Fireware XTM v11.0.1

Release Notes for XTM 1050 and Firebox X Peak, Core, and Edge e-Series Appliances

Revision Date: 9/02/09

> ***Note*** The Fireware XTM v11.0.1 release resolves a number of problems found in the Fireware XTM v11.0 release, specifically for upgrades from previous versions of WatchGuard appliance software to the new Fireware XTM OS. For a list of issues fixed in this release, see the Resolved Issues section later in these release notes.
> Because this release corrects problems relating to the upgrade to Fireware XTM, the Fireware XTM v11.0 software has been removed from the WatchGuard Software Downloads page and replaced with Fireware XTM v11.0.1.

Introduction to Fireware XTM v11.0.x

WatchGuard is pleased to release Fireware XTM v11 OS for the Firebox X Edge, Core, and Peak e-Series and 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 - 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 or Active/Passive configuration 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 to devices managed by a WatchGuard Management Server and works with either local or Active Directory user names and groups.
- Edge users can now download and use the full WSM suite of management applications
- 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 TCP-UDP, HTTP, or HTTPS 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:

- The Web UI no longer allows multiple read-write administration sessions at the same time
- 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
- Ability to use Mobile VPN with a dynamically addressed external interface without using DynDNS
- Support for metrics on static routes
- Scheduled reboot option now available for all Firebox devices
- Improved reliability of traffic handling on network interface 4-7
- Some features that previously required a "Pro" upgrade have become standard in Fireware XTM. These features include traffic management, QoS, and support for third-party VPN certificates.

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.
- The required hardware and software components as shown in the Systems Requirements table below.
- An active LiveSecurity subscription.
- 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.
- Documentation for this product is available at www.watchguard.com/help/documentation

System Requirements

	If you have WatchGuard System Manager client software only installed	**If you install WatchGuard System Manager and WatchGuard Server software**	**Fireware XTM Web UI**
Operating System	Windows Vista (32-bit), XP SP2, or Windows Server 2003 *You can use 64-bit Windows operating systems that support 32-bit applications	Windows Vista (32-bit), XP SP2, or Windows Server 2003 *You can use 64-bit Windows operating systems that support 32-bit applications	N/A
Browser	IE 6, IE 7, Firefox v3, Firefox v3.5	IE 6, IE 7, Firefox v3.0, Firefox v3.5	IE 7, Firefox v3.x
Minimum CPU	Intel Pentium IV 1GHz	Intel Pentium IV 2GHz	N/A
Minimum Memory	1 GB	2 GB	N/A
Minimum Available Disk Space	250 MB	1 GB	N/A

For information on the system requirements for Mobile VPN client software and Single Sign-on software, see the product help system.

Downloading Software

1. Go to the LiveSecurity web site's Software Downloads page at http://www.watchguard.com/archive/softwarecenter.asp
2. Log in to the LiveSecurity web site. Then, select the product line you use and look for the Fireware XTM software download section.

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` - Use this file to install WatchGuard System Manager v11.0.
- `WSM11_0_1.exe` - Use this file to upgrade WatchGuard System Manager from v11.0 to v11.0.1. This is a partial installer. You must have WSM v11.0 installed before you can install this file.

Select the correct Fireware XTM OS image for your hardware.

XTM 1050

- `XTM_OS_1050_11_0_1.exe`

Firebox X Core or Peak e-Series

- `XTM_OS_Core_Peak_11_0_1.exe`

If you want to downgrade a Firebox X Core or Peak e-Series from Fireware XTM v11.0.x to Fireware v10.x, you must download this file:

- `utm_core_peakdown2fw.zip`

Firebox X Edge e-Series

- `XTM_OS_Edge_11_0_1.exe` - Use this file to upgrade your Edge OS and configuration from v11.0 to v11.0.1
- `edge_11_0_1.exe` - Use this file to upgrade your Edge OS and configuration from v10.2.9 or higher to Fireware XTM.
- `XTM_edge_11.0_1.zip` - Use this file to upgrade your Edge OS from v10.2.9 or higher to Fireware XTM. No configuration conversion is possible if you use this file.

