

# WatchGuard<sup>®</sup> WFS to Fireware<sup>®</sup> Pro Migration Guide

---

WatchGuard System Manager v8.3  
WatchGuard Firebox System v7.4.1



---

## Notice to Users

---

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

## Copyright, Trademark, and Patent Information

---

Copyright© 1998 - 2006 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 subfolder 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: 8.3-352-2674-001

---

### ADDRESS:

505 Fifth Avenue South  
Suite 500  
Seattle, WA 98104

### SUPPORT:

[www.watchguard.com/support](http://www.watchguard.com/support)  
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](http://www.watchguard.com).

# Contents

---

CHAPTER Introduction .....	1
Introducing WatchGuard System Manager 8.3 and Fireware 8.3 .....	1
Using Multiple Versions of Appliance Software .....	1
WatchGuard Servers .....	2
Comparing WFS and Fireware .....	3
<i>Appliance software feature matrix</i> .....	3
Planning Your Migration .....	7
Upgrading Subscription Services .....	7
Using this Migration Guide .....	8
CHAPTER Migrating from WFS 7.x (No VPN Manager) to Fireware Pro .....	9
Migrating to Fireware .....	9
Documenting Your Current Security Policy .....	9
Backing Up Your WFS Configuration and Firebox Image .....	10
<i>Saving your configuration file</i> .....	10
<i>Saving the Firebox software image</i> .....	11
Documenting VPN Tunnels .....	11
Installing Software on the Management Station .....	11
Installing Fireware on Your Firebox .....	12
<i>Using the Quick Setup Wizard</i> .....	12
<i>Using fbxinstall.exe</i> .....	13
CHAPTER Migrating from WFS 7.3 with VPN Manager to Fireware Pro .....	15
Migrating to Fireware .....	15
Documenting Your Security Policy .....	16
Backing Up Your WFS Configuration and Firebox Image .....	16
<i>Saving your configuration file</i> .....	16

<i>Saving the Firebox software image</i> .....	17
Documenting VPN Tunnels .....	17
Installing Software on the Management Station .....	17
Introducing the WatchGuard Management Server .....	18
<i>Management Server license</i> .....	18
Migrating Your VPN Manager Data to a Management Server .....	19
<i>If the Firebox was a VPN Manager DVCP server</i> .....	19
<i>If the Firebox was a Basic DVCP server</i> .....	19
<i>Running the Management Server Setup wizard</i> .....	20
Installing Fireware on Your Firebox .....	20
<i>Using the Quick Setup Wizard</i> .....	20
<i>Using fbxinstall.exe</i> .....	21
CHAPTER Migrating from WSM 8.x/WFS 7.4 to Fireware Pro .....	23
Migrating to Fireware .....	23
Documenting Your Security Policy .....	23
Backing Up Your WFS Configuration and Firebox Image .....	24
<i>Saving your configuration file</i> .....	24
<i>Saving the Firebox software image</i> .....	25
Documenting VPN Tunnels .....	25
Installing Software on the Management Station .....	25
Installing Fireware on Your Firebox .....	26
<i>Using the Quick Setup Wizard</i> .....	26
<i>Using fbxinstall.exe</i> .....	27
CHAPTER Using Fireware Policy Manager .....	29
Rebuilding Your Network Configuration with Fireware Policy Manager .....	29
<i>Opening Policy Manager</i> .....	30
<i>Working with interfaces</i> .....	30
<i>Secondary networks and external alias addresses</i> .....	31
<i>DHCP Server</i> .....	32
Network Address Translation (NAT) .....	33
Virtual Private Networking .....	34
<i>MUVPN and Fireware</i> .....	35
<i>BOVPN and Fireware</i> .....	35
Services .....	35
<i>Using the policy generated by the Quick Setup Wizard</i> .....	35
<i>Using the "Any" alias</i> .....	36
<i>Policy Manager and Firebox management</i> .....	36
Proxies .....	36
<i>Quick Setup Wizard and proxies</i> .....	37
Authentication .....	38
<i>Authenticating through the Firebox</i> .....	39
<i>Authentication time-outs</i> .....	39

---

<i>Using Firebox System Monitor to close authentication sessions</i> .....	39
Intrusion Prevention/Default Packet Handling .....	40
<i>Blocked Sites</i> .....	40



# Introduction

---

## Introducing WatchGuard System Manager 8.3 and Fireware 8.3

---

WatchGuard® System Manager (WSM) 8.0 was an important software release for WatchGuard customers. With the WSM 8.0 release, we introduced Fireware® appliance software.

Fireware is the next generation of security appliance software available from WatchGuard. Appliance software is the software that supplies the run-time instructions for the Firebox to correctly operate. Management software is the software application that you install on a computer to configure, monitor, and control the Firebox. It sends instructions to the appliance software you install on the Firebox.

WatchGuard System Manager v8.3 supports three versions of appliance software:

- Fireware- This is the default appliance software on Firebox X Core e-Series devices. This next generation appliance software enables WatchGuard to expand the number of features available to Firebox X customers.
- Fireware Pro - This is the default appliance software on Firebox X e-Series Peak appliances. Its advanced network features include dynamic routing, High Availability, and QoS. It enables customers with complex networks to more effectively protect their networks. Fireware Pro is available as an update for previously released Firebox X Core devices.
- WatchGuard Firebox System (WFS) - This is the default appliance software on Firebox X Core appliances.

This *Migration Guide* is written for users who have Firebox X Core devices running WFS appliance software and want to migrate to Fireware appliance software and take advantage of the new features and functionality available with Fireware. There is no automated migration tool available at this time.

Because of this, you must prepare a migration plan to match the requirements of your Firebox installation. This guide will help you prepare and deploy your migration plan.

---

## Using Multiple Versions of Appliance Software

---

When you install WatchGuard System Manager, it automatically installs the software tools you must have to configure and manage a Firebox X Core or Peak with any version of appliance software that can run on your Firebox. These include:

- Fireware Firebox System Manager and WFS Firebox System Manager
- Fireware Policy Manager and WFS Policy Manager
- Fireware HostWatch and WFS HostWatch

When you use WatchGuard System Manager to connect to a Firebox, it identifies which appliance software the Firebox uses. If you select a Firebox, and then click a management tool icon, WatchGuard System Manager automatically starts the correct management tool for the version of appliance software installed on that Firebox.

For example, connect to a Firebox X5000 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.

You cannot install more than one version of WSM 8.x on your management station at the same time. However, you can install WSM 7.4.1 or earlier on the same management station on which you have installed WSM 8.x. You might want to do this because:

- You want to see WFS 7.4.1 and WSM 8.x on the same computer so you can use WFS 7.4.1 as a base for your new Fireware configuration file.
- You want to continue to use VPN Manager to manage a Firebox that has not yet migrated to Fireware.

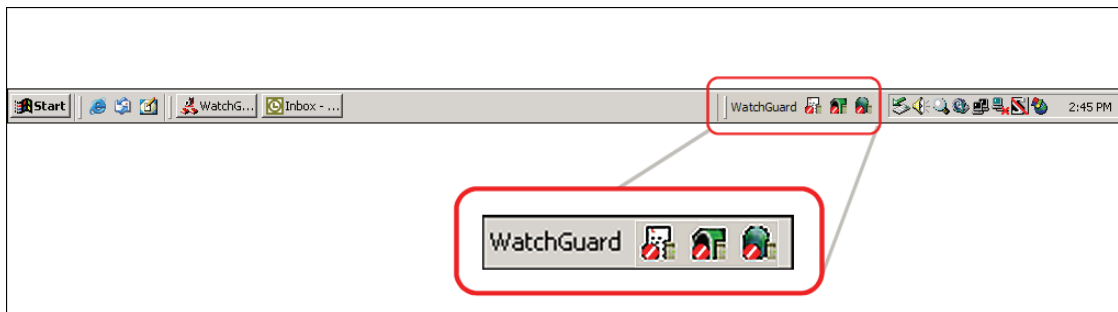
---

## WatchGuard Servers

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

- Management Server
- Log Server
- WebBlocker Server

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



### Management Server

With WFS, WatchGuard enabled simple VPN configuration with the Dynamic VPN Configuration Protocol (DVCP) and VPN Manager. With VPN Manager you could control the VPN tunnels of a distributed enterprise from one easy-to-use management interface using DVCP. In earlier versions of WSM, the DVCP server had to operate on a Firebox.

With WSM 8.x, the VPN Manager functionality is replaced with WatchGuard Management Server. You install the Management Server on a computer with the Windows operating system. This increases scalability and flexibility for the network administrator. The Management Server has the same functions as the DVCP server from previous releases of WSM. These functions are:

- 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 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 so users cannot browse 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

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

### Appliance software feature matrix

There are significant differences between the WFS appliance software and the new Fireware appliance software. A summary of these differences is shown in the table below. When both appliance software packages include a feature, but Fireware implementation is different from WFS, we include more information in the last column.

Feature or Functional Area		WFS	Fireware	Fireware Pro	Notes on Fireware/Fireware Pro Implementation
<b>Upgradeable</b>	Model Upgradeable	Yes	Yes	Yes	
<b>Networking Features</b>	Interface Independence	No	Yes	Yes	Fireware offers flexible interface configuration. Any available Firebox interface can be configured as external, trusted, or optional.
	Default Firebox Trusted interface IP address	192.168.253.1	10.0.1.1	10.0.1.1	
	Interface trust relationships	Forced	User-defined	User-defined	
	Traffic Management/QoS	No	No	Yes	
	Multi-WAN	No	Yes	Yes	
	Dynamic Routing	No	Yes - RIP only	Yes - RIP, BGP, and OSPF	
	Secondary Networks	Yes	Yes	Yes	In Fireware 8.3, you can now define secondary network addresses on the same subnet as a Firebox primary interface. This replaces the network alias function available in WFS and earlier versions of Fireware.

