Fireware XTM v11 Release Candidate 1 (RC1)

Release Notes for XTM 1050 and e-Series Appliances

Introduction

WatchGuard is pleased to release Fireware XTM v11 OS RC1 for the Firebox X Edge, Core, and Peak e-Series devices. This release candidate software also includes a Fireware XTM OS update for our brand new XTM 1050 devices.

Fireware XTM v11 is a new operating system for your Firebox e-Series or XTM device that combines the best of WatchGuard's Edge and Fireware appliance software features and offers exciting new Extensible Threat Management features. The Fireware XTM v11 release is the first release that offers you a choice of management interfaces to manage your Firebox:

- WatchGuard System Manager with Fireware XTM Policy Manager - updated with many new management features,
- Fireware XTM Web UI - a completely redesigned web browser-based interface that you can use to manage any Fireware XTM device
- Fireware XTM CLI - the first fully supported command line interface for all WatchGuard XTM devices

For existing Edge, Core and Peak e-Series customers, the Fireware XTM v11 release also introduces many new features for the WatchGuard Firebox product line. Major new features include:

- FireCluster - Active/Active load balancing for a pair of Firebox X Core/Peak e-Series or XTM 1050 devices
- Enhanced HTTPS proxy with deep packet inspection and dynamic certificate status checking using OCSP (Online Certificate Status Protocol)
- Role Based Access Control (RBAC) for more granular delegation of management responsibilities for administrators. This feature only applies for devices managed by a WatchGuard Management Server.
- Control access to RBAC based on Active Directory user name or group
- A consolidated WatchGuard Server Center from which you can configure and manage all WatchGuard servers running on a local Windows-based computer.
- Centralized management for all devices running Fireware XTM OS with new Fireware XTM templates. Other new features include the ability to do scheduled configuration changes, OS updates, and feature key synchronization for centrally managed devices.
- Application Blocker profiles you can apply to any HTTP proxy policy
- A new, improved, and more powerful Gateway AV engine
- New call setup security features for the SIP and H.323 Application Layer Gateways (SIP and H.323 proxies have been renamed as application layer gateways in v11)
- HTTP proxy redirect to a caching proxy server
- Automatic redirection to the Firebox authentication page when a user tries to browse the Web without authentication
- Severity levels for IPS signatures

- Override WebBlocker with a password, and create a different inactivity timeout for each web site
- Increased proxy performance
- Log Server performance and scalability enhancements
- Reporting enhancements, including the ability to define the format of report content, on-demand reporting, and new report types
- Transparent Bridge mode
- Support for network bridging of multiple interfaces
- Port independence for Firebox X Edge users, and the ability to configure your own trust relationships between Edge network interfaces
- Support for multicast routing through a BOVPN tunnel to support one-way multicast streams between networks protected by WatchGuard devices
- Support for limited broadcast routing through a branch office VPN tunnel. The tunnel supports broadcasts to the broadcast IP address of 255.255.255.255 only.
- NAT loopback support
- SSL VPN no longer requires clients to open port 4100
- Support for VLANs on external interfaces

Minor feature enhancements include:

- Support for Mobile VPN with IPSec user roaming
- Several Intrusion Prevention subscription service enhancements
- Single Sign-On improvements
- TCP/UDP proxy support for HTTP traffic filtering
- QoS and scheduling support for managed VPN tunnel policies
- Support for metrics on static routes

See the *Product/Feature Matrix* later in this document for a list of features supported in Fireware XTM and notes about changes in feature implementation for our Firebox X Edge, Core, and Peak e-Series devices. When you review this list of changes in feature implementation, it is important to understand that a few features that have been supported in previous releases of Fireware or Edge appliance software are NOT supported in Fireware XTM OS. These features are limited to:

- The Firebox X Edge no longer includes an FTP server
- We no longer support Microsoft Windows 2000
- The TFTP Proxy has been removed. We now offer a pre-defined TFTP packet filter.
- SIP and H.323 packet filters are no longer supported. Users can now use the SIP and H.323 application layer gateways (called Proxies in v10.x).
- Administrators that log in to the Web UI do not automatically get access through the Firebox. They must additionally authenticate through the port 4100 authentication portal
- VPN support (branch office VPN, Mobile VPN with IPSec, SSL, or PPTP) is not available on Firebox X Edge e-Series devices when you use the serial modem or when you enable your external interface as a wireless interface.
- If you have configured custom event notification rules, these rules are dropped from your configuration when you upgrade from Fireware v10.x to Fireware XTM.