There are two files available for download if you use Single Sign-on:

- WG-Authentication-Gateway.exe (SSO Agent software - required for Single Sign-on)
- WG-Authentication-Client.msi (SSO Client software - optional)

For information about how to install and set up Single Sign-on, see the product documentation.

Upgrade from Fireware XTM v11.0 to v11.0.1

Before you upgrade from Fireware XTM v11.0 to Fireware XTM v11.0.1, go to the WatchGuard Software Downloads Center. Download and save the file that matches the WatchGuard device you want to upgrade. You can use Policy Manager or the Web UI to complete the upgrade procedure.

From the Web UI:

1. On your management computer, launch the OS executable file you downloaded from the WatchGuard Software Downloads Center. This installation extracts an upgrade file called `utm_[Firebox_model].sysa-dl` to the default location of `C:\Program Files\Common files\WatchGuard\resources\FirewareXTM\11.0\[Firebox_model].`
2. Connect to your Firebox with the Web UI and select **System > Upgrade OS**.
3. Browse to the location of the `utm_[Firebox_model].sysa-dl` file from Step 1 and click **Upgrade**.

From Policy Manager:

1. On your management computer, launch the OS executable file you downloaded from the WatchGuard Software Downloads Center. This installation extracts an upgrade file called `utm_[Firebox_model].sysa-dl` to the default location of `C:\Program Files\Common files\WatchGuard\resources\FirewareXTM\11.0\[Firebox_model].`
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_[Firebox_model].sysa-dl` file from Step 1.

Installation and Upgrade Instructions for Firebox X Edge v10.2.9 or higher

Before you install Fireware XTM v11.0.1 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.
>
> Any Edge devices that are centrally managed with a WatchGuard Management Server must be updated individually using the process in these release notes. You cannot use the Scheduled Firmware Updates feature to update a device from Edge v10.x to Fireware XTM v11.

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 v11.0.x. To upgrade your Edge, connect to your Edge from a Windows-based 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 (see the specific instructions below for more information).

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. If you do not use the wizard (i.e. if you update directly from the v10.2.9 or higher web interface using the "sysa-dl" file), your configuration is not converted and your Edge reverts to its default configuration when the upgrade to Fireware XTM is complete.

> ***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 it has been successfully updated, you must connect to the Edge with this URL:
> *https://<IP address of your Edge>:8080*
>
> ***Note*** The default credentials for the Edge are: admin/readwrite and status/readonly. After you upgrade your Edge to Fireware XTM, you must use the user name "admin" when you want to log in to the Edge with read/write privileges.

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 from a local Windows computer:

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_1.exe` file you downloaded from the software download site. The Firebox X Edge Update Wizard starts.
3. Use the Firebox X Edge Update Wizard to load Fireware XTM v11.0.1 on your Edge and convert your configuration file to v11.0.1. This upgrade can take as much as 10 minutes. Do not disconnect the power to your Edge during the upgrade.
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 use WSM and Policy Manager with your Edge, you must install WSM software. To install WSM, download the `WSM11s.exe` and the `WSM11_0_1.exe` files from the software download site.

To upgrade your Firebox X Edge from v10.2.9 or higher to Fireware XTM v11 from a local non-Windows computer:

> ***Note*** If you upgrade your Edge to Fireware XTM from a non-Windows-based computer or from any computer using the XTM_edge_11_0_1.zip file, your Edge configuration will be reset to its factory default settings when the upgrade is complete.

1. Connect to your Edge System Status page and select **Administration > Backup** to back up your existing Edge configuration file.
2. Decompress the `XTM_edge_11_0_1.zip` file you downloaded from the software download site.
3. On the System Status page, click **Update**.
4. Click **Browse**. Find and select the `utm_edge.sysa-dl` file, then click **Open**.
5. Click **Update**. To complete the installation, you must restart the Firebox X Edge. When the update is complete the System Status page shows Fireware XTM v11_0_1.

