth apply to all traffic that matches each policy. If two policies share an action that has a maximum bandwidth of 100 kbps, then all traffic that matches those policies will be limited to 100 kbps. Each policy will not get 100 kbps; they get 100 kbps combined.

If you have limited bandwidth on an interface used for several applications, each using unique ports, you might need all the high priority connections to share one Traffic Management action. If you have lots of bandwidth to spare, you could create separate Traffic Management actions for each application.

Set traffic priority in a policy

Many different algorithms can be used to prioritize network traffic. Fireware uses a high performance, class-based queuing method based on the Hierarchical Token Bucket algorithm. Prioritization in Fireware is applied per policy and is equivalent to CoS (class of service) levels 0 to 7 where 0 is normal priority (default) and 7 is the highest priority. Use the table below as a guideline when you assign priorities. Level 5 is commonly used for streaming data such as VoIP or video conferencing. Reserve levels 6 and 7 for policies that allow system administration connections to make sure they are always available and avoid interference from other high priority network traffic.

Priority	Description
0	Routine (HTTP, FTP)
1	Priority
2	Immediate (DNS)
3	Flash (Telnet, SSH, RDP)
4	Flash Override
5	Critical (VoIP)
6	Internetwork Control (Remote router configuration)
7	Network Control (Firewall, router, switch management)

To configure traffic priority for a policy:

1. From the **Edit Policy Properties** dialog box, click the **Advanced** tab.

The screenshot shows the 'Edit Policy Properties' dialog box with the 'Advanced' tab selected. The 'QoS Marking' section has 'Override per-interface settings' checked, with 'Marking Type' set to 'DSCP', 'Marking Method' set to 'Preserve', and 'Value' set to '0 (Best Effort)'. The 'Traffic Priority' section also has 'Override per-interface settings' checked, with 'Prioritize Traffic Based On' set to 'Custom Value' and 'Value' set to '0 (Normal)'.

2. Firebox interfaces may be defined to prioritize traffic based on QoS Marking. You must override any per-interface QoS Marking if you want to set traffic priority in a policy. To do this, select the **Override per-interface settings** check box.
3. From the drop-down list next to **Prioritize Traffic Based On**, select **Custom Value**.
4. From the **Value** drop-down list, select a priority level. Use the table in this section as a guide. Click **OK**.

Set connection and bandwidth limits

You can define an alarm to occur when network capacity is exceeded according to the parameters that you specify. You can configure the alarm to make the Firebox send an event notification to the SNMP management system, or to send a notification in the form of an email message or a pop-up window on the management station.

1. Start to define the Traffic Management action, as described in steps 1 and 2 of [Define a Traffic Management action](#).
2. Use the **Connection Rate** drop-down list to set a maximum number of connections per second that can occur before Traffic Management actions start. The default configuration puts no limits on the connection rate. If you select **Custom**, you can type the maximum connection rate. When this limit is reached, the Traffic Management action starts.
3. If you want to receive a notification when the connection rate is exceeded, select the **Alarm when capacity exceeded** check box. Click **Notification** and set the notification parameters, as described in [Set logging and notification preferences](#).
4. Use the **Maximum Bandwidth** drop-down list to set or remove the bandwidth limits for this action. Use **No Limit** to remove bandwidth restrictions for important traffic, or select a maximum kilobytes per second bandwidth. When the maximum bandwidth limit is reached, the extra traffic will be dropped and a log message will be shown in Traffic Monitor.
5. Click **OK**.
The new action appears in the Traffic Management Actions dialog box.
6. If you started defining the Traffic Management action from a policy definition, the new action now appears in **Traffic Management** on the **Advanced** tab. If you started to define the action from selecting **Setup > Actions > Traffic Management**, you must apply the setting to a policy, as explained in [Apply the Traffic Management action to a policy](#).

About QoS Marking

Today's networks often consist of many kinds of network traffic that compete for bandwidth. All traffic, whether of prime importance or negligible importance, has an equal chance of reaching its destination in a timely manner. Quality of Service (QoS) Marking gives critical traffic preferential treatment to make sure it is delivered quickly and reliably.