Before You Start

Before you install this release, make sure that you have:

- A Firebox X Core or Peak e-Series device running Fireware v10.2.x, a Firebox X Edge e-Series device running v10.2.9 or higher, or a WatchGuard XTM 1050.
- An appropriate Firebox and the required hardware and software components as shown in Minimum System Requirements below.
- Feature key for your Firebox – If you upgrade your Firebox from an earlier version of Fireware or Edge appliance software, you can use your existing feature key. If you have any questions or problems with your feature key, email beta@watchguard.com.

Documentation for this product is available in an updated HTML help system available at these URLs:

For WSM: http://www.watchguard.com/help/docs/wsm/11/en-US/index.html

For the Web UI: http://www.watchguard.com/help/docs/webui/11/en-US/index.html

Minimum System Requirements

	If you have WatchGuard System Manager client software only installed	If you install WatchGuard System Manager and WatchGuard Server software
Operating System	Windows Vista (32-bit), XP SP2, or Windows Server 2003	Windows Vista (32-bit), Windows XP SP2, or Windows Server 2003
Browser	IE 6, IE 7, Firefox v2	IE 6, IE 7, Firefox v2
CPU	Intel Pentium IV	Intel Pentium IV
Processor Speed	1 GHz	2 GHz
Memory	512 MB	1 GB
Available Disk Space	80 MB	1 GB

Downloading Software

Release candidate software and documentation are available for download on the WatchGuard support web site at this link: https://www.watchguard.com/support/faqs/beta_agreement.asp. You must have a valid LiveSecurity account to get access to the beta software download page.

There are several software files available for download. See the descriptions below so you know what software packages you will need for your upgrade.

All users can now download the WatchGuard System Manager software. With this software package you can install WSM and the WatchGuard Server Center software:

- `WSM11s.exe`

Select the correct Fireware XTM OS RC1 image for your hardware:

- `XTM_OS_Core_Peak_11_0.exe` (for Firebox X Core and Peak e-Series devices)

- `XTM_OS_1050_11_0.exe` (for WatchGuard XTM 1050 devices)
- `XTM_OS_Edge_11_0.exe` (for Firebox X Edge e-Series devices)
- `edge_11_0.exe` (for Firebox X Edge e-Series devices using v10.2.9)

You may need to download the following package in case you wish to downgrade your Firebox X Core or Peak e-Series from Fireware XTM v11.0 to v10.2.x:

- `utm_core_peak.down2fw.sysa-dl`

To use Single Sign-on, you must download these two files:

- WG-Authentication-Gateway.exe (SSO Agent software)
- WG-Authentication-Client.msi (SSO Client software)

Installation and Upgrade Instructions for Firebox X Edge

Before you install Fireware XTM v11 RC1 software, read the information in the Known Issues section below.

> ***Note*** To upgrade your Firebox X Edge e-Series to Fireware XTM from Edge v10.x or earlier, you must have Edge v10.2.9 or higher installed on your Edge.

Upgrade your Firebox X Edge e-Series from Fireware XTM v11 Beta 5 to RC1

You can upgrade to Fireware XTM Release Candidate directly from Beta 5. If you have an earlier version of Fireware XTM beta software installed on your Firebox, you must first downgrade to v10.2.9 or 10.2.10 before you upgrade to the Release Candidate build. Downgrade instructions are provided below.

1. On the computer you use to connect to the Edge, find and run the `XTM_OS_Edge_11_0.exe` file you downloaded from the WatchGuard beta site.
2. From the Fireware XTM Web UI, select **System > Backup Image** to save a backup image of your Firebox.
3. From the Fireware XTM Web UI, select **System > Update OS**.
4. Click **Upgrade**.

Upgrade your Firebox X Edge e-Series v10.2.9 or higher to Fireware XTM v11

Your Edge must have Firebox X Edge v10.2.9 or higher installed before you can upgrade to Fireware XTM v11. To upgrade your Edge, connect to your Edge from a computer on a local (not routed) network behind the Edge on which you have administrator privileges. You can also upgrade your Edge from a computer on an external network.

The Update Wizard updates the operating system on your Edge and converts your Edge configuration to be compatible with Fireware XTM. The wizard converts all predefined and custom policies, security subscriptions, authentication settings, network settings, NAT settings, branch office VPNs, default threat protection settings, and logging and time settings.