To upgrade your Firebox X Edge from v10.2.9 or higher to Fireware XTM v11 from a Windows computer on the external network:

To upgrade your Edge from a computer on the external network, you can use the same instructions as for a local Windows computer, except you must know:

- Before you try to upgrade the Edge, the Edge must be configured to allow WatchGuard System Manager (WSM) access. To enable WSM access, go to **Administration > WSM Access**.
- The Update Wizard prompts you for a WSM Access passphrase. The WSM Access passphrase is the configuration passphrase you set when you enable WSM access on the Edge.
- The upgrade can take as much as 20 minutes to complete.
- When the upgrade is complete, you can connect to the Edge from the external network only with WatchGuard System Manager or the CLI. To enable external connections from the Web UI, you must edit the WatchGuard Web UI policy with Policy Manager or the CLI.

Downgrade Firebox X Edge e-Series from Fireware XTM v11 to v10.2.9 or higher

Before you downgrade a Firebox X Edge e-Series from Fireware XTM v11 to Firebox X Edge v10.2.9 or higher, 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 can 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.
   After the downgrade, make sure to use the correct URL to connect to the Edge device (a URL that does not specify port 8080).
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 v10.2.x or higher

Before you install the WSM and Fireware XTM v11 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.x or higher installed on your Firebox.

Upgrade your Firebox X Core or Peak e-Series from Fireware to Fireware XTM v11.0.x

1. We strongly advise you to back up your current Fireware v10.2.x or higher 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 any WatchGuard servers, 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. Launch `WSM11_0_1.exe` and use the on-screen procedure to install the software. When you run the WSM v11.0.1 install program, select the options to install client software and the appropriate server software.
6. After the `WSM11_0_1.exe` install program is complete, launch `XTM_OS_Core_Peak_11_0_1.exe` and use the on-screen procedure to install the software.

7. 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**.
8. Launch Policy Manager. Click **Yes** when prompted to upgrade to v11.
9. Click **Yes** to convert the configuration file to v11.
10. From Policy Manager, select **File > Upgrade**.
11. When the **Save** dialog box appears, click **Save**. Click **Yes** to save the file to your management computer.
12. When the Upgrade dialog box appears, type your configuration passphrase and click **OK**.
13. 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.
14. Click **OK**.
15. Click **Yes** to upgrade your Firebox now.
16. Click **Yes** when asked to create a Firebox backup image.
17. 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_peakdown2fw.zip` 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 higher 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 the WatchGuard Software Downloads page. Download and save the `utm_core_peakdown2fw.zip` file and extract the contents to your WSM management computer. 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_peakdown2fw.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.

As with High Availability in Fireware v10.x, you cannot enable FireCluster if any external interface is configured to use DHCP or PPPoE.

Fireware/Edge v10.x Features Not Supported in Fireware XTM

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 Web UI no longer supports multiple read-write administration sessions. The second user who tries to establish a read-write administrator connection to a Firebox is denied.
- 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.
- Fireware XTM v11.0 does not include the ability to create a BOVPN tunnel that is specific to a port and protocol, or the ability to select multiple tunnel routes in a tunnel to be grouped into one Phase 2 Security Association. Fireware XTM 11 always creates one individual Phase 2 SA for each tunnel route in a tunnel.
- 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.
- This release does not include a localized user interface or localized documentation.

Resolved Issues

The Fireware XTM v11.0.1 release resolves a number of problems found in the Fireware XTM v11.0 release, specifically for upgrades from previous versions of WatchGuard appliance software to the new Fireware XTM OS.