QoS functionality must be able to differentiate the various types of data streams that flow across your network. It must then mark data packets. The Firewall feature called QoS Marking creates different classifications of service for different kinds of network traffic. When you mark traffic, you change up to six bits on packet header fields defined for this purpose. The Firewall and other QoS-capable external devices can make use of this marking and provide appropriate handling of a packet as it travels from one point to another in a network.

Firewall supports two types of QoS Marking: IP Precedence marking (also known as Class of Service) and Differentiated Service Code Point (DSCP) marking. For more information on these types, see [Marking types and values](#).

Before you begin

- Make sure your LAN equipment supports QoS Marking and handling. You might also need to make sure your ISP supports QoS.
- The use of QoS 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.

Per-interface and per-policy QoS Marking

You can use Quality of Service Marking on a per-interface or per-policy basis. When you define QoS Marking for an interface, packets leaving that interface are marked. QoS Marking for a policy marks traffic that uses the policy. The QoS Marking for a policy overrides any QoS Marking set on an interface.

For example, suppose your Firewall receives QoS-marked traffic from the external network and sends it to the trusted network. However, you want only the traffic to your executive team from external to trusted to be differentiated by QoS Marking. You set the QoS Marking for the trusted interface to **Clear**. Then, you add a policy with QoS Marking set for the traffic to your executive team.

QoS Marking and IPSec traffic

If you want to apply QoS to IPSec traffic, you must create a specific firewall policy for the corresponding IPSec policy and apply QoS Marking to that policy.

Consider also the setting of the **Enable TOS for IPSec** check box in the **VPN Settings** dialog box. If you select this check box, any existing marking is preserved when the packet is encapsulated in an IPSec header. If the check box is cleared, the TOS bits are reset and no marking is preserved.

Marking types and values

Fireware supports two types of QoS Marking: IP Precedence marking (also known as Class of Service) and Differentiated Service Code Point (DSCP) 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. Both methods allow you to either preserve the bits in the header, which may have been marked previously by an external device, or change them 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. Fireware DSCP marking supports three 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 QoS Marking.
- **Assured Forwarding (AF)**
Assured Forwarding 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.

Within the Assured Forwarding (AF) type of per-hop behavior, traffic can be assigned to three classes: Low, Medium, and High.

Class-Selector (CSx) code points are defined to be backward compatible with IP Precedence values. CS1 through CS7 are identical to IP Precedence values 1 through 7.

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*
10		AF Class 1 - Low
12		AF Class 1 - Medium
14		AF Class 1 - High
16	2	
18		AF Class 2 - Low
20		AF Class 2 - Medium
22		AF Class 2 - High
24	3	
26		AF Class 3 - Low
28		AF Class 3 - Medium
30		AF Class 3 - High
32	4	
34		AF Class 4 - Low
36		AF Class 4 - Medium
38		AF Class 4 - High
40	5	
46		EF
48	6	Internet Control
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 the following RFC <http://www.rfc-editor.org/rfc/rfc2474.txt>.

Enable QoS Marking for an interface

Use this procedure to set the default marking behavior as traffic goes out of an interface. These settings can be overridden by settings defined for a policy.

1. From Policy Manager, select **Setup > Global Settings**.
The Global Settings dialog box appears.
2. At the bottom of the dialog box, clear the **Disable all traffic management and QoS features** check box and click **OK**.
You might want to disable these features at a later time if you do performance testing or network debugging.
3. From Policy Manager, select **Network > Configuration**.
The Network Configuration dialog box appears.
4. Select the interface for which you want to enable QoS Marking and click **Configure**.
The Interface Settings dialog box appears.
5. Click the **Advanced** tab.

The screenshot shows the 'Advanced' tab of the 'Interface Settings' dialog box. It contains three main sections: 'Network Interface Card (NIC) Settings', 'Traffic Management', and 'QoS'. The 'QoS' section is expanded, showing 'Marking Type' as 'IP Precedence', 'Marking Method' as 'Preserve', and 'Value' as '0 (Normal)'. There is an unchecked checkbox for 'Prioritize traffic based on QoS Marking'.

