

WatchGuard® Fireware Migration Guide

WatchGuard Fireware v8.0
WatchGuard System Manager v8.0



Notice to Users

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

Copyright, Trademark, and Patent Information

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

Complete copyright, trademark, patent, and licensing information can be found in the *WatchGuard System Manager User Guide*. A copy of this book is automatically installed into a sub-folder of the installation directory called Documentation. You can also find it online at:
<http://www.watchguard.com/help/documentation/>

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

Guide Version: 8.0-Beta9

ADDRESS:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

SUPPORT:

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

SALES:

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

ABOUT WATCHGUARD

WatchGuard is a leading provider of network security solutions for small- to mid-sized enterprises worldwide, delivering integrated products and services that are robust as well as easy to buy, deploy and manage. The company's Firebox X family of expandable integrated security appliances is designed to be fully upgradeable as an organization grows and to deliver the industry's best combination of security, performance, intuitive interface and value. WatchGuard Intelligent Layered Security architecture protects against emerging threats effectively and efficiently and provides the flexibility to integrate additional security functionality and services offered through WatchGuard. Every WatchGuard product comes with an initial LiveSecurity Service subscription to help customers stay on top of the security landscape with vulnerability alerts, software updates, expert security instruction and superior customer care. For more information, please call (206) 521-8340 or visit www.watchguard.com.

Contents

CHAPTER 1 Introducing WatchGuard System Manager with Fireware Pro	.1
What is Fireware Pro?	1
<i>Using Fireware appliance software tools</i>	2
What's New with WatchGuard System Manager?	2
<i>Enhancements to WFS appliance software</i>	3
<i>WatchGuard Servers</i>	3
Comparing WFS and Fireware Pro	4
<i>WatchGuard Firebox System vs. Fireware Feature Matrix</i>	4
Planning Your Migration	9
CHAPTER 2 Installing the WatchGuard System Manager software	11
Documenting Your Security Policy	11
Installing the management station software	11
<i>Installation requirements</i>	12
<i>Saving Your WFS Configuration</i>	12
<i>Installing the software</i>	14
Setting Up the Management Server	14
<i>Passwords and the Key Files</i>	15
Migrating Basic DVCP Tunnels while setting up a Management Server	17
<i>Procedure #1</i>	17
<i>Procedure #2</i>	17
<i>Viewing the network with WatchGuard System Manager</i>	18
<i>Upgrade appliance software to WFS 7.4</i>	19
Setting Up the Log Server	20
<i>Introducing the new Log Viewer</i>	20
<i>Merging log files from WFS 7.3 and before into the new XML format</i>	21
Setting Up the WebBlocker Server	21

CHAPTER 3 Putting Fireware on the Firebox	23
Using the Quick Setup Wizard	23
<i>Connecting to the Firebox</i>	31
Using fbxinstall.exe	33
<i>Restoring a Backup Image</i>	33
<i>Upgrading to Fireware Pro</i>	33
CHAPTER 4 Making a Fireware Configuration	35
Basic Configuration Properties	36
<i>Connecting to a Firebox with Fireware Pro</i>	36
<i>Working with Interfaces</i>	36
<i>Configuring your Network</i>	38
<i>DHCP Server</i>	39
Intrusion Prevention/Default Packet Handling	41
<i>Blocked Sites</i>	41
Network Address Translation (NAT)	43
<i>Logging</i>	44
Firewall Authentication	45
Virtual Private Networking	46
<i>Firebox Managed Clients</i>	46
<i>Remote User</i>	46
<i>Mobile User VPN</i>	46
<i>Gateways</i>	47
<i>Tunnels</i>	48
<i>IPSec Routing Policies</i>	48
Services	50
<i>Service-based NAT</i>	50
CHAPTER 5 Working with Proxies	53
Proxy Migration	53
Configuring the HTTP Proxy	55
Configuring the Incoming SMTP Proxy	61
<i>Clone the SMTP-Incoming Proxy Action</i>	62
Outgoing SMTP	66
<i>Clone the SMTP Outgoing proxy action</i>	66
FTP Proxy	70
<i>Clone the FTP-Client or FTP-Server proxy action.</i>	70

Introducing WatchGuard System Manager with Fireware Pro

WatchGuard® System Manager (WSM) v8.0 is an important software release for WatchGuard customers. This release introduces our next-generation, Fireware™ Pro appliance software. It also enhances the current WSM management software. With WSM v8.0, you can manage Firebox® X Edge, Firebox X Core, and Firebox X Peak devices at the same time from the same management station. With Fireware Pro appliance software on a Firebox X Core or Peak, you can use advanced networking features such as dynamic routing and a feature-rich IPS.

This *Migration Guide* introduces the features of WatchGuard System Manager v8.0, as well as our Fireware appliance software. It includes a feature by feature comparison between WFS and Fireware Pro appliance software. It also shows you how to:

- Install the new software package
- Migrate from WFS to Fireware Pro
- Restore a WFS 7.x configuration on a Firebox with Fireware appliance software

What is Fireware Pro?

Fireware™ Pro is the next generation of security appliance software available from WatchGuard. *Appliance software* is a software application stored in the memory of your firewall hardware. The Firebox uses the appliance software with the configuration file to operate. When you upgrade your Firebox® X Core or Firebox X Peak device, you write a new version of the appliance software to its memory.

The WatchGuard® System Manager now supports two versions of appliance software:

- WFS - This is the default appliance software on Firebox III and Firebox X Core appliances. This is an enhanced version of the appliance software successfully used by WatchGuard customers since 1998. WatchGuard System Manager v8.0 includes WFS v7.4.
- Fireware Pro - This is the default appliance software on Firebox X Peak appliances. This next generation appliance software enables WatchGuard to expand the number of features available to Firebox X customers. Advanced networking features like multi-WAN support, dynamic routing, and QoS enable customers with complex networking environments to more effectively protect their networks, while simultaneously benefiting from WatchGuard's proactive Deep Application Inspection capabilities.

Using Fireware appliance software tools

When you install WatchGuard System Manager, it automatically installs the software tools you must have to configure and manage a Firebox X Core or Firebox X Peak with Fireware Pro appliance software. These include:

- Fireware Firebox Manager
- Fireware Policy Manager
- Fireware HostWatch

When you add an device to the WatchGuard System Manager **Devices** tab, the system identifies which appliance software the Firebox uses. If you select a Firebox and then click a management tool icon on the toolbar, it automatically starts the correct management tool for the version of appliance software installed on that Firebox.

For example, add a Firebox X5000 to the **Devices** tab using the instructions found in the *WatchGuard System Manager User Guide*. Select the Firebox X5000. Click the Policy Manager icon on the WSM toolbar. Fireware Policy Manager starts and opens the configuration file.

What's New with WatchGuard System Manager?

With this release, there are many changes to the WatchGuard® System Manager – some large and some small. In this section we tell you the most important enhancements.

New WatchGuard System Manager features

We made the VPN Manager the primary management software for all the Firebox devices, log servers, and management servers in your network. From WatchGuard System Manager, you can start monitoring and configuration tools such as Policy Manager, HostWatch, and the Firebox System Manager.

WatchGuard System Manager also includes:

- Simple management of a network with more than one WatchGuard hardware platforms:
 - Firebox III
 - Firebox X Core
 - Firebox X Edge
 - Firebox X Peak
 - Firebox SOHO6 and Firebox SOHO6 Wireless
 - Firebox S6 and Firebox S6 Wireless
- A Management Server that operates on a Windows server instead of on a gateway Firebox. This solution is more scalable and flexible and lets you easily set up a large network with many offices and VPN tunnels.
- A feature that allows to use SNMP to monitor important device statistics. You can also transmit SNMP traps to SNMP servers.
- Log messages stored in an XML format.

New features introduced with Fireware Pro

The Fireware Pro appliance software improves WatchGuard's ability to supply new features on the same hardware platform. Fireware Pro is available as an upgrade to the WatchGuard System Manager. Contact your reseller or visit our Web site for more information. Features new to this release include:

- Enhancements to the Gateway AntiVirus service such as a feature to examine outgoing messages, to lock attachments with suspicious content and better reports

- Interface independence
- Signature-based intrusion prevention with stateful signature matching
- Multi-WAN for more flexibility and network connection time
- Dynamic routing of these protocols: BGP, OSPF, RIPv1 & v2
- Quality of Service (QoS) which uses “virtual pipes” to route the traffic to align with your business requirements
- Active Directory and LDAP integration
- Application Server Load Sharing and enhanced policy management interface for advanced controls and more granular control of your security policy

Enhancements to WFS appliance software

The WatchGuard System Manager v8.0 includes WFS v7.4 appliance software. This version has two important features.

- WSM 8.0 uses a Management Server that operates on a Windows server rather than a gateway Firebox. This allows for much more scalability and flexibility when you set up a large, distributed network.
- You can now use Remote User VPN with PPTP and Mobile User VPN to a Firebox that gets its external IP address from an ISP, which uses static DHCP or static PPPoE.

WatchGuard Servers

There are three servers in this release that do Firebox management functions:

- Management server
- Log server
- WebBlocker server

You can configure the servers from a Windows toolbar which you install with the servers. The toolbar appears in the Windows taskbar at the bottom of your computer monitor. The toolbar is used to start, stop, and configure each server.



Management Server

WatchGuard pioneered simple, 1*2*3 VPN configuration with the Dynamic VPN Configuration Protocol (DVCP). A DVCP server controls the VPN tunnels of a distributed enterprise from one, easy to use management interface. A limit to previous versions of WSM was that you could only use the Firebox as a DVCP server.

With WSM 8.0, we move the DVCP off the Firebox and on to a computer using the Windows operating system. This gives increased scalability and flexibility for the network administrator. The management server has the same functions as the DVCP/CA server from previous releases of WSM. These functions are:

Comparing WFS and Fireware Pro

- Centralized management of VPN tunnel configurations
- Certificate authority for distributing certificates for IPSec tunnels

Log Server

The Log Server collects log messages, event messages, alarms, and diagnostic messages from one or more Firebox devices. The log messages are now kept in an *.xml format. This allows you to use third-party XML tools to create your own custom reports. The Log Server was formerly known as the WatchGuard Security Event Processor (WSEP).

WebBlocker Server

The WebBlocker Server operates with an HTTP Proxy policy to prevent users from browsing to specified Web sites. You set the categories of permitted Web sites during Firebox configuration. The HTTP Proxy on the Firebox then uses information on the WebBlocker Server to find out if a Web site is in a restricted category.

Comparing WFS and Fireware Pro

Many of the tools and features you use in WFS are also in Fireware® Pro. Some are enhanced with more settings or improvements in the methods used to configure and enable them. We also added features such as dynamic routing, multi-WAN support, and a signature-based intrusion prevention system. At the same time, we did not move all of the WFS appliance software features into Fireware Pro.

This table is a summary of the features in each type of appliance software.

WatchGuard Firebox System vs. Fireware Feature Matrix

Feature or Functional Area	Complete	Ease of Use	Like WFS	Notes	
Upgradeable	Model upgradeable	Yes	Yes	Yes	<ul style="list-style-type: none"> • Different license key/file format. • FIREWARE feature required before product will allow traffic-passing policies. LSS will provide licenses with this feature. This means LSS registration is required for the product to function.
Networking Features	Port Independence	Yes	Yes	N/A	
	Secondary IP-address	Yes	Yes	Yes	
	QOS	Yes	Yes	N/A	
	Dual WAN	Yes	Yes	N/A	May expose more configuration flexibility in future releases.
	WAN Failover	Yes	Yes	N/A	<ul style="list-style-type: none"> • May expose more configuration flexibility in future releases. • IPSec failover TBD.
	Server load balancing (VIP)	Future Release	N/A	N/A	Subsequent release.

Feature or Functional Area	Complete	Ease of Use	Like WFS	Notes	
	Dynamic Routing	Yes	No	N/A	Basically same UI as in Vclass. We intend to make this user-friendly in a future release.
	VLAN	Future Release		N/A	
	DHCP Client	Yes	Yes	Yes	
	DHCP Server	Yes	Yes	Improved	Multiple ranges for each interface can turn on/off per interface.
	PPPoE Client	Yes	Yes	Yes	
	Drop-In Mode	Future Release			Feature dropped for 8.0. Will reappear in a subsequent release with improved behavior.
High Availability	Active / Standby	Yes	Yes	Improved	Generally, an improvement over WFS HA. One noticeable change though is you have to dedicate an interface to HA.
	Active / Active	Future Release			
Application Layer Filtering	HTTP Inbound	Yes	No	N/A	WFS does not support inbound HTTP application layer filtering.
	HTTP Outbound	Yes	No	No	A big improvement over WFS in terms of configuration capabilities and security.
	Web Blocker	Yes	Yes	Yes	Uses same server as WFS
	SMTP-Incoming	Yes	No	No	An improvement over WFS in terms of configuration capabilities.
	SMTP-Outgoing	Yes	No	No	An improvement over WFS in terms of configuration capabilities.
	Gateway Antivirus SMTP	Yes	Yes	Yes	
	FTP Proxy	Yes	No	No	<ul style="list-style-type: none"> An improvement over WFS in terms of configuration capabilities. Exception: doesn't proxy data channel.
	DNS Proxy	Yes	No	Almost	An improvement over WFS in terms of configuration capabilities.
	Outgoing (TCP) proxy	Yes	No	Almost	
	IDS/IPS (PAD)	Yes	No	Yes	Enhanced PAD capabilities with new proxy architecture
	IPS (signature based)	Yes	No	N/A	New in Fireware 8.0

Comparing WFS and Fireware Pro

Feature or Functional Area	Complete	Ease of Use	Like WFS	Notes	
Authentication	Radius	Yes	No	Almost	No UI integration with the authentication server. Does not download list of users and groups.
	LDAP	Yes	No	N/A	No UI integration with the authentication server. Does not download list of users and groups.
	Active Directory	Yes	No	N/A	<ul style="list-style-type: none"> No UI integration with the authentication server. Does not download list of users and groups. Have to disable SMB packet signing.
	Firebox authentication	Yes	Yes	Yes	
	Windows NT	N/A	N/A	N/A	Feature dropped.
	SOHO style outbound HTTP authentication	Future Release			
	Authentication Web page for other authentication	Yes	Yes	cbse	<ul style="list-style-type: none"> No applet. URL: https://<appip>:4100 Timeout value fixed at 2 hours. Configurable in a future release.
VPN	PPTP	Yes	Yes	Yes	<ul style="list-style-type: none"> Stable. Limit of 50 PPTP tunnels per device (same as WFS). One PPTP client behind any NAT device.
	PPTP with Radius Auth	Yes	Yes	Yes	
	PPTP Pass-through	Yes	On by default	Almost	Does not support more than one PPTP client tunneling to the same endpoint yet.
	MUVPN	Yes	Yes	Yes	<ul style="list-style-type: none"> External authentication is the only supported authentication mechanism for MUVPN. Same version of Safenet client as WFS and SOHO.
	BOVPN	Yes	Yes	Yes	<ul style="list-style-type: none"> Tunnels negotiate when traffic is passed (no auto-start). No DNS resolution in IKE
	HW AES	Yes	N/A	N/A	

Feature or Functional Area	Complete	Ease of Use	Like WFS	Notes	
Management	IPSec Pass-through	Yes	Off by default	Yes	<ul style="list-style-type: none"> • Turned off by default to push people towards using NAT-T which is more stable and scalable solution. • To configure IPSec pass-through, you have to enable the global option, and create an IPSec policy to allow the traffic.
	IPSec Licensing	Yes	Yes	No	Number of phase-2 SA are licensed. WFS licensed phase-1 SA.
	NAT Traversal (UDP encapsulation of IPSec)	Yes	On by default	Yes	Can be turned off in the UI if necessary.
	DNS Resolution in IKE	Future release	N/A	No	
	Tunnel auto-start on boot	Future release	N/A	No	
	Management interface to all tools	Yes	Yes	Yes	
	Manage single appliances (more than one)	Yes	Yes	Yes	
	Interface to DVCP server	Yes	Yes	Yes	
Management Server	Drag and drop VPN setup for Fireware, WFS, and SOHO	Yes	Yes	Yes	
	Moved from Firebox to Mgmt Station	Yes	Maybe	Yes	A little more difficult that running the DVCP server on the Firebox. We will have to continue to improve the setup wizards.
	SSL/CSK Gateway (SOHO)	Yes	N/A	Yes	
	Supports Fireware, WFS, SOHO	Yes	Yes	Yes	
	Basic DVCP	Dropped			<ul style="list-style-type: none"> • Customers using basic DVCP will have to switch to Enhanced DVCP (what used to be VPN-Manager and is now WSM). • DVCP Server setup wizard will migrate an existing Firebox DVCP server to a management station.
Web Backer	45 categories	Future Release			
Fireware FSM		Yes	Yes	Yes	Very similar to WFS FSM

Comparing WFS and Fireware Pro

Feature or Functional Area	Complete	Ease of Use	Like WFS	Notes	
Fireware Host Watch	Tunnel Display/Monitor	Yes	Yes	Yes	• Only tunnels that are “up” will display in the front panel tree.
		Yes	Yes	Improved	You can add sites to the blocked sites list
	WFS to Fireware	Future Release	Yes	N/A	Will produce a comprehensive report of the configuration conversion and identify any areas that need customer attention.
Conversion					
Fireware Policy Management	Policy Manager	Yes	Yes	Yes	Entirely new for Fireware 8.0
	Firewall Policies	Yes	Yes	Improved	Incoming/outgoing gone. Replaced with from/to model
	BOVPN Setup	Yes	Yes	Improved	New UI model for VPN clearly identifies firewall policies that act on tunnel traffic
	MUVPN Setup	Yes	Yes	Yes	Xauth only
	PPTP Setup	Yes	Yes	Yes	Same limit of 50 PPTP connections/tunnels per device.
	Custom ordered policies	Yes	Yes	N/A	
	Auto-policy ordering	Yes	Yes	Yes	Policy ordering algorithm same in WFS policy ordering
	1:1 NAT	Yes	Yes	Yes	
	Dynamic NAT	Yes	Yes	Yes	
	Static NAT	Yes	Yes	Yes	
CLI	Fireware CLI	Yes	No	No	Not heavily advertised. Required for Common Criteria certification. POLICY CONFIGURATION IS NOT COMPATIBLE WITH FIREWARE POLICY MANAGER.
	WFS FBSH	N/A	No	N/A	Not distributed/released
Web UI		Future Release			
Logging	Log Server	Yes	Yes	Yes	New XML log-server
	Log Viewer	Yes	Yes	Yes	New XML log viewer
	Log content	Yes	Yes	No	All logs are new with Fireware 8.0.
Reporting	Historical Reports	Yes	Yes	Improved	Five new reports added. Support for XML log files.

Feature or Functional Area	Complete	Ease of Use	Like WFS	Notes	
Supportability	Access to troubleshooting information (ike dat, ...)	Yes	Yes	No	Improved user access.
	On Line Help	No	No	Yes	We may not be able to ship as complete of a help system this time due to schedule constraints.