- Automatic Gateway AV updates on the XTM 1050 now work correctly. [39878]
- Incoming connections that use a Static NAT rule in the To field of the policy no longer fail when your configuration also contains a matching 1-to-1 NAT rule. [39895]
- When you upgrade your Firebox X Edge e-Series to Fireware XTM, Dynamic NAT is now enabled for any non-RFC1918 addresses on the trusted or optional interface. [39919]
- Active Directory and LDAP authentication are now correctly enabled when you upgrade from v10.2.x to v11 and do not save the configuration to your device again. [39937]
- The Firebox X Edge MAC address override feature is now correctly converted during the Fireware XTM upgrade. [39950]
- You can now correctly add multiple managed BOVPN tunnels and gateways after you upgrade to Fireware XTM. [39958]
- After you upgrade a Firebox X Edge e-Series from v10.2.9 or higher, PFS is no longer disabled in the BOVPN tunnel settings. [39898]
- WebBlocker on a Firebox X Edge e-Series no longer shows the log message "http-proxy failed to send urif request to 'default'" and stops working after you upgrade to Fireware XTM. [39913]
- A problem that caused the Firebox to crash with log messages that include the text "webblocker@0x08048000" has been fixed. [39741]
- An issue that caused WebBlocker to stop working on Firebox X Core/Peak e-Series devices because of invalid WebBlocker exceptions after an upgrade to Fireware XTM has been fixed. [39892]
- WebBlocker no longer stops working correctly on a Firebox X Edge e-Series after you upgrade from v10.2.9 or higher if a custom WebBlocker server URL was used. [40004]

Known Issues and Limitations

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

General

- The minimum recommended 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]
- When you use **Policy Manager > File > Backup** or **Restore** features, the process can take a long time but does complete successfully. [35450]

Upgrade Issues

- After you upgrade a Firebox X Edge, it is important to know that you must use the user name "admin" when you want read/write access to the Edge. In previous releases of Edge appliance software, you could use a name other than "admin" in your administrative credentials, but this is no

longer possible in Fireware XTM. You must log in to the Edge with the user name "admin" and the read/write passphrase you set during the upgrade.

- 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 during the configuration upgrade. You must edit your Phase 2 encryption setting manually when the upgrade is complete to select an appropriate encryption setting.
- If you have special characters (, ;) in the policy names of your v10.x configuration, you must remove them from your policy names after you upgrade to Fireware XTM v11 so that reporting and monitoring operate correctly. [36577]
- In WSM version 10.x, you could create a Traffic Management action that set both incoming and outgoing traffic bandwidth for an external interface. This action could operate on a policy that managed traffic to and from a trusted network. To reproduce this feature in Fireware XTM v11.0, you must create a Traffic Management action that sets the maximum upload speed on the external interface and the maximum download speed on the trusted interface.
- Fireware XTM includes a new standard TFTP packet filter option. If your v10.2.x configuration file had a custom packet filter named "TFTP," you cannot save changes to your configuration after your upgrade until you delete your custom packet filter and move the policy configuration to a standard TFTP policy template. [39817]
- The Firebox X Edge **Require user authentication** and **Trusted Hosts** features do not exist in Fireware XTM, because of the increased granularity available when you configure policies for Edge users. During the Edge upgrade, the users are added to a local group called *Local-Users*. If you previously had **Require user authentication** enabled, you must use this group in your policies to enforce user authentication. The **Trusted Hosts** feature is no longer necessary.
- After you upgrade to Fireware XTM, the GMT time zone is not correctly set on the Firebox. It may be off by one hour. [39984]
- When you upgrade a Firebox X Edge to Fireware XTM v11.0.x, the PFS settings in your VPN tunnels are not correctly converted. You must check the PFS settings in your VPN tunnels after you upgrade. [39898]

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]
- If you restore a backup image to a managed client device managed by a Management Server, it is possible that the shared secret becomes out of sync.

  Workaround:
  Connect to the Management Server from WSM. Select the managed device and select **Update Device**. Select the radio button **Reset server configuration (IP address/ Hostname, shared secret)**.