> ***Note*** The new Web UI is available only on port 8080 by default. You can change this port in the Web UI after you complete the Update Wizard. To connect to the Edge after your configuration is converted, you must connect to the Edge with this URL:
> *https://<IP address of your Edge>:8080*

The Update Wizard does not convert some features. After you finish this procedure, examine your configuration for the following features, which are not converted by the Update Wizard:

- MAC access control lists
- Traffic Management
- VLANs
- Modem settings
- Mobile VPN configuration
- SNMP
- Single Sign-On

To upgrade your Firebox X Edge from v10.2.9 or higher to Fireware XTM v11:

1. Connect to your Edge System Status page and select **Administration > Backup** to back up your existing Edge configuration file.
2. Run the Edge_11_0.exe file you downloaded from the beta software download site. The Firebox X Edge Update Wizard starts.
3. Use the Firebox X Edge Update Wizard to load Fireware XTM v11 on your Edge and convert your configuration file to v11.
4. When the wizard is complete, you can connect to the Fireware XTM Web UI on your Edge with the URL https://<IP address of Edge>:8080.
5. If you want to test WSM and Policy Manager with your Edge, you must install WSM software. To install WSM, download the WSM11s.exe file from the beta software download site.

Downgrade your Firebox X Edge e-Series from Fireware XTM v11 to v10.2.x

Before you downgrade a Firebox X Edge e-Series from Fireware XTM v11 to Firebox X Edge v10.2.x, go to the WatchGuard Software Downloads Center. Download and save the file that matches the version of Edge software to which you want to downgrade. You use Policy Manager or the Web UI to complete the downgrade procedure.

From the Web UI:

1. Connect to your Edge System Status page and select **System > Upgrade OS**.
2. Browse to and select the `yakfw.sysa-dl` file that you saved. Click **Upgrade**. This restores the operating system version you selected. The Edge will reboot and become active with the v10.2.x configuration that was in use on the Edge immediately before the upgrade to v11.
3. You can also choose to restore the backup configuration file you saved before you upgraded to v11.

Installation and Upgrade Instructions for Firebox X Core/Peak

Before you install the WSM and Fireware XTM v11 RC1 software, read the information in the Known Issues section below.

> ***Note*** To upgrade your Firebox X Core or Peak e-Series to Fireware XTM v11 from an earlier version of Fireware, you must have Fireware v10.2.8 or higher installed on your Firebox.

Upgrade your Firebox X Core or Peak e-Series to the Fireware XTM RC1

You can upgrade to Fireware XTM RC1 directly from Beta 5. If you have an earlier version of Fireware XTM beta software installed on your Firebox, you must first downgrade to v10.2.9 or 10.2.10 before you upgrade to the Release Candidate build. Downgrade instructions are provided below.

1. We strongly advise you to back up your current v10.2.x or Beta 5 system configuration before you upgrade. From Policy Manager, select **File > Backup** to back up your existing Fireware configuration file and Fireware image.
2. Close all other programs on your management computer.
3. It is not necessary to uninstall previous versions of WSM unless you have installed WatchGuard server software on your computer. If you have installed server software, uninstall WSM using these instructions:
   From the Windows Start Menu, select **Control Panel > Add/Remove Software** and uninstall your previous version of WSM. If you use the WebBlocker Server or Management Server, select **No** when asked if you want to remove data from these servers. Make sure that you restart your computer to complete the uninstall process.
4. Launch `WSM11s.exe` and use the on-screen procedure to install the software. When you run the WSM v11 install program, select the options to install client software and the appropriate server software.
5. After the `WSM11s.exe` install program is complete, launch `XTM_OS_Core_Peak_11_0.exe` and use the on-screen procedure to install the software.
6. Open WSM v11 and select **File > Connect to Device**. The **Connect to Firebox** dialog box appears. In the **Name/IP address** text box, type the IP address of your Firebox. Click **OK**.
7. Launch Policy Manager. Click **Yes** when prompted to upgrade to v11.
8. Click **Yes** to convert the configuration file to v11.
9. From Policy Manager, select **File > Upgrade**.
10. When the **Save** dialog box appears, click **Save**. Click **Yes** to save the file to your management computer.
11. When the Upgrade dialog box appears, type your configuration passphrase and click **OK**.
12. Click **OK**.
    The default path is C:\Program Files\Common Files\WatchGuard\resources\FirewareXTM\11.0\Core_Peak\FW1100BNNNNNN.wgu where "NNNNNN" is the release build number.
13. Click **OK**.
14. Click **Yes** to upgrade your Firebox now.
15. Click **Yes** when asked to create a Firebox backup image.
16. Type an encryption key to encrypt the backup file. Click **OK**.
    If you get an error, click OK or Cancel and continue with the procedure.