Planning Your Migration

As with any major software migration, a well-designed plan for your upgrade from WFS to Fireware™ Pro can decrease the effect on your users, improve your experience, and make sure a secure installation of the new product features. If possible, we recommend that you do this migration in a network lab as an alternative to your production network. You can also do this migration during non-operational hours when a short time with no connection to the Internet does not harm your business.

The length of the migration depends upon the complexity of your network and of your current Firebox® configuration. The software installation and Fireware Pro installation should take no more than 30 minutes. However, the time necessary to migrate your DVCP server to the Management Station and to create your new Fireware Pro configuration varies based on the number of tunnels and policies you have. We recommend that you set aside up to eight hours.

This *Migration Guide* supplies detailed instructions to successfully migrate from WFS to Fireware Pro. These include steps to:

- Document your current WFS configuration
- Backup your current WFS configuration
- Install Watchguard System Manager on the management station
- Configure the Management Server and migrate your DVCP server(s)
- Configure the Log Server
- Configure the WebBlocker Server and download the database
- Install Fireware Pro on the device
- Open WSM and connect to the Firebox
- Open Fireware Policy Manager
 - Make the changes in Fireware Policy Manager that reflect the WFS configuration
 - Network configuration
 - NAT settings
 - Service configurations
 - Create and test VPN tunnels as necessary
- Deploy the Firebox and test the Fireware configuration

Installing the WatchGuard System Manager software

Before you can operate a Firebox with WatchGuard Fireware Pro, you must install the WatchGuard System Manager v8.0 upgrade on your management station. If the Firebox was a DVCP/CA server, you must move the configuration properties to the Management Server. If you completed these steps, you can go to XXX In this chapter, we tell how to:

- Document your security policy
- Back up the WFS configuration file and image
- Install WatchGuard System Manager software on a management station
- Set up WatchGuard servers

Documenting Your Security Policy

A good security policy is not just a firewall configuration file. It is a process which a network administrator documents and which management regularly reviews. Your Fireware Pro migration is a good opportunity to revisit your security policy. Because you must make a new configuration file for the Fireware Pro appliance software, you should examine which policies you need to do business. Use these guidelines:

- Each policy you open makes your network less secure
- Policies from the Internet into your network are more dangerous than policies from your network out to the Internet
- Adding specific source and destination addresses makes a policy more secure

Note

To successfully migrate to WatchGuard Fireware you must begin from WFS 7.3.

Installing the management station software

You must install the WatchGuard System Management software before you migrate a Firebox to Fireware Pro.

Installation requirements

Before you install WatchGuard System Manager, make sure that you have these items:

- WatchGuard Firebox security device
- WatchGuard System Manager CD-ROM
- A serial cable (blue)
- Three crossover Ethernet cables (red)
- Three straight Ethernet cables (green)
- Power cable
- LiveSecurity service license key

It is also good to restart your Firebox before you start the upgrade procedure. This clears the RAM component and helps to prevent problems during the upgrade.

Software encryption

The management station software is available with three types of encryption.

Base

Uses 40-bit encryption

Medium

Uses 56-bit DES encryption

Strong

Uses 128-bit 3DES encryption

A minimum of 56-bit encryption is necessary for the IPSec standard. To use virtual private networking with IPSec or PPTP, 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. For more information, log in to the LiveSecurity Service and refer to the online resources at:

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

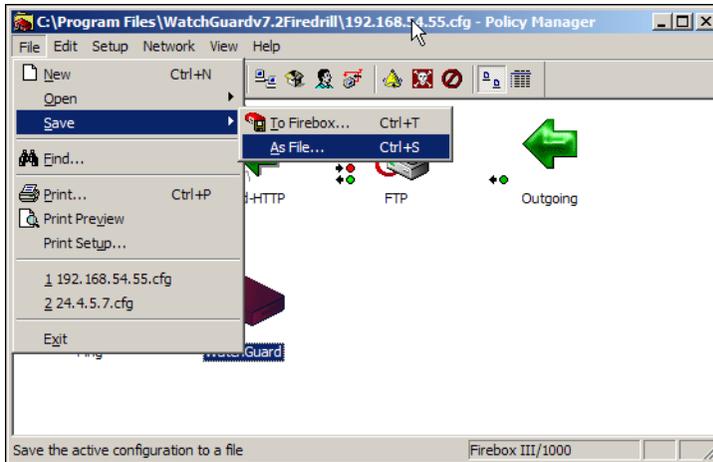
Saving Your WFS Configuration

Before you upgrade to WatchGuard System Manager v8.0, save your current configuration file and appliance software image.

Saving the configuration file

You can save the configuration file of a Firebox on the device itself. You can also save it as a file on a local hard disk drive. Before you migrate, we recommend that you save the configuration file to a local hard disk drive.

- 1 From WFS Policy Manager, select **File > Save > As File**.

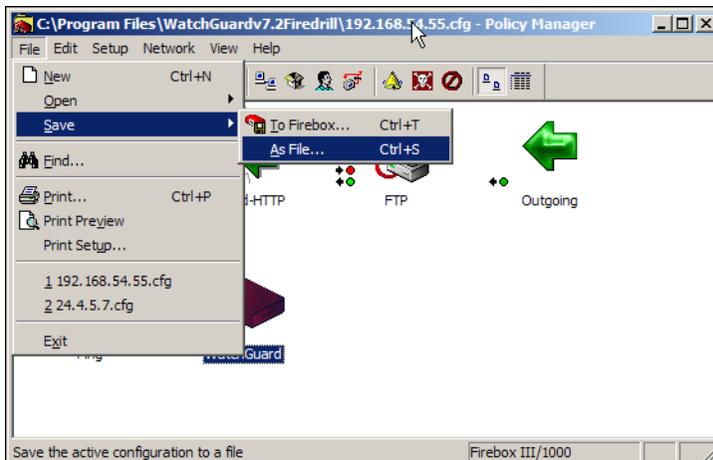


- 2 Type the name of the configuration file. Click **Save**.
The configuration file has the file extension *.wfg. You can also save this to a network folder.

Saving the appliance software image

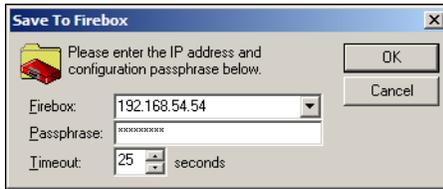
A very important step in the upgrade is to save the appliance software image. The Firebox keeps this file on a backup partition of the Firebox hard disk drive. You must have the appliance software image to restore the WFS appliance software on your Firebox if you move to Fireware Pro and must get access to WFS again. To create the WFS backup file:

- 1 From WFS Policy Manager, select **File > Save > To Firebox**.

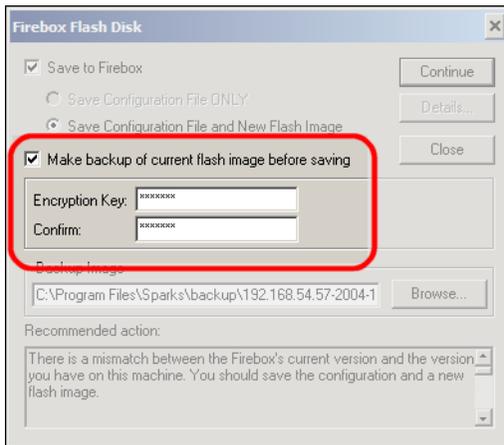


Setting Up the Management Server

- 2 Type the configuration passphrase. Click **OK**.



- 3 Select **Make backup of current flash image before saving**.



- 4 Type a strong encryption key that is easy to remember. Type it again.
- 5 Click **Continue**.
The backup image has the file extension *.fbi.

Installing the software

With WatchGuard System Manager v8.0, you can have more than one management software version on one management station. Make sure you select a different folder name for each installation.

- 1 If you have not done so, download the WatchGuard System Manager software. The speed of your Internet connection sets the time to download the software.
Make sure that you write down the name and the path of the file when you save it to your hard disk drive.
- 2 When the download is complete, open the file and use the instructions on the screens to help you through the installation.
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.
- 3 At the end of the installation wizard, a check box appears that you can select to start the QuickSetup Wizard. For this upgrade, we recommend that you use the QuickSetup Wizard at this time only if you do have no VPN tunnels and do not use VPN Manager.

Setting Up the Management Server

WatchGuard® pioneered simple, 1*2*3 VPN configuration with the Dynamic VPN Configuration Protocol (DVCP). A DVCP server controls the VPN tunnels of a distributed enterprise from one, easy to use management interface. A limit to previous versions of WatchGuard System Manager (WSM) was that you could only use the Firebox® as a DVCP server.

With WSM 8.0, we move the DVCP off the Firebox and on to a computer using the Windows operating system. This gives increased scalability and flexibility for the network administrator. The Management Server has the same functions as the DVCP/CA server from previous releases of WSM. These functions are:

- Centralized management of VPN tunnel configurations
- Certificate authority to make and to send out certificates for IPSec tunnels.

The installation software can install the Management Server on the same computer as the management station. You can also install it on a different computer. You must install the Management Server software on a computer that is behind a Firebox with a static external IP address. The Management Server does not operate correctly if it is behind a Firebox with a dynamic IP address on its external interface.

Use the Management Server to do these tasks:

- Start and stop the Management Server
- Set Management Server passphrases
- Enter a Management Server license key
- Configure diagnostic log messages from the Management Server
- Set the certificate authority properties such as domain name and publication period
- Start WatchGuard System Manager to manage Firebox clients, VPN tunnels, and security templates
- Start the Certificate Authority user interface

Passwords and the Key Files

The WatchGuard Management Server encrypts important information that it keeps on the Firebox and on your local hard disk drive. It uses a number of passwords to protect sensitive information stored on disk or to secure traffic with client systems. During configuration, you set two passwords and the system creates system passwords:

- Master password - The Management Server uses the master password to encrypt the password file. This protects all of the other passwords. Select and save the master password carefully and safely. Use best practices when you select the password. Do not use the same string for the master password and the administrator password.
It is necessary to use the master password to:
 - Migrate the Management Server data to a different computer
 - Restore a lost or corrupt master key file
 - Change the master password
- Administrative password - You use the administrative password to connect to the WatchGuard System Manager software. You use this password frequently. Use best practices when you select the password.
- System passwords - The Management Server automatically makes other passwords. It uses these passwords to encrypt files, traffic on VPN tunnels, and for the Certificate Authority private keys. You cannot see these passwords with the user interface.

The Management Server saves the administrative and system passwords in a password file. It encrypts the data in the password file with the master password. The master password is not saved. The Management Server makes an encryption key from the master password and the key is saved on the local disk of the Management Server.

The default location for the password file and encryption key are:

- C:\Documents and Settings\WatchGuard\wgauth\wgauth.ini
- C:\Documents and Settings\WatchGuard\wgauth\wgauth.key

These files are only used by the Management Server software. It is not necessary to change these files.

Setting Up the Management Server

You use the Management Server Setup Wizard to configure your Management Server. If you use a Firebox as a DVCP server, the wizard also moves the DVCP server features and Certificate Authority from the Firebox to your Management Server.

- 1 From the Windows desktop, double-click the Management Server icon on the WatchGuard toolbar. The Management Server Setup Wizard appears.



- 2 Select **Start Service**.

If the Management Server has not been configured, then the Management Server Setup Wizard starts automatically. The wizard goes through these steps:

Create a master encryption key

You must have a master password to control access to the WatchGuard Management Station. Type a password with a minimum of eight characters and then confirm. It is important to remember this password. If you do not know your password, there is no procedure to learn it from the Management Server or the Firebox.

Create a Management Server passphrase

Type a password of at least eight characters to manage the WatchGuard Management Server.

Identify the gateway Firebox

Type the IP address and passphrases for your gateway Firebox. The gateway Firebox protects the Management Server from the Internet. The gateway Firebox protects the Management Server from the Internet. If the gateway Firebox is configured as a DVCP server, the server is moved from the gateway Firebox to the Management Server.

Provide a license key

Type the license key for the Management Server.

Identify your organization name

Type the name of your organization.

Make sure the configuration of your server is correct

This is an information screen that shows the configuration information for your server.

The wizard is configuring your server

This is an information screen that appears while the configuration options are applied to your Management Server.

The Management Server Setup Wizard is complete

This is an information screen that appears when the installation and configuration of the Management Server is complete.

Migrating Basic DVCP Tunnels while setting up a Management Server

WatchGuard System Manager 8.0 provides a wizard that migrates your WFS DVCP server configuration to the new WatchGuard management server. This wizard is called the Management Server Setup Wizard and is launched from the WatchGuard toolbar in the Windows taskbar.

This wizard moves your DVCP server from your Firebox to a Windows based computer that you designate as your management server. It also converts the Firebox you were using as a DVCP server into a gateway Firebox that protects the management server from the Internet. Finally, it converts any basic DVCP tunnels connected to the gateway Firebox into regular tunnels. Basic DVCP tunnels are not supported in WSM 8.0.

However, the Management Server Setup Wizard is not able to convert all the basic DVCP tunnels that you have in your network. It only converts the tunnels that use the gateway Firebox as one of the endpoints. These tunnels are isolated from the gateway Firebox. If you have any isolated basic DVCP tunnels in your network, you need to use one of these two procedures to convert your tunnels so they are managed by WSM 8.0.

Procedure #1

This workaround requires you to disable any isolated basic DVCP tunnels before using the Management Server Setup Wizard.

- 1 Using the Policy Manager, remove the basic DVCP tunnel configuration at each endpoint (Firebox) for the tunnel.
Do this for each Firebox that is an endpoint for an isolated tunnel.
- 2 Download the configuration to each Firebox and restart the Firebox.
- 3 Use the Management Server Setup Wizard to:
 - Move your DVCP server to your management server
 - Convert your old DVCP server into a gateway Firebox
 - Convert any Basic DVCP tunnels connected to the gateway Firebox to regular tunnels
- 4 Reestablish previously disabled tunnels.
- 5 Launch WatchGuard System Manager
- 6 Add each endpoint Firebox to the management server
- 7 Drag-n-drop a Firebox onto another Firebox to create a tunnel between the two firewalls.
- 8 Do this for each tunnel that needs to be reestablished.

Procedure #2

This workaround allows you to minimize the downtime for your isolated Basic DVCP tunnels.

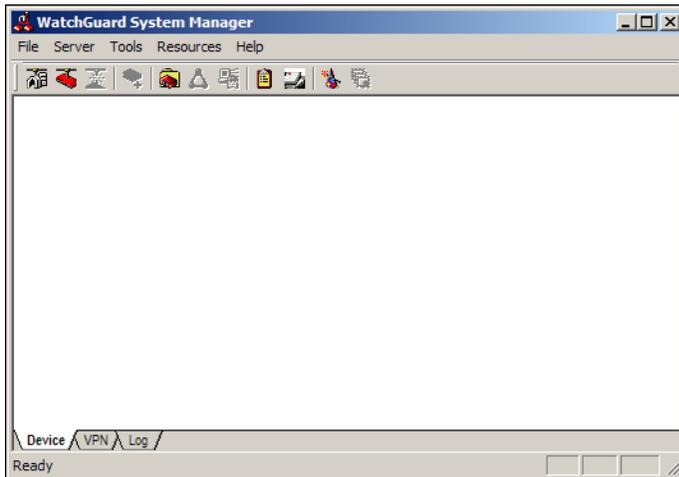
- 1 Acquire a VPN Manager license key with enough capacity to convert all of your Basic DVCP tunnels to Advanced DVCP tunnels.
 - 2 Install the license key into VPN Manager.
 - 3 Use VPN Manager to convert all your Basic DVCP tunnels to Advanced DVCP tunnels.
- Use the Management Server Setup Wizard to:
- Move your DVCP server to your management server
 - Convert your old DVCP server into a gateway Firebox
 - Convert any Basic DVCP tunnels connected to the gateway Firebox to regular tunnels
 - All of your Advanced DVCP tunnels are converted to regular tunnels, regardless of whether or not they use the gateway Firebox as an endpoint

Viewing the network with WatchGuard System Manager

After you complete the Management Server Configuration Wizard, your network can at this time use WSM 8.0. If you had Firebox clients connected to a Firebox DVCP server, those Firebox devices connect to the Management Server. There is a policy on your gateway Firebox to let traffic from your Firebox clients to the Management Server. To examine the new Management Server and tunnels:

- 1 From the Windows desktop, select **Start > Program Files > WatchGuard System Manager 8.0 > WatchGuard System Manager**.

WatchGuard System Manager 8 is the default name of the folder for the Start menu icons. You can change this folder name during installation. The WatchGuard System Manager window opens.



- 2 From WatchGuard System Manager, select **File > Connect To > Management Server**.

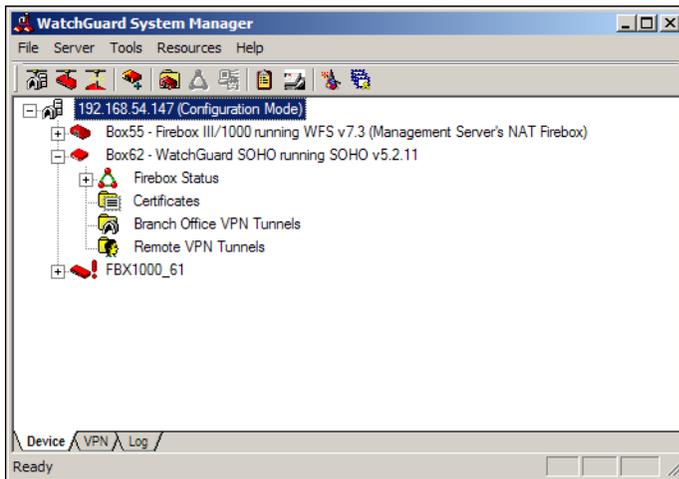


Or, click the **Connect to Management Server** icon on the WatchGuard System Manager toolbar. The Connect to Management Server dialog box appears.



- 3 Use the drop-down list to select your Management Server or type its IP address. Type the management passphrase. Click **OK**.
The server appears in the WatchGuard System Manager Device tab.

- Expand the Management Server entry to see the Firebox clients managed by this Management Server.



Upgrade appliance software to WFS 7.4

After you install the WSM management software and WFS 7.4 on the gateway Firebox, you can use WFS Policy Manager to put WFS 7.4 on other Firebox devices. This is an optional procedure. Your Management Server can connect to and manage Firebox devices which use WFS 7.3.

- From WatchGuard System Manager, select **File > Connect To > Device**.



Or, click the Connect to Device icon on the WatchGuard System Manager toolbar. The Connect to Device dialog box appears.

- Use the drop-down list to select your Firebox or type its trusted IP address. Type the status passphrase. Click **OK**.

The device appears in the WatchGuard System Manager **Device** tab.

- Select the Firebox on the **Device** tab. Then, select **Tools > Policy Manager**.