6. From the **Marking Type** drop-down list, select either **DSCP** or **IP Precedence**.
7. Set the marking method:
 - o **Preserve**: Do not change the bit's current value. The Firebox prioritizes the traffic based on this value.
 - o **Assign**: Assign the bit a new value.
 - o **Clear**: Clear the bit (set it to zero).
8. If you selected **Assign** in the previous step, select a marking value. If you chose the IP precedence marking type you can select values from 0 (normal priority) through 7 (highest priority). If you selected the DSCP marking type, the values are 0 - 56.
For more information on these values, see [Marking types and values](#).
9. Select the **Prioritize traffic based on QoS Marking** check box.
10. Click **OK**.

Enable QoS Marking for a policy

In addition to marking the traffic that leaves a Firebox interface, you can also mark traffic on a per-policy basis. The marking action you select is applied to all traffic that uses the policy. Multiple policies that use the same marking actions have no effect on each other.

1. From Policy Manager, select **Setup > Global Settings**.
The Global Settings dialog box appears.
2. At the bottom of the dialog box, clear the **Disable all traffic management and QoS features** check box. Click **OK**.
3. From Policy Manager, double-click the icon for the policy whose traffic you want to mark.
The Edit Policy Properties dialog box appears.
4. Click the **Advanced** tab. Click the **QoS** tab halfway down the dialog box.

The screenshot shows the 'QoS' tab in a configuration window. It has three sub-tabs: 'NAT', 'QoS', and 'Sticky Connection'. The 'QoS' sub-tab is active. It contains two main sections: 'QoS Marking' and 'Traffic Priority'. In the 'QoS Marking' section, the 'Override per-interface settings' checkbox is checked. Below it, 'Marking Type' is a dropdown menu set to 'DSCP', 'Marking Method' is a dropdown menu set to 'Preserve', and 'Value' is a dropdown menu set to '0 (Best Effort)'. In the 'Traffic Priority' section, the 'Override per-interface settings' checkbox is also checked. Below it, 'Prioritize Traffic Based On' is a dropdown menu set to 'Custom Value', and 'Value' is a dropdown menu set to '0 (Normal)'.

5. Firebox interfaces can have their own QoS Marking settings. To enable QoS Marking for a policy, you must override any per-interface QoS Marking. To do this, select the **Override per-interface settings** check box.
6. From the **Marking Type** drop-down list, select either **DSCP** or **IP Precedence**.
7. Set the marking method:
 - o **Preserve:** Do not change the bit's current value. The Firebox prioritizes the traffic based on this value.
 - o **Assign:** Assign the bit a new value.
 - o **Clear:** Clear the bit (set it to zero).
8. If you selected **Assign** in the previous step, select a marking value. If you chose the IP precedence marking type you can select values from 0 (normal priority) through 7 (highest priority). If you selected the DSCP marking type, the values are 0 - 56. For more information on these values, see [Marking types and values](#). We recommend that you assign a priority higher than 5 only to WatchGuard administrative policies, such as the WatchGuard policy, the WG-Logging policy, or the WG-Mgmt-Server policy. Give high priority business traffic a priority of 5 or lower.

32 High Availability

About WatchGuard High Availability



To use the features described in this chapter, you must have Fireware Pro installed on your Firebox.

High Availability (HA) refers to the ability of a network to operate when hardware or software fails. When you add redundancy to your network, you remove one point of vulnerability.

The WatchGuard High Availability feature enables the installation of two Firebox devices in a failover configuration. The configuration includes one Firebox we identify as the primary device and the other we identify as the secondary device. One of these devices is always in active mode and the other in standby mode. These two Fireboxes are known as peers. They constantly send messages to each other to communicate their status.

HA failover occurs when the internal heartbeat is lost or when an HA-monitored physical interface is down. When a failover event occurs, the standby system becomes active. After a Firebox becomes active, it stays active until it goes offline and the standby Firebox starts as the active unit.

When High Availability is enabled, WSM continues to support:

- Secondary networks on external, trusted, or optional interfaces
- Multi-WAN connections
(Limitation: a multi-WAN failover caused by a failed connection to a link monitor host does not trigger HA failover. HA failover occurs only when the physical interface is down or does not respond. HA failover takes precedence over multi-WAN failover.)
- VLANs

When High Availability is enabled, the following connections are disconnected when a failover event occurs:

- Mobile VPN with PPTP
- Mobile VPN with IPSec
- Mobile VPN with SSL

Users must manually reestablish these connections after a failover.