- 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 before you start the uninstall WSM. You can then uninstall WatchGuard System Manager successfully.

Web UI

- The Fireware XTM Web UI does **not** support the configuration of some features. These features include:
  - FireCluster
  - Full proxy configuration options
  - The editing of static NAT rules
  - Manual policy precedence
  - Certificate export
  - You cannot enable diagnostic logging or change diagnostic log levels
  - You cannot turn on or off notification of BOVPN events
  - You cannot add or remove static ARP entries to the device ARP table
  - You cannot save a device configuration file to your local computer
  - You cannot get the encrypted Mobile VPN with IPSec end-user configuration profile, known as the `.wgx` file. The Web UI generates only a plain-text version of the end-user configuration profile, with file extension `.ini`.
  - You cannot edit the name of a policy, use a custom address in a policy, or use *Host Name (DNS lookup)* to add an IP address to a policy.
- You cannot use the Web UI to configure a DNS server for the DHCP settings of a wireless guest account. You must use Policy Manager or the CLI to add the DNS server. [39980]
- If you configure a policy in the Web UI with a status of **Disabled**, then open Policy Manager and make a change to the same policy, the action assigned to the policy when it denies packets is changed to **Send TCP RST**. [34118]
- If you use the Web UI to edit an existing proxy policy that has alarm settings enabled, the alarm settings may be disabled when you save your configuration. [38585]
- You cannot create read-only Mobile VPN with IPSec configuration files with the Web UI. [39176]

Command Line Interface (CLI)

- The CLI does not support the configuration of some features:
  - You cannot add or edit a proxy action.
  - You cannot get the encrypted Mobile VPN with IPSec end-user configuration profile, known as the `.wgx` file. The CLI generates only a plain-text version of the end-user configuration profile, with file extension `.ini`.
- The CLI performs minimal input validation for many commands.

Networking

- External interfaces configured with dynamic IP addresses may not respond correctly to ping requests. [39870]

- You cannot correctly add multicast addresses in a policy with Policy Manager or the Web UI. If you must use a multicast address in a policy, you must use the CLI to add the address. [39947, 39948]
- You must reboot your Firebox after you enable the MAC access control list or add a new MAC address before the change takes effect. [39987]
- You must make sure that any disabled network interfaces do not have the same IP address as any active network interface or routing problems can occur. [37807]
- If you enable the MAC/ IP binding feature by clicking the **Only allow traffic sent from or to these MAC/IP addresses** check box but do not add any entries to the table, the MAC/IP binding feature does not become active. This is to help make sure administrators do not accidently block themselves from their own Firebox. [36934]
- The option to release or renew a DHCP lease manually when the external interface is configured to use DHCP is missing in this release. [37478]
- Any network interfaces that are part of a bridge configuration disconnect and re-connect automatically when you save a configuration from a computer on the bridge network that includes configuration changes to a network interface. [39474]
- If you enable a network interface and change the **Interface Name (Alias)** at the same time you enable the interface, the interface does not become active until you reboot the Firebox. [39815]
- When you configure policy based routing for a VLAN that is configured on an external interface, Policy Manager may not show policy based routing correctly. [39491]
- 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]
- The MAC Address Override feature is not available on a Firebox X Edge that has a wireless interfaced configured as an external interface. [38241]

FireCluster

- When you have an active/active FireCluster and use the WebBlocker Override feature, you may be prompted to enter your override password twice. [39263]
- Every network interface enabled in a FireCluster is automatically monitored by FireCluster. You must make sure that all enabled interfaces are physically connected to a network device.

- You cannot manage WatchGuard devices configured in a FireCluster through a branch office VPN tunnel. [39732]
- 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]
- FireCluster does not support dynamic routing.