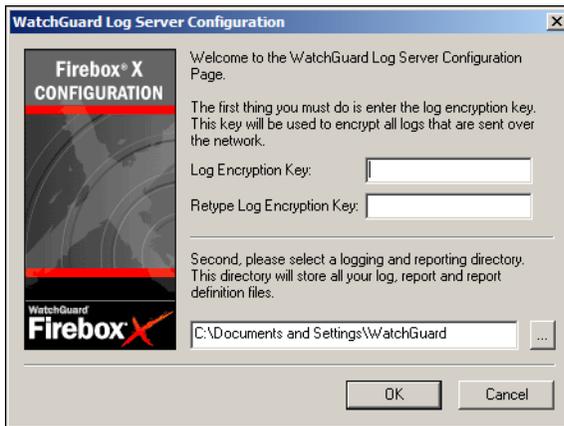
- From Policy Manager, select **File > Save > To Firebox**.

First, Policy Manager prompts you to save to a local hard disk drive. Then it saves the new configuration file to the Firebox.

Setting Up the Log Server

You must also use Policy Manager define the Log Servers for each Firebox. For more information, see the user guides in the Documentation folder on your management station.

- 1 From the WatchGuard toolbar, select the **Log Server** icon.
The WatchGuard Log Server Configuration dialog box appears.



- 2 Type the encryption key to use for the secure connection between the Firebox and the log hosts. The default encryption key is the status passphrase as selected in the QuickSetup Wizard. Log Server encryption keys are a minimum of eight characters.
- 3 Confirm the encryption key.
- 4 Select a directory to keep all logs, reports, and report definition files.
- 5 Click **OK**.

Introducing the new Log Viewer

The WatchGuard Firebox X Core and Firebox X Peak send log messages to one log management computer. This is known as the Log Server. The log messages are saved in an XML format in the WatchGuard folder on the log server. The extension of the file name is .wgl.xml. You can open this file using an XML editing tool to see full log messages.

The Firebox sends log messages to a primary or backup Log Server. The default location for the files are on the installation drive at:

- \Documents and Settings\WatchGuard\Logs.
- \Documents and Settings\watchguard\reports
- \Documents and Settings\watchguard\report-defs

Note

Monitor the connection periodically to make certain that your Firebox X is connected.

Merging log files from WFS 7.3 and before into the new XML format

When you migrate from a previous version of WatchGuard System Manager to WSM 8.0, you can convert log files from .wgl to .xml format. This is also helpful if you operate in a mixed environment with different versions of WSM. After converting, you can use your WSM 8.0 LogViewer or reporting tools on log files created with WatchGuard Management System 7.3 or earlier.

When you convert a log file from .wgl to .xml:

- The XML file is usually smaller than the .wgl file. This is because XML log records are variable in length.
- If you open a log file in an XML editor, you can see some duplicate entries. This is a function of how report tools operated in WSM 7.3 and earlier and does not cause problems in reports which use the log file.

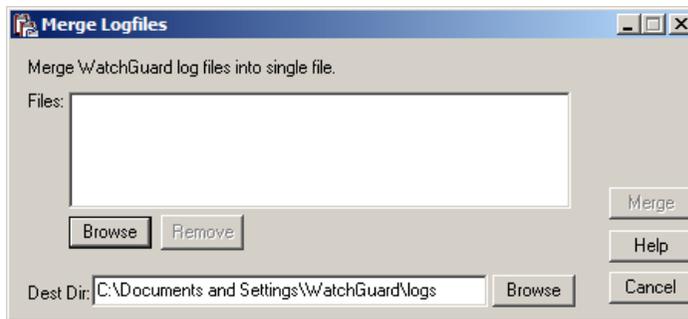
Note

The FTP proxy does not report bytes sent and received so this data is not available in a report.

To convert a log file from .wgl to .xml:

- 1 Right-click the Log Server icon on your Windows desktop tray and select **Merge Log Files...**

The Merge Log files dialog box appears. This dialog box controls merges, and also updates, of log files.



- 2 Click **Browse** to find the location of the log file to convert to XML. If you select more than one log file at the same time, the utility merges all the files into one file. It also converts the format to XML.
- 3 Click **Merge**.
The log files are updated to .xml format and saved to a new file in the specified directory.

Note

Log records used in reports and visible in log viewer are converted.

Setting Up the WebBlocker Server

The WebBlocker Server operates with an HTTP Proxy policy to prevent users from browsing to specified Web sites. You set the categories of permitted Web sites during Firefox configuration. The HTTP Proxy on the Firefox then uses information on the WebBlocker Server to find out if a Web site is in a restricted category.

Setting Up the WebBlocker Server

The first time you connect to the WebBlocker Server, it downloads the WebBlocker database.

- 1 From the Windows desktop, click the WebBlocker Server icon on the WatchGuard toolbar. The Download WebBlocker Database dialog box appears.



- 2 Click **Download**.
The file is more than 60 megabytes. The speed of your connection to the Internet controls the time to download the file.
- 3 When the file download is complete, right-click the WebBlocker Server icon. Select **Start Service**.

CHAPTER 3 **Putting Fireware on the Firebox**

There are two methods to put Fireware on a Firebox which has WFS 7.x:

- Use the Quick Setup Wizard to make a simple configuration file and to save the configuration file and Fireware to the Firebox. This is the preferred method.
- Use the fbxinstall.exe command line utility

Using the Quick Setup Wizard

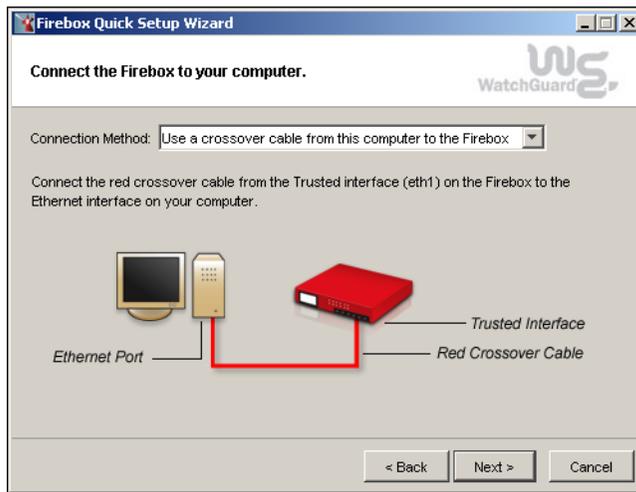
We recommend that you use the Quick Setup Wizard to put Fireware Pro on the Firebox along with a basic configuration file. Because this procedure removes all configuration properties and software, we strongly recommend that you back up the WFS configuration and image. See “Saving Your WFS Configuration,” on page 12 for more information.

- 1 From the Windows desktop, select **Start > Programs > WatchGuard System Manager 8 > Quick Setup Wizard**. Click Next to start the wizard.



- 2 You can connect to the Firebox with crossover cable or an Ethernet cable. Use the Connection Method drop list to select how you connect the Firebox to the management

station. Then make the cable connections you select. When you complete the connections, click Next.



- 3 You can use the Fireware appliance software on a Firebox X Peak or a Firebox X Core. You can not use a Firebox III or Firebox X Edge device. Use the Firebox Model drop-down list to select the model line of your unit. The screen changes to match the selection. Instructions appear on how to start the unit in Safe Mode.

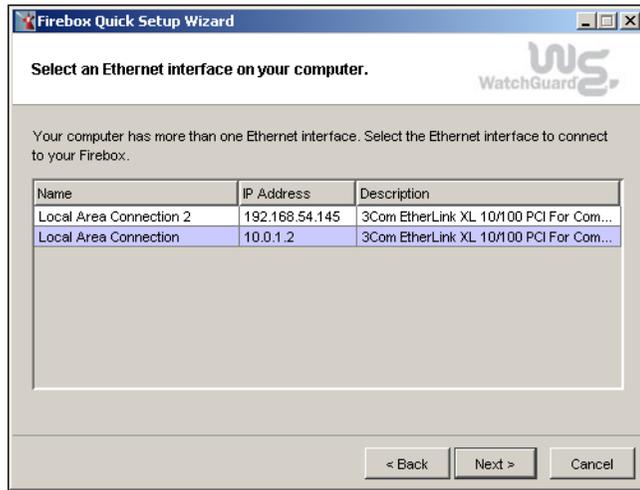
NOTE

The Firebox must be in safe mode to configure it with Fireware.

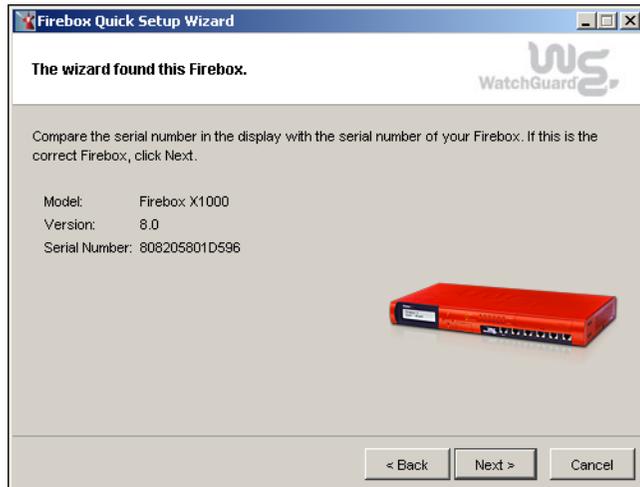


- 4 Click Next. Verify that the Firebox front panel display matches the wizard. Click Next again.

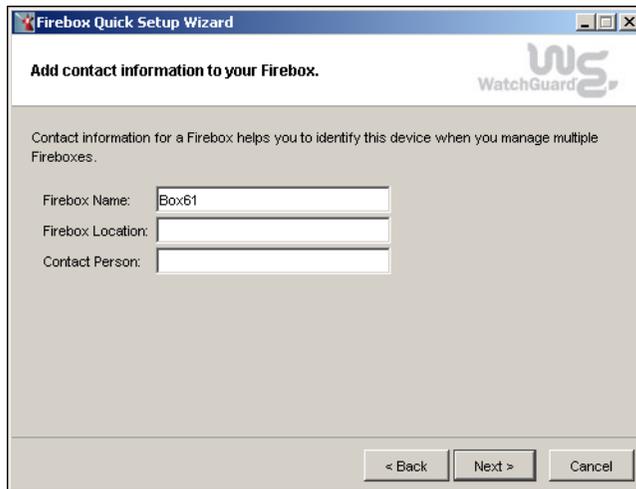
- 5 If your management station has more than one interface, you must select the interface you use to configure the Firebox. Select the correct interface and then click Next.



- 6 The Quick Setup Wizard looks for a Firebox on the same network as the management station interface. If there is more than one Firebox, you must select the correct Firebox from a list and click Next. When a Firebox is found and selected, a status screen appears. Verify that this is the correct Firebox, and then click Next.



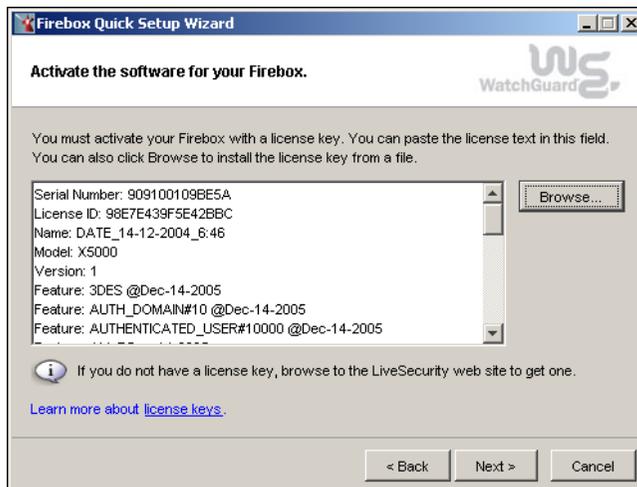
7 Type the identifying information for the Firebox



The screenshot shows the 'Firebox Quick Setup Wizard' window. The title bar reads 'Firebox Quick Setup Wizard'. The main heading is 'Add contact information to your Firebox.' with the WatchGuard logo to the right. Below the heading, a paragraph states: 'Contact information for a Firebox helps you to identify this device when you manage multiple Fireboxes.' There are three text input fields: 'Firebox Name:' containing 'Box61', 'Firebox Location:', and 'Contact Person:'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

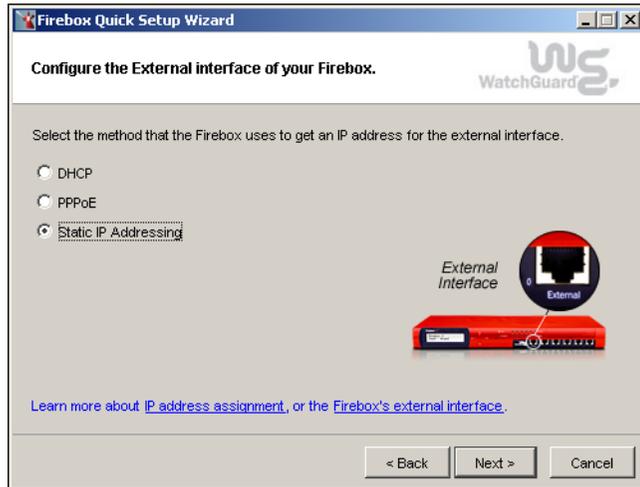
Click Next

8 Add the license. Click Next.

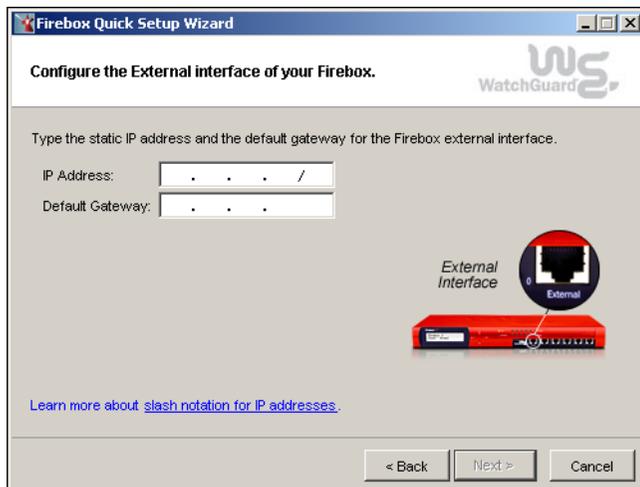


The screenshot shows the 'Firebox Quick Setup Wizard' window. The title bar reads 'Firebox Quick Setup Wizard'. The main heading is 'Activate the software for your Firebox.' with the WatchGuard logo to the right. Below the heading, a paragraph states: 'You must activate your Firebox with a license key. You can paste the license text in this field. You can also click Browse to install the license key from a file.' There is a large text area containing the following license information: 'Serial Number: 909100109BESA', 'License ID: 98E7E439F5E42BBC', 'Name: DATE_14-12-2004_6:46', 'Model: X5000', 'Version: 1', 'Feature: 3DES @Dec-14-2005', 'Feature: AUTH_DOMAIN#10 @Dec-14-2005', and 'Feature: AUTHENTICATED_USER#10000 @Dec-14-2005'. To the right of the text area is a 'Browse...' button. Below the text area, there is an information icon and the text: 'If you do not have a license key, browse to the LiveSecurity web site to get one.' Below that is a blue link: 'Learn more about [license keys](#).' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

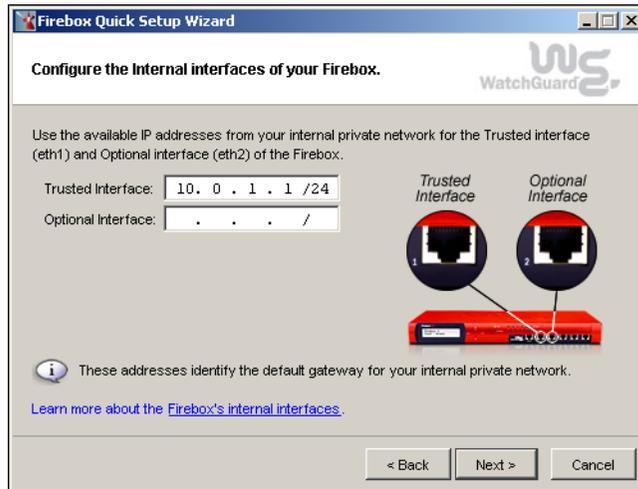
- 9 Select **Static IP Addressing** for this example. Click **Next**.



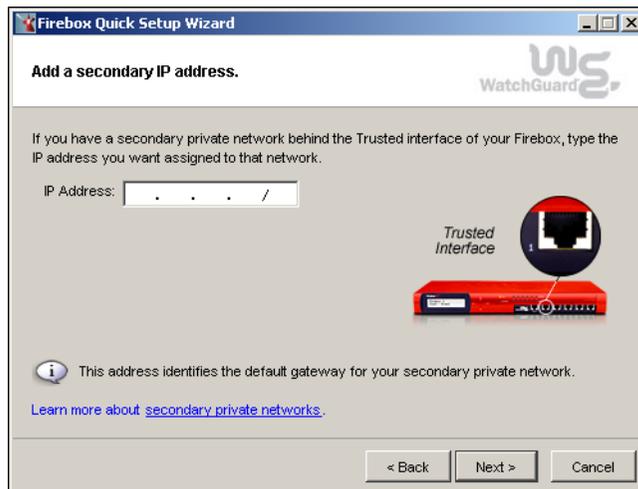
- 10 Type the IP address and default gateway. Click **Next**.



- 11 Type the trusted interface IP address and the optional interface address if you use one. Click Next.



- 12 Type a secondary IP address if there is one. Click Next.



- 13 Type and repeat the passphrases for the Firebox. Click Next.

The screenshot shows the 'Firebox Quick Setup Wizard' window with the title 'Create passphrases for your Firebox.' The WatchGuard logo is in the top right. The main text reads: 'Provide new status and configuration passphrases for your Firebox. Retype the passphrases to confirm they were entered correctly.' There are two sets of input fields: 'Status Passphrase: (read-only access)' and 'Retype Passphrase:', followed by 'Configuration Passphrase: (read-write access)' and 'Retype Passphrase:'. All fields contain asterisks. An information icon and text state: 'A passphrase must use a minimum of 8 characters.' A link says 'Learn how to create strong passphrases.' At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

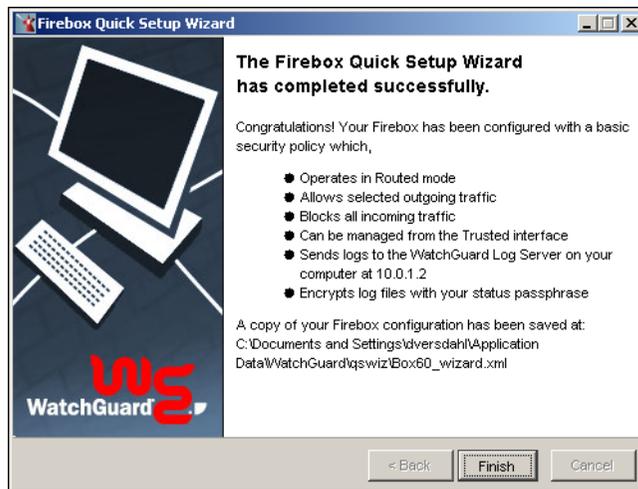
- 14 A temporary IP address is listed. Click Next.

