Fireware XTM v11.6.1 Release Notes

Select a language:

- English — Fireware XTM v11.6.1 Release Notes
- 中文(简体，中华人民共和国) — Fireware XTM v11.6.1 发行说明
- Français (France) — Notes de publication de Fireware XTM v11.6.1
- 日本語 — Fireware XTM v11.6.1 リリースノート
- Español (América Latina) — Notas de lanzamiento de Fireware XTM v11.6.1

English

Fireware XTM v11.6.1 Release Notes

Supported Devices	XTMv, XTM 2, 3, 5, and 8 Series XTM 1050, XTM 2050
Fireware XTM OS Build	346666
WatchGuard System Manager Build	347361
Revision Date	1 November 2012

Introduction

WatchGuard is pleased to announce the release of Fireware XTM v11.6.1 and WatchGuard System Manager v11.6.1.You can install Fireware XTM OS v11.6.1 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. This release introduces support for the new high-performance XTM 5 Series models 515, 525, 535, and 545 and provides an update to our localized user interfaces and documentation. The release also includes several key product enhancements:

- An XTM device configured in bridge mode can now pass VLAN traffic between 802.1Q switches or bridges.
- FireCluster support for XTM 25, 26, and 33 wired models.

Finally, there are several key bug fixes included in this release and described in the Resolved Issues section.

For more information about the feature enhancements included in Fireware XTM v11.6.1, see the product documentation or review What's New in Fireware XTM v11.6.1.

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. If you use WatchGuard System Manager (WSM), make sure your WSM version is equal to or higher than the version of Fireware XTM OS installed on your XTM device and the version of WSM installed on your Management Server.
- 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 v11.6.1 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 physical device, 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 updated localized Fireware XTM management user interfaces (WSM application suite and Web UI)and product help. 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 v11.6.1 Operating System Compatibility

Revised September 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	Android 4.x and higher
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 IPSec for Android devices	✓	✓	✓	–	✓
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 current Fireware XTM and WSM 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_6_1s.exe` — Use this file to upgrade WatchGuard System Manager from v11.x to WSM v11.6.1.

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_1.exe` `xtm_xtm2050_11_6_1.zip`
XTM 1050	`XTM_OS_XTM1050_11_6_1.exe` `xtm_xtm1050_11_6_1.zip`
XTM 8 Series	`XTM_OS_XTM8_11_6_1.exe` `xtm_xtm8_11_6_1.zip`
XTM 5 Series	`XTM_OS_XTM5_11_6_1.exe` `xtm_xtm5_11_6_1.zip`
XTM 330	`XTM_OS_XTM330_11_6_1.exe` `xtm_xtm330_11_6_1.zip`
XTM 33	`XTM_OS_XTM33_11_6_1.exe` `xtm_xtm33_11_6_1.zip`
XTM 2 Series Models 21, 22, 23	`XTM_OS_XTM2_11_6_1.exe` `xtm_xtm2_11_6_1.zip`
XTM 2 Series Models 25, 26	`XTM_OS_XTM2A6_11_6_1.exe` `xtm_xtm2a6_11_6_1.zip`

XTMv All editions	`xtmv_11_6_1.ova`
	`xtmv_11_6_1.exe`
	`xtmv_11_6_1.zip`

Single Sign-On Software

There are two files available for download if you use Single Sign-On.

- `WG-Authentication-Gateway_11_6.exe` (SSO Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO)
- `WG-Authentication-Client_11_6.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_6.exe` (32-bit support)
- `TO_AGENT_64_11_6.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_6.exe` (Client software for Windows)
- `WG-MVPN-SSL_11_6.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 v11.6.1

Before you upgrade from Fireware XTM v11.x to Fireware XTM v11.6.1, 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.

If you use WatchGuard System Manager (WSM), make sure your WSM version is equal to or higher than the version of Fireware XTM OS installed on your XTM device and the version of WSM installed on your Management Server.

> **Note** *If you are upgrading to WSM v11.6.1 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 v11.6.1 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\11.6.1\[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 v11.6.1 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\11.6.1\[model] or [model][product_code].
3. Install and open WatchGuard System Manager v11.6.1. 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.x. You can install the v11.6.x server and client software on top of your existing installation to upgrade your WatchGuard software components.

Upgrade your FireCluster to Fireware XTM v11.6.1

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

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

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

Downgrade from Fireware XTM v11.6.x 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 an XTM 5 Series model 515, 525, 535 or 545 to a version of Fireware XTM OS lower than v11.6.1. 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.x to an earlier version of Fireware XTM, you either:

- Restore the full backup image you created when you upgraded to Fireware XTM v11.6.x 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 v11.6.1 release resolves a number of problems found in earlier Fireware XTM v11.x releases.

General

- Several issues have been resolved in this release that caused XTM devices to crash when configured to use Application Control or IPS. *[66937, 65426, 65636, 67312, 66135, 67159, 67399, 67310]*
- An issue was resolved that caused some XTM device processes to crash when running Mu Dynamics default published vulnerability test. *[66490]*
- An issue was resolved that caused a kernel crash and device reboot. *[67329]*
- The XTM 2 Series device can now handle a large file transfer without interface instability. *[67367]*
- A problem that caused incorrect data to display on the XTM 5 Series LCD screen has been resolved. *[67197]*

WatchGuard System Manager

- Policy Manager now displays the correct VLAN limits for XTM 5 Series models 505, 510, 520, and 530 with a standard Fireware XTM feature key (not Pro). *[67780]*

Web UI

- You can now successfully configure and apply Traffic Management actions for XTM 2 and 3 Series devices from the Web UI. *[67221, 66645]*

Centralized Management

- Firebox X Edge e-Series devices can now be successfully managed with templates. *[67658]*

Logging & Reporting

- The notification message sent when a local Log or Report database is down now correctly shows the host IP address instead of "???". *[41731]*
- The Log Server can now handle backup files greater than 2GB in size without generating an error message: “Error (8199), Exception during backup of oldest log data: File is not a zip file” exception". *[66811]*
- The DHCP lease activity report now works correctly. *[66062]*
- Log Collector now handles XTM device log data that spans multiple SSL/TLS records without crashing. *[66347]*

Proxies and Security Services

- A problem has been resolved that caused poor performance on XTM 2 Series models 25 and 26 because of an incorrect memory allocation for security subscription signatures. *[67240]*
- A deny message is now correctly sent to the web browser in most cases when Application Control blocks content in the Web/Web 2.0 category. *[66201]*
- The WebBlocker automatic database update time is no longer off by one hour when daylight savings time is in effect on the host server's timezone. *[67551]*

Networking

- If you use PPPoE or DHCP for an external interface on an XTM device configured to use multi-WAN, the XTM device no longer loses the default routes for external interfaces after the external interface reconnects. *[67424, 67520]*
- A problem has been resolved that caused a static route to fail after an external interface configured to use PPPoE is disconnected, then reconnected. *[67520]*
- Tagged VLAN traffic is now correctly recognized when an XTM device is configured in Bridge mode. *[64355]*

Command Line Interface

- The CLI command “restore factory default all” now successfully restores a device to its factory default settings. *[66240]*

FireCluster

- An issue has been resolved that caused Policy Manager to incorrectly display an interface IP address as 0.0.0.0/24 when you viewed a FireCluster configuration for a cluster in drop-in mode. *[63551]*

Mobile VPN

- The Mobile VPN with SSL process no longer crashes during a FireCluster failover. *[66118]*

Known Issues and Limitations

These are known issues for Fireware XTM v11.6.1 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]*
- 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]*
- Some XTM devices display a model mismatch error when you first apply your feature key to the device. *[68995]*
- Some XTM 5 Series Model 505 shows as wrong model number on LCD display. *[69377]*

- 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]*
- 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.
- 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]*
- 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]*
- 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.

- Windows Update fails through HTTPS proxy with DPI. *[67513]*

Workaround
1. Create an HTTPS packet filter policy to bypass the proxy deep inspection setting, with a username in the From field. Manually log in to the firewall as that user when you perform activations and apply Windows Updates.
2. Create an HTTPS packet filter policy to bypass the proxy deep inspection setting, with scheduled operating hours in the early morning or another low-usage time. Schedule Windows Update for that time period.
3. Set up a WSUS server on your network, and create a bypass policy for that server.

Security Subscriptions

- 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]*
- IPS Signature Update v4.232 could cause XTM devices to crash. *[68907]*

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

- 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]*

- 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.

- 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]
- When you make a change to the configured cluster interface for a FireCluster, you must reboot the FireCluster for the change to take effect. If the FireCluster is in fully managed mode through a Management Server, the FireCluster will reboot without notice. [69763]

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**.

- 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]*
- 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

Chinese (中文)

Fireware XTM 11.6.1 发行说明

支持的设备	XTMv、XTM 2、3、5 和 8 系列 XTM 1050、XTM 2050
Fireware XTM OS 内部版本	346666
WatchGuard System Manager 内部版本	347361
修订日期	2012 年 8 月 8 日

简介

WatchGuard很高兴地宣布发布FirewareXTMv11.6.1版和WatchGuardSystemManagerv11.6.1版。您可以在任意WatchGuardXTM设备上安装FirewareXTMOSv11.6.1，包括2系列、3系列、5系列、8系列、XTM 1050和2050设备，以及任意版本的XTMv。该版本中引入了对新的高性能XTM5系列型号515、525、535和545的支持，以及为本地化用户接口和文档提供更新服务。该版本还包括一些关键产品增强：

- 桥接模式中配置的 XTM 设备现在可以通过 802.1Q 交换机或网桥间的 VLAN 流量。
- 针对 XTM 25、26 和 33 有线型号的 FireCluster 支持。

最后，此版本中包含一些关键漏洞修复，并在 已解决的问题 该部分中有所描述。

有关 Fireware XTM v11.6.1 版中包含的功能增强的详细信息，请参阅产品文档或查看 Fireware XTM v11.6.1 版的新增功能。

开始之前

安装本版本之前，请确保已准备好以下事项：

- WatchGuard XTM 2 系列、3 系列、5 系列、8 系列、XTM 1050 或 XTM 2050 设备，或 XTMv (任意版本)。
- 以下列出了必需的硬件和软件组件。如果使用的是 WatchGuard System Manager (WSM)，请确保您的 WSM 版本不低于安装在 XTM 设备中的 Fireware XTM OS 的版本和安装在 Management Server 上的 WSM 的版本。
- XTM 设备的功能密钥—如果将 XTM 设备从较早版本的 Fireware XTM OS 进行升级，您可使用现有的功能密钥。如果使用的是 XTMv，功能密钥必须通过购买 XTMv 时收到的序列号来生成。

请注意，您可在运行 Fireware XTM v11 较早版本的设备上安装和使用 WatchGuard System Manager v11.6.1 版和所有 WSM 服务器组件。如果是这样，我们建议您使用与 Fireware XTM OS 版本相符的产品文档。

如果您拥有新的 XTM 物理设备，请确保使用 *随设备附带的* XTM 快速启动指南中的说明。如果是新的 XTMv 安装，请确保仔细阅读 *XTMv 设置指南* 以获得重要的安装和设置说明。

该产品的文档可从 WatchGuard 网站上找到，网址为：www.watchguard.com/help/documentation。

本地化

此版本包括更新的本地化 Fireware XTM 管理用户接口 (WSM 应用程序套件和 Web UI) 和产品帮助。支持的语言有：

- 中文 (简体，中华人民共和国)
- 法文 (法国)
- 日文
- 西班牙文 (拉丁美洲地区)

> ***Note*** *除了这些语言之外，我们还提供韩文和繁体中文的本地化 Web UI 支持。只对 Web UI 本身进行了本地化。在这两个语言版本中，WSM 和所有帮助文件和用户文档仍为英文。*

请注意，大多数数据输入仍必须然使用标准的 ASCII 字符。您可在某些 UI 部分使用非 ASCII 字符，其中包括：

- 代理拒绝消息
- 无线 Hotspot 标题、术语和状态，以及消息
- WatchGuard Server Center 用户、组和角色名称

从设备操作系统返回的所有数据 (如日志数据) 都会以英文显示。此外，Web UI 系统状态菜单中的所有条目和第三方公司提供的所有软件组件仍将是英文。

Fireware XTM Web UI

默认情况下，WebUI 会以您的 Web 浏览器中设置的语言启动。当前所选语言的名称会显示在每个页面的顶部。要更改为其它语言，请单击显示的语言名称。将出现下拉列表，然后可以选择要使用的语言。

WatchGuard System Manager

在安装 WSM 时，可以选择要安装的语言包。显示在 WSM 中的语言将和 Microsoft Windows 环境中所选的语言匹配。例如，如果使用的是 Windows XP 且希望使用日文版的 WSM，请前往控制面板 > 区域和语言选项，然后从语言列表中选择日文。

Log and Report Manager、CA Manager、隔离 Web UI 和无线热点

这些 Web 页面将自动以 Web 浏览器中设置的首选语言显示。

Fireware XTM 和 WSM v11.6.1 操作系统兼容性

修订时间：2012 年 6 月

WSM/ Fireware XTM 组件	Microsoft Windows XP SP2 (32 位)	Microsoft Windows Vista (32 位和 64 位)	Microsoft Windows 7 (32 位和 64 位)	Microsoft Windows 服务器 2003 (32 位)	Microsoft Windows 服务器 2008 和 2008 R2*	Mac OS X 10.5 版和 10.6 版和 10.7 版
WatchGuard System Manager 应用程序	✓	✓	✓	✓	✓	
Fireware XTM Web UI *支持的浏览器：* *IE 7、IE 8、Firefox 3.x 及更高版本*	✓	✓	✓	✓	✓	✓
Log and Report Manager Web UI *支持的浏览器：Firefox 3.5 及更高版本、IE8 及更高版本、Safari 5.0 及更高版本、Chrome 10 及更高版本。需要 Javascript。*	✓	✓	✓	✓	✓	✓
WatchGuard 服务器	✓	✓	✓	✓	✓	
单一登录代理软件 (包括 Event Log Monitor)				✓	✓	
单点登录客户端软件	✓	✓	✓	✓	✓	
Terminal Services 代理软件**				✓ ***	✓	
Mobile VPN with IPSec 客户端软件	✓	✓	✓			支持 Native (Cisco) IPSec 客户端
Mobile VPN with SSL 客户端软件	✓	✓	✓	✓		✓

**支持 Microsoft Windows Server 2008 32 位和 64 位；支持 Windows Server 2008 R2 64 位。*

***采用手动或单一登录认证方式的 Terminal Services 支持功能适用于 Microsoft Terminal Services 或 Citrix XenApp 4.5、5.0、6.0 和 6.5 环境。*

**** 需要 Microsoft Windows Server 2003 SP2。*

认证支持

此表为您提供了关于密钥功能或 Fireware XTM 所支持的认证服务器类型的概览。使用认证服务器，您能够在您的 XTM 设备配置中配置基于用户和基于组的防火墙以及 VPN 策略。在各类第三方认证服务器的支持下，您可以指定故障转移的备份服务器 IP 地址。

✓ — 由 WatchGuard 提供完整支持

 — 尚不支持，但是由 WatchGuard 客户成功地进行了测试

	Active Directory[1]	LDAP	RADIUS[2]	SecurID[2]	Firebox (Firebox-DB) 本地认证
Mobile VPN with IPSec/Shrew Soft	✓	✓	✓3	–	✓
适用于 iPhone/iPad iOS 和 Mac OS X 的 Mobile VPN with IPSec				✓	✓
适用于 Windows 的 Moblie VPN with SSL	✓	✓	✓4	✓4	✓
适用于 Mac 的 Moblie VPN with SSL	✓	✓	✓	✓5	✓
Mobile VPN with PPTP	–	–	✓	不可用	✓
端口 4100 上的内建认证网页	✓	✓	✓	✓	✓
Windows 单一登录支持 (配有或未配有客户端软件)	✓	–	–	–	–
Terminal Services 手动认证	✓				✓
通过单一登录的 Terminal Services 认证	✓6	–	–	–	–
Citrix 手动认证					✓

1. *除非另有说明，Active Directory 支持包括单域和多域支持。*
2. *RADIUS 和 SecurID 支持包括一次性密码和与 RADIUS 集成的询问/响应认证。在很多情况下，SecurID 也可用于与其他 RADIUS 实施项(包括 Vasco) 一同使用。*
3. *Shrew Soft 客户端不支持双重认证。*
4. *Fireware XTM 支持 RADIUS Filter ID 11 进行组认证。*
5. *支持 PIN 码 + Tokencode 模式。不支持 Next Tokencode 模式和 SMS OneTimePasswords。*
6. *仅支持单域 Active Directory 配置。*
7. *有关 WatchGuard TO Agent 和 SSO Agent 所支持的操作系统兼容性的详细信息，请参阅最新的 Fireware XTM 和 WSM 操作系统兼容性表。*

XTMv 系统要求

要安装 XTMv 虚拟设备，必须在您使用的 ESXi 版本所支持的任意服务器硬件上安装 VMware ESXi 4.1 或 5.0 主机。您还必须在支持的 Windows 计算机中安装 VMware vSphere Client 4.1 或 5.0。如果愿意的话，您可以使用 vCenter Server 代替 vSphere 客户端。

XTMv 的硬件要求与 VMware ESXi 的硬件要求相同。有关 VMware 硬件兼容性的详细信息，请参阅 VMware 兼容性指南，地址是 http://www.vmware.com/resources/compatibility/search.php。

每台 XTMv 虚拟机需要 3 GB 的磁盘空间。

推荐的资源分配设置

	小型办公室	中型办公室	大型办公室	数据中心
虚拟 CPU	1	2	4	8 个或更多
内存	1 GB	2 GB	4 GB	4 GB 或更多

下载软件

1. 请登录至 WatchGuard 门户 并选择文章与软件选项卡。
2. 从搜索部分中，取消选中文章和已知问题复选框并搜索可用的软件下载。选择要下载其相关软件的 XTM 设备。

可供下载的软件文件有若干个。请参见下列说明，以便了解您的升级操作需要哪些软件包。

WatchGuard System Manager

所有用户现在都可以下载 WatchGuard System Manager 软件。可以通过该软件包安装 WSM 和 WatchGuard Server Center 软件：

`WSM11_6_1s.exe`—使用此文件将 WatchGuard System Manager 从 v11.x 版升级至 WSM v11.6.1 版。

Fireware XTM OS

为您的 XTM 设备选择正确的 Fireware XTM OS 映像。如果想要使用 WSM 安装或升级 OS，请使用 .exe 文件。如果想要使用 Fireware XTM Web UI 安装或升级 OS，请使用 .zip 文件。使用 .ova 文件部署新的 XTMv 设备。

拥有的硬件	从这些 Fireware XTM OS 包中选择
XTM 2050	`XTM_OS_XTM2050_11_6_1.exe` `xtm_xtm2050_11_6_1.zip`
XTM 1050	`XTM_OS_XTM1050_11_6_1.exe` `xtm_xtm1050_11_6_1.zip`
XTM 8 系列	`XTM_OS_XTM8_11_6_1.exe` `xtm_xtm8_11_6_1.zip`
XTM 5 系列	`XTM_OS_XTM5_11_6_1.exe` `xtm_xtm5_11_6_1.zip`
XTM 330	`XTM_OS_XTM330_11_6_1.exe` `xtm_xtm330_11_6_1.zip`
XTM 33	`XTM_OS_XTM33_11_6_1.exe` `xtm_xtm33_11_6_1.zip`
XTM 2 系列型号 21、22、23	`XTM_OS_XTM2_11_6_1.exe` `xtm_xtm2_11_6_1.zip`
XTM 2 系列型号 25、26	`XTM_OS_XTM2A6_11_6_1.exe` `xtm_xtm2a6_11_6_1.zip`

XTMv 全部版本	`xtmv_11_6_1.ova`
	`xtmv_11_6_1.exe`
	`xtmv_11_6_1.zip`

单一登录软件

如果使用单一登录，有两个文件可供下载。

- WG-Authentication-Gateway_11_6.exe (SSO 代理软件 — 单一登录所需，包含可选的用于无客户端 SSO 的 Event Log Monitor)
- WG-Authentication-Client_11_6.msi(SSO 客户端软件 — 可选)

有关如何安装和设置单一登录的信息，请参阅产品文档。

Terminal Services 认证软件

- TO_AGENT_32_11_6.exe (32 位支持)
- TO_AGENT_64_11_6.exe (64 位支持)

Windows 和 Mac 的 Mobile VPN with SSL 客户端

如果要通过 SSL 实现移动 VPN，有两个文件可供下载：

- WG-MVPN-SSL_11_6.exe (用于 Windows 的客户端软件)
- WG-MVPN-SSL_11_6.dmg (用于 Mac 的客户端软件)

适用于 Windows 的 Mobile VPN with IPSec 客户端

您可从我们的网站下载适用于 Windows 的 Shrew Soft VPN 客户端。有关 Shrew Soft VPN 客户端的详细信息，请参阅帮助或访问 Shrew Soft, Inc. 的网站。

从 Fireware XTM 11.x 版升级至 11.6.1 版

从 Fireware XTM v11.x 版升级至 Fireware XTM v11.6.1 版之前，请下载并保存与您所要升级的 WatchGuard 设备相匹配的 Fireware XTM 操作系统文件。所有可用软件都可以在 WatchGuard 门户、文章和软件选项卡中找到。您可使用 Policy Manager 或 Web UI 来完成升级步骤。强烈建议您在升级前备份设备配置和 WatchGuard Management Server 配置。没有这些备份文件将无法进行降级。

如果使用的是 WatchGuard System Manager (WSM)，请确保您的 WSM 版本不低于安装在 XTM 设备中的 Fireware XTM OS 的版本和安装在 Management Server 上的 WSM 的版本。

> ***Note*** *如果您正在将 WSM v11.4.x 版或更早版本升级至 WSM v11.6.1 版，使用知识库文章 6995 中介绍的步骤备份 Log and Report Server 数据非常重要。由于 Log and Report Server 数据库的结构在 WSM v11.5.1 版中发生更改，此操作非常必要。首次升级至 WSM v11.5.1 版或更高版本时，现有日志和报告数据的时间戳将从本地时区更改为 UTC 时间。知识库文章为您提供了关于升级的详细信息以及关于 Log and Report Manager 的重要信息 (WSM v11.5.1 版中同时更新)。*

备份 WatchGuard Management Server 配置

从安装 Management Server 的计算机中：

1. 在 WatchGuard Server Center 中，选择 **备份/恢复管理服务器**。
   将启动 WatchGuard Server Center Backup/Restore Wizard。
2. 单击 **下一步**。
   将显示选择操作屏幕。
3. 选择 **备份设置**。
4. 单击 **下一步**。
   将显示指定备份文件屏幕。
5. 单击**浏览**以选择备份文件的位置。请确保将配置文件保存到以后恢复配置时可以访问的位置。
6. 单击 **下一步**。
   将显示 WatchGuard Server Center Backup/Restore Wizard 已完成的屏幕。
7. 单击 **完成** 以退出向导。

通过 Web UI 升级至 Fireware XTM v11.6.1 版

1. 前往 **系统 > 备份映像** 或使用 USB 备份功能来备份当前的配置文件。
2. 在管理计算机上，启动从 WatchGuard 软件下载中心下载的操作系统软件文件。
   如果使用基于 Windows 的安装程序，此安装将提取出更新文件，文件名为 *[xtm series]_[product code].sysa-dl*，默认路径为 C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\11.6.1\[model](或 [model][product_code])。
3. 使用 Web UI 连接至 XTM 设备，并选择 **系统 > 升级操作系统**。
4. 浏览到步骤 2 中 *[xtm series]_[product code].sysa-dl* 的位置并单击 **升级**。

从 WSM/Policy Manager v11.x 版升级至 Fireware XTM v11.6.1 版

1. 选择 **文件 > 备份** 或使用 USB 备份功能来备份当前的配置文件。
2. 在管理计算机上，启动从 WatchGuard 门户下载的操作系统可执行文件。此安装将提取出更新文件，文件名为 *[xtm series]_[product code].sysa-dl* l，默认路径为 C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\11.6.1\[model](或 [model][product_code]) 。
3. 安装并打开 WatchGuard System Manager v11.6.1 版。连接至 XTM 设备并启动 Policy Manager。
4. 在 Policy Manager 中，选择 **文件 > 升级**。出现提示时，浏览到步骤 2 *[xtm series]_[product code].sysa-dl* 中的文件并选中它。

有关 WatchGuard 服务器软件升级的常规信息

从 v11.0.1 版或更高版本更新至 WSM v11.6.x 版时，无需卸载以前的 v11.x 版服务器或客户端软件。可在现有安装的基础上安装 v11.6.x 版服务器和客户端软件，从而升级 WatchGuard 软件组件。

将 FireCluster 升级至 Fireware XTM 11.6.1 版

有两种方法来升级 FireCluster 上的 Fireware XTM 操作系统。使用哪种方法取决于您当前使用的 Fireware XTM 版本。

将 FireCluster 从 Fireware XTM v11.4.x 版或 v11.5.x 版升级

使用以下步骤将 FireCluster 从 Fireware XTM v11.4.x 版或 v11.5.x 版升级至 Fireware XTM v11.6.x 版：

1. 在 Policy Manager 中，打开群集配置文件
2. 选择 **文件 > 升级**。
3. 键入配置密码。
4. 键入或选择升级文件的位置。
5. 要创建备份映像，请选择 **是**。
   将显示群集成员列表。
6. 选中每台要升级设备的复选框。
   每台设备完成升级后会显示一条消息。

升级完成后，每个群集成员将重启并重新加入群集。如果同时升级群集中的两台设备，将依次进行升级。这是为了确保在升级时不会出现网络访问中断。

Policy Manager 首先将备份成员升级，然后等待其重新引导并作为备份重新加入群集。接着，Policy Manager 升级主控设备。请注意，主控设备角色在重新引导以结束升级流程之前不会发生更改。那时，备份将作为主控设备进行接管。

要从远程位置执行升级，请确保在外部接口上配置了 FireCluster 管理接口 IP 地址，并且管理 IP 地址是公共地址且可路由。有关详细信息，请参阅 关于管理 IP 地址的接口。

从 Fireware XTM 11.3.x 版升级 FireCluster

要将 FireCluster 从 Fireware XTM v11.3.x 版升级至 Fireware XTM v11.6.x 版，必须执行手动升级。有关手动升级的步骤，请参阅知识库文章。升级 FireCluster 的 Fireware XTM 操作系统。

降级说明

从 WSM v11.6.x 版降级至 WSM v11.x 版

如果要从 v11.6.x 版还原至较早版本的 WSM，您必须卸载 WSM v11.6.x 版。在卸载时，请在卸载程序询问是否要删除服务器配置和数据文件时选择 **是** 。删除服务器配置和数据文件后，您必须恢复在升级至 WSM v11.6.x 版之前所备份的数据和服务器配置文件。

接着，安装在升级至 WSM v11.6.x 版之前所使用的相同版本的 WSM。安装程序将检测现有的服务器配置，并尝试从 **完成** 对话框重新启动服务器。如果使用的是 WatchGuard Management Server，请使用 WatchGuard Server Center 来恢复在首次升级至 WSM v11.6.x 版之前所创建的 Management Server 配置备份。检查是否所有的 WatchGuard 服务器都在运行。

从 Fireware XTM v11.6.x 版降级至 Fireware XTM v11.x 版

> ***Note*** *无法将 XTM 2050、XTM 330 或 XTM 33 设备降级至低于 v11.5.1 版的 Fireware XTM OS 版本。无法将 XTM 5 系列型号 515、525、535 或 545 降级至低于 v11.6.1 版的 Fireware XTM OS 版本。无法将 XTMv 降级至低于 v11.5.4 版的 Fireware XTM OS 版本。*

如果要从 Fireware XTM v11.6.x 版降级至较早版本的 Fireware XTM，您可以：

- 恢复在升级至 Fireware XTM v11.6.x 版时所创建的完整备份映像，以完成降级；或
- 使用在升级前创建的 USB 备份文件作为自动恢复映像，然后将 USB 驱动器插入设备后以恢复模式启动。这不适用于 XTMv 用户。

要以恢复模式启动 WatchGuard XTM 330、5 系列、8 系列、XTM 1050 或 XTM 2050 设备：

1. 断开 XTM 设备电源。
2. 在接通设备电源的同时，按住设备前面板上的向上箭头。
3. 一直按住此按钮，直到 LCD 显示屏上显示“正在启动恢复模式”。

要以恢复模式启动 WatchGuard XTM 2 系列或 XTM 33 设备：

1. 断开电源。
2. 将电源连接至设备时按住设备背面的重置按钮。
3. 一直按住该按钮直至前面的 Attn 灯变成长亮的橙色。

已解决的问题

Fireware XTM v11.6.1 版本解决了一系列在较早的 Fireware XTM v11.x 版本中所发现的问题。

常规

- 在配置为使用 Application Control 或 IPS 时，导致 XTM 设备崩溃的几个问题在此版本中已经解决。*[66937, 65426, 65636, 67312, 66135, 67159, 67399, 67310]*
- 运行 Mu Dynamics 默认公开漏洞测试时，导致某些 XTM 设备进程崩溃的问题已解决。*[66490]*
- 导致内核崩溃或设备重启的问题已解决。*[67329]*
- XTM 2 系列设备现在可处理大型文件传输，并且不会产生接口不稳定的情况。*[67367]*
- 导致 XTM 5 系列 LCD 屏幕上显示错误数据的问题已解决。*[67197]*

