Fireware XTM v11.6 Release Notes

Supported Devices	XTMv, XTM 2, 3, 5, and 8 Series XTM 1050, XTM 2050
Fireware XTM OS Build	344207
WatchGuard System Manager Build	344359
Revision Date	10 July 2012

Introduction

WatchGuard is pleased to announce the release of Fireware XTM v11.6 and WatchGuard System Manager v11.6.You can install Fireware XTM OS v11.6 on any WatchGuard XTM device, including 2 Series, 3 Series, 5 Series, 8 Series, XTM 1050 and 2050 devices, and with any edition of XTMv. The new features, feature enhancements, and bug fixes included in this release have been carefully chosen to improve the efficiency, performance, and reliability of all XTM devices.

Feature areas with significant enhancements include:

Authentication

- Single Sign-On support for Citrix and Terminal Services environments
- Authentication portal support for mobile devices
- Authentication auto-redirect to host name to allow use of commercial CA-signed certificates

WatchGuard Servers

- Easy access to HIPAA and PCI Compliance Reporting on new Compliance reporting tab
- Automatic WebBlocker database updates
- New scheduled task options for OS updates, feature key synchronization, and reboots for Management Server management groups

Networking

- Increased maximum number of VLANs
- Wireless Hot Spot splash screen updated to use HTTP
- Configurable dynamic routing policies

Branch Office VPN

- Inbound IPSec pass-through
- Improved VPN Phase 2 key expiration settings
- VPN log message header improvements
- New VPN Diagnostics Report

Security Services and Proxies

- HTTP proxy default deny message layout and text improvements
- More data sources for Reputation Enabled Defense (RED)
- SIP-ALG registration expiration

Other Features and Improvements

- Packet filter throughput increase for all XTM 5 and 8 Series models
- PCAP file download option from Firebox System Manager Diagnostic Tasks
- Help updated to HTML5, with improved search results

***New!* Feature Preview**

Fireware XTM v11.6 introduces a preview of three new features, all developed to help you with policy review and troubleshooting. Now available in the WebUI and CLI only, we will make these features available in WSM and include further development work in future releases.

- Policy Checker — lets you simulate and understand how traffic is handled through your XTM device
- XTM Configuration Report — offers an easy to read, printable report of many key configuration settings for your XTM device
- Authentication Server Connection Tool — Test and diagnose Active Directory and LDAP connections and verify group membership

In addition to these product enhancements, we are pleased to release a large number of bug fixes and smaller enhancements. For more information, see the Resolved Issues section.

For more information about the feature enhancements included in Fireware XTM v11.6, see the product documentation or review What's New in Fireware XTM v11.6.

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, or XTMv (any edition).
- 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. If you use XTMv, your feature key must be generated with the serial number you received when you purchased XTMv.

Note that you can install and use WatchGuard System Manager v11.6 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.

If you have a new XTM device hardware, make sure you use the instructions in the *XTM Quick Start Guide* that shipped with your device. If this is a new XTMv installation, make sure you carefully review the *XTMv Setup Guide* for important installation and setup instructions.

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 v11.6 Operating System Compatibility

Revised June 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 *Supported Browsers: IE 7 and 8, Firefox 3.x & above*	✓	✓	✓	✓	✓	✓
Log and Report Manager Web UI *Supported browsers: Firefox 3.5 & above, IE8 & above, Safari 5.0 & above, Chrome 10 & above. Javascript required.*	✓	✓	✓	✓	✓	✓
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	✓	✓	✓			Native (Cisco) IPSec client is supported
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 or Single Sign-On 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 OS X	⚑	⚑	⚑	✓	✓
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	✓	⚑	⚑	⚑	✓
Terminal Services Authentication with Single Sign-On	✓6	–	–	–	–
Citrix Manual Authentication	⚑	⚑	⚑	⚑	✓

1. *Active Directory support includes both single domain and multi-domain support, unless otherwise noted.*
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.*
6. *Only single domain Active Directory configurations are supported.*
7. *For information about the supported Operating System compatibility for the WatchGuard TO Agent and SSO Agent, see the Fireware XTM and WSM v11.6 Operating System Compatibility table.*

XTMv System Requirements

To install an XTMv virtual device, you must have a VMware ESXi 4.1 or 5.0 host installed on any server hardware supported by the ESXi version you use. You must also install the VMware vSphere Client 4.1 or 5.0 on a supported Windows computer. If you prefer, you can use vCenter Server instead of the vSphere client.

The hardware requirements for XTMv are the same as the hardware requirements for VMware ESXi. For information about VMware hardware compatibility, see the VMware Compatibility Guide at http://www.vmware.com/resources/compatibility/search.php.

Each XTMv virtual machine requires 3 GB of disk space.