## Comparing WFS and Fireware

Feature or Functional Area	WFS	Fireware	Fireware Pro	Notes on Fireware/Fireware Pro Implementation
DHCP Client	Yes	Yes	Yes	
DHCP Server	Yes	Yes	Yes	In Fireware, you can add up to 6 DHCP scopes per interface.
DHCP Relay	No	Yes	Yes	
Drop-In Mode	Yes	Yes	Yes	In Fireware, the Firebox passes the ARP request through, instead of applying proxy ARP.
<b>High Availability</b>				
Active/Standby	Option	No	Yes	In Fireware, you can use HA together with a Management Server to manage your VPN tunnels.
<b>Application Layer Filtering</b>				
HTTP Inbound	No	Yes	Yes	
HTTP Outbound	Yes	Yes	Yes	Includes substantial feature enhancements, including improved pattern matching, configurable antivirus and IPS signature scanning, and support for regular expressions.
WebBlocker	Yes	Yes	Yes	Both WFS 7.4.1 and Fireware include 40 categories of web content.
SMTP Inbound	Yes	Yes	Yes	Includes substantial feature enhancements, including improved pattern matching, configurable antivirus and IPS signature scanning, and support for regular expressions.
SMTP Outbound	Yes	Yes	Yes	
FTP Inbound	Yes	Yes	Yes	Includes substantial feature enhancements, including the ability to block downloads and uploads by file name, IPS signature scanning, and support for regular expressions.
FTP Outbound	Yes	Yes	Yes	
DNS	Yes	Yes	Yes	Includes substantial feature enhancements, including the ability to block DNS queries based on pattern-matching for any query name.
Outgoing (TCP)	No	Yes	Yes	In Fireware, the TCP proxy can apply signature-based IPS to all outgoing TCP traffic, not only HTTP traffic as in WFS.
Firewall-based IPS (protocol anomaly detection)	Yes	Yes	Yes	Enhanced protocol anomaly detection including the ability to set thresholds for multiple flood-based attacks and new options for default unhandled packet handling.
Signature-based IPS	No	Yes	Yes	
<b>Authentication</b>				
RADIUS	Yes	Yes	Yes	
LDAP/Active Directory	No	Yes	Yes	

Feature or Functional Area	WFS	Fireware	Fireware Pro	Notes on Fireware/Fireware Pro Implementation	
VPN	Windows NT Server authentication with 2000/2003 compatibility (NTLM)	Yes	No	No	
	Firebox database	Yes	Yes	Yes	
	SecurID	Yes	Yes	Yes	
	Cryptocard	Yes	No	No	
	PPTP	Yes	Yes	Yes	
	PPTP with RADIUS authentication	Yes	Yes	Yes	
	MUVPN (IPSec)	Yes	Yes	Yes	In Fireware, you can use any supported authentication server to authenticate MUVPN connections.
Management	BOVPN (IPSec)	Yes	Yes	Yes	There is no auto-start for VPN tunnels. You must send traffic across the tunnel for the tunnel to build.
	AES encryption	No	Yes	Yes	Fireware enables the hardware-based AES encryption chip.
	Unified management interface	No	Yes	Yes	You can start all management tools from WatchGuard System Manager.
	Manage more than one device	Yes	Yes	Yes	Use WatchGuard System Manager to manage one or more devices, including centralized management and monitoring of Firebox X Edge devices.
	Certificate Authority	Yes	Yes	Yes	Certificate Authority moves from the Firebox to the Management Server.
	Drag-and-drop VPN setup for WatchGuard appliances	Yes	Yes	Yes	Available for these models: Firebox SOHO 6, Firebox III, Firebox X Edge, Firebox X Core, and Firebox X Peak
	Management Server	No	Yes	Yes	Starting with WSM 8.0. Installations of WFS 7.3 and earlier use VPN Manager instead of the WatchGuard Management Server.
Monitoring Tools	Basic DVCP	Yes	No	No	If you currently use Basic DVCP, you must use the Management Server Setup wizard to migrate your tunnels to the Management Server.
	Firebox System Manager	Yes	Yes	Yes	Fireware supplies enhanced logging, the ability to add an IP address to the Blocked Sites list from Traffic Monitor, the ability to log off an authenticated user from the Authentication List, and detailed information on subscription services.
	HostWatch	Yes	Yes	Yes	You can now add any IP address to the Blocked Sites list from HostWatch. You can also set the Firebox interface you want as the HostWatch focus point. HostWatch no longer supports log file playback.

## Comparing WFS and Fireware

Feature or Functional Area	WFS	Fireware	Fireware Pro	Notes on Fireware/Fireware Pro Implementation	
<b>Policy Management</b>	Performance Console	No	Yes	Yes	Ability to graphically monitor a large number of system, policy, and VPN parameters, and to save information to XML or CSV format for use with third-party analysis tools.
	Policy Manager	Yes	Yes	Yes	Fireware Policy Manager has three tabs so you can configure policies for network traffic, MUVPN traffic, and BOVPN traffic separately. WFS services are now known as Fireware policies.
	Policies	Yes	Yes	Yes	Services are now known as policies.
	Policy flow logic	Incoming/Outgoing	From/To	From/To	Because of port independence, traffic rules are set in policies "from" a source "to" a destination.
	Policy Management	Yes	Yes	Yes	The Any service no longer has the highest priority. Firewall policies no longer affect IPSec policies.
	Policy precedence control	Automatic	Automatic/Manual	Automatic/Manual	With Fireware, you can set policy precedence manually, or use the default precedence order set by Policy Manager.
	1:1 NAT	Yes	Yes	Yes	The rules set in Fireware Policy Manager, Network > NAT, do not apply to IPSec VPN traffic. NAT through a VPN is configured when you create the VPN tunnel.
	Dynamic NAT	Yes	Yes	Yes	The rules set in Fireware Policy Manager, Network > NAT, do not apply to IPSec VPN traffic. NAT through a VPN is configured when you create the VPN tunnel.
<b>Logging</b>	Static NAT/ Port Forwarding	Yes	Yes	Yes	Fireware 8.3 introduces policy-based NAT. You can use an IP address for Dynamic NAT that is not the primary external interface IP address on a per-policy basis.
	Log Server	Yes	Yes	Yes	Log Server now keeps files in an XML format.
	XML Log Format	No	Yes	Yes	More verbose log message content. There is a conversion tool to move log files from WFS format to XML.
	LogViewer	Yes	Yes	Yes	
	SNMP	No	Yes	Yes	You can configure the Firebox to accept SNMP polls from an SNMP server. You can also configure the Firebox to send traps to an SNMP server.
<b>Reporting</b>	Advanced log message options	Yes	Yes	Yes	Fireware supplies more diagnostic logging. For more information, see the Reference Guide.
	Historical Reports	Yes	Yes	Yes	8.x includes new reports and support for XML log files.
<b>Options</b>	Spam blocking	Spam-Screen	spam-Blocker	spamBlocker	spamBlocker offers an easier-to-use, more effective spam blocking solution.

Feature or Functional Area	WFS	Fireware	Fireware Pro	Notes on Fireware/Fireware Pro Implementation
WebBlocker	Yes	Yes	Yes	Both Fireware and WFS now support 40 WebBlocker categories.
Antivirus	Gateway AntiVirus for E-mail	Gateway AntiVirus / Intrusion Prevention Service	Gateway AntiVirus / Intrusion Prevention Service	With the GAV/IPS service, you can scan both SMTP and HTTP traffic for viruses.
Signature-Based IPS	No	Yes	Yes	
Common Criteria CLI	No	Yes	Yes	This feature is available only in Common Criteria mode.

## Planning Your Migration

There is no automated process to migrate your Firebox from WFS appliance software to Fireware®. You must build a new configuration file for your Firebox. This procedure can take a lot of time, but can also give you a good opportunity to examine the policies in your configuration. You may learn that there are policies in your current configuration that are not necessary. Look at each policy before you add it to your Fireware configuration and consider if the policy is sufficiently restrictive to give your network the most security.

It is a good idea to take the time to review your security policy and make sure that you implement best-practices network security in your new Firebox configuration. For more information, see [https://www.watchguard.com/docs/whitepaper/securitypolicy\\_wp.pdf](https://www.watchguard.com/docs/whitepaper/securitypolicy_wp.pdf)

As with any major software migration, a well-designed plan for your migration from WFS to Fireware or Fireware Pro can decrease the effect on your users and improve your experience. This *Migration Guide* supplies detailed instructions to successfully migrate from WFS to Fireware. These include steps to:

- Document and examine your current WFS configuration
- Create backup files of your existing configuration
- Install WatchGuard System Manager and Fireware on your management station
- Configure the Management Server and migrate your DVCP server(s)
- Install Fireware on the device
- Connect to the Firebox from WSM and open Fireware Policy Manager
  - Make the changes in Fireware Policy Manager that reflect the WFS configuration
  - Create and test VPN tunnels as necessary
- Deploy the Firebox and test the Fireware configuration

## Upgrading Subscription Services

Fireware® does not support Gateway AntiVirus (GAV) for E-mail or SpamScreen. Instead, Fireware users have the option to purchase subscriptions to the more robust antivirus and spam blocking solutions: Gateway AntiVirus/IPS and spamBlocker. When you upgrade to Fireware, the GAV for E-mail and SpamScreen features stop working. If you have a current GAV for E-mail or SpamScreen subscription that has

not yet expired, you can purchase the new Gateway AntiVirus/IPS and spamBlocker service subscriptions at a reduced cost. Contact your reseller for more information.

All LiveSecurity and WebBlocker subscriptions continue with no change when you upgrade.

---

## Using this Migration Guide

---

This *Migration Guide* includes the migration procedures for three different groups of users. Carefully read the description of the groups shown below and select the group to which you belong. The migration procedure for each group is given in a separate chapter of this guide.

### *WFS 7.x (No VPN Manager) to Fireware Pro*

You have a Firebox X Core that uses WFS 7.x. You do not use VPN Manager and have never configured a WatchGuard Management Server. For migration instructions, go to Chapter 2.

### *WFS 7.3 or below and VPN Manager to Fireware Pro*

You have a Firebox X Core that uses WFS 7.3 or lower. You use VPN Manager or Basic DVCP to configure and manage some or all of your BOVPN tunnels. For migration instructions, go to Chapter 3.

### *WSM 8.x/WFS 7.4 to Fireware Pro*

You have a Firebox X Core. You use WatchGuard System Manager 8.x, and your Firebox is running WFS 7.4. You have a WatchGuard Management Server already configured. For migration instructions, go to Chapter 4.

### **Best Practices**

---

To reduce downtime during migration: Install WSM 8.3 and build your new Fireware configuration before you install Fireware on your Firebox. Make sure you read the complete *Migration Guide* before you continue.

---

# Migrating from WFS 7.x (No VPN Manager) to Fireware Pro

This Migration Guide includes the migration procedures for three different groups of users, with separate chapters for each. Use this chapter to help you migrate to Fireware if:

- You have a Firebox X Core currently installed with WFS 7.x and
- You are not using VPN Manager and a DVCP server to manage branch office VPN tunnels.