WatchGuard System Manager

- Policy Manager 现在为配有标准 Fireware XTM 功能密钥(非 Pro 版)的 XTM 5 系列型号 505、510、520 和 530 显示正确的 VLAN 限制。*[67780]*

Web UI

- 现在您可以通过 Web UI 成功配置并应用 XTM 2 和 3 系列设备的流量管理操作。*[67221, 66645]*

Centralized Management

- 现在可以通过模板来成功地管理 Firebox X Edge e-Series 设备。*[67658]*

日志记录和报告

- 当本地日志或报告数据库出现故障时所发送的通知消息，现在正确地显示主机 IP 地址，而不是“???”。*[41731]*
- Log Server 现在可以处理大小超过 2GB 的备份文件，并且不生成错误消息：“错误 (8199)，最早的日志数据备份期间出现异常：文件不是压缩文件”“异常”。*[66811]*
- DHCP 租用活动报告现在正常工作。*[66062]*
- Log Collector 现在可以处理覆盖多个 SSL/TLS 记录的 XTM 设备日志数据，并且不会出现崩溃。*[66347]*

代理和安全服务

- 由于安全订阅签名的内存分配不正确而导致 XTM 2 系列型号 25 和 26 性能不佳的问题已解决。*[67240]*
- 在大多数 Application Control 阻止了 Web/Web 2.0 类别中内容的情况下，拒绝消息现在被正确地发送至 Web 浏览器。*[66201]*
- 当夏令时影响主机服务器的时区时，WebBlocker 自动数据库更新时间不再在 1 小时后关闭。*[67551]*

联网

- 如果您在配置为使用多广域网的 XTM 设备上的外部接口中，使用 PPPoE 或 DHCP，则在外部接口重新连接后，XTM 设备不再丢失外部接口的默认路由。*[67424, 67520]*
- 导致静态路由在配置为使用 PPPoE 的外部接口断开连接并重新连接后发生故障的问题已解决。*[67520]*
- 在桥接模式下配置 XTM 设备时，标记的 VLAN 流量现在已正确识别。*[64355]*

Command Line Interface

- CLI 命令“restore factory default all”现在成功将设备恢复至出厂默认设置。*[66240]*

FireCluster

- 导致您在 Drop-in 模式中查看群集的 FireCluster 配置时 Policy Manager 未正确显示接口 IP 地址 (0.0.0.0/24) 的问题已解决。*[63551]*

Mobile VPN

- FireCluster 故障转移期间，Mobile VPN with SSL 进程不再崩溃。*[66118]*

已知问题和限制

这些是FirewareXTMv11.6.1版和所有管理应用程序的已知问题。如果可行，我们将提供解决此问题的方法。

常规

- 将 USB 驱动器连接到 XTM 设备时，设备不会自动向 USB 驱动器保存单个支持快照。*[64499]*

> **Workaround**
> 请使用 CLI 命令“usb diagnostic enable”使设备能够将诊断支持快照保存到 USB 驱动器。有关该命令的详细信息，请参阅 *Command Line Interface 参考指南*。

- 对于在 XTM v11.5.1 版发布之前所生产的 XTM 型号 2、5、8 和 1050，显示在 Firebox System Manager 状态报告中的“Sysb”版本将显示为空白。
- 11.5.1 版中的 ICMP 洪水攻击保护的工作原理与早期版本不同。在 11.5.1 版中，XTM 设备会计算 ping 请求与回复的合并总数，而不再只是 ping 请求的总数。由于 ICMP 洪水攻击保护的默认阈值未增加，因此洪水攻击保护的触发频率可能比早期版本高。*[63094]*

> **Workaround**
> 在默认数据包处理”设置中，将丢弃 ICMP 洪水攻击”的阈值从默认的 1000 个数据包/秒增加到更大的数值。

- 当 XTM 设备的可用内存大小低于 20M 时，将 XTM 设备配置保存到设备中可导致网络中断。*[64474]*
-
- XTM 830F 上的 ETH1 接口为光纤端口，因此您无法从配备以太网接口的计算机来使用 WSM Quick Setup Wizard。请使用配备光纤网络接口卡的计算机，或使用同时具有光纤和以太网接口的交换机进行连接。*[59742]*
- 要关闭 XTM 5 Series 设备，您必须按住后部的电源开关 4-5 秒。*[42459]*
- 对于 XTM 5 Series 设备，接口 0 不支持 Auto-MDIX，也不会自动感应电缆极性。
- 在 XTM 2 系列设备上，平均负载始终显示为 1 或更大值，即使设备上无负载时也是如此。*[63898]*
- XTM 2 Series 设备重新引导最高可花费 5 分钟。
- 如果使用的是 **Policy Manager > 文件 > 备份** 或者 **恢复** 功能，成功完成该过程会花费较长的时间。*[35450]*
- 您无法使用 Web UI 中的升级操作系统选项 **将 XTM 2 系列** 设备从 v11.5.1 版降级到 v11.4.1 版。*[63323]*
- Amazon Web Services (AWS) 需要使用基于 IPSec 隧道的 BGP。Amazon.com 所述的支持 Web Services 的操作当前不受 WatchGuard 产品支持。*[41534]*
- XTM 配置报告并不包括所有设置。不包括的设置为：
  - 次要接口 IP 地址 *[66990]*
  - 已配置的 QoS 设置 *[66992]*
  - 静态 MAC 绑定 *[66993]*
  - IPv6 配置 *[66994]*

XTMv

- XTMv 在其序列号更改时无法自动更改自签名证书。*[66668]*

> **Workaround**
> 如果从路径 Firebox System Manager > 查看 > 证书来手动删除证书，然后重新引导 XTMv 设备，则将自动生成带有正确序列号的自签名证书。

- 如果在 VMware Player(此版本未正式支持)中导入 OVA 文件，则您必须使用键盘上的回车键来接受 XTMv 最终用户许可协议 (EULA)。此 **确定** 与 EULA 末尾的**取消**按钮不会显示在 VMware Player 中。

WatchGuard System Manager

- 如果使用 Firebox System Manager 通过 VPN 隧道进行 ping 操作，您将收到消息“缓冲区空间不足”。这不是内存问题。如果未建立 VPN 隧道，您将看到该消息。确保设置好 VPN 隧道，然后重试。*[59339]*
- 对于没有外部接口的 XTM 设备，WatchGuard System Manager 无法显示该设备默认网关的正确 IP 地址。*[56385]*
- 在运行 Microsoft Windows XP 的计算机中安装 WatchGuard System Manager 或任何服务器软件时，即使 Windows 出现提示，也请勿为任何 WSM 应用程序(包括安装程序)启用兼容模式。*[56355]*
- 远程管理并配置为 Drop-in 模式的 Firebox 或 XTM 设备可能无法连接到同样配置为 Drop-in 模式且位于网关 Firebox 或 XTM 设备后的 Management Server。*[33056]*
- 如果将备份图像恢复到由 Management Server 管理的托管客户端设备，共享密码可能会不同步。

> **Workaround**
> 从 WSM 连接到 Management Server。选择受管理的设备并选择 **更新设备**。选择单选按钮 **重设服务器配置(IP 地址/主机名、共享密钥)**。

- 在 64 位 Windows 系统中升级、安装或卸载 WSM 期间，WSM 安装程序所侦测到的任何正在运行的应用程序都可成功停止，但是安装程序可能无法识别到它们已经停止。*[39078]*

> **Workaround**
> 关闭安装应用程序。右键单击 Windows 任务栏上的 WatchGuard Server Center 图标，然后退出 WatchGuard Server Center。请确保所有已侦测到的应用程序已停止，然后重试 WSM 安装或卸载。

- 当您在安装了 64 位操作系统的计算机上的 Microsoft SBS (Small Business Server) 2008 和 2011 上运行 WSM v11.3.x 版或更高版本的安装程序(仅 WSM 客户端组件或选定的任意 WSM 服务器组件)时，您会看到 Microsoft Windows 错误“*lssProc.x64 已停止工作*”。在关闭错误对话框时，安装即已完成。*[57133]*

Web UI

- Fireware XTM Web UI 不支持某些功能的配置。这些功能包括：
  - FireCluster

  - 证书导出
  - 无法打开或关闭 BOVPN 事件通知
  - 无法添加或删除设备 ARP 表中的静态 ARP 条目
- 无法获取已加密的 Mobile VPN with IPSec 最终用户配置文件，即 .wgx 文件。Web UI 仅生成纯文本版本的最终用户配置文件，文件扩展名为 .ini。
- 您无法编辑策略的名称、在策略中使用自定义地址，或使用"主机名称(DNS 查询)将 IP 地址添加到策略中。
- 当您在 Web UI 中所配置策略的状态为禁用时，打开 Policy Manager 并对同一策略进行更改，当策略拒绝包时所分配给策略的操作将更改为 Send TCP RST。*[34118]*
- 无法使用 Web UI 来创建只读 Mobile VPN with IPSec 配置文件。*[39176]*

命令行界面 (CLI)

- CLI 不支持某些功能的配置。
  - 您无法添加或编辑代理操作。
  - 无法获取已加密的 Mobile VPN with IPSec 最终用户配置文件，即 .wgx 文件。CLI 仅生成纯文本版本的最终用户配置文件，文件扩展名为 .ini。
- CLI 为很多命令执行最小输入验证。
- 对于 XTM 2050，CLI 命令"show interface"的输出不会清楚指明您在 CLI 中用来配置接口的接口号。"对于所有接口，"show interface" CLI 命令将接口号显示为设备 (A0, A2 … A7; B0, B1 … B7; C0, C1) 前面的接口标签，后跟一条短横线，然后是连续的接口号 (0 – 17)。" *[64147]*

> **Workaround**
> 使用出现在短横线后面的连续接口号作为接口号来配置接口。对于 B1-9 接口，CLI 命令中的接口编号应在 8-15 之间。对于 C0-1 接口，CLI 命令中的接口编号应在 16-17 之间。

代理

- Policy Manager 和 Web UI 不提供任何关于 WebBlocker Override 可能对 HTTPS 不起作用的警告。*[67208]*
- HTTPS DPI(深度数据包检测)不适用于使用 IE 9.0(启用 TLS 1.1 和 1.2，但未启用 TLS 1.0 和 SSL 3.0) 的用户。*[65707]*

> **Workaround**
> 使用其他浏览器，或在您的 IE 9.0 配置中启用 TLS 1.0 和 SSL 3.0。

- XTM 设备仅可存储一个 HTTPS 代理服务器证书，并且一次仅能保护一个 HTTPS 网站。*[41131]*
- 当 XTM 设备处于高负载下时，有些代理连接可能错误中断。*[61925, 62503]*
- 使用 HTTP 缓存代理服务器的功能不可结合 TCP-UDP 代理使用。*[44260]*
- 您无法在 Firebox 后通过 Polycom PVX 软件电话向位于外部网络的 Polycom PVX 拨打基于 SIP 的电话。*[38567]*

> **Workaround**
> 您可以使用 H.323 协议代替 SIP。

- 当尝试从运行 iOS的 Apple设备传输 YouTube视频流时，您将看到该错误消息：服务器未正确配置。

Workaround
1. 编辑 HTTP 代理策略。
2. 单击 **视图/编辑代理**。
3. 选择 **允许通过未修改内容的范围请求** 复选框。
4. 保存对 XTM 设备的更改。

- 在联系人标头包含域名时，SIP-ALG 不会正确发送联系人标头。它只会发送一个空的字符串：联系人：< >。如果联系人标头包含 IP 地址，则 SIP-ALG 将正确发送联系人标头：Contact: <sip:10.1.1.2:5060>. *[59622]*

Workaround
配置 PBX 以发送带有 IP 地址而非域名的联系人标头。

安全订阅

- 某些 IPS 签名信息(例如 CVE 号)在 Firebox System Manager 中不可用。我们在 WatchGuard 网站上 IPS 的 Web 安全门户上提供搜索功能和 IPS 签名的 CVE 信息，访问网址为：http://www.watchguard.com/SecurityPortal/ThreatDB.aspx
- Skype 检测仅阻止新的 Skype 会话。如果在启用 Application Control 时用户已登录 Skype 且 Skype 会话已启动，Application Control 则不会检测该活动。
- 仅对于 XTM 2 Series 设备，Application Control 会在升级、备份或恢复时暂时被禁用。当操作完成后，Application Control 会再次开始工作。
- 不能通过 WatchGuard System Manager 基于角色的管理功能为 Application Control 管理分配角色。*[59204]*
- 无法通过 Branch Office VPN 隧道使用 WebBlocker Server。*[56319]*

联网

- 如果在 Fireware XTM v11.5.x 版或更早版本中手动创建动态路由选择策略，则当您升级至 v11.6 时，这些策略中的到...和从...列表将被清除。如果启用动态路由选择，则升级时将自动创建新策略。*[67721]*
- XTM 设备在桥接模式中配置时，Policy Checker 不起作用。*[66855]*
- DHCP 保留名称中存在单引号，导致 DHCP 保留失败。*[65529]*
- 无法在 VLAN 上配置数据流量管理操作或使用 Qos 标记。*[56971, 42093]*
- 无法将无线接口桥接到 VLAN 接口。*[41977]*
- 如果计算机作为 DHCP 客户端直接连接到 XTM 2 Series 设备，启动 Web Setup Wizard 时 Web Setup Wizard 可能会发生故障。出现此问题的原因在于使用向导的过程中，计算机在设备重新引导后获取 IP 地址过慢。*[42550]*

Workaround
1. 在使用 Web Setup Wizard 过程中，如要将您的计算机直接连接到 XTM 2 Series 设备，请对计算机使用静态 IP 地址。
2. 运行 Web Setup Wizard 时，在您的计算机与 XTM 2 Series 设备间使用交换机或集线器。

- 当为配置为 Drop-In 模式的 XTM 2 Series 设备配置从属网络时，可能需等待几分钟的时间使连接到从属网络的计算机出现在 XTM 2 Series 的 ARP 例表中。*[42731]*

- 您必须确保所有禁用的网络接口均未使用与任何活动的网络接口相同的 IP 地址，否则将出现活动网络接口或路由问题。*[37807]*
- 如果选中 仅允许发自或发送至这些 MAC/IP 地址的数据流量 复选框来启用 MAC/IP 绑定，但不向表中添加任何条目，则不会激活 MAC/IP 绑定功能。这样可以确保管理员不会意外地阻止自己与其 XTM 设备的连接。*[36934]*
- 当您从桥接网络中的计算机上保存配置，而该配置包含网络接口配置更改时，任何作为桥接配置一部分的网络接口均将自动断开并重新连接。*[39474]*
- 当您将配置于外部接口上的 VLAN 的 IP 地址从静态更改为 PPPoE，而 Firebox 无法获取 PPPoE 地址时，Firebox System Manager 以及 Web UI 可能会继续显示之前使用的静态 IP 地址。*[39374]*
- 在通过 混合路由模式 配置来配置 XTM 设备时，所有桥接的接口都会在 Web UI 中将其接口和默认网关 IP 地址显示为 0.0.0.0。*[39389]*
- 在以网桥模式配置 XTM 设备时，XTM 设备上 LCD 屏幕会将桥接接口的 IP 地址显示为 0.0.0.0。*[39324]*
- 当在桥接模式中配置 XTM 设备时，可通过用户接口配置 HTTP 重定向功能(本版本不支持)。*[38870]*
- 当以网桥模式配置 XTM 设备时，静态 MAC/IP 地址绑定功能将无效。*[36900*
- 在您将配置模式从混合路由更改至桥接，或由桥接更改至混合路由模式后，CLI 和 Web UI 可能仍会继续显示之前的配置模式。*[38896]*
- RIPv1 动态路由无效。*[40880]*
- 当管理员通过 Firebox System Manager > 阻止的站点"选项卡将 IP 地址添加到 临时阻止的站点"列表后，如仍接收到来自该 IP 地址的流量，则其阻止到期时间将不断重置。*[42089]*

多 WAN

- 如果 XTM 设备配置中在其 Branch Office VPN tunnel 路由启用了 1-to-1 NAT，则配置用于使用多 WAN 的 XTM 设备可能无法正确地路由传入流量。*[67001]*
- 如果您的设备配置用来使用多 WAN 路由表模式，则多 WAN 粘滞连接不起作用。*[62950]*
- 当您为 WAN 故障转移启用了多 WAN 立即故障回复选项时，某些流量可能会逐渐进行故障转移。*[42363]*

无线

- 当您使用通道 36、40、149 或 165 时，5GHz 无线频段不起作用。*[65559]*

认证

- 安装在 VMware 中的 Citrix 4.5/5/0 服务器无法通过终端服务器单一登录进行工作。*[66156]*

> **Workaround**
> 该功能只能通过 VMware 中安装的 Citrix 6.0 和 6.5 服务器进行工作。

- 在启用 TLS 的 Active Directory 环境中，不支持无客户端 SSO。
- 如果使用 Terminal Services 认证，不会对 TCP 或 UDP 以外的任何协议的数据流量进行认证。其中包括 DNS、NetBIOS 和 ICMP 数据流量。
- 无法同时使用 *自动将用户重定向到身份验证页面* 认证选项和终端服务认证选项。
- 为使 XTM 设备能正确处理来自 Terminal 或 Citrix 服务器的系统相关数据流量，Terminal Services Agent 会使用一种名为 Backend-Service 的特定用户帐户。鉴于此，您可能需要添加策略以允许来自该用户帐户的数据流量通过您的 XTM 设备。您可在产品帮助系统中了解有关 Backend-Service 运作方式的详细信息。

- 为使认证重定向功能正常运作，不能通过基于 IP 地址或包含 IP 地址的别名的传出策略来允许 HTTP 或 HTTPS 数据流量。验证重定向功能仅在用于端口 80 和 443 的策略针对用户或用户组验证进行配置后可用。*[37241]*

Centralized Management

- 无法选择在 XTM v11.x 设备配置模板中设置流量管理操作。*[55732]*
- 如果将 CentralizedManagement 与订阅早期版本 WSM 中的模板的设备一同使用，当您从 WSM 11.x 版升级至 11.4 版或更高版本时，这些模板会被更新且设备不会再订阅这些模板。每个设备都会保留其模板配置。现有设备更新后，会在其对象名称中使用“T_”(以匹配先前订阅这些模板的设备中的对象名称)。升级后，可在修订历史记录中查看升级过程中发生的模板升级。
- 当 XTM 模板应用到受管设备时，Management Server 只会在新的修订将与当前修订不同时为该设备创建一个新的配置修订。同样，也不会出现为何未创建新配置修订的反馈信息。*[57934]*

FireCluster

- 即使启用了 NTP，FireCluster 备份主控设备上的时间也可能与群集主控设备不同步。*[66134]*

> **Workaround**
> 手动同步备份主控设备的时间。连接至群集，启动 Firebox System Manager，然后选择工具 > 同步时间。此操作将群集成员的时间与管理计算机的时间同步。

- 某些交换机启用了生成树协议 (STP) 时，FireCluster 故障转移可能需要 10 秒或更长时间。*[66180]*

> **Workaround**
> 禁用交换机上的 STP，配置交换机以使用快速 STP，或使用不同的交换机。

- 升级 FireCluster 的 Fireware XTM OS 后，您可能需要重新导入 HTTPS DPI 证书。[65280]
- 您无法使用 XTM 设备接口的次要 IP 地址来管理活动/活动模式中配置的 FireCluster。*[64184]*

> **Workaround**
> 使用 XTM 设备的主要 IP 地址来处理活动/活动 FireCluster 的所有管理连接。

- 被授予权限通过基于角色的管理来监控 FireCluster 的用户无法在 Log and Report Manager 中看到 FireCluster 设备。*[65398]*
- 当 Mobile VPN with SSL 或 PPTP 被配置为使用包含群集 IP 地址的 IP 地址池时，FireCluster 备份主控设备可能变为非活动状态。*[63762]*

> **Workaround**
> 避免使用与群集 IP 地址有冲突的 IP 地址池。

- 如果无法通过管理 IP 地址访问 Log Server，则只能连接当前 FireCluster 主控设备。如果 Log Server 是通过外部网络连接的，但管理 IP 地址位于可信任网络或可选网络，则可能发生这种情况。*[64482]*

- 如果将 FireCluster 的网络配置从路由模式更改为 Drop-in 模式，然后再改回路由模式，则群集接口的 IP 地址在 Policy Manager 中显示不正确 **网络 > 配置** 对话框重新启动服务器。正确的群集接口显示在 FireCluster 配置对话框中。*[63905]*
- 在内存不足的系统中，Gateway AV 更新可能导致 FireCluster 故障转移 *[62222]*

Workaround
降低系统检查 Gateway AV 更新的频率以最大程度降低发生此情况的几率。

- 如果受监视的链路在两个 FireCluster 成员上均出现故障，非主控设备成员会切换到被动模式，因此不会处理任何数据流量。如果多 WAN 故障转移是由与链路监视器主机的连接故障所引起的，则不会触发 FireCluster 故障转移。只有在物理接口停止工作或无响应时才会发生 FireCluster 故障转移。
- 每个 XTM 设备都有分配给设备接口的一系列默认 IP 地址，范围起始值为 10.0.0.1。最大的默认 IP 地址取决于接口的数量。如果将主要或备份群集接口的 IP 地址设置为任一默认 IP 地址，则两个设备都会重新启动，且备份主控设备会变得不活动。*[57663]*

Workaround
请勿将任一默认 IP 地址用作主要或备份群集接口 IP 地址。

- 如含有主动/主动 FireCluster 并使用了 WebBlocker 替代功能，可能会提示您输入替代密码两次。*[39263]*
- FireCluster 中启用的每个网络接口会自动受 FireCluster 监视。您必须确保所有启用的接口均物理连接至网络设备。
- 如果使用 HP ProCurve 交换机，您可能无法在主动/主动模式中配置您的 FireCluster，因为这些交换机可能不支持添加静态 ARP 条目。*[41396]*
- 如果您使用来自同一网络的 Mobile VPN with IPSec 客户端作为 FireCluster 上配置的外部网络地址，则某些流量可能将不能通过 VPN 隧道。*[38672]*
- 当连接至被动 FireCluster 成员时，Mobile VPN with PPTP 用户不会出现在 Firebox System Manager 中。当使用主动/被动 FireCluster 时，PPTP 只连接到主动 Firebox。*[36467]*
- 无法将 VLAN 接口 IP 地址用于 FireCluster 管理 IP 地址。[45159]
- 要将 FireCluster 从 11.3.x 版手动升级至 11.5.1 版，管理计算机必须与 FireCluster 管理 IP 地址位于同一网络。[63278]

日志记录和报告

- 当您更改 WatchGuard Log Server 的日志级别并单击应用时，更改内容将生效。*[60088]*

Workaround
1. 在 WatchGuard Server Center 中的 Log Server 日志记录选项卡上，更改来自 Log Server 的日志消息的日志级别，并单击 **应用**。
2. 在服务器树中，右键单击 Log Server 并选择 **停止服务器**。在确认消息中，选择 **是**。
3. 再次右键单击 Log Server 并选择 **启动服务器**。

- Log and Report Manager 中的被拒绝数据包的摘要报告尚不可用。*[63192]*
- 在 Log and Report Manager 中查看时，Web 活动趋势报告的 PDF 输出在 x 轴上不包含时间标签。该报告下方的表中包括日期和时间信息。*[64162]*
- 从 Fireware XTM 11.4.x 版升级到 11.5.1 版时，在升级期间左右生成的报告可能不会显示在 Log and Report Manager 中。*[64325]*

- 如果日常报告计划名称中包含冒号或其他某些字符(例如：“1:35”)，则系统将返回一个错误。*[63427]*

Workaround
确保您的报告计划名称仅使用在 Windows 文件名中有效的字符。您可以在下列文章中找到有效字符 http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247%28v=vs.85%29.aspx。

- 在 32 位 Windows 系统上，Log Collector 达到 2GB 虚拟大小限制时会崩溃。*[64249]*
- 新的 Log and Report Manager 中有两个排序问题。按目标排序时，字段将以 IP 地址排序，而不以目标主机名称(如果可用)排序。按处置排序时，某些处于“拒绝”状态的项目在组中排序不准确。*[62879]*
- 11.3版中配置的每天或每周“存档的报告”会在升级至WSM11.4版或更高版本后自动转换为计划的报告。

Mobile VPN

- 当组名称包含星号或句号字符(*、.)时，您无法生成 Mobile VPN with IPSec 的配置文件。*[66815]*
- 如果您将 Mobile VPN with SSL 流量的诊断日志级别设为“调试”级别，将停止在 Firebox System Manager > Traffic Manager 中的日志消息显示。*[65165]*

Workaround
将 Mobile VPN with SSL 的诊断日志级别设为任何粒度低于“调试”的日志级别。

- 如果您添加了可为 XTM 设备增加 Mobile VPN with SSL 许可的新功能密钥，您必须重新引导 XTM 设备来启用额外的 Mobile VPN with SSL 用户。*[65620]*
- 当您首次将 Mobile VPN wth SSL v11.5.1 客户端连接至升级到 v11.5.2 版的 XTM 设备时，客户端升级有时会失败。*[65635]*

Workaround
手动安装 Mobile VPN with SSL 客户端。

- 当 Windows 系统帐户为中文时，您无法从基于 Windows 的计算机建立 Mobile VPN with SSL 连接。*[58208]*
- 使用来自 iPhone 或 iPad 的内置 IPSec 客户端时，客户端连接的持续时间达到 1 小时 45 分钟时将中断连接。这是由 iPhone/iPad 所用的 Cisco 客户端存在的限制所造成的。必须重新连接 IPSec 客户端来重新建立 VPN 隧道。*[63147]*
- 来自 Android 移动设备的 Mobile VPN with PPTP 连接无法在 3G 手机网络上持续有效。*[63451]*
- 当 XTM 设备具有多 WAN 配置(采用循环法模式)时，来自 Mobile VPN with IPSec 客户端的连接可能通过错误的外部接口路由。*[64386]*
- 您不能配置 Mobile VPN with SSL 将网络流量桥接到桥接接口。*[61844]*
- Mobile VPN with SSL 用户不能通过终结于主动/主动 FireCluster 的分支机构 VPN 隧道连接到某些网络资源。*[61549]*
- 如果在 XTM 设备接口与 Shrew Soft VPN 客户端之间建立了一条 VPN 隧道，则将无法 ping 此接口的 IP 地址。您可以 ping 位于该网络上的计算机，但不能 ping 此接口 IP 地址本身。*[60988]*

- 如果有多个同时连接到 XTM 设备的 Shrew Soft VPN 客户端发出第 2 阶段的重新生成密钥，则客户端连接可能中断。*[60261*]
- Shrew Soft VPN 客户端发出的第 1 阶段重新生成密钥会导致客户端中断连接(如果连接时间超过 24 小时)。在这种情况下，我们建议您将 XTM 设备上的重新生成密钥设置为 23 小时，比 Shrew Soft 客户端配置中通过硬编码设置的重新生成密钥少一小时。这将强制 XTM 设备发出重新生成密钥，并向客户端提供必须重新建立隧道的通知。*[60260, 60259]*
- 如在 FTP 传输期间发生 IPSec 重新生成密钥事件，Mobile VPN with IPSec 连接上的连续 FTP 会话将终止。*[32769]*

Workaround
增加重新生成密钥字节计数。

- 当认证算法设置为 SHA 256 时，Mobile VPN for SSL Mac 客户端可能无法连接到 XTM 设备。*[35724]*

Branch Office VPN

- 预共享密钥超过 50 个字符时，手动 Branch Office VPN 将出现故障。*[65215]*
- VPN 网关和 VPN 隧道请勿使用相同的名称。*[66412]*
- 您不可以在 Branch Office VPN 隧道中使用长度超过 50 个字符的预共享密钥。*[65215]*
- 在以多 WAN 模式配置 XTM 设备时，您必须选择要包含在多 WAN 配置中的接口。如果选择了某个接口使其不包含在多 WAN 配置中(即，清除了该接口的复选框)，系统不会为该网络创建路由。如果已将 Branch Office VPN 配置为包含同一接口，则会产生问题。在此情况下，VPN 隧道无法与其远程对等方进行协商。*[57153]*

Workaround
如果使用多 WAN 且 Branch Office VPN 隧道存在无法与其远程对等方协商，必须打开多 WAN 配置并选择所选多 WAN 配置模式旁边的配置。确保相应的接口已包含在多 WAN 配置中。

- 如果 XTM 设备的外部 IP 地址中存在包含 IP 50 和 IP 51 协议的入站静态 NAT 策略，则 Branch Office VPN 隧道不会传递数据流量。[*41822]*
- 当 CRL 分发点(如 WatchGuard Management Server 或您使用的第三方分发站点)离线时，将无法建立托管 Branch Office VPN 隧道。*[55946]*
- BOVPN 隧道路由 *任何* 在 Fireware XTM 中已更改。如果 Branch Office VPN 隧道为隧道路由的本地部分使用了“任意”，则 Fireware XTM 将其解释为网络 0.0.0.0 以及子网掩码 0.0.0.0(以斜线记法为 0.0.0.0/0)。如远程 IPSec 对等端未将 0.0.0.0/0 作为其第 2 阶段 ID 发送，第 2 阶段协商将失败。*[40098]*

Workaround
请勿将 *任何* 用于隧道路由的本地”或远程”部分。更改您隧道路由的本地部分。键入实际参与到隧道路由的 XTM 设备背后的计算机的 IP 地址。联系远程 IPSec 对等端的管理员，以确定其隧道路由的远程部分(或其第 2 阶段 ID 的远程部分)使用了何种设备。

- 如果在您的配置中存在较大数量的 Branch Office VPN 隧道，在 Policy Manager 中显示这些隧道可能会花费较长时间。*[35919]*

Workaround
在 Policy Manager 中，选择 **查看 > 策略突出显示**。根据 **流量类型清除突出显示的防火墙策略** 复选框。

使用 CLI

11.x 版本完全支持 Fireware XTM CLI(命令行接口)。有关如何启动和使用 CLI 的信息，请参阅 *CLI 命令参考指南*。您可在文档网站上下载该 CLI 指南，网址为：
http://www.watchguard.com/help/documentation/xtm.asp。

技术支持

如需技术支持，请致电 WatchGuard Technical Support，也可登录 WatchGuard 门户网站，网址是：
http://www.watchguard.com/support。联系技术支持时，必须提供您注册的产品序列号或合作伙伴 ID。

	电话号码
美国最终用户	877.232.3531
国际最终用户	+1 206.613.0456
得到授权的 WatchGuard 分销商	206.521.8375

French (Français)

Notes de Version de Fireware XTM v11.6.1

Périphériques Pris en Charge	XTMv, XTM 2, 3, 5 et 8 Series XTM 1050, XTM 2050
Version du Système d'Exploitation Fireware XTM	346666
Génération de WatchGuard System Manager	347361
Date de révision	8 août 2012

Introduction

WatchGuard a le plaisir d'annoncer la parution de Fireware XTM v11.6.1 et de WatchGuard System Manager v11.6.1. Vous pouvez installer le système d'exploitation Fireware XTM v11.6.1 sur n'importe quel périphérique XTM WatchGuard, y compris les périphériques 2 Series, 3 Series, 5 Series, 8 Series, XTM 1050 et 2050, et sur toutes les versions de XTMv. Cette version prend en charge les nouveaux périphériques ultra performants XTM 5 Series, modèles 515, 525, 535 et 545. Elle permet de mettre à jour nos interfaces utilisateur localisées et leur documentation. Cette version contient également plusieurs améliorations importantes du produit :

- Un périphérique XTM configuré en mode pont permet désormais le passage du trafic marqué réseau local virtuel (VLAN) entre des commutateurs ou ponts 802.1Q.
- Prise en charge de FireCluster pour les modèles câblés XTM 25, 26 et 33.