The screenshot shows the 'Firebox Quick Setup Wizard' window with the title 'Provide a temporary IP address for your Firebox.' The WatchGuard logo is in the top right. The main text reads: 'Use an available IP address that is on the same network as your computer.' There is an input field for 'IP Address:' containing '10.0.1.1 /24'. An information icon and text state: 'Your computer is using this IP address: IP Address: 10.0.1.2/24'. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

15 This information screen appears while the wizard configures the Firebox.



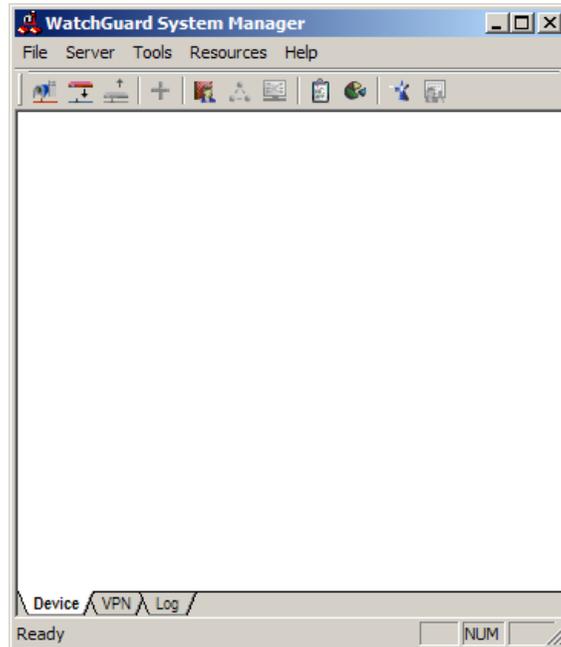
16 The process is complete. Click Finish.



You are now ready to configure the Firebox.

Connecting to the Firebox

- 1 Open WatchGuard System Manager

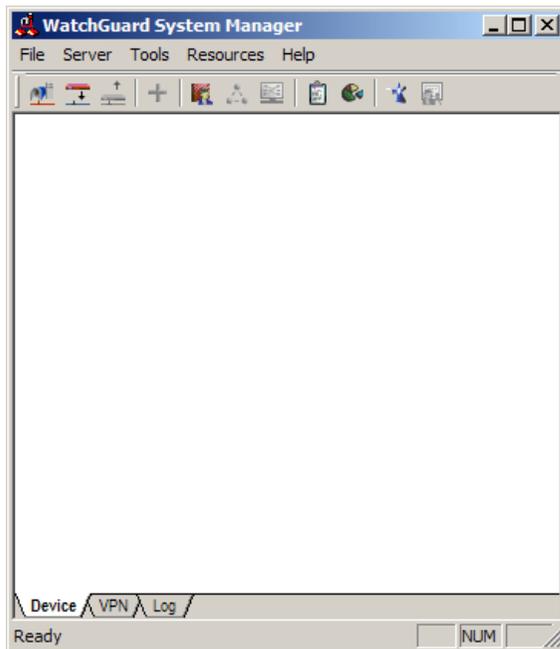


- 2 Click the connect to Device icon

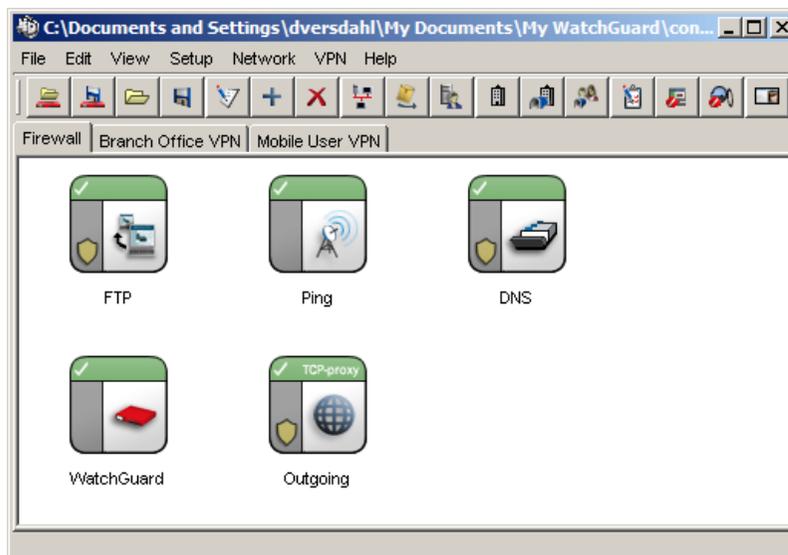


- 3 Type the trusted interface IP address. Click OK.

- 4 Click the Policy Manager icon.



- 5 The Firewall Policy Manager is where you make the configuration changes that match what you have in your WFS 7.x policy.



To allow communication with the external interface you need to:

- Open the appropriate policies
- Make changes to the Firewall connections
- Check the blocked sites and make certain that none affect traffic on your network
- Check the blocked ports and make certain that none affect traffic on your network
- Save your changes

Using fbxinstall.exe

You can also use the `Fbxinstall.exe` utility to install Fireware 8.0. `fbxinstall.exe` is a command line utility that allows you to:

- Upgrade a Firebox X with WFS 7.x firmware and a WFS 7.x configuration to Fireware Pro
- Restore an upgraded Firebox from WFS 8.0 back to its original WFS 7.x software and configuration

Restoring a Backup Image

This process restores a backup image to a Firebox running WFS 8.0.

- 1 Connect a serial cable between the Firebox and your management station.
If you have more than one com port note which port you use.
- 2 Open a command prompt.
- 3 Type `fbxinstall`
- 4 To restore a backup image type
`fbxinstall 10.10.10.1/24 -restore 10.10.10.1/24.fbi`
Where 10.10.10.1/24 is the trusted IP address and 10.10.10.1/24.fbi is the Firebox backup file. The installation process automatically defaults to com port 1.
- 5 Turn off power to the Firebox X.
Press any key.
- 6 Turn on power to the Firebox X.
- 7 A maintenance utility is sent to the Firebox.
- 8 The installation program contacts the Firebox.
- 9 The backup file is installed on the Firebox.

The installation completes.

Upgrading to Fireware Pro

This is a secondary method of installing appliance software on the Firebox X. Once this process is complete you need to use the Quick Setup wizard.

- 1 Connect a serial cable between the Firebox and your management station.
If you have more than one com port note which port you use.
- 2 Open a command prompt.
- 3 Type `fbxinstall`
- 4 To install Fireware 8.0 type
`fbxinstall 10.10.10.1/24`
Where 10.10.10.1/24 is the trusted IP address of the Firebox. The installation process automatically defaults to com port 1.
- 5 Turn off power to the Firebox X.
Press any key
- 6 Turn on power to the Firebox X.
- 7 A maintenance utility is sent to the Firebox.
- 8 The installation program contacts the Firebox.
- 9 WFS 8.0 is installed on the Firebox.

10 The installation completes.

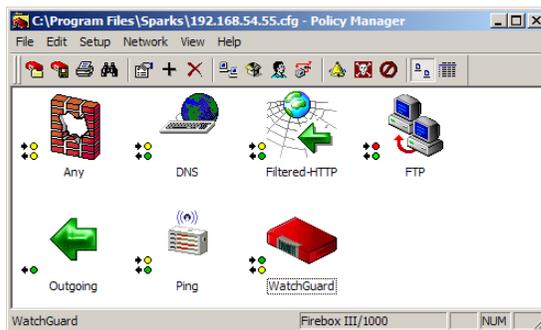
WFS 8.0 is installed. You now create a new configuration file using the Quick Setup wizard.

CHAPTER 4 Making a Fireware Configuration

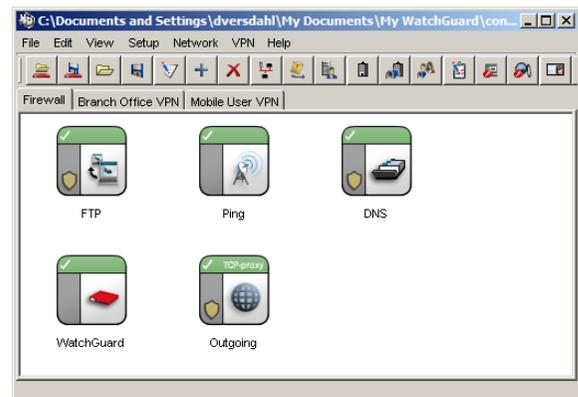
At this time, there is no configuration tool which automatically converts a WFS 7.x configuration file to a Fireware Pro configuration. The two appliance software versions are very different. You begin with the configuration file you saved at the end of the Fireware Quick Setup wizard.

One method is to quickly make your Fireware configuration file is to open the new Fireware file in one window. At the same time, open the WFS configuration file in a second window. Put the two windows on the Windows desktop so that they are both visible. desktop. For example, resize each window so that they are tiled horizontally.

WFS 7.3 Policy Manager



Fireware Policy Manager



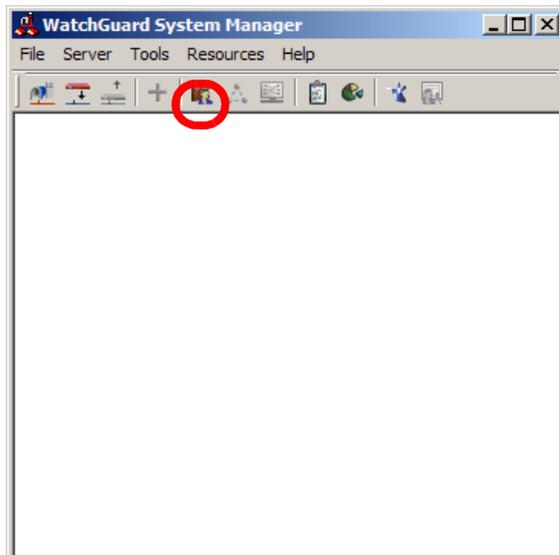
This section describes the essential information you need to migrate your current WFS configuration to Fireware. It describes some of the differences between the behavior of a feature or implementation in WFS and in Fireware.

For more information about using the Policy Manager for Fireware see the Fireware Configuration Guide.

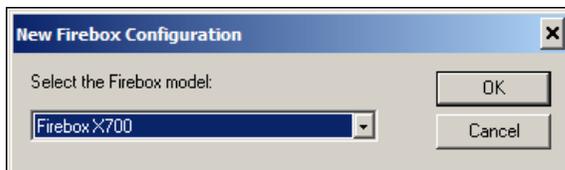
Basic Configuration Properties

Connecting to a Firebox with Fireware Pro

- 1 From WSM, click the Policy Manager icon.



- 2 This opens an empty Policy Manager. Select File > New.
- 3 You are asked to select a Firebox model



Select the model that matches your Firebox X (Fireware 8.0) and name the file. Click OK.

- 4 The untitled.xml Policy Manager for Fireware opens.



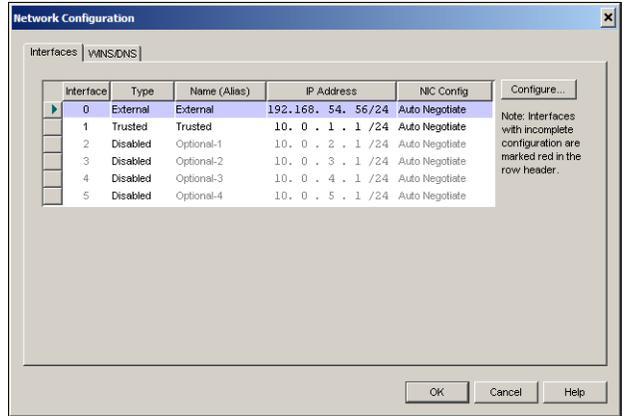
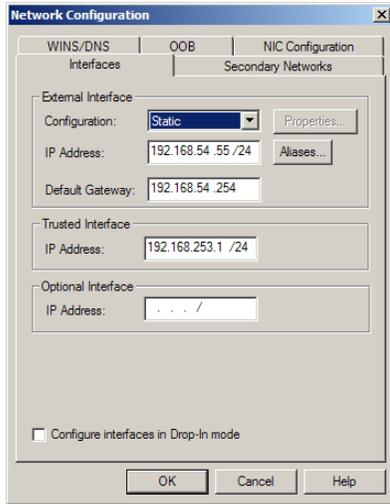
Working with Interfaces

The information in Fireware Policy Manager **Network > Configuration** is enhanced to give more flexibility on how each physical interface is mapped to a particular interface type, such as trusted, optional or external. For each interface defined in WFS Policy Manager, configure a matching

entry in Firewall Policy Manager by selecting the appropriate interface entry and clicking Configure. If an interface is not necessary, select Disabled as the interface type.

WFS 7.3 Network Configuration

Fireware Network Configuration



Multiple interfaces of a given type are available. This is what gives support for the new Multi WAN feature of Fireware.

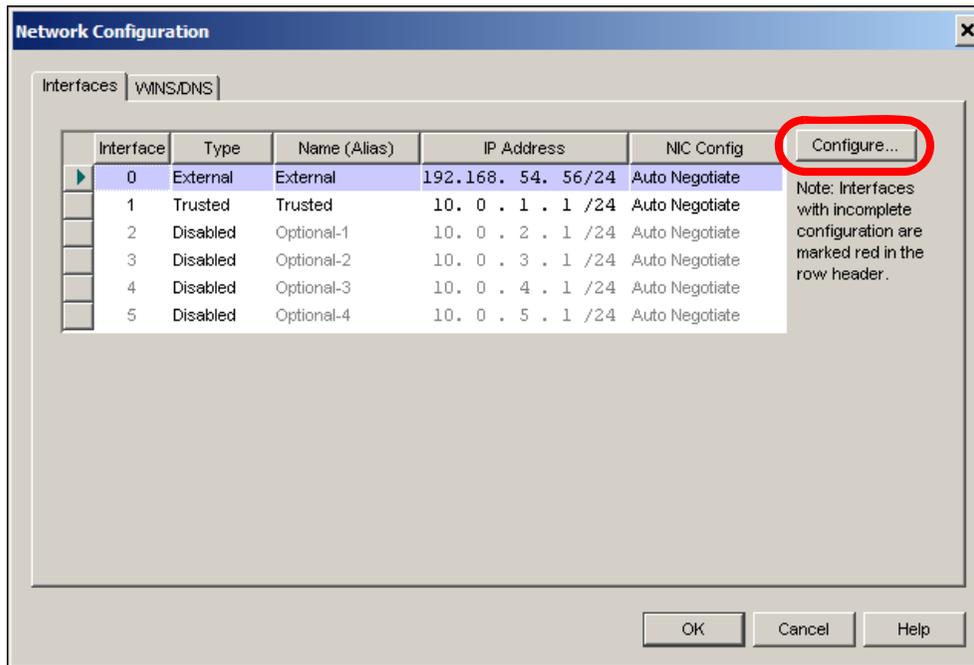
This dialog box is also where you create secondary networks as well as make any adjustments to the NIC speed.

NOTE

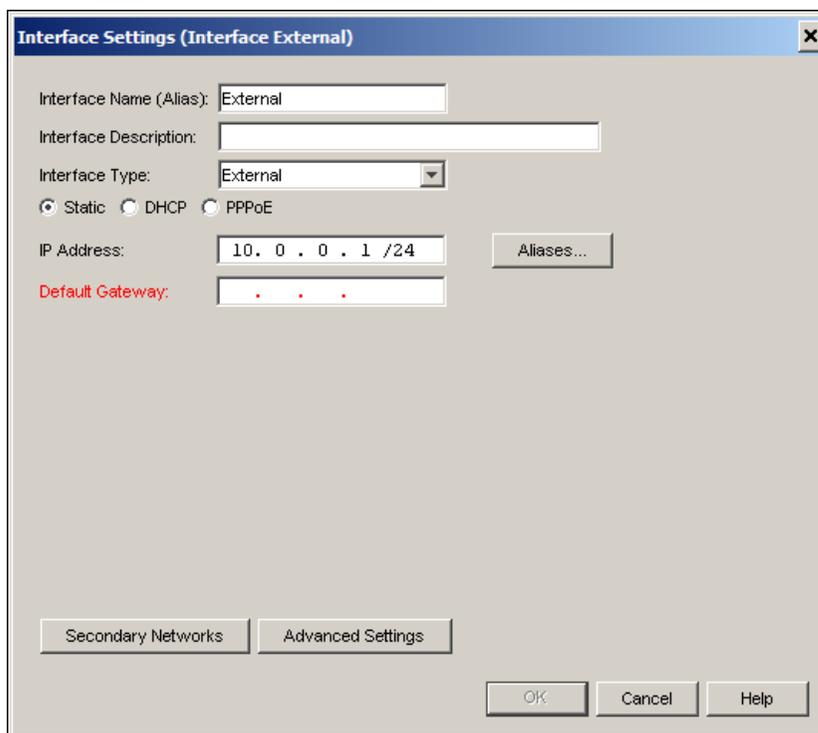
Fireware does not support aliases or secondary networks on an external interface using DHCP or PPPoE. You cannot migrate these items at this time.

Configuring your Network

- 1 Select an interface from Fireware Policy Manager Network > Configuration.



- 2 Click Configure.
The Interface Settings dialog box opens.

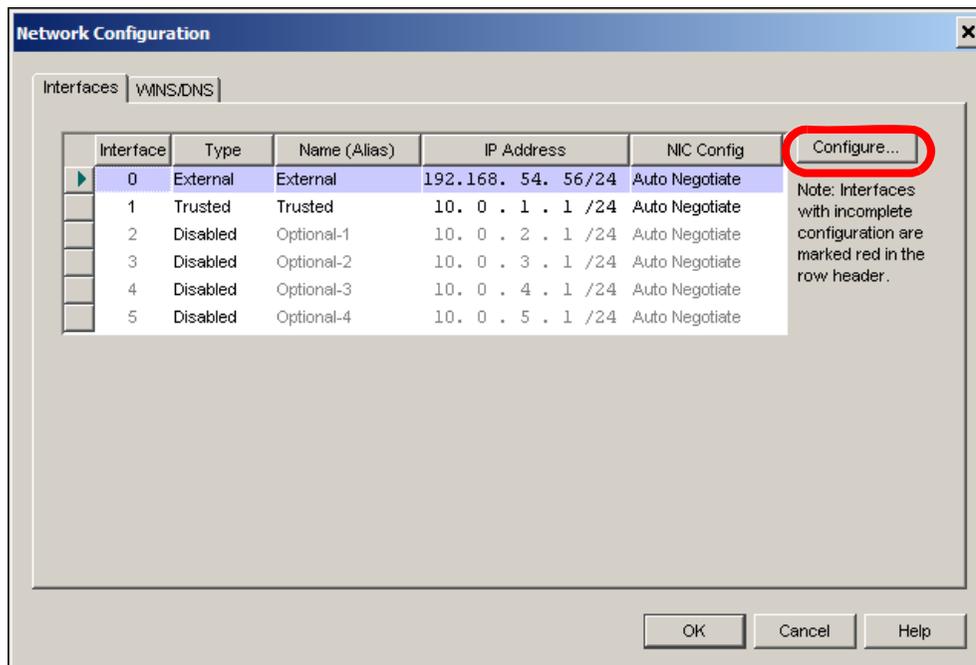


- 3 Type the interface name and description.