Recommended Resource Allocation Settings

	Small Office	Medium Office	Large Office	Datacenter
Virtual CPUs	1	2	4	8 or more
Memory	1 GB	2 GB	4 GB	4 GB or more

Downloading Software

1. Log in to the WatchGuard Portal and select the Articles & Software tab.
2. From the Search section, clear the Articles and Known Issues check boxes 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_6s.exe` — Use this file to upgrade WatchGuard System Manager from v11.x to WSM v11.6.

Fireware XTM OS

Select the correct Fireware XTM OS image for your XTM device. Use the .exe file if you want to install or upgrade the OS using WSM. Use the .zip file if you want to install or upgrade the OS using the Fireware XTM Web UI. Use the .ova file to deploy a new XTMv device.

If you have….	Select from these Fireware XTM OS packages
XTM 2050	`XTM_OS_XTM2050_11_6.exe` `xtm_xtm2050_11_6.zip`
XTM 1050	`XTM_OS_XTM1050_11_6.exe` `xtm_xtm1050_11_6.zip`
XTM 8 Series	`XTM_OS_XTM8_11_6.exe` `xtm_xtm8_11_6.zip`
XTM 5 Series	`XTM_OS_XTM5_11_6.exe` `xtm_xtm5_11_6.zip`
XTM 330	`XTM_OS_XTM330_11_6.exe` `xtm_xtm330_11_6.zip`
XTM 33	`XTM_OS_XTM33_11_6.exe` `xtm_xtm33_11_6.zip`
XTM 2 Series Models 21, 22, 23	`XTM_OS_XTM2_11_6.exe` `xtm_xtm2_11_6.zip`
XTM 2 Series Models 25, 26	`XTM_OS_XTM2A6_11_6.exe` `xtm_xtm2a6_11_6.zip`

XTMv All editions	`xtmv_11_6.ova`
	`xtmv_11_6.exe`
	`xtmv_11_6.zip`

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 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 v11.6

Before you upgrade from Fireware XTM v11.x to Fireware XTM v11.6, 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 and your WatchGuard Management Server configuration before you upgrade. It is not possible to downgrade without these backup files.

> ***Note*** *If you are upgrading to WSM v11.6 from WSM v11.4.x or earlier, it is important to back up your Log and Report Server data using the procedure described in Knowledge Base article 6995. This is necessary because the Log and Report Server database structure changed in WSM v11.5.1. When you upgrade to WSM v11.5.1 or higher for the first time, the timestamps of existing log and report data will be converted to UTC from the local time zone. This Knowledge Base article gives you details on this upgrade, and important information about the Log and Report Manager (also new in WSM v11.5.1).*

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.

Upgrade to Fireware XTM v11.6 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* l to the default location of C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\11.6\[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 v11.6 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* l to the default location of C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\11.6\[model] or [model][product_code].
3. Install and open WatchGuard System Manager v11.6. 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 v11.6. You can install the v11.6 server and client software on top of your existing installation to upgrade your WatchGuard software components.

Upgrade your FireCluster to Fireware XTM v11.6

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 or v11.5.x

Use these steps to upgrade a FireCluster from Fireware XTM v11.4.x or v11.5.x to Fireware XTM v11.6:

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 v11.6, 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 v11.6 to WSM v11.x

If you want to revert from v11.6 to an earlier version of WSM, you must uninstall WSM v11.6. 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 v11.6.

Next, install the same version of WSM that you used before you upgraded to WSM v11.6. 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 v11.6. Verify that all WatchGuard servers are running.

Downgrade from Fireware XTM v11.6 to Fireware XTM v11.x

> ***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. You cannot downgrade XTMv to a version of Fireware XTM OS lower than v11.5.4.*

If you want to downgrade from Fireware XTM v11.6 to an earlier version of Fireware XTM, you either:

- Restore the full backup image you created when you upgraded to Fireware XTM v11.6 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. This is not an option for XTMv users.

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.

Resolved Issues

The Fireware XTM v11.6 release resolves a number of problems found in earlier Fireware XTM v11.x releases.

General

- Temperatures are now displayed correctly on the LCD. *[65051]*
- Uptime on the LCD is now automatically refreshed approximately every 90 seconds. *[65160]*
- The Arm/Disarm LED now operates correctly. *[65066]*
- Fan speeds and voltages are now displayed correctly on the LCD. *[65847]*
- Policy Manager now tries to verify that the device was upgraded to the new version after an upgrade. *[65148]*
- XTM backup images saved with an encryption key that contains any of the XML reserved characters (&, <, >, ‘, or “) can now be restored with Policy Manager and the Web UI. *[65512]*

WatchGuard System Manager

- WSM no longer shows certificates with a validity period that extends beyond January 19, 2038 as expired. *[65492]*
- Quarantine Server periodic email notifications no longer fail if the admin user’s password has special characters. *[66163]*
- In WatchGuard System Manager v11.5.3 a condition could occur that caused corruption of the Management Server configuration file, dvcp.cfg. When this problem occurred, the creation of a drag and drop managed VPN tunnel caused WatchGuard System Manager to crash. This problem was resolved in WSM v11.5.4 and the fix has been carried forward into WSM v11.6. *[66701]*