Enfin, plusieurs correctifs de bogues sont proposés dans cette version. Ils sont décrits dans la section Problèmes Résolus.

Pour de plus amples informations sur les fonctionnalités améliorées par Fireware XTM v11.6.1, lisez la documentation relative au produit ou consultez Nouveautés de Fireware XTM v11.6.1.

Avant de Commencer

Avant d'installer cette version, vérifiez que vous disposez des éléments suivants :

- Un périphérique WatchGuard XTM 2 Series, 3 Series, 5 Series, 8 Series, XTM 1050, XTM 2050 ou XTMv (toutes versions).
- Les composants matériels et logiciels requis, illustrés dans le tableau ci-dessous. Si vous utilisez WatchGuard System Manager (WSM), assurez-vous que votre version de WSM est égale ou supérieure à celle du système d'exploitation Fireware XTM installé sur votre périphérique XTM et à la version de WSM installée sur votre Management Server.
- Clé de fonctionnalité pour votre périphérique XTM : si vous faites une mise à niveau de votre périphérique XTM à partir d'une version antérieure du système d'exploitation Fireware XTM, vous pouvez utiliser la clé de fonctionnalité existante. Si vous utilisez XTMv, votre clé de fonctionnalité doit être générée à partir du numéro de série que vous avez reçu lors de l'achat de XTMv.

Remarque : vous pouvez installer et utiliser WatchGuard System Manager v11.6.1 et tous les composants de serveur WSM avec des périphériques fonctionnant sous des versions antérieures de Fireware XTM v11. Dans ce cas, nous vous recommandons d'utiliser la documentation du produit qui correspond à la version de votre système d'exploitation Fireware XTM.

Si vous avez un nouveau périphérique physique XTM, assurez-vous de suivre les instructions du *Guide de démarrage rapide XTM* livré avec votre périphérique. S'il s'agit d'une nouvelle installation de XTMv, lisez attentivement le *Guide de configuration de XTMv* qui contient d'importantes consignes concernant son installation et sa configuration.

La documentation pour ce produit est disponible sur le site Web de WatchGuard à l'adresse www.watchguard.com/help/documentation.

Localisation

Cette version comprend la mise à jour et la localisation des interfaces utilisateur de gestion de Fireware XTM (suite d'applications WSM et Web UI) et de l'aide du produit. Les langues suivantes sont prises en charge :

- Chinois (simplifié, RPC)
- Français (France)
- Japonais
- Espagnol (Amérique latine)

> ***Note*** *Outre ces langues, nous offrons une prise en charge de l'interface Web UI en coréen et en chinois traditionnel. Uniquement l'interface Web UI a été localisée. WSM, les fichiers d'aide et la documentation utilisateur restent en anglais pour ces deux langues.*

Notez que la plupart des saisies de données doivent encore être effectuées avec des caractères ASCII standard. Vous pouvez utiliser des caractères non ASCII dans certaines zones de l'interface, notamment pour les zones suivantes :

- message de refus du proxy ;
- titre, conditions générales et message relatifs au hotspot sans fil ;
- noms d'utilisateurs WatchGuard Server Center, de groupes et de rôles

Toutes les données renvoyées à partir du système d'exploitation du périphérique (par exemple, des données de journal) sont affichées uniquement en anglais. De plus, tous les éléments du menu d'état du système Web UI et tous les composants logiciels fournis par des entreprises tierces restent en anglais.

Fireware XTM Web UI

L'interface Web UI démarre par défaut dans la langue que vous avez définie dans votre navigateur Web. La langue sélectionnée apparaît en haut de chaque page. Pour changer la langue, cliquez sur le nom de langue qui s'affiche. Une liste déroulante s'affiche et vous pouvez y sélectionner la langue que vous souhaitez utiliser.

WatchGuard System Manager

Lorsque vous installez WSM, vous pouvez sélectionner les packs de langues que vous souhaitez installer. La langue affichée dans WSM correspond à celle que vous sélectionnez dans votre environnement Microsoft Windows. Par exemple, si vous utilisez Windows XP et que vous souhaitez utiliser WSM en Japonais, accédez à Panneau de configuration > Options régionales et linguistiques, puis sélectionnez Japonais dans la liste de langues.

Log and Report Manager, CA Manager, Quarantine Web UI et Point d'accès sans fil

Ces pages Web s'affichent automatiquement dans la langue que vous avez définie dans votre navigateur Web.

Compatibilité des Systèmes d'Exploitation – Fireware XTM et WSM v11.6.1

Révisé en juin 2012

WSM/ Composant de Fireware XTM	Microsoft Windows XP SP2 (32 bits)	Microsoft Windows Vista (32 bits et 64 bits)	Microsoft Windows 7 (32 bits et 64 bits)	Microsoft Windows Server 2003 (32 bits)	Microsoft Windows Server 2008 et 2008 R2*	Mac OS X v10.5, v10.6 et v10.7
Application WSM (WatchGuard System Manager)	✓	✓	✓	✓	✓	
Fireware XTM Web UI *Navigateurs pris en charge : IE 7 et 8, Firefox 3.x et versions ultérieures*	✓	✓	✓	✓	✓	✓
Log and Report Manager Web UI *Navigateurs pris en charge : Firefox 3.5 et versions ultérieures, IE 8 et versions ultérieures, Safari 5.0 et versions ultérieures, Chrome 10 et versions ultérieures. JavaScript requis.*	✓	✓	✓	✓	✓	✓
Serveurs WatchGuard	✓	✓	✓	✓	✓	
Logiciel agent Single Sign-On (SSO) (Inclut Event Log Monitor)				✓	✓	
Logiciel client Single Sign-On (SSO)	✓	✓	✓	✓	✓	
Logiciel agent Terminal Services**				✓ ***	✓	
Logiciel client Mobile VPN with IPSec	✓	✓	✓			Le client IPSec natif (Cisco) est pris en charge
Logiciel client Mobile VPN with SSL	✓	✓	✓	✓		✓

** Prise en charge de Microsoft Windows Server 2008 32 bits et 64 bits ; ainsi que de Windows Server 2008 R2 64 bits.*

*** La prise en charge de Terminal Services avec authentification manuelle ou Single Sign-On fonctionne dans un environnement Microsoft Terminal Services ou Citrix XenApp 4.5, 5.0, 6.0 et 6.5.*

**** Microsoft Windows Server 2003 SP2 requis.*

Prise en charge de l'authentification

Ce tableau vous donne un aperçu des types de serveurs d'authentification pris en charge par les principales fonctionnalités de Fireware XTM. Le fait d'utiliser un serveur d'authentification vous permet de configurer des stratégies de pare-feu et de réseaux privés virtuels (VPN) basées sur les utilisateurs et sur des groupes dans la configuration de votre périphérique XTM. Pour chaque type de serveur d'authentification tierce pris en charge, vous pouvez indiquer l'adresse IP d'un serveur de sauvegarde pour le basculement.

✓ : entièrement pris en charge par WatchGuard

 : pas encore pris en charge, mais testé avec succès par les clients de WatchGuard

	Active Directory[1]	LDAP	RADIUS[2]	SecurID[2]	Firebox (Firebox-DB) Authentification locale
Mobile VPN with IPSec/Shrew Soft	✓	✓	✓3	–	✓
Mobile VPN with IPSec pour iPhone/iPad iOS et Mac OS X				✓	✓
Mobile VPN with SSL pour Windows	✓	✓	✓4	✓4	✓
Mobile VPN with SSL pour Mac	✓	✓	✓	✓5	✓
Mobile VPN with PPTP	–	–	✓	N.A.	✓
Page Web d'authentification intégrée sur le port 4100	✓	✓	✓	✓	✓
Prise en charge de Windows Single Sign-On (avec ou sans logiciel client)	✓	–	–	–	–
Authentification manuelle des Terminal Services	✓				✓
Authentification Terminal Services avec SSO (Single Sign-On).	✓6	–	–	–	–
Authentification manuelle de Citrix					✓

1. *La prise en charge d'Active Directory est valable pour les domaines uniques et les multidomaines, sauf mention contraire.*
2. *La prise en charge de RADIUS et de SecurID comprend les mots de passe à usage unique et l'authentification des défis/réponses intégrés à RADIUS. La plupart du temps, SecurID peut également être utilisé avec d'autres implémentations RADIUS, dont Vasco.*
3. *Le client Shrew Soft n'est pas compatible avec l'authentification à deux facteurs.*
4. *Fireware XTM prend en charge l'attribut FilterID 11 de RADIUS pour l'authentification groupée.*
5. *Le mode PIN + code de jeton est pris en charge. Le mode prochain code de jeton et les mots de passe à usage unique par SMS ne sont pas pris en charge.*
6. *Seules les configurations Active Directory pour domaine unique sont prises en charge.*

7. *Pour de plus amples informations sur les systèmes d'exploitation compatibles avec WatchGuard TO Agent et SSO Agent, reportez-vous au tableau actuel de compatibilité des systèmes d'exploitation de Fireware XTM et WSM.*

Configuration requise pour XTMv

Pour installer un périphérique virtuel XTMv, un hôte VMware ESXi 4.1 ou 5.0 doit être installé sur un serveur compatible avec la version d'ESXi que vous utilisez. Vous devez également installer VMware vSphere Client 4.1 ou 5.0 sur un ordinateur Windows compatible. Si vous préférez, vous pouvez utiliser vSphere Server au lieu de vSphere Client.

Le matériel requis pour XTMv est le même que pour VMware ESXi. Pour de plus amples informations concernant la compatibilité du matériel VMware, reportez-vous au Guide de compatibilité de VMware, à l'adresse http://www.vmware.com/resources/compatibility/search.php.

Chaque machine virtuelle XTMv nécessite 3 Go d'espace libre.

Paramètres recommandés d'attribution des ressources

	Petit bureau	Moyen bureau	Grand bureau	Centre de données
Processeurs virtuels	1	2	4	8 ou plus
Mémoire	1 Go	2 Go	4 Go	4 Go ou plus

Téléchargement du Logiciel

1. Connectez-vous au Portail WatchGuard et sélectionnez l'onglet Articles et logiciels.
2. Dans la section Recherche, décochez les cases Articles et Problèmes connus et recherchez les téléchargements de logiciels disponibles. Sélectionnez le périphérique pour lequel vous souhaitez télécharger le logiciel.

Plusieurs fichiers de logiciel sont disponibles au téléchargement. Consultez les descriptions pour connaître les packages logiciels dont vous avez besoin pour votre mise à niveau.

WatchGuard System Manager

Tous les utilisateurs peuvent télécharger le logiciel WatchGuard System Manager. Grâce à ce package logiciel, vous pouvez installer WSM et le logiciel WatchGuard Server Center :

`WSM11_6_1s.exe` : utilisez ce fichier pour mettre à niveau WatchGuard System Manager de v11.x vers WSM v11.6.1.

Système d'exploitation Fireware XTM

Sélectionnez l'image du système d'exploitation Fireware XTM correspondant à votre périphérique XTM. Utilisez le fichier EXE si vous voulez installer ou mettre à niveau le système d'exploitation à l'aide de WSM. Utilisez le fichier ZIP si vous voulez installer ou mettre à niveau le système d'exploitation à l'aide de Fireware XTM Web UI. Utilisez le fichier OVA pour déployer un nouveau périphérique XTMv.

Si vous avez….	Sélectionnez parmi ces packages de système d'exploitation Fireware XTM
XTM 2050	`XTM_OS_XTM2050_11_6_1.exe` `xtm_xtm2050_11_6_1.zip`
XTM 1050	`XTM_OS_XTM1050_11_6_1.exe` `xtm_xtm1050_11_6_1.zip`
XTM 8 Series	`XTM_OS_XTM8_11_6_1.exe` `xtm_xtm8_11_6_1.zip`
XTM 5 Series	`XTM_OS_XTM5_11_6_1.exe` `xtm_xtm5_11_6_1.zip`
XTM 330	`XTM_OS_XTM330_11_6_1.exe` `xtm_xtm330_11_6_1.zip`
XTM 33	`XTM_OS_XTM33_11_6_1.exe` `xtm_xtm33_11_6_1.zip`
XTM 2 Series Modèles 21, 22, 23	`XTM_OS_XTM2_11_6_1.exe` `xtm_xtm2_11_6_1.zip`
XTM 2 Series Modèles 25, 26	`XTM_OS_XTM2A6_11_6_1.exe` `xtm_xtm2a6_11_6_1.zip`

XTMv
Toutes versions
	`xtmv_11_6_1.ova`
	`xtmv_11_6_1.exe`
	`xtmv_11_6_1.zip`

Logiciel Single Sign-on (SSO)

Deux fichiers sont disponibles au téléchargement pour les utilisateurs de Single Sign-On.

- `WG-Authentication-Gateway_11_6.exe` (logiciel SSO Agent : requis pour Single Sign-on, inclut Event Log Monitor en option pour Clientless SSO)
- `WG-Authentication-Client_11_6.msi` (logiciel client SSO, facultatif)

Pour plus d'informations sur l'installation et la configuration de Single Sign-On, consultez la documentation du produit.

Logiciel d'authentification Terminal Services

- `TO_AGENT_32_11_6.exe` (prise en charge 32 bits)
- `TO_AGENT_64_11_6.exe` (prise en charge 64 bits)

Client Mobile VPN with SSL pour Windows et Mac

Deux fichiers sont disponibles au téléchargement pour les utilisateurs de Mobile VPN with SSL :

- `WG-MVPN-SSL_11_6.exe` (Logiciel client pour Windows)
- `WG-MVPN-SSL_11_6.dmg` (Logiciel client pour Mac)

Client Mobile VPN with IPSec pour Windows

Vous pouvez télécharger le client Shrew Soft VPN pour Windows depuis notre site Web. Pour de plus amples informations concernant le client Shrew Soft VPN, consultez l'aide ou rendez-vous sur le site Web de Shrew Soft, Inc..

Mise à Niveau de Fireware XTM v11.x vers v11.6.1

Avant toute mise à niveau de Fireware XTM v11.x vers Fireware XTM v11.6.1, téléchargez et enregistrez le fichier du système d'exploitation de Fireware XTM qui correspond au périphérique WatchGuard que vous souhaitez mettre à niveau. Vous pouvez consulter tous les logiciels disponibles sur le Portail WatchGuard, à l'onglet Articles et logiciels. Vous pouvez utiliser Policy Manager ou Web UI pour terminer la procédure de mise à niveau. Nous vous conseillons vivement de sauvegarder la configuration de votre périphérique et la configuration de votre WatchGuard Management Server avant la mise à niveau. Il serait impossible de revenir à la version antérieure sans ces fichiers de sauvegarde.

Si vous utilisez WatchGuard System Manager (WSM), assurez-vous que votre version de WSM est égale ou supérieure à celle du système d'exploitation Fireware XTM installé sur votre périphérique XTM et à la version de WSM installée sur votre Management Server.

> ***Note*** *Si vous migrez vers WSM v11.6.1 à partir de WSM v11.4.x ou d'une version antérieure, il est important de sauvegarder les données de Log Server et Report Server selon la procédure décrite dans l'article 6995 de la base de connaissances. Cette étape est nécessaire, car la structure des bases de données Log Server et Report Server a été modifiée dans WSM v11.5.1. Lorsque vous migrez vers WSM v11.5.1 ou une version ultérieure pour la première fois, les horodatages des données de journal et de rapport existantes sont convertis de votre fuseau horaire local en UTC. Cet article de la base de connaissances vous fournit les détails de cette mise à niveau, ainsi que des informations importantes sur Log and Report Manager (nouveauté de WSM v.11.5.1).*

Sauvegarder votre configuration WatchGuard Management Server

Depuis l'ordinateur où vous avez installé le Management Server :

1. Dans WatchGuard Server Center, sélectionnez **Sauvegarde/Restauration de Management Server**.
   L'Assistant WatchGuard Server Center Backup/Restore Wizard démarre.
2. Cliquez sur **Suivant**.
   L'écran de sélection d'une action s'affiche.
3. Sélectionnez **Paramètres de sauvegarde**.
4. Cliquez sur **Suivant**.
   L'écran Spécifier un fichier de sauvegarde s'ouvre.
5. Cliquez sur **Parcourir** pour sélectionner un emplacement pour le fichier de sauvegarde. Assurez-vous d'enregistrer le fichier de configuration à un emplacement auquel vous pourrez accéder plus tard pour rétablir le fichier de configuration.
6. Cliquez sur **Suivant**.
   L'écran indiquant que l'Assistant WatchGuard Server Center Backup/Restore Wizard a terminé s'affiche.
7. Cliquez sur **Terminer** pour quitter l'Assistant.

Mise à niveau vers Fireware XTM v11.6.1 depuis l'interface Web UI

1. Allez dans **Système > Image de sauvegarde** ou utilisez la fonction de sauvegarde USB pour sauvegarder votre fichier de configuration actuel.

2. Sur votre ordinateur de gestion, lancez le fichier exécutable du système d'exploitation que vous avez téléchargé à partir du centre de téléchargement de logiciels WatchGuard.
   Si vous utilisez le programme d'installation Windows, cette installation extrait un fichier de mise à niveau appelé *[série xtm]_[code produit].sysa-dl* l dans l'emplacement par défaut de C:\Program Files (x86)\Common files\WatchGuard\resources\FirewareXTM\11.6.1\[modèle] ou [modèle][code_produit].
3. Connectez-vous à votre périphérique XTM à l'aide de l'interface Web UI et sélectionnez **Système > Mettre à niveau le système d'exploitation**.
4. Accédez à l'emplacement du fichier *[série xtm]_[code produit].sysa-dl* de l'étape 2 et cliquez sur **Mettre à niveau**.

Mise à niveau vers Fireware XTM v11.6.1 depuis WSM/Policy Manager v11.x

1. Sélectionnez **Fichier > Sauvegarder** ou utilisez la fonction de sauvegarde USB pour sauvegarder votre fichier de configuration actuel.
2. Sur votre ordinateur de gestion, lancez le fichier exécutable du système d'exploitation que vous avez téléchargé depuis le Portail WatchGuard. Cette installation extrait un fichier de mise à niveau appelé *[série xtm]_[code produit].sysa-dl* l dans l'emplacement par défaut de C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\11.6.1\[modèle] ou [modèle][code_produit].
3. Installez et ouvrez WatchGuard System Manager v11.6.1. Connectez-vous à votre périphérique XTM et démarrez Policy Manager.
4. Dans Policy Manager, sélectionnez **Fichier > Mettre à niveau**. À l'invite, accédez au fichier *[série xtm] _[code produit].sysa-dl* de l'étape 2.

Informations générales concernant les mises à niveau logicielles de WatchGuard Server

Il n'est pas nécessaire de désinstaller votre ancien serveur v11.x ou logiciel client lorsque vous procédez à une mise à niveau de v11.0.1 ou d'une version ultérieure vers WSM v11.6.x. Vous pouvez installer le serveur v11.6.x et le logiciel client par-dessus l'installation existante pour mettre à niveau les composants de votre logiciel WatchGuard.

Mise à Niveau de votre FireCluster vers Fireware XTM v11.6.1

Il existe deux méthodes pour mettre à niveau le système d'exploitation Fireware XTM sur votre FireCluster. La méthode à suivre dépend de la version du Fireware XTM que vous utilisez actuellement.

Mise à niveau de FireCluster depuis Fireware XTM v11.4.x ou v11.5.x

Suivez la procédure décrite ci-dessous pour mettre à niveau un FireCluster depuis Fireware XTM v11.4.x ou v11.5.x vers Fireware XTM v11.6.x :

1. Ouvrez le fichier de configuration du cluster dans Policy Manager.
2. Sélectionnez **Fichier > Mettre à niveau**.
3. Tapez le mot de passe de configuration.
4. Entrez ou sélectionnez l'emplacement du fichier de mise à niveau.
5. Pour créer une image de sauvegarde, sélectionnez **Oui**.
   Une liste des membres du cluster s'affiche.
6. Activez la case à cocher correspondant à chaque périphérique que vous souhaitez mettre à niveau.
   Un message s'affiche une fois la mise à niveau terminée pour chaque périphérique.

Une fois la mise à niveau terminée, chaque membre du cluster redémarre et rejoint le cluster. Si vous mettez à jour les deux périphériques du cluster au même moment, les périphériques sont mis à niveau individuellement. Ce système permet d'éviter les interruptions d'accès au réseau au cours de la mise à niveau.

Policy Manager met d'abord à niveau le membre de sauvegarde, puis attend qu'il ait redémarré et rejoint le cluster en tant que sauvegarde. Ensuite, il met à niveau le maître. Remarque : le rôle du maître n'est pas modifié tant que le système n'a pas redémarré pour terminer le processus de mise à niveau. C'est alors que le membre de sauvegarde prend le rôle du maître.

Pour procéder à une mise à niveau à distance, assurez-vous que l'interface FireCluster de l'adresse IP de gestion est configurée sur l'interface externe et que les adresses IP de gestion sont publiques et routables. Pour plus d'informations, voir À propos de l'interface pour l'adresse IP de gestion.

Mise à niveau de FireCluster depuis Fireware XTM v11.3.x

Pour mettre à niveau un FireCluster depuis Fireware XTM v11.3.x vers Fireware XTM v11.6.x, vous devez effectuer une mise à niveau manuelle. Pour connaître la procédure à suivre pour une mise à niveau manuelle, consultez l'article de la base de connaissances intitulé Mise à niveau du système d'exploitation Fireware XTM pour un FireCluster.

Instructions de Rétrogradation

Rétrogradation de WSM v11.6.x à WSM v11.x

Si vous souhaitez revenir de la version v11.6.x à une version antérieure de WSM, vous devez désinstaller WSM v11.6.x. Lors de la désinstallation, choisissez **Oui** lorsque le programme demande si vous voulez supprimer les fichiers de données et de configuration du serveur. Une fois les fichiers de données et de configuration serveur supprimés, vous devez restaurer les fichiers de données et de configuration serveur sauvegardés avant la mise à niveau vers WSM v11.6.x.

Ensuite, installez la même version de WSM que vous aviez utilisée avant la mise à niveau vers WSM v11.6.x. Le programme d'installation devrait détecter votre configuration de serveur existante et essayer de redémarrer vos serveurs depuis la **boîte de dialogue** Terminer. Si vous utilisez un WatchGuard Management Server, utilisez WatchGuard Server Center pour restaurer la sauvegarde de la configuration du Management Server que vous aviez créée lors de votre première mise à niveau vers WSM v11.6.x. Vérifiez que tous les serveurs WatchGuard fonctionnent.

Rétrogradation de Fireware XTM v11.6.x à Fireware XTM v11.x

> ***Note*** *Vous ne pouvez pas rétrograder un XTM 2050, un XTM 330 ou un XTM 33 vers une version du système d'exploitation Fireware XTM antérieure à v11.5.1. Vous ne pouvez pas rétrograder un XTM 5 Series modèle 515, 525, 535 ou 545 vers une version du système d'exploitation Fireware XTM antérieure à v11.6.1. Vous ne pouvez pas rétrograder XTMv vers une version du système d'exploitation Fireware XTM antérieure à v11.5.4.*

Si vous souhaitez revenir de la version Fireware XTM v11.6.x à une version antérieure de Fireware XTM, vous devez :

- Restaurer l'image de sauvegarde complète que vous avez créée lors de la mise à niveau vers Fireware XTM v11.6.x pour terminer la rétrogradation ; ou
- Utiliser le fichier de sauvegarde USB que vous aviez créé avant la mise à niveau en tant qu'image d'auto-restauration, puis redémarrer en mode récupération avec le lecteur USB branché à votre périphérique. Cela ne concerne pas les utilisateurs de XTMv.

Pour démarrer un périphérique WatchGuard XTM 330, 5 Series, 8 Series, XTM 1050 ou XTM 2050 en mode de récupération, procédez comme suit :

1. Mettez le périphérique XTM hors tension.
2. Pendant que vous mettez le périphérique sous tension, appuyez sur le bouton fléché vers le haut sur le panneau avant du périphérique.
3. Maintenez le bouton enfoncé jusqu'à ce que le message Démarrage du mode récupération apparaisse sur l'affichage LCD.

Pour démarrer un périphérique WatchGuard XTM 2 Series ou XTM 33 en mode récupération :

1. Débranchez l'alimentation.
2. Maintenez enfoncé le bouton de réinitialisation situé à l'arrière du périphérique pendant que vous le mettez sous tension.
3. Assurez-vous que le témoin du bouton Attn devienne orange fixe avant de relâcher le bouton.