## Migrating to Fireware

---

To successfully migrate to Fireware, you must:

- 1 Document and analyze your current security policy
- 2 Back up the WFS configuration file and image, and document the properties of any VPN tunnels you have defined
- 3 Install WatchGuard System Manager software and Fireware Pro appliance software on a management station
- 4 Install Fireware on your Firebox
- 5 Build a new Fireware configuration policy using WatchGuard System Manager 8.3 and save it to your Firebox

### Best Practices

---

To reduce downtime during migration: Install WSM 8.3 and build your new Fireware configuration before you install Fireware on your Firebox. Make sure you read the complete *Migration Guide* before you continue.

---

## Documenting Your Current Security Policy

---

A good security policy is not just a firewall configuration file. It is a process that a network administrator documents and that management regularly reviews to make sure that the rules your firewall applies

---

## Backing Up Your WFS Configuration and Firebox Image

correctly reflect the information management and security goals of your company. Your migration is a good opportunity to examine your security policy. Because you must make a new configuration file for the Fireware® appliance software, it is a good idea to examine which policies you must have to do business. Use these guidelines:

- Each policy you open makes your network less secure
- Policies that allow traffic from the Internet to your network are more dangerous than policies that allow traffic from your network to the Internet
- Specify source and destination addresses to make a policy more secure

For more information about network security policies, see [https://www.watchguard.com/docs/whitepaper/securitypolicy\\_wp.pdf](https://www.watchguard.com/docs/whitepaper/securitypolicy_wp.pdf)

---

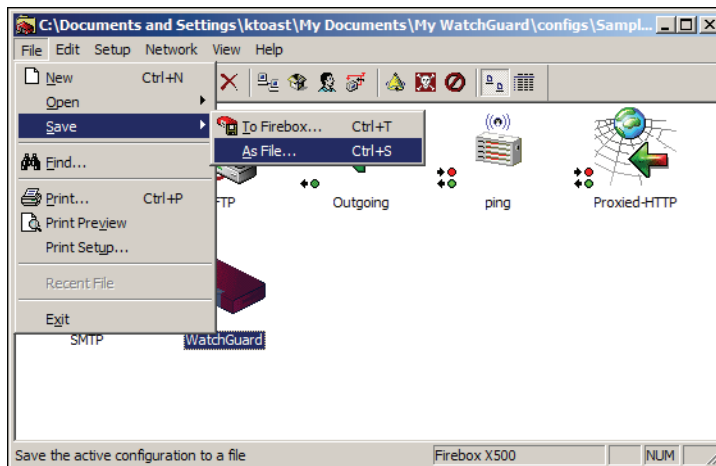
## Backing Up Your WFS Configuration and Firebox Image

Before you install WatchGuard System Manager 8.3 and Fireware appliance software, you must back up the software image on your Firebox and the configuration file kept on your management station. If you do not back up your WFS installation, you cannot go back to WFS easily if you have problems during migration.

### Saving your configuration file

You can save the configuration file to the Firebox. You can also save it as a file on a local hard disk drive. Before you install an upgrade, 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**. We recommend that you also save this file to a network folder.  
The configuration file has the file extension \*.cfg.

## Saving the Firebox software image

A very important step in the migration is to save the Firebox software image. This puts an encrypted copy of the Firebox flash disk on your management station. To create the WFS software backup file:

- 1 Open Firebox System Manager. It is not necessary to connect to the Firebox.
- 2 Select **Tools > Advanced > Flash Disk Management**.
- 3 Select **Make Backup of Current Image**. Click **Continue**.  
A verification prompt appears. Make sure that the management station can connect to the Firebox Trusted interface with the network (TCP/IP).
- 4 Click **Continue**.  
The Connect To Firebox dialog box appears.
- 5 From the **Firebox** drop-down list, select a Firebox or type the IP address used by the management station to connect to the Firebox. Type the configuration (read/write) passphrase. Click **OK**.
- 6 Select a file name for the Firebox backup file.  
The Enter Encryption Key dialog box appears.
- 7 Type a key to encrypt the backup file. Click **OK**.  
This makes sure that no one can get sensitive information from the backup file. Make sure that you secure this encryption key in a safe location. You cannot restore a backup file to the Firebox if you forget this encryption key.
- 8 When the backup is successful, an Operation Complete message appears. Click **OK**.  
It is not necessary to restart the Firebox after this procedure.

## Documenting VPN Tunnels

If you have manual branch office VPN tunnels that you have created to another WatchGuard Firebox or some other IPSec-compliant VPN endpoint, it is a good idea to completely remove the manual VPN tunnel configuration information from both VPN endpoints before you migrate to Fireware. This is especially important if you plan to use WatchGuard System Manager and Fireware to manage your BOVPN tunnels in the future.

Make sure to document all properties of each VPN tunnel before you remove the tunnel information. You must create the branch office VPN tunnels again after you migrate to Fireware.

## Installing Software on the Management Station

Before you migrate your Firebox to Fireware appliance software, you must first install WatchGuard System Manager 8.3 and Fireware 8.3 on your management station. You do not have to delete WFS first. You can have both WFS and Fireware appliance software installed on your management station, as long as you install the software in two different directories. However, you cannot install two versions of WSM 8.x—such as WSM 8.2 and 8.3—on your management station at the same time.

- 1 Download the WatchGuard System Manager 8.3 and Fireware 8.3 software, if you do not already have it. You can download the latest software from the WatchGuard web site at <https://www.watchguard.com/archive/softwarecenter.asp>.  
Make sure that you write down the name and path of the file when you save it to your hard disk drive.
- 2 Open each file and use the instructions on the screens to help you through the installation. Make sure you install WSM in a different directory than WFS.  
The WSM installation utility includes a screen in which you select the components of the software or the upgrades to install. You can install all the components, but you cannot configure all components without the correct feature key.

- 3 At the end of the WSM installation wizard, a check box appears that you can select to start the Quick Setup Wizard. The next section helps you through this process.

---

## Installing Fireware on Your Firebox

---

When you have created backup files of your WFS configuration file and Firebox image and you have downloaded WSM 8.3 and Fireware 8.3 software to your management station, you are ready to install Fireware on your Firebox. There are two methods to use to put Fireware Pro on a Firebox that is running WFS 7.x appliance software:

- Use the Quick Setup Wizard to make a simple configuration file and 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 and a basic configuration file on the Firebox. Before you start the wizard, make sure:

- You have saved a copy of your WFS configuration file to a directory outside the WatchGuard installation directory with the procedure described in “Saving your configuration file” on page 10.
- You have created a backup copy of the WFS image on your Firebox with the procedure described in “Saving the Firebox software image” on page 11.
- You have downloaded and installed WatchGuard System Manager 8.3 and Fireware 8.3 on your management station.
- You copied the feature key for your Firebox from the WatchGuard LiveSecurity web site. You must paste this key into a text box in the wizard. This feature key is linked to the serial number of your Firebox. To get a copy of your feature key, go to <https://www.watchguard.com/archive/manageproducts.asp>
- Your management station is on the same network as the Firebox. The wizard uses TCP discovery to find the Firebox on the network. If there is more than one Firebox on the network, you must select the correct Firebox from a list the wizard gives you.

You can start the Quick Setup Wizard automatically when you install the WSM software. Or, you can start the wizard manually. From the Windows desktop, select **Start > WatchGuard System Manager 8.3 > Quick Setup Wizard**.

The wizard asks you for this information:

- The type of Firebox you have
- Feature key for the Firebox
- External interface information for the Firebox
- Network configuration preference (routed or drop-in mode)
- Status and configuration passphrases

When the wizard is complete, you can start to build a new Fireware configuration file that matches your business needs. For more information on how to connect to the Firebox and use Fireware Policy Manager, see Chapter 5, “Using Fireware Policy Manager.”

## Using fbxinstall.exe

You can also use the fbxinstall.exe utility to install Fireware Pro. Fbxinstall.exe is a command line utility that allows you to upgrade a Firebox X Core from WFS appliance software to Fireware Pro appliance software. After this procedure is complete, you must use the Quick Setup Wizard to give the Firebox a basic configuration. You can then add to the Fireware configuration file to meet the needs of your organization.

To install Fireware Pro on a Firebox with fbxinstall.exe:

- 1 Connect a serial cable between the Firebox and COM1 on your management station.
- 2 Connect the trusted interface of the Firebox to the Ethernet port on your management station with a cross-over cable.
- 3 Change the IP address on your management station to 10.10.10.2/24. Set the default gateway on your management station to 10.10.10.1.
- 4 Open a command prompt.
- 5 Type `fbxinstall 10.10.10.2/24`  
This IP address is used to connect to the Firebox to complete the reset process, but is not actually assigned to the Firebox.
- 6 When the fbxinstall procedure is done, use the Quick Setup Wizard to create a new configuration file. See "Using the Quick Setup Wizard" on page 12 for more information.  
Remember to reset your management station IP address and default gateway back to their original state when you are done with the fbxinstall procedure.



# Migrating from WFS 7.3 with VPN Manager to Fireware Pro

This Migration Guide includes the migration procedures for three different groups of users, with separate chapters for each. Use this chapter to help you migrate to Fireware if:

- You have a Firebox X Core currently installed with WFS 7.3  
and
- You use VPN Manager or Basic DVCP and a DVCP server to manage some or all of your branch office VPN tunnels.

## Migrating to Fireware

---

To successfully migrate to Fireware, you must:

- Document and analyze your security policy
- Back up the WFS configuration file and image
- Install WatchGuard System Manager software and Fireware appliance software on a management station
- Migrate the DVCP Server on your Firebox to a WatchGuard Management Server installed on a Windows computer
- Install Fireware on your Firebox
- Build a new Fireware configuration policy using WatchGuard System Manager 8.3 and save it to your Firebox

### Best Practices

---

To reduce downtime during migration: Install WSM 8.3 and build your new Fireware configuration before you install Fireware on your Firebox. Make sure you read the complete *Migration Guide* before you continue.