When a High Availability Firebox becomes active, its non-HA interfaces get a new MAC address with the format 00:00:5E:00:01:xy. The non-HA interfaces of the standby Firebox keep their original MAC addresses, which start with 00:90:7F.

High Availability requirements and restrictions

Make sure you understand these requirements and restrictions before you begin:

- The two Fireboxes in an HA configuration must be the same model and must use the same software version. If the software versions are different, you must upgrade the Firebox with the old version to match the other Firebox. The Firebox with the old software must have a license for the upgraded software.
- You must define one Firebox in the pair as the primary and the other as the secondary Firebox. We recommend that you select the Firebox with the most features as the primary Firebox. If you purchase an upgrade for your High Availability pair, you must apply the upgrade to the serial number of the primary Firebox when you activate the upgrade on the LiveSecurity web site. Both Fireboxes in the High Availability pair will use the licensed features of the primary Firebox.
- Each active interface on the primary HA Firebox must connect to the same hub or switch as its matching active interface on the secondary HA Firebox.
- You cannot use DHCP Server or DHCP Relay on any interface in which HA is enabled.



High availability requires an interface or interfaces dedicated specifically for HA synchronization.

About High Availability and proxy sessions

When High Availability is activated and a failover event occurs, all outgoing TCP sessions are disconnected. Users must manually reestablish all interactive or persistent sessions. This is because proxy session state is not retained between HA peers. Consider adding specific packet filter policies to your configuration for telnet, ssh, or any other policy for which you want failover. Note that Intrusion Prevention Service (IPS) does not operate with these new policies.

If you use proxy policies with signature-based Gateway AV/IPS and a failover event occurs, the standby Firebox becomes the active Firebox and automatically checks for signature updates.

About High Availability and server load balancing

If you use High Availability and server load balancing, no real-time synchronization occurs when a failover event occurs. The secondary Firebox sends connections to all servers in the server load balancing list to see which servers are available. It then applies the server load balancing algorithm to all available servers.

High Availability status

To see the status of High Availability in Firebox System Manager, [start Firebox System Manager](#) and find the High Availability information on the right portion of the window, as described in [Firebox status](#).