Problèmes Résolus

La version Fireware XTM v11.6.1 résout de nombreux problèmes rencontrés sur les versions Fireware XTM v11.x antérieures :

Général

- Résolution de plusieurs problèmes provoquant le plantage des périphériques XTM que l'on configurait pour utiliser Application Control ou IPS. *[66937, 65426, 65636, 67312, 66135, 67159, 67399, 67310]*
- Résolution d'un problème qui entraînait le plantage de certains processus du périphérique XTM lorsque l'on exécutait le test de vulnérabilité publiée par défaut Mu Dynamics. *[66490]*
- Résolution d'un problème qui provoquait le plantage du noyau et le redémarrage de l'appareil. *[67329]*
- Le périphérique XTM 2 Series peut désormais gérer le transfert d'un fichier volumineux sans compromettre la stabilité de l'interface. *[67367]*
- Résolution d'un problème qui entraînait l'apparition de données erronées sur l'affichage LCD du périphérique XTM 5 Series. *[67197]*

WatchGuard System Manager

- Policy Manager affiche désormais correctement les limites du réseau local virtuel (VLAN) sur les modèles 505, 510, 520 et 530 du XTM 5 Series avec une clé de fonctionnalité Fireware XTM standard (non Pro). *[67780]*

Web UI

- Vous pouvez désormais configurer et appliquer des actions de gestion du trafic sur les périphériques XTM 2 Series et 3 Series à partir de l'interface Web UI. *[67221, 66645]*

Centralized Management

- Les périphériques Firebox X Edge e-Series peuvent désormais être gérés avec des modèles. *[67658]*

Journalisation et génération de rapports

- Le message de notification envoyé lorsqu'une base de données Log Server ou Report Server locale ne fonctionne pas affiche à présent l'adresse IP hôte au lieu de « ??? ». *[41731]*
- Log Server peut désormais gérer les fichiers de sauvegarde de plus de 2 Go sans générer le message d'erreur : « Erreur (8199), Exception lors de la sauvegarde des données de journal les plus anciennes : Le fichier n'est pas un fichier zip. » *[66811]*
- Le rapport d'activité du bail DHCP fonctionne désormais comme il faut. *[66062]*
- Log Collector sait maintenant gérer les données de journal des périphériques XTM réparties sur plusieurs enregistrements SSL/TLS. *[66347]*

Proxies et services de sécurité

- Résolution d'un problème qui détériorait les performances des modèles 25 et 26 du XTM 2 Series en raison d'une attribution de mémoire inadaptée pour les signatures de sécurité par abonnement. *[67240]*
- Un message de refus est maintenant envoyé aux navigateurs Web dans la majorité des cas lorsqu'Application Control bloque un contenu de la catégorie Web/Web 2.0. *[66201]*
- Suppression du décalage d'une heure de la mise à jour automatique de la base de données WebBlocker, qui se produisait sur le serveur hôte pendant l'application de l'heure d'été. *[67551]*

Mise en réseau

- Si vous utilisez le protocole PPPoE ou DHCP pour l'interface externe d'un périphérique XTM configuré pour utiliser le multi-WAN, le périphérique ne perd plus les routes par défaut des interfaces externes après la reconnexion de l'interface externe. *[67424, 67520]*
- Résolution d'un problème qui entraînait l'échec des routes statiques lorsqu'une interface externe configurée pour utiliser PPPoE était déconnectée, puis reconnectée. *[67520]*
- Le trafic marqué réseau local virtuel (VLAN) est à présent reconnu correctement lorsqu'un périphérique XTM est configuré en mode pont. *[64355]*

Command Line Interface

- La commande de Command Line Interface « restore factory default all » rétablit désormais correctement les paramètres usine par défaut du périphérique. *[66240]*

FireCluster

- Résolution d'un problème à cause duquel Policy Manager affichait à tort une adresse IP d'interface 0.0.0.0/24 lorsque l'on consultait la configuration FireCluster d'un cluster en mode d'insertion. *[63551]*

Mobile VPN

- Le processus Mobile VPN with SSL ne plante plus après un basculement FireCluster. *[66118]*

Problèmes et Restrictions Connus

À l'instar de toutes les applications de gestion, Fireware XTM v11.6.1 a des problèmes connus. Quand cela est possible, nous proposons un moyen pour contourner le problème.

Général

- Lorsque vous branchez un lecteur USB sur un périphérique XTM, le périphérique n'enregistre pas automatiquement de cliché de support unique sur le lecteur USB. *[64499]*

> **Workaround**
> Utilisez la commande Command Line Interface « usb diagnostic enable » afin que le périphérique enregistre un cliché de support de diagnostic sur le lecteur USB. Pour plus d'informations concernant cette commande, reportez-vous au *Guide de référence de Command Line Interface*.

- La version « Sysb » indiquée dans le rapport d'état de Firebox System Manager sera vierge pour les modèles XTM 2, 5, 8 et 1050 qui ont été conçus avant la sortie du XTM v11.5.1.
- La protection contre les attaques ICMP Flood fonctionne différemment dans la version 11.5.1 par rapport aux versions antérieures. Dans la version v11.5.1, le périphérique XTM calcule le nombre de demandes et de réponses ping, et non simplement le nombre de demandes ping. Dans la mesure où le seuil par défaut de protection contre les attaques ICMP Flood n'a pas augmenté, la protection peut se déclencher plus fréquemment que dans les versions antérieures. *[63094]*

> **Workaround**
> Dans les paramètres Gestion des paquets par défaut, augmentez le seuil par défaut de « Drop ICMP Flood Attack » (qui est de 1 000 paquets/seconde par défaut).

- Lorsque le niveau de mémoire libre sur votre périphérique XTM est inférieur à 20 Mo, l'enregistrement de la configuration de votre périphérique XTM sur le périphérique peut provoquer une interruption du réseau. *[64474]*
-
- L'interface ETH1 du XTM 830F étant un port pour fibre optique, vous ne pouvez pas utiliser le WSM Quick Setup Wizard depuis un ordinateur doté d'une interface Ethernet. Utilisez un ordinateur doté d'une carte réseau fibre, ou connectez-vous à l'aide d'un commutateur entre les interfaces fibre et Ethernet. *[59742]*
- Pour éteindre un périphérique XTM 5 Series, vous devez appuyer sur le bouton marche/arrêt et le maintenir enfoncé pendant 4 à 5 secondes. *[42459]*
- Sur les périphériques XTM 5 Series, l'interface 0 ne prend pas en charge Auto-MDIX et ne polarise pas automatiquement le câble.
- Sur les périphériques XTM 2 Series, la charge moyenne affiche toujours 1 au minimum, même s'il n'y a aucune charge sur le périphérique. *[63898]*
- Le démarrage d'un périphérique XTM 2 Series peut durer 5 minutes.
- Lorsque vous recourez aux fonctionnalités **Policy Manager > Fichier > Sauvegarde** ou **Restaurer,** le processus peut prendre un certain temps avant son achèvement. *[35450]*
- Vous ne pouvez pas rétrograder un périphérique XTM 2 Series d'une version 11.5.1 à une version 11.4.1 avec l'option de **mise à niveau du SE** disponible dans l'interface Web UI. *[63323]*

- Amazon Web Services (AWS) requiert l'utilisation de BGP via un tunnel IPSec. Les opérations indiquées par Amazon.com pour la prise en charge d'AWS ne sont pas actuellement assurées par les produits WatchGuard. *[41534]*
- Le Rapport de configuration XTM ne contient pas tous les paramètres. Sont notamment exclus :
  - L'adresse IP de l'interface secondaire *[66990]*
  - Les paramètres QoS configurés *[66992]*
  - Les liaisons MAC statiques *[66993]*
  - La configuration IPv6 *[66994]*

XTMv

- XTMv ne modifie pas automatiquement le certificat autosigné lorsque son numéro de série change. *[66668]*

> **Workaround**
> Un nouveau certificat autosigné comportant le bon numéro de série sera généré en supprimant manuellement le certificat dans Firebox System Manager > Afficher > Certificats, puis en redémarrant le périphérique XTMv.

- Si vous importez le fichier OVA dans VMware Player (qui n'est pas pris en charge officiellement par cette version), vous devez utiliser la touche Entrée de votre clavier pour accepter le contrat de licence d'utilisateur final de XTMv. Les boutons **OK** et **Annule**r 'apparaissent pas à la fin du contrat de licence sur VMware Player.

WatchGuard System Manager

- Si vous utilisez Firebox System Manager pour envoyer une requête ping dans un tunnel VPN, vous recevez le message « Aucune mémoire tampon disponible ». Ce n'est pas un problème de mémoire. Ce message apparaît lorsque le tunnel VPN n'est pas établi. Vérifiez que le tunnel VPN est opérationnel, puis réessayez. *[59339]*
- WatchGuard System Manager n'affiche pas l'adresse IP correcte pour la passerelle par défaut d'un périphérique XTM qui ne dispose d'aucune interface externe. *[56385]*
- Lorsque vous installez WatchGuard System Manager ou un logiciel serveur sur un ordinateur sous Microsoft Windows XP, il ne faut activer le mode de compatibilité pour aucune des applications WSM, y compris le programme d'installation, même si Windows vous y invite. *[56355]*
- Les périphériques Firebox ou XTM gérés à distance en mode d'insertion peuvent ne pas se connecter au Management Server derrière une passerelle Firebox ou un périphérique XTM également configuré(e) en mode d'insertion. *[33056]*
- Si vous restaurez une image de sauvegarde vers un périphérique client géré par Management Server, il est possible que le secret partagé ne soit plus synchronisé.

> **Workaround**
> Connectez-vous à Management Server à partir de WSM. Sélectionnez le périphérique géré et choisissez **Mettre à jour le périphérique**. Activez la case d'option **Réinitialiser la configuration du serveur (Adresse IP/Nom d'hôte, secret partagé**).

- Lors d'une mise à niveau, d'une installation ou d'une désinstallation de WSM sur un système Windows 64 bits, il est possible d'arrêter les applications en cours d'exécution qui ont été détectées par le

programme d'installation WSM, mais ce dernier peut ne pas reconnaître qu'elles ont été arrêtées. *[39078]*

Workaround
Fermez l'application du programme d'installation. Cliquez avec le bouton droit sur l'icône WatchGuard Server Center dans la barre des tâches Windows et quittez l'application. Vérifiez que toutes les applications détectées sont arrêtées, puis recommencez l'installation ou la désinstallation de WSM.

- Lorsque vous exécutez le programme d'installation WSM v11.3.x ou une version ultérieure (soit le composant client WSM seul ou tous les composants serveur WSM sélectionnés) sur Microsoft SBS (Small Business Server) 2008 et 2011 sur un ordinateur ayant un système d'exploitation 64 bits, un message d'erreur Microsoft Windows s'affiche : «*lssProc.x64 has stopped working (lssProc.x64 a cessé de fonctionner)*». Lorsque vous refermez la boîte de dialogue du message d'erreur, l'installation se poursuit. *[57133]*

Web UI

- Fireware XTM Web UI ne prend pas en charge la configuration de certaines fonctionnalités. Elles comprennent :
  - FireCluster
  - L'exportation du certificat
  - Vous ne pouvez pas activer ou désactiver la notification des événements BOVPN
  - Vous ne pouvez pas ajouter ou supprimer des entrées ARP statiques dans la table ARP du périphérique
- Vous ne pouvez pas obtenir le fichier .wgx, qui est le profil de configuration chiffré de l'utilisateur final Mobile VPN with IPSec. Web UI génère uniquement une version en texte brut du profil de configuration de l'utilisateur final, portant l'extension .ini.
- Vous ne pouvez pas modifier le nom d'une stratégie, utiliser une adresse personnalisée dans une stratégie ou un nom d'hôte (Recherche DNS) pour ajouter une adresse IP à une stratégie.
- Si vous configurez une stratégie dans Web UI comme étant Désactivée, ouvrez Policy Manager et modifiez la même stratégie ; l'action de refus des paquets attribuée à la stratégie a été modifiée en Envoi TCP RST. *[34118]*
- Vous ne pouvez créer des fichiers de configuration de Mobile VPN with IPSec en lecture seule avec Web UI. *[39176]*

Command Line Interface (CLI)

- CLI ne prend pas en charge la configuration de certaines fonctionnalités :
  - Vous ne pouvez ni ajouter ni modifier une action de proxy.
  - Vous ne pouvez pas obtenir le fichier .wgx, qui est le profil de configuration chiffré de l'utilisateur final Mobile VPN with IPSec. CLI génère uniquement une version en texte brut du profil de configuration de l'utilisateur final, portant l'extension .ini.
- CLI effectue une validation des entrées minimales de plusieurs commandes.
- Pour le XTM 2050, le résultat de la commande CLI « show interface » n'indique pas exactement le numéro d'interface que vous utilisez dans le CLI pour configurer une interface. La commande CLI « show interface » indique le numéro d'interface tel qu'il apparaît sur l'étiquette de l'interface devant le périphérique (A0, A2 … A7; B0, B1 … B7; C0, C1), suivi par un tiret, puis le numéro d'interface consécutif (0 – 17), pour toutes les interfaces. *[64147]*

Workaround
Utilisez le numéro d'interface consécutif qui apparaît après le tiret en tant que numéro d'interface pour configurer l'interface. Pour les interfaces B1-9, le numéro d'interface de la commande CLI doit être compris entre 8 et 15. Pour les interfaces C0-1, le numéro d'interface de la commande CLI doit être 16-17.

Proxies

- Policy Manager et Web UI ne préviennent pas que la fonction Annulation de WebBlocker peut ne pas fonctionner avec HTTPS. *[67208]*
- La DPI (inspection des paquets en profondeur) HTTPS ne fonctionne pas lorsqu'on utilise IE 9.0 avec TLS 1.1 et 1.2, mais sans TLS 1.0 et SSL 3.0. *[65707]*

Workaround
Utilisez un autre navigateur ou activez TLS 1.0 et SSL 3.0 dans votre configuration d'IE 9.0.

- Le périphérique XTM ne peut stocker qu'un seul certificat de serveur proxy HTTPS et ne peut protéger qu'un seul site Web HTTPS à la fois. *[41131]*
- Lorsqu'un périphérique est soumis à une charge intense, certaines connexions proxy peuvent ne pas s'arrêter correctement. *[61925, 62503]*
- L'utilisation d'un serveur proxy de cache HTTP en association avec le proxy TCP-UDP est impossible. *[44260]*
- Vous ne pouvez pas passer d'appel SIP depuis un téléphone logiciel Polycom PVX derrière un Firebox vers un Polycom PVX sur le réseau externe. *[38567]*

Workaround
Vous pouvez utiliser le protocole H.323 à la place du protocole SIP.

- Lorsque vous essayez de diffuser des vidéos YouTube depuis un périphérique Apple exécutant iOS, le message d'erreur suivant pourrait s'afficher : « The server is not correctly configured. » (Le serveur n'est pas correctement configuré.)

Workaround
1. Modifiez votre stratégie de proxy HTTP.
2. Cliquez sur **Afficher/Modifier le proxy**.
3. Cochez la case **Autoriser les requêtes de plage via « non modifié »** .
4. Enregistrez les modifications apportées à votre périphérique XTM.

- Le protocole SIP-ALG n'envoie pas d'en-tête Contact correctement lorsque cet en-tête contient un nom de domaine. Il envoie seulement une chaîne vide avec : Contact : < >. Si l'en-tête Contact contient une adresse IP, le protocole SIP-ALG envoie l'en-tête Contact correctement : Contact : <sip:10.1.1.2:5060>. *[59622]*

Workaround
Configurez le système de gestion des appels (PBX) pour envoyer l'en-tête Contact avec une adresse IP, pas un nom de domaine.

Services de sécurité par abonnement

- Certaines informations de signature IPS, telles que le numéro CVE, ne sont pas disponibles dans Firebox System Manager. Nous offrons des capacités de recherche et des informations CVE pour les signatures IPS au sein d'un portail de sécurité Web pour IPS sur le site Web de WatchGuard, auquel vous pouvez accéder à l'adresse http://www.watchguard.com/SecurityPortal/ThreatDB.aspx.
- La détection Skype bloque uniquement les nouvelles sessions Skype. Si un utilisateur est connecté à Skype et une session Skype a déjà démarré lorsqu'Application Control est activé, il se peut qu'Application Control ne détecte pas l'activité.
- Pour les périphériques XTM 2 Series uniquement, Application Control est temporairement désactivé lors d'une mise à niveau, une sauvegarde ou une restauration. Une fois l'opération terminée, Application Control recommence à fonctionner.
- Il n'est pas possible d'assigner un rôle pour la gestion d'Application Control depuis la fonction d'administration de WatchGuard System Manager à base de rôles. *[59204]*
- Vous ne pouvez pas utiliser WebBlocker Server via un tunnel Branch Office VPN. *[56319]*

Mise en réseau

- Si vous avez manuellement créé des stratégies de routage dynamique dans Fireware XTM v11.5.x ou une version antérieure, les listes d'expéditeurs et de destinataires de ces stratégies sont effacées lors de la mise à niveau vers la version v11.6. Si le routage dynamique est activé, de nouvelles stratégies seront automatiquement créées lors de la mise à niveau. *[67721]*
- Le vérificateur de stratégie ne fonctionne pas lorsque votre périphérique XTM est configuré en mode pont. *[66855]*
- La présence d'une apostrophe dans le nom d'une réservation DHCP provoque l'échec de la réservation. *[65529]*
- Vous ne pouvez pas configurer d'actions de gestion du trafic ni utiliser le marquage QoS sur les réseaux locaux VLAN. *[56971, 42093]*
- Vous ne pouvez relier par pont une interface sans fil à une interface VLAN. *[41977]*
- Le Web Setup Wizard peut échouer si l'ordinateur est connecté directement à un périphérique XTM 2 Series tel qu'un client DHCP lors du lancement du Web Setup Wizard. Ceci peut se produire, car l'ordinateur ne peut pas obtenir une adresse IP assez rapidement après le redémarrage du périphérique pendant l'exécution de l'assistant. *[42550]*

  Workaround
  1. Si votre ordinateur est connecté directement à un périphérique XTM 2 Series lors de l'exécution du Web Setup Wizard, utilisez une adresse IP statique sur votre ordinateur.
  2. Utilisez un commutateur ou un concentrateur entre votre ordinateur et le périphérique XTM 2 Series lorsque vous lancez le Web Setup Wizard.

- Lorsqu'un réseau secondaire est configuré pour un périphérique XTM 2 Series en mode d'insertion, l'affichage des ordinateurs connectés au réseau secondaire dans la liste ARP de XTM 2 Series peut prendre du temps. *[42731]*
- Vous devez vous assurer que les interfaces réseau désactivées ne portent pas la même adresse IP que toute interface réseau active pour éviter que des problèmes de routage se produisent. *[37807]*

- Si vous activez le lien MAC/IP en cochant la case N'autoriser que le trafic envoyé vers/depuis ces adresses MAC/IP sans ajouter d'entrées dans la table, le lien MAC/IP ne s'active pas. Cette mesure de précaution permet aux administrateurs de ne pas se bloquer accidentellement depuis leurs propres périphériques XTM. *[36934]*
- Toute interface réseau appartenant à une configuration par pont se déconnecte et se reconnecte automatiquement lors de l'enregistrement d'une configuration depuis un ordinateur du pont comportant les modifications de configuration vers une interface réseau. *[39474]*
- Lorsque vous modifiez l'adresse IP d'un réseau VLAN configuré sur une interface externe de statique à PPPoE et que le Firebox ne peut pas obtenir d'adresse PPPoE, Firebox System Manager et Web UI risquent de continuer à afficher l'adresse IP statique utilisée précédemment. *[39374]*
- Lorsque vous configurez votre périphérique XTM en mode routage mixte, toute interface reliée par pont affiche son interface et 0.0.0.0 comme adresse IP de passerelle par défaut dans Web UI. *[39389]*
- Lorsque vous configurez votre périphérique XTM en mode pont, l'écran LCD de votre périphérique XTM affiche 0.0.0.0 comme adresse IP des interfaces reliées par pont. *[39324]*
- Lorsque vous configurez votre périphérique XTM en mode pont, la fonction de redirection HTTP est configurable depuis l'interface utilisateur, mais ne fonctionne pas sur cette version. *[38870]*
- Le lien d'adresse MAC/IP statique ne fonctionne pas si votre périphérique XTM est configuré en mode pont. *[36900]*
- Lorsque vous modifiez votre mode de configuration de routage mixte en pont ou de pont en routage mixte, CLI et Web UI risque de continuer à afficher le mode de configuration précédent. *[38896]*
- Le routage dynamique de RIP v1 ne fonctionne pas. *[40880]*
- Lorsqu'une adresse IP est ajoutée à la liste des sites temporairement bloqués par l'administrateur via Firebox System Manager > onglet Sites bloqués, le temps d'expiration est réinitialisé en permanence lorsque le trafic provient de l'adresse IP. *[42089]*

Multi-WAN

- Les périphériques XTM configurés pour utiliser la fonctionnalité multi-WAN peuvent ne pas acheminer le trafic entrant correctement s'ils sont configurés avec 1-to-1 NAT activé pour les routes des tunnels Branch Office VPN. *[67001]*
- La connexion persistante multi-WAN ne fonctionne pas si votre périphérique est configuré pour utiliser le mode table de routage multi-WAN. *[62950]*
- Lorsque vous activez l'option Multi-WAN Restauration immédiate du basculement WAN, certains trafics peuvent basculer par étapes. *[42363]*

Sans fil

- La bande sans fil 5 GHz ne fonctionne pas avec les canaux 36, 40, 149 ou 165. *[65559]*

Authentification

- Les serveurs Citrix 4.5/5/0 installés sur VMware ne fonctionnent pas avec Terminal Server Single Sign-On. *[66156]*

> **Workaround**
> En revanche, cette fonctionnalité fonctionne avec les serveurs Citrix 6.0 et 6.5 installés sur VMware.

- La fonction Clientless SSO n'est pas prise en charge dans un environnement Active Directory avec le chiffrement TLS activé.

- Si vous utilisez l'authentification Terminal Services, aucune vérification de l'authentification n'est faite contre le trafic de tout protocole autre que TCP ou UDP. Ceci inclut le trafic DNS, NetBIOS et ICMP.
- Il n'est pas possible d'utiliser *Rediriger automatiquement les utilisateurs vers la page d'authentification* l'option d'authentification avec l'authentification de Terminal Services.
- Pour permettre à votre périphérique XTM de traiter correctement le trafic lié au système en provenance du serveur terminal ou Citrix, Terminal Services Agent utilise un compte d'utilisateur spécial appelé Backend-Service. Pour cette raison, il se peut que vous deviez ajouter des stratégies afin d'autoriser le trafic depuis ce compte utilisateur jusqu'à votre périphérique XTM. Pour en savoir plus sur le fonctionnement du Backend-Service, consultez le système d'aide.
- Pour qu'une redirection d'authentification fonctionne correctement, le trafic HTTP ou HTTPS ne peut pas être autorisé via une stratégie sortante basée sur des adresses IP ou des alias contenant des adresses IP. La redirection d'authentification fonctionne uniquement lorsque les stratégies des ports 80 et 443 sont configurées pour l'authentification des utilisateurs ou de groupes d'utilisateurs. *[37241]*

Centralized Management

- Il n'y a pas d'option permettant de configurer une action de gestion de trafic dans un modèle de configuration de périphérique XTM v11.x. *[55732]*
- Si vous utilisiez Centralized Management avec des périphériques abonnés à des modèles dans des versions antérieures de WSM, lorsque vous faites une mise à niveau de WSM 11.x vers v11.4 ou une version plus récente, ces modèles sont mis à jour et les périphériques ne sont plus abonnés. Chaque périphérique conserve la configuration de son modèle Les modèles existants sont mis à jour pour utiliser « T_ » dans leurs noms d'objet (pour correspondre aux noms d'objet dans les périphériques qui y étaient abonnés). Après la mise à niveau, vous pourrez constater la mise à niveau du modèle dans l'historique de révision.
- Lorsqu'un modèle XTM est appliqué à un périphérique géré, Management Server crée une nouvelle révision de configuration pour le périphérique uniquement si la nouvelle révision sera différente de la révision actuelle. Il n'y a aucun retour d'information quant à la raison pourquoi une nouvelle révision de configuration n'a pas été créée. *[57934]*

FireCluster

- L'heure du FireCluster maître de sauvegarde peut être différente de celle du cluster maître, même si le protocole NTP est activé. *[66134]*

> **Workaround**
> Vous devez la synchroniser manuellement avec l'heure du cluster maître. Connectez-vous au cluster, lancez Firebox System Manager, puis sélectionnez Outils > Synchroniser l'heure. Cela synchronise l'heure des deux membres du cluster sur l'heure de l'ordinateur de gestion.

- Lorsque le protocole STP est activé sur certains commutateurs, le basculement de FireCluster peut prendre plus de 10 secondes. *[66180]*

> **Workaround**
> Désactivez le protocole sur le commutateur, configurez le commutateur pour qu'il utilise un protocole STP rapide ou utilisez un autre commutateur.

- Il peut s'avérer nécessaire de réimporter le certificat DPI HTTPS après la mise à niveau du système d'exploitation Fireware XTM d'un FireCluster. [65280]
- Vous ne pouvez pas utiliser l'adresse IP secondaire de l'interface d'un périphérique XTM pour gérer un FireCluster configuré en mode actif/actif. *[64184]*

Workaround
Servez-vous de l'adresse IP principale du périphérique XTM pour toutes les connexions de gestion à un FireCluster actif/actif.

- Les utilisateurs autorisés à surveiller un FireCluster via une administration basée sur les rôles ne peuvent pas voir le périphérique FireCluster dans Log and Report Manager. *[65398]*
- Le maître de sauvegarde de FireCluster peut devenir inactif lorsque Mobile VPN with SSL ou PPTP est configuré pour utiliser un pool d'adresses IP qui inclut l'adresse IP du cluster. *[63762]*

Workaround
Évitez d'utiliser une adresse IP qui entre en conflit avec les adresses IP du cluster.

- Si le Log Server ne peut pas être atteint depuis les adresses IP de gestion, seul le maître du FireCluster sera en mesure de se connecter. Cela peut se produire si le Log Server est connecté via un réseau externe, mais les adresses IP de gestion sont situées sur un réseau approuvé ou facultatif. *[64482]*
- Si vous modifiez la configuration réseau d'un FireCluster en le faisant passer du mode routé au mode d'insertion, puis que vous revenez au mode routé, l'adresse IP de l'interface du cluster ne s'affiche pas correctement dans la boîte de dialogue Policy Manager **Configuration > réseau**. Les interfaces correctes du cluster sont indiquées dans la boîte de dialogue de configuration du FireCluster. *[63905]*
- Les mises à jour de Gateway AV dans un système disposant d'un niveau de mémoire limité peuvent engendrer un basculement du FireCluster. *[62222]*

Workaround
Limitez la fréquence à laquelle le système vérifie si des mises à jour de Gateway AV sont disponibles afin de réduire les chances que ce problème survienne.

- Si un lien surveillé est défaillant sur les deux membres FireCluster, le membre non maître bascule en mode passif et ne traite alors plus aucun trafic. Un basculement multi-WAN dû à un échec de connexion à un hôte de contrôle des liaisons ne déclenche pas de basculement FireCluster. Le basculement FireCluster a lieu uniquement lorsque l'interface physique est inactive ou ne répond pas.
- Chaque périphérique XTM dispose d'une série d'adresses IP par défaut attribuées aux interfaces du périphérique dans une plage commençant par 10.0.0.1. L'adresse IP par défaut la plus élevée dépend du nombre d'interfaces. Si vous définissez l'adresse IP de l'interface du cluster primaire ou de sauvegarde sur l'une des adresses IP par défaut, les deux périphériques redémarrent et le maître de sauvegarde devient inactif. *[57663]*

Workaround
N'utilisez aucune des adresses IP comme adresse IP de l'interface du cluster primaire ou de sauvegarde.

- Lorsque vous avez un FireCluster actif/actif et que vous utilisez la fonctionnalité de contournement de WebBlocker, vous pouvez être invité à saisir votre mot de passe de contournement à nouveau. *[39263]*
- Chaque interface réseau activée dans un FireCluster est automatiquement surveillée par FireCluster. Vous devez vérifier que toutes les interfaces disponibles sont connectées physiquement à un périphérique réseau.
- Si vous utilisez des commutateurs HP ProCurve, il se peut que vous ne puissiez pas configurer votre FireCluster en mode actif/actif, car ces commutateurs peuvent ne pas prendre en charge l'ajout d'entrées ARP statiques. *[41396]*
- Si vous utilisez le client Mobile VPN with IPSec depuis le même réseau que le réseau externe configuré sur votre FireCluster, quelques trafics risquent de ne pas passer par le tunnel VPN. *[38672]*
- Les utilisateurs Mobile VPN with PPTP ne s'affichent pas dans Firebox System Manager lorsque vous vous connectez à un membre FireCluster passif. PPTP est connecté uniquement au Firebox actif lorsque vous utilisez un FireCluster actif/passif. *[36467]*
- Il est impossible d'utiliser une adresse IP d'interface VLAN pour une adresse IP de gestion de FireCluster. [45159]
- Pour effectuer une mise à niveau manuelle d'un FireCluster de la version 11.3.x vers la version 11.5.1, l'ordinateur de gestion doit se situer sur le même réseau que les adresses IP de gestion du FireCluster. [63278]

Journalisation et génération de rapports

- Lorsque vous modifiez le niveau de journalisation de votre WatchGuard Log Server et que vous cliquez sur Appliquer, il ne se passe rien. *[60088]*

> **Workaround**
> 1. Dans WatchGuard Server Center, sur l'onglet Journalisation de Log Server, modifiez le niveau de journalisation des messages de journal de Log Server et cliquez sur **Appliquer des**.
> 2. Dans l'arborescence Serveurs, cliquez avec le bouton droit sur Log Server et sélectionnez **Arrêter le serveur**. Dans le message de confirmation, sélectionnez **Oui**.
> 3. Cliquez à nouveau avec le bouton droit sur Log Server et sélectionnez **Démarrer le serveur**.