When the backup and upgrade are finished, the Firebox reboots.

Downgrade your Firebox X Core/Peak e-Series from Fireware XTM v11 to Fireware v10.2.x

To downgrade from Fireware XTM to Fireware, you must download a special downgrade file from the software downloads page. The file is called `utm_core_peak.down2fw.sysa-dl` and downgrades your device to Fireware v10.2.8. Once your Firebox is downgraded to v10.2.8, you can then restore your Fireware configuration, or upgrade to v10.2.9 or 10.2.10 and try the upgrade to Fireware XTM again.

1. Before you downgrade your Firebox X Core or Peak e-Series from Fireware XTM v11 to Fireware v10.2.8, you must browse to https://www.watchguard.com/support/faqs/beta_sw.asp. Download and save the `utm_core_peak.down2fw.sysa-dl` file to your WSM management station. Then:
2. Open WSM v11. Connect to your Firebox and launch Policy Manager.
3. From Policy Manager, select **File > Upgrade**. When prompted, browse to and select the `utm_core_peak.down2fw.sysa-dl` file that you saved.

During the downgrade procedure, the Storage LED on the front of the Firebox will blink rapidly. When the downgrade procedure is complete, the Firebox will start v10.2.8 with the configuration file you had before the upgrade to v11. The version number appears as "10.2.8dwn" to indicate that it is a downgrade. We recommend that you restore your previous v10.2.x backup after you downgrade from v11, or install any released v10.2.x operating system before you perform another upgrade to v11.

Upgrade HA to FireCluster

WSM v11 includes a HA upgrade wizard to help you upgrade the software on both your HA devices so you can enable FireCluster. With FireCluster, you can choose to configure your two devices in an active/passive cluster or an active/active cluster. Before you begin the upgrade process, we strongly recommend that you connect to the online help at http://www.watchguard.com/help/docs/wsm/11/en-US/index.html and read the chapter about FireCluster. There are important differences in license requirements and network integration you must understand before you implement FireCluster. Note that the HA upgrade wizard helps you to update the OS on your HA devices. You must reconfigure the devices for FireCluster manually when the upgrade is complete.

If you are in routed mode and have HA enabled in your Fireware v10.2.x configuration file, WSM launches the HA Upgrade Wizard automatically when you select **File > Upgrade** from Policy Manager. The Wizard upgrades the OS on your first HA device, then puts it in a factory-default state until the second HA box is updated. The Wizard then prompts you to upgrade your second device.

Now, you can connect to the second HA device with WSM Policy Manager and select **FireCluster > Setup**. The FireCluster Setup Wizard will launch to help you enable and configure your FireCluster. When you complete the Setup Wizard, you must save your configuration to the active device. Then, you must reboot both devices in your FireCluster.

Installation and Upgrade Instructions for XTM 1050

Before you install the WSM and Fireware XTM v11 RC1 software, read the information in the Known Issues section below.

Upgrade your XTM 1050 to Fireware XTM v11 RC1

1. On the computer you use to connect to the XTM 1050, find and run the `XTM_OS_1050_11_0.exe` file you downloaded from the WatchGuard beta site. This installation extracts an upgrade file called `utm_xtm1050.sysa-dl` to the default location of `C:\Program Files\Common files\WatchGuard\resources\FirewareXTM\11.0\XTM10`.
2. Connect to your XTM 1050 with the Web UI and select **System > Upgrade OS**.
3. Browse to the location of the `utm_xtm1050.sysa-dl` file referenced in Step 1 and click **Upgrade**.

Known Issues and Limitations

These are known issues for Fireware XTM v11 RC1 and all management applications. Where available, we include a way to work around the issue.

General

- The minimum supported screen resolution for all WatchGuard System Manager applications and the Fireware XTM Web UI is 1024x768.
- If your Firebox X Edge e-Series device is connected to a modem, it may not boot correctly if you try to set your Edge into Recovery Mode. [30284]
- If you upgrade to Fireware XTM from an earlier version of Fireware and used a branch office VPN Phase 2 encryption setting of **None**, this setting is not correctly converted when during the configuration upgrade. You must edit your Phase 2 encryption setting manually when the upgrade is complete.