- 4 Select the interface type of truster, external, optional or disabled.
- 5 Select static, DHCP pr PPPoE.
- 6 Type the interface IP address.
- 7 Type the default gateway.
- 8 Click OK.

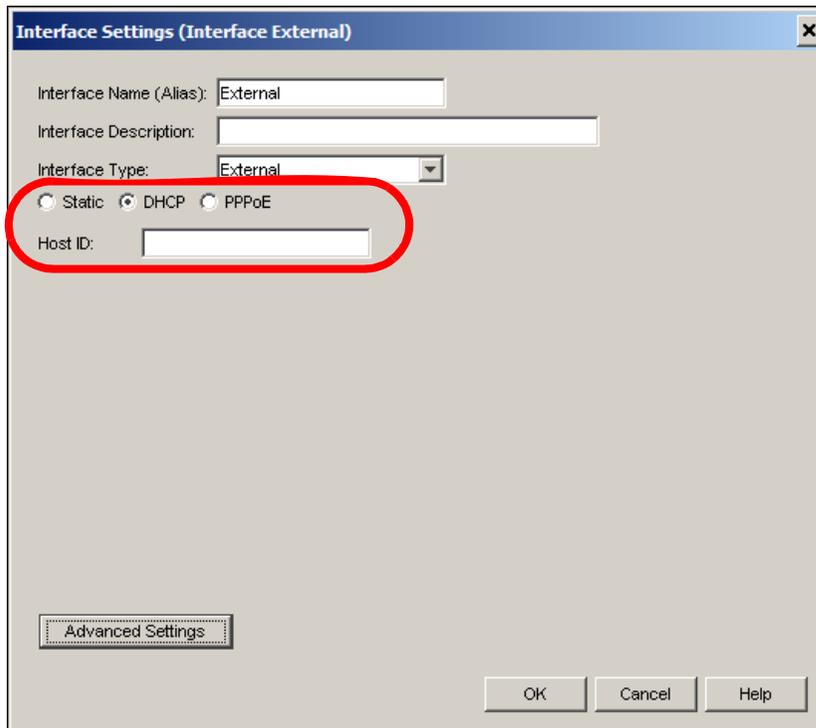
DHCP Server

- 1 From Fireware Policy Manager Network > Configuration.



- 2 Select any trusted or optional interface and click Configure.

- 3 Select the DHCP radio button and type the Host ID.



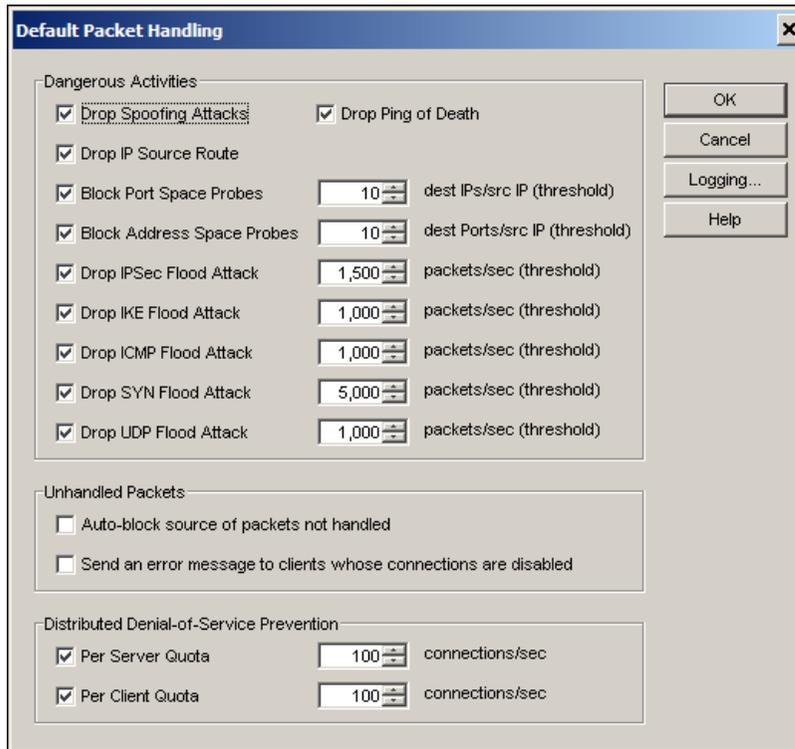
The screenshot shows a dialog box titled "Interface Settings (Interface External)". It contains the following fields and controls:

- Interface Name (Alias): External
- Interface Description: (empty text box)
- Interface Type: External (dropdown menu)
- Static DHCP PPPoE (radio buttons, with DHCP selected and circled in red)
- Host ID: (empty text box, circled in red)
- Advanced Settings (button)
- OK, Cancel, Help (buttons)

- 4 Click OK.

Note that with Fireware you must enable the DHCP server for each interface. The WFS DHCP server configuration took a list of address ranges and functions on the appropriate trusted or optional interfaces. With Fireware you specify the address ranges you want the server to hand out for each interface.

Intrusion Prevention/Default Packet Handling



Many of the same options are available in WFS Policy Manager. Nearly all the options are the same. However, by default, logging of broadcast traffic is turned on by default. To turn this off, add a policy that matches the traffic with logging disabled.

In the **Logging** dialog, the logging for **Incoming/Outgoing packets not handled** is managed by the **Logging** dialog from the **Default** policy.

Auto-block source of packets not handled is managed by added a new deny policy with the **Auto block sites that attempt to connect** checkbox selected. Be very careful to explicitly limit the From and To to a set of addresses that do not include valid traffic.

Fireware uses a new algorithm to block SYN flood attacks that is based upon threshold limits instead of validation.

Blocked Sites

Fireware's blocked sites support has changed so that this list can apply it to all interfaces. Be very careful to not add entries here that may also include any real networks accessible from the Firebox such as trusted, optional, external or other routed networks. If it is necessary to include

these (such as via a supernet), make certain to add a Blocked Sites Exceptions entry for the networks or hosts that are safe. .

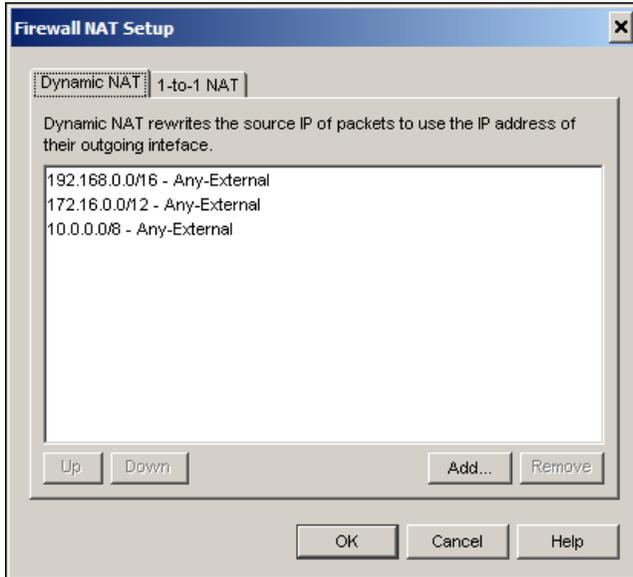


NOTE

If you list the IP address of your trusted network as a blocked site you create a Denial of Service (DOS) and effectively disable the trusted network.

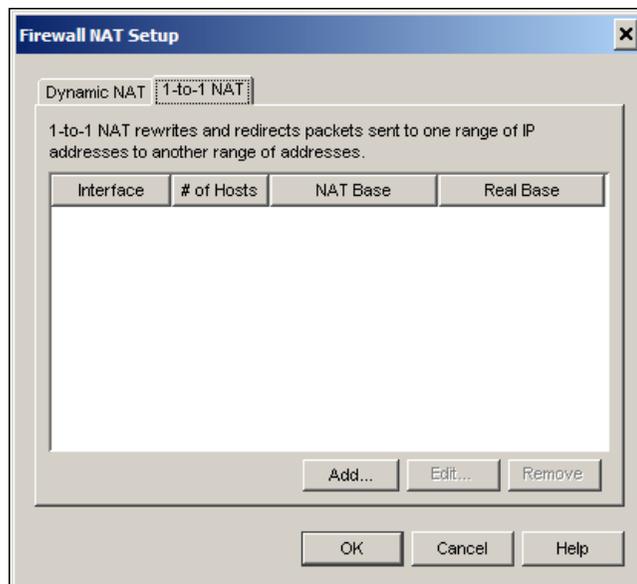
Network Address Translation (NAT)

Dynamic NAT



1-to-1 NAT Setup (Advanced)

- 1 Select the 1-to-1 NAT tab from Firewall Policy Manager Network > Firewall NAT.



- To add an entry click **Add**.

Add 1-to-1 Mapping

Type

Map Type: **IP Range**

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: No of Hosts to NAT:

NAT Base: Real Base:

OK Cancel

- Type the information and click **OK**.

Logging

The logging setup dialog has new selections in Fireware Policy Manager.

- From Policy Manger select **Setup > Logging**.

Logging Setup

Use these settings to configure where the Firebox will send log messages.

WatchGuard Log Server

Select the checkbox to send log messages to the WatchGuard Log Server.

Send log messages to the log servers at these IP addresses:

Syslog Server

Select the checkbox to send log messages to a Syslog server.

Send log messages to the Syslog server at this IP address:

Firebox Internal Storage

Select the checkbox to save log messages in Firebox Internal storage.

Send log messages in Firebox internal storage

OK Cancel Help

- 2 To add a log host click **Configure**.



- 3 Type an encryption key and then confirm it.

Encryption keys are a minimum of eight (8) characters.

- 4 To add a Syslog host select Syslog and click **Configure**.
- 5 Type the IP address of the Syslog Server.
- 6 Select a facility for each log type.
- 7 Click **OK**.

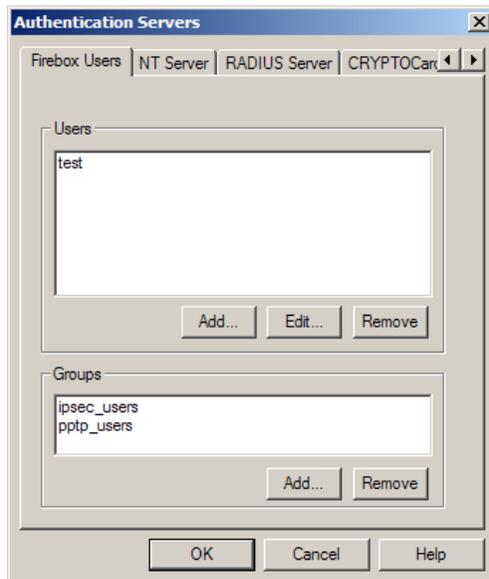
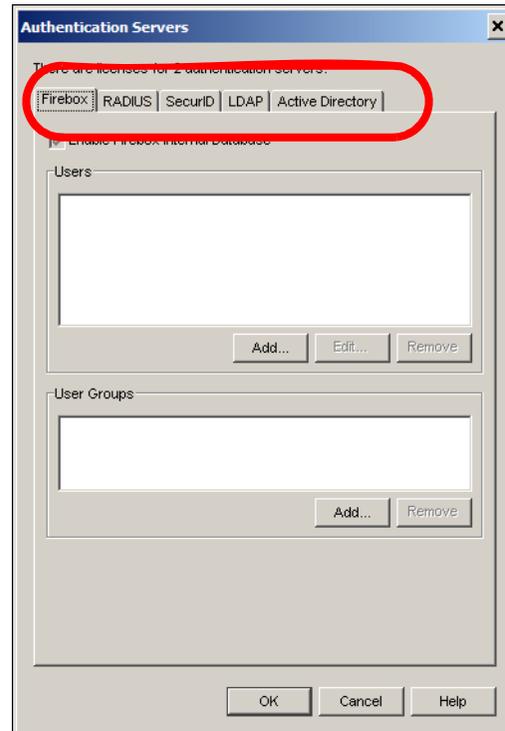
Firewall Authentication

The Java applet used for firewall authentication is no longer used. This eliminates the need for the time-outs listed here. Instead, a Web page is available at the same URL using https instead of http. The authentication mechanism relies on associated connections from the authenticated user to determine if the user is to remain authenticated. After some short time following the last closed or timed-out connection, the authenticated user is automatically logged out.

Authentication Servers

The same entry is available in Fireware Policy Manager.

- 1 From Policy Manager select **Setup > Authentication Servers**.
 - **Firebox**
There are no changes here. However, if you have either the pptp_users or ipsec_users groups listed, you do not need to migrate them. They are automatically migrated with your PPTP or MUVPN settings.
 - **NT Server**
Fireware does not support NT Server authentication. This cannot be migrated at this time.
 - **RADIUS Server**
Fireware uses PAP when authenticating any firewall or MUVPN user. It uses MSCHAPv2 when authenticating a PPTP user (if PPTP is configured to use RADIUS). Thus, the server needs to allow both mechanisms if both types of users are to be supported.
 - **CRYPTOCard Server**
Fireware does not support CRYPTOCard authentication. This cannot be migrated at this time.
 - **SecurID Server**
There are no changes.

WSM 7.x Firewall Authentication**WFS 8.0 Authentication Servers****Virtual Private Networking****Firebox Managed Clients**

The DVCP client only communicates with a WSM 8.0 management server. It is not backwards compatible with any previous version.

Remote User

From Policy Manager select VPN > Remote Users.

Mobile User VPN

Fireware only supports MUVPN using Extended Authentication Groups. If you are migrating MUVPN configurations using direct "Firebox Authenticated Users", simply go through the wizard and use the Firebox database as the Authentication Server.

Policies within Fireware are split into three sets, or arenas. The arenas are associated with either Firewall policies, VPN policies or MUVPN policies (as indicated by the three tabs in the main service arena).



In order to allow traffic across VPNs or MUVPNs, you must add policies to the associated arena.

Gateways

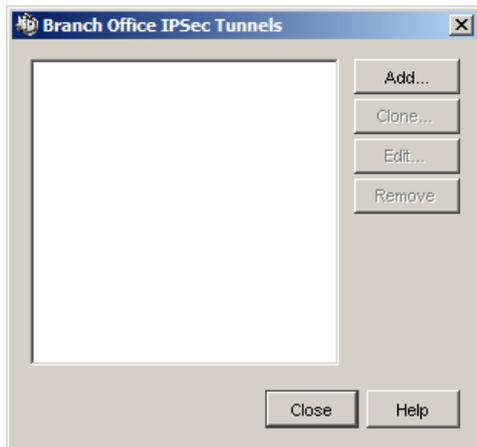
From Policy Manager select VPN > Branch Office Gateways.



Fireware does not support connection initiation to dynamic IP addressed peers. You cannot migrate this type of configuration at this time.

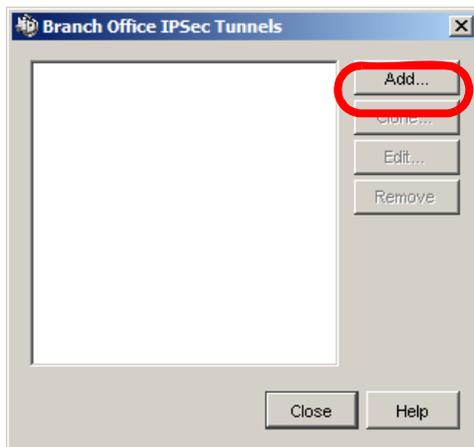
Tunnels

From Policy Manager select VPN > Branch Office Tunnels.

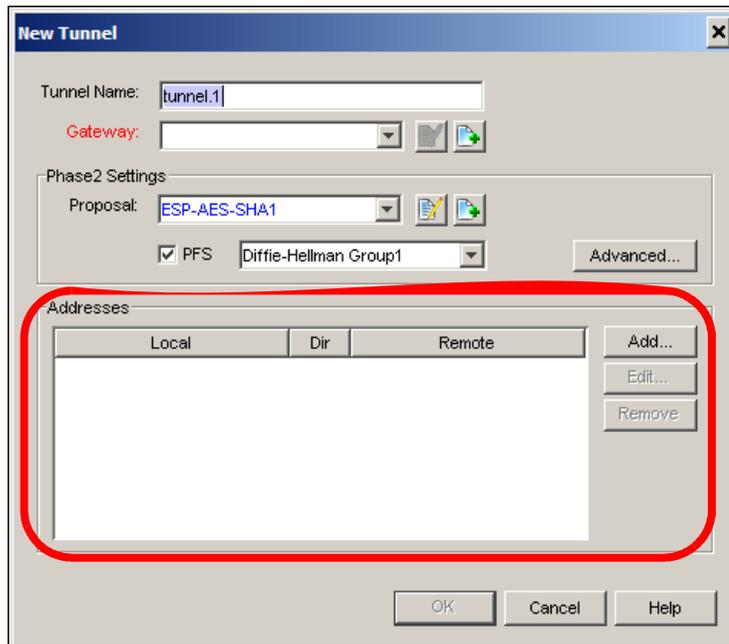


IPsec Routing Policies

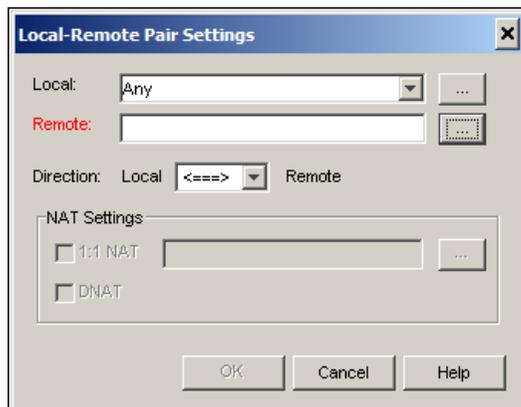
- 1 Adjust the Addresses section from Policy Manager VPN > Branch Office Tunnels.



- 2 Click Add.



- 3 In the Addresses section of the New Tunnel dialog box click Add.



- 4 Complete the information in the Local-Remote Pair Settings dialog box.
- 5 Click OK.

If the WFS routing policies configuration shows multiple policies using the same tunnel, then you cannot migrate this configuration. In Fireware, each entry in the "Addresses" section results in a set of SAs (a tunnel in WFS terms). Thus, the peer gateway also needs modification to accept multiple tunnels after migrating or the VPN does not negotiate successfully.

If any normal routes listed in WFS Policy Manager Network > Routes overlap or include an IPSec route, it may result in a tunnel that does not function. Fireware uses the normal route table to determine at which interface a tunnel is established. Thus, if a normal route exists pointing to the trusted interface and that route includes hosts or networks specified in the IPSec routes and that tunnel is meant to be established on the external interface, the tunnel will fail. The normal routes need to be broken up so that they do not include any entries in the IPSec routes or the normal routes need to point to the proper tunnel endpoint interface.

Services

Fireware handles services in a completely different manner than in WFS. The biggest change is the lack of **Incoming** and **Outgoing** tabs in what are now called policy icons.