- Le rapport de synthèse des paquets refusés n'est pas encore disponible dans Log and Report Manager. *[63192]*
- Le fichier PDF créé pour le rapport Tendance des activités Web n'inclut pas les étiquettes de temps sur l'axe des abscisses lorsqu'il est visualisé dans Log and Report Manager. Les informations relatives à la date et à l'heure sont incluses dans le tableau figurant sous le rapport. *[64162]*
- Lorsque vous effectuez une mise à niveau de Fireware XTM v11.4.x vers v11.5.1, les rapports créés au moment de la mise à niveau peuvent ne pas s'afficher dans Log and Report Manager. *[64325]*
- Si un nom de calendrier de rapport quotidien comprend un signe deux-points ou certains caractères (exemple : « 1:35 »), le système indique une erreur. *[63427]*

> **Workaround**
> Veillez à ce que les noms de vos calendriers de rapports utilisent uniquement des caractères valables pour les noms de fichiers Windows. Vous pourrez trouver des caractères valables dans des articles tels que http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247%28v=vs.85%29.aspx .

- Le collecteur de journal plante s'il atteint la limite de taille virtuelle de 2 Go sur les systèmes Windows 32 bits. *[64249]*
- Deux problèmes de tri sont à signaler dans le nouveau Log and Report Manager. Lorsque vous triez par Destination, le champ effectue un tri par adresse IP, pas par nom d'hôte de destination (le cas échéant). Lorsque vous triez par Disposition, certains éléments dont l'état est « refuser » ne sont pas correctement triés dans les groupes. *[62879]*
- Tous les « Rapport archivés » quotidiens ou hebdomadaires présents dans votre configuration v11.3 sont automatiquement convertis en rapports planifiés après une mise à niveau vers WSM v11.4 ou une version plus récente.

Mobile VPN

- Vous ne pouvez pas générer de fichiers de configuration Mobile VPN with IPSec lorsque le nom du groupe contient des caractères tels qu'un astérisque ou un point (*, .). *[66815]*
- Si vous réglez le niveau du journal de diagnostic du trafic Mobile VPN with SSL sur « débogage », les messages de journal cessent d'apparaître dans Firebox System Manager > Traffic Manager. *[65165]*

Workaround
Réglez le niveau du journal de diagnostic de Mobile VPN with SSL sur un niveau moins détaillé que « débogage ».

- Si vous ajoutez une clé de fonctionnalité ajoutant des licences Mobile VPN with SSL sur votre périphérique XTM, vous devez redémarrer le périphérique pour activer les nouveaux utilisateurs Mobile VPN with SSL. *[65620]*
- Lorsque vous connectez pour la première fois un client Mobile VPN with SSL v11.5.1 à un périphérique XTM passé à la version v11.5.2, la mise à niveau du client échoue parfois. *[65635]*

Workaround
Installez le client Mobile VPN with SSL manuellement.

- Vous ne pouvez pas établir de connexion Mobile VPN with SSL à partir d'un ordinateur Windows lorsque le compte système Windows est en chinois. *[58208]*
- Lorsque vous utilisez le client IPSec intégré depuis un iPhone ou un iPad, la connexion du client se déconnecte lorsque la durée de connexion atteint 1 heure et 45 minutes. Ceci est dû à une limitation dans le client Cisco utilisé dans les iPhone et iPad. Vous devez reconnecter le client IPSec afin de rétablir le tunnel VPN. *[63147]*
- Les connexions Mobile VPN with PPTP depuis des périphériques mobiles Android ne fonctionnent pas de manière constante sur les réseaux mobiles 3G. *[63451]*
- Les connexions du client Mobile VPN with IPSec peuvent transiter via la mauvaise interface externe lorsque le périphérique XTM est configuré pour multi-WAN en mode Tourniquet. *[64386]*
- Vous ne pouvez pas configurer Mobile VPN with SSL de manière à établir un trafic réseau par pont vers une interface reliée par un pont. *[61844]*
- Les utilisateurs de Mobile VPN with SSL ne peuvent pas se connecter à certaines ressources réseau via un tunnel Branch Office VPN qui aboutit sur un FireCluster actif/actif. *[61549]*
- Vous ne pouvez pas envoyer de requête ping sur l'adresse IP de l'interface du périphérique XTM sur lequel un client Shrew Soft VPN a établi un tunnel VPN. Vous pouvez envoyer des requêtes ping sur ce réseau, mais pas directement sur l'adresse IP de l'interface. *[60988]*
- Les connexions du client Shrew Soft VPN peuvent être interrompues si plusieurs clients sont connectés à un périphérique XTM qui envoie en même temps des nouvelles clés de phase 2. *[60261]*]

- Les nouvelles clés de phase 1 émises par le client Shrew Soft VPN provoquent la déconnexion du client si ce dernier est connecté depuis plus de 24 heures. Dans ce cas, nous vous conseillons de définir le renouvellement de clé sur votre périphérique XTM à 23 heures, soit une heure de moins que le renouvellement de clé codé en dur dans la configuration du client Shrew Soft. Cela a pour effet de forcer le périphérique XTM à démarrer le renouvellement de clé et d'informer le client que le tunnel doit être rétabli. *[60260, 60259]*
- Une session FTP continue via une connexion Mobile VPN with IPSec peut s'interrompre si un renouvellement des clés IPSec s'effectue pendant le transfert FTP. *[32769]*

Workaround
Augmentez le nombre d'octets alloués au renouvellement des clés.

- Le client Mac Mobile VPN for SSL peut ne pas réussir à se connecter à un périphérique XTM si l'algorithme d'authentification utilisé est SHA 256. *[35724]*

Branch Office VPN

- Les Branch Office VPN manuels échouent lorsque la clé prépartagée dépasse 50 caractères. *[65215]*
- Ne donnez pas le même nom à une passerelle VPN et à un tunnel VPN. *[66412]*
- Vous ne pouvez pas utiliser de clé prépartagée de plus de 50 caractères de long pour les tunnels Branch Office VPN. *[65215]*
- Lorsque vous configurez votre périphérique XTM en mode multi-WAN, vous devez sélectionner quelles interfaces inclure dans votre configuration multi-WAN. Si vous choisissez de ne pas inclure certaines interfaces dans votre configuration multi-WAN (c.-à-d. vous désactivez la case à cocher pour ces interfaces), le système ne crée pas de route pour ce réseau. Cela peut provoquer un problème si vous avez un réseau Branch Office VPN (BOVPN) configuré pour inclure cette même interface. Dans ce cas, le tunnel VPN pourrait ne pas arriver à négocier avec son pair distant. *[57153]*

Workaround
Si vous utilisez le multi-WAN et avez des problèmes avec vos tunnels Branch Office VPN qui n'arrivent pas à négocier avec leurs pairs distants, vous devez ouvrir votre configuration multi-WAN et sélectionner Configurer à côté du mode de configuration multi-WAN que vous avez choisi. Assurez-vous que les interfaces correctes sont incluses dans votre configuration multi-WAN.

- Un tunnel Branch Office VPN ne laisse pas passer de trafic si une stratégie NAT (traduction d'adresses réseau) statique entrante qui inclut les protocoles IP 50 et 51 existe pour l'adresse IP externe du périphérique XTM. [*41822]*
- Les tunnels BOVPN gérés ne peuvent pas se mettre en place si le point de distribution CRL (par exemple, WatchGuard Management Server ou un site de distribution CRL tiers que vous utilisez) est hors ligne. *[55946]*
- L'option *Toute* route dans un tunnel BOVPN a été modifiée dans Fireware XTM. Si un tunnel BOVPN utilise toute route de la partie locale d'un tunnel, Fireware XTM l'interprète comme un réseau 0.0.0.0 et un masque de sous-réseau 0.0.0.0 (soit en notation de barre oblique, 0.0.0.0/0). Si le pair distant IPSec n'envoie pas 0.0.0.0/0 comme son ID de Phase 2, les négociations de Phase 2 échouent. *[40098]*

Workaround
N'utilisez pas l'option *Toute* route pour la partie locale ou distante de la route du tunnel. Modifiez la partie locale de la route de votre tunnel. Saisissez l'adresse IP des ordinateurs situés derrière le périphérique XTM qui participent réellement au routage du tunnel. Contactez l'administrateur du pair distant IPSec pour déterminer la partie distante de sa route du tunnel utilisée par ce périphérique (ou la partie distante de son ID de phase 2).

- Si vous disposez d'un grand nombre de tunnels BOVPN dans votre configuration, leur affichage dans Policy Manager peut mettre un certain temps. *[35919]*

Workaround
Dans Policy Manager, sélectionnez **Afficher > Mise en surbrillance des stratégies**. Décochez la case **Mettre en surbrillance les stratégies de pare-feu en fonction du type** de trafic.

Utilisation de la CLI

Fireware XTM CLI (Command Line Interface) est pris en charge intégralement par les versions v11.x. Pour plus d'informations sur le démarrage et l'utilisation du CLI, consultez le *Guide de référence de commande* CLI. Vous pouvez télécharger le guide CLI depuis le site Web de documentation à l'adresse http://www.watchguard.com/help/documentation/xtm.asp.

Assistance Technique

Pour obtenir une assistance technique, contactez le Support technique WatchGuard par téléphone ou sur le Web à l'adresse http://www.watchguard.com/support. Lorsque vous contactez le Support technique, vous devez fournir le numéro de série de votre produit enregistré ou votre ID partenaire.

	Numéro de téléphone
Utilisateurs finaux aux États-Unis	877.232.3531
Utilisateurs finaux internationaux	+1 206.613.0456
Revendeurs WatchGuard agréés	206.521.8375

Japanese (日本語)

Fireware XTM v11.6.1 リリース ノート

サポートされるデバイス	XTMv、XTM 2、3、5、および 8 Series XTM 1050、XTM 2050
Fireware XTM OS ビルド	346666
WatchGuard System Manager ビルド	347361
改訂日	2012年8月8日

概要

WatchGuardでは、FirewareXTMv11.6.1およびWatchGuardSystemManagerv11.6.1をリリースいたしました。FirewareXTMOSv11.6.1はどのWatchGuardXTMデバイス(2Series、3Series、5Series、8Series、XTM1050および2050デバイスを含む)にも、またXTMvの全エディションを用いてインストールしていただけます。本リリースは、新しい高性能XTM5Seriesモデル515、525、535、および545へのサポートを含み、ローカライズユーザーインターフェースおよびドキュメントへのアップデートを提供します。また、いくつかの主要製品の機能強化も行われました。

- ブリッジモードで構成されたXTMデバイスは、802.1Qスイッチまたはブリッジ間でVLANトラフィックの通過が可能です。
- XTM 25、26、および 33 の有線モードに FireCluster がサポートされています。

そして、主なバグ修正がいくつか行われました (本リリースおよび 解決済みの問題 セクションに記載)。

Fireware XTM v11.6.1 における機能強化に関する詳細は、製品ドキュメントまたは次を参照してください: Fireware XTM v11.6.1 の新機能。

開始する前に

このリリースをインストールする前に、次のものがあることを確認してください。

- WatchGuard XTM 2 Series、3 Series、5 Series、8 Series、XTM 1050、または XTM 2050 デバイス、あるいは XTMv (全エディション)。
- 以下に示されたハードウェアとソフトウェアの必須コンポーネント。WatchGuard System Manager (WSM) を使用している場合、お使いの WSM バージョンが XTM デバイスにインストールされている Fireware XTM OS バージョンと Management Server にインストールされている WSM バージョン以降であることを確認してください。
- お使いの XTM デバイスの機能キー — XTM デバイスを前バージョンの Fireware XTM OS からアップグレードされる場合、既存の機能キーをお使いいただけます。XTMv を使用している場合、XTMv を購入した際に受け取ったシリアル番号で機能キーを生成する必要があります。

WatchGuard System Manager v11.6.1 および全ての WSM サーバーコンポーネントは、Fireware XTM v11 の以前のバージョンを使用するデバイスにインストールして使用できます。この場合、お使いの Fireware XTM OS バージョンに対応する製品マニュアルを使用することをお勧めします。

新しい物理 XTM デバイスを使用している場合、デバイスに同梱されている *XTM クイックスタート ガイド* の指示に従ってください。今回、新たに XTMv のインストールを行う場合には、*XTMv セットアップ ガイド* のインストールおよびセットアップに関する指示に注意しながら従ってください。

この製品に関するマニュアルは WatchGuard Web サイト、www.watchguard.com/help/documentation、をご覧ください。

ローカライゼーション

本リリースには、最新の、ローカライズされた Fireware XTM 管理ユーザインターフェース (WSM アプリケーション スイートと Web UI) と製品のヘルプが含まれています。サポートする言語:

- 中国語 (簡体字、中華人民共和国)
- フランス語 (フランス)
- 日本語
- スペイン語 (南米)

> ***Note*** *これらの言語に加えて韓国語および繁体字中国語用にローカライズされた Web UI サポートが提供されます。Web UI のみがローカライズされています。これら 2 つの言語において、WSM、すべてのヘルプファイルおよびドキュメントは英語のままです。*

ほとんどのデータ入力は、これまでと同様に標準 ASCII 文字を使用して行う必要があることにご注意ください。非 ASCII 文字は、UI の以下のようなエリアで使用できます。

- プロキシ拒否メッセージ
- ワイヤレス Hotspot のタイトル、利用条件、およびメッセージ
- WatchGuard Server Center のユーザー、グループ、およびロール名

デバイスのオペレーティング システムから返されるあらゆるデータ (ログ データなど) は英語のみで表示されます。また Web UI のシステム ステータスメニューのすべての項目およびサード パーティにより提供されるあらゆるソフトウェア コンポーネントは英語のままとなります。

Fireware XTM Web UI

Web UI は、デフォルトによりユーザーが Web ブラウザで設定している言語で起動します。現在選択されている言語名が、各ページの先頭に表示されます。別の言語に変更するには、表示される言語名をクリックしてください。言語のドロップダウン リストが表示され、使用する言語を選択することができます。

WatchGuard System Manager

WSM をインストールする際には、インストールする言語パックを選択することができます。WSM で表示される言語は、ユーザーがお使いの Microsoft Windows 環境で選択した言語と同じです。たとえば、Windows XP を使用していて WSM を日本語で使用する場合は、コントロール パネル>地域と言語のオプションへと進み、言語のリストから日本語を選択します。

Log and Report Manager、CA Manager、Quarantine Web UI、およびワイヤレス Hotspot

これらのWebページは、ユーザーがWebブラウザで選択した言語設定に従って自動的にその言語で表示されます。

Fireware XTM および WSM v11.6.1 オペレーティング システムの互換性

改訂日：2012年6月

WSM/ Fireware XTM コンポーネント	Microsoft Windows XP SP2 (32ビット)	Microsoft Windows Vista (32ビット & 64ビット)	Microsoft Windows 7 (32ビット & 64ビット)	Microsoft Windows サーバー 2003 (32ビット)	Microsoft Windows サーバー 2008 & 2008 R2*	Mac OS X v10.5, v10.6, & v10.7
WatchGuard System Manager アプリケーション	✓	✓	✓	✓	✓	
Fireware XTM Web UI *対応ブラウザ:* *IE 7 および 8、Firefox 3.x & 以降*	✓	✓	✓	✓	✓	✓
Log and Report Manager Web UI *対応ブラウザ: Firefox 3.5 & 以降、IE8 & 以降、Safari 5.0 & 以降、Chrome 10 & 以降。Javascript が必要。*	✓	✓	✓	✓	✓	✓
WatchGuard サーバー	✓	✓	✓	✓	✓	
シングル サインオン エージェント ソフトウェア (Event Log Monitor を含む)				✓	✓	
シングル サインオン クライアント ソフトウェア	✓	✓	✓	✓	✓	
Terminal Services エージェント ソフトウェア**				✓ ***	✓	
Mobile VPN with IPSec クライアント ソフトウェア	✓	✓	✓			ネイティブ (Cisco) IPSec クライアント対応。
Mobile VPN with SSL クライアント ソフトウェア	✓	✓	✓	✓		✓

**Microsoft Windows Server 2008 32 ビットおよび 64 ビット サポート、Windows Server 2008 R2 64 ビット サポート。*

*** 手動またはシングル サインオン認証による Terminal Services サポートは、Microsoft Terminal Services または Citrix XenApp 4.5、5.0、6.0、6.5 環境で動作します。*

**** Microsoft Windows Server 2003 SP2 が必要。*

認証サポート

この表によって、Fireware XTM の主要機能によってサポートされている認証サーバーの種類を簡単に見ることができます。認証サーバーを使用することで、お使いの XTM デバイスの構成に、ユーザおよびグループベースのファイヤウォールと VPN ポリシーを構成することができます。サポートされているサード パーティ認証サーバーの各タイプによって、フェイルオーバー用にバックアップ サーバーの IP アドレスを指定できます。

✓ — WatchGuard による完全サポート

 — 未サポート、しかし WatchGuard の顧客によって試験通過済み

	Active Directory[1]	LDAP	RADIUS[2]	SecurID[2]	Firebox (Firebox-DB) ローカル認証
Mobile VPN with IPSec/Shrew Soft	✓	✓	✓3	–	✓
iPhone/iPad iOS および Mac OS X 用の Mobile VPN with IPSec				✓	✓
Windows 用 Mobile VPN with SSL	✓	✓	✓4	✓4	✓
Mac 用 Mobile VPN with SSL	✓	✓	✓	✓5	✓
Mobile VPN with PPTP	–	–	✓	該当なし	✓
Port 4100 の内蔵認証 Web ページ	✓	✓	✓	✓	✓
Windows シングル サインオン サポート (クライアント ソフトウェアあり/なし)	✓	–	–	–	–
Terminal Services の手動認証	✓				✓
シングル サインオンによる Terminal Services 認証	✓6	–	–	–	–
Citrix の手動認証					✓

1. *Active Directory のサポートには、記載がない限り、シングルドメインとマルチドメイン サポートの両方が含まれます。*
2. *RADIUS および SecurID サポートには RADIUS に統合されたワンタイム パスワードおよびチャレンジ/レスポンス認証が含まれます。多くの場合、SecurID は Vasco を含むその他の RADIUS 実装とも使用できます。*
3. *Shrew Soft クライアントは二要素認証をサポートしていません。*
4. *Fireware XTM はグループ認証用に RADIUS 属性 Filter ID 11 をサポートしています。*
5. *PIN+トークンコード モードをサポートしています。NextTokencode モードと SMS ワンタイム パスワードはサポートされていません。*
6. *シングルドメインの Active Directory 構成のみがサポートされています。*
7. *WatchGuard TO Agent および SSO Agent に対するオペレーティング システムの互換性情報については、最新の Fireware XTM および WSM オペレーティング システム互換表をご覧ください。*

XTMv システム要件

XTMv 仮想デバイスをインストールするには、お使いの ESXi バージョンによってサポートされているサーバーハードウェアに VMware ESXi 4.1 または 5.0 ホストがインストールされている必要があります。また、対応する Windows コンピュータに VMware vSphere Client 4.1 または 5.0 をインストールする必要があります。ご希望により、vSphere クライアントの代わりに vCenter Server を使用することもできます。

XTMv のハードウェア要件は VMware ESXi のハードウェア要件と同じです。VMware ハードウェアの互換性の詳細については、以下の VMware 互換性ガイドをご覧ください http://www.vmware.com/resources/compatibility/search.php。

各 XTMv 仮想マシンには 3 GB のディスク容量が必要です。

推奨されるリソース割当設定

	小規模事業所	中規模事業所	大規模事業所	データセンター
仮想 CPU	1	2	4	8 以上
メモリ	1 GB	2 GB	4 GB	4 GB 以上

ソフトウェアのダウンロード

1. WatchGuard ポータルにログインして、記事&ソフトウェアタブを選択します。
2. 検索セクションから、記事および既知の問題チェックボックスのチェックを外し、利用できるソフトウェア ダウンロードを検索します。ソフトウェアをダウンロードする XTM デバイスを選択します。

ダウンロードできるソフトウェア ファイルは複数あります。各製品の下にあるそれぞれの説明を読んで、アップグレードに必要なソフトウェア パッケージを探してください。

WatchGuard System Manager

WatchGuard System Manager ソフトウェアは、すべてのユーザーがダウンロード可能です。このソフトウェア パッケージは、WSM および WatchGuard Server Center ソフトウェアをインストールします:

`WSM11_6_1s.exe` — このファイルを使用して WatchGuard System Manager を v11.x から WSM v11.6.1 にアップグレードします。

Fireware XTM OS

お使いの XTM デバイスに適した Fireware XTM OS イメージを選んでください。WSM を使用して OS をインストールまたはアップグレードしたい場合には、.exe ファイルを使用します。Fireware XTM Web UI を使用して OS をインストールまたはアップグレードしたい場合には、.zip ファイルを使用します。新しい XTMv デバイスをデプロイするには、.ova ファイルを使用します。

以下をお持ちの場合・・・	対応する Fireware XTM OS パッケージを選択します
XTM 2050	`XTM_OS_XTM2050_11_6_1.exe` `xtm_xtm2050_11_6_1.zip`
XTM 1050	`XTM_OS_XTM1050_11_6_1.exe` `xtm_xtm1050_11_6_1.zip`
XTM 8 Series	`XTM_OS_XTM8_11_6_1.exe` `xtm_xtm8_11_6_1.zip`
XTM 5 Series	`XTM_OS_XTM5_11_6_1.exe` `xtm_xtm5_11_6_1.zip`
XTM 330	`XTM_OS_XTM330_11_6_1.exe` `xtm_xtm330_11_6_1.zip`
XTM 33	`XTM_OS_XTM33_11_6_1.exe` `xtm_xtm33_11_6_1.zip`
XTM 2 Series モデル 21、22、23	`XTM_OS_XTM2_11_6_1.exe` `xtm_xtm2_11_6_1.zip`
XTM 2 Series モデル 25、26	`XTM_OS_XTM2A6_11_6_1.exe` `xtm_xtm2a6_11_6_1.zip`

XTMv 全エディション	`xtmv_11_6_1.ova`
	`xtmv_11_6_1.exe`
	`xtmv_11_6_1.zip`

シングル サインオン ソフトウェア

シングル サインオンを使用している場合、ダウンロード可能なファイルは 2 つあります。

- WG-Authentication-Gateway_11_6.exe (SSO エージェント ソフトウェア - シングル サインオンに必須で、クライアントレス SSO の場合、オプションの Event Log Monitor を含みます)
- WG-Authentication-Client_11_6.msi (SSO クライアント ソフトウェア - 任意)

シングル サインオンのインストールや設定方法については、製品マニュアルをご覧ください。

Terminal Services 認証ソフトウェア

- TO_AGENT_32_11_6.exe (32 ビット サポート)
- TO_AGENT_64_11_6.exe (64 ビット サポート)

Windows および Mac 用 Mobile VPN with SSL クライアント

Mobile VPN with SSL をお使いの場合、ダウンロード可能なファイルは次の 2 種類です。

- WG-MVPN-SSL_11_6.exe (Windows 用クライアント ソフトウェア)
- WG-MVPN-SSL_11_6.dmg (Mac 用クライアントソフトウェア)

Windows 用 のMobile VPN with IPSec クライアント

当社の Web サイトから、Windows 用の Shrew Soft VPN クライアントをダウンロードできます。Shrew Soft VPN クライアントの詳細については、ヘルプまたは Shrew Soft, Inc. のウェブサイトをご覧ください。

Fireware XTM v11.x から v11.6.1 へのアップグレード

Fireware XTM v11.x から Fireware XTM v11.6.1 にアップグレードする前に、アップグレードする WatchGuard デバイスに一致する Fireware XTM OS ファイルをダウンロードし保存してください。利用できるソフトウェアはすべて WatchGuard ポータル、記事 & ソフトウェアタブで見つけることができます。アップグレード作業は、Policy Manager および Web UI から行うことが可能です。アップグレードを行う前に、デバイス構成および WatchGuard Management Server 構成をバックアップすることを強くお勧めします。これらのバックアップファイルがなければダウングレードすることができません。

WatchGuard System Manager (WSM) を使用している場合、お使いの WSM バージョンが XTM デバイスにインストールされている Fireware XTM OS バージョンと Management Server にインストールされている WSM バージョン以降であることを確認してください。

> ***Note*** *WSM v11.4.x 以前のバージョンから WSM v11.6.1 にアップグレードする場合には、ナレッジベースの記事 6995 に記載された手順に従って Log and Report Server のデータをバックアップすることが重要です。これは、WSM v11.5.1 で Log and Report Server のデータベース構造が変更するために必要です。WSM v11.5.1 以降のバージョンに初めてアップグレードする場合には、既存の Log and Report Server のタイムスタンプは現地のタイムゾーンから UTC に変換されます。ナレッジベースの記事にはこのアップグレードについての詳細、Log and Report Manager についての重要な情報 (WSM v11.5.1 で新たに追加) が記載されています。*

WatchGuard Management Server 構成のバックアップ

Management Server をインストールしたコンピュータから:

1. WatchGuard Server Center から、**Management Server のバックアップ/回復**を選択します。
   WatchGuard Server Center バックアップ/復元ウィザードが起動します。
2. **次へ**
   をクリックします。操作を選択する画面が表示されます。
3. **バックアップ設定**を選択します。
4. **次へ**
   をクリックします。バックアップファイルを指定する画面が表示されます。
5. **参照** をクリックし、バックアップファイルの場所を選択します。構成ファイルは、必ず後で構成を復元する場合にアクセスできる場所に保存してください。
6. **次へ**
   をクリックします。WatchGuard Server Center のバックアップ/復元ウィザードが完了しました画面が表示されます。
7. **終了** をクリックし、ウィザードを終了します。

Web UI から Fireware XTM v11.6.1 へのアップグレード

1. **システム>イメージのバックアップ** の順に進むか、または USB バックアップ機能を使用して現在の構成ファイルをバックアップします。
2. WatchGuardソフトウェアダウンロードセンターからダウンロードしたOSファイルを、管理コンピュータ上で起動します。
   Windowsベースのインストーラを使用している場合には、このインストールによって *[xtm series]_[product code].sysa-dl* というアップグレードファイルがデフォルトで C:\Program Files (x86)\Common files\WatchGuard\resources\FirewareXTM\11.6.1\[model]または[model][product_code]に保存されます。

3. お使いの XTM デバイスに Web UI を用いて接続し、**システム>OS のアップグレード** の順に選択します。
4. ステップ 2 から *[xtm series]_[product code].sysa-dl* の検索を行い **アップグレード** をクリックします。

WSM/Policy Manager v11.x から Fireware XTM v11.6.1 へのアップグレード

1. **ファイル>バックアップ** を順に選択します。または USB バックアップ機能を使用して現在の構成ファイルをバックアップします。
2. WatchGuard ポータルからダウンロードした OS 実行ファイルを、管理コンピュータ上で起動します。このインストールによって *[xtm series]_[product code].sysa-dl* というアップグレード ファイルがデフォルトで C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\11.6.1\[model] または [model][product_code] に保存されます。
3. WatchGuard System Manager v11.6.1 をインストールして開きます。お使いの XTM デバイスに接続し、Policy Manager を起動します。
4. Policy Manager から、**ファイル>アップグレード** の順に選択します。指示が表示されたら、ステップ 2 から *[xtm series]_[product code].sysa-dll* ファイルを検索して選択します。

WatchGuard サーバー ソフトウェアのアップグレードの詳細

v11.0.1 以降から WSM v11.6.1 にアップデートする場合、それまで使用していた v11.x サーバーもしくはクライアント ソフトウェアをアンインストールする必要はありません。既存のソフトウェアがインストールされた状態で v11.6.1 サーバーおよびクライアント ソフトウェアをインストールし、WatchGuard ソフトウェア コンポーネントをアップグレードすることができます。

FireCluster を Fireware XTM v11.6.1 にアップグレード

FireCluster で Fireware XTM OS をアップグレードする方法は 2 通りあります。使用する方法は、現在使用されている Fireware XTM のバージョンによって決まります。

Fireware XTM v11.4.x または v11.5.x から FireCluster のアップグレード

以下のステップに従って Fireware XTM v11.4.x または v11.5.x から Fireware XTM v11.6.x に FireCluster をアップグレードします。

1. Policy Manager でクラスタ構成ファイルを開きます。
2. **ファイル > アップグレード** を選択します。
3. 構成パスフレーズを入力します。
4. アップグレード ファイルの場所を入力または選択します。
5. バックアップ イメージを作成するには、**はい** を選択します。
   クラスタ メンバーのリストが表示されます。
6. アップグレードする各デバイスのチェックボックスをオンにします。
   各デバイスのアップグレードが完了したことを示すメッセージが表示されます。

アップグレード完了後、各クラスタ メンバーが再起動してクラスタに再結合されます。クラスタの両方のデバイスを同時にアップグレードすると、一度に 1 つのデバイスのみがアップグレードされます。これは、アップグレード実行中にネットワークを中断せずにアクセスできることを確認するためです。

Policy Manager はバックアップ メンバーをアップグレードしてから、再起動を待ち、バックアップとしてクラスタに再び加わります。その後、Policy Manager がマスタをアップグレードします。マスタの役割は、再起動してアップグレード プロセスが完了するまで変更されません。その際、バックアップはマスタとしての役割を引き継ぎます。