WatchGuard System Manager

- Remote managed Firebox devices configured in drop-in mode may not be able to connect to a Management Server that is behind a gateway Firebox also configured in drop-in mode. [33056]
- You cannot uninstall WatchGuard System Manager successfully when the WatchGuard Server Center is running on a computer using 64-bit Windows Vista. [39078]

  Workaround:

  Exit the WatchGuard Server Center. You can then uninstall WatchGuard System Manager successfully.

Networking

- When you change the IP address of a VLAN configured on an external interface from static to PPPoE and the Firebox cannot get a PPPoE address, Firebox System Manager and the Web UI may continue to show the previously used static IP address. [39374]
- When you configure your Firebox with a Mixed Routing Mode configuration, any bridged interfaces show their interface and default gateway IP address as 0.0.0.0 in the Web UI. [39389]
- When you configure your Firebox in Bridge Mode, the LCD display on your Firebox shows the IP address of the bridged interfaces as 0.0.0.0. [39324]
- When you configure your Firebox in Bridge Mode, the HTTP redirect feature is configurable from the user interface but does not work in this release. [38870]
- Static MAC/IP address binding does not work when your Firebox is configured in Bridge mode. [36900]
- When your Firebox is configured to use Bridge mode, the physical interface of the Firebox does not appear correctly in log messages. Instead, the interface is represented as "tbrX". [36783]
- When you change your configuration mode from Mixed Routing to Bridge or from Bridge to Mixed Routing, the CLI and Web UI may continue to show the previous configuration mode. [38896]

Wireless

- When you set the external interface as a wireless client and configure static NAT to use the eth0 interface as its source IP address, inbound static NAT does not operate correctly. [38239]

FireCluster

- When you have an active/active FireCluster and use the WebBlocker Override feature, you may be prompted to enter your override password multiple times. [39263]
- Every network interface enabled in a FireCluster is automatically monitored by FireCluster. You must make sure that all enabled interfaces are connected to an active interface.
- FireCluster is not supported if you use either a Drop-in or Bridge network configuration mode on your WatchGuard devices. [37287]
- If you use the Mobile VPN with IPSec client from the same network as the external network address configured on your FireCluster, some traffic may not go through the VPN tunnel. [38672]
- Mobile VPN with PPTP users do not appear correctly in Firebox System Manager when you are connected to a passive FireCluster member. [36467]

Logging and Reporting

- If you use an ISS server to serve published reports, you must configure the IIS server to recognize .png file extensions or you get an error about missing files. For information on how to configure your IIS server to recognize .png file extensions, see http://www.libpng.org/pub/png/png-iis-config.html. [39319]
- The Report Server does not pull data from the database automatically after you restart the PostgresSQL database. [35063]

  Workaround:

  From the WatchGuard Server Center, restart the Report Server.

Authentication

- In order for the Authentication Redirect feature to work, HTTP or HTTPS traffic cannot be allowed through an outgoing policy based on IP addresses or aliases that contain IP addresses. The Authentication Redirect feature operates only when port 80 and 443 policies are configured for user or user group authentication. [37241]

Proxies

- Microsoft Outlook communication using RPC over HTTPS fails when you have deep packet inspection enabled in your HTTPS proxy. [37503]

  Workaround:

  Add Microsoft Exchange in your HTTPS proxy exception list.

- You cannot make a SIP-based call from Polycom PVX softphone behind a Firebox to a Polycom PVX on the external network. [38567]

  Workaround:

  You can use the H.323 protocol instead of SIP.

Mobile VPN with IPSec

- A continuous FTP session over a Mobile VPN with IPSec connection could get terminated if an IPSec rekey occurs during the FTP transfer. [32769]

Workaround:

Increase the rekey byte count.

Manual BOVPN

- The VPN Keep-Alive feature is not available for the Firebox X Edge e-Series. [37769]
- If you have a large number of branch office VPN tunnels in your configuration, the tunnels may take a long time to appear in Policy Manager. [35919]
- When you set the Phase 2 SA expiration to zero by setting the Life-time and Life-size values to 0, the Firebox changes the rekey life-time to 8 hours. [37209]

Certificates

- You cannot import a CRL in DER format into Firebox System Manager. You must convert the CRL from DER to an acceptable format before you import the CRL into Firebox System Manager. [36643]
- DSA algorithm-based digital certificates are not supported in this release. [38758]

Workaround:

Use RSA algorithm-based digital certificates.

