Fireware XTM v11.2.3

Release Notes for XTM 2, 5, and 8 Series, XTM 1050, and Firebox X Peak, Core and Edge e-Series Appliances

Fireware XTM OS Build 267784
WatchGuard System Manager Build 267305

Release Notes Revision Date: April 20, 2010

Introduction

WatchGuard is pleased to announce the release of Fireware XTM v11.2.3. For those customers who upgrade from Fireware v10.x and previous, Fireware XTM v11.2.3 is a major feature release, with enhancements in virtually all areas of functionality. For those customers who upgrade from earlier releases of v11.x, the v11.2.3 release contains a number of defect fixes for issues reported by WatchGuard customers. This release includes improvements to FireCluster, proxies, Mobile VPN with SSL, and more.

See the Resolved Issues section below for a complete list of resolved issues.

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 or higher, a Firebox X Edge e-Series device running v10.2.9 or higher, or a WatchGuard XTM 1050 or XTM 8, 5, or 2 Series device. If this is a new device, make sure you follow the instructions in the Quick Start Guide that ships with your device before you try to upgrade to v11.2.3.
- The required hardware and software components as shown in the Systems Requirements table below.
- An active LiveSecurity subscription.
- Feature key for your Firebox or XTM device – If you upgrade your Firebox e-Series from an earlier version of Fireware or Edge appliance software, you can use your existing feature key.
- Updated online documentation system for this product is available at www.watchguard.com/help/documentation
- See the Resolved Issues section below for a complete list of resolved issues.

Fireware XTM and WSM v11.2.3 Operating System Compatibility

Fireware XTM v11.2.3 and WSM v11.2.3 Operating System Compatibility

WSM/ Fireware XTM Component	Microsoft Windows XP SP2 (32-bit)	Microsoft Windows Vista (32-bit)	Microsoft Windows Vista (64-bit)	Microsoft Windows 7 (32-bit & 64-bit)	Microsoft Windows Server 2003 (32-bit)	Microsoft Windows Server 2008* (32-bit & 64-bit)	Mac OS X v10.5 & v10.6
WatchGuard System Manager application	✓	✓	✓	✓	✓	✓	
Fireware XTM Web UI *Supported Browsers: IE 7, Firefox 3.x*	✓	✓	✓	✓	✓	✓	✓
WatchGuard Servers	✓	✓	✓	✓	✓	✓	
Single Sign-On Agent software	✓	✓			✓	✓	
Single Sign-On Client software	✓	✓	✓	✓	✓		
Mobile VPN with IPSec client software	✓	✓	✓	✓			
Mobile VPN with SSL client software	✓	✓	✓	✓			✓

Revised 4/8/10

**Microsoft Windows Server 2008 R2 is not supported.*

System Requirements

	If you have WatchGuard System Manager client software only installed	If you install WatchGuard System Manager and WatchGuard Server software
Minimum CPU	Intel Pentium IV 1GHz	Intel Pentium IV 2GHz
Minimum Memory	1 GB	2 GB
Minimum Available Disk Space	250 MB	1 GB

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.

WatchGuard System Manager

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

- `WSM11_2_3s.exe` - Use this file to upgrade WatchGuard System Manager from v10.2.x or v11.x to WSM v11.2.3.

Fireware XTM OS

Select the correct Fireware XTM OS image for your hardware.

If you have….	Select this Fireware XTM OS package
XTM 1050	`XTM_OS_1050_11_2_3.exe`
XTM 8 Series	`XTM_OS_XTM8_11_2_3.exe`
XTM 5 Series	`XTM_OS_XTM5_11_2_3.exe`
XTM 2 Series	`XTM_OS_XTM2_11_2_3.exe`
Firebox X Core or Peak e-Series	`XTM_OS_Core_Peak_11_2_3.exe` If you want to downgrade a Firebox X Core or Peak e-Series from Fireware XTM v11.2.1 to Fireware v10.2.x, you must download this file: `utm_core_peakdown2fw.zip`
Firebox X Edge e-Series	`XTM_OS_Edge_11_2_3.exe` - use this file to upgrade your OS and configuration from v11.0.x to v11.2.3. `edge_11_2_3.exe` - use this file to upgrade your OS and configuration from v10.2.9 or higher to Fireware XTM. `XTM_edge_11_2_3.zip` - use this file to upgrade your OS from v10.2.9 or higher to Fireware XTM. No configuration conversion is possible if you use this file. You can also use this file to upgrade from previous versions of XTM 11 to v11.2.3.

Single Sign-on Software

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.x to v11.2.3

Before you upgrade from Fireware XTM v11.x to Fireware XTM v11.2.3, 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.

> ***Note*** If you are currently running v11.0 or v11.0.1 on your Firebox X Edge e-Series, you must upgrade to v11.0.2 before you upgrade to v11.2.3 to avoid possible file system corruption. This issue does not apply to any other model.

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\11.2.3\[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\11.2.3\[Firebox_model]`
2. Open WatchGuard System Manager v11.2.3. 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.

Upgrade WatchGuard server software

It is not necessary to uninstall your v11.0.x server or client software when you update from v11.0.1 or higher to Fireware XTM v11.2.3. You can install the v11.2.3 server and client software on top of your existing installation to upgrade your WatchGuard software components.

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

Before you install Fireware XTM v11.2.3 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 v11.2.3.

Upgrade your Firebox X Edge e-Series v10.2.9 or higher to Fireware XTM v11.2.3

Your Edge must have Firebox X Edge v10.2.9 or higher installed before you can upgrade to Fireware XTM v11.2.3. 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.
>
> ***Note*** After you upgrade your Edge from v10.2.9 or higher to v11.2.3, you must enable each type of Mobile VPN that you used in your previous Edge configuration again. This includes Mobile VPN with IPSec, SSL, or PPTP.

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 with IPSec
- Mobile VPN with SSL
- Mobile VPN with PPTP
- SNMP
- Single Sign-On

To upgrade your Firebox X Edge from v10.2.9 or higher to Fireware XTM v11.2.3 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_2_3.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 v11.2.3 on your Edge and convert your configuration file to v11.2.3. 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 `WSM11_2_3s.exe` file from the software download site.