Web UI

- Mobile VPN with SSL can now be configured when all external interfaces are configured as VLANs. *[63871]*
- Auto-generated PPTP and Mobile VPN Firebox-DB groups can no longer be deleted. *[67007]*

Centralized Management

- WatchGuard System Manager no longer crashes when you try to create a new drag-and-drop tunnel and any of the existing tunnels refer to non-existent VPN resources. *[66823]*
- When you launch Policy Manager from WSM for a fully-managed device, Policy Manager launched from WSM connected to a Management Server will always get the configuration from, and save changes to, the Management Server. *[56721]*
- WSM no longer shows “the device version does not match” maintenance alert for a device that has been upgraded when WSM polling has been paused for that device. *[66045]*
- Expired certificates are now automatically renewed for managed devices. *[67012]*
- Single Sign-On authentication sessions are now preserved in XTM 11.4.x and later configuration templates. *[66326]*

Logging & Reporting

- The DHCP Lease Activity Report now includes only leases granted by the XTM device. [63656]
- Log and Report Manager now displays the BUM Report tab only when the selected server is a Management Server. *[64426]*

- Numerous issues in individual device and server reports have been fixed. *[64931, 64991, 64992, 65044, 66025, 66142, 66905, 66963, 66041, 66041]*
- This release includes improved support for localized external PostgreSQL servers. *[64430, 64902, 64904]*
- The Authentication Denied report now includes authentication failures from all authentication servers, not just Firebox-DB. *[62831, 65717, 65689]*
- The Management, Quarantine, and Report Servers now correctly start sending log messages to a Log Server after their connection to the Log Server is lost, then restarted. *[66066]*
- External Bandwidth report generation was improved to better handle cases where the counters are reset to 0, following a device reboot or memory overflow on Fireware XTMv 11.5.x or older. *[66461]*
- The WebBlocker disposition now shows correctly in the Web Audit by Category report. *[66390]*
- The time stamps in PDF server reports no longer display in UTC. *[66005]*
- The User Authentication Denied report is now included in the Daily and Weekly Appliance Report schedules that are automatically added by the Report Server. *[66881]*
- The Audit Trail report is now included in the Weekly Appliance Report schedule automatically added by the Report Server. *[66881]*

Networking

- Several issues have been fixed related to multi-WAN link monitoring. *[66789, 67009 66452]*
- Modem failover now operates correctly. *[66059, 66592, 66071]*
- Static routes configured with a gateway address on the local network for devices configured in drop-in mode now operate correctly. *[44121]*
- Dynamic routing policies are no longer hidden, as they were prior to XTM OS v11.6. You can now enable logging for dynamic routing protocol traffic. *[61064, 62919]*
- Many unnecessary log messages have been eliminated. *[65599, 65763, 62595, 39623, 67237, 66680, and 65633]*
- A problem that caused memory leaks when using Firebox System Manager diagnostics tools has been resolved. *[64835]*
- When dynamic routing is configured, and appliance is learning routes via BGP, OSPF, or RIP, the route table eth#.out is no longer filled with random routes learned via dynamic routing protocols even when those routes are deleted from a remote router. *[66001*]
- A problem has been resolved that caused damage to data on a USB device during a reboot. *[66898]*

Wireless

- Wireless clients can now get an IP address from the AP when using the WEP encryption algorithm. *[66221]*
- Policy Manager, Web UI and CLI now validate the IP address specified for the Wireless Guest Network interface. *[65994]*
- A problem that sometimes caused a crash to occur on a wireless device when you changed its configuration from an access point to a wireless client has been fixed. *[65510]*

FireCluster

- A problem that could result in the disruption of traffic on connections that span multiple failovers has been fixed. As an example of the problem, in the past, a lengthy FTP file download that continued across multiple failovers may have needed to be restarted. *[66336]*
- The real time clock is now updated when time is synchronized between members of a cluster to better minimize a mismatch in time after one of the members is rebooted. *[66134]*