リモート ロケーションからアップグレードを実行するには、管理 IP アドレス用の FireCluster インターフェイスが外部インターフェイスに対して構成され、管理 IP アドレスがパブリックでありルーティング可能であることを確認します。詳細については、管理 IP アドレス用インターフェイスについてをご覧ください。

Fireware XTM v11.3.x から FireCluster のアップグレード

FireCluster を Fireware XTM v11.3.x から Fireware XTM v11.6.x にアップグレードするには、手動でアップグレードする必要があります。手動でアップグレードする方法は、ナレッジベースの記事をご覧ください。FireCluster の Fireware XTM OS をアップグレード。

ダウングレードに関する説明

WSM v11.6.x から WSM v11.x へのダウングレード

WSM v11.6.x から以前のバージョンに戻す場合は、WSM v11.6.x をアンインストールする必要があります。アンインストールする場合、サーバー構成とデータファイルを削除するかどうかを尋ねるので、はいを選択します。サーバー構成とデータファイルを削除した後、WSM v11.6.x にアップグレードする前にバックアップしたデータおよびサーバー構成ファイルを復元する必要があります。

次に、WSM v11.6.x にアップグレードする前に使用していたのと同じバージョンの WSM をインストールします。インストーラが既存のサーバー構成を見つけ出し、**終了** ダイアログボックスよりお使いのサーバーを再起動しようと試みます。WatchGuard Management Server を使用している場合、WatchGuard Server Center を使用し、WSM v11.6.x にアップグレードする前に作成したバックアップ Management Server 構成を復元します。全ての WatchGuard サーバーが動作していることを確認します。

Fireware XTM v11.6.x から Fireware XTM v11.x へのダウングレード

> ***Note*** *XTM 2050、XTM 330 または XTM 33 デバイスを v11.5.1 より以前のバージョンの Fireware XTM OS にダウングレードすることはできません。XTM 5 Series モデル 515、525、535 または 545 を v11.6.1 より以前のバージョンの Fireware XTM OS にダウングレードすることはできません。XTMv を v11.5.4 より以前のバージョンの Fireware XTM OS にダウングレードすることはできません。*

FirewareXTMv11.6.xからFirewareXTMの前のバージョンにダウングレードする場合、以下のいずれかを行います。

- Fireware XTM v11.6.x にアップグレードする際に作成したフルバックアップイメージを復元し、ダウングレードを完全に行います、または
- アップグレード前に自動復元イメージで作成した USB バックアップファイルを使用し、デバイスに接続した USB ドライブをリカバリーモードで起動します。XTMv のユーザーはこのオプションを使用できません。

WatchGuardXTM330、5Series、8Series、XTM1050、またはXTM2050デバイスをリカバリモードで起動するには:

1. XTM デバイスの電源を切断します。
2. フロント パネルの上矢印 (↑) を押しながらデバイスの電源をオンにします。
3. LCD ディスプレイに「Recovery Mode starting」と表示されるまで、ボタンを押下します。

WatchGuardXTM2SeriesまたはXTM33デバイスをリカバリーモードで起動するには、以下の手順を実行します。

1. 電源を切ります。
2. 後部のリセットボタンを押しながらデバイスの電源を接続します。
3. 前部の Attn ライトがオレンジ色に点灯するまで、ボタンを押し続けます。

解決済みの問題

FirewareXTM v11.6.1リリースでは、以前のFirewareXTM v11.xリリースで見つかった多くの問題点が解決されています。

全般

- Application Control またはIPSを使用する構成を行った場合にXTMデバイスにクラッシュをもたらす、いくつかの問題点が本リリースで解決されています。*[66937, 65426, 65636, 67312, 66135, 67159, 67399, 67310]*
- Mu Dynamics のデフォルトの脆弱性テストを実行する際にいくつかのXTM デバイスのプロセスにクラッシュをもたらした問題点が解決されました。*[66490]*
- カーネル クラッシュとデバイスの再起動をもたらす問題点が解決されました。*[67329]*
- XTM 2 Series デバイスでは、インターフェースが不安定になることなく、大容量ファイルを転送することができます。*[67367]*
- XTM 5 Series LCD スクリーンに誤ったデータが表示される問題点が解決されました。*[67197]*

WatchGuard System Manager

- Policy Manager は、標準 Fireware XTM 機能キーの付いた XTM 5 Series モデル 505、510、520、および 530 (Proではなく) に正しい VLAN 制限を表示します。*[67780]*

Web UI

- Web UI から XTM 2 および 3 Series デバイス用に Traffic Management のアクションを構成および適用することができます。*[67221, 66645]*

Centralized Management

- Firebox X Edge e-Series デバイスはテンプレートを使って管理することができます。*[67658]*

ログ記録&レポート

- ローカル ログまたはレポート データベースが故障したときに送信される通知メッセージは、「???」ではなく、適切にホスト IP アドレスを表示します。*[41731]*
- ログサーバーは次のエラーメッセージを生成することなく、2 GB を超えるバックアップファイルを処理することができます： 「エラー (8199)、古いログデータのバックアップ中における例外：ファイルは zip ファイルではありません」例外」。*[66811]*
- DHCP のリースアクティビティ レポートも正常に機能します。*[66062]*
- Log Collector はクラッシュすることなく、複数の SSL/TLS 記録に及ぶXTM デバイスのログデータを処理できます。*[66347]*

プロキシおよびセキュリティサービス

- セキュリティ サブスクリプション署名への誤ったメモリ割当てによって XTM 2 Series モデル 25 と 26 で起こる性能不足の問題点が解決されました。*[67240]*
- Application Control が Web/Web 2.0 カテゴリでコンテンツをブロックすると、大抵の場合 拒否メッセージが正常に Web ブラウザに送信されます。*[66201]*
- WebBlocker 自動データベース更新時間は、ホスト サーバーのタイムゾーンでデイライト セービングタイムが実施されている時に 1 時間ずれてオフになることはありません。*[67551]*

ネットワーク

- 複数 WAN を使用するよう構成された XTM デバイスにおいて外部インターフェースに PPPoE または DHCP を使用する場合、XTM デバイスは外部インターフェースへの再接続後に外部インターフェース用のデフォルトのルートを失うことはありません。*[67424, 67520]*
- PPPoE を使用するよう構成された外部インターフェースが切断され、再接続された後に、静的ルートが失われる問題点が解決されました。*[67520]*
- XTM デバイスがブリッジ モードに構成されると、タグ付けされた VLAN トラフィックは正しく認識されます。*[64355]*

Command Line Interface

- CL1 コマンド「すべての工場出荷時の初期設定を回復」は、デバイスを工場出荷時の初期設定に回復します。*[66240]*

FireCluster

- FireCluster のクラスタ用の構成をドロップイン モードで表示した場合に、Policy Manager が誤って IP アドレスを 0.0.0.0/24 として表示する問題点が解決されました。 *[63551]*

Mobile VPN

- The Mobile VPN with SSL プロセスは FireCluster のフェールオーバー中にクラッシュしません。*[66118]*

既知の問題および制限

Fireware XTM v11.6.1 およびすべての管理アプリケーションにおける既知の問題は以下のとおりです。問題を回避する方法がある場合は、それも併記されています。

全般

- USB ドライブを XTM デバイスに接続しているとき、デバイスは 1 つのサポート スナップショットを USB ドライブを自動的に保存しません。*[64499]*

> **Workaround**
> CLI コマンド 「USB 診断の有効化」を使用してデバイスを有効にし、診断サポート スナップショットを USB ドライブに保存します。このコマンドについての詳細は *Command Line Interface リファレンス ガイドをご覧ください*。

- Firebox System Manager ステータス レポートに表示された 「Sysb」バージョンは、XTM v11.5.1 リリースの前に製造された XTM モデル 2、5、8、1050 の場合ブランクで表示されます。
- ICMP フラッド攻撃の防御は 11.5.1 では、旧バージョンと違う動作をします。v11.5.1 では、XTM デバイスは PING リクエストの合計ではなく、PING リクエストと応答を合わせた合計数を数えます。ICMP フラッド攻撃の防御の既定のしきい値が増加しなかったため、フラット攻撃の防御は旧リリースの場合より頻繁にトリガできます。*[63094]*

> **Workaround**
> 既定のパケット処理設定では、既定値の 1000 パケット/秒からそれ以上大きい数字へのドロップ ICMP フラッド攻撃の場合にしきい値が増加します。

- XTM デバイスの空きメモリ レベルが 20M 以下のときに、XTM デバイス構成をデバイスに保存するとネットワーク崩壊の原因となります。*[64474]*
-
- XTM 830F の ETH1 インターフェースはファイバ オプティック ポートであるため、イーサネット インターフェース搭載コンピュータから WSM Quick Setup Wizard を使用することはできません。ファイバ NIC 搭載コンピュータを使用するか、ファイバおよびイーサネット インターフェース両方に対応するスイッチを使用して接続してください。*[59742]*
- XTM 5 Series デバイスの電源をオフにするには、背面の電源スイッチを 4～5 秒間押したままにする必要があります。*[42459]*
- XTM 5 Series デバイスの場合、インターフェイス 0 が Auto-MDIX をサポートしないため、ケーブルの極性が自動判別されません。
- XTM 2 Series デバイスでは、デバイスに負荷がかかっていない場合でも、平均負荷は常に 1 以上で表示されます。*[63898]*
- XTM 2 Series デバイスが再起動するには 5 分ほどかかることがあります。
- **Policy Manager >ファイル>バックアップ** または **復元** 機能を使用する場合は、処理に時間を要しますが、正常に完了します。*[35450]*
- Web UI の OS のアップグレード オプションを使用して、XTM 2 Series デバイスを v11.5.1 から v11.4.1 にダウングレードすることはできません。*[63323]*
- Amazon Web Services (AWS) には IPSec トンネル上で BGP の使用が必要です。Amazon.com で説明されている Amazon Web Services をサポートするオペレーションは、現在 WatchGuard 製品で対応していません。*[41534]*

- XTM 構成レポートにはすべての設定は含まれていません。含まれていない設定:
  - セカンダリ インターフェースの IP アドレス *[66990]*
  - 構成された QoS 設定 *[66992]*
  - 静的 MAC バインディング *[66993]*
  - IPv6 構成 *[66994]*

XTMv

- 自己署名証明書のシリアル番号が変わった時に、XTMv が自動的に自己署名証明書を変更することはありません。*[66668]*

> **Workaround**
> Firebox System Manager >表示>証明書から証明書を手動で削除し、XTMv デバイスを再起動すると、正しいシリアル番号の付いた新しい自己署名証明書が生成されます。

- VMware Player (本リリースでは正式にサポートされていません) に OVA ファイルをインポートしたら、キーボードの「Enter」キーを使用して、XTMv エンド ユーザー ライセンス契約 (EULA) に同意しなければなりません。この **OK** および EULA の最後にある **キャンセル**ボタンは VMware Player には表示されません。

WatchGuard System Manager

- Firebox System Manager を使用して VPN トンネルにおいて ping すると、「バッファの空き容量はありません」というメッセージが表示されます。これは、メモリの問題ではありません。このメッセージは VPN トンネルが構築されていない場合に表示されます。VPN トンネルが構築されていることを確認してから、再試行してください。*[59339]*
- 外部インターフェイスがない XTM デバイスの既定ゲートウェイの場合、WatchGuard System Manager に正しい IP アドレスが表示されません。*[56385]*
- WatchGuard System Manager またはその他あらゆるサーバーソフトウェアを Microsoft Windows XP を実行中のコンピュータにインストールする場合、たとえ Windows によって指示されても、WSM アプリケーション (インストーラを含む) に対する互換モードを有効にしてはなりません。*[56355]*
- ドロップイン モードに構成しているリモート管理対象の Firebox または XTM デバイスは、同じくドロップイン モードに構成しているゲートウェイ Firebox または XTM デバイスの配下にある Management Server に接続できないことがあります。*[33056]*
- Management Server が管理している管理対象クライアント デバイスに、バックアップ イメージを復元すると、共有シークレットが同期されなくなることがあります。

> **Workaround**
> WatchGuard System Manager (WSM) から Management Server に接続します。次に管理対象デバイスを選択し、**デバイスの更新**を選択します。**サーバー構成をリセットする (IP アドレス/ホスト名、共有シークレット)** ラジオボタンを選択します。

- 64 ビットの Windows システムにおける WSM のアップグレード、インストール、またはアンインストール中には、WSM インストーラで検出された実行中のアプリケーションは停止されますが、それが停止したことをインストーラが認識しない場合があります。*[39078]*

Workaround
インストーラ アプリケーションを閉じます。Windows のタスクバーにある WatchGuard Server Center アイコンを右クリックして、WatchGuard Server Center を終了します。削除したアプリケーションがすべて停止したことを確認し、WSM のインストールまたはアンインストールを再試行してください。

- 64 ビットのオペレーティング システムがインストールされた Microsoft SBS (Small Business Server) 2008 または 2011 上で、WSM v11.3.x 以降のインストーラ (WSM クライアント コンポーネントのみ、または任意で選択した WSM サーバーコンポーネント) を使用する場合、Microsoft Windows に次のエラーが表示されます: *IssProc.x64 は停止しました*」という Microsoft Windows エラーが表示されます。エラーのダイアログボックスを閉じると、インストールが完了します。*[57133]*

Web UI

- FirewareXTM WebUI は、一部の機能の構成をサポートしていません。以下の機能がその対象となります。
  - FireCluster
  - 証明書のエクスポート
  - BOVPN イベント通知のオンとオフ
  - デバイスの ARP テーブルに対する、静的 ARP エントリの追加と削除
- 暗号化された Mobile VPN with IPSec エンド ユーザー用構成プロファイル (.wgx ファイル) の取得。Web UI が生成できるのは、プレーン テキスト形式のエンド ユーザー用構成プロファイル (.ini ファイル) だけです。
- ポリシー名の編集、ポリシーでのカスタム アドレスの使用、ホスト名 (DNS 参照) を使用してポリシーに IP アドレスを追加すること。
- Web UI からポリシーを無効に構成し、Policy Manager を開いてそのポリシーに変更を加えると、ポリシーに割り当てられた、パケットを拒否したときのアクションは、TCP RST の送信に変更されます。*[34118]*
- 読み取り専用の Mobile VPN with IPSec 構成ファイルは、Web UI を使って作成することはできません。*[39176]*

コマンド ライン インターフェイス (CLI)

- CLI では、以下のような一部の機能に対する構成をサポートしていません。
  - プロキシ アクションの追加と編集。
  - 暗号化された Mobile VPN with IPSec エンド ユーザー用構成プロファイル (.wgx ファイル) の取得。CLI が生成できるのは、プレーン テキスト形式のエンド ユーザー用構成プロファイル (.ini ファイル) だけです。
- CLI ではほとんどのコマンドで、入力に対して最低限の検証しか行われません。
- XTM 2050 の場合、CLI コマンド「show interface」の出力で、CLI で使用するインターフェイス番号を明確に示しインターフェイスを構成することはありません。「show interface」CLI コマンドでは、すべてのインターフェイスに対して、デバイス (A0, A2 … A7; B0, B1 … B7; C0, C1) の前にインターフェイス ラベルとしてインターフェイス番号に続いてダッシュ、その次に連続インターフェイス番号 (0 – 17) が示されます。*[64147]*

Workaround
インターフェイス番号としてダッシュの後に表示される連続インターフェイス番号を使用して、インターフェイスを構成します。B1-9 インターフェースの CLI コマンドのインターフェース番号は 8-15 の範囲内でなければなりません。C0-1 インターフェースの CLI コマンドのインターフェース番号は 16-17 の範囲内でなければなりません。

プロキシ

- Policy Manager と Web UI は、WebBlocker のオーバーライドが HTTPS には適用できない場合があるという警告を表示しません。*[67208]*
- HTTPS DPI (Deep Packet Inspection) は、TLS 1.1 と 1.2 が有効になっていて、TLS 1.0 と SSL 3.0 が有効になっていない IE 9.0 を使用しているユーザーには適用されません。*[65707]*

> **Workaround**
> 別のブラウザを使用するか、お使いの IE 9.0 で TLS 1.0 と SSL 3.0 を有効にしてください。

- XTM デバイスは 1 つの HTTPS Proxy Server 証明書しか保存できず、1 度に 1 つの HTTPS Web サイトしか保護することができません。*[41131]*
- XTM デバイスに高負荷がかかっているとき、プロキシ接続に正しく終了できないものが出てくる可能性があります。*[61925, 62503]*
- HTTP キャッシュ プロキシ サーバーを使用する機能は、TCP-UDP プロキシと併せて利用することはできません。*[44260]*
- Firebox の配下にある Polycom PVX ソフトフォンから、外部ネットワークにある Polycom PVX へは、SIP を使った通話を行うことができません。*[38567]*

> **Workaround**
> SIP の代わりに H.323 プロトコルを使用してください。

- iOS が作動している Apple デバイスから YouTube 動画のストリームを試みると、以下のエラーが表示されることがあります: 「サーバーが正しく構成されていません。」

> **Workaround**
> 1. HTTP プロキシ ポリシーを編集します。
> 2. **プロキシの表示/編集**をクリックします。
> 3. **変更されていない範囲要求を許可** チェック ボックスを選択します。
> 4 XTM デバイスに変更を保存します。

- Contact ヘッダーにドメイン名が含まれている場合、SIP-ALG はContact ヘッダーを正しく送信しません。空の文字列を送信します: Contact: < >。Contact ヘッダーに IP アドレスが含まれている場合、SIP-ALG は Contact ヘッダーを正しく送信します: お問い合わせ: <sip:10.1.1.2:5060>。*[59622]*

> **Workaround**
> Contact ヘッダーではドメイン名ではなく IP アドレスを送信するように PNX を構成します。

セキュリティ登録

- CVE 番号など、いくつかの IPS 署名情報は Firebox System Manager では使用できません。WatchGuard Web サイト上での IPS 用として、Web セキュリティポータルでの IPS 署名に使用する CVE 情報と検索機能を提供しており、以下よりアクセスできます。
  http://www.watchguard.com/SecurityPortal/ThreatDB.aspx
- Skype 検出は、新しい Skype セッションのみをブロックします。Application Control が有効化された時点において、ユーザーがすでに Skype にログインしており Skype セッションが開始されている場合、Application Control はそのアクティビティを検出しません。

- XTM 2 Series デバイスの場合のみ、アップグレード、バックアップ、または復元を行う間 Application Control は一時的に無効となります。処理が完了すると、Application Control は動作を再開します。
- WatchGuard System Manager のロールに基づく管理機能から、Application Control 管理のロールを割り当てることはできません。*[59204]*
- Branch Office VPN トンネルを経由した WebBlocker Server の使用はできません。*[56319]*

ネットワーク

- Fireware XTM v11.5.x 以前のバージョンで、手動でダイナミックルーティング ポリシーを作成すると、v11.6 にアップグレードする際にこれらのポリシーにおける宛先および送信者リストは削除されます。ダイナミックルーティングが有効になっている場合、アップグレードを行うと自動的に新しいポリシーが作成されます。*[67721]*
- お使いの XTM デバイスがブリッジ モードで構成されている場合には、Policy Checker は使用できません。*[66855]*
- DHCP 予約名にアポストロフィーがあると、DHCP の予約が正常に行えなくなります。*[65529]*
- VLAN 上でトラフィック管理アクションの構成および QoS マーキングの使用はできません。*[56971, 42093]*
- ワイヤレス インターフェイスを VLAN インターフェイスにブリッジすることはできません。*[41977]*
- Web Setup Wizard を起動するときにお使いのコンピュータが DHCP クライアントとして XTM 2 Series デバイスに直接接続されている場合、Web Setup Wizard は失敗することがあります。これは、ウィザードの動作中にデバイスが再起動した後、一定の時間以内に IP アドレスを取得できないためです。*[42550]*

  Workaround
  1. Web Setup Wizard の動作中にお使いのコンピュータが XTM 2 Series デバイスに直接接続されている場合は、コンピュータ上で静的 IP アドレスを使用してください。
  2. Web Setup Wizard を実行する際に、お使いのコンピュータと XTM 2 Series デバイスの間にスイッチまたはハブを使用してください。

- ドロップイン モードに構成された XTM 2 Series デバイスにセカンダリ ネットワークを構成すると、セカンダリ ネットワークに接続するコンピュータが XTM 2 Series の ARP リストに表示されるまでに数分かかることがあります。*[42731]*
- 無効にしたネットワーク インターフェイスが、アクティブないずれかのネットワーク インターフェイスと同じ IP アドレスを持っていないことを確認してください。ルーティングに問題が発生する原因となります。*[37807]*
- これらの MAC/IP アドレスの間でのみトラフィックの送信を許可するチェック ボックスを使用して MAC/IP アドレスのバインドを有効にしても、テーブルにエントリを何も追加しないと、MAC/IP アドレスのバインド機能はアクティブになりません。これは、管理者が自分の XTM デバイスから自分自身を誤ってブロックすることを防ぐためです。*[36934]*
- ブリッジ ネットワーク上のコンピュータから、ネットワーク インターフェイスに対する変更を含んだ構成を保存すると、そのブリッジ構成に含まれる全ネットワーク インターフェイスが、自動的に切断、再接続されます。*[39474]*
- 外部インターフェイス上に構成している VLAN の IP アドレスを静的から PPPoE に変更し、Firebox が PPPoE アドレスを取得できなかった場合、以前使用されていた静的 IP アドレスが Firebox System Manager と Web UI で表示されることがあります。*[39374]*
- XTM デバイスを混合ルーティング モードで構成すると、ブリッジされた全インターフェイスとそのデフォルト ゲートウェイの IP アドレスが、0.0.0.0 として Web UI に表示されます。*[39389]*
- XTM デバイスをブリッジモードで構成する時、お使いの XTM デバイスの LCD 画面にブリッジされたインターフェイスの IP アドレスが 0.0.0.0 と表示されます。*[39324]*
- XTM デバイスをブリッジ モードに構成したとき、ユーザーインターフェイスから HTTP リダイレクト機能を構成することができますが、この機能は本リリースでは動作しません。*[38870]*

- お使いの XTM デバイスがブリッジモードに構成されている場合、静的 MAC/IP アドレス バインドは実現しません。*[36900*
- 構成モードを混合ルーティングからブリッジへ、またはブリッジから混合ルーティングへ変更しても、CLI と Web UI では以前の構成モードが表示されることがあります。*[38896]*
- RIPv1 の動的ルーティングは動作しません。*[40880]*
- 管理者が Firebox System Manager > ブロックされたサイトタブで、一時的にブロックされたサイトリストに IP アドレスを追加すると、その IP アドレスからトラフィックを受信するたびに有効期限がリセットされます。*[42089]*

複数 WAN

- Branch office VPN トンネルのルートにおいて 1-to-1 NAT が有効にされた状態でデバイスが構成されていると、複数 WAN を使用するために構成された XTM デバイスの受信トラフィックを正確にルートできなくなる可能性があります。*[67001]*
- お使いのデバイスが複数 WAN ルーティングテーブル モードを使用するように構成されていると、複数 WAN スティッキー接続は行なえません。*[62950]*
- WAN フェールオーバーのために複数 WAN をすぐにフェールバックオプションを有効にした場合、一部のトラフィックで徐々にフェールオーバーが発生することがあります。*[42363]*

認証方法

- チャンネル 36、40、149、または 165GHz を使用すると、5GHz ワイヤレスバンドは動作しません。*[65559]*

認証

- VMware にインストールされた Citrix 4.5/5/0 サーバーは、ターミナル サーバーのシングル サインオンでは動作しません。*[66156]*

> **Workaround**
> この機能は VMware にインストールされた Citrix 6.0 および 6.5 サーバーで動作します。

- クライアントレス SSO は、TLS 対応の Active Directory 環境でサポートされません。
- Terminal Services 認証を使用する場合、TCP または UDP でないプロトコルのトラフィックに対して認証確認は行われません。これには DNS、NetBIOS、または ICMP トラフィックが含まれます。
- ターミナルサービスの認証と一緒に *ユーザーを認証* ページへ*自動的にリダイレクトする* 認証オプションを使用することはできません。
- TerminalサーバーまたはCitrixサーバーからのシステムに関連するトラフィックをXTMデバイスに正しく処理させるには、TerminalServicesエージェントがBackend-Serviceという特別ユーザーアカウントを使用します。これにより、このユーザーアカウントからのXTMデバイスを経由したトラフィックを許可する様にポリシーの追加が必要な場合があります。製品ヘルプシステムからBackend-Serviceの動作についての情報が得られます。
- 認証リダイレクト機能を正常に動作させるには、IP アドレスや IP アドレスを含むエイリアスに基づいた送信ポリシーで、HTTP や HTTPS トラフィックを許可しないでください。ポート 80 と 443 をユーザーまたはユーザー グループの認証に使うようポリシーを構成しているときにのみ、認証リダイレクト機能は動作します。*[37241]*

Centralized Management

- XTM v11.x デバイス構成テンプレートにおいて、Traffic Management アクションを設定するオプションはありません。*[55732]*

- WSM 旧バージョンでテンプレートに登録したデバイスとCentralized Management を使用している場合、WSM 11.x から v11.4 以上へアップグレードを行うと、これらのテンプレートは更新され、デバイスの登録が行われなくなりました。各デバイスはそれぞれのテンプレート構成を保持します。既存のテンプレートはオブジェクト名に「_」を使用するように更新されます (これにより登録に使用されるデバイス内のオブジェクト名と一致します)。アップグレードを行うと、アップグレード中に改訂履歴にテンプレートのアップグレードが表示されます。
- XTM テンプレートが管理対象デバイスに適用されると、新しいバージョンが現在のバージョンと異なる場合のみ、Management Server はそのデバイスに対して新しい構成改訂版を作成します。新しい構成改訂版がなぜ作成されなかったのかという理由の説明はありません。*[57934]*

FireCluster

- FireCluster バックアップ マスタにおける時間は、NTP が有効な場合にも、クラスタ マスタとの同期を止めることができます。*[66134]*

> **Workaround**
> バックアップ マスタの時間を手動で同期します。クラスタに接続し、Firebox System Manager を起動したら、ツール>時間の同期を選択します。これにより、クラスタ メンバー両方の時間が管理コンピュータの時間に同期されます。

- 一部のスイッチでスパニング ツリー プロトコル (STP) が有効になっていると、FireCluster のフェイルオーバーには 10 秒以上かかる場合があります。*[66180]*

> **Workaround**
> スイッチの STP を無効にして、迅速な STP を使用するようスイッチを構成するか、別のスイッチを使用してください。

- FireCluster の Fireware XTM OS FireCluster をアップグレードした後、HTTPS DPI 証明書を再インポートしなければならない場合があります。[65280]
- アクティブ/アクティブ モードで構成された FireCluster を管理するために、XTM デバイスのセカンダリ IP アドレスを使用することはできません。*[64184]*

> **Workaround**
> アクティブ/アクティブ FireCluster へのすべての管理接続には、XTM デバイスのプライマリ IP アドレスを使用します。

- 役割ベースの管理によって FireCluster をモニターするためのアクセス権を付与されたユーザーは、Log and Report Manager で FireCluster デバイスを見ることはできません。*[65398]*
- Mobile VPN with SSL または PPTP がクラスタ IP アドレスを含む IP アドレス プールを使用するように設定されているとき、FireCluster バックアップ マスタは有効にならないことがあります。*[63762]*

> **Workaround**
> クラスタ IP アドレスと競合する IP アドレス プールの使用を避けてください。

- 管理 IP アドレスから Log Server にアクセスできない場合、現在の FireCluster マスターのみを接続できます。これは Log Server が外部ネットワークを通して接続されているときに発生することがありますが、管理 IP アドレスは信頼済みまたは任意ネットワーク上にあります。*[64482]*

- ルーテッド モードからドロップイン モードに FireCluster のネットワーク構成を変更してから、ルーテッド モードに再び変更すると、クラスタ インターフェイスの IP アドレスは Policy Manager **ネットワーク > 構成**ダイアログ ボックスに正しく表示されません。正しいクラスタ インターフェイスはFireCluster の構成ダイアログ ボックスに表示されます。*[63905]*
- メモリ容量が少なくなったシステムで Gateway AV をアップデートすると、FireCluster フェールオーバーを招くことがあります。*[62222]*

Workaround
これが発生する可能性を最小限に抑えるために、システムがGateway AV 更新をチェックする頻度を少なくします。

- 両方の FireCluster メンバーで監視対象リンクが失敗すると、非マスタ メンバーがパッシブモードに切り替わり、結果としてすべてのトラフィックが処理されません。FireCluster フェールオーバーは、リンク モニタ ホストへの接続失敗によって発生した複数 WAN フェールオーバーによってトリガされることはありません。FireCluster フェールオーバーは、物理インターフェイスがダウンしたり、応答しない場合にだけ発生します。
- 各 XTM デバイスは、10.0.0.1 で始まる範囲のデバイスインターフェイスに割り当てられた既定の IP アドレスのセットを有します。既定の IP アドレス最高値は、インターフェイスの数によります。プライマリまたは バックアップ クラスタ インターフェイスの IP アドレスをいずれかの既定 IP アドレスに設定する場合、両方のデバイスは再起動し、バックアップマスタは非アクティブとなります。*[57663]*

Workaround
プライマリまたはバックアップ クラスターインターフェイスの IP アドレスとして、既定 IP アドレスを使用しないでください。

- アクティブ/アクティブの FireCluster がある場合に WebBlocker 上書き機能を使うと、上書き用パスワードを入力するメッセージが 2 回表示されることがあります。*[39263]*
- FireCluster で有効にしたネットワーク インターフェイスはすべて、FireCluster が自動的に監視します。そのため、有効なインターフェイスがネットワーク デバイスに物理的に接続されていることを確認してください。
- HP ProCurve スイッチを使用している場合、これらのスイッチが静的 ARP エントリをサポートしないため FireCluster をアクティブ/アクティブ モードに構成することができない場合があります。*[41396]*
- FireCluster に設定した外部ネットワーク アドレスと同じネットワークから、Mobile VPN with IPSec クライアントを使用すると、トラフィックが VPN トンネルを通過しないことがあります。*[38672]*
- パッシブの FireCluster メンバーに接続しているとき、Mobile VPN with PPTP のユーザーは Firebox System Manager に表示されません。また、アクティブ/パッシブの FireCluster を使用しているときは、PPTP がアクティブな Firebox にのみ接続します。*[36467]*
- FireCluster 管理 IP アドレスに対して、VLAN インターフェイス IP アドレスを使用することはできません。[45159]
- v11.3.x から v11.5.1 に FireCluster の手動アップグレードを実行するには、管理コンピュータを FireCluster 管理 IP アドレスと同じネットワークに置く必要があります。[63278]

ログ記録およびレポート

- WatchGuard Log Server のログレベルを変更して適用をクリックすると、変更が反映されます。*[60088]*

Workaround
1. WatchGuard Server Center のLog Server へのログタブで、Log Server からのログメッセージのログレベルを変更して**適用**をクリックします。
2. サーバーツリーでLog Serverを右クリックして **サーバーの停止を選択します。**確認メッセージで**はい**を選択します。
3. Log Serverを再度右クリックして **サーバーの開始を選択します**。

- Log and Report Manager では、まだ拒否されたパケットの概要レポートをご利用いただくことはできません。*[63192]*
- Web アクティビティのトレンド レポートの PDF 出力には、Log and Report Manager に表示された x 軸に時間ラベルが含まれません。レポートの下のテーブルには、日付と時間情報が含まれます。*[64162]*
- Fireware XTM v11.4.x から v11.5.1 にアップグレードするとき、アップグレードの時間の傍で生成されたレポートは Log and Report Manager に表示されません。*[64325]*
- 日次のレポート スケジュール名に、コロンまたは特定のその他の文字が使用されている場合 (例: 「1:35」) が含まれる場合、システムはエラーを返します。*[63427]*

Workaround
日次のレポート スケジュール名に Windows ファイル名に使用できる文字だけが使用されていることを確認してください。使用できる文字は次の説明などを参考にしてください:
http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247%28v=vs.85%29.aspx .