To upgrade your Firebox X Edge from v10.2.9 or higher to Fireware XTM v11.2.3 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_2_3.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_2_3.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_2.

To upgrade your Firebox X Edge from v10.2.9 or higher to Fireware XTM v11.2.3 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 v11.2.3 to v10.2.9

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 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 e-Series with Fireware v10.2.x

Before you install the WSM and Fireware XTM v11.2.3 software, read the information in the Known Issues section below.

> ***Note*** Before you upgrade a new Firebox X Core or Peak e-Series to Fireware XTM v11.x, you must first run the v10.2.x Quick Setup Wizard. After the basic v10.2.x. configuration has been saved to your Firebox, use the upgrade instructions below to upgrade to Fireware XTM v11.x.

> ***Note*** If your Firebox X Core or Peak e-Series device uses a Fireware version older than v10.2, you must first upgrade your Firebox to Fireware v10.2.x before you can upgrade to Fireware XTM v11.2.1.

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 v10.2.x or earlier 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** to uninstall your previous version of WSM. When the WSM installer starts, select the option to **Modify current installation by adding or removing components** and click **Next**. Clear the **Server Software** check box and, if you use any WatchGuard servers, select **No** when asked if you want to delete server configuration files from these servers. Make sure that you restart your computer to complete the uninstall process.
4. Launch `WSM11_2_3s.exe` and use the on-screen procedure to install the software. When you run the WSM v11.2 installation program, select the options to install WSM client software and the appropriate WSM server software.
5. After the `WSM11_2_3s.exe` install program is complete, launch `XTM_OS_Core_Peak_11_2_3.exe` and use the on-screen procedure to install the Firebox XTM software image.
6. Open WSM v11.2.3 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 v11.2.3.
8. Click **Yes** to convert the configuration file to v11.2.3.
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\11.2.3\Core_Peak\ FW110203BNNNNNN.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 v11.2.3 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.x. 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.x. 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.x, or install any released v10.2.x operating system before you perform another upgrade to v11.x.

Upgrade HA to FireCluster

WSM v11.x 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.

As soon as the second device is upgraded, 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.

Mobile VPN Client Software

With Fireware XTM v11.2.3, WatchGuard is releasing a new Mobile VPN with IPSec client, as well as new Mobile VPN with SSL clients.

Mobile VPN with IPSec

For more information, see the Mobile VPN with IPSec v11.2.3 release notes available on the Software Downloads page with the client download.

Mobile VPN with SSL client for Windows and Mac

The v11.2.3 Mobile VPN with SSL client is integrated into the Fireware XTM v11.2.3 OS. When an SSL client computer running an earlier version of the client software connects to a Firebox running v11.2.3, the user sees a prompt to upgrade the SSL client version to 5.4 for windows and 5.1 for Mac. Select **Yes** to upgrade the Mobile VPN client version to v11.2.3.

There is a Known Issue for customers who upgrade from Fireware XTM v11.2.1 to v11.2.3. for v11.2.1 users, the upgrade process described above will fail. To upgrade the client software from v11.2.1 to v11.2.3, you have two options:

- Use your web browser to connect to https://<IP address of your Firebox or XTM device>/sslvpn.html. You can then download the new installer and install it manually.
- Download the client software from the Software Downloads page and email it to your users to install on their computers.

If you are running Fireware XTM, Mobile VPN with SSL continues to operate if the user chooses not to upgrade, however, the user does not receive the fixes available in the v11.2.3 Mobile VPN with SSL client. When you upgrade from Fireware or Edge OS to Fireware XTM, you must upgrade your Mobile VPN with SSL client.

Resolved Issues in Fireware XTM v11.2.3

The Fireware XTM v11.2.3 release resolves a number of problems found in earlier Fireware XTM v11.x releases.

Upgrade Issues

- The TCP-UDP proxy configuration IM and P2P settings are now correctly converted during an upgrade from Fireware v10.x. [41949]
- CSRs (certificate signing requests) and private keys are now removed during an upgrade from Fireware v10.x. [39894]
- A custom proxy deny message no longer causes device lockup and problems with saving the configuration after an upgrade. [42507]
- After an upgrade of a managed device from Fireware v10.2.x, the Management Server no longer fails with error: "Element 'unknown': This element is not expected" when you try to add the upgraded device. [41978]
- Drop-in mode now operates correctly after an upgrade from Fireware v10.x. [41512]
- Mobile VPN with SSL Active Directory authentication requests are now correctly processed through a BOVPN tunnel after an upgrade from Fireware v10.x. [41716]
- NTP and DNS requests now operate correctly through a BOVPN tunnel after an upgrade from Fireware v10.x. [41991]
- An upgrade from Fireware XTM v11.1 to Fireware XTM v11.2.3 no longer creates pending SSLVPN certificates that cause Mobile VPN with SSL connects to fail. [42586]

General

- When you start a Firebox X Core or Peak e-Series appliance in recovery mode, the LCD display now correctly displays the "Recovery Mode" message. [43590]
- For Firebox X Edge models that limit the maximum number of IP addresses with outbound access, the IP addresses with outbound access are automatically timed out once per hour. [42539]
- A UDP flood to port 0 no longer causes loss of the management connection to the device. [42665]
- Firebox X Edge e-Series devices now can forward DNS queries. [42709]
- On Firebox X Edge e-Series devices, the WINS server is no longer automatically set to the same IP address as the primary DNS server when no WINS server was configured. [41622]
- Firebox X Edge e-Series Wireless devices no longer fail to assign DHCP addresses to connected wireless clients. [42386]

Authentication

- The web server on the Firebox or XTM device now sends the full certificate chain when a third party certificate is used. [43295]

Branch Office VPN

- 1-to-1 NAT now operates correctly for a manual BOVPN tunnel. [42796]
- Dynamic NAT now works correctly for Branch Office VPN tunnel switching traffic. [43572]
- BOVPN failover now operates correctly between a Firebox that uses Fireware v10.x and a Firebox or XTM device that use Fireware 11.2.3. [42316]
- Managed BOVPN tunnels no longer fail on an XTM 1050 active/passive FireCluster. [43370]
- If the remote side of a branch office VPN tunnel is configured with multiple WANs and the local side is configured to use PPPoE, the VPN traffic from the remote side no longer stops if the PPPoE dynamic IP address is changed on the local side [42669]
- The iked process no longer crashes after a WAN failover when a large number of BOVPN tunnels cannot be established. [43592]
- BOVPN kernel log messages "kernel esp_input:" no longer appear in the log files. [42712]

Mobile VPN with SSL

- The log message "wgagent Start tag expected, '<' not found" no longer appears when passing SSLVPN traffic. [42220]
- Mobile VPN with SSL and Mobile VPN with PPTP now operate correctly on an XTM 505 device. [42218]
- A dash (-) in an Active Directory password no longer causes Mobile VPN with SSL connections to fail. [43663]
- For an upgrade of the Mobile VPN with SSL client from v10.x to v11, the upgrade process now displays a message to indicate that the upgrade was successful. [40715]
- Mobile VPN with SSL now supports SecurID authentication new pin mode. [40828]
- The Mobile VPN with SSL client no longer crashes on Snow Leopard (Mac OS X 10.6.2). [42548]

Mobile VPN with IPSec

- The "§" symbol is now supported in Mobile VPN with IPSec passphrases when you use Active Directory authentication. [41884]

Networking

- A configuration with a large number of VLANs, all with DHCP enabled, no longer causes a stack trace to appear in Traffic Monitor. [42620]
- An incoming PPTP policy with 1-to-1 or static NAT no longer causes PPTP sessions to disconnect. [42204]
- A Traffic Management action to set the maximum bandwidth on the Trusted interface no longer limits the maximum bandwidth on the External interface. [42760]

WatchGuard System Manager

- Policy Manager now opens when the Status password contains a space. [42823]

- WatchGuard System Manager can now manage a device that contains "&" in the **System > Device Configuration** settings. [41551]

Firebox System Manager (FSM)

- The Traffic Meter on the FSM Front Panel now uses the correct scale for the device model. [42870]
- Traffic Monitor no longer displays a refresh error after a FireCluster failover of the cluster master. [42775]
- FSM no longer incorrectly shows GMT Summer Time on the Front Panel and in log files. [43812]
- FSM Status Report now shows the bridge MAC address table. [40977]
- Firebox System Manager no longer disconnects when you open the FSM Status Report. [43355]
- Branch office VPN routes now appear in the FSM Status Report. [41604]
- Mobile VPN with SSL tunnels now correctly appear on the FSM Front Panel when your Firebox or XTM is configured to bridge VPN traffic. [42663]

Web UI

- You can now add external VLAN interfaces to a policy-based routing configuration from the Fireware XTM Web UI. [42308]
- The Web UI now correctly stops you from using non-ASCII backup image passwords, which are not allowed in Policy Manager. [42043]

Quarantine Server

- You can now successfully delete and forward selected email from the Email Quarantine report. [42885]
- The date and time now appear correctly in the Email Quarantine report when viewed from an Italian client OS. [43721]

Log Server

- Logging for FireCluster no longer fails after you upgrade to Fireware to Fireware XTM v11.x. [42892]
- The Log Collector process no longer hangs or crashes when many devices are connected with a high rate of incoming log messages. [43631]
- You can now successfully back up a Log Server to a remote computer. [42892]

Report Server

- Report Server can now resolve host names. [42725]
- The data on the Gateway Antivirus reports now matches the data for Gateway AV in Firebox System Manager. [40940]
- Report Server now operates correctly when your admin passphrase has a special character in it. [42652]
- The User Authentication Report now generates correctly and for the appropriate time period. [43275]

FireCluster

- With Fireware v11.2.3, the way MAC addresses are assigned for an active/passive FireCluster has changed. After you upgrade an active/passive FireCluster to v11.2.3, it could be necessary to flush the ARP cache of connected network switches or routers to update the MAC address. Active/passive FireCluster now uses a virtual MAC address to give faster cluster member failover.
- An active/passive FireCluster no longer stops passing packets after a reboot. [42792]
- You can now connect to FireCluster management IP addresses from a different subnet. [43931]
- Security subscriptions no longer stop working when a passive device in an active/passive FireCluster has expired licenses. [41717]
- spamBlocker now scores spam on an active/passive failover if the device in passive mode does not have an active spamBlocker feature key. [41694]
- Signatures now sync correctly when a cluster member joins an active/active FireCluster. [42717]
- The devices in an active/passive FireCluster no longer take a very long time to boot. [43368]
- The backup member of a FireCluster now correctly becomes active after a failover. [41996]

Proxies

- The WebBlocker process no longer crashes when you save changes to a WebBlocker action. [42074]
- The log files for customers who use an active/passive FireCluster no longer fill up with log messages that refer to "kernel SM: ACK transmit failed". [42869]
- A problem that caused an "eip: 0xb7826e2d" CFM stack trace on the XTM 1050 has been resolved. [43657]
- The HTTPS proxy now returns a complete and valid chain of trust, including all intermediate CAs. [42661]
- Certificates are now handled correctly when you use the HTTPS proxy to protect an HTTPS server. [42229]
- A problem that caused HTML and JavaScript to display as garbled text during the download of a web page has been resolved. [42764]
- 1-to-1 NAT traffic is no longer blocked as unhandled external packets because of a corrupt SMTP proxy policy. [41271]
- A problem that caused a process to cache when the SIP proxy was enabled has been resolved. [41127]
- Proxy diagnostic log messages no longer multiple copies of the incorrect log message "`unable to parse license info`". [42484]
- Spam exceptions are no longer blocked by spamBlocker when BDAT/Chunking is enabled after you upgrade from v11.1 to v11.2. [42680]

- The Gateway AV and IPS version information is now updated correctly after a Gateway AV or IPS update. [42687, 42188, 43234]
- Gateway AV now correctly detects and blocks .js files as viruses. [42509]

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 v11.2 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.

Known Issues and Limitations

These are known issues for Fireware XTM v11.2.3 and all management applications. Where available, we include a way to work around the issue.

General

- To power off an XTM 5 Series device, you must press and hold the rear power switch for 4-5 seconds. [42459]
- On an XTM 5 Series device, the link light for network interface 0 remains lit when the device is powered off using the rear power switch. [42388]
- For XTM 5 Series devices, Interface 0 does not support Auto-MDIX and does not automatically sense cable polarity.
- On an XTM 2 Series device, the link speed lights remain lit for network interfaces 3, 4, and 5 when the ports are disabled. [42713]
- 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 to its factory default settings. [30284]
- When you use the **Policy Manager > File > Backup** or **Restore** features, the process can take a long time but does complete successfully. [35450]
- Policy Manager opens the locally stored copy of your configuration, instead of the configuration from the device, when you use a status passphrase with a "-" character as the first character in the passphrase (for example: "-1234567"). [42616]

> **Workaround:**
>
> Do not use the "-" character as the first character in your status or configuration passphrase.

Upgrade Issues

- After you upgrade a Firebox X Edge from v10.2.x, it is important to know that you must use the user name "admin" when you want read/write access to the Edge. In versions older than v11.0 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.
- The disk space occupied by data in the Report Server database before you upgrade to v11.2.x is not freed until after the number of days specified in the **Keep reports on the Report Server** setting in your Report Server configuration. Because of this, the Report Server database consumes more disk space until this number of days pass.
- 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 v10.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.x, 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.
- 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.
- The DNS suffix and second DNS server entries are not converted when you upgrade from v10.2.x to v11.x on Firebox X Edge e-Series. [40774]

Workaround:

Add the DNS suffix and second DNS entries again after you upgrade to v11.x.

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 turn on or off notification of BOVPN events
  - You cannot add or remove static ARP entries to the device ARP table
  - 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.
- 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]
- You cannot use angle brackets "< or >" in the Admin or Status password or login fails. [40823]

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]

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.

Logging and Reporting

- You cannot use a v11.x Report Server with a v10.x Log Server. You must upgrade both servers for reporting to work correctly. You can, however, use v11.x Report Manager with a v10.x Report Server.

Multi-WAN

- When you enable the Multi-WAN **Immediate failback** option for WAN failover, some traffic may fail over gradually. [42363]

Networking

- You cannot bridge a wireless access point to an interface configured as trusted or optional if that network interface is already part of a bridge. [39603]
- The Web Setup Wizard can fail if your computer is directly connected to an XTM 2 Series device as a DHCP client when you start the Web Setup Wizard. This can occur because the computer cannot get an IP address quickly enough after the device reboots during the wizard. [42550]

Workaround:

1. If your computer is directly connected to the XTM 2 Series device during the Web Setup Wizard, use a static IP address on your computer.
2. Use a switch or hub between your computer and the XTM 2 Series device when you run the Web Setup Wizard.

- When a secondary network is configured for an XTM 2 Series device configured in Drop-In Mode, it can sometimes take a few minutes for computers that connect to the secondary network to appear in the ARP list of the XTM 2 Series. [42731]
- After you enable the MAC access control list or add a new MAC address, you must reboot your Firebox 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 with 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 v11.x. [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]
- 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]
- The dynamic routing of RIPv1 does not work. [40880]
- IPSec Pass-Through does not work when you configure static NAT for the IPSec traffic. [41249]
- When an IP address is added to the Temporary Blocked Site list by the administrator through the Firebox System Manager > Blocked Sites tab, the expiration time is constantly reset when traffic is received from the IP address. [42089]
- NAT loopback does not work together with Server Load Balancing. [41090]

Firebox X Edge e-Series Wireless

- When a Firebox X Edge e-Series is configured as both a wireless access point and as a Mobile VPN with SSL endpoint, the wireless connection does not work correctly if the SSL VPN address pool is configured on the same subnet as the wireless access point. [42429]
- 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.

- 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 in Firebox System Manager when you are connected to a passive FireCluster member. PPTP is only connected to the active Firebox when using an active/passive FireCluster. [36467]
  - FireCluster does not support dynamic routing. [39442]

Authentication

- The Active Directory search algorithm has changed in Fireware XTM. For Active Directory authentication to work correctly in Fireware XTM v11.x, the groups that your users are members of must be included in the Search Base you specify in the Active Directory authentication setup. In Fireware v10.2.x and earlier, it was necessary for only the user objects to be in the Search Base. [40482]

  Workaround:

  If the Search Base that you currently use contains user objects, but not the groups that the users are members of, make the Search Base broader. For example, use the root container dc=domain,dc=domain, as in dc=mycompany,dc=com.

- For the Authentication Redirect feature to operate correctly, 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 policies for port 80 and 443 are configured for user or user group authentication. [37241]

Single Sign-On

- User authentication may fail when you use the Single Sign-On agent if non-ASCII characters are used in group names or user names. [41883]

Proxies

- Skype is a new option in Application Blocker in Fireware XTM v11.2. Application Blocker can only block the initial login to Skype. It cannot block traffic for a Skype client that has previously logged in. If a user with a laptop logs in to Skype when the computer is not connected to your network, and then the user connects to your network while the Skype client is still active, Application Blocker cannot block the Skype traffic until the user exits and logs out of the Skype application.

- 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. Gateway AntiVirus also does not use code emulation capabilities of the AV engine on Firebox X Edge e-series appliances.

Certificates

- DSA algorithm-based digital certificates are not supported in this release. [38758]

Workaround:

Use RSA algorithm-based digital certificates.

Mobile VPN with PPTP

- If you use Mobile VPN with PPTP together with CryptoCard RADIUS, the PPTP connection fails when you authenticate. [42304]

Mobile VPN with SSL

- Users who try to upgrade their Mobile VPN with SSL client from Fireware XTM v11.2.1 to v11.2.3 (or any future version) will fail. The failure does not damage the v11.2.1 client installation. [43970]

Workaround:

To upgrade your Mobile VPN with SSL client from v11.2.1 to v11.2.3, use your web browser to connect to https://<IP address of a Firebox or XTM device>/sslvpn.html. You can then download and install the new client software. Or, you can download the client software from the Software Downloads page and email it your users to install on their computer.

- 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]
- When the Macintosh SSL VPN client disconnects or is stopped manually, the client disables the AirPort wireless adapter on the Mac. [39914]

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]

Branch Office VPN

- Mobile VPN with IPSec tunnel switching does not work if the virtual IP pool for the mobile users is the same as a trusted or optional network that routes through the branch office VPN tunnel. [40974]
- 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).

- 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]

Using the CLI

The Fireware XTM CLI (Command Line Interface) is fully supported for v11.x releases. 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

Resolved Issues in Fireware XTM v11.2.1 and v11.2.2

- It is no longer possible to save configuration changes to the Firebox or XTM device with the Escape key and the configuration passphrase. [42609]
- Per-policy and global NAT settings now apply correctly to IPSec traffic. [39366]
- This release includes improvements to the Single Sign-on agent software that affected customers with a large number (>1000) of Single Sign-on users. [42406, 42407, 42408]
- WatchGuard System Manager and Firebox System Manager connections no longer fail after you upgrade your device from Fireware v10.2.11 to Fireware XTM v11.x. [41806]
- Ping traffic through a branch office VPN tunnel configured to a Firebox or XTM device configured for multi-WAN is now encrypted correctly. [42617]
- The external IP address of a Firebox X Edge e-Series device is no longer counted as an active IP address in the Outbound Access List. [42581]
- The Firebox X Edge e-Series no longer includes VPN traffic in the results on the Outbound Access List. [42582]
- DHCP relay now works correctly with multiple VLANs. [42288]
- Firebox System Manager no longer fails with the error "`Missing data for XPATH /network/wan/failback_status/failback_status`" when connected through an active/passive FireCluster configured with multi-WAN. [42334]
- The Management Server now correctly handles Edge configuration templates that have properties with values longer than 1023 characters. [42630]
- The Fireware to Fireware XTM upgrade process now correctly upgrades Mobile VPN resource entries with zero route functionality enabled. [42216]
- This release resolves an issue that caused management connections to fail after several days of device uptime. [40768]

Proxies

- The H.323 ALG no longer drops a call when the call is on hold longer than the timeout setting. [40370]
- The H.323 ALG no longer times out when audio and video content is being sent between Polycom systems. [40377]
- The H.323 ALG no longer fails with kernel panic error (`EIP: 0060: [<380112c6>])` when dynamic NAT is not used. [40757]
- NetMeeting to NetMeeting connections configured to use the H.323 ALG no longer time out when audio and video content is being sent. [40692]
- Trusted phones configured to use the SIP ALG can now make correctly re-negotiate connections when a call is put on hold several times. [40447]

- The SIP ALG now correctly recognizes the hold signal and maintains audio and video content after a long hold period. [40100]
- The HTTP proxy now supports more possible characters in the customizable deny message. [42566]
- Multi-byte languages are now supported in SMTP notification messages. [38335]
- The SMTP proxy now correctly recognizes multi-byte attachment file names. [39559]
- You can now add user email addresses longer than 32 characters to the Quarantine Server. [42283]

Mobile User with SSL

- The Mobile VPN with SSL client upgrade no longer fails when the client is used with CryptoCard two-factor authentication. [42467]
- The **Force users to authenticate after a connection is lost** option now works correctly. [42470]
- You can now correctly save changes to the Mobile VPN with SSL Advanced configuration. [42426]

Web UI

- The Firebox X Edge Outbound Access List feature is now available for both wired and wireless devices. [42602]
- The Web UI can now correctly display third-party certificates. [41324]
- The HTTP proxy now includes configuration for Application Blocker in the Web UI. [40331]

WatchGuard Servers

- Symantec Backup Exec backups no longer fail because of an embedded "..\" in the registry keys of the WatchGuard server products. [40010]
- Report Manager now displays the correct counts for "bytes_in" and "bytes_out". [42628]
- Report Manager now correctly displays reports after you upgrade your device from Fireware v10.x to Fireware XTM. [42651]
- On-demand reports generated with the Reporting Web UI now correctly handle the date for non-English locales and generate without error. [42522]
- Report start and end dates that cross a month boundary are now handled correctly in the Reporting Web UI. [42547]
- The Reporting Web UI no longer gives an HTTP 403 error when the WSM Report Server is installed in a non-default location. [42552]
- It is no longer necessary to restart the Report Server and Log Server when you restart the PostgreSQL database. [35063]

Resolved Issues in Fireware XTM v11.2

Upgrade Issues

- The upgrade from a Firebox X Edge e-Series v10.2.9 or higher to Fireware XTM v11.2 no longer fails if a custom policy is used. [41704] [41809]
- When you upgrade a Firebox X Edge e-Series from v10.2.9 or higher to v11.2, the upgrade no longer fails if the alias **Wireless Guest Network** is used in the **From** field of a policy. [41098]
- This release resolves an issue that prevented the successful upgrade from Fireware v10.2.8 configured to use High Availability to Fireware XTM v11.x. [41908]
- It is no longer necessary to remove custom TFTP packet filter policies from your Fireware v10.2.x configuration before you upgrade to Fireware XTM. [39817]

General

- You can now schedule a weekly reboot of your Firebox or XTM device. [40860]
- This release resolves an OpenSSL TLS renegotiation vulnerability, CVE-2009-3555 TLS: MITM attacks via session renegotiation. [41353]
- This release resolve an issue that caused the Firebox to crash with a stack trace: `eip: c015217a free_block() crash`. [41853]
- WatchGuard Service Center now correctly uninstalls on 64bit Windows 2008 Server. [41275]

Authentication

- When you enable the **Authentication Settings > Limit users to a single login session** check box, you can now prevent a second login attempt from disconnecting the first authenticated session with the same user name. [38024]
- This release resolves a problem that caused the *admd* process to fail if a user that belonged to more than 10 groups authenticated to the Firebox. [40987]