Each policy icon now has a tab for configuring the familiar "From:" and "To:" traffic specification, a tab for viewing and managing the properties of the policy, and an advanced tab. When migrating a WFS Policy Manager service into the Fireware Policy Manager, you need to create at least one policy for the information represented by the WFS **Incoming** tab and one for the **Outgoing** tab. This change is only necessary when the current WFS connection setting is either **Enabled and Allowed** or **Enabled and Denied** with logging **Denied Packets** set.

The lack of direction associated with the policy means that it is implied by the traffic specification chosen. For example, a policy that allows traffic from Trusted to External represents a WFS service icon with the **Outgoing** tab set similarly. This mechanism provides a great deal of flexibility, especially when multiple types of physical interfaces are used. However, it also presents the potential for misusing the Any service when populating the "From:" and "To:" entries.

Keep in mind that Any literally means any traffic—trusted, optional or external. Initially, you need to restrict the use of this service as much as possible. When managing the first migration, apply "Any" only when no other policy is sufficient. For example, when migrating a WFS service that allows incoming from Any to Any, migrate it into a Fireware policy that allows from External to Firebox (maybe with a NAT entry specified to port forward the connections to a trusted server).

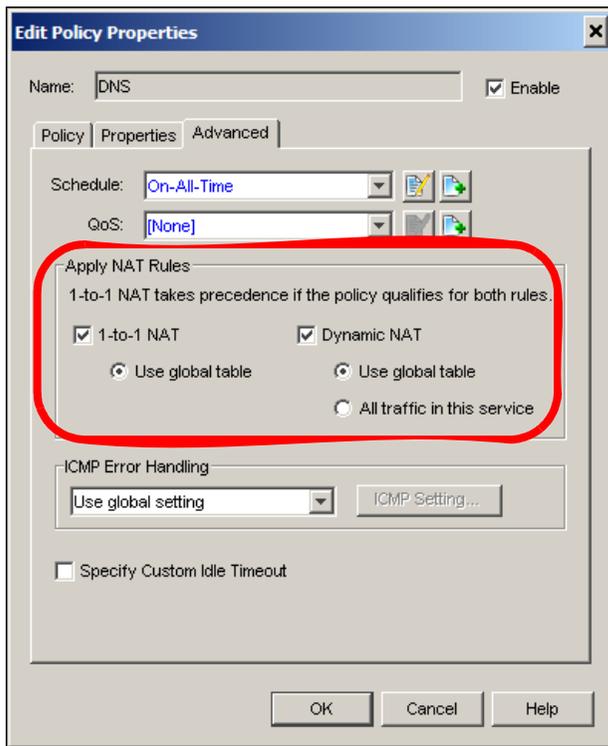
These name changes are for packet filter services:

WFS	Fireware 8.0
Outgoing	TCP-UDP
Outgoing-TCP	TCP
Outgoing-UDP	UDP
WatchGuard	WG-Firebox-Mgmt
WatchGuard-Logging	WG-Logging
WebBlocker	WG-WebBlocker
Soho_Management_Gateway	WG-SmallOffice-Mgmt

Service-based NAT

Fireware always has service-based NAT enabled. However, it still functions by default exactly as WFS versions do, making use of the "global" dynamic and 1-to-1 NAT tables in Fireware Policy Manager Network > Firewall NAT. If you have a policy that needs to manage NAT settings

differently than those provided by the global NAT tables, modify the Global NAT Rules on the Advanced tab.



CHAPTER 5 **Working with Proxies**

Fireware 8.0 proxy configuration offers new choices and more configuration possibilities than what is available in WSM 7.x. You have the ability to control more of the actions of each proxy while maintaining complete network security.

In this section you learn how to migrate your WFS 7.x proxies to Fireware 8.0:

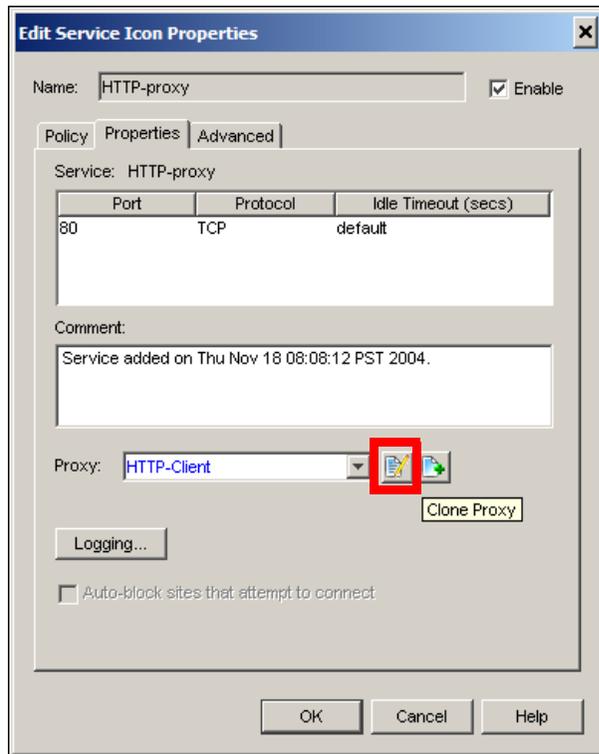
- FTP
- HTTP
- SMTP

For information about working with proxies see the Fireware Configuration Guide.

Proxy Migration

Services that are proxied have undergone some important changes.

The configuration associated with the proxies in Fireware is now separate from the policy. It is possible to create proxy configurations that are sharable between multiple policies. The product ships with suggested default configurations for the various proxied protocols for use in different scenarios. These default configurations can be referenced, but not changed. To modify a configuration, or action, there is a clone feature that allows you to create a new action based upon an existing action.



With the removal of directionality, the default proxy actions are named so that they represent typical situations in which they are used to protect resources. For example, there is an HTTP Client proxy. Client means that this proxy serves as protection for HTTP clients. In other words, it is most likely used on an outgoing policy.

Open proxy actions in Fireware Policy Manager Setup > Actions > Proxy Actions.

The best approach for adding proxied services is to use the same method as WFS and Policy Manager for Fireware Edit > Add Policies and select the best proxy for migration.

NOTE

Fireware no longer supports the DCE-RPC, H323 or RTSP proxies. There is a Netmeeting packet filter that does not support NAT. The Proxy and Proxied-HTTP proxies are replaced with the TCP-Proxy.

Proxy configuration for Fireware has many more features and flexibility than WFS. As a result, there are very few direct correlation points between what is configured in WFS Policy Manager and where it shows up in Fireware Policy Manager. The most important concept to understand is that the proxies in Fireware are all configured using similar mechanisms. Once understood, they provide a powerful tool to protect resources comprehensively and intelligently.

When configuring any proxy, the dialog is divided into three primary areas:

- Information at the top
- Categories on the left
- Detail configuration settings on the right

The categories are typically separated into areas for general settings, some protocol specific items, and then some common configuration items such as IPS and alarms. Some of the configuration categories display rulesets--embedded policy tables that are designed to selectively apply certain actions based upon particular protocol content.

NOTE

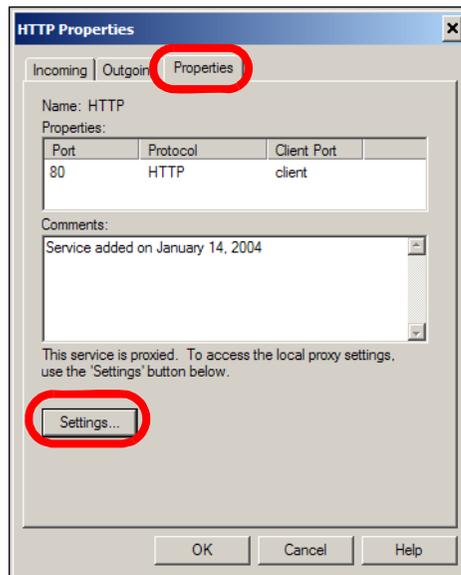
Watchguard System Manager v8.0 supports on the destination port only.

Configuring the HTTP Proxy

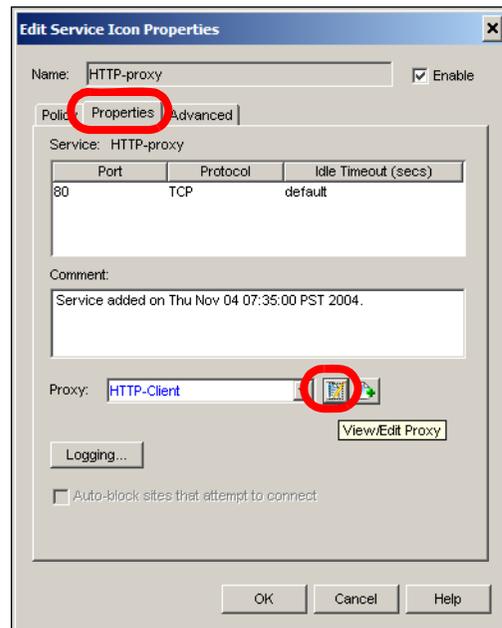
This section illustrates how various parameters are configured in the HTTP proxy in WFS 7.x and Fireware 8.0. Use this information as a guide when you create Fireware 8.0 policies that mirror your WFS 7.x policies.

From Policy Manager double-click the HTTP proxy icon and select the **Properties** tab.

WFS 7.x

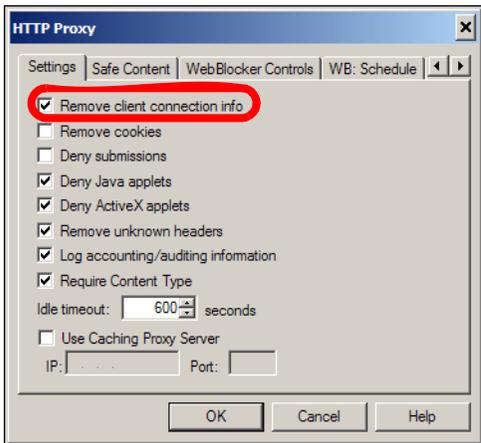


Fireware 8.0



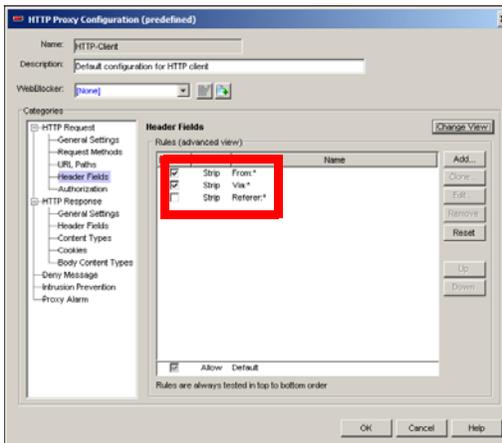
WFS 7.x

Settings > Remove client connection info



Fireware 8.0

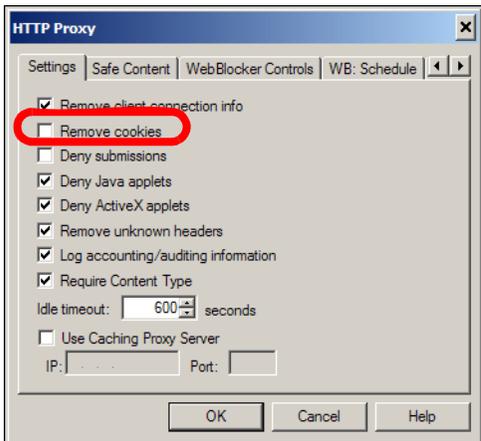
HTTP Request > Header Fields, strip or allow



the patterns "From:" and "Via"

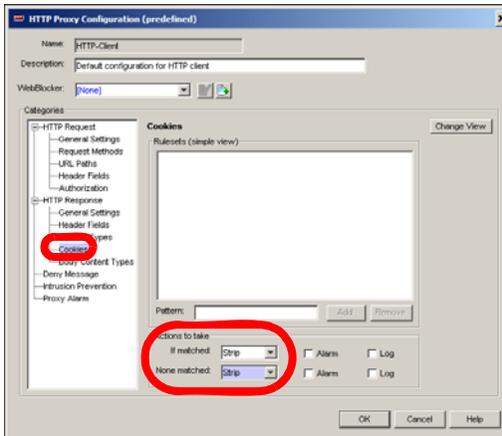
WFS 7.x

Settings > Remove cookies



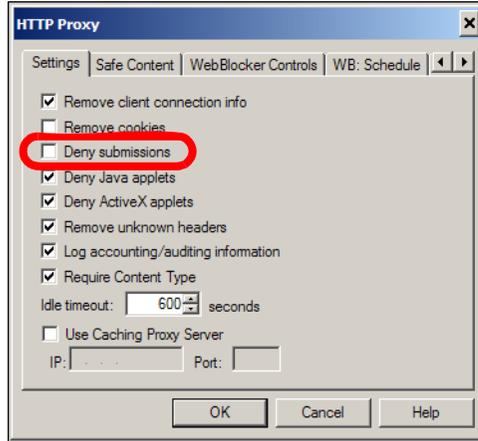
Fireware 8.0

HTTP Response > Cookies, set the "None matched" action to strip or allow



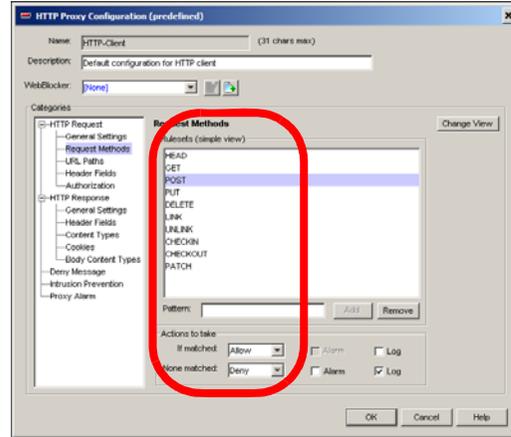
WFS 7.x

Settings > Deny submissions



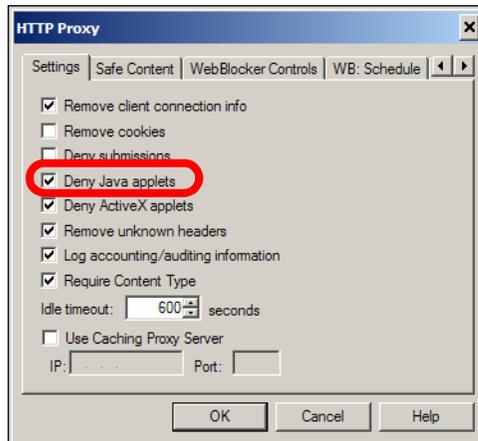
Fireware 8.0

In HTTP Request > Request Methods, deny or allow the pattern "POST"



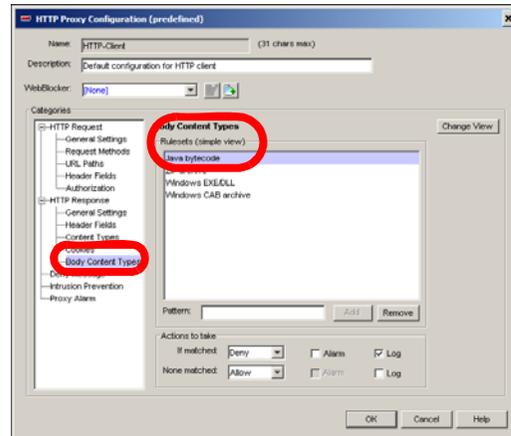
WFS 7.x

Settings > Deny Java applets



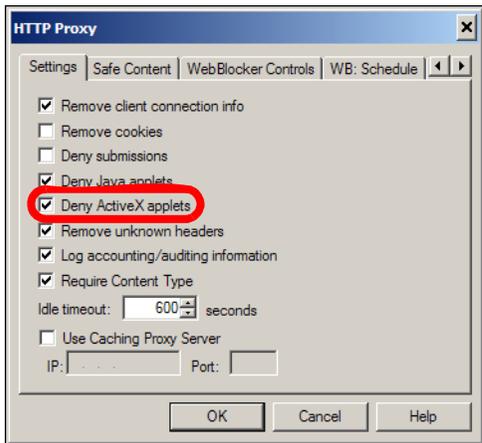
Fireware 8.0

In HTTP Response > Body Content Types, deny or allow the "Java bytecode" rule



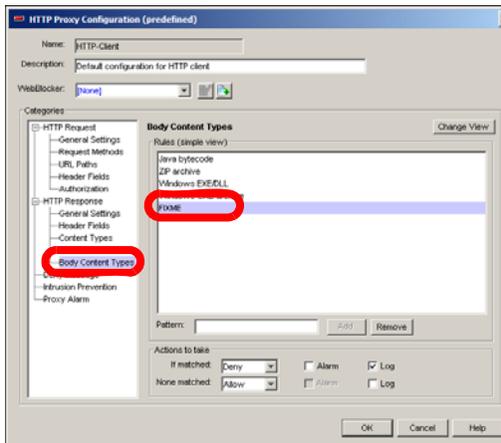
WFS 7.x

Settings > Deny ActiveX applets



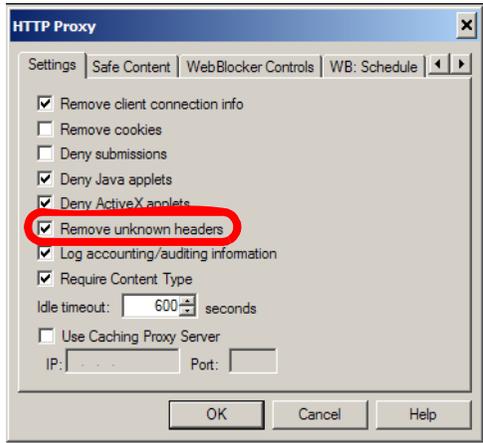
Fireware 8.0

In HTTP Response > Body Content Types, deny or allow the "FIXME" rule



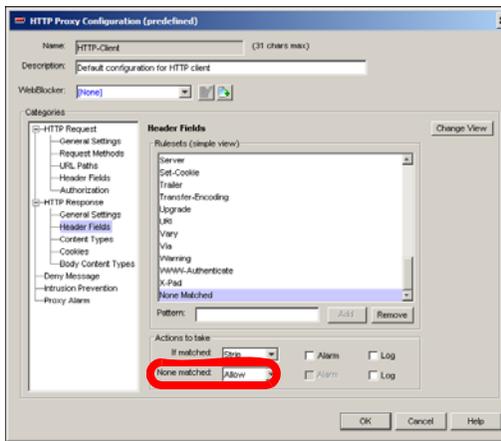
WFS 7.x

Settings > Remove unknown headers



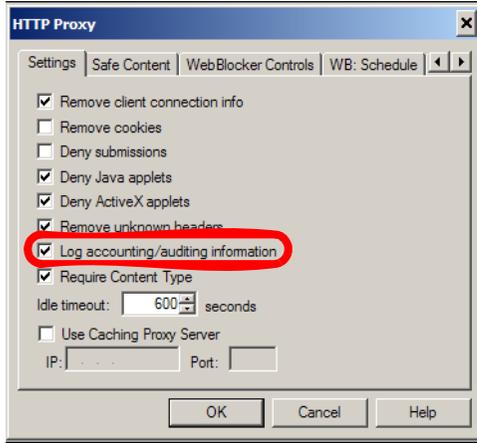
Fireware 8.0

In HTTP Response > Header Fields, set the "None matched" action to strip or allow