- 32 ビット Windows システムで、2GB 仮想サイズ制限に達すると、Log collector がクラッシュします。*[64249]*
- 新しい Log and Report Manager に 2 つのソート問題があります。宛先ごとにソートするとき、フィールドは宛先ホスト名 (可能な場合) ではなく、IP アドレスごとにソートします。配置ごとにソートすると、「拒否」状態の一部のアイテムはグループ内で正確にソートされません。*[62879]*
- v11.3 構成に存在する日毎または週毎の「Archived Reports」は、WSM v11.4 以上へのアップグレードの後、予定されたレポートとして自動的に変換されます。

Mobile VPN

- グループ名にアスタリスクやピリオドなどの文字 (*, .) が含まれている場合、Mobile VPN with IPSec 構成ファイルを作成することはできません。*[66815]*
- Mobile VPN with SSL の診断ログレベルを「デバッグ」レベルに設定すると、Firebox System Manager > Traffic Manager でログメッセージが表示されなくなります。*[65165]*

Workaround
Mobile VPN with SSL の診断ログレベルを「デバッグ」よりも粒度の粗いログレベルに設定します。

- XTM デバイスに Mobile VPN with SSL ライセンスを加える新しい機能キーを追加する場合には、XTM デバイスを再起動して、追加の Mobile VPN with SSL を有効にしなければなりません。*[65620]*
- Mobile VPN wth SSL v11.5.1 クライアントを v11.5.2 にアップグレードされた XTM デバイスに初めて接続する場合には、クライアントのアップグレードに失敗することがあります。*[65635]*

Workaround
Mobile VPN with SSL クライアントを手動でインストールしてください。

- Windows システムのアカウントが中国語の場合には、Windows ベースのコンピュータから Mobile VPN with SSL 接続を構築することはできません。*[58208]*
- iPhone または iPad から組み込み IPSec クライアントを使用するとき、接続期間が 1 時間 45 分に達すると、クライアント接続が切断されます。これは、iPhone/iPad で使用された Cisco クライアントの制限によるものです。VPN トンネルを確立するには、IPSec クライアントを接続し直す必要があります。*[63147]*
- Android モバイル デバイスから Mobile VPN with PPTP 接続は、3G モバイル ネットワークで一貫して作動しません。*[63451]*
- XTM デバイスがラウンド ロビン モードの複数 WAN に対して構成されているとき、Mobile VPN with IPSec クライアントからの接続は間違った外部インターフェイス経由でルートできます。*[64386]*
- ブリッジ インターフェイスにネットワーク トラフィックをブリッジするために、Mobile VPN with SSL を構成できません。*[61844]*
- Mobile VPN with SSL ユーザーは、アクティブ/アクティブ FireCluster で終了する Branch Office VPN トンネル経由で、一部のネットワーク リソースに接続できません。*[61549]*
- Shrew Soft VPN クライアントが VPN トンネルを確立した XTM デバイス インターフェイスの IP アドレスを ping できません。そのネットワークでコンピュータを ping することはできますが、インターフェイスの IP アドレス自体は ping できません。*[60988]*
- XTM デバイスに複数のクライアントが接続され Phase 2 キーの再生成を同時に発行している場合、Shrew Soft VPN クライアント接続がドロップする可能性があります。*[60261]*
- 24 時間以上接続されていると、フェーズ 1 キーの再作成が Shrew Soft VPN クライアントにより初期化されクライアントが切断される原因となります。この場合、当社は XTM デバイスのキーの再生成を 23 時間に設定するようにお勧めします -- Shrew Soft クライアント構成ではハードコードされたキーの再生成より 1 時間短くしてください。このために、XTM デバイスはキーの再生成を開始し、クライアントにトンネルを再作成する必要があることを通知しなければならなくなります。*[60260, 60259]*
- IPSec キーの再生成が FTP 転送中に発生したとき、Mobile VPN with IPSec 接続での連続した FTP セッションが切断されることがあります。*[32769]*

Workaround
キーの再生成を行うバイト数を増やしてください。

- 認証アルゴリズムが SHA 256 に設定されている場合、Mobile VPN for SSL Mac クライアントは XTM デバイスに接続できないことがあります。*[35724]*

Branch Office VPN

- Manual Branch Office VPN は事前共有キーの文字数が 50 文字を超えると失敗します。*[65215]*
- VPN ゲートウェイと VPN トンネルに同じ名前を使用しないでください。*[66412]*
- Branch office VPN トンネルには 50 文字以上の事前共有キーを使用することはできません。*[65215]*
- お使いの XTM デバイスを複数 WAN モードで構成する時、その複数 WAN 構成に含めるインターフェイスを選択することが必要です。複数 WAN 構成に含めないと選択するインターフェイスがある場合 (インターフェイスのチェックボックスをオフにします) 、システムはそのネットワークにルートを作成しません。同じインターフェイスを含む Branch Office VPN 構成があると、問題を引き起こす原因となります。この場合、VPN トンネルはリモートピアとのネゴシエーションに失敗します。*[57153]*

Workaround
複数 WAN を使用しており、Branch Office VPN トンネルがリモートピアとのネゴシエーションに失敗するという問題が起こっている場合、複数 WAN 構成を開き、選択されている複数 WAN 構成モードの隣にある構成を選択します。複数 WAN 構成に適切なインターフェイスが含まれていることを確認してください。

- XTM デバイスの外部 IP アドレスとして IP 50 および IP 51 プロトコルを含むインバウンド静的 NAT ポリシーが存在すると、Branch Office VPN トンネルはトラフィックを通過させません。*[41822]*
- CRL 配布ポイント (WatchGuard Management Server またはお使いのサード パーティ CRL 配布サイト) がオフラインの場合、管理対象の Branch Office VPN トンネルは確立できません。*[55946]*
- BOVPN トンネル ルートにおける、*任意* の使い方は、Fireware XTM で変更されました。トンネル ルートのローカル部分に対して Branch Office VPN トンネルで任意を設定すると、0.0.0.0 のネットワークと 0.0.0.0 のサブネット マスクである(スラッシュ表記法では 0.0.0.0/0) と Fireware XTM は解釈します。リモートの IPSec ピアがフェーズ 2 ID として 0.0.0.0/0 を送信しない場合、フェーズ 2 のネゴシエーションは失敗します。*[40098]*

Workaround
トンネルルートのローカルまたはリモート部分に対して、*任意*を使用しないでください。トンネルルートのローカル部分を変更します。トンネルのルーティングに実際に関与する、コンピュータのIPアドレスを入力します(XTMデバイスの裏にあります)。トンネルルートのリモート部分 (またはフェーズ2IDのリモート部分) に対してデバイスが何を使っているか、リモートIPSecピアの管理者に問い合わせます。

- 構成中に多数の Branch Office VPN トンネルがある場合、そのトンネルが Policy Manager に表示されるまで時間が長くかかることがあります。*[35919]*

Workaround
Policy Manager から、**表示>ポリシーの強調表示**の順に選択します。**トラフィックのタイプに基づいて Firewall のポリシーを強調表示** チェック ボックスの選択を外します。

CLI の使用

Fireware XTM CLI (コマンドライン インターフェイス) は v11.x リリースで完全にサポートされています。CLI を起動して使用する方法については、 *『CLI コマンド リファレンス ガイド』*をご覧ください。CLI ガイドはこちらのドキュメンテーション Web ページ http://www.watchguard.com/help/documentation/xtm.asp をご覧ください。

技術サポート

技術的なサポートについては、WatchGuardテクニカルサポートまでお電話でお問い合わせいただくか、または次のWebサイトから、WatchGuard Portalにログインしてください: http://www.watchguard.com/support。技術サポートへのお問い合わせ時には、登録済みの製品シリアル番号、パートナーID のいずれかをお手元にご用意ください。

	電話番号
米国のエンド ユーザー	877-232-3531
米国以外のエンド ユーザー	+1-206-613-0456
WatchGuard 正規販売代理店	206-521-8375

Spanish (Español)

Notas de Lanzamiento de Fireware XTM v11.6.1

Dispositivos admitidos	XTMv, XTM 2, 3, 5, y 8 Series XTM 1050, XTM 2050
Compilación del Sistema Operativo de Fireware XTM	346666
Compilación de WatchGuard System Manager	347361
Fecha de la revisión	8 de agosto de 2012

Introducción

WatchGuard se complace en anunciar el lanzamiento de Fireware XTM v11.6.1 y WatchGuard System Manager v11.6.1. Puede instalar el sistema operativo Fireware XTM v11.6.1 en cualquier dispositivo WatchGuard XTM, que incluye 2 Series, 3 Series, 5 Series, 8 Series, dispositivos XTM 1050 y 2050; y con cualquier edición de XTMv. Este lanzamiento presenta soporte para los nuevos XTM 5 Series de alto rendimiento, modelos 515, 525, 535 y 545, y ofrece una actualización para nuestras interfaces de usuario localizadas y documentación. Este lanzamiento también incluye varias mejoras clave del producto:

- Un dispositivo XTM que se configuró en modo puente, ahora puede pasar tráfico VLAN entre conmutadores 802.1Q o puentes.
- FireCluster soporta XTM 25, 26 y modelos por cable 33.

Por último, hay varias correcciones de errores clave que se incluyeron en este lanzamiento y que se describen en la sección Problemas Solucionados.

Para obtener más información sobre las mejoras de las funciones que se incluyeron en el Fireware XTM v11.6.1, consulte la documentación del producto o revise las Novedades de Fireware XTM v11.6.1.

Antes de Empezar

Antes de instalar este lanzamiento, asegúrese de tener los siguientes requisitos:

- Un dispositivo de WatchGuard XTM 2 Series, 3 Series, 5 Series, 8 Series, XTM 1050 o XTM 2050, o XTMv (cualquier edición).
- Los componentes de hardware y software requeridos se muestran a continuación. Si usa WatchGuard System Manager (WSM), asegúrese de que su versión WSM sea igual o superior a la versión del sistema operativo Fireware XTM que instaló en su dispositivo XTM y la versión de WSM que instaló en su Management Server.
- Tecla de función para su dispositivo XTM: Si actualiza su dispositivo XTM desde una versión de sistema operativo Fireware XTM anterior, puede utilizar su tecla de función existente. Si usa XTMv, su tecla de función se debe generar con el número de serie que recibió cuando compró XTMv.

Tenga en cuenta que puede instalar y utilizar WatchGuard System Manager v11.6.1 y todos los componentes del servidor WSM con dispositivos que funcionan con versiones anteriores de Fireware XTM v11. En este caso, le recomendamos que utilice la documentación del producto que coincida con su versión de sistema operativo Fireware XTM.

Si posee un dispositivo físico XTM nuevo, asegúrese de usar las instrucciones en la *Guía de inicio rápido de XTM* que viene con su dispositivo. Si esta es una instalación nueva de XTMv, asegúrese de revisar cuidadosamente la *Guía de configuración de XTMv* para instrucciones importantes de configuración e instalación.

La documentación para este producto está disponible en el sitio web de WatchGuard en www.watchguard.com/help/documentation.

Localización

Este lanzamiento incluye interfaces actualizadas y localizadas de usuario de administración Fireware XTM (conjunto de aplicaciones WSM y Web UI) y ayuda del producto. Los idiomas admitidos son:

- Chino (Simplificado, República Popular China [PRC])
- Francés (Francia)
- Japonés
- Español (Latinoamericano)

> ***Note*** *Además de estos idiomas, ofrecemos el soporte de la Web UI localizada para coreano y chino tradicional. Sólo la UI Web en sí misma ha sido localizada. WSM y todos los archivos de ayuda y la documentación del usuario permanecen en inglés en el caso de estos dos idiomas.*

Tenga en cuenta que la mayor parte de la entrada de datos aún debe realizarse utilizando caracteres estándares del Código Estándar Estadounidense para el Intercambio de Información (ASCII). Puede utilizar otros caracteres que no sean del ASCII en algunas áreas de la interfaz de usuario (UI), entre ellas:

- Deny message del servidor proxy;
- título, términos y condiciones, y mensaje del hotspot inalámbrico; y
- usuarios, grupos y nombres de roles de WatchGuard Server Center.

Los datos enviados desde el sistema operativo del dispositivo (p. ej., datos de registro) se muestran sólo en inglés. Además, todos los elementos del menú Estado del Sistema de la UI Web y los componentes de software provistos por compañías externas quedan en inglés.

Fireware XTM Web UI

La UI Web se iniciará en el idioma que haya configurado en su explorador web de manera predeterminada. El nombre del idioma seleccionado actualmente se muestra en la parte superior de cada página. Para cambiar a un idioma diferente, haga clic en el nombre del idioma que aparece. Aparecerá una lista desplegable de idiomas y allí puede seleccionar el que desea utilizar.

WatchGuard System Manager

Cuando instala WSM, puede elegir qué paquetes de idiomas desea instalar. El idioma que se muestra en WSM coincidirá con el idioma que seleccione en su entorno de Microsoft Windows. Por ejemplo, si utiliza Windows XP y desea usar WSM en Japonés, ingrese en Panel de control > Opciones regionales y de idioma y seleccione Japonés de la lista de idiomas.

Log y Report Manager, CA Manager, Quarantine Web UI, y Hotspot Inalámbricas

Estas páginas web se muestran automáticamente en la preferencia de idioma que ha configurado en su explorador web.

Compatibilidad del Sistema Operativo Fireware XTM y WSM v11.6.1

Revisado en Junio de 2012

WSM/ Componente de Fireware XTM	Microsoft Windows XP SP2 (32 bits)	Microsoft Windows Vista (32-bit & 64 bits)	Microsoft Windows 7 (32-bit & 64 bits)	Microsoft Windows Servidor 2003 (32 bits)	Microsoft Windows Servidor 2008 & 2008 R2*	Mac OS X v10.5, v10.6, & v10.7
Aplicación WatchGuard System Manager	✓	✓	✓	✓	✓	
Fireware XTM Web UI *Navegadores Admitidos: IE 7 y 8, Firefox 3.x & superior*	✓	✓	✓	✓	✓	✓
Web UI de Log and Report Manager *Navegadores Admitidos: Firefox 3.5 & superior, IE8 & superior, Safari 5.0 & superior, Chrome 10 & superior. Se necesita Javascript.*	✓	✓	✓	✓	✓	✓
Servidores de WatchGuard	✓	✓	✓	✓	✓	
Software Agente de Inicio de Sesión Único (Incluye Event Log Monitor)				✓	✓	
Software Cliente de Inicio de Sesión Único	✓	✓	✓	✓	✓	
Software Agente de Terminal Services**				✓ ***	✓	
Software Cliente de Mobile VPN with IPSec	✓	✓	✓			Soporta cliente (Cisco) IPSec nativo
Software Cliente de Mobile VPN with SSL	✓	✓	✓	✓		✓

**Soporte para Microsoft Windows Server 2008 32 bits y 64 bits; soporte para Windows Server 2008 R2 64 bits.*

** * El soporte de Terminal Services con autenticación de Inicio de sesión único o manual funciona en entornos Microsoft Terminal Services o Citrix XenApp 4.5, 5.0, 6.0 y 6.5.*

**** Se necesita Microsoft Windows Server 2003 SP2.*

Soporte de Autenticación

Este cuadro le brindará una revisión rápida de los tipos de servidores de autenticación que se soportan mediante las funciones clave del Fireware XTM. Al usar un servidor de autenticación le brinda la capacidad para configurar firewall de usuario y de grupo y políticas VPN en su configuración del dispositivo XTM. Con cada tipo de servidor de autenticación de terceros que se soporta, puede especificar una dirección IP de servidor de respaldo para conmutación por error.

✓ — Completamente admitido por WatchGuard

 — Todavía no admitido, pero probado con éxito por los clientes de WatchGuard

	Active Directory [1]	LDAP	RADIUS [2]	SecurID [2]	Firebox (Firebox-DB) Autenticación Local
Mobile VPN with IPSec/Shrew Soft	✓	✓	✓ [3]	–	✓
Mobile VPN with IPSec para iPhone/iPad iOS y Sistema Operativo MAC X				✓	✓
Mobile VPN with SSL para Windows	✓	✓	✓ [4]	✓ [4]	✓
Mobile VPN with SSL para Mac	✓	✓	✓	✓ [5]	✓
Los usuarios de Mobile VPN with PPTP pueden autenticarse en el dispositivo XTM o usar autenticación extendida en un servidor RADIUS o VACMAN Middleware Server.	–	–	✓	N/D	✓
Página Web de Autenticación Incorporada en Puerto 4100	✓	✓	✓	✓	✓
Soporte de Inicio de Sesión Único Windows (con o sin software cliente)	✓	–	–	–	–
Autenticación Manual de Terminal Services	✓				✓
Autenticación de Terminal Services con Inicio de Sesión Único	✓ [6]	–	–	–	–
Autenticación Manual Citrix					✓

1. *El soporte Active Directory incluye soporte tanto único como múltiple, excepto que se indique lo contrario.*
2. *El soporte RADIUS y SecurID incluyen soporte para contraseñas únicas y autenticación de respuesta o desafío integrada con RADIUS. En varios casos, también se puede utilizar SecurID con otras implementaciones RADIUS, incluso Vasco.*
3. *El cliente Shrew Soft no admite autenticación de dos factores.*
4. *Fireware XTM soporta RADIUS Filter ID 11 para autenticación de grupo.*
5. *Admite modo Tokencode + PIN. No admite modo Next Tokencode y contraseñas únicas SMS.*

6. *Admite configuraciones Active Directory de dominio único.*
7. *Para obtener más información sobre la compatibilidad del Sistema Operativo que se admite para WatchGuard TO Agent y SSO Agent, consulte el Fireware XTM actual y el cuadro de Compatibilidad de sistema operativo WSM.*

Requisitos del Sistema XTMv

Para instalar un dispositivo XTMv virtual, debe tener un host VMware ESXi 4.1 ó 5.0 instalado en cualquier hardware de servidor que soporte la versión ESXi que utiliza. También debe instalar el Cliente VMware vSphere 4.1 ó 5.0 en un equipo que admite Windows. Si prefiere, puede utilizar Servidor vCenter en vez del cliente vSphere.

Los requisitos de hardware para XTMv son los mismos que los requisitos de hardware para VMware ESXi. Para obtener más información sobre la compatibilidad de hardware VMware, consulte la Guía de compatibilidad VMware en http://www.vmware.com/resources/compatibility/search.php.

Cada máquina virtual XTMv requiere 3 GB de espacio en disco.

Configuraciones de Asignación de Recurso Recomendadas

	Oficina Pequeña	Oficina Mediana	Oficina Grande	Centro de Datos
CPUs virtuales	1	2	4	8 o más
Memoria	1 GB	2 GB	4 GB	4 GB o más

Cómo Descargar Software

1. Inicie sesión en el Portal de WatchGuard y seleccione la pestaña Artículos & Software.
2. Desde la Búsqueda, desmarque las casillas Artículos y Problemas conocidos, y busque las descargas de software disponibles. Seleccione el dispositivo XTM para el que desea descargar el software.

Hay varios archivos de software disponibles para descargar. Vea las descripciones a continuación para saber qué paquetes de software necesitará para su actualización.

WatchGuard System Manager

Todos los usuarios ahora pueden descargar el software de WatchGuard System Manager. Con este paquete de software, puede instalar WSM y el software de WatchGuard Server Center:

`WSM11_6_1s.exe` : utilice este archivo para actualizar WatchGuard System Manager de v11.x a WSM v11.6.1.

Sistema Operativo Fireware XTM

Seleccione la imagen del sistema operativo Fireware XTM correcta para su dispositivo XTM. Use el archivo .exe si desea instalar o actualizar el sistema operativo utilizando WSM. Use el archivo .zip si desea instalar o actualizar el sistema operativo utilizando la Interfaz de usuario web Fireware XTM. Use el archivo .ova para implementar un dispositivo nuevo de XTMv.

Si tiene...	Elija entre estos paquetes de sistema operativo Fireware XTM
XTM 2050	`XTM_OS_XTM2050_11_6_1.exe` `xtm_xtm2050_11_6_1.zip`
XTM 1050	`XTM_OS_XTM1050_11_6_1.exe` `xtm_xtm1050_11_6_1.zip`
XTM 8 Series	`XTM_OS_XTM8_11_6_1.exe` `xtm_xtm8_11_6_1.zip`
XTM 5 Series	`XTM_OS_XTM5_11_6_1.exe` `xtm_xtm5_11_6_1.zip`
XTM 330	`XTM_OS_XTM330_11_6_1.exe` `xtm_xtm330_11_6_1.zip`
XTM 33	`XTM_OS_XTM33_11_6_1.exe` `xtm_xtm33_11_6_1.zip`
XTM 2 Series Modelos 21, 22, 23	`XTM_OS_XTM2_11_6_1.exe` `xtm_xtm2_11_6_1.zip`
XTM 2 Series Modelos 25, 26	`XTM_OS_XTM2A6_11_6_1.exe` `xtm_xtm2a6_11_6_1.zip`

XTMv
Todas las ediciones
	`xtmv_11_6_1.ova`
	`xtmv_11_6_1.exe`
	`xtmv_11_6_1.zip`

Software de Inicio de Sesión Único

Hay dos archivos disponibles para descargar si utiliza Inicio de Sesión Único.

- `WG-Authentication-Gateway_11_6.exe` (El software SSO Agent: se requiere para Inicio de Sesión Único e incluye Event Log Monitor opcional para SSO sin cliente)
- `WG-Authentication-Client_11_6.msi` (Software de SS0 Client: opcional)

Para obtener información sobre cómo instalar y configurar Inicio de Sesión Único, vea la documentación del producto.

Software de Autenticación de Terminal Services

- `TO_AGENT_32_11_6.exe` (soporte para 32 bits)
- `TO_AGENT_64_11_6.exe` (soporte para 64 bits)

Cliente de Mobile VPN with SSL para Windows y Macintosh

Hay dos archivos disponibles para descargar si utiliza Mobile VPN with SSL:

- `WG-MVPN-SSL_11_6.exe` (Software cliente para Windows)
- `WG-MVPN-SSL_11_6.dmg` (Software cliente para Mac)

Cliente Mobile VPN with IPSec para Windows

Puede descargar el cliente Shrew Soft VPN para Windows desde nuestro sitio web. Para obtener más información sobre cliente Shrew Soft VPN, consulte la ayuda o visite el sitio web de Shrew Soft, Inc..

Actualización de Fireware XTM v11.x a v11.6.1

Antes de realizar la actualización de Fireware XTM v11.x a Fireware XTM v11.6.1, descargue y guarde el archivo del sistema operativo de Fireware XTM que coincida con el dispositivo WatchGuard que desea actualizar. Puede encontrar todo el software disponible en Portal de WatchGuard Artículos & pestaña de Software. Puede utilizar Policy Manager o la Web UI para finalizar el procedimiento de actualización. Le recomendamos enfáticamente que realice una copia de seguridad de la configuración de su dispositivo y de la configuración de WatchGuard Management Server antes de realizar la actualización. No se puede regresar a la versión anterior sin estos archivos de copia de seguridad.

Si usa WatchGuard System Manager (WSM), asegúrese de que su versión WSM sea igual o superior a la versión del sistema operativo Fireware XTM que instaló en su dispositivo XTM y la versión de WSM que instaló en su Management Server.

> ***Note*** *Si actualiza a WSM v11.6.1 desde WSM v11.4.x o anterior, es importante realizar una copia de seguridad de sus datos de Log y Report Server mediante el procedimiento que se describe en Base de consulta, artículo 6995. Esto es necesario ya que la estructura de la base de datos de Log y Report Server cambió en WSM v11.5.1. Cuando actualiza WSM v11.5.1 o superior por primera vez, las marcas de tiempo del registro existente y los datos de informe se convertirán a UTC desde la zona horaria local. Este artículo de Base de consulta le brinda detalles sobre esta actualización e información importante sobre Log y Report Manager (también nuevo en WSM v11.5.1).*

Realice una Copia de Seguridad de su Configuración de WatchGuard Management Server

Desde la computadora donde instaló el Management Server:

1. Desde WatchGuard Server Center, seleccione **Copia de Seguridad/Restaurar Management Server**.
   Se inicia el WatchGuard Server Center Backup/Restore Wizard.
2. Haga clic en **Siguiente**.
   Aparece la pantalla Seleccionar una acción.
3. Seleccione **Configuración de respaldo**.
4. Haga clic en **Siguiente**.
   Aparece la pantalla Especificar un archivo de copia de seguridad.
5. Haga clic en **Buscar** para seleccionar una ubicación para el archivo de copia de seguridad. Asegúrese de guardar el archivo de configuración en una ubicación a la que pueda acceder posteriormente para restablecer la configuración.
6. Haga clic en **Siguiente**.
   Aparece la pantalla WatchGuard Server Center Backup/Restore Wizard ha finalizado.
7. Haga clic en **Finalizar** para salir del asistente.

Actualización a Fireware XTM v11.6.1 desde la Web UI

1. Vaya a **Sistema > Imagen de Copia de Seguridad** o utilice la característica de seguridad USB para realizar una copia de seguridad de su archivo de configuración actual.

2. En su equipo de administración, inicie el archivo del sistema operativo que descargó del Centro de Descargas de Software de WatchGuard.
   Si utiliza el instalador basado en Windows, esta instalación extrae un archivo de actualización llamado *[xtm series]_[product code].sysa-dl* a la ubicación por defecto de C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\11.6.1\[model] or [model][product_code].
3. Conéctese a su dispositivo XTM con la UI Web y seleccione **Sistema > Actualización del Sistema Operativo**.
4. Busque la ubicación de *[xtm series]_[product code].sysa-dl* del Paso 2 y haga clic **Actualizar**.