---

## Documenting Your Security Policy

A good security policy is not just a firewall configuration file. It is a process that a network administrator documents and that management regularly reviews to make sure that the rules your firewall applies correctly reflect the information management and security goals of your company. Your migration is a good opportunity to examine your security policy. Because you must make a new configuration file for the Fireware® appliance software, it is a good idea to examine which policies you must have to do business. Use these guidelines:

- Each policy you open makes your network less secure
- Policies that allow traffic from the Internet to your network are more dangerous than policies that allow traffic from your network to the Internet
- Specify source and destination addresses to make a policy more secure

For more information about network security policies, see

[https://www.watchguard.com/docs/whitepaper/securitypolicy\\_wp.pdf](https://www.watchguard.com/docs/whitepaper/securitypolicy_wp.pdf)

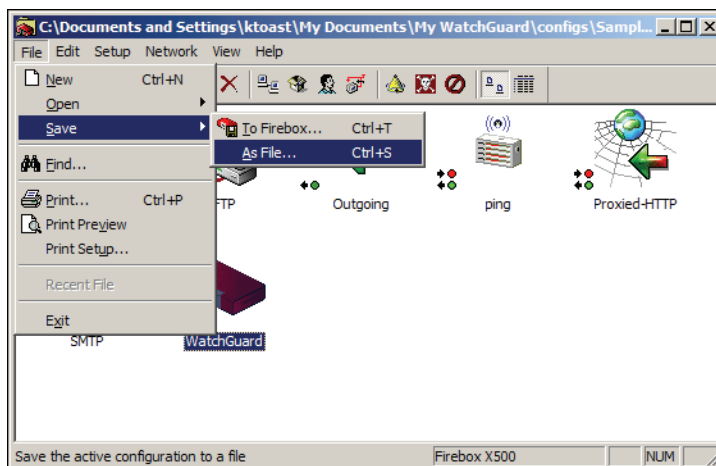
## Backing Up Your WFS Configuration and Firebox Image

Before you install WatchGuard System Manager 8.3 and Fireware appliance software, you must back up the software image on your Firebox and the configuration file kept on your management station. If you do not back up your WFS installation, you cannot go back to WFS easily if you have problems during migration.

### Saving your configuration file

You can save the configuration file to the Firebox. You can also save it as a file on a local hard disk drive. Before you install an upgrade, 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**. We recommend that you also save this file to a network folder.  
The configuration file has the file extension \*.cfg.

## Saving the Firebox software image

A very important step in the migration is to save the Firebox software image. This puts an encrypted copy of the Firebox flash disk on your management station. To create the WFS software backup file:

- 1 Open Firebox System Manager. It is not necessary to connect to the Firebox.
- 2 Select **Tools > Advanced > Flash Disk Management**.
- 3 Select **Make Backup of Current Image**. Click **Continue**.  
A verification prompt appears. Make sure that the management station can connect to the Firebox Trusted interface with the network (TCP/IP).
- 4 Click **Continue**.  
The Connect To Firebox dialog box appears.
- 5 From the **Firebox** drop-down list, select a Firebox or type the IP address used by the management station to connect to the Firebox. Type the configuration (read/write) passphrase. Click **OK**.
- 6 Select a file name for the Firebox backup file.  
The Enter Encryption Key dialog box appears.
- 7 Type a key to encrypt the backup file. Click **OK**.  
This makes sure that no one can get sensitive information from the backup file. Make sure that you secure this encryption key in a safe location. You cannot restore a backup file to the Firebox if you forget this encryption key.
- 8 When the backup is successful, an Operation Complete message appears. Click **OK**.  
It is not necessary to restart the Firebox after this procedure.

## Documenting VPN Tunnels

If you have manual branch office VPN tunnels that you have created to another WatchGuard Firebox or some other IPSec-compliant VPN endpoint, it is a good idea to completely remove the manual VPN tunnel configuration information from both VPN endpoints before you migrate to Fireware. This is especially important if you plan to use WatchGuard System Manager and Fireware to manage your BOVPN tunnels in the future.

Make sure to document all properties of each VPN tunnel before you remove the tunnel information. You must create the branch office VPN tunnels again after you migrate to Fireware.

## Installing Software on the Management Station

Before you migrate your Firebox to Fireware appliance software, you must first install WatchGuard System Manager 8.3 and Fireware 8.3 on your management station. You do not have to delete WFS first. You can have both WFS and Fireware appliance software installed on your management station, as long as you install the software in two different directories. However, you cannot install two versions of WSM 8.x—such as WSM 8.2 and 8.3—on your management station at the same time.

- 1 Download the WatchGuard System Manager 8.3 and Fireware 8.3 software, if you do not already have it. You can download the latest software from the WatchGuard web site at <https://www.watchguard.com/archive/softwarecenter.asp>.  
Make sure that you write down the name and path of the file when you save it to your hard disk drive.
- 2 Open each file and use the instructions on the screens to help you through the installation. Make sure you install WSM in a different directory than WFS.  
The WSM installation utility includes a screen in which you select the components of the software or the upgrades to install. You can install all the components, but you cannot configure all components without the correct feature key.



- 3 At the end of the WSM installation wizard, a check box appears that you can select to start the Quick Setup Wizard. Do **not** start the Quick Setup Wizard at this time. You must migrate your VPN Manager configuration or any Basic DVCP tunnels to a WatchGuard Management Server before you install Fireware on the Firebox with the Quick Setup Wizard.

---

**Note**

---

If you use VPN Manager on your Firebox X Core, it is important to run the Management Server Setup wizard before you put Fireware on your Firebox. When you put Fireware on your Firebox, Fireware puts an entirely new image on the Firebox flash disk. When the new Fireware image is on the flash disk, the VPN Manager information is gone from the flash disk. You must run the Management Server Setup Wizard to pull the VPN Manager information off the Firebox before you put Fireware on your Firebox.

---

---

**Introducing the WatchGuard Management Server**

---

In older versions of its firewall software, WatchGuard offered simple branch office VPN configuration with VPN Manager and the Dynamic VPN Configuration Protocol (DVCP). VPN Manager controls many VPN tunnels with one easy-to-use management interface. With WatchGuard Firebox System 7.3 and earlier, the configuration information for these managed VPN tunnels was kept on a DVCP server installed on a Firebox.

With WatchGuard System Manager 8.x, the DVCP server is moved off the Firebox. The functionality moves to a Windows computer and the name changes to the WatchGuard Management Server. This makes the Firebox a more scalable and flexible solution for the network administrator. The Management Server has the same functions as the VPN Manager server. These functions are:

- Central management of BOVPN tunnels
- Certificate Authority to make and send out certificates for IPSec VPN tunnels

When you install WSM, you can install the Management Server at the same time. It is a good idea to 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.

After it is installed, you can access the Management Server configuration from an icon installed in the WatchGuard toolbar. From the Management Server Configuration window, you can:

- Start and stop the Management Server
- Set Management Server passphrases
- Enter a Management Server license key
- Configure the properties of the Certificate Authority, the client certificate, and the Certificate Revocation List

**Management Server license**

You must use the VPN Manager license to configure the Management Server. You must have your VPN Manager license before you can move your VPN Manager configuration from a Firebox to a Management Server. You can use a WatchGuard System Manager license to increase the total number of devices managed by the Management Server. For more information, go to [https://www.watchguard.com/support/AdvancedFaqs/wsm8\\_srvrkey.asp](https://www.watchguard.com/support/AdvancedFaqs/wsm8_srvrkey.asp)

---

## **Migrating Your VPN Manager Data to a Management Server**

---

WatchGuard System Manager 8.3 supplies a wizard that migrates your WFS VPN Manager configuration to the new WatchGuard Management Server. This wizard is known as 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 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.x.

The wizard does these actions:

- Gets a master encryption key to encrypt the configuration and passphrase files of the Management Server
- Gets a passphrase to connect to the DVCP server from the management station
- Gets the IP address and configuration passphrase for the Firebox that was used as a DVCP server
- Connects to the Firebox
- Gets the VPN Manager configuration file from the Firebox
- Uses this configuration file to find if the Firebox was a basic DVCP server or an advanced DVCP server
- Changes the “wg\_dvcp” and “wg\_ca” services of the gateway Firebox, and uses NAT (network address translation) to send traffic to the new Management Server on the management station
- Saves the changes to the Firebox
- Starts the Management Server

### **If the Firebox was a VPN Manager DVCP server**

If the Firebox was a VPN Manager DVCP server, the wizard does these actions:

- Uses the configuration properties of the DVCP server to configure the CA on the Management Server
- Gets the DVCP configuration file (dvcp.cfg) from the Firebox
- Uses the DVCP configuration file to set the Management Server license key, policy templates, security templates, and DVCP clients
- Removes the DVCP server from the Firebox
- Removes the DVCP server configuration properties from the Firebox configuration file

After migration is complete, your managed VPN tunnels continue to operate correctly.

### **If the Firebox was a Basic DVCP server**

The Management Server Setup wizard does not migrate all Basic DVCP VPN tunnels configured on the Firebox. It converts only the VPN tunnels that use the gateway Firebox as one of the endpoints. Basic DVCP tunnels are not supported in WSM 8.3.

If you have Basic DVCP VPN tunnels that do not have the DVCP server Firebox as one of the VPN endpoints, you must:

- Document the properties of the basic VPN tunnel.
- Remove the VPN tunnel information on the Basic DVCP server, and then restart the Basic DVCP Client.

---

## Installing Fireware on Your Firebox

You can then use the Management Server Setup wizard to migrate to a new Management Server and use the Quick Setup Wizard to create a new configuration file for your Firebox (described later in this chapter). Then you must add the VPN endpoints to your Management Server configuration as managed devices and create the VPN tunnels again.

Note that you must have a license available for each advanced VPN tunnel you create. This was not required when you used Basic DVCP and can make you have to purchase additional licenses.

### Running the Management Server Setup wizard

- 1 From the Windows desktop, double-click the Management Server icon in the WatchGuard toolbar.



- 2 Select **Start Service**.

If the Management Server has not been configured, then the Management Server Setup wizard starts automatically.

---

## Installing Fireware on Your Firebox

When you have created backup files of your WFS configuration file and Firebox image and you have downloaded WSM 8.3 and Fireware 8.3 software to your management station, you are ready to install Fireware on your Firebox. There are two methods to use to put Fireware Pro on a Firebox that is running WFS 7.x appliance software:

- Use the Quick Setup Wizard to make a simple configuration file and 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 and a basic configuration file on the Firebox. Before you start the wizard, make sure:

- You have saved a copy of your WFS configuration file to a directory outside the WatchGuard installation directory with the procedure described in "Saving your configuration file" on page 16.
- You have created a backup copy of the WFS image on your Firebox with the procedure described in "Saving the Firebox software image" on page 17.
- You have downloaded and installed WatchGuard System Manager 8.3 and Fireware 8.3 on your management station.
- You copied the feature key for your Firebox from the WatchGuard LiveSecurity web site. You must paste this key into a text box in the wizard. This feature key is linked to the serial number of your Firebox. To get a copy of your feature key, go to <https://www.watchguard.com/archive/manageproducts.asp>

- Your management station is on the same network as the Firebox. The wizard uses TCP discovery to find the Firebox on the network. If there is more than one Firebox on the network, you must select the correct Firebox from a list the wizard gives you.

You can start the Quick Setup Wizard automatically when you install the WSM software. Or, you can start the wizard manually. From the Windows desktop, select **Start > WatchGuard System Manager 8.3 > Quick Setup Wizard**.