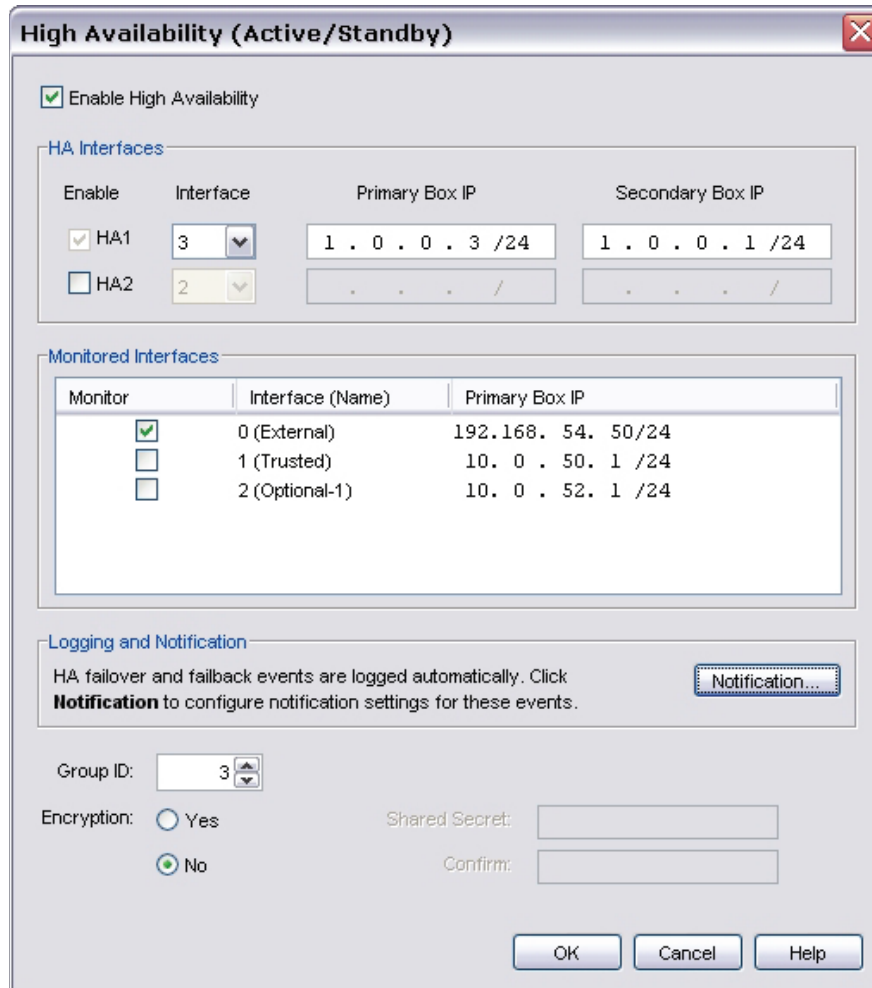
Install High Availability

When you purchase the High Availability upgrade, you receive a certificate. To install High Availability:

1. Use the instructions on the certificate to go to the LiveSecurity Service web site and activate your upgrade. After you activate the upgrade, you get a High Availability feature key.
2. [Import the feature key to the Firebox](#). We recommend you use the Firebox with the most features as the primary Firebox. Both Fireboxes in the High Availability pair will use the license features of the primary Firebox.

Configure High Availability

1. If you have not done so already, [install High Availability](#).
2. From Policy Manager, select **Network > High Availability**.
The *High Availability* dialog box appears.



High Availability (Active/Standby)

☒ Enable High Availability

HA Interfaces

Enable	Interface	Primary Box IP	Secondary Box IP
<input checked="" type="checkbox"/> HA1	3	1 . 0 . 0 . 3 /24	1 . 0 . 0 . 1 /24
<input type="checkbox"/> HA2	2	. . . /	. . . /

Monitored Interfaces

Monitor	Interface (Name)	Primary Box IP
<input checked="" type="checkbox"/>	0 (External)	192.168. 54. 50/24
<input type="checkbox"/>	1 (Trusted)	10. 0 . 50. 1 /24
<input type="checkbox"/>	2 (Optional-1)	10. 0 . 52. 1 /24

Logging and Notification

HA failover and failback events are logged automatically. Click **Notification** to configure notification settings for these events.

Group ID: 3

Encryption: ☐ Yes ☒ No

Shared Secret:

Confirm:

OK Cancel Help

3. Select the **Enable High Availability** check box.

Define HA interfaces

1. The **HA1** check box is automatically selected when you enable High Availability. If you want to change the interface you use for HA1, select an interface number from the **Interface** drop-down list.
2. In the **Primary Box IP** text box, you can change the default IP address. This IP address should be from a reserved or unassigned network. This becomes the permanent IP address for that interface. We recommend that you select the Firebox with the most features as the primary Firebox.
3. In the **Secondary Box IP** text box, type an IP address from the same subnet as the interface with High Availability enabled on the active Firebox.
4. Select the **HA2** check box if you want to enable the HA2 interface.
The HA2 interface is optional.

Select interfaces to be monitored

In the **Monitor Interfaces** box, you can select the interfaces you want to monitor for physical link status. The Firebox monitors the selected interfaces and, if the interface is not active, starts an HA failover. Select the check box adjacent to the interface name to enable monitoring. Clear the check box adjacent to the interface name to turn off monitoring of an interface. We recommend that you monitor all enabled interfaces.

Define notification

High Availability events are always logged. If you want to configure notification settings for HA failover and failback events, select **Notification**. For information on this dialog box, see [Set logging and notification preferences](#).