Using the CLI

The Fireware XTM CLI (Command Line Interface) is fully supported for the v11 release and a new and complete draft is available with the release candidate. For information on how to start and use the CLI, see the CLI Command Reference Guide. You can download the CLI guide from the beta software download site.

Technical Assistance

Support for the Fireware XTM RC1 is available from the Fireware XTM v11 beta board on the WatchGuard Support Forum.

Log in to http://forum.watchguard.com and select the Fireware XTM v11 Beta Board. If you do not see the 11 Beta Board in the list, send an email to beta@watchguard.com and ask to join the Fireware XTM v11 beta program.

Make sure to include your WatchGuard Forum use name and the serial number of the Firebox used for testing.

You can get support log information with Firebox System Manager (FSM). The FSM support log feature includes logs, as well as the following system information:

- Process list
- Memory use
- ARP table
- Network interface statistics
- Routes
- Compact flash use

- The Firebox debug directory (/tmp/debug) contents, including any other debug information stored by the components in this directory.

Feature/Product Matrix

Rows highlighted in blue represent new features or features supported in earlier releases that are no longer supported in Fireware XTM OS v11.

Feature/Functional Area		Edge v10.x appliance software	Fireware v10.x appliance software	Fireware XTM OS	Notes on Fireware XTM Implementation
Upgradeable	Model Upgradeable	Yes	Yes	Yes	A Firebox X Edge cannot be upgraded to a Firebox X Core or Peak. A Firebox X Core cannot be upgraded to a Firebox X Peak.
Networking Features	Interface Independence	No	Yes	Yes	On the Edge, LAN0-LAN2 operate as a three-port hub for the trusted interface.
	Interface trust relationships	Forced	User-defined	User-defined	For Edge users, policies are no longer configured as “incoming” and “outgoing.” Policies are now configured “to” a destination “from” a source.
	Traffic Management/QoS	Yes	Yes (Fireware Pro only)	Yes	A Pro upgrade is no longer required to use this feature. You can now apply a QoS action to managed VPN tunnel policies.
	Multi-WAN	Yes (Edge Pro only)	Yes (Fireware Pro required for weighted round-robin and Interface Overflow)	Yes (With same Pro requirements as in Edge/ Fireware v10.x)	New routing algorithms are supported for Edge users with a Pro upgrade. All multi-WAN interfaces are active at the same time.
	Interface bridging	No	No	Yes	You can connect two or more

Feature/Functional Area		Edge v10.x appliance software	Fireware v10.x appliance software	Fireware XTM OS	Notes on Fireware XTM Implementation
					interfaces to form a single interface to give more bandwidth to a group of servers on the same subnet, or to avoid physical networking restrictions.
	Interface MTU setting	Yes	Yes	Yes	Physical interfaces only.
	VLANs	Yes (Edge Pro only)	Yes (Fireware Pro only)	Yes (A Pro upgrade is no longer required)	You can now configure a VLAN on the external interface. Edge users can now configure multiple VLANs on one interface.
	Policy-based routing	Yes (Edge Pro only)	Yes (Fireware Pro only)	Yes (with Pro upgrade only)	
	Server load balancing	No	Yes (Fireware Pro only)	Yes (for Core/Peak devices with Pro upgrade only)	
	Dynamic Routing	No	Yes (Fireware Pro only)	Yes (for Core/Peak devices with Pro upgrade only)	Dynamic routing is not supported for Firebox X Edge devices in this release.
	Secondary Networks	No	Yes	Yes	You can now configure DHCP server to give IP addresses for a secondary network.
	DHCP Client	Yes	Yes	Yes	
	DHCP Server	Yes	Yes	Yes	
	DHCP Relay	Yes	Yes	Yes	

Feature/Functional Area		Edge v10.x appliance software	Fireware v10.x appliance software	Fireware XTM OS	Notes on Fireware XTM Implementation
	DHCP address reservation	Yes	Yes	Yes	
	Static MAC/IP address binding	No	Yes	Yes	
	MAC Access Control	Yes	No	Yes	
	Drop-In Mode	No	Yes	Yes	
	Routed Configuration Mode	Yes	Yes	Yes	In Fireware XTM, this is known as Mixed Routing Mode.
	Bridge Mode	No	No	Yes	
FireCluster (High Availability)	Active/Standby	No	Yes	Yes	This feature has been redesigned and is now known as FireCluster. We do not support Firebox X Edges with this feature.
	Active/Active	No	No	Yes	You can now configure load balancing. We do not support Firebox X Edges with this feature.
Application Layer Filtering					
	HTTP Proxy	Yes	Yes	Yes	You can now redirect HTTP traffic to a caching proxy server. The proxy now includes inbound HTTP server protection for Edge devices.
	HTTPS Proxy with Deep Packet Inspection	Yes (Outbound only, and used only to apply WebBlocker to HTTPS traffic)	Yes (Outbound and Inbound)	Yes (Outbound and Inbound)	Fireware XTM includes options for deep packet inspection, including content type filtering, URL filtering, and Protocol Anomaly