The wizard asks you for this information:

- The type of Firebox you have
- Feature key for the Firebox
- External interface information for the Firebox
- Network configuration preference (routed or drop-in mode)
- Status and configuration passphrases

When the wizard is complete, you can start to build a new Fireware configuration file that matches your business needs. For more information on how to connect to the Firebox and use Fireware Policy Manager, see Chapter 5, "Using Fireware Policy Manager."

## Using fbxinstall.exe

You can also use the fbxinstall.exe utility to install Fireware Pro. Fbxinstall.exe is a command line utility that allows you to upgrade a Firebox X Core from WFS appliance software to Fireware Pro appliance software. After this procedure is complete, you must use the Quick Setup Wizard to give the Firebox a basic configuration. You can then add to the Fireware configuration file to meet the needs of your organization.

To install Fireware Pro on a Firebox with fbxinstall.exe:

- 1 Connect a serial cable between the Firebox and COM1 on your management station.
- 2 Connect the trusted interface of the Firebox to the Ethernet port on your management station with a cross-over cable.
- 3 Change the IP address on your management station to 10.10.10.2/24. Set the default gateway on your management station to 10.10.10.1.
- 4 Open a command prompt.
- 5 Type `fbxinstall 10.10.10.2/24`  
This IP address is used to connect to the Firebox to complete the reset process, but is not actually assigned to the Firebox.
- 6 When the fbxinstall procedure is done, use the Quick Setup Wizard to create a new configuration file. See "Using the Quick Setup Wizard" on page 20 for more information.

Remember to reset your management station IP address and default gateway back to their original state when you are done with the fbxinstall procedure.



# Migrating from WSM 8.x/WFS 7.4 to Fireware Pro

This Migration Guide includes the migration procedures for three different groups of users, with separate chapters for each. Use this chapter to help you migrate to Fireware if:

- You use WatchGuard System Manager 8.x and have a Firebox X Core currently installed with WFS 7.4 and
- You have a WatchGuard Management Server already installed and running, or do not use a Management Server at all.

## Migrating to Fireware

---

To successfully migrate to Fireware, you must:

- Document and analyze your security policy
- Back up the WFS configuration file and image
- Install the latest WatchGuard System Manager software (if necessary) and Fireware appliance software on a management station
- Install Fireware on your Firebox
- Build a new Fireware configuration policy using WatchGuard System Manager 8.3 and save it to your Firebox

### Best Practices

---

To reduce downtime during migration: Install WSM 8.3 and build your new Fireware configuration before you install Fireware on your Firebox. Make sure you read the complete *Migration Guide* before you continue.

---

## Documenting Your Security Policy

---

A good security policy is not just a firewall configuration file. It is a process that a network administrator documents and that management regularly reviews to make sure that the rules your firewall applies correctly reflect the information management and security goals of your company. Your migration is a

---

## Backing Up Your WFS Configuration and Firebox Image

good opportunity to examine your security policy. Because you must make a new configuration file for the Fireware® appliance software, it is a good idea to examine which policies you must have to do business. Use these guidelines:

- Each policy you open makes your network less secure
- Policies that allow traffic from the Internet to your network are more dangerous than policies that allow traffic from your network to the Internet
- Specify source and destination addresses to make a policy more secure

For more information about network security policies, see

[https://www.watchguard.com/docs/whitepaper/securitypolicy\\_wp.pdf](https://www.watchguard.com/docs/whitepaper/securitypolicy_wp.pdf)

---

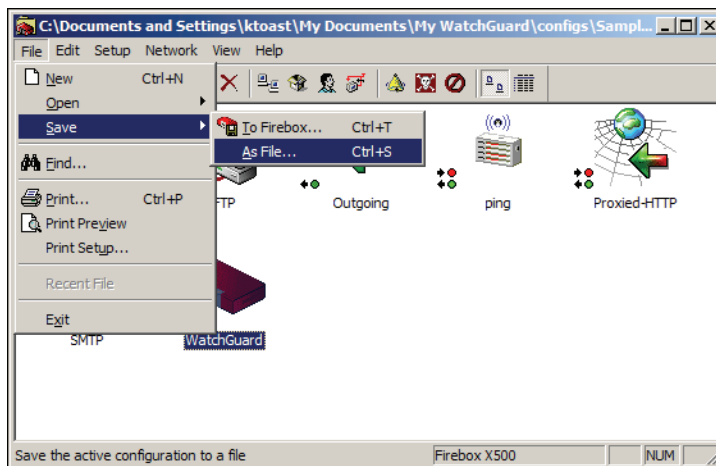
## Backing Up Your WFS Configuration and Firebox Image

Before you install WatchGuard System Manager 8.3 and Fireware appliance software, you must back up the software image on your Firebox and the configuration file kept on your management station. If you do not back up your WFS installation, you cannot go back to WFS easily if you have problems during migration.

### Saving your configuration file

You can save the configuration file to the Firebox. You can also save it as a file on a local hard disk drive. Before you install an upgrade, 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**. We recommend that you also save this file to a network folder.  
The configuration file has the file extension \*.cfg.

## Saving the Firebox software image

A very important step in the migration is to save the Firebox software image. This puts an encrypted copy of the Firebox flash disk on your management station. To create the WFS software backup file:

- 1 Open Firebox System Manager. It is not necessary to connect to the Firebox.
- 2 Select **Tools > Advanced > Flash Disk Management**.
- 3 Select **Make Backup of Current Image**. Click **Continue**.  
A verification prompt appears. Make sure that the management station can connect to the Firebox Trusted interface with the network (TCP/IP).
- 4 Click **Continue**.  
The Connect To Firebox dialog box appears.
- 5 From the **Firebox** drop-down list, select a Firebox or type the IP address used by the management station to connect to the Firebox. Type the configuration (read/write) passphrase. Click **OK**.
- 6 Select a file name for the Firebox backup file.  
The Enter Encryption Key dialog box appears.
- 7 Type a key to encrypt the backup file. Click **OK**.  
This makes sure that no one can get sensitive information from the backup file. Make sure that you secure this encryption key in a safe location. You cannot restore a backup file to the Firebox if you forget this encryption key.
- 8 When the backup is successful, an Operation Complete message appears. Click **OK**.  
It is not necessary to restart the Firebox after this procedure.

## Documenting VPN Tunnels



Before you install Fireware appliance software on your Firebox, you must document any manual and managed BOVPN tunnel information.

### *If you have manual BOVPN tunnels*

If you have manual branch office VPN tunnels that you have created to another WatchGuard Firebox or some other IPSec-compliant VPN endpoint, it is a good idea to completely remove the manual VPN tunnel configuration information from both VPN endpoints before you migrate to Fireware. This is especially important if you plan to use WatchGuard System Manager and Fireware to manage your BOVPN tunnels in the future.

Make sure to document all properties of each VPN tunnel before you remove the tunnel information. You must create the branch office VPN tunnels again after you migrate to Fireware.

### *If you have managed BOVPN tunnels*

If you have managed BOVPN tunnels with configuration information kept on your current Management Server, all your tunnel information is lost when you migrate to Fireware. Before you install Fireware on your Firebox, make sure you remove all managed VPN tunnels. After you install Fireware, you must add the managed devices again and create new VPN tunnels using drag-and-drop.

## Installing Software on the Management Station

Before you migrate your Firebox to Fireware appliance software, you must first install WatchGuard System Manager 8.3 and Fireware 8.3 on your management station. You do not have to delete WFS first. You can have both WFS and Fireware appliance software installed on your management station, as long

as you install the software in two different directories. However, you cannot install two versions of WSM 8.x—such as WSM 8.2 and 8.3—on your management station at the same time.

- 1 Download the WatchGuard System Manager 8.3 and Fireware 8.3 software, if you do not already have it. You can download the latest software from the WatchGuard web site at <https://www.watchguard.com/archive/softwarecenter.asp>.  
Make sure that you write down the name and path of the file when you save it to your hard disk drive.
- 2 Open each file and use the instructions on the screens to help you through the installation. Make sure you install WSM in a different directory than WFS.  
The WSM installation utility includes a screen in which you select the components of the software or the upgrades to install. You can install all the components, but you cannot configure all components without the correct feature key.
- 3 At the end of the WSM installation wizard, a check box appears that you can select to start the Quick Setup Wizard. The next section helps you through this process.

---

## Installing Fireware on Your Firebox

---

When you have created backup files of your WFS configuration file and Firebox image and you have downloaded WSM 8.3 and Fireware 8.3 software to your management station, you are ready to install Fireware on your Firebox. There are two methods to use to put Fireware Pro on a Firebox that is running WFS 7.x appliance software:

- Use the Quick Setup Wizard to make a simple configuration file and 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 and a basic configuration file on the Firebox. Before you start the wizard, make sure:

- You have saved a copy of your WFS configuration file to a directory outside the WatchGuard installation directory with the procedure described in “Saving your configuration file” on page 24.
- You have created a backup copy of the WFS image on your Firebox with the procedure described in “Saving the Firebox software image” on page 25.
- You have downloaded and installed WatchGuard System Manager 8.3 and Fireware 8.3 on your management station.
- You copied the feature key for your Firebox from the WatchGuard LiveSecurity web site. You must paste this key into a text box in the wizard. This feature key is linked to the serial number of your Firebox. To get a copy of your feature key, go to <https://www.watchguard.com/archive/manageproducts.asp>
- Your management station is on the same network as the Firebox. The wizard uses TCP discovery to find the Firebox on the network. If there is more than one Firebox on the network, you must select the correct Firebox from a list the wizard gives you.

You can start the Quick Setup Wizard automatically when you install the WSM software. Or, you can start the wizard manually. From the Windows desktop, select **Start > WatchGuard System Manager 8.3 > Quick Setup Wizard**.

The wizard asks you for this information:

- The type of Firebox you have
- Feature key for the Firebox
- External interface information for the Firebox

- Network configuration preference (routed or drop-in mode)
- Status and configuration passphrases

When the wizard is complete, you can start to build a new Fireware configuration file that matches your business needs. For more information on how to connect to the Firebox and use Fireware Policy Manager, see Chapter 5, "Using Fireware Policy Manager."

## Using fbxinstall.exe

You can also use the fbxinstall.exe utility to install Fireware Pro. Fbxinstall.exe is a command line utility that allows you to upgrade a Firebox X Core from WFS appliance software to Fireware Pro appliance software. After this procedure is complete, you must use the Quick Setup Wizard to give the Firebox a basic configuration. You can then add to the Fireware configuration file to meet the needs of your organization.