Define HA Group ID and encryption settings

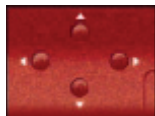
1. Use the **Group ID** value control to identify this HA group on the network. If you use more than one HA pair on the same network, this number must be different for each pair.
2. Click the **Yes** radio button to encrypt all HA traffic between the Fireboxes. This is usually not necessary, and uses more resources.
or
Click the **No** radio button to not encrypt HA traffic between the Fireboxes.
3. If you selected **Yes** to encrypt HA traffic, in the **Shared Secret** field, type a shared secret to encrypt HA traffic between the Fireboxes. Type the shared secret again in the **Confirm** field.

Finish the configuration

1. [Save the configuration file](#) to the active Firebox.
2. Close Policy Manager.

Set up hardware for HA

1. Use a crossover cable to connect the HA1 interface on one Firebox to the HA1 interface on the other Firebox. If HA2 is enabled, connect both HA2 interfaces as well.
2. Put the secondary unit in safe mode. To do this:
If your device is a Firebox X Core or Peak e-Series device, turn the Firebox off, and then turn it back on while you press and hold the down arrow button on the Firebox front panel.
If your device is a Firebox X Core or Peak (not an e-Series device), turn the Firebox off, and then turn it back on while you press and hold the up arrow button on the Firebox front panel.



Synchronize the configuration

1. [Start Firebox System Manager](#) and connect to the primary Firebox.
2. Select **Tools > High Availability > Synchronize Configuration**. When prompted, type the configuration passphrase.
You see a message that says High Availability is enabled.

Create a backup image of a Firebox in an HA pair

When a Firebox is in a High Availability pair, you can back up the flash image of the Firebox only when it is the active Firebox. To create a backup image (.fxi) of the active Firebox:

1. From Policy Manager, select **File > Backup**.
2. Type the configuration passphrase. Click **OK**.
3. Type and confirm an encryption key. This key is used to encrypt the backup file. Use a strong encryption key that is easy to remember.
4. Browse or type the location for the backup file. Click **OK**.
The backup file is created.
5. Click **OK** when the backup is finished.

Manually control High Availability

Although High Availability operations usually occur automatically, you can do some of the functions manually from Firebox System Manager if you prefer this method, or if you are troubleshooting a technical problem. Before you can use these procedures, you must [start Firebox System Manager](#).

Enabling the current Firebox as a standby peer

To manually make the current Firebox the standby peer in a High Availability configuration:
From Firebox System Manager, select **Tools > High Availability > Enable as Secondary**.

Synchronizing the configuration

You must synchronize the configuration when one Firebox configuration changes while the other is disconnected from the HA peer or turned off.
From Firebox System Manager, select **Tools > High Availability > Synchronize Configuration**.

Forcing a failover

You can cause a failover to occur on the current Firebox. The peer becomes active immediately and the current Firebox becomes standby.
From Firebox System Manager, select **Tools > High Availability > Force Failover**.

Forcing a failover and transferring management to peer

The **Force Admin** option is similar to **Force Failover** except that it transfers the management of High Availability from the current Firebox to the peer. The current Firebox is put into a state where it cannot become active. If the peer is available, the peer becomes active. The current Firebox cannot become active again unless you restart it (or the active Firebox issues the **Restart Peer** command) and then a failover occurs or you force a failover back to the original Firebox.
From Firebox System Manager, select **Tools > High Availability > Force Admin**.

Restarting the peer

When you connect to an HA configuration, you communicate only to the active Firebox. To restart the peer Firebox, you must send the command from the active Firebox:
From Firebox System Manager, select **Tools > High Availability > Restart Peer**.



When the Firebox is in a high CPU or traffic condition and you use Firebox System Manager to control HA operations, you might get an incorrect timeout message. In this case, the operation might have actually finished, and the timeout message is not valid.

Upgrade software in an HA configuration

If you install the software on the active Firebox, the standby Firebox in the High Availability configuration does not automatically upgrade. You must upgrade each Firebox. You cannot upgrade the software on a Firebox that is in standby mode.

1. Upgrade the active Firebox.
The Firebox restarts when the upgrade is complete. When this occurs, the standby Firebox becomes the active Firebox.
2. Upgrade the Firebox that is now active (previously the standby Firebox).