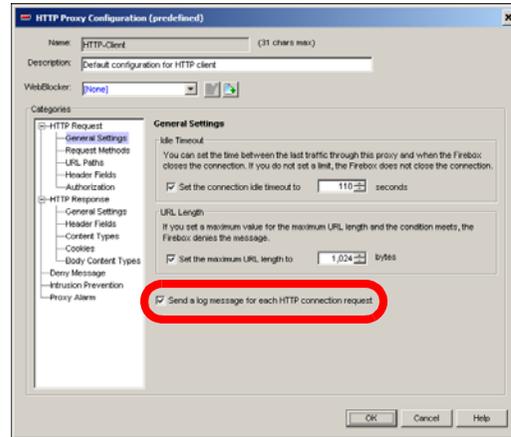
WFS 7.x

Settings > Log accounting/auditing information



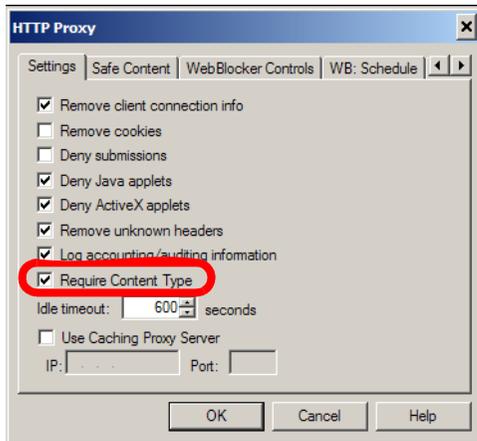
Fireware 8.0

In HTTP Request > General Settings, toggle "Send a log message for each HTTP connection request"



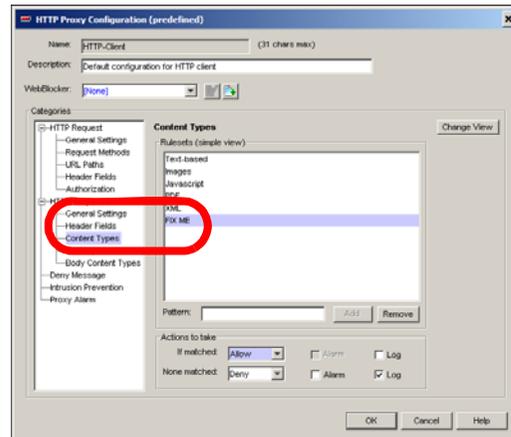
WFS 7.x

Settings > Require Content Type



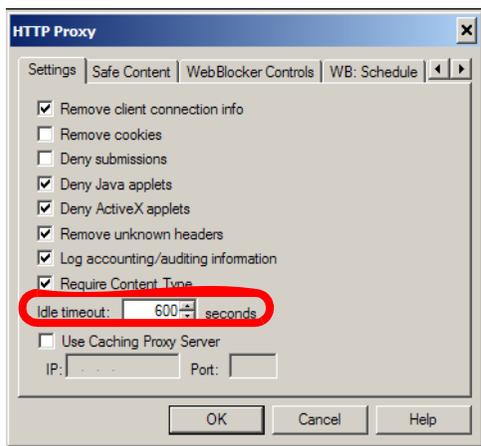
Fireware 8.0

In HTTP Response > Content Types, enable or disable the "FIXME" rule.



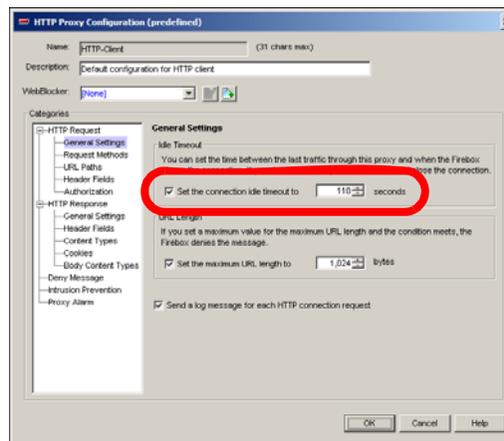
WFS 7.x

Settings > Idle timeout



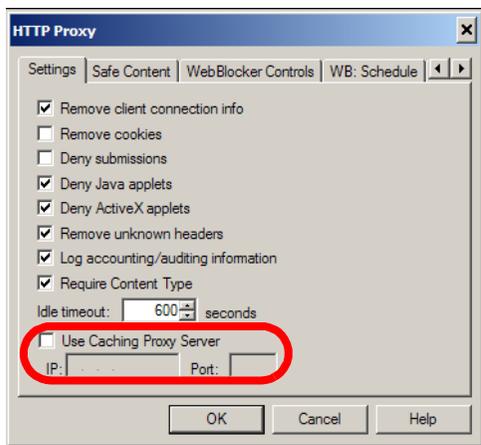
Fireware 8.0

In HTTP Request > General Settings, adjust the "Idle Timeout"



WFS 7.x

Settings > Use Proxy Cache Server

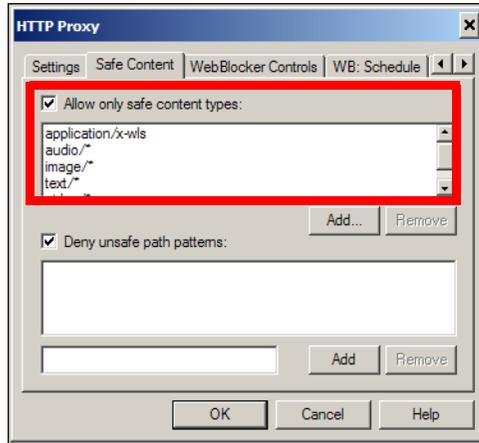


Fireware 8.0

Fireware does not currently support this feature. You cannot migrate this parameter.

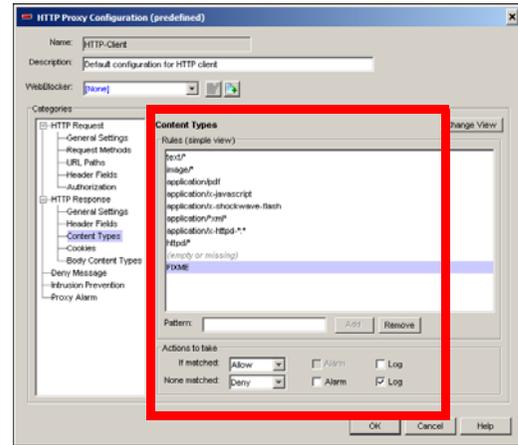
WFS 7.x

Safe Content > Allow only safe content types



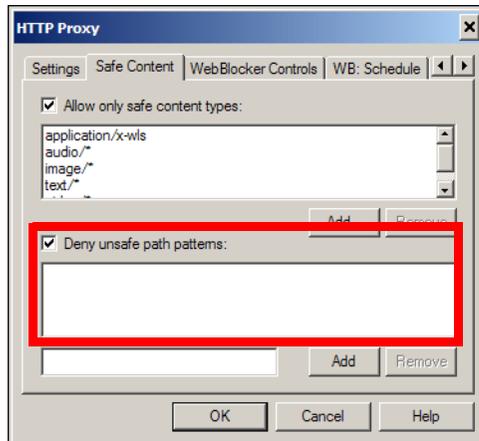
Fireware 8.0

HTTP Response > Content types



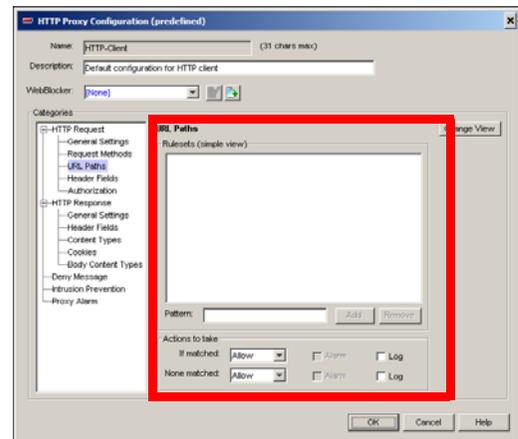
WFS 7.x

Safe Content > Deny Unsafe Path Patterns



Fireware 8.0

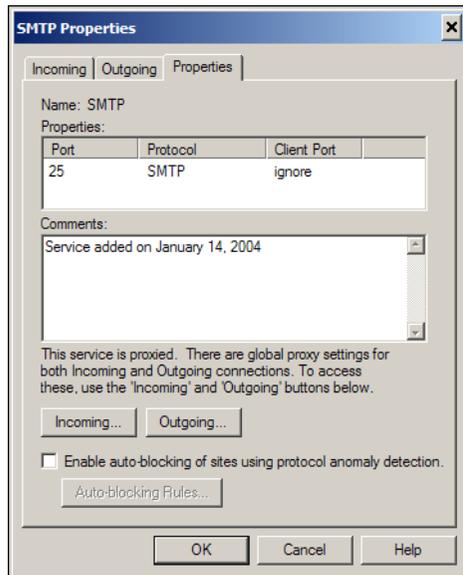
HTTP Request > URL Paths



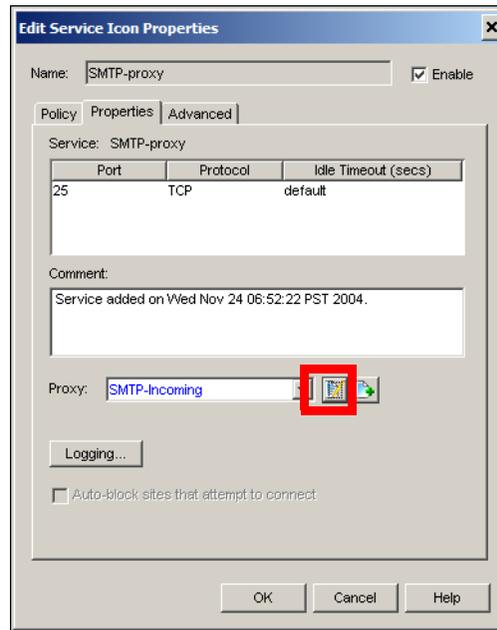
Configuring the Incoming SMTP Proxy

This section illustrates how various parameters are configured in the incoming SMTP proxy in WFS 7.x and Fireware 8.0. Use this information as a guide when you create Fireware 8.0 policies that mirror your WFS 7.x policies.

WFS 7.x



Fireware 8.0



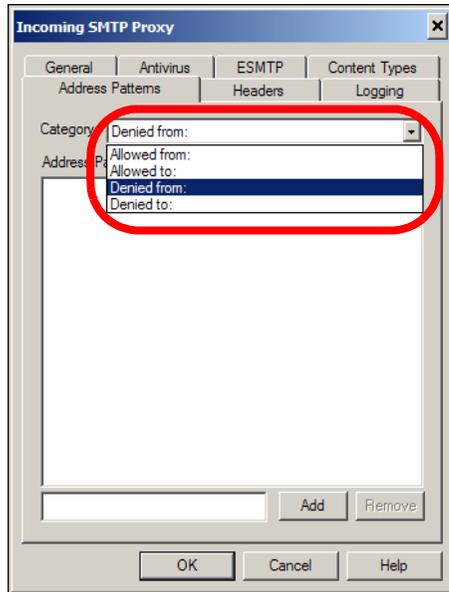
Clone the SMTP-Incoming Proxy Action

General

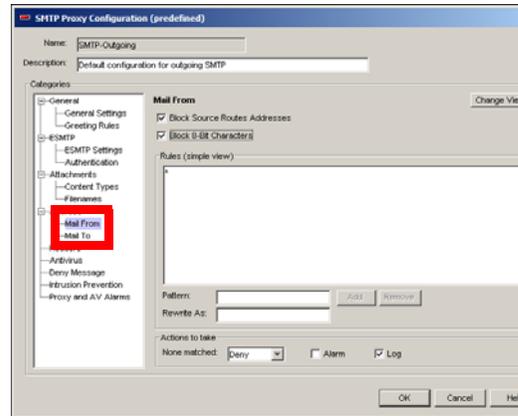
Some of this information is available in **General > General Settings**. The "Address Validation (RFC-822 Compliance)" is now managed in **General > Greeting Rules** by the "Non-allowed characters" rule.

Address Patterns

WFS 7.x



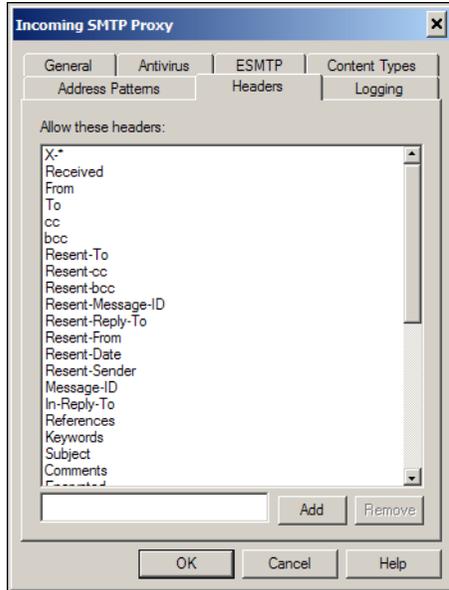
Fireware 8.0



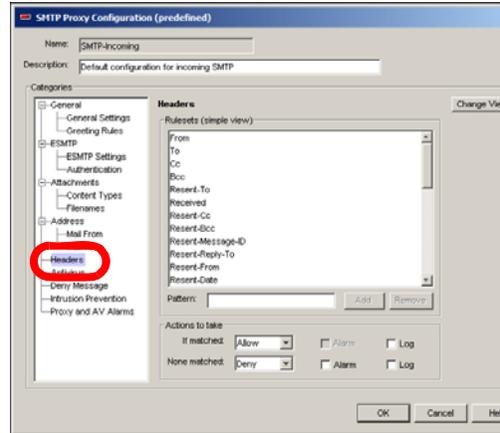
If there is a mixture of allowed and denied entries, you must change the ruleset view and apply the different actions on a per-rule basis.

Headers

WFS 7.x

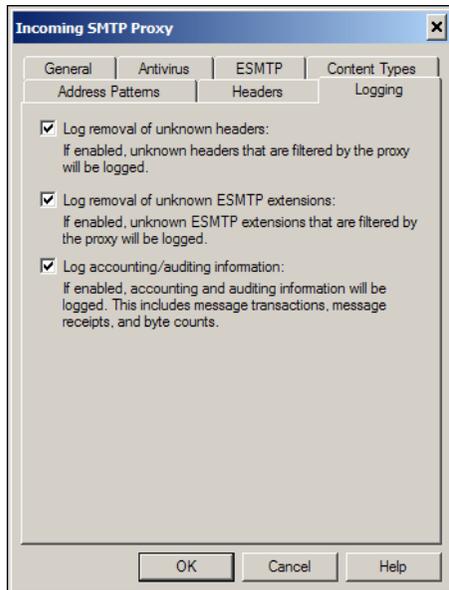


Fireware 8.0

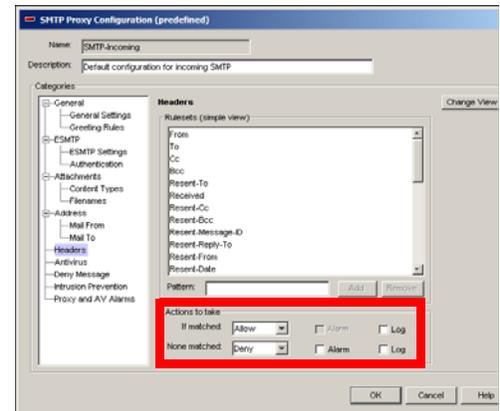


Logging

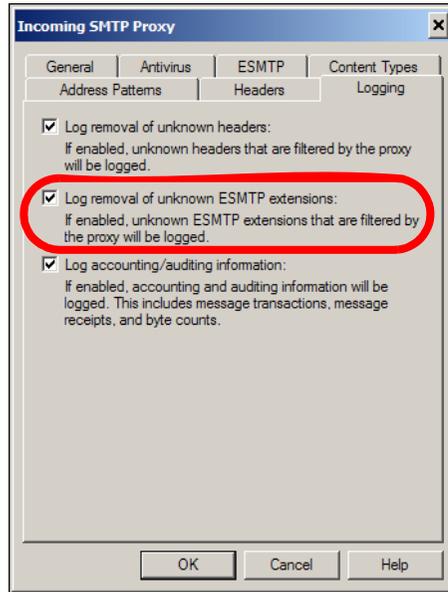
WFS 7.x



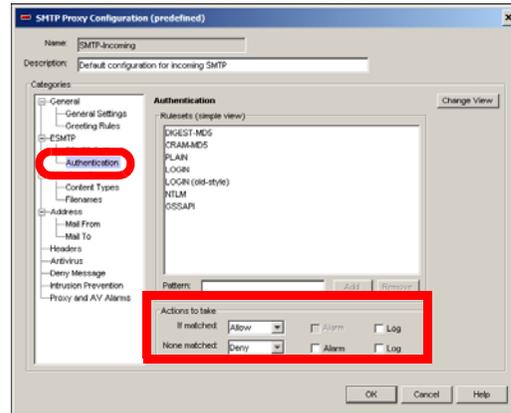
Fireware 8.0



WFS 7.x

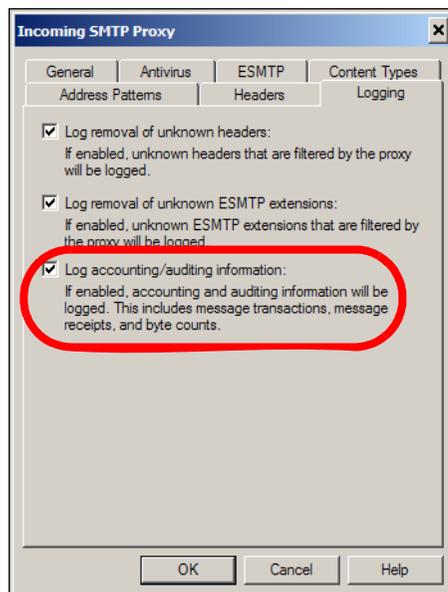


Fireware 8.0

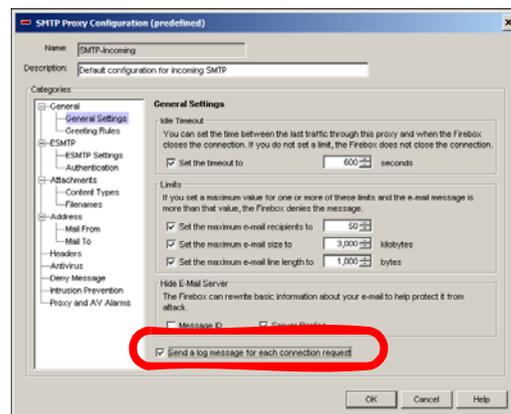


“Log accounting/auditing information” is the “Send a log message for each connection request” in General > General Settings.