To install Fireware Pro on a Firebox with fbxinstall.exe:

- 1 Connect a serial cable between the Firebox and COM1 on your management station.
- 2 Connect the trusted interface of the Firebox to the Ethernet port on your management station with a cross-over cable.
- 3 Change the IP address on your management station to 10.10.10.2/24. Set the default gateway on your management station to 10.10.10.1.
- 4 Open a command prompt.
- 5 Type `fbxinstall 10.10.10.2/24`  
This IP address is used to connect to the Firebox to complete the reset process, but is not actually assigned to the Firebox.
- 6 When the fbxinstall procedure is done, use the Quick Setup Wizard to create a new configuration file. See "Using the Quick Setup Wizard" on page 26 for more information.

Remember to reset your management station IP address and default gateway back to their original state when you are done with the fbxinstall procedure.

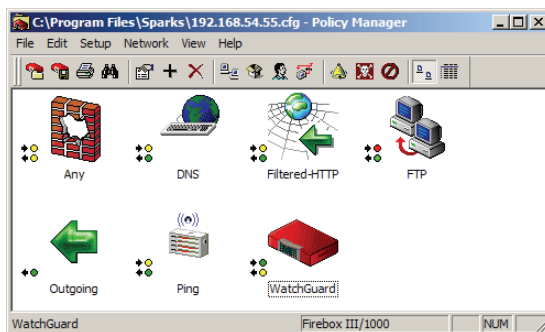


# Using Firewall Policy Manager

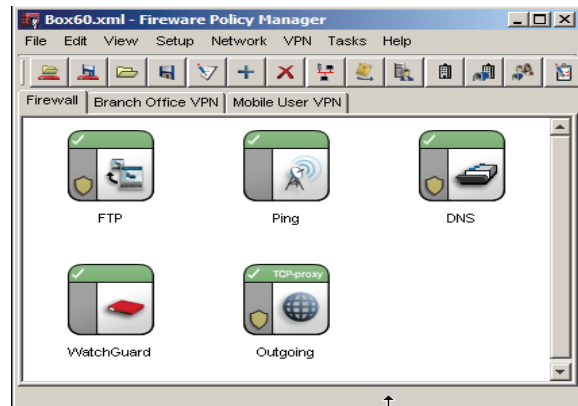
At this time, there is no configuration tool that automatically converts a WFS 7.x configuration file to a Fireware/Fireware Pro configuration file. The two appliance software versions are very different. You must start with the configuration file you saved at the end of the Fireware Quick Setup Wizard.

One method 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 you can see them at the same time. You might want to resize each window so that they are tiled horizontally.

**WFS 7.3 Policy Manager**



**Fireware Policy Manager**



## Rebuilding Your Network Configuration with Firewall Policy Manager

When you complete the Fireware Quick Setup Wizard, you have a very basic configuration that allows you to install the Firebox on your network. We recommend that the first thing you do after you install the Firebox is to connect to it with Policy Manager and add any additional configuration information necessary for your Firebox to operate correctly on your network.

This type of configuration information can include:

- Adding secondary networks
- Adding network and host routes
- Setting up DHCP

- Configuring NAT

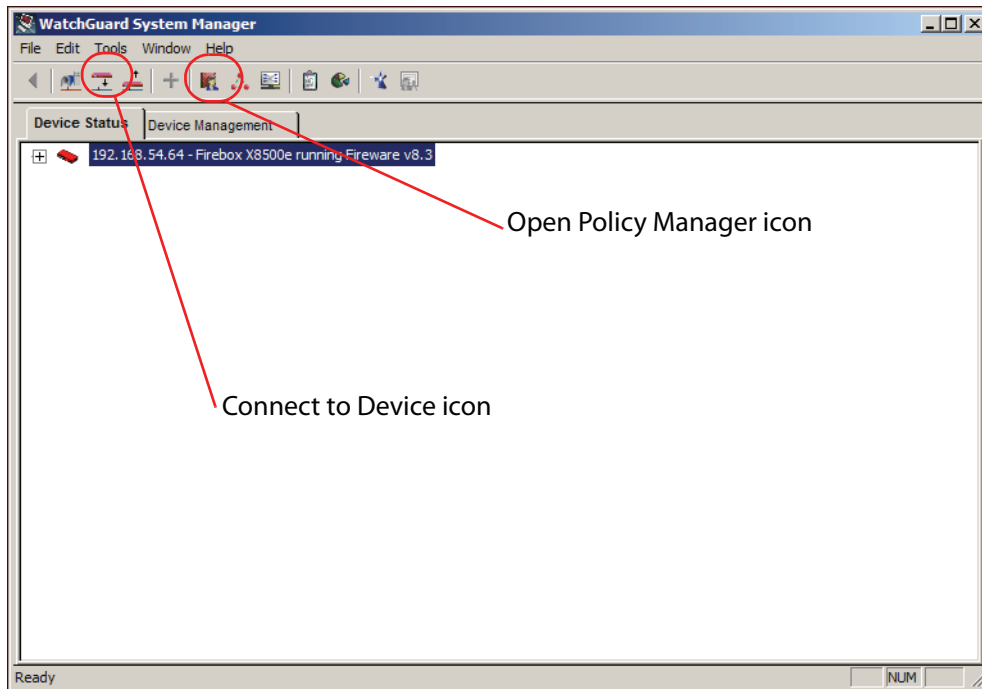
With Fireware, you also have the option to configure additional external interfaces. This feature is known as multi-WAN and is described in the *WatchGuard System Manager User Guide*.

In this section, we show you some of the user interface changes that you see when you configure network properties for your Firebox.

## Opening Policy Manager

To open Policy Manager, you first want to open WatchGuard System Manager and connect to your Firebox:

- 1 From your Windows Start menu, select **All Programs > WatchGuard System Manager 8.3 > WatchGuard System Manager**.
- 2 Select **File > Connect to Device** or the Connect to Device icon. Type the IP address and status passphrase for your Firebox.

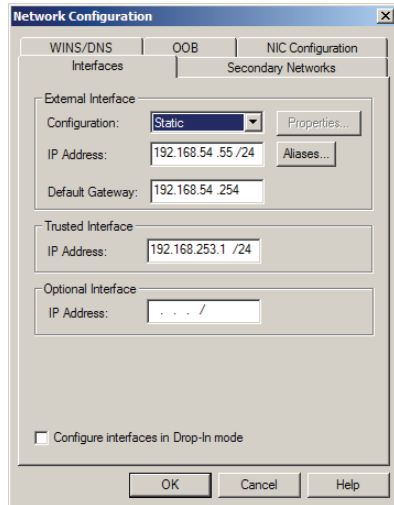


- 3 Right-click on the Firebox name in WSM and select **Policy Manager** or select the Policy Manager icon.  
Fireware Policy Manager launches and shows the configuration file for your Firebox.

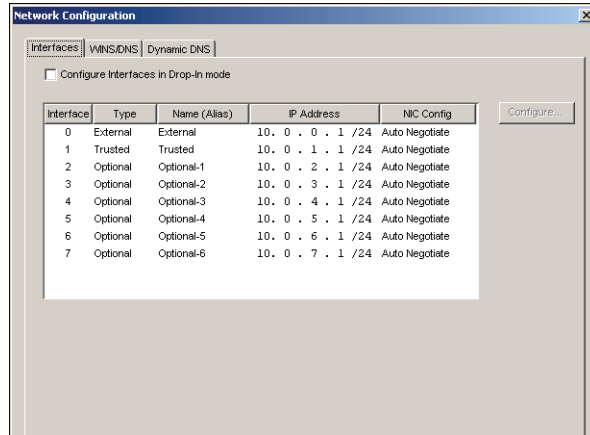
## Working with interfaces

When you select **Network > Configuration** you can see that the interface is now more flexible in 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 Fireware Policy Manager. To do this, select the appropriate interface entry and click **Configure**. If an interface is not necessary, select **Disabled** as the interface type.

**WFS 7.3 Network Configuration**



**Fireware Network Configuration**



To support the new Multi-WAN feature of Fireware, you can now have more than one interface configured as external, trusted, or optional. Because of this, there are new Firebox aliases available when you configure policies. The WFS alias "external" is different from the Fireware alias "external." In Fireware, the Any-External alias is equivalent to the external alias in WFS. These default aliases are:

*Any-Trusted*

This is an alias for all Firebox interfaces configured as "trusted" interfaces (as defined in Policy Manager: select **Network > Configuration**), and any network you can get access to through these interfaces.

*Any-External*

This is an alias for all Firebox interfaces of type "external" (as defined in Policy Manager: select **Network > Configuration**), and any network you can get access to through these interfaces.

*Any-Optional*

These are aliases for all Firebox interfaces of type "optional" (as defined in Policy Manager: select **Network > Configuration**), and any network you can get access to through these interfaces.

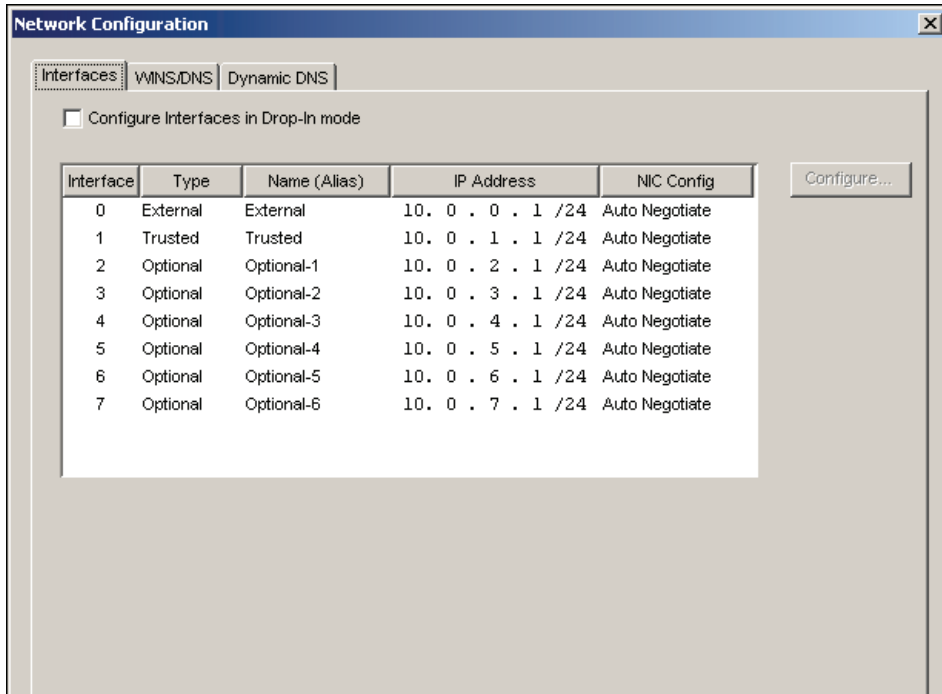
**Secondary networks and external alias addresses**

In the **Network Configuration** dialog box for each interface, you have the option to define secondary networks and addresses. The secondary network feature has been expanded in Fireware to allow support for secondary networks on the same network segment as the primary interface IP address. The enhanced secondary networks and addresses feature replaces the network alias function available in WFS. In WFS, you added a host IP address as an "Alias" to the external interface to use the IP address for Static NAT in a service. In Fireware, to use an additional IP address on the external interface for Static NAT, you add the IP address in slash notation, and you add it as a Secondary Network.