Actualización a Fireware XTM v11.6.1 desde WSM/Policy Manager v11.x

1. Seleccione **Archivo > Copia de Seguridad** o utilice la característica de seguridad USB para realizar una copia de seguridad de su archivo de configuración actual.
2. En su equipo de administración, inicie el archivo ejecutable del sistema operativo que descargó del portal de WatchGuard. Esta instalación extrae un archivo de actualización llamado *[xtm series]_ [product code].sysa-dl* a la ubicación por defecto de C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\11.6.1\[model] or [model][product_code].
3. Instale y abra WatchGuard System Manager v11.6.1 Conéctese al dispositivo XTM e inicie Policy Manager.
4. Desde Policy Manager, seleccione **Archivo > Actualizar**. Cuando se le solicite, busque y seleccione el archivo *[xtm series]_[product code].sysa-dl* del Paso 2.

Información General para Actualizaciones del Software del Servidor de WatchGuard

No es necesario desinstalar su software cliente o servidor anterior v11.x cuando realiza la actualización de v11.0.1 o superior a WSM v11.6.x. Puede instalar el software cliente y el servidor v11.6.x encima de su instalación existente para actualizar sus componentes de software de WatchGuard.

Actualice su FireCluster a Fireware XTM v11.6.1

Hay dos métodos para actualizar el Sistema Operativo de Fireware XTM en su FireCluster. El método que le corresponde usar depende de la versión de Fireware XTM que utilice actualmente.

Actualización de FireCluster desde Fireware XTM v11.4.x ó v11.5.x

Siga estos pasos para actualizar un FireCluster desde Fireware XTM v11.4.x ó v11.5.x a Fireware XTM v11.6.x:

1. Abra el archivo de configuración del clúster en el Policy Manager
2. Seleccione **Archivo > Actualizar**.
3. Ingrese la contraseña de configuración.
4. Ingrese o seleccione la ubicación del archivo de actualización.
5. Para crear una imagen de copia de seguridad, seleccione **Sí**.

   Aparece una lista de los miembros del clúster.
6. Seleccione la casilla de selección para cada dispositivo que desee actualizar.

   Aparece un mensaje cuando la actualización de cada dispositivo esté concluida.

Cuando la actualización está concluida, cada clúster miembro se reinicia y se reintegra al clúster. Si actualiza ambos dispositivos en el clúster a la vez, los dispositivos se actualizan de a uno por vez. El propósito de esto es asegurar que no haya una interrupción en el acceso de red al momento de la actualización.

El Policy Manager actualiza primero el miembro de respaldo y luego espera que se reinicie y vuelve a juntar el clúster como una copia de seguridad. El Policy Manager actualiza el principal. Tenga en cuenta que el rol del principal no cambiará hasta que se reinicie para completar el proceso de actualización. En ese momento la copia de seguridad finaliza como el principal.

Para realizar la actualización desde una ubicación remota, asegúrese de que la interfaz de FireCluster para la dirección IP de administración esté configurada en la interfaz externa y que las direcciones IP de administración sean públicas y enrutables. Para obtener más información, consulte Acerca de la Interfaz para Dirección IP de Administración.

Actualización de FireCluster desde Fireware XTM v11.3.x

Para actualizar un FireCluster desde Fireware XTM v11.3.x a Fireware XTM v11.6.x, debe realizar una actualización manual. Para conocer los pasos para la actualización manual, consulte el artículo Base de consulta Actualizar el Sistema Operativo de Fireware XTM para un FireCluster.

Instrucciones de Regresión

Regresar de WSM v11.6.x a WSM v11.x.

Si desea regresar de v11.6.x a una versión anterior de WSM, debe desinstalar WSM v11.6.x. Cuando lo desinstale, elija **Sí** cuando el desinstalador le pregunte si desea eliminar la configuración del servidor y los archivos de datos. Después de eliminar los archivos de datos y de configuración del servidor, debe restablecer los archivos de datos y configuración del servidor que guardó en una copia de seguridad antes de realizar la actualización a WSM v11.6.x.

A continuación, instale la misma versión de WSM que utilizó antes de realizar la actualización a WSM v11.6.x. El instalador debe detectar su configuración actual del servidor e intentar restablecer sus servidores desde el cuadro de diálogo **Finalizar**. Si utiliza un WatchGuard Management Server, utilice el WatchGuard Server Center para restablecer la configuración del Management Server de respaldo que creó antes de realizar la actualización a WSM v11.6.x por primera vez. Verifique que todos los servidores WatchGuard estén en funcionamiento.

Regresar de Fireware XTM v11.6.x a Fireware XTM v11.x

> ***Note*** *No puede regresar un dispositivo XTM 2050, un XTM 330 o XTM 33 a una versión de sistema operativo Fireware XTM anterior a v11.5.1. No puede regresar un XTM 5 Series modelo 515, 525, 535 ó 545 a una versión de sistema operativo Fireware XTM anterior a v11.6.1. No puede regresar un XTMv a una versión de sistema operativo Fireware XTM anterior a v11.5.4.*

Si desea regresar de Fireware XTM v11.6.x a una versión anterior de Fireware XTM, puede:

- Restablecer la imagen de copia de seguridad completa que creó cuando realizó la actualización a Fireware XTM v11.6.x para completar el regreso a la versión anterior; o
- Utilizar el archivo de copia de seguridad USB que creó antes de realizar la actualización como su imagen de restablecimiento automático, y luego iniciar sesión en modo de recuperación con la unidad USB conectada a su dispositivo. Esta no es una opción para usuarios de XTMv.

Para iniciar un dispositivo WatchGuard XTM 330, 5 Series, 8 Series, XTM 1050 o XTM 2050 en modo de recuperación:

1. Apague el dispositivo XTM.
2. Presione la flecha hacia arriba en el panel delantero del dispositivo mientras lo enciende.

3. Mantenga el botón presionado hasta que aparezca "Iniciando Modo de Recuperación" en la pantalla LCD.

Para iniciar un dispositivo WatchGuard XTM 2 Series o XTM 33 en modo de recuperación:

1. Desconecte la alimentación.
2. Presione y sostenga el botón Restablecer en la parte posterior mientras conecta la alimentación al dispositivo.
3. Mantenga el botón presionado hasta que la luz Attn en la parte delantera se ilumine de color naranja.

Problemas Solucionados

El lanzamiento de Fireware XTM v11.6.1 soluciona varios problemas hallados en los lanzamientos anteriores de Fireware XTM v11.x.

General

- Se resolvieron varios problemas en este lanzamiento que hicieron que los dispositivos XTM se bloqueen cuando se configuró para usar Application Control o IPS. *[66937, 65426, 65636, 67312, 66135, 67159, 67399, 67310]*
- Se resolvió un problema que causó que algunos procesos del dispositivo XTM se bloqueen cuando funciona una prueba de vulnerabilidad publicada por defecto Mu Dynamics. *[66490]*
- Se resolvió un problema que causó que un núcleo se bloquee y se reinicie el dispositivo. *[67329]*
- Ahora el dispositivo XTM 2 Series puede manejar una gran transferencia de archivo sin la inestabilidad de la interfaz. *[67367]*
- Se resolvió un problema que causó que datos incorrectos se mostraran en la pantalla LCD XTM 5 Series. *[67197]*

WatchGuard System Manager

- Ahora Policy Manager muestra los límites VLAN correctos para XTM 5 Series modelos 505, 510, 520 y 530 con una tecla de función estándar Fireware XTM (no Pro). *[67780]*

Web UI

- Ahora puede configurar y aplicar de manera exitosa las acciones de Administración de tráfico para dispositivos XTM 2 y 3 Series desde la Web UI. *[67221, 66645]*

Centralized Management

- Ahora los dispositivos Firebox X Edge e-Series se pueden administrar de manera exitosa con plantillas. *[67658]*

Generación de Registros & Presentación de Informes

- El mensaje de notificación que se envía cuando un Log local o base de datos de Informe se inactiva, ahora muestra de manera correcta la dirección IP del host en vez de... *[41731]*
- Ahora el Log Server puede manejar archivos de copia de seguridad mayores a 2 GB de tamaño sin generar un mensaje de error: "Error (8199), Excepción durante copia de seguridad de datos de registro más viejos: El archivo no es un archivo zip; excepción". *[66811]*
- Ahora el informe de actividad de concesión DHCP funciona correctamente. *[66062]*
- Ahora el Log Collector maneja datos de registro del dispositivo XTM que abarcan registros SSL/TLS sin bloquearse. *[66347]*

Servicio de Seguridad y Proxies

- Se solucionó un problema que causó bajo rendimiento en XTM 2 Series modelos 25 y 26 debido a una asignación de memoria incorrecta para firmas de suscripción de seguridad. *[67240]*
- Ahora un mensaje de negación se envía de manera correcta al explorador web en la mayoría de los casos cuando Application Control bloquea el contenido en la categoría Web/Web 2.0. *[66201]*
- La hora de actualización de la base de datos automática de WebBlocker no se desactiva más por una hora cuando se aplica el ahorro de energía eléctrica en el host de las zonas horarias del servidor. *[67551]*

Redes

- Si usa PPPoE o DHCP para una interfaz externa en un dispositivo XTM que se configuró para utilizar WAN múltiple, el dispositivo XTM ya no pierde las rutas por defecto para interfaces externas luego de volver a conectar una interfaz externa. *[67424, 67520]*
- Se solucionó un problema que causó la falla de una ruta estática luego de que una interfaz externa configurada para usar PPPoE se desconecta, luego se vuelve a conectar. *[67520]*
- Ahora el tráfico VLAN etiquetado se reconoce de manera correcta cuando un dispositivo XTM se configura en modo puente. *[64355]*

Referencia de la Command Line Interface de Fireware XTM

- Ahora el comando CLI "restablecer todas las predeterminadas de fábrica" restaura de manera exitosa un dispositivo a sus configuraciones predeterminadas de fábrica. *[66240]*

FireCluster

- Se solucionó un problema que causó que el Policy Manager mostrara de manera incorrecta una dirección IP de interfaz como 0.0.0.0/24 cuando visualizaba una configuración FireCluster para un clúster en modo directo. *[63551]*

Mobile VPN

- El proceso Mobile VPN with SSL ya no se bloquea durante una conmutación por error de FireCluster. *[66118]*

Problemas Conocidos y Limitaciones

Estos son problemas conocidos de Fireware XTM v11.6.1 y todas las aplicaciones de administración. Cuando esté disponible, incluimos una solución para el problema.

General

- Cuando conecta una unidad USB a un dispositivo XTM, el dispositivo no guarda automáticamente una captura de pantalla de soporte en la unidad USB. *[64499]*

> **Workaround**
> Utilice el comando CLI “Habilitar diagnóstico de la unidad USB” para habilitar el dispositivo y guardar una captura de pantalla de soporte de diagnóstico en la unidad USB. Para obtener más detalles sobre este comando, consulte la *Guía de referencia de Command Line Interface*.

- La versión "Sysb" que aparece en el informe de estado del Firebox System Manager mostrará un espacio en blanco para los modelos XTM 2, 5, 8 y 1050 que fueron fabricados antes del lanzamiento de XTM v11.5.1.
- La protección contra la congestión ICMP funciona diferente en 11.5.1 con respecto a las versiones anteriores. En v11.5.1, el dispositivo XTM cuenta la cantidad total combinada de solicitudes y respuestas de ping en vez de contar solo la cantidad total de solicitudes de ping. Debido a que el umbral predeterminado para la protección contra los ataques de congestión del servidor ICMP no aumentó, la protección contra la congestión podría activarse con más frecuencia que en los lanzamientos anteriores. *[63094]*

> **Workaround**
> En las configuraciones de Administración de paquetes predeterminadas, aumente el umbral para disminuir Ataques de congestión del servidor ICMP, del valor predeterminado de 1000 paquetes/segundo a un número mayor.

- Cuando el nivel de memoria libre en su dispositivo XTM es menor que 20 M, si guarda la configuración del dispositivo XTM en el dispositivo se pueden generar problemas en la red. *[64474]*
-
- La interfaz ETH1 en el XTM 830F es un puerto de fibra óptica, por lo tanto no puede usar el WSM Quick Setup Wizard desde un equipo con una interfaz Ethernet. Utilice un equipo con un Fiber NIC o conecte utilizando un conmutador con ambas interfaces, Ethernet y Fiber. *[59742]*
- Para desconectar un dispositivo XTM 5 Series, debe presionar y mantener el conmutador de energía trasero durante 4 ó 5 segundos. *[42459]*
- Para los dispositivos XTM 5 Series, la interfaz 0 no admite la Interfaz cruzada dependiente del medio (MDIX) automática y no detecta la polaridad del cable automáticamente.
- En los dispositivos XTM 2 Series, la carga promedio aparece siempre con valor 1 o superior, incluso cuando no hay carga en el dispositivo. *[63898]*
- Un dispositivo XTM 2 puede tardar hasta 5 minutos en reiniciarse.
- Cuando usa las funciones **Policy Manager > Archivo > Copia de Seguridad** o **Restablecer,** el proceso puede tardar mucho tiempo pero se completa con éxito. *[35450]*
- No puede regresar un dispositivo XTM 2 Series de v11.5.1 a v11.4.1 con la opción de **Actualizar el sistema operativo** en la Web UI. *[63323]*

- Amazon Web Services (AWS) requiere el uso de BGP mediante un túnel IPSec. Las operaciones descritas por Amazon.com para admitir los Amazon Web Services no son admitidas actualmente por los productos WatchGuard. *[41534]*
- El informe de configuración de XTM no contiene todas las configuraciones. Las configuraciones que no se incluyen son:
  - Dirección IP secundaria de interfaz *[66990]*
  - Ajustes de QoS configurados *[66992]*
  - Vínculos MAC estáticos *[66993]*
  - Configuración del IPv6 *[66994]*

XTMv

- El XTMv no cambia de manera automática el certificado autofirmado cuando cambia su número de serie. *[66668]*

> **Workaround**
> Un certificado autofirmado nuevo con el número de serie correcto se generará si elimina manualmente el certificado desde Firebox System Manager > Visualizar > Certificados y luego reiniciar el dispositivo XTMv.

- Si importa el archivo OVA en VMware Player (el cual no se admite de manera oficial en este lanzamiento), debe usar la tecla "Ingresar" de su teclado para aceptar el Acuerdo de licencia de usuario final (EULA) del XTMv. Aparece la primera página del asistente. **Aceptar** y **Los botones de Cancelación** en la parte final del EULA no aparecen en VMware Player.

WatchGuard System Manager

- Si usa Firebox System Manager para hacer ping sobre un túnel VPN, obtendrá un mensaje que dice "Espacio de Memoria Intermedia No Disponible". No es un problema de memoria. Visualiza ese mensaje si el túnel VPN no se estableció. Asegúrese de que el túnel VPN esté en funcionamiento y vuelva a intentarlo. *[59339]*
- WatchGuard System Manager no muestra la dirección IP correcta para la puerta de enlace determinada de un dispositivo XTM que no tiene interfaz externa. *[56385]*
- Cuando instale el WatchGuard System Manager o cualquier software de servidor en un equipo que funciona con Microsoft Windows XP, no se debe activar el modo de compatibilidad aún si Windows lo indica, para algunas de las aplicaciones WSM, incluso el instalador. *[56355]*
- Es posible que los dispositivos Firebox o XTM de administración remota que se configuran en Modo directo no puedan conectarse a Management Server que está detrás de un Firebox de puerta de enlace o un dispositivo XTM también configurado en Modo directo. *[33056]*
- Si restaura una imagen de copia de seguridad a un dispositivo del cliente administrado por un Management Server, es posible que el secreto compartido se desincronice.

> **Workaround**
> Conéctese a Management Server desde WSM. Seleccione el dispositivo administrado y luego **Actualizar dispositivo**. Seleccione el botón de radio **Reiniciar la configuración del servidor (dirección IP/nombre de host, secreto compartido**).

- Durante una actualización, instalación o desinstalación WSM en sistemas Windows 64 bits, cualquier aplicación que funcione y se detecte a través del instalador WSM se puede detener de manera exitosa, pero el instalador puede no reconocer que se detuvieron. *[39078]*

> **Workaround**
> Cierre la aplicación del instalador. Haga clic con el botón derecho en el ícono WatchGuard Server Center en su barra de tareas de Windows y salga del WatchGuard Server Center. Asegúrese de que todas las aplicaciones que se detectaron se detengan y luego vuelva a intentar la instalación o desinstalación de WSM.

- Cuando ejecute el instalador de WSM v11.3.x o superior (ya sea el componente del cliente WSM únicamente o cualquier componente seleccionado del servidor WSM) en Microsoft SBS (Small Business Server) 2008 y 2011 en un equipo que tiene instalado un sistema operativo de 64 bits, aparecerá un error de Microsoft Windows "*IssProc.x64 ha dejado de funcionar*". Cuando cierre el cuadro de diálogo de error, la instalación se completa. *[57133]*

Web UI

- La Fireware XTM Web UI no admite la configuración de algunas funciones. Estas funciones incluyen:
  - FireCluster
  - Exportación de certificados
  - No puede activar o desactivar la notificación de eventos de BOVPN.
  - No puede agregar o quitar entradas de ARP estáticas en la tabla ARP del dispositivo.
- No puede obtener el perfil de configuración de usuario final de Mobile VPN with IPSec cifrado, conocido como el archivo .wgx. La Web UI genera sólo una versión de texto simple del perfil de configuración de usuario final, con extensión de archivo .ini.
- No puede editar el nombre de una política, usar una dirección personalizada en una política ni usar el nombre de host (búsqueda de DNS) para agregar una dirección IP a una política.
- Si configura una política en la Web UI con un estado de Desactivado, luego abra Policy Manager y realice un cambio en la misma política, la acción asignada a la política cuando niega paquetes cambia a Enviar TCP RST. *[34118]*
- No puede crear archivos de configuración de Mobile VPN with IPSec de solo lectura con la Web UI. *[39176]*

Command Line Interface (CLI)

- La CLI no admite la configuración de algunas funciones:
  - No puede agregar o editar una acción de proxy.
  - No puede obtener el perfil de configuración de usuario final de Mobile VPN with IPSec cifrado, conocido como el archivo .wgx. La CLI genera sólo una versión de texto simple del perfil de configuración de usuario final, con extensión de archivo .ini.
- La CLI realiza una validación mínima de entrada para varios comandos.
- Para el XTM 2050, la salida del comando del CLI "mostrar interfaz" no indica claramente el número de interfaz que utiliza en el CLI para configurar una interfaz. El comando del CLI “mostrar interfaz” muestra el número de interfaz que aparece en la etiqueta de interfaz al frente del dispositivo (A0, A2 … A7; B0, B1 … B7; C0, C1), seguido de un guión y de un número consecutivo de interfaz (0 al 17) para todas las interfaces. *[64147]*

Workaround
Utilice el número consecutivo de interfaz que aparece después del guión como número de interfaz para configurar la interfaz. Para las interfaces B1-9, el número de interfaz en el comando CLI debe estar en el rango del 8 al 15. Para las interfaces C0-1, el número de interfaz en el comando CLI debe ser 16, 17.

Servidores Proxy

- El Policy Manager y la Web UI no ofrecen alguna advertencia de que la anulación de WebBlocker puede no funcionar para HTTPS. *[67208]*
- HTTPS DPI (Inspección profunda de paquetes) no funciona para usuarios que utilizan IE 9.0 con TLS 1.1 y 1.2 habilitadas, pero TLS 1.0 y SSL 3.0 no habilitadas. *[65707]*

Workaround
Utilice un explorador diferente, o active TLS 1.0 y SSL 3.0 en su configuración IE 9.0.

- EL dispositivo XTM puede almacenar solamente un certificado de servidor Proxy HTTPS y puede proteger solamente un sitio Web HTTPS por vez. *[41131]*
- Cuando un dispositivo XTM está trabajando con una carga alta, es posible que algunas conexiones proxy no terminen correctamente. *[61925, 62503]*
- La capacidad para utilizar un servidor proxy HTTP de caché no está disponible en conjunto con el proxy TCP-UDP. *[44260]*
- No puede realizar una llamada basada en SIP desde un softphone Polycom PVX detrás de un Firebox a un Polycom PVX en la red externa. *[38567]*

Workaround
Puede usar el protocolo H.323 en lugar del SIP.

- Cuando intenta transmitir videos de YouTube de un dispositivo Apple que funciona con iOS, puede ver este mensaje de error: "El servidor no está configurado correctamente".

Workaround
1. Edite su política de proxy HTTP.
2. Haga clic en **Ver/Editar proxy**.
3. Seleccionar el **Permitir solicitudes de rango a través del no modificado** seleccione esta casilla de verificación.
4 Guarde este cambio en su dispositivo XTM.

- El SIP-ALG no envía el encabezado de contacto correctamente cuando éste contiene un nombre de dominio. Sólo envía una cadena vacía de: Contacto: < >. Si el encabezado de contacto contiene una dirección IP, el SIP-ALG envía el encabezado de contacto correctamente: Contacto: <sip:10.1.1.2:5060>. *[59622]*

Workaround
Configure el PBX para enviar el encabezado de contacto con una dirección IP, no un nombre de dominio.

Suscripciones de Seguridad

- Alguna información de firmas IPS, como el número de CVE, no está disponible en Firebox System Manager. Proporcionamos capacidades de búsqueda e información CVE para firmas IPS en un portal de seguridad web para IPS en el sitio web de WatchGuard, al cual puede acceder en http://www.watchguard.com/SecurityPortal/ThreatDB.aspx
- La detección de Skype bloquea sólo las nuevas sesiones de Skype. Si un usuario ya inició sesión en Skype y tiene una sesión de Skype iniciada cuando se activa Application Control, es posible que Application Control no detecte la actividad.
- En los dispositivos XTM 2 Series únicamente, Application Control se desactiva de manera temporaria durante una actualización, una copia de seguridad o una restauración. Cuando la operación se completa, Application Control comienza a funcionar nuevamente.
- No se puede asignar un rol para la administración de Application Control desde la función de administración basada en roles de WatchGuard System Manager. *[59204]*
- No se puede utilizar un WebBlocker Server a través de un túnel VPN para sucursales. *[56319]*

Redes

- Si creó de manera manual las políticas de enrutamiento dinámico en Fireware XTM v11.5.x o anterior, las listas Para y De en estas políticas se borran cuando actualiza a v11.6. Si se activa el enrutamiento dinámico, se crearán nuevas políticas de manera automática cuando actualice. *[67721]*
- El Verificador de política no funciona cuando su dispositivo XTM se configura en Modo puente. *[66855]*
- Un apóstrofe en el nombre de la reserva DHCP causa la falla de la reserva DHCP. *[65529]*
- No se pueden configurar las acciones de administración de tráfico ni utilizar el marcado QoS en VLAN. *[56971, 42093]*
- No puede conectar una interfaz inalámbrica a una interfaz VLAN. *[41977]*
- El Web Setup Wizard puede fallar si su computadora se conecta directamente a un dispositivo XTM 2 Series como un cliente de Protocolo de configuración dinámica de host (DHCP) cuando inicia el Web Setup Wizard. Esto puede ocurrir porque la computadora no puede obtener una dirección IP lo suficientemente rápido después de que el dispositivo se reinicia durante el asistente. *[42550]*

Workaround
1. Si su computadora se conecta directamente al dispositivo XTM 2 Series durante el Web Setup Wizard, use una dirección IP estática en su computadora.
2. Use un interruptor o concentrador entre su computadora y el dispositivo XTM 2 Series cuando ejecute el Web Setup Wizard.

- Cuando se configura una secondary network para un dispositivo XTM 2 Series configurado en Modo Drop-In, a veces puede requerir unos minutos que las computadoras que se conectan a la secondary network aparezcan en la lista de ARP del XTM 2 Series. *[42731]*
- Debe asegurarse de que las interfaces de red desactivadas no tengan la misma dirección IP que alguna interfaz de red activa o pueden presentarse problemas de enrutamiento. *[37807]*
- Si activa el enlace de la dirección MAC/IP con la casilla de selección Sólo permitir tráfico enviado desde o hacia estas direcciones MAC/IP, no agregue entradas en la tabla, la función de enlace de MAC/IP no se activa. Esto es para ayudar a garantizar que los administradores no se bloqueen de forma accidental desde su propio dispositivo XTM. *[36934]*

- Las interfaces de red que forman parte de una configuración de bridge se desconectan y vuelven a conectarse automáticamente cuando guarda una configuración de una computadora en la red en bridge que incluye cambios de configuración a una interfaz de red. *[39474]*
- Cuando cambia la dirección IP de una VLAN configurada en una interfaz externa de estática a PPPoE, y el Firebox no puede obtener una dirección PPPoE, Firebox System Manager y la Web UI pueden continuar mostrando la dirección IP estática anteriormente utilizada. *[39374]*
- Cuando configura su dispositivo XTM con una configuración de Modo de Enrutamiento Combinado, cualquier interfaz hacia la cual se establece el bridge muestra su interfaz y dirección IP privada predeterminada como 0.0.0.0 en la Web UI. *[39389]*
- Cuando configura su dispositivo XTM en Modo Bridge, la pantalla de LCD de su dispositivo XTM muestra la dirección IP de las interfaces con bridge como 0.0.0.0. *[39324]*
- Cuando configura su dispositivo XTM en Modo Bridge, la función de redirección HTTP se puede configurar desde la interfaz de usuario, pero no funciona en este lanzamiento. *[38870]*
- El enlace de direcciones MAC/IP estáticas no funciona cuando su dispositivo XTM está configurado en Modo Bridge. *[36900]*
- Cuando cambia su modo de configuración de enrutamiento combinado a bridge o de bridge a enrutamiento combinado, la CLI y Web UI pueden continuar mostrando el modo de configuración anterior. *[38896]*
- El dynamic routing de RIPv1 no funciona. *[40880]*
- Cuando una dirección IP se agrega a la lista de sitios temporalmente bloqueados por el administrador a través de la pestaña Firebox System Manager > Sitios bloqueados, el tiempo de caducidad se restablece constantemente cuando se recibe tráfico desde la dirección IP. *[42089]*

WAN Múltiple

- Los dispositivos XTM que se configuraron para usar WAN múltiple pueden fallar al enrutar tráfico entrante de manera correcta si el dispositivo se configuró con 1 a 1 NAT activado en sus rutas de túnel VPN para sucursales. *[67001]*
- La sticky connection de WAN múltiple no funciona si su dispositivo se configuró para usar el modoTabla de enrutamiento de WAN múltiple. *[62950]*
- Cuando activa la opción Failback inmediata de WAN múltiple a través de Conmutación de error de WAN, cierto tráfico puede conmutarse por error de forma gradual. *[42363]*

Método de Autenticación

- Las bandas inalámbricas 5 GHz no funcionan cuando usa los canales 36, 40, 149 ó 165. *[65559]*

Autenticación

- Los servidores Citrix 4.5/5/0 que se instalaron en VMware no funcionan con el servidor de terminal de Inicio de sesión único. *[66156]*

> **Workaround**
> Esta característica funciona con los servidores Citrix 6.0 y 6.5 que se instalaron en VMware.

- No se admite el SSO sin cliente en un entorno de Active Directory con TLS habilitado.
- Si utiliza la autenticación de Terminal Services, no se verifica la autenticación contra el tráfico de ningún protocolo que no sea TCP o UDP. Esto incluye al tráfico DNS, NetBIOS y ICMP.
- No se puede utilizar la *Redirige automáticamente a los usuarios a la página de autenticación* opción de autenticación junto con la autenticación de Terminal Services.

- Para habilitar su dispositivo XTM para que procese correctamente el tráfico relacionado proveniente del servidor Terminal o Citrix, el Agente de Terminal Services utiliza una cuenta de usuario especial denominada Backend-Service. Debido a esto, es posible que deba agregar políticas para permitir el tráfico desde esta cuenta de usuario a través de su dispositivo XTM. Puede obtener más información sobre cómo funciona Backend-Service en el sistema de ayuda del producto.
- Para que la función de Redireccionamiento de Autenticación funcione correctamente, no se puede permitir el tráfico HTTP o HTTPS a través de una política saliente basada en direcciones IP o alias que contengan direcciones IP. La función de Redireccionamiento de Autenticación funciona solamente cuando las políticas para los puertos 80 y 443 se configuran para la autenticación de usuario y grupo de usuarios. *[37241]*

Centralized Management

- No hay opción para configurar una acción de administración de tráfico en una plantilla de configuración del dispositivo XTM v11.x. *[55732]*
- Si utilizó Centralized Management con dispositivos suscritos a plantillas en versiones anteriores de WSM, cuando realice la actualización de WSM 11.x a v11.4 o superior, estas plantillas serán actualizadas y los dispositivos ya no estarán suscritos. Cada dispositivo mantiene la configuración de su plantilla. Las plantillas existentes son actualizadas para utilizar "T_" en sus nombres objetivos (para coincidir con los nombres objetivos de los dispositivos que solían suscribirse a ellas). Después de realizar la actualización, verá la actualización de plantilla que ocurre durante la actualización en su historial de revisión.
- Cuando se aplica una plantilla XTM a un dispositivo administrado, el