

What are the major differences between Fireware and WFS appliance software?

Fireware/General

This document applies to:

Appliance	Firebox X Core / Firebox X Core e-Series / Firebox X Peak / Firebox X Peak e-Series
Appliance Software versions	WFS 7.4.1 / Fireware Pro 8.3
Management Software versions	WatchGuard System Manager 8.3

Introduction

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. Fireware Pro includes such features as dynamic routing, multi-WAN support, and an optional subscription to a signature-based intrusion prevention system. At the same time, we did not move all WFS appliance software features into Fireware Pro.

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

Appliance software feature matrix

There are significant differences between the WFS appliance software and the new Fireware Pro 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
Upgradeable	Model Upgradeable	Yes (except Firebox III)	Yes	Yes	
Networking Features	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	

Feature or Functional Area		WFS	Fireware	Fireware Pro	Notes on Fireware/Fireware Pro Implementation
	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.
	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.
High Availability	Active/Standby	Option	No	Yes	In Fireware, you can use HA together with a Management Server to manage your VPN tunnels.
Application Layer Filtering	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.

Feature or Functional Area		WFS	Fireware	Fireware Pro	Notes on Fireware/Fireware Pro Implementation
Authentication	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	
	RADIUS	Yes	Yes	Yes	
	LDAP/Active Directory	No	Yes	Yes	
	Windows NT Server authentication with 2000/2003 compatibility (NTLM)	Yes	No	No	
VPN	Firebox database	Yes	Yes	Yes	
	SecurID	Yes	Yes	Yes	
	Cryptocard	Yes	No	No	
	PPTP	Yes	Yes	Yes	
	PPTP with RADIUS authentication	Yes	Yes	Yes	
Management	MUVPN (IPSec)	Yes	Yes	Yes	In Fireware, you can use any supported authentication server to authenticate MUVPN connections.
	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.

Feature or Functional Area	WFS	Fireware	Fireware Pro	Notes on Fireware/Fireware Pro Implementation	
	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.
Monitoring Tools	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.
	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 Management	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.

Feature or Functional Area	WFS	Fireware	Fireware Pro	Notes on Fireware/Fireware Pro Implementation	
	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.
Logging	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.
	Advanced log message options	Yes	Yes	Yes	Fireware supplies more diagnostic logging. For more information, see the Reference Guide.
Reporting	Historical Reports	Yes	Yes	Yes	8.x includes new reports and support for XML log files.
Options	Spam blocking	SpamScreen	spam-Blocker	spam-Blocker	spamBlocker offers an easier-to-use, more effective spam blocking solution.
	WebBlocker	Yes	Yes	Yes	Both Fireware and WFS now support 40 WebBlocker categories.
	Antivirus	Gateway AntiVirus for E-mail (Firebox X Core only)	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.

Was this document helpful? Please send your feedback to faq@watchguard.com.

SUPPORT:

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

COPYRIGHT © 2006 WatchGuard Technologies, Inc. All rights reserved.

WatchGuard, the WatchGuard logo, Firebox, Core, and Fireware are registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries.