



Fireware XTM v11.5.3 Release Notes

Supported Devices	XTM 2, 3, 5, and 8 Series XTM 1050, XTM 2050
Fireware XTM OS Update 1 Build	341451
WatchGuard System Manager Build	339420
Revision Date	26 June 2012

Introduction

Note On May 21, 2012, we released an update for Fireware XTM v11.5.3, named Fireware XTM OS v11.5.3 Update 1. This update replaced the original XTM v11.5.3 file on our XTM Software Downloads pages. This update is for appliance software only, and is intended to improve stability and provide additional key bug fixes for all XTM customers. For a list of issues resolved in Update 1, see the [Resolved Issues](#) section in these release notes. We recommend that you upgrade your XTM devices from v11.5.3 to v11.5.3 Update 1 as soon as possible to take advantage of the product enhancements in this update. There are no updates to WatchGuard System Manager or any auxiliary software (such as Mobile VPN client software, Single Sign-On software, etc.). We have included the complete XTM v11.5.3 release notes content below for your reference.

WatchGuard is excited to announce the general release of Fireware XTM v11.5.3 and WatchGuard System Manager v11.5.3. This release demonstrates a continuing commitment to quality to WatchGuard customers, with a significant number of bug fixes and several minor enhancements. You can install Fireware XTM OS v11.5.3 on any WatchGuard XTM device, including 2 Series, 3 Series, 5 Series, 8 Series, XTM 1050, and XTM 2050 devices.

Minor enhancements include:

- Changes to the routes section of the Firebox System Manager Status Report to improve consistency in the way IPv4 and IPv6 routes are displayed.
- New IP address validity checking in Mobile VPN configurations to help prevent common errors with overlapping IP addresses.

In addition to these product enhancements, we are pleased to release a large number of bug fixes to our existing customer base. For more information, see the [Resolved Issues](#) section.

For more information about the feature enhancements included in Fireware XTM v11.5.3, see [What's New in Fireware XTM v11.5.3](#).

Before You Begin

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

- A WatchGuard XTM 2 Series, 3 Series, 5 Series, 8 Series, XTM 1050, or XTM 2050 device.
- The required hardware and software components as shown below.
- Feature key for your XTM device — If you upgrade your XTM device from an earlier version of Fireware XTM OS, you can use your existing feature key.

Note that you can install and use WatchGuard System Manager v11.5.3 and all WSM server components with devices running earlier versions of Fireware XTM v11. In this case, we recommend that you use the product documentation that matches your Fireware XTM OS version.

Documentation for this product is available on the WatchGuard web site at www.watchguard.com/help/documentation.

Localization

This release includes localized Fireware XTM management user interfaces (WSM application suite and Web UI), as localized for the v11.5.1 release. Updates to the help or user interface that have occurred since the release of v11.5.1 remain in English. Supported languages are:

- Chinese (Simplified, PRC)
- French (France)
- Japanese
- Spanish (Latin American)

Note *In addition to these languages, we offer localized Web UI support for Korean and Traditional Chinese. Only the Web UI itself has been localized. WSM, and all help files and user documentation, remain in English for these two languages.*

Note that most data input must still be made using standard ASCII characters. You can use non-ASCII characters in some areas of the UI, including:

- Proxy deny message
- Wireless hotspot title, terms and conditions, and message
- WatchGuard Server Center users, groups, and role names

Any data returned from the device operating system (e.g. log data) is displayed in English only. Additionally, all items in the Web UI System Status menu and any software components provided by third-party companies remain in English.

Fireware XTM Web UI

The Web UI will launch in the language you have set in your web browser by default. The name of the currently selected language is shown at the top of each page. To change to a different language, click the language name that appears. A drop-down list of languages appears and you can select the language you want to use.

WatchGuard System Manager

When you install WSM, you can choose what language packs you want to install. The language displayed in WSM will match the language you select in your Microsoft Windows environment. For example, if you use Windows XP and want to use WSM in Japanese, go to Control Panel > Regional and Language Options and select Japanese from the language list.

Log and Report Manager, CA Manager, Quarantine Web UI, and Wireless Hotspot

These web pages automatically display in whatever language preference you have set in your web browser.

Fireware XTM and WSM v11.5.3 Operating System Compatibility

Revised March 2012

WSM/ Fireware XTM Component	Microsoft Windows XP SP2 (32-bit)	Microsoft Windows Vista (32-bit & 64-bit)	Microsoft Windows 7 (32-bit & 64-bit)	Microsoft Windows Server 2003 (32-bit)	Microsoft Windows Server 2008 & 2008 R2*	Mac OS X v10.5, v10.6, & v10.7
WatchGuard System Manager Application	✓	✓	✓	✓	✓	
Fireware XTM Web UI <i>Supported Browsers: IE 7 and 8, Firefox 3.x & above</i>	✓	✓	✓	✓	✓	✓
Log and Report Manager Web UI <i>Supported browsers: Firefox 3.5 & above, IE8 & above, Safari 5.0 & above, Chrome 10 & above. Javascript required.</i>	✓	✓	✓	✓	✓	✓
WatchGuard Servers	✓	✓	✓	✓	✓	
Single Sign-On Agent Software (Includes Event Log Monitor)				✓	✓	
Single Sign-On Client Software	✓	✓	✓	✓	✓	
Terminal Services Agent Software**				✓ ***	✓	
Mobile VPN with IPSec Client Software	✓	✓	✓			Supports iOS devices using native IPSec client software
Mobile VPN with SSL Client Software	✓	✓	✓	✓		✓

* Microsoft Windows Server 2008 32-bit and 64-bit support; Windows Server 2008 R2 64-bit support.


** Terminal Services support with manual authentication operates in a Microsoft Terminal Services or Citrix XenApp 4.5, 5.0, 6.0 and 6.5 environment.






































*** Microsoft Windows Server 2003 SP2 required.

Authentication Support

This table gives you a quick view of the types of authentication servers supported by key features of Fireware XTM. Using an authentication server gives you the ability to configure user and group-based firewall and VPN policies in your XTM device configuration. With each type of third-party authentication server supported, you can specify a backup server IP address for failover.

 — Fully supported by WatchGuard

 — Not yet supported, but tested with success by WatchGuard customers

	Active Directory ¹	LDAP	RADIUS ²	SecurID ²	Firebox (Firebox-DB) Local Authentication
Mobile VPN with IPSec/Shrew Soft			 ³	—	
Mobile VPN with IPSec for iPhone/iPad iOS and Mac OSX					
Mobile VPN with SSL for Windows			 ⁴	 ⁴	
Mobile VPN with SSL for Mac				 ⁵	
Mobile VPN with PPTP	—	—		N/A	
Built-in Authentication Web Page on Port 4100					
Windows Single Sign-On Support (with or without client software)		—	—	—	—
Terminal Services Manual Authentication					
Citrix Manual Authentication					

1. Active Directory support includes both single domain and multi-domain support.
2. RADIUS and SecurID support includes support for both one-time passphrases and challenge/response authentication integrated with RADIUS. In many cases, SecurID can also be used with other RADIUS implementations, including Vasco.
3. The Shrew Soft client does not support two-factor authentication.
4. Fireware XTM supports RADIUS Filter ID 11 for group authentication.
5. PIN + Tokencode mode is supported. Next Tokencode mode and SMS OneTimePasswords are not supported.

Downloading Software

1. Log in to the [WatchGuard Portal](#) and select the Articles & Software tab.
2. From the Search section, clear the Articles check box and search for available Software Downloads.
Select the XTM device for which you want to download software.

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_5_3s.exe` — Use this file to upgrade WatchGuard System Manager from v11.x to WSM v11.5.3.

Fireware XTM OS

Select the correct Fireware XTM OS image for your hardware. Use the .zip file if you will install the OS using the Fireware XTM Web UI.

If you have....	Select from these Fireware XTM OS packages
XTM 2050	<code>XTM_OS_XTM2050_11_5_3.exe</code> <code>xm_xtm2050_11_5_3.zip</code>
XTM 1050	<code>XTM_OS_XTM1050_11_5_3.exe</code> <code>xm_xtm1050_11_5_3.zip</code>
XTM 8 Series	<code>XTM_OS_XTM8_11_5_3.exe</code> <code>xm_xtm8_11_5_3.zip</code>
XTM 5 Series	<code>XTM_OS_XTM5_11_5_3.exe</code> <code>xm_xtm5_11_5_3.zip</code>
XTM 330	<code>XTM_OS_XTM330_11_5_3.exe</code> <code>xm_xtm330_11_5_3.zip</code>
XTM 33	<code>XTM_OS_XTM33_11_5_3.exe</code> <code>xm_xtm33_11_5_3.zip</code>
XTM 2 Series Models 21, 22, 23	<code>XTM_OS_XTM2_11_5_3.exe</code> <code>xm_xtm2_11_5_3.zip</code>
XTM 2 Series Models 25, 26	<code>XTM_OS_XTM2A6_11_5_3.exe</code> <code>xm_xtm2a6_11_5_3.zip</code>

Single Sign-On Software

There are two files available for download if you use Single Sign-On. Both files have been updated to v11.5.3.

- `WG-Authentication-Gateway.exe` (SSO Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO)
- `WG-Authentication-Client.msi` (SSO Client software - optional)

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

Terminal Services Authentication Software

- `TO_AGENT_32_11_5_2.exe` (32-bit support)
- `TO_AGENT_64_11_5_2.exe` (64-bit support)

Mobile VPN with SSL Client for Windows and Mac

There are two files available for download if you use Mobile VPN with SSL:

- `WG-MVPN-SSL_11_5_3.exe` (Client software for Windows)
- `WG-MVPN-SSL_11_5_3.dmg` (Client software for Mac)

Mobile VPN with IPSec client for Windows

You can download the Shrew Soft VPN client for Windows from our web site. For more information about the Shrew Soft VPN client, see the help or visit the [Shrew Soft, Inc. web site](#).

Upgrade from Fireware XTM v11.x to v11.5.3

Before you upgrade from Fireware XTM v11.x to Fireware XTM v11.5.3, download and save the Fireware XTM OS file that matches the WatchGuard device you want to upgrade. You can find all available software on the [WatchGuard Portal](#), Articles & Software tab. You can use Policy Manager or the Web UI to complete the upgrade procedure. We strongly recommend that you back up your device configuration, your WatchGuard Management Server configuration, AND your Log Server and Report Server databases before you upgrade. It is not possible to downgrade without these backup files.

Back up your WatchGuard Management Server Configuration

From the computer where you installed the Management Server:

1. From WatchGuard Server Center, select **Backup/Restore Management Server**.
The WatchGuard Server Center Backup/Restore Wizard starts.
2. Click **Next**.
The Select an action screen appears.
3. Select **Back up settings**.
4. Click **Next**.
The Specify a backup file screen appears.
5. Click **Browse** to select a location for the backup file. Make sure you save the configuration file to a location you can access later to restore the configuration.
6. Click **Next**.
The WatchGuard Server Center Backup/Restore Wizard is complete screen appears.
7. Click **Finish** to exit the wizard.

Back Up your Log Server, Report Server, Quarantine Server

If you are upgrading to WSM v11.5.3 from WSM v11.4.x or earlier, it is important to back up your Log and Report Server data using the procedure below. This is necessary because the Log and Report Server database structure changed in WSM v11.5.1. If you are new to v11.5.x, this is a very important change for you to understand and it is described in *Log and Report Manager Web UI*. You may also want to back up your Quarantine Server, if you use one. These steps are not necessary when you upgrade from v11.5.x to v11.5.3.

1. From WatchGuard Server Center, note the directory path in which your Log and Report Server database is installed. Then, stop all servers.
2. From **Control Panel > Administrative Tools > Services**, stop the PostgreSQL-8.2 Server.
3. Back up or make a copy of the contents of the directory containing your Log Server and Report Server configuration.

On Windows XP SP2 or Windows Server 2003, if you accepted the default installation, the Log and Report Server database will be in this location:

%SYSTEMDRIVE%\Documents and Settings\WatchGuard

On Windows Vista, Windows, 7, Windows Server 2008, or Windows Server 2008 R2, if you accepted the default installation, the Log Server and Report Server databases will be in this location:

%SYSTEMDRIVE%\ProgramData\WatchGuard

4. Back up the Log Server and Report Server database directory, if they were changed from the default. You can find the database locations in WatchGuard Server Center on the Log Server and Report Server **Database Maintenance** tabs. By default, the database is located in the directory listed in Step 3 and this step is not necessary.
5. Back up the Log Server directory where the database backup files are stored, if it was changed from the default. The Log Server **Database Maintenance** tab shows this directory path.
6. Back up the Report Server directory where the XML files for the Available Reports are stored, if it was changed from the default. The Report Server **Server Settings** tab shows this directory path.

Upgrade to Fireware XTM v11.5.3 from Web UI

1. Go to **System > Backup Image** or use the USB Backup feature to back up your current configuration file.
2. On your management computer, launch the OS software file you downloaded from the WatchGuard Software Downloads Center.
If you use the Windows-based installer, this installation extracts an upgrade file called *[xtm series]_[product code].sysa-dl* to the default location of C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\11.5.3\[model] or [model][product_code].
3. Connect to your XTM device with the Web UI and select **System > Upgrade OS**.
4. Browse to the location of the *[xtm series]_[product code].sysa-dl* from Step 2 and click **Upgrade**.

Upgrade to Fireware XTM v11.5.3 from WSM/Policy Manager v11.x

1. Select **File > Backup** or use the USB Backup feature to back up your current configuration file.
2. On your management computer, launch the OS executable file you downloaded from the WatchGuard Portal. This installation extracts an upgrade file called *[xtm series]_[product code].sysa-dl* to the default location of C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\11.5.3\[model] or [model][product_code].
3. Install and open WatchGuard System Manager v11.5.3. Connect to your XTM device and launch Policy Manager.
4. From Policy Manager, select **File > Upgrade**. When prompted, browse to and select the *[xtm series]_[product code].sysa-dl* file from Step 2.

General Information for WatchGuard Server Software Upgrades

It is not necessary to uninstall your previous v11.x server or client software when you update from v11.0.1 or higher to WSM v11.5.3. You can install the v11.5.3 server and client software on top of your existing installation to upgrade your WatchGuard software components. When you first upgrade to WSM v11.5.x, your Log Server and Report Server will be upgraded during installation. The timestamps of existing log and report data will be converted to UTC from the local time zone. Here are specific details of what to expect with each upgrade:

Log Server Upgrade Details

- UTC migration is done from the newest data in your database to the oldest data. The conversion to UTC can take a long time if you have a large amount of data in your database. For example, in a recent test at WatchGuard, it took approximately 16 hours to update a 100 GB database on a Dell PowerEdge 860 with a 250 GB 7200 RPM SATA disk, and a 3.2 GHz dual core Pentium D CPU. This information is provided for informational purposes only. Results may differ depending on the size of your database and the type of hardware you use.
- No data will appear in the Log and Report Manager Web UI until it has been migrated.
- If you have failure notification enabled, the Log Server will send an email notification when the migration starts, and when it finishes, as well as if an error occurs.
- If you stop the Log Server during migration, migration will resume automatically when you restart the Log Server.
- During migration, the Report Server is not able to get access to any log data.
- You can use the WSM v11.4 or earlier LogViewer with a v11.5.x Log Server.
- The PostgreSQL version bundled with WSM has been upgraded to 8.2.21. If you have configured your Log Server to use an external PostgreSQL database, make sure to update to the latest minor version of PostgreSQL server release you use, or make sure that the version you use is current for your timezone before you upgrade.

Report Server Upgrade Details

- The conversion to UTC can take a long time if you have a large amount of data in your Report Server database.
- If you have failure notification enabled, the Report Server will send an email notification when the migration starts, and when it finishes, as well as if an error occurs.
- During migration, the Report Server is not able to get access to any log data. On-demand reports are not available until UTC migration is done. Most existing archived reports will remain available, and the timestamps in existing archived reports will not be updated to UTC.

-
- If you stop the Report Server during migration, migration will resume automatically when you restart the Report Server.
 - You cannot use a v11.5.x Report Server with Log Servers running an earlier version of software. You must use Log Server v11.5.x and the new v11.5.x Log and Report Manager Web UI.
 - The PostgreSQL version bundled with WSM has been upgraded to 8.2.21. If you have configured your Report Server to use an external PostgreSQL database, make sure to update to the latest minor version of PostgreSQL server release you use, or make sure that the version you use is current for your timezone before you upgrade.

For more information about how to track the status of your Log or Report Server upgrade, see WatchGuard Knowledge Base article 6902.

Upgrade your FireCluster to Fireware XTM v11.5.1

There are two methods to upgrade Fireware XTM OS on your FireCluster. The method you use depends on the version of Fireware XTM you currently use.

Upgrade a FireCluster from Fireware XTM v11.4.x

Use these steps to upgrade a FireCluster from Fireware XTM v11.4.x to Fireware XTM v11.5.x:

1. Open the cluster configuration file in Policy Manager
2. Select **File > Upgrade**.
3. Type the configuration passphrase.
4. Type or select the location of the upgrade file.
5. To create a backup image, select **Yes**.
A list of the cluster members appears.
6. Select the check box for each device you want to upgrade.
A message appears when the upgrade for each device is complete.

When the upgrade is complete, each cluster member reboots and rejoins the cluster. If you upgrade both devices in the cluster at the same time, the devices are upgraded one at a time. This is to make sure there is not an interruption in network access at the time of the upgrade.

Policy Manager upgrades the backup member first and then waits for it to reboot and rejoin the cluster as a backup. Then Policy Manager upgrades the master. Note that the master's role will not change until it reboots to complete the upgrade process. At that time the backup takes over as the master.

To perform the upgrade from a remote location, make sure the FireCluster interface for management IP address is configured on the external interface, and that the management IP addresses are public and routable. For more information, see [About the Interface for Management IP Address](#).

Upgrade a FireCluster from Fireware XTM v11.3.x

To upgrade a FireCluster from Fireware XTM v11.3.x to Fireware XTM v11.5.x, you must perform a manual upgrade. For manual upgrade steps, see the Knowledge Base article [Upgrade Fireware XTM OS for a FireCluster](#).

Downgrade Instructions

Downgrade from WSM v11.5.3 to WSM v11.x

If you want to revert from v11.5.3 to an earlier version of WSM, you must uninstall WSM v11.5.3. When you uninstall, choose **Yes** when the uninstaller asks if you want to delete server configuration and data files. After the server configuration and data files are deleted, you must restore the data and server configuration files you backed up before you upgraded to WSM v11.5.3.

Next, install the same version of WSM that you used before you upgraded to WSM v11.5.3. The installer should detect your existing server configuration and try to restart your servers from the **Finish** dialog box. If you use a WatchGuard Management Server, use WatchGuard Server Center to restore the backup Management Server configuration you created before you first upgraded to WSM v11.5.3. Verify that all WatchGuard servers are running.

Note You cannot downgrade an XTM 2050, an XTM 330, or an XTM 33 device to a version of Fireware XTM OS lower than v11.5.1.

Downgrade from Fireware XTM v11.5.3 to Fireware XTM v11.x

If you want to downgrade from Fireware XTM v11.5.3 to an earlier version of Fireware XTM, you either:

- Restore the full backup image you created when you upgraded to Fireware XTM v11.5.2 to complete the downgrade; or
- Use the USB backup file you created before the upgrade as your auto-restore image, and then boot into recovery mode with the USB drive plugged in to your device.

To start a WatchGuard XTM 330, 5 Series, 8 Series, XTM 1050, or XTM 2050 device in recovery mode:

1. Power off the XTM device.
2. Press the up arrow on the device front panel while you turn the power on.
3. Keep the button depressed until "Recovery Mode starting" appears on the LCD display.

To start a WatchGuard XTM 2 Series or XTM 33 device in recovery mode:

1. Disconnect the power.
2. Press and hold the Reset button on the back while you connect the power to the device.
3. Keep the button depressed until the Attn light on the front turns solid orange.

Log and Report Manager Web UI

With the release of WatchGuard System Manager v11.5.1, we introduced an important update to the log and report viewing tools. The functionality from the LogViewer, Report Manager, and Reporting Web UI tools has been merged into the new Log and Report Manager web UI. The functionality from these three important visibility tools is now available in a single interface that is dynamically created for you based on your user access rights, and the type of WatchGuard server software you've installed.

Changes to the Log Viewing Tool

The upgraded log viewing component provides improved performance, including high performance data export functionality. The new tool also introduces log frequency visualization. The following sub-features of pre-v11.5.x LogViewer have not been carried forward to the new Log and Report Manager web UI:

- The ability to "Save selection as..." .html, .pdf, or .xml from Log and Report Manager. You can save log messages to a .csv file from the Actions > Export Logs menu.
- The ability to "Send selection as..." .csv or .pdf directly from Log and Report Manager. You can use your preferred email program to manually send the exported .csv file.
- The ability to "Export selected data" to sqlite database format or "Import data" from sqlite database with Log and Report Manager. You can use your Log Server to export data.

Changes to the Report Viewing Tool

The upgraded functionality of the report viewing tool includes the ability to drill-down through your report data and introduces report pivots. The Log and Report Manager web UI is designed to give you an interactive reporting experience, not to generate static report content. The Report Server will, however, continue to support the generation of static .html and .pdf. reports. Because of this, the following options have not been carried forward to the new Log and Report Manager web UI:

- The ability to "Save as..." .csv, .html, . or .pdf file formats directly from Log and Report Manager. Note that you can save summary reports directly in .pdf format.
- The ability to "Send to..." an email address.
- The report filter option available on some report types has been removed.

Changes to the User Report Viewing Tool

The Reporting Web UI has been completely replaced by the new Log and Report Manager web UI. You can use this new tool to give your users access to reports. The ability to add a custom logo and colors has been deprecated with this release.

For more information about the functionality of the new Log and Report Manager web UI, see the WatchGuard System Manager Help.

Resolved Issues

The Fireware XTM v11.5.3 and Update 1 releases resolve a number of problems found in earlier Fireware XTM v11.x releases.

Resolved in Fireware XTM OS v11.5.3 Update 1

- This release improves proxy throughput on XTM 1050 and XTM 8 Series devices by increasing the total_queue_threshold and tcp_drop_threshold values to prevent congestion.
- This release resolves several issues that resulting in XTM devices unexpectedly restarting because of a kernel crash. [65037, 65548, 65984, 64611, 65771, 65975]
- The XTM 2 Series and 3 Series modem failover feature now operates correctly. [65497]
- The wireless hotspot acceptance page URL has been updated to use HTTP and port 4106. [61394]
- Several problems have been resolved that caused crashes of the SIP ALG processes and resulted in dropped or one-way calls. [65786, 66569]
- A problem was resolved that caused HTTP downloads to stall when your XTM device was configured to use Gateway AV, IPS, and Application Control. [65462]
- A problem that caused the firewalld process to stall has been resolved. [66495]
- Multi-WAN Link Monitor host by domain name now works correctly. [66029]
- You can now create more than 10 VLANs on an external interface. [65257]
- A problem that caused a FireCluster failover delay has been resolved. [66180]
- Static routes to an XTM device interface are now correctly cleaned up when the interface goes down. [66456]
- A problem that caused the configd process to fail has been resolved. [66512]
- DHCP address assignment now works correctly on an XTM device configured in PPPoE half bridge mode. [66570]

Resolved in Fireware XTM OS v11.5.3

General

- An instability issue found on some XTM 2 devices, where the device could pass traffic normally but could not be managed with WSM or Web UI, has been fixed. [64546]
- .A Support Snapshot (a support.tgz file) can now be correctly saved to a USB drive. [64897]

Policy Manager

- You can now use an IP address with a leading zero (10.19.09.0 vs 10.19.9.0) without causing branch office VPN failures. [65189]
- Policy Manager now updates the Mobile VPN with IPSec policies when the configured Virtual IP Address Pool is changed. [65241]

Authentication

- The Event Log Monitor has been enhanced to more effectively retrieve group information in a clientless SSO environment. [65300]
- The SSO Client now responds appropriately when a client computer resumes from a hibernate or sleep state. [65561]

-
- In the SSO Setup Wizard, the Event Log Monitor check box is now clear by default. [65825]
 - The SSO Agent can now correctly load configuration information when the network interface is unavailable. [65802]

Proxies

- HTTP proxy performance has been improved when downloading very large files. [65967]
- A chunking handling issue in the HTTP proxy has been resolved. [65505]
- The SMTP proxy now correctly detects a multi-line 550 response as a valid response. [64463]
- When you use TLS with the default optional allowed rules in the SMTP proxy, email messages can now be delivered successfully to mail servers that do not support TLS. [64650]
- A SIP ALG memory leak issue has been resolved. [65749]
- The SIP ALG now allows provisional ACKs. [65247]
- A problem that caused the SIP ALG to crash has been resolved. [60222]

Security Services

- Gateway AV now detects password-encrypted virus attachments as scan errors. [65047]
- Gateway AV signature update memory utilization has been optimized in this release. This prevents Gateway AV scanning failures caused by a lack of memory. [64940, 64511, 62222]
- The HTTP response no longer stalls when both Gateway AV and RED are enabled. [65877]
- The UTF8 encoded X-WatchGuard-AntiVirus header no longer breaks attachments with long file names. [64883]
- WebBlocker can now correctly fail over to a configured backup server. [65211]

Centralized Management

- Device configuration templates that contain a TCP-UDP proxy policy and a WebBlocker action now work correctly with WatchGuard devices running Fireware XTM v11.3.x. [65408]

Logging & Reporting

- The frequently seen log message: "failed to get routing rules" has been suppressed. [65463]
- A problem that caused log messages to take up to 15 minutes to fail over to a backup Log Server in some networks has been resolved. [62275]
- The Log Collector can now gracefully recover from errors related to a lack of shared memory. [65101]
- Report Manager no longer shows "500 Internal Server Error" when you try to get access to device reports on February 29th of a calendar leap year. [65735]
- Report Manager can now successfully generate PDF output for reports that contain a bar chart. [65099]
- Report Server no longer stops responding to requests while it generates ConnectWise reports data. [65725]
- The Application Usage and Blocked Applications reports no longer display the incorrect IP address value in the y-axis. [65302]
- You can now specify "https://" as part of the ConnectWise Server address without causing WatchGuard Server Center to fail. [64712]

Networking

- Configuration files that include a large number of 1-to-1 NAT entries no longer cause a traffic interruption when saved. [60037]

-
- A problem that caused a significant memory spike when you configured the DHCP server lease time to one second has been resolved. [65242]
 - A problem that caused XTM device performance degradation to occur on devices configured with at least one VLAN interface and many secondary IP addresses has been resolved. [65591]

FireCluster

- A problem that could cause members in a cluster to lock up until rebooted has been resolved. This problem would only occur on a cluster for which proxies were configured. [61091]
- A crash that could occur when one or more connections spanned multiple failovers (at least two failovers in a row) has been corrected. [66008, 66177]
- A problem that could cause connections to time out prematurely has been corrected. In most cases, the symptom would be the disruption of a service (e.g. an FTP download would fail). The problem could affect connections assigned to the non-master of an Active/Active cluster or connections assigned to the new master of an Active/Passive cluster following a failover. [66110]
- Log messages about a FireCluster reboot have been improved to include the reason for the reboot. [65115]
- A problem that prevented a FireCluster failover from occurring because of an error in interpreting the health of the FireCluster Monitored Port has been resolved. [65441]
- An Application Control bug that caused both members of an active/passive FireCluster to reboot has been resolved. [65770]

Mobile VPN with SSL

- Policy Manager and Web UI now display a warning message if Mobile VPN with SSL is enabled and the external IP address of the XTM device is modified. [65806]
- A problem that caused the Mobile VPN with SSL client to crash when connecting from a computer using the Mac OSX 64-bit operating system has been resolved. [65776]
- The Mobile VPN with SSL client running on a computer using Windows 7 64-bit OS can now operate correctly with a third-party web server certificate. [65535]

Mobile VPN with IPSec

- The Mobile VPN with IPSec Shrew Soft client can now connect to an XTM device configured with a static IP address. [64920]

Branch Office VPN

- The latency of packets that traverse a branch office VPN tunnel has been improved. [65333]
- This release resolves a problem that caused an IKEd stacktrace issue in FireCluster. [63108, 65292]

CLI

- You can now use the CLI vlan-id command with the “external dhcp” option successfully. [65478]
- The CLI show sysinfo command now displays the correct CPU utilization values. [64521]

Known Issues and Limitations

These are known issues for Fireware XTM v11.5.2 and all management applications. Where available, we include a way to work around the issue.

General

- When you connect a USB drive to an XTM device, the device does not automatically save a single Support Snapshot to the USB drive. [64499]

Workaround

Use the CLI command “usbdiagnostic enable” to enable the device to save a diagnostic support snapshot to the USB drive. For details about this command, see the *CLI Command Reference Guide*

- The "Sysb" version displayed in the Firebox System Manager Status Report will show blank for XTM models 2, 5, 8, and 1050 that were manufactured prior to the XTM v11.5.1 release.
- ICMP flood protection works differently in 11.5.1 than in earlier versions. In v11.5.1 the XTM device counts the combined total number of ping requests and replies, rather than just the total number of ping requests. Since the default threshold for ICMP Flood Attack protection did not increase, the flood protection could trigger more frequently than it did in earlier releases. [63094]

Workaround

In the Default Packet Handling settings, increase the threshold for Drop ICMP Flood Attack from the default value of 1000 packets/second to a higher number.

- When the level of free memory on your XTM device is lower than 20M, saving your XTM device configuration to the device can cause network disruption. [64474]
- The ETH1 interface on the XTM 830F is a fiber-optic port, so you cannot use the WSM Quick Setup Wizard from a computer with an Ethernet interface. Use a computer with a Fiber NIC, or connect using a switch with both Fiber and Ethernet interfaces. [59742]
- 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 XTM 330 and XTM 2050 devices, the uptime record that shows on the LCD display does not automatically refresh. To refresh the update record, you must cycle through the LCD menu options. [65160]
- On XTM 2 Series devices, the load average is always displayed at 1 or higher, even when there is no load on the device. [63898]
- An XTM 2 Series device can take up to 5 minutes to reboot.
- When you use the **Policy Manager > File > Backup** or **Restore** features, the process can take a long time but does complete successfully. [35450]
- You cannot downgrade an XTM 2 Series device from v11.5.1 to v11.4.1 with the **Upgrade OS** option in the Web UI. [63323]

-
- Amazon Web Services (AWS) requires the use of BGP over an IPSec tunnel. The operations outlined by Amazon.com to support Amazon Web Services are not currently supported by WatchGuard products. [41534]

WatchGuard System Manager

- In Firebox System Manager, if you try to import a certificate, the import fails if the certificate file contains text above the “---BEGIN CERTIFICATE” section. The certificate file must start with “---BEGIN CERTIFICATE” and end with “---END CERTIFICATE” and it can only contain one certificate. [64081]

Workaround

Edit the cacert.pem file to remove any text that appears above “---BEGIN CERTIFICATE”.

- WatchGuard System Manager does not display the correct IP address for the default gateway of an XTM device that has no External interface. [56385]
- When you install WatchGuard System Manager or any server software on a computer running Microsoft Windows XP, compatibility mode should not be enabled even if prompted by Windows, for any of the WSM applications, including the installer. [56355]
- Remote managed Firebox or XTM devices configured in Drop-in Mode may not be able to connect to a Management Server that is behind a gateway Firebox or XTM device 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)**.

- During a WSM upgrade, install, or uninstall on a 64-bit Windows systems, any running applications detected by the WSM installer can be stopped successfully, but the installer may not recognize that they have been stopped. [39078]

Workaround

Close the installer application. Right-click on the WatchGuard Server Center icon on your Windows task bar and exit the WatchGuard Server Center. Make sure all detected applications are stopped and then retry the WSM install or uninstall.

- When you run the WSM v11.3.x or higher installer (either the WSM client component only or any selected WSM server components) on Microsoft SBS (Small Business Server) 2008 and 2011 on a computer installed with a 64-bit operating system, you see a Microsoft Windows error "*!ssProc.x64 has stopped working*". When you close the error dialog box, the installation completes. [57133]

Web UI

- The Fireware XTM Web UI does not support the configuration of some features. These features include:
 - FireCluster
 - 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.
- You may need to reboot your XTM device after you import a third-party web certificate before the certificate will take effect. [65589]
- 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.
- For the XTM 2050, the output of the CLI command “show interface” does not clearly indicate the interface number you use in the CLI to configure an interface. The “show interface” CLI command shows the interface number as the interface label on the front of the device (A0, A2 ... A7; B0, B1 ... B7; C0, C1) followed by a dash, and then the consecutive interface number (0 – 17), for all interfaces. [64147]

Workaround

Use the consecutive interface number that appears after the dash as the interface number to configure the interface. For the B1-9 interfaces, the interface number in the CLI command should be in the range 8-15. For the C0-1 interfaces, the interface number in the CLI command should be 16-17.

Proxies

- HTTPS DPI (Deep Packet Inspection) does not work for users who use IE 9.0 with TLS 1.1 and 1.2 enabled, but TLS 1.0 and SSL 3.0 not enabled. [65707]

Workaround

Use a different browser, or enable TLS 1.0 and SSL 3.0 in your IE 9.0 configuration.

-
- The XTM device can store only one HTTPS Proxy Server certificate and can protect only one HTTPS web site at a time. [41131]
 - When an XTM device is under high load, some proxy connections may not terminate correctly. [61925, 62503]
 - When you enable both DPI and OCSP in the HTTPS proxy, you may see occasional certificate warnings or error messages. [63001]...
 - The ability to use an HTTP caching proxy server is not available in conjunction with the TCP-UDP Proxy. [44260]
 - 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.

- When you try to stream YouTube videos from an Apple device running iOS, you may see this error message: "The server is not correctly configured."

Workaround

1. Edit your HTTP proxy policy.
2. Click **View/Edit proxy**.
3. Select the **Allow range requests through unmodified** check box.
4. Save this change to your XTM device.

- The SIP-ALG does not send the Contact header correctly when the Contact header contains a domain name. It only sends an empty string of: Contact: <>. If the Contact header contains an IP address, the SIP-ALG sends the Contact header correctly: Contact: <sip:10.1.1.2:5060>. [59622]

Workaround

Configure the PBX to send the Contact header with an IP address, not a domain name.

Security Subscriptions

- The Gateway AV signature update process is memory-intensive. To avoid memory contention or negative side effects resulting from a spike in memory use, we recommend that you extend the signature update interval to 8-24 hours.
- Some IPS signature information, such as the CVE number, is not available in Firebox System Manager. We provide search capabilities and CVE information for IPS signatures on a web security portal for IPS on the WatchGuard web site, which you can access at <http://www.watchguard.com/SecurityPortal/ThreatDB.aspx>
- Skype detection blocks only new Skype sessions. If a user is already logged in to Skype and a Skype session is already started when Application Control is enabled, Application Control may not detect the activity.
- For XTM 2 Series devices only, Application Control is temporarily disabled during an upgrade, back up, or restore. When the operation is complete, Application Control starts to work again.
- It is not possible to assign a role for Application Control management from the WatchGuard System Manager role-based administration feature. [59204]
- You cannot use a WebBlocker Server through a branch office VPN tunnel. [56319]

Networking

- An apostrophe in a DHCP reservation name causes the DHCP reservation fail. [65529]
- You cannot configure traffic management actions or use QoS marking on VLANs. [56971, 42093]
- You cannot bridge a wireless interface to a VLAN interface. [41977]
- 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]
- 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 accidentally block themselves from their own XTM device. [36934]
- 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 XTM device 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 XTM device in Bridge Mode, the LCD display on your XTM device shows the IP address of the bridged interfaces as 0.0.0.0. [39324]
 - When you configure your XTM device 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 XTM device is configured in Bridge mode. [36900]
 - 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]
 - 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]

Multi-WAN

- If you use PPPoE on an XTM device configured to use multi-WAN, the XTM device can lose the default routes for external interfaces after PPPoE reconnects. [67424]
- When you enable the Multi-WAN Immediate failback option for WAN failover, some traffic may fail over gradually. [42363]

Wireless

- The 5GHz Wireless band does not work when you use channels 36, 40, 149 or 165. [65559]

Authentication

- Clientless SSO is not supported on a TLS-Enabled Active Directory environment.
- If you use Terminal Services authentication, no authentication verification is done against traffic of any protocol that is not TCP or UDP. This includes DNS, NetBIOS, and ICMP traffic.
- Terminal Services authentication support does not work with Single Sign-On.
- It is not possible to use the *Auto redirect users to authentication* page for authentication option together with Terminal Services authentication.
- To enable your XTM device to correctly process system-related traffic from your Terminal or Citrix server, the Terminal Services Agent uses a special user account named Backend-Service. Because of this, you may need to add policies to allow traffic from this user account through your XTM device. You can learn more about how Backend-Service operates in the product help system.
- 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]

Centralized Management

- WSM may display a version mismatch maintenance alert for a managed device, if the device was upgraded while WSM had paused polling the device. [66045]

Workaround

For a basic managed device or a fully managed device, from the Device Management tab, update the OS. After the OS update is complete, select the Device Status tab and refresh the device status. WSM then polls the device and updates the version number for the device.

- There is no option to set up a Traffic Management action in an XTM v11.x Device Configuration Template. [55732]
- You cannot delete authentication users or groups if you use a Management Server configuration template with the authentication server set to “any”. [65293]
- If you used Centralized Management with devices subscribed to templates in earlier versions of WSM, when you upgrade from WSM 11.x to v11.4 or higher, these templates are updated and the devices are no longer subscribed. Each device retains its template configuration. Existing templates are updated to use “T_” in their object names (to match the object names in the devices that used to subscribe to them). After you upgrade, you’ll see the template upgrade that occurs during upgrade in your revision history.
- When a XTM template is applied to a managed device, the Management Server creates a new configuration revision for the device only if the new revision is going to be different from the current revision. There is also no feedback about why a new configuration revision was not created. [57934]

FireCluster

- The time on the FireCluster backup master can get out of sync with the cluster master, even when NTP is enabled. [66134]

Workaround

Manually synchronize the time of the backup master. Connect to the cluster, launch Firebox System Manager, and then select Tools > Synchronize Time. This synchronizes the time on both cluster members to the time on the management computer.

- When spanning tree protocol (STP) is enabled on some switches, a FireCluster failover can take 10 seconds or longer. [66180]

Workaround

Disable STP on the switch, configure the switch to use rapid STP, or use a different switch.

- For an XTM 330 active/active FireCluster, a cluster member may lock up after you upgrade the Fireware XTM OS. The upgrade of the individual cluster member may be successful, but the device might go into an unresponsive state soon after the upgrade. [65771][65767]

Workaround

Reboot or power cycle the unresponsive device. This usually solves the problem, so that the cluster can form after the device is up and running.

- You might need to re-import the HTTPS DPI certificate after you upgrade the Fireware XTM OS for a FireCluster. [65280]
- You cannot use the secondary IP address of an XTM device interface to manage a FireCluster configured in active/active mode. [64184]

Workaround

Use the primary IP address of an XTM device for all management connections to an active/active FireCluster.

- Users granted access to monitor FireCluster through role-based administration cannot see the FireCluster device in Log and Report Manager. [65398]
- The FireCluster backup master may become inactive when Mobile VPN with SSL or PPTP is configured to use an IP address pool that includes the cluster IP address. [63762]

Workaround

Avoid using an IP address pool that conflicts with the cluster IP addresses.

- If the Log Server cannot be reached from the management IP addresses, only the current FireCluster master will be able to connect. This can occur if the Log Server is connected through an External network, but the management IP addresses are on a Trusted or Optional network. [64482]
- If you change the network configuration of a FireCluster from Routed mode to Drop-in mode, and then change it back to Routed mode, the IP address of the cluster interface is not correctly shown in the Policy Manager **Network > Configuration** dialog box. The correct cluster interfaces are shown in the FireCluster configuration dialog box. [63905]
- Gateway AV updates in a system that is low on memory may result in a FireCluster failover [62222]

Workaround

Reduce the frequency that the system checks for Gateway AV updates to minimize the chance of this occurring.

- If a monitored link fails on both FireCluster members, the non-master member is switched into passive mode and consequently does not process any traffic. A multi-WAN failover caused by a failed connection to a link monitor host does not trigger FireCluster failover. FireCluster failover occurs only when the physical interface is down or does not respond.
- Each XTM device has a set of default IP addresses assigned to the device interfaces in a range starting with 10.0.0.1. The highest default IP address depends on the number of interfaces. If you set the IP address of the Primary or Backup cluster interface to one of the default IP addresses, both devices restart, and the backup master becomes inactive. [57663]

Workaround

Do not use any of the default IP addresses as the Primary or Backup cluster interface IP address.

- 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.
- If you use HP ProCurve switches, you may not be able to configure your FireCluster in active/active mode because these switches may not support the addition of static ARP entries. [41396]
- 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]
- It is not possible to use a VLAN interface IP address for a FireCluster management IP address. [45159]
- To perform a manual upgrade of a FireCluster from v11.3.x to v11.5.1, the management computer must be on the same network as the FireCluster management IP addresses. [63278]

Logging and Reporting

- Links to individual reports in the index.html or index.pdf file generated for a combined report are not correct. [65137]

Workaround

You can manually navigate to the report by correcting the error in the report path.

- The Denied Packets Summary report is not yet available in the Log and Report Manager. [63192]
- The PDF output of the Web Activity Trend report does not include time labels on the x-axis when viewed in Log and Report Manager. Date and time information is included in the table below the report. [64162]
- When you upgrade from Fireware XTM v11.4.x to v11.5.1, reports generated near the time of the upgrade may not show up in Log and Report Manager. [64325]
- The User Authentication Denied report does not contain records of denied authentication attempts if you use an authentication server other than Firebox-DB. [65717]
- If you use Mobile VPN with PPTP configured to use RADIUS authentication, the User Authentication Denied report does not contain records of denied authentication attempts. It incorrectly includes only allowed authentication attempts. [65689]
- In the WatchGuard Server Center > Report Server > Server Settings tab, the name of the server that you type in the ConnectWise Server (Site), is case sensitive. If the ConnectWise server name does not exactly match the name of the server specified in the ConnectWise server certificate, reports fail with 'Error: Certificate validation failed.' [64393]

Workaround

Make sure the hostname specified for the ConnectWise server in WatchGuard Server Center is a case-sensitive match of the value of the CN attribute in the subject name field of the ConnectWise server's certificate.

- If a daily report schedule name includes a colon or certain other characters (for example: "1:35"), the system returns an error. [63427]

Workaround

Make sure that your report schedule names use only characters that are valid in Windows file names. You can find valid characters in articles such as <http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247%28v=vs.85%29.aspx> .

- Log collector will crash when it reaches the 2GB virtual size limit on 32-bit Windows systems. [64249]
- There are two sorting issues in the new Log and Report Manager. When you sort by Destination, the field sorts by IP address and not the destination host name (if available). When you sort by Disposition, some items in the "deny" state do not sort accurately within groups. [62879]

-
- Any configured daily or weekly “Archived Reports” you have in your v11.3 configuration are automatically converted to scheduled reports after you upgrade to WSM v11.4 or higher.

Mobile VPN

- If you set the diagnostic log level for Mobile VPN with SSL traffic to “debug” level, log messages stop displaying in Firebox System Manager > Traffic Manager. [65165]

Workaround

Set the diagnostic log level for Mobile VPN with SSL to any log level less granular than “debug”.

- If you add a new feature key that adds Mobile VPN with SSL licenses for your XTM device, you must reboot your XTM device to enable the additional Mobile VPN with SSL users. [65620]
- When you connect a Mobile VPN with SSL v11.5.1 client for the first time to an XTM device upgraded to v11.5.2, the client upgrade sometimes fails. [65635]

Workaround

Install the Mobile VPN with SSL client manually.

- You cannot establish a Mobile VPN with SSL connection from a Windows-based computer when the Windows system account is Chinese. [58208]
- When you use the built in IPsec client from an iPhone or iPad, the client connection will disconnect when the connection duration reaches 1 hour and 45 minutes. This is caused by a limitation in the Cisco client used by iPhone/iPad. You must reconnect the IPsec client to reestablish the VPN tunnel. [63147]
- Mobile VPN with PPTP connections from Android mobile devices do not work consistently on 3G mobile networks. [63451]
- Firewall XTM Web UI does not allow you to enable Mobile VPN with SSL if the only external interface is an external VLAN interface. [63871]

Workaround

Use Policy Manager to configure Mobile VPN with SSL if your only external interface is an external VLAN.

- Connections from the Mobile VPN with IPsec client can route through the wrong external interface when the XTM device is configured for multi-WAN in round-robin mode. [64386]
- You cannot configure Mobile VPN with SSL to bridge network traffic to a bridged interface. [61844]
- Mobile VPN with SSL users cannot connect to some network resources through a branch office VPN tunnel that terminates on an active/active FireCluster. [61549]
- You cannot ping the IP address of the XTM device interface to which a Shrew Soft VPN client established a VPN tunnel. You can ping computers on that network, but not the interface IP address itself. [60988]
- Shrew Soft VPN client connections can drop if there are multiple clients connected to an XTM device at the same time issuing Phase 2 rekeys. [60261]
- Phase 1 rekeys initiated by the Shrew Soft VPN client cause the client to be disconnected, if connected more than 24 hours. In this case, we recommend that you set the rekey on your XTM device to 23 hours – one hour shorter than the rekey hard-coded in the Shrew Soft client configuration. This forces the XTM device to initiate the rekey, and gives the client a notification that the tunnel must be re-established. [60260, 60259]
- 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.

- The Mobile VPN for SSL Mac client may not be able to connect to an XTM device when the authentication algorithm is set to SHA 256. [35724]

Branch Office VPN

- Do not use the same name for both a VPN Gateway and a VPN Tunnel. [66412]
- You cannot use a pre-shared key greater than 50 characters in length for a branch office VPN tunnel. [65215]
- When you configure your XTM device in multi-WAN mode, you must select which interfaces to include in your multi-WAN configuration. If there are any interfaces that you choose not to include in your multi-WAN configuration (i.e. you clear the check box for that interface), the system does not create a route for that network. This can cause a problem if you have a branch office VPN configured to include that same interface. In this case, the VPN tunnel can fail to negotiate with its remote peer. [57153]

Workaround

If you use multi-WAN and have problems with your branch office VPN tunnels failing to negotiate with their remote peers, you must open your multi-WAN configuration and select Configure adjacent to your chosen multi-WAN configuration mode. Make sure that the appropriate interfaces are included in your multi-WAN configuration.

- A branch office VPN tunnel does not pass traffic if an inbound static NAT policy that includes IP 50 and IP 51 protocols exists for the external IP address of the XTM device. [41822]
- Managed branch office VPN tunnels cannot be established if the CRL distribution point (for example, the WatchGuard Management Server or a third-party CRL distribution site you use) is offline. [55946]
- 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 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]

Workaround

From Policy Manager, select **View > Policy Highlighting**. Clear the **Highlight Firewall policies based on traffic type** check box.

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 <http://www.watchguard.com/help/documentation/xtm.asp>.

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or log in to the WatchGuard Portal on the Web at <http://www.watchguard.com/support>. When you contact Technical Support, you must supply your registered Product Serial Number 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