WFS 7.x



Fireware 8.0



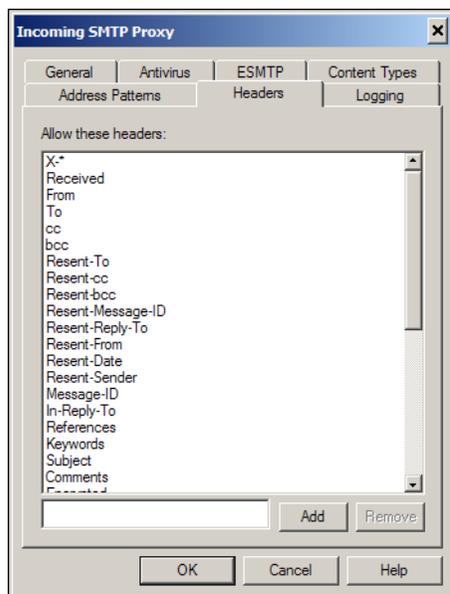
Outgoing SMTP

This section illustrates how various parameters are configured in the outgoing SMTP proxy in WFS 7.x and Fireware 8.0. Use this information as a guide when you create Fireware 8.0 policies that mirror your WFS 7.x policies.

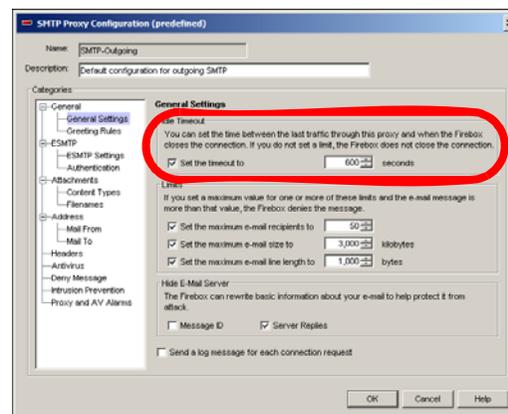
Clone the SMTP Outgoing proxy action

General

WFS 7.x



Fireware 8.0

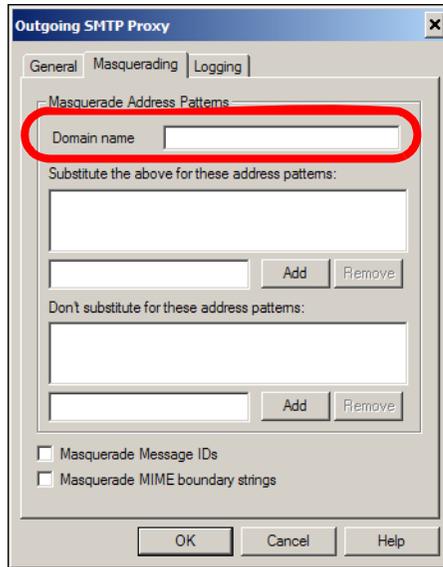


“Allow these Header Patterns” is available in Headers.

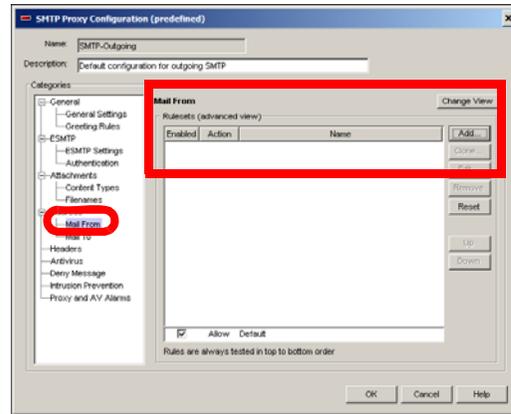
“Idle” value is available in General > General Settings.

Masquerading

WFS 7.x

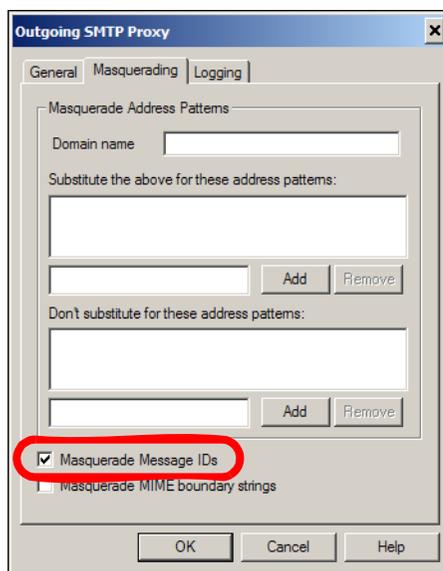


Fireware 8.0

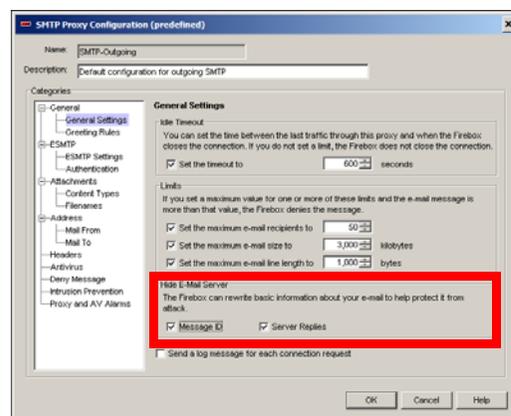


Build Any patterns in the Address > Mail From ruleset under the "advanced view" (click "Change View"). When you add a rule here, you have the option of specifying a "Replace" action. The "Domain Name" listed in WFS is the value with which to replace it.

WFS 7.x



Fireware 8.0

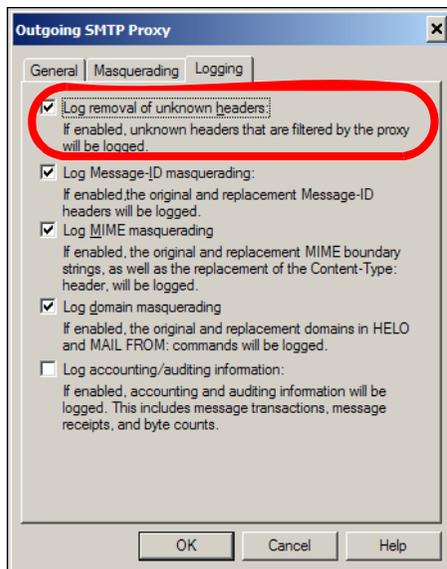


“Masquerade Message IDs” is not fully available in Fireware. You can rewrite the user ID portion of the Message ID by enabling the “Message ID” checkbox in General > General Settings > Hide E-Mail Server.

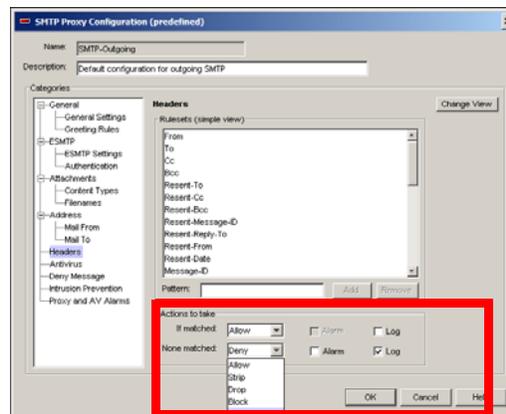
“Masquerade MIME boundary strings” is not available in Fireware. You cannot migrate this setting.

Logging

WFS 7.x



Fireware 8.0

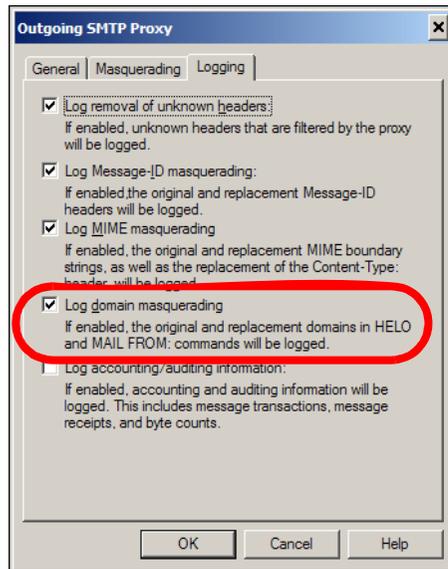


“Log removal of unknown headers” is the “Log” checkbox in the “None matched” action from “Actions to take” within Headers.

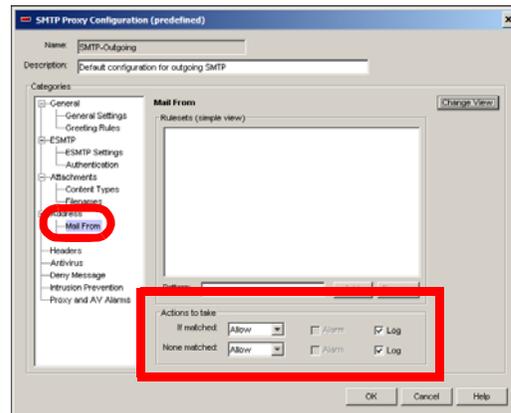
“Log Message-ID masquerading” is not available in Fireware. You cannot migrate this setting.

“Log MIME masquerading” is not available in Fireware. You cannot migrate this setting.

WFS 7.x

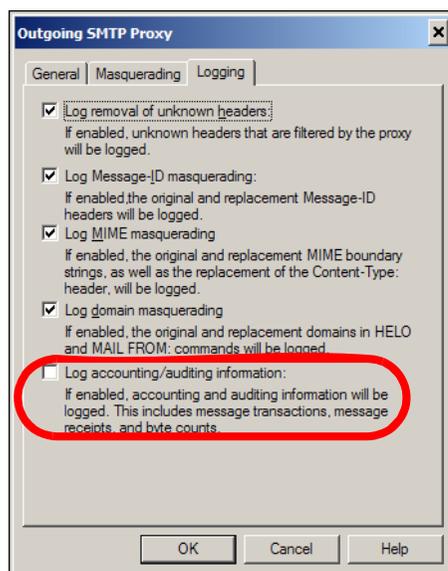


Fireware 8.0

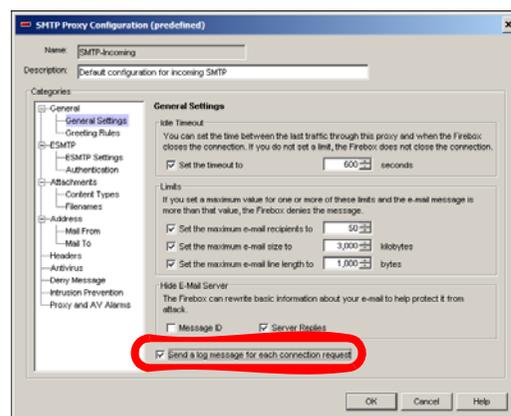


”Log domain masquerading” is available via the ”Log” checkbox in the ”Rule actions” section of Address > Mail From for any rule that is added.

WFS 7.x



Fireware 8.0



”Log accounting/auditing information” is the ”Send a log message for each connection request” in General > General Settings.

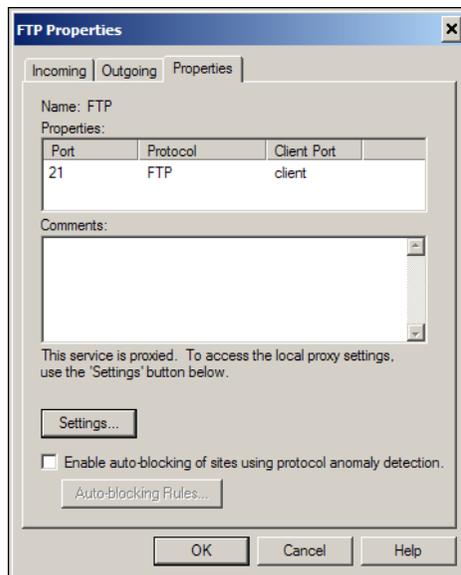
FTP Proxy

This section illustrates how various parameters are configured in the FTP proxy in WFS 7.x and Fireware 8.0. Use this information as a guide when you create Fireware 8.0 policies that mirror your WFS 7.x policies.

Clone the FTP-Client or FTP-Server proxy action.

WFS 7.x

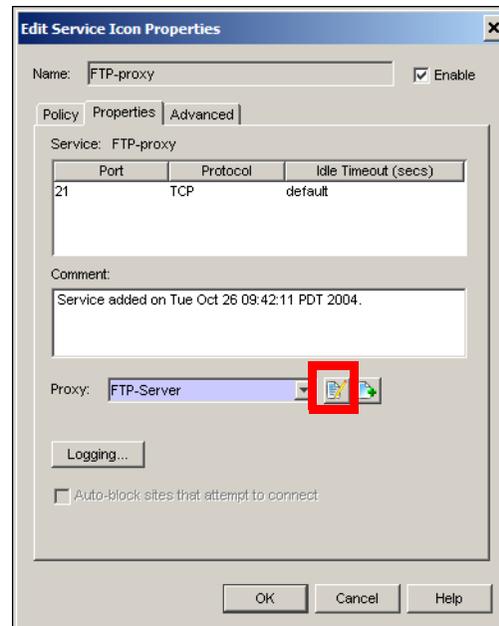
Make incoming FTP connections read



only

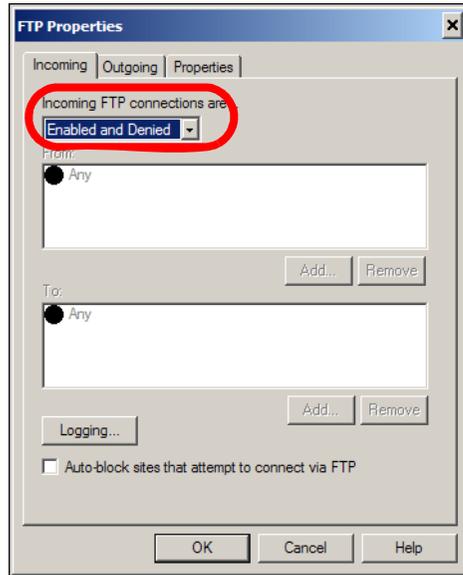
Fireware 8.0

Set the "Upload" "Actions to take" "If matched:" and "None matched" to "Deny"



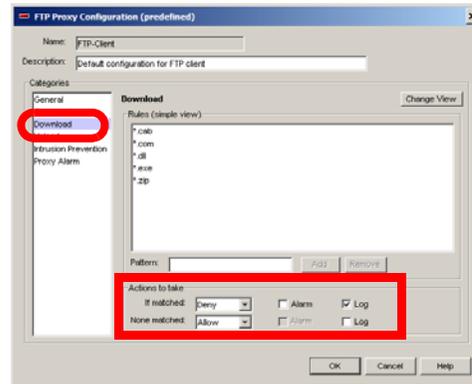
WFS 7.x

Make connections ready only



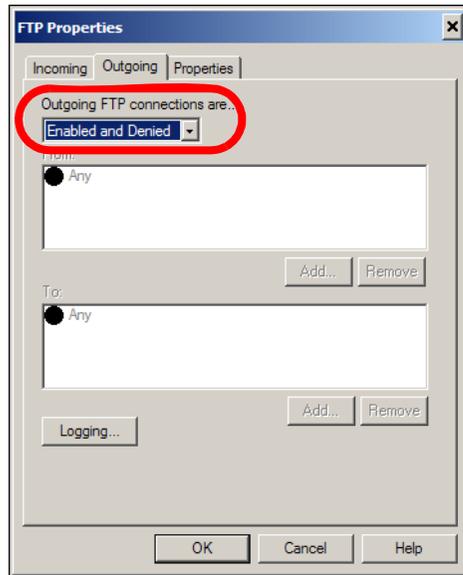
Fireware 8.0

Make connections ready only



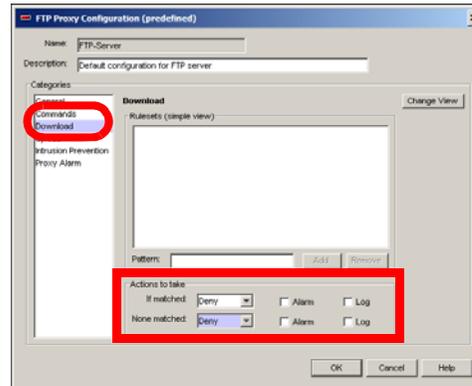
WFS 7.x

Deny incoming SITE command

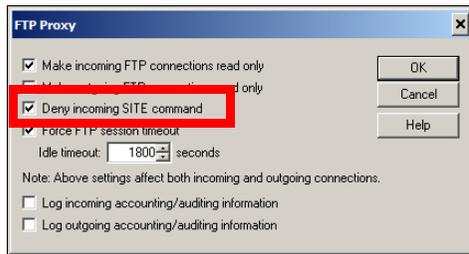


Fireware 8.0

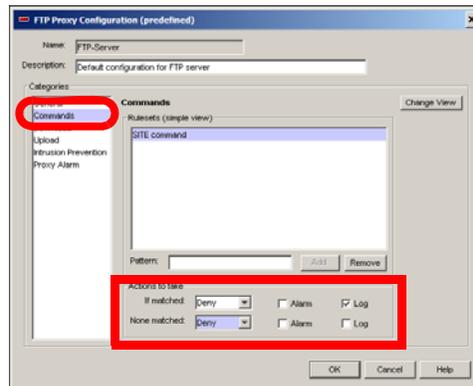
Restrict the SITE command from the allowed list in the "Commands" ruleset.



WFS 7.x



Fireware 8.0

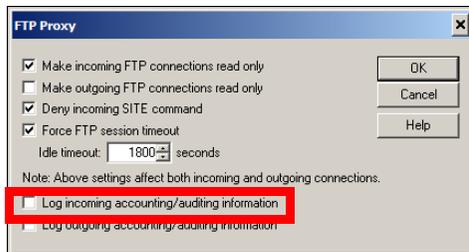


Force FTP session timeout is not available in Fireware. You cannot migrate this option.

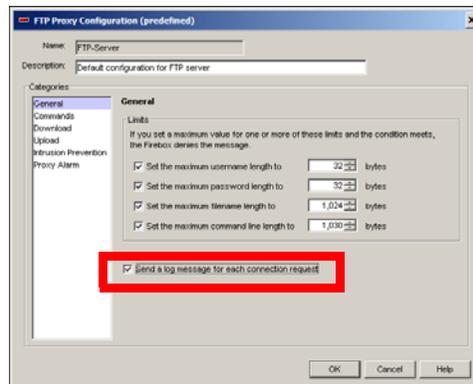
“Log incoming accounting/auditing information”

Enable the “Send a log message for each connection request” checkbox.

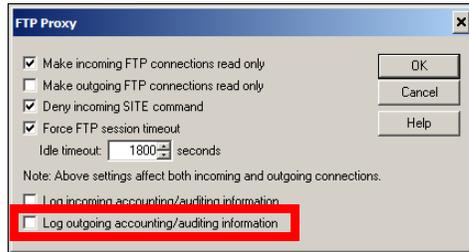
WFS 7.x



Fireware 8.0



WFS 7.x



Fireware 8.0