WatchGuard Server Center

- If the WatchGuard Server Center is open when you uninstall WSM, you see multiple warning messages to close the application, instead of just a single warning. [36901]

Management Server

- You cannot log in to the Management Server if you have configured a managed device that has a device name that is the same as a user name configured with an "administrator" role on the Management Server. [39692]

Logging and Reporting

- LogViewer can freeze if you move the scroll bar very quickly. [39461]
- The LogViewer *Search* function is very slow when you search a large log database. [38833]
- If you use an IIS 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]
- If you restart the PostgreSQL database, you must also restart the Report Server and the Log Server. [35063]
- You cannot use a v11.0 Report Server with a v10.x Log Server. You must upgrade both servers for reporting to work correctly. You can, however, use v11.0 Report Manager with a v10.x 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]
- When you enable the Authentication Redirect feature, it is possible that some users experience an "authentication redirect loop" in which they are asked to authenticate over and over again. If the user selects to log out, then logs back in, the problem goes away. [39739]
- The new feature 'Auto redirect users to authentication web page for authentication' captures traffic sent between networks on the same interface. [39737]

Workaround:

Add an HTTP policy or HTTPS policy that matches the flow of traffic for which you do not want the auto-redirect to occur.
Example: After you enable the redirect feature, you want users on a secondary network of an interface to get to an internal web page hosted on a server on the primary network of the interface without having to authenticate. You can add a policy with the secondary network IP address in the **From** field and the primary network IP address in the **To** field.

Proxies

- When you enable IPS in POP3 proxy policies and a file is blocked by IPS, the resulting notification does not include the file name for the blocked file. [38087]
- If you use WebBlocker and also have the **HTTP Proxy > Use external proxy caching server for HTTP traffic** check box enabled, the WebBlocker Override feature does not operate correctly. [39685]
- 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.

Security Subscriptions

- To optimize performance of web browsing on the Firebox X Edge e-Series, Gateway AntiVirus does not scan the following content types when used with the HTTP proxy: text/*, image/*, audio/*, video/*, application/javascript, application/x-javascript, and application/x-shockwave-flash. The content types appear in the HTTP-Client proxy action configuration for the Edge, but Gateway AV does not scan for these content types. All other content types, including executable files, are scanned.

Mobile VPN with SSL

- If you change your SSL configuration from **Routed Network Traffic** to **Bridge Network Traffic**, you must restart your Firebox before the configuration change occurs. [36159]
- The Macintosh SSL VPN client may not be able to connect to a Firebox when the authentication algorithm is set to SHA 256. [35724]
- If your Firebox X Edge e-Series is set to factory-default mode when you install Fireware XTM v11.0, the Mobile VPN client software is not available for download from the Edge. You must run the Fireware XTM v11.0 installation program again. [33539]

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.

- When you use the Web UI or CLI to configure Mobile VPN with IPSec user profiles, user groups with extended authentication may show incorrectly as Firebox Local Authentication groups. [39695]

Manual BOVPN

- The use of *Any* in a BOVPN tunnel route is changed in Fireware XTM. If a branch office VPN tunnel uses *Any* for the Local part of a tunnel route, Fireware XTM interprets this to mean network 0.0.0.0 and subnet mask 0.0.0.0 (in slash notation, 0.0.0.0/0). If the remote IPSec peer does not send 0.0.0.0/0 as its Phase 2 ID, Phase 2 negotiations fail. [40098]

Workaround:

Do not use *Any* for the Local or the Remote part of the tunnel route. Change the Local part of your tunnel route. Type the IP addresses of computers behind the Firebox that actually participate in the tunnel routing. Contact the administrator of the remote IPSec peer to determine what that device uses for the Remote part of its tunnel route (or the Remote part of its Phase 2 ID).

- If you use the Web UI to configure your BOVPN tunnel settings, and set the Phase 2 key expiration to "0", the value is incorrectly changed to "1". [39869]
- 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 both the Life-time and Life-size values to 0, the Firebox changes the rekey life-time to 8 hours. [37209]
- Fireware XTM v11.0 does not include the ability to configure inbound dynamic NAT in a branch office VPN tunnel. [40027]

Workaround:

You can configure your Firebox to match the functionality of the dynamic inbound NAT using per-policy dynamic NAT.