33 WatchGuard File Locations

Locations of WatchGuard System Manager files

The table below gives the locations where common data files are kept by the WatchGuard System Manager software. Because it is possible to configure the Windows operating system (OS) to put these directories on different disk drives, you must know the correct location of these files based on the configuration of Windows on your computer. It is also possible to configure log files to be kept in a different directory than other installation files. If you change the default location of log files, these default locations do not apply. If you are using an OS version that is not English, you must translate directory names (such as Documents and Settings or Program Files) to match the OS language you use.

File Type	Location
User-created data	
User-created data (shared)	C:\Documents and Settings\All Users\Shared WatchGuard
Certificates	My Documents\My WatchGuard\certs\<IP Address of Management Server>
WatchGuard applications	C:\Program Files\WatchGuard\wsm10.0
Shared application libraries	C:\Program Files\Common Files\WatchGuard\wsm10
Management Server data	C:\Documents and Settings\WatchGuard\wmserver
Quarantine Server data	C:\Documents and Settings\WatchGuard\wqserver
Certificate Authority data	C:\Documents and Settings\WatchGuard\wgca
WebBlocker Server data	C:\Documents and Settings\WatchGuard\wbserver
Future product upgrade images	C:\Program Files\Common Files\WatchGuard\resources\Fireware\10
Help files (Fireware & WSM)	C:\Program Files\WatchGuard\wsm10.0\help\fireware
Help files (WFS)	C:\Program Files\WatchGuard\wsm10.0\help\wfs

Locations of application and user-created files

These tables give the default locations where the WatchGuard software applications and servers look for their data files or for data files created by users (such as Firebox configuration files). In some cases, the default location changes based on where the software application opened a file of a similar type. In these cases, the software application remembers the last place the file was read/written and looks in that location first.

Because it is possible to configure the Windows operating system (OS) to put these directories on different disk drives, you must determine the exact location of these files based on the configuration of Windows on your computer.

It is also possible to configure log files to be kept in a different directory than other installation files. If you change the default location of log files, these default locations do not apply.

If you are using an OS version that is not English, you must translate directory names (such as *Documents and Settings* or *Program Files*) to match the OS language you use.

Policy Manager for Fireware appliance software

Operation	File Type	Default Location
Read/Write	Firebox backups	C:\Documents and Settings\All Users\Shared WatchGuard\backups
Read	Product upgrade images	C:\Program Files\Common Files\WatchGuard\Resources\Fireware\10
Read	Blocked Sites	My Documents\My WatchGuard
Read	Blocked Sites exceptions	My Documents\My WatchGuard
Read/Write	Firebox configuration files	My Documents\My WatchGuard/configs
Read/Write	Firebox license files	My Documents\My WatchGuard/configs
Read	Initial license import	My Documents\My WatchGuard
Write	MUVPN.wgx file	C:\Documents and Settings\All Users\Shared WatchGuard\muvpn

Policy Manager for WFS appliance software

Operation	File Type	Default Location
Read	Logging Notification	Current working directory
Read	Spam rules import	Current working directory
Write	Saved backups	C:\Documents and Settings\All Users\Shared WatchGuard\backups
Write	MUVPN SPDs (.wgx)	C:\Documents and Settings\All Users\Shared WatchGuard\muvpn
Read	Blocked Sites imports	Current working directory

Flash Disk Management for WFS appliance software

Operation	File Type	Default Location
Read/Write	Backup image	C:\Documents and Settings\All Users\Shared WatchGuard\backups

Report Manager

File Type	Default Location
Report log	C:\Documents and Settings\<user name>\Application Data\WatchGuard\wgreports
Reporting files	C:\Documents and Settings\<user name>\Application Data\WatchGuard\wgreports

LogViewer

File Type	Default Location
LogViewer configuration files	C:\Documents and Settings\<user name>\Application Data\WatchGuard\enhanced_logviewer
LogViewer debug log files	C:\Documents and Settings\<user name>\Application Data\WatchGuard\enhanced_logviewer
LogViewer exported files	C:\Documents and Settings\WatchGuard\logs
LogViewer saved log files	C:\Documents and Settings\WatchGuard\reports
LogViewer search query files	C:\Documents and Settings\<user name>\Application Data\WatchGuard\enhanced_logviewer\searches