## DHCP Server

The procedure to configure DHCP server functionality on a Firebox with Fireware is different from WFS. You must configure DHCP server functionality on each trusted or optional interface you want to be a DHCP server. You can configure up to six DHCP scopes per interface.

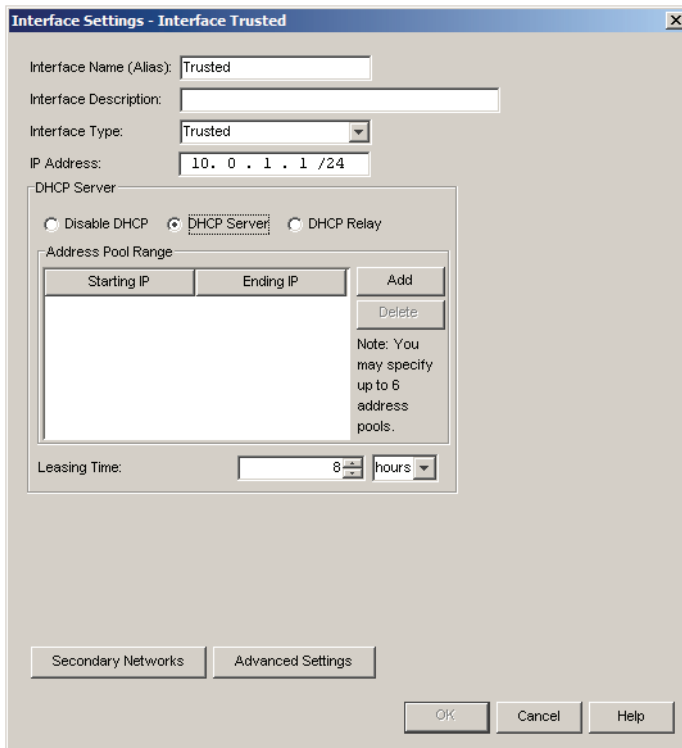
- 1 From Fireware Policy Manager, select **Network > Configuration**.



- 2 Select any trusted or optional interface and click **Configure**.
- 3 Select the **DHCP Server** radio button.
- 4 To add an IP address range, click **Add** and type the first and last IP addresses. You can configure a maximum of six address ranges.

5 Use the arrow buttons to change the **Default Lease Time**.

This is the time interval that a DHCP client can use an IP address that it receives from the DHCP server. When the time is near its limit, the client sends data to the DHCP server to get a new lease

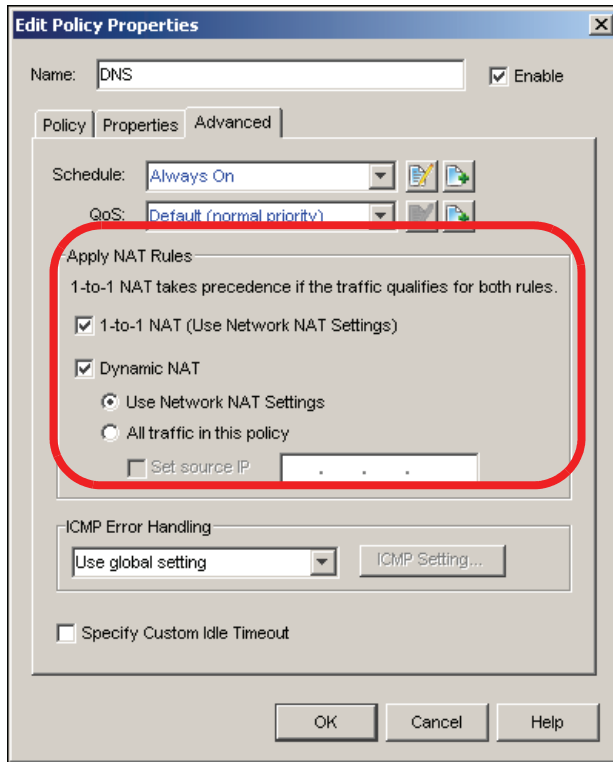


## Network Address Translation (NAT)

There are few differences in NAT functionality between WFS and Fireware. To find the firewall NAT settings, the navigation has changed from **Setup > NAT** in WFS, to **Network > NAT** in Fireware. In Fireware, 1-to-1 NAT has higher precedence than dynamic NAT, so it is no longer necessary to add exceptions for 1-to-1 NAT rules.

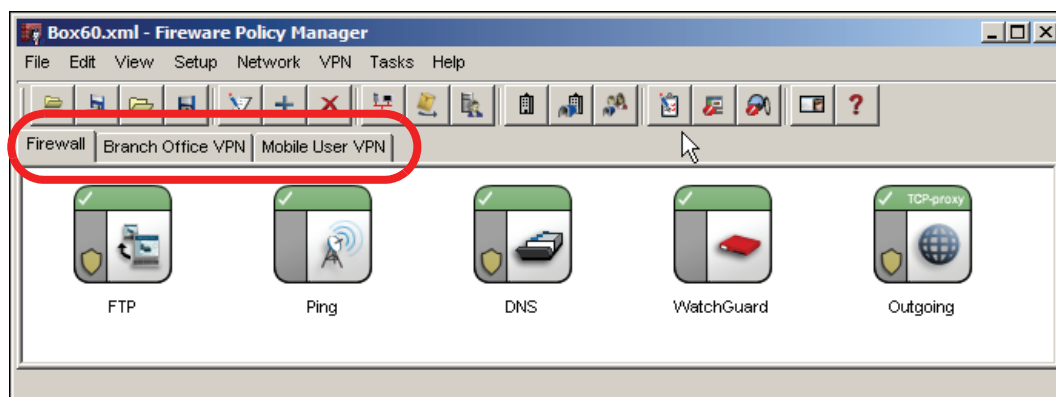
Policy-based NAT (service-based NAT in WFS) is enabled by default in Fireware. However, it still functions exactly as WFS versions do, making use of the firewall dynamic and 1-to-1 NAT tables that you see if you select **Network > NAT** in Fireware Policy Manager. If you have a policy that must manage NAT settings

differently than those supplied by the firewall NAT tables, edit the NAT rules on the **Advanced** tab of the **Policy Properties** dialog box.



## Virtual Private Networking

In Fireware, you can configure policies for the firewall separately from MUVPN or BOVPN policies. Each set of policies is configured on a different tab in Fireware Policy Manager.



When you configure MUVPN or BOVPN tunnels, Policy Manager automatically adds the Any policy to the appropriate policy set. If you want to restrict the ports accessible through the VPN tunnel, you can remove the Any policy and add the policies you want.

## MUVPN and Fireware

Both WFS and Fireware appliance software use the same MUVPN client software. There are two primary differences between the MUVPN implementation of WFS and Fireware:

- In WFS, you could create MUVPN profiles for individual users or for groups. In Fireware, you must configure group accounts that enable extended authentication. You then send the same .wgx file to all users in that group. You cannot configure a .wgx file for a single user.
- If you want to allow MUVPN users to get access to the Internet through the Firebox and your MUVPN allowed resource is set to “All traffic through tunnel,” you must edit the appropriate policy in the **Firewall** tab of Policy Manager to allow traffic from the “Tunnel-Switch” alias to “Any-External.”

## BOVPN and Fireware

If you use NAT through a branch office VPN tunnel, it is important to understand that the NAT settings you apply to your firewall policy on the Policy Manager **Firewall** tab do not apply to any VPN tunnels. If you want to use NAT through a VPN tunnel, you must configure NAT when you configure the VPN tunnel. For more information about the use of NAT in a BOVPN tunnel, see [https://www.watchguard.com/support/Fireware\\_Howto/](https://www.watchguard.com/support/Fireware_Howto/).

---

### Note

---

In Fireware, the routing policies configured in a BOVPN tunnel are known as “Local-Remote Pairs.”

---

## Services

---

In Fireware® you configure services with a very different procedure from WFS. The largest change is that there are no **Incoming** and **Outgoing** tabs in the definitions. Also, services are now known as *policies*. Each policy icon has a tab to configure the familiar **From** and **To** traffic settings, a tab to see and manage the properties of the policy, and an **Advanced** tab. When you migrate a WFS service to Fireware Policy Manager, you must create at least one policy for the information shown in the WFS **Incoming** tab and one for the **Outgoing** tab. This change is necessary only when the current WFS connection setting is either **Enabled and Allowed** or **Enabled and Denied** with log messages enabled for **Denied Packets**. The direction of the traffic the policy controls is decided by the network or host address information you enter in the policy. For example, a policy that allows traffic from Trusted to External is similar to a WFS service icon with the **Outgoing** tab set to allow traffic from Trusted to External. This increases flexibility, especially when you have more than one type of physical interface in use. However, it also gives the potential to misuse the Any service when you complete the **From** and **To** entries.

## Using the policy generated by the Quick Setup Wizard

The Firebox configuration file created when you use the Fireware Quick Setup Wizard is different in several ways from the default configuration file created with WFS. Because most users start with this basic configuration file when they build their new Fireware configuration, it is important to understand the differences:

- The Fireware Quick Setup Wizard adds an **Outgoing** policy to Policy Manager. This policy applies the HTTP proxy to all outbound HTTP traffic. In WFS, the HTTP proxy was not enabled by default. This supplies a more secure default configuration, but can cause problems for users who are not accustomed to using the HTTP proxy.

- Because the **Outgoing** policy does not include rules for UDP traffic, the wizard automatically adds a **DNS** policy to allow outbound DNS requests.
- In Fireware, you can set policy precedence automatically or manually. If you change your Policy Manager to show in detailed mode (**Policy Manager > View > Details**), the policies are shown in order of precedence. You can move policies up or down in the view to change their precedence, or select **View > Auto-order mode** to change the order automatically.