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. For information on how to start and use the CLI, see the *CLI Command Reference Guide*. You can download the CLI guide from the documentation web site at www.watchguard.com/help/documentation.

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or on the Web at http://www.watchguard.com/support. When you contact Technical Support, you must supply your registered Product Serial Number, LiveSecurity key or Partner ID.

	Phone Number
U.S. End Users	877.232.3531
International End Users	+1 206.613.0456
Authorized WatchGuard Resellers	206.521.8375

Feature/Product Matrix

This table shows a list of product features and the releases in which the feature is present. Only the most recent releases of Edge and Fireware are included. See the *Notes* column for important implementation differences.

Rows highlighted in blue represent new features in Fireware XTM v11.0. Rows highlighted in gray represent features supported in earlier releases that are no longer supported in Fireware XTM OS v11.0.

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 switch 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

Feature/Functional Area		Edge v10.x appliance software	Fireware v10.x appliance software	Fireware XTM OS	Notes on Fireware XTM Implementation
					time.
	Interface bridging	No	No	Yes	You can connect two or more 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

Feature/Functional Area		Edge v10.x appliance software	Fireware v10.x appliance software	Fireware XTM OS	Notes on Fireware XTM Implementation
					secondary network.
	DHCP Client	Yes	Yes	Yes	
	DHCP Server	Yes	Yes	Yes	
	DHCP Relay	Yes	Yes	Yes	
	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/Passive	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

Feature/Functional Area		Edge v10.x appliance software	Fireware v10.x appliance software	Fireware XTM OS	Notes on Fireware XTM Implementation
					Edge devices.
	HTTPS Proxy	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 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)	

Feature/Functional Area		Edge v10.x appliance software	Fireware v10.x appliance software	Fireware XTM OS	Notes on Fireware XTM Implementation
	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 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	

Feature/Functional Area		Edge v10.x appliance software	Fireware v10.x appliance software	Fireware XTM OS	Notes on Fireware XTM Implementation
	VASCO DIGIPASS	No	Yes	Yes	
	Single Sign-On	Yes	Yes	Yes	For Active Directory domains only.
	Browser-based user authentication	Yes	Yes	Yes	
	Trusted hosts	Yes	No	No	In Fireware XTM, you can control authentication on a per-policy basis.
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	

Feature/Functional Area		Edge v10.x appliance software	Fireware v10.x appliance software	Fireware XTM OS	Notes on Fireware XTM Implementation
	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	
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.

Feature/Functional Area		Edge v10.x appliance software	Fireware v10.x appliance software	Fireware XTM OS	Notes on Fireware XTM Implementation
	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.
	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.

Feature/Functional Area		Edge v10.x appliance software	Fireware v10.x appliance software	Fireware XTM OS	Notes on Fireware XTM Implementation
Policy Management	WSM Policy Manager for offline policy configuration	No	Yes	Yes	
	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	

Feature/Functional Area		Edge v10.x appliance software	Fireware v10.x appliance software	Fireware XTM OS	Notes on Fireware XTM Implementation
	Policy disposition	Allow, Deny, No Rule	Allow, Deny, Deny (Send Reset)	Allow, Deny, Deny (Send Reset)—with granular control of the reset message	
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 your Firebox model. All XTM 1050 and Firebox X Peak e-Series devices include a Pro upgrade. If you have a Firebox X Core or Edge e-Series, see the table below to understand the additional features available with a Fireware XTM Pro upgrade.

Feature	Firebox X Core e-Series (Pro)	Edge e-Series (Pro)
Multi-WAN Load Balancing	X	X
FireCluster	X	
VLANs	Same as standard	Up to 50 VLANs
Dynamic Routing (OSPF and BGP)	X	
Policy-Based Routing	X	X
Server Load Balancing	X	