Feature/Functional Area		Edge v10.x appliance software	Fireware v10.x appliance software	Fireware XTM OS	Notes on Fireware XTM Implementation
					Detection.
	WebBlocker	Yes	Yes	Yes	Firebox X Core/Peak e-Series users now have a WebBlocker override option.
	SMTP Proxy	Yes (Inbound only)	Yes (Outbound and Inbound)	Yes (Outbound and Inbound)	There are many new configuration options for Edge users, including a new proxy action to protect outbound SMTP.
	POP3 Proxy	Yes (Outbound only)	Yes (Outbound and Inbound)	Yes (Outbound and Inbound)	There are many new configuration options for Edge users, including a new proxy action to protect a POP3 server located behind an Edge.
	FTP Proxy	Yes (Outbound only)	Yes (Outbound and Inbound)	Yes (Outbound and Inbound)	The proxy now includes inbound FTP server protection for Edge devices.
	TFTP Proxy	Yes	Yes	No	
	DNS Proxy	No	Yes (Outbound and Inbound)	Yes (Outbound and Inbound)	
	Transparent proxy support for VoIP	Yes	Yes	Yes	The SIP and H.323 proxy policies have been more accurately renamed as ALGs (Application Layer Gateways). Fireware XTM includes new

Feature/Functional Area		Edge v10.x appliance software	Fireware v10.x appliance software	Fireware XTM OS	Notes on Fireware XTM Implementation
					configuration options for increased call setup security and operates in more VoIP topologies.
	Outgoing Proxy, also known as the TCP/UDP proxy	Yes	Yes	Yes	Fireware XTM allows you to block or allow traffic based on the severity of the signature.
	Firewall-based default threat protection (protocol anomaly detection)	Yes	Yes	Yes	
	Signature-based IPS	Yes	Yes	Yes	
	Virus Detection	Yes	Yes	Yes	Fireware XTM includes a new Gateway AV implementation and supports more archive/compres-sion files.
	Spam Detection	Yes	Yes	Yes	
	SMTP Email Quarantine	Yes	Yes	Yes	
Authentication	RADIUS	Yes	Yes	Yes	
	LDAP/Active Directory	Yes	Yes	Yes	
	Firebox database	Yes	Yes	Yes	
	SecurID	No	Yes	Yes	
	VASCO DIGIPASS	No	Yes	Yes	
	Single Sign-On	Yes	Yes	Yes	For Active Directory domains only.

Feature/Functional Area		Edge v10.x appliance software	Fireware v10.x appliance software	Fireware XTM OS	Notes on Fireware XTM Implementation
	Browser-based user authentication	Yes	Yes	Yes	
	Trusted hosts	Yes			
Mobile VPN	Mobile VPN with PPTP	Yes	Yes	Yes	
	Mobile VPN with SSL	Yes	Yes	Yes	Fireware XTM includes a new option to bridge SSL traffic.
	Mobile VPN with IPSec	Yes	Yes	Yes	Fireware XTM includes new configuration options to support user roaming.
Branch Office VPN	BOVPN (IPSec)	Yes	Yes	Yes	
	1-to 1 NAT over BOVPN	No	Yes	Yes	Fireware XTM includes 1-to-1 NAT over BOVPN support for Edge devices.
	Dynamic NAT over BOVPN	No	Yes	Yes	Fireware XTM allows you to set the IP address to use as the masquerade point on all devices.
	Multicast over BOVPN	No	No	Yes	
	Broadcast over BOVPN	No	No	Yes	
	VPN Failover	Yes	Yes	Yes	Edge users can now configure a VPN to fail over to a second local gateway, as well as to a second remote gateway.
	Dead Peer Detection	Yes	Yes	Yes	