- FireCluster "join" failure log message have been improved to display the reason for the failure in plain text. The reasons include: *[66775]*
  - cluster version mismatch
  - hardware version mismatch
  - software version mismatch
  - configuration mismatch
  - model mismatch
  - appliance not in member list
  - authentication failure
  - message size mismatch
  - unknown cluster message type
  - serial number mismatch
  - device message mismatch
  - error in processing sync file
- A problem that caused an unexpected failover on a busy appliances has been corrected. This failover could occur when internal log rotation happened to coincide with the generation of the cluster heartbeat. *[66943]*
- A crash that sometimes occurred when you add a second XTM device to create an active/active FireCluster has been fixed. *[66384]*
- An HA event alarm is now correctly generated when a FireCluster failover occurs. *[65976]*
- Firebox System Manager now displays a Front Panel warning when it is connected to a FireCluster with different XTM OS versions on each member. *[65148]*
- Firebox System Manager no longer displays duplicate log messages when connected to an active/active FireCluster. *[65273]*
- In an active/passive FireCluster, the DHCP server on the XTM device now correctly provides IP addresses to its clients after a failover occurs. *[65493, 67328]*
- Beginning in Fireware XTM v11.5.1, the backup device in an active/passive FireCluster issues IGMP "Membership Query" and ICMPv6 "Multicast Listener Query" using the virtual MAC address of the outgoing interface. The VMAC should only be used by the master device. If the non-master device generates traffic using VMAC as the source, the switch connected to that interface may observe MAC address moves from one interface to another frequently. The problem will no longer occur. *[66870]*
- Blocked sites can now be synchronized among cluster members in both active/active and active/passive FireClusters. *[63558, 66077, 65593]*
- An active/passive FireCluster no longer accepts and forwards packets addressed to the multicast MAC address of an active/active FireCluster deployed on the same subnet.. *{56152]*

Branch Office VPN

- Firebox System Manager no longer shows incorrect “Expires in” time for tunnels with large expiration times. *[64058]*
- Policy Manager, Web UI and CLI now enforce consistent limits for Phase 1 and Phase 2 lifetime settings. *[66362]*
- This release resolves an issue where inbound traffic through a branch office VPN tunnel is dropped when the tunnel is configured to use global 1-to1 NAT. *[66247]*

Known Issues and Limitations

These are known issues for Fireware XTM v11.6 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 "usb diagnostic enable" to enable the device to save a diagnostic support snapshot to the USB drive. For details about this command, see the *Command Line Interface 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 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]*

- The XTM Configuration Report does not contain all settings. Settings not included are:
  - Secondary interface IP address *[66990]*
  - Configured QoS settings *[66992]*
  - Static MAC bindings *[66993]*
  - IPv6 configuration *[66994]*

XTMv

- XTMv does not automatically change the self-signed certificate when its serial number changes. *[66668]*

> **Workaround**
> A new self-signed certificate with the correct serial number is generated if you manually delete the certificate from Firebox System Manager > View > Certificates and then reboot the XTMv device.

- If you import the OVA file in VMware Player (which is not officially supported in this release), you must use the "Enter" key on your keyboard to accept the XTMv End User License Agreement (EULA). The **OK** and **Cance**l buttons at the conclusion of the EULA do not appear in VMware Player.

WatchGuard System Manager

- If you use Firebox System Manager to ping across a VPN tunnel, you get a message that reads “No Buffer Space Available.” This is not a memory problem. You see this message if the VPN tunnel is not established. Make sure the VPN tunnel is up and try again. *[59339]*
- 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 "*IssProc.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

- The Policy Manager and Web UI do not provide any warning that the WebBlocker Override may not work for HTTPS. *[67208]*
- 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

- If you manually created dynamic routing policies in Fireware XTM v11.5.x or earlier, the To and From lists in these policies are cleared when you upgrade to v11.6. If dynamic routing is enabled, new policies will be created automatically when you upgrade. *[67721]*
- Policy Checker does not work when your XTM device is configured in Bridge mode. *[66855]*
- An apostrophe in a DHCP reservation name causes the DHCP reservation to 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]*
- XTM devices configured to use multi-WAN can fail to route incoming traffic correctly if the device is configured with 1-to-1 NAT enabled in its branch office VPN tunnel routes. *[67001]*
- The multi-WAN sticky connection does not work if your device is configured to use the multi-WAN Routing Table mode. *[62950]*
- 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

- Citrix 4.5/5/0 servers installed in VMware do not work with Terminal Server Single Sign-On. *[66156]*

> **Workaround**
> This feature works with Citrix 6.0 and 6.5 servers installed in VMware.

- 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.
- It is not possible to use the *Automatically redirect users to the authentication page* 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

- 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

- When you change the log level for your WatchGuard Log Server and click Apply, the change does take effect. *[60088]*

Workaround
1. In WatchGuard Server Center, on the Log Server Logging tab, change the log level for log messages from the Log Server and click **Apply**.
2. In the Servers tree, right-click Log Server and select **Stop Server**. In the confirmation message, select **Yes**.
3. Right-click Log Server again and select **Start Server**.

- 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]*
- 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

- You cannot generate a Mobile VPN with IPSec configuration file when the group name contains the characters the asterisk or period characters(*, .). *[66815]*
- 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 wth 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]*
- 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 cilents 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

- Manual branch office VPN fails when the pre-shared key exceeds 50 characters. *[65215]*
- 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 XTM device 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