Proxies

- The SMTP proxy no longer strips attachments from a Yahoo® mail account because of improper content type formats used by Yahoo. [41710]
- The HTTPS proxy now correctly matches Gmail® to the WebBlocker categories *Web-Based email* and *Chat*. [41607]
- FTP traffic no longer fails through an HTTP Proxy with a "line parsing error" when a caching proxy server is used. [41483]
- Microsoft® Outlook communication that uses RPC over HTTPS no longer fails when you have deep packet inspection enabled in your HTTPS proxy. [37503]
- When you use Deep Packet Inspection with the HTTPS proxy and the time it takes to download a file exceeds the HTTPS proxy action **Idle Timeout** setting, the file download no longer fails. [41289]

Subscription Services

- The WebBlocker Override feature now works on XTM 8 Series devices configured in Bridge Mode. [41321]

Wireless

- This release resolves a problem where the *networkd* process sometimes crashed and all wireless connections failed. [40418]
- WPA-PSK passphrases can now include as many as 63 characters. [40780]

Networking

- You can now use static NAT with PPPoE when you use IP addresses that are not part of the primary external network. [40506]
- The feature to block port and address space probes has been enhanced to improve the detection of slow port and IP scans. [41775]
- DHCP Relay now works correctly when sent through a Branch Office VPN on a Firebox or XTM device configured to use PPPoE. [41702]
- You can now schedule a time to automatically restart the PPPoE connection. [39624]
- SNMP traffic generated by a device on a trusted or optional interface now passes through the Firebox to an external network. [41399]
- If you edit a static MAC entry and then change the MAC address, the change now takes effect. [40738]

Multi-WAN

- When you change your multi-WAN configuration mode from *Failover* to *Routing Table*, the routing table is now correctly updated without the need for a reboot. [41696]
- This release resolves an issue that prevented multi-WAN Round Robin with equal weights to operate correctly with a Fireware XTM *Standard* license. [41695]
- When you use Multi-WAN together with Branch Office VPN, VPN tunnel traffic now routes through the correct external interface. [41971] [41953]

FireCluster

- Network traffic routed among interfaces is no longer disrupted when you use active/passive FireCluster. [41530]
- The *sessiond* process no longer crashes when you enable FireCluster. [41124]
- The subnet mask on the backup master management IP address is no longer automatically set to */8* or */16*. [41281]
- You can now manage WatchGuard devices configured in a FireCluster through a Branch Office VPN tunnel. [39732]
- When you configure an active/passive FireCluster, the Firebox now sends a GARP for 1-to-1 NAT IP addresses that are not configured as secondary network addresses on an external interface. [40688]
- IPSec Pass-through now works correctly with an active/passive FireCluster. [41373]

Branch Office VPN

- Fragmented traffic over a Branch Office VPN no longer fails when the external interface is configured as a VLAN. [41535]
- BOVPN Failover now completes when you disconnect the Ethernet cable from the primary external interface. [41677]
- The Firebox no longer locks up when there is a high volume of fragmented UDP packets sent over a branch office VPN tunnel configured to use AES encryption in phase 2. [41475] [41229]

Mobile VPN

- Proxy ARP is now enabled for the IP addresses assigned to Mobile VPN with SSL clients connected to the Firebox. [40989]
- The SSL VPN Client for Macintosh® now supports v10.6 (Snow Leopard). [40953]
- The Mobile VPN with IPSec v11.2 client correctly supports the use of certificates for authentication. [41464]
- If you have an underscore "_" in the group name, the Mobile VPN with IPSec connection now passes traffic correctly. [40858]
- If the PPTP client option, **Include Windows logon domain,** is selected, the PPTP connection to the Firebox now operates correctly. [40856]

Web UI

- You can now add a static NAT entry that uses a secondary external IP address. [41663]
- The option to configure diagnostic logging is now available in the Web UI. [39212]
- This release resolves an issue that caused the Web UI to display "`Code: 0 Error: 0`" when you add a branch office VPN gateway. [41286]
- This release resolves an issue that caused the Web UI to display "`Code: 0 Error: 0` when you configure Gateway AV or IPS. [41518]

Policy Manager

- The error `HTTP response code: 500` no longer occurs when you save your configuration multiple times in a short amount of time. [41266]

Firebox System Manager

- When you connect HostWatch to a Firebox that has many connections, HostWatch no longer shows a blank connection list. [40772] [41721]
- This release resolves an issue that caused a Java null pointer exception when the Front Panel display refreshes. [41156]
- The Security Subscriptions tab now correctly displays statistics if the feature key contains a combination of expired and active licenses. [41400]

Management Server

- You can now 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]
- The `Apache.exe` process no longer crashes when you apply a BOVPN managed policy with more than18 ports in the policy. [41395]

Centralized Management

- When you use a custom alias in a policy template, the alias no longer changes to *none* when the template is updated. [41272]

Log Server

- This release resolves an issue that caused the Windows Event log file to fill up with the error message: `Error (9235), database error: ERROR: invalid byte sequence for encoding.` [40983]
- The Log Server no longer fails to start if the partition on the hard drive selected for the Log Server become full. [40995]
- LogViewer no longer freezes if you move the scroll bar very quickly. [39461]

Certificates

- WSM connections no longer fail when you use third-party certificates for your web server. [41248]

Resolved Issues in Fireware XTM v11.1

General

- The WSM Quick Setup Wizard now allows you to enter a feature key that contains a model upgrade for Edge e-Series. [40405]
- Fireware XTM v11.1 resolves a cross site scripting vulnerability found in the web server used with the authentication applet. [40332]
- Fireware XTM v11.1 resolves a cross site scripting vulnerability found in the WatchGuard servers' Apache HTTP server implementation. [40581]
- The lighttpd version used by Fireware XTM has been upgraded to v1.4.22 to resolve several reported vulnerabilities. [38808]
- The ISC DHCP server version has been upgraded to v4.1.0p1 to resolve several reported vulnerabilities. [40032]
- HostWatch now shows VLAN traffic. [40401]
- You can now right-click in Firebox System Manager > Traffic Monitor to add an IP address to the blocked sites list. [40488]
- ServiceWatch now correctly displays bandwidth for auto-generated BOVPN policies created by the WatchGuard Management Server. [40364]

Authentication

- The Authentication redirect feature now works when you use a wireless guest network on the Firebox X Edge e-Series. [40029]
- This release resolves an issue that causes Active Directory authentication to fail with the following log message: `user="test1" domain=TESTQAWIN2K30.` [40786]

Proxies

- You can now enable notification for Application Blocker. [40422]
- Application Blocker has been enhanced to add support for Winny, a popular peer to peer application used in Japan. [35027]
- You can now unlock a file with an "&" in the file name with the `unlock.exe` utility. [40718]
- This release resolves several reported issues in which certain web applications did not work through the HTTP Proxy. [40293] [38121] [40392]
- This release resolves an issue that caused FTP proxy traffic to stop after a multi-WAN failover. [37965]

Subscription Services

- Subscription services now update when you use an internal HTTP proxy server. [40517]
- WebBlocker override now works on Firebox X e-Series devices configured in Bridge Mode. [39283]
- The Quarantine Server client now accepts *firstname.lastname@domain.com* email format. [39743]

Networking

- You can now use either Policy Manager or the Web UI to add multicast addresses in a policy. [39947, 39948]
- If you enable a network interface and change the **Interface Name (Alias)** at the same time you enable the interface, the interface now becomes active without the need for a reboot.[39815]
- When you use multi-WAN, DNS servers with static IP addresses on WAN 1 are now used even when other external interfaces use DNS servers from an ISP through PPPoE or DHCP. [40322]
- DHCP relay through a branch office VPN tunnel now works. [40844]
- You can now change the MTU of an external interface configured with PPPoE. [40705]
- The DHCP server now works when there are multiple VLANs in the configuration. [40556]
- Server Load Balancing now works when the internal server IP addresses are on different subnets. [41041]
- We have made enhancements to the Server Load Balancing server status detection mechanism. [40300] [40519]

- The Server Load Balancing Stickiness function has been improved to maintain a sticky connection state until the idle timeout is reached. [40297]
- Static MAC address binding now works when your device is configured in Bridge Mode. [40665]
- This release resolves an issue that prevented some Windows computers from getting an IP address via DHCP when your device is configured in Drop-In Mode. [40184]
- The Blocked Ports and Blocked Sites features now apply only to traffic on an external interface. [39918]

Multi-WAN

- Several multi-WAN issues related to PPPoE and branch office and Mobile VPN have been resolved. [40007]
- Multi-WAN now works when the source IP address for incoming traffic is on the same network subnet as one of the external interfaces of the Firebox. [41026]
- This release resolves an issue that caused the external interfaces to become inactive when you used multi-WAN configured in Round-robin mode. [40357]

FireCluster

- Firebox devices with a model upgrade in the feature key can now join a FireCluster. [39370]

Branch Office VPN

- The choice of **Any** has been removed from the Tunnel Route Settings Local and Remote drop-down menu. The Web UI now shows "any (0.0.0.0/0)". [40409]
- This release resolves an issue that caused the IKED process to crash and all IPSec tunnels to fail. [40442]

Mobile VPN

- The Windows SSL VPN client has been updated to support Window7 and Windows 64-bit operating systems. [39841]
- This release resolves an issue that caused SSL VPN to fail to connect after an upgrade from v10.2.x to v11.0.x. When this problem occurred, the SSL VPN client logs showed: `sslvpn State: initialization of prerequisites Debug.` [40408]
- This release resolves several reported vulnerabilities in the SSL VPN client for Mac. [40292]
- Mobile VPN with PPTP and SSL now continue to work when the LiveSecurity subscription is expired in your Firebox feature key. [41045]
- When you disconnect the Mobile VPN with SSL client from one Firebox and then connect to a different Firebox, the SSL VPN profile is now updated to show the new connection. [41052]
- The Mobile VPN with IPSec v11.1 client supports Windows 7 (32-bit and 64-bit) and contains additional bug fixes.

Web UI

- You can now export your device configuration with the Web UI. [35234]
- The Web UI now prevents the use of custom SSL VPN ports that conflict with ports used by the Firebox. [39382]

Policy Manager

- The Firebox no longer becomes unresponsive if you use more than 28 characters in a proxy policy name. [40679]
- The alias "Firebox" is now treated the same as other aliases the Firebox determines policy precedence. [38891]

Management Server

- When a Firebox is in Full Management Mode and you clear the **Enable TCP Syn Checking** check box, TCP Syn Checking is now correctly disabled. [40853]
- When a Firebox is under centralized management, an update from the WatchGuard Management Server no longer overwrites any blocked sites configured manually on the Firebox. [40312]
- You can now right-click on a device and add that device to a folder. [36077]
- The ability to schedule a reboot time is now available from the Management Server. [38230]
- You can now perform a mass update of managed devices to force all selected appliances to check for a configuration update. [36958]
- The Management Server now sorts the IPSec-action-list and abs-ipsec-action-list for tunnels created by the Management Server. The IPSec actions for Manual BOVPN tunnels are left in the order sorted by the user. Manual tunnels are always placed at the top of the list, followed by the sorted list of the tunnels created by the Management Server.
- For each firewall policy template in use, there is now a single firewall policy created in the appliance configuration. As an example, if you have three tunnels (to different endpoints) that all use the same firewall policy template, there is a single firewall policy with the attributes set in the template. If there are two firewall policy templates in use, then two firewall policies are created. [38877]

Report Server

- If you use an IIS server to serve published reports, you no longer get an error about missing files. [39319]

Log Server

- The performance of the LogViewer *Search* function has been improved in v11.1. To facilitate the performance improvements, a log database migration will occur when you upgrade from v11.0.x to v11.1. During the migration, all log messages generated for a particular device are not visible until the migration is finished. [38833]

Certificates

- You can now import a CRL in DER format into Firebox System Manager. [36643]

- This release resolves a memory leak that occurred when you used 3rd-party certificates on the Firebox and kept WatchGuard System Manager or Firebox System Manager connected. [41008]
- WatchGuard System Manager and Firebox System Manager no longer display the certificates status as valid even if a certificate is invalid. [40378]

Resolved Issues in Fireware XTM v11.0.2

General

- The Fireware XTM OS installer now installs SNMP MIB files in `C:\Documents and Settings\All Users\Shared WatchGuard\SNMP`. [40283]
- Time zones using GMT -1 now operate correctly. [39984]
- The on-demand report "Top Client by Send and Received" now runs correctly. [40652]
- The Quarantine Server **Email Notification** text box now allows more than 32 characters. [40339]
- Firebox System Manager no longer displays Trial Subscription Service licenses as "unlicensed." [40005]
- This release resolves an issue that caused incorrect time on the Firebox X Edge e-Series (up to 15 minutes a day). [40099]
- You can now enable logging for traffic sent from the Firebox. The new logging option is available in Policy Manager under **Setup > Logging > Diagnostic Log Level > Turn on logging of traffic sent by the Firebox itself**. [40066]

Authentication

- The Active Directory server optional settings now apply to Mobile VPN with IPSec clients. [33083]
- This release resolves an issue in which an Authentication Redirect loop occurred when the same user had multiple authenticated sessions to the Firebox from the same IP address and one of the sessions was terminated by the Firebox. [39739]
- When you use Active Directory authentication with *userPrincipalName* or *sAMAccountName* for the **Login Attribute** and a *Searching User* configured, the Firebox no longer allows authentication attempts to succeed with invalid usernames. [40386]

Proxies

- The `spamd` process no longer restarts when you make changes to your spamBlocker settings. [39893]

Networking

- 1-to-1 NAT configured from an optional network to an external network now works correctly. [40025]

- The ARP Spoof Attack threshold has been increased to prevent false detection of ARP spoof attacks from Linux servers using multiple NIC cards on the same subnet (also known as ARP flux). [40122]

Multi-WAN

- This release resolves an issue that caused the Firebox to reboot every 2 minutes when multi-WAN is configured in round-robin mode. [40038]
- This release resolves an issue that prevented an external interface from becoming active again after ping or TCP interface monitoring failed. [40682]
- Multi-WAN interfaces configured with dynamic IP addresses now respond correctly to ping packets and management connections. [39870]
- The Firebox no longer routes traffic out all external interfaces when you select only one external interface in your multi-WAN Routing Table configuration. [39968]
- The method to determine Multi-WAN sticky connections has been improved to look at both the destination IP address and the source IP address. [39970]
- This release resolves an issue that caused the WAN Fail Back button to appear in FSM even though the WAN failback had already occurred. [38722]
- When you configure multi-WAN interface monitoring by domain name, the Firebox now does a DNS lookup after the first failed TCP or ping probe. [40578]

FireCluster

- You can now connect to the Management IP address of the Backup Master Firebox or Passive Firebox from a trusted or optional interface when the Management IP address is on an external interface. [40372]
- When you configure an Active/Passive FireCluster, you no longer need to have active security subscriptions licenses on the Passive Firebox. [40096]

Branch Office VPN

- Fireware XTM now includes the ability to configure inbound dynamic NAT in a branch office VPN tunnel. [40027]
- You can now configure BOVPN tunnel Phase 2 encryption settings as "Null". [38176]
- The Web UI now allows you to configure BOVPN tunnel settings, and set the Phase 2 key expiration lifetime to "0". [39869]
- You can now enable 1-to-1 NAT for a BOVPN tunnel when the tunnel direction is set to incoming. [40103]

Mobile VPN

- When you use individual users in a Mobile VPN with IPSec policy, Fireware XTM no longer limits the connection to the first user in the policy. [40114]
- When the idle timeout is reached for a Mobile VPN connection, Fireware XTM now correctly disconnects the user. This allows the client to re-connect and pass traffic. This issue applies to Mobile VPN with PPTP, IPSec, and SSL. [40497] [40529]

- PPTP connections are no longer disconnected when you modify a static NAT configuration. [39774]

Web UI

- When a licensed feature is expired, the Web UI now shows the feature as expired instead of showing a negative number. [40537]
- You can now use the Web UI to configure a DNS server for the DHCP settings of a wireless guest account. [39980]
- You can now configure MAC Address Override for an external interface. [40012]

Policy Manager

- When you edit a Traffic Management action associated with a firewall policy, the selected Traffic Management action no longer resets to "Defaults (No Limits)". [39586]
- When you configure policy-based routing for a VLAN that is configured on an external interface, Policy Manager now shows the correct configuration. [39491]

Management Server

- When FireCluster is configured on a managed device and then disabled, the Management Server now correctly shows the device as not having FireCluster enabled. [39875]
- The Management Server Setup Wizard no longer imports the external secondary IP addresses. [40242]
- When a **Scheduled OS Update** is in process and the Management Server tries to update a remote device that is not available, the update now times out after 60 seconds to prevent delaying the rest of the device OS updates. [39771]
- The **Cleanup Tasks** option no longer removes tasks that are still active or in the scheduled state. [39874]
- The Scheduled Feature Key Synchronization wizard now remembers the previously selected devices. [39873]
- The Scheduled Feature Key Synchronization feature now shows only supported devices. [39872]
- When you drag a device onto a Policy Template to change its configuration mode from *basic management* to *full management*, a "Login Failure" error no longer occurs. [40108]
- When you use role-based administration, a user with *Device Monitor* privileges can no longer remove a managed BOVPN tunnel. [40236]
- When a managed device has never contacted the Management Server, the update status for that device now shows as "Pending" instead of "Complete (Jan 01, 1970 08:00:00)". [39786]

Upgrade from version 10.2.x Issues

- When you upgrade from Edge v10.2.9 or higher, custom policies are now correctly shown in the XTM Custom Folder. [40489]

- This release resolves an issue in which WatchGuard System Manager was not able to connect to a Firebox X Core or Peak e-Series device after you upgraded from v10.2.x to v11.0.1 when PPTP was enabled. [39981]

Resolved Issues in Fireware XTM v11.0.1

- 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]