Feature/Functional Area		Edge v10.x appliance software	Fireware v10.x appliance software	Fireware XTM OS	Notes on Fireware XTM Implementation
Management	Management interface	Web only	WSM only	WSM, Web UI, and Command Line Interface	You can now choose the type of management interface you want to use with your Firebox.
	Centralized management	Yes	No	Yes	Use WatchGuard System Manager to manage one or more devices, including centralized management and monitoring of Firebox X Core and Peak devices.
	Backup/Restore	Yes—configuration file and licenses only	Yes—full flash image	Yes—full flash image for Core/Peak devices; configuration and license file only for Edge devices	
	Certificate Authority	No	Yes	Yes	
	Third-party certificate support for VPNs	Yes	Yes (Fireware Pro only)	Yes	No Pro license is required to use third-party VPN certificates in Fireware XTM.
	Drag-and-drop VPN setup for WatchGuard devices	Yes	Yes	Yes	Fireware XTM provides new control over QoS and policy scheduling for Edge devices.
	Management Server	Yes—as a device under centralized management only.	Yes	Yes	Yes
	Role-based administration	No	No	Yes	You must configure and use a Management Server to use the role-based administration

Feature/Functional Area		Edge v10.x appliance software	Fireware v10.x appliance software	Fireware XTM OS	Notes on Fireware XTM Implementation
					feature.
	Auditing	No	No	Yes	Fireware XTM includes audit reporting for configuration changes, updates to the OS, and license changes.
	WatchGuard Server Center	No	No	Yes	Use the new WatchGuard Server Center to set up, monitor, and configure your local servers.
Monitoring Tools	Firebox System Manager	No	Yes	Yes	You can now set notifications to occur for an event only after it occurs the first time. Traffic Manager now supports new interactive diagnostic tools, including TCPdump and DNS lookup. There is a new option to export certificates.
	HostWatch	No	Yes	Yes	HostWatch columns now show bytes and bytes/second.
	Performance Console	No	Yes	Yes	Fireware XTM includes a new streamlined counter set.
Policy Management	WSM Policy Manager for offline policy configuration	No	Yes	Yes	

Feature/Functional Area		Edge v10.x appliance software	Fireware v10.x appliance software	Fireware XTM OS	Notes on Fireware XTM Implementation
	Web UI Policy Manager	Yes	No	Yes	Existing Edge web user interface has been replaced with a new web user interface that also works with Core and Peak e-Series devices and the XTM 1050.
	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 precedence control	Automatic	Automatic/ Manual	Automatic/ Manual	With Fireware and Fireware XTM, you can set policy precedence manually, or use the default precedence order set by Policy Manager. This feature is not available if you use the Fireware XTM Web UI.
	1-to-1 NAT	Yes	Yes	Yes	
	Dynamic NAT	Yes	Yes	Yes	
	Static NAT/ Port Forwarding	Yes	Yes	Yes	
	NAT loopback	Yes	No	Yes	
	Per Policy Override for NAT	No	Yes	Yes	
	Per Policy Override for QoS	No	Yes	Yes	
	Policy scheduling	No	Yes	Yes	
	Policy disposition	Allow, Deny, No Rule	Allow, Deny, Deny (Send Reset)	Allow, Deny, Deny (Send Reset)—with granular control of the reset message	

Feature/Functional Area		Edge v10.x appliance software	Fireware v10.x appliance software	Fireware XTM OS	Notes on Fireware XTM Implementation
Logging	Log Server	Yes	Yes	Yes	Edge users can now install their own Log Server.
	XML Log Format	Yes	Yes	Yes	
	WSEP Log Format	Yes	Yes	No	
	LogViewer	Yes	Yes	Yes	
	SNMP	Yes	Yes	Yes	Fireware XTM supports SNMP v3 and the ability to send traps on all devices. Fireware XTM includes new system MIBs.
	Advanced log message options	No	Yes	Yes	
	Event Notifications	No	Yes	Yes	In Fireware XTM, an event must occur before you can configure a custom event notification.
Reporting	Reports	Limited. Some report data available on the Security Services page.	Yes	Yes	

Fireware XTM with a Pro Upgrade

The features available with a Pro upgrade depend on the type and model of your Firebox or XTM device. Here is a summary of the features available with a Pro upgrade in Fireware XTM v11.

Feature	Core e-Series	Core/Peak e-Series and XTM 1050 (Pro)	Edge e-Series	Edge e-Series (Pro)
Multi-WAN Load Balancing		X		X
FireCluster		X		
VLANs	X	X	20 Max	50 Max
Dynamic Routing (OSPF and BGP)		X		
Policy-Based Routing		X		X
Server Load Balancing		X		
Multi-WAN Load Balancing		X		X