### Using the “Any” alias

The “Any” alias refers to all traffic sent from any source to any destination. You must restrict the use of the “Any” alias in your policies as much as you can. When you manage the migration, apply the “Any” alias only when no other policy will operate correctly. For example, when you migrate a WFS service that allows incoming from Any to Any, migrate it to a Fireware policy that allows from External to Firebox (maybe with a NAT entry specified to port forward the connections to a trusted server).

### Policy Manager and Firebox management

WatchGuard System Manager 8.3 includes the ability to create and manage VPN tunnels, similar to the features of VPN Manager. It also includes a feature that allows you to centrally configure and manage a large number of Firebox X Edge devices from a central location. If you manage other Firebox devices with a Management Server protected by a WatchGuard Firebox, make sure that the configuration of your gateway Firebox includes these provisions:

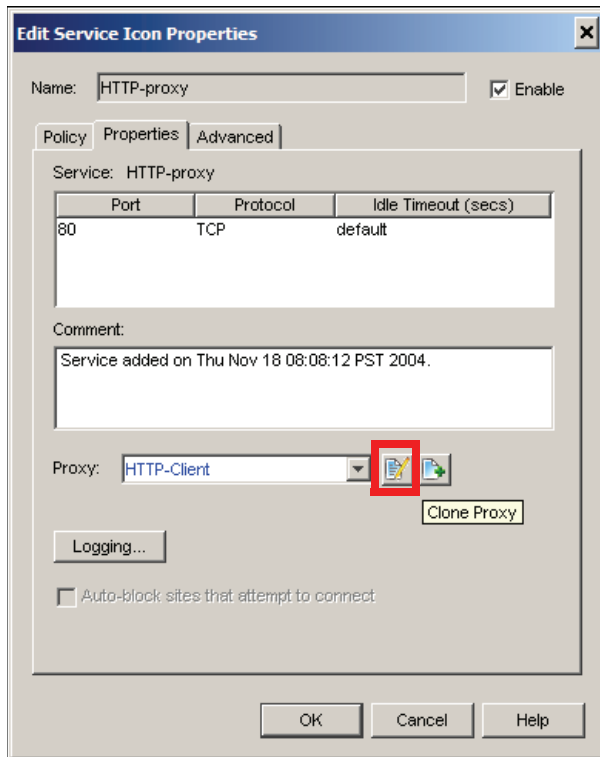
- If you manage Firebox SOHO or Firebox X Edge devices, make sure your gateway Firebox includes the **WG-SmallOffice-Mgmt** policy, configured to apply static NAT and allow traffic from the Any-External alias to the IP address of your Management Server. You make your configuration more secure if you replace the Any-External alias with the external IP addresses of any managed devices.
- If you manage Firebox III, Firebox X Core, or Firebox X Peak devices, make sure your gateway Firebox includes the **WG-Mgmt-Server** policy, configured to apply static NAT and allow traffic from the Any-External alias to the IP address of your Management Server. You make your configuration more secure if you replace the Any-External alias with the external IP addresses of any managed devices.

---

## Proxies

Proxy configuration for Fireware® has many more features and greater flexibility than WFS. Because of this, there are very few direct correlation points between what is configured in WFS Policy Manager and where a feature appears in Fireware Policy Manager. The most important thing to understand is that the proxies in Fireware are all configured with similar procedures. After you understand the procedures, they supply a powerful tool to protect resources comprehensively and intelligently. For more information about configuring proxies in Fireware, see the *WatchGuard System Manager User Guide*, “Configuring Proxies” chapter.

The configuration properties for the proxies in Fireware are now separate from the policies. It is possible to create proxy configurations, known as a proxy action, that you can share among multiple policies. Fireware includes default configurations for the different proxy policies. You cannot change these default configurations. To edit a configuration, or action, there is a clone feature that allows you to create a new action based on an existing action.



The default proxy actions are named to represent the situations in which they are used to protect resources. For example, there is an HTTP Client proxy action and an HTTP Server proxy action. The HTTP-Client proxy action was created to protect HTTP clients. In other words, it is most likely used on a policy applied to outbound traffic. The HTTP-Server proxy action was created to protect a web server. It is most likely used on a policy allowing access to a web server from external users.

To open proxy actions in Fireware Policy Manager, select **Setup > Actions > Proxies**.

#### Note

In each proxy action there is a **Send a log message with summary information for each transaction** check box. If you do not select this check box, you do not get detailed report data in Historical Reports.

## Quick Setup Wizard and proxies

When you used the Quick Setup Wizard in WFS, an "Outgoing" service was automatically added to your Firebox configuration. This service allowed outgoing TCP and UDP connections by default and did not apply any proxies to this traffic.

The Fireware Quick Setup Wizard automatically adds a new type of "Outgoing" policy to your Firebox configuration. This policy enables the TCP proxy, with the proxy action for HTTP-Client traffic selected. This causes the Firebox to proxy traffic in the same way the WFS "Proxy" service did when you used WFS appliance software.

If you remove the Fireware "Outgoing" policy from Policy Manager, you cannot add it back to your configuration. It is put there by default for your convenience when you use the wizard, but is not one of the policies shown in the **Edit > Add Policies** list.

---

## **Authentication**

---

With Fireware, the list of supported authentication servers has changed significantly. Windows native mode (NT) and CRYPTOCard authentication are not supported in Fireware. If you used WFS NT Server authentication, you can now use Active Directory or RADIUS authentication if you have a Windows 2000/2003 domain. For more information, see [https://www.watchguard.com/support/Fireware\\_Howto/](https://www.watchguard.com/support/Fireware_Howto/).

Supported authentication methods include:

### *Firebox*

There are no changes in Firebox authentication.

### *RADIUS Server*

You must make sure your RADIUS server supports both PAP and MSCHAPv2. 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).

### *SecurID Server*

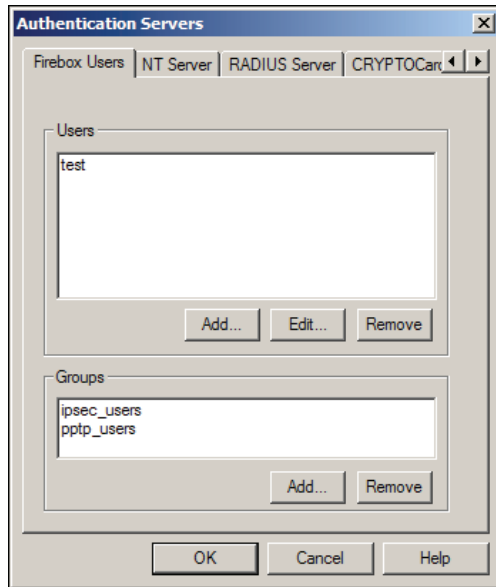
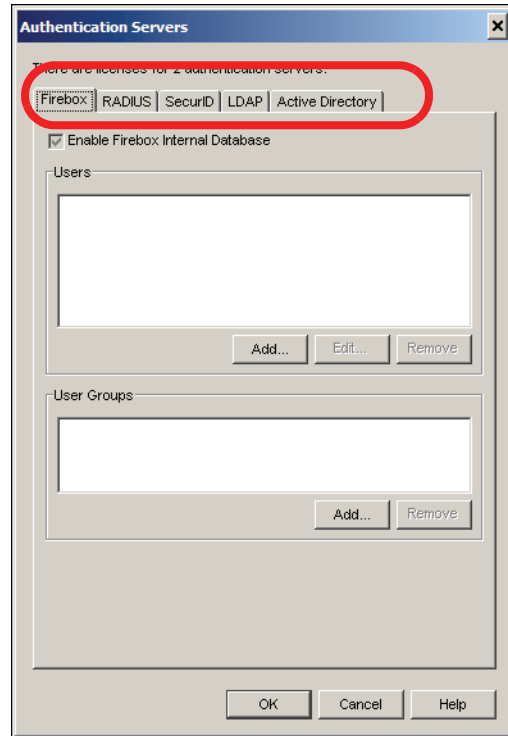
There are no changes in SecurID authentication.

### *LDAP*

With Fireware, you can use an LDAP (Lightweight Directory Access Protocol) authentication server to authenticate your users to the Firebox.

### *Active Directory*

With Fireware, you can use an Active Directory authentication server to authenticate your users to the Firebox.

**WSM 7.x Firewall Authentication****WFS Authentication Servers****Authenticating through the Firebox**

The Java applet used for firewall authentication in WFS is not used in Fireware® Pro/Fireware. Instead, a web page is available at the same URL using *https* instead of *http*. I

In WFS, your users authenticated with the URL that looked like: `http://10.1.1.1:4100`

In Fireware, your users must type:

`https://IP address of a Firebox interface:4100/`

or

`https://Host name of the Firebox:4100`

**Authentication time-outs**

In WFS, when an authenticated user closed the web browser window in which they authenticated, the authenticated session stops. In Fireware, if the user closes the web browser window in which they authenticated, the user stays authenticated until the authentication time-out occurs. This time-out is controlled in **Policy Manager > Setup > Global Settings**.

**Using Firebox System Monitor to close authentication sessions**

You can see a list of all currently authenticated users on the **Firebox System Monitor > Authenticated User** tab. You can also remove an authenticated user from the list. To do this, right-click their user name and then stop their authenticated session.

---

## **Intrusion Prevention/Default Packet Handling**

---

Many of the same options are available in Fireware® as were available in WFS Policy Manager. However, by default, log messages for broadcast traffic are turned on. To turn this off, add a policy that matches the traffic and disable log messages in that policy.

The **Auto-block source of packets not handled** option is disabled by default. If you enable this option, you must be very careful or you could block many external sites that you do not want to block.

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

### **Blocked Sites**

Fireware's blocked sites support has changed. The blocked sites list can now apply to all interfaces. Be very careful to not add entries here that could 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 sure to add a **Blocked Sites Exceptions** entry for the networks or hosts that are safe.

Fireware will automatically add sites to the Blocked Sites list on any interface.

### **Migrating WFS blocked sites to Fireware**

Fireware blocks sites on all interfaces. WFS blocks sites only on the external interface. Therefore you cannot copy the default Blocked Sites list from a WFS configuration to a Fireware configuration. A default WFS configuration includes the private subnets (10.0.0.0/8, 192.168.0.0/16, 172.16.0.0/16) on the Blocked Sites list. If you copy this configuration to Fireware, all internal subnets are blocked on all interfaces, which could cause a Denial of Service (DoS) and effectively disable the trusted network.

### **Using HostWatch to block sites**

You can now add sites to the blocked sites list from the HostWatch user interface. Right-click on a connection in the connections list and select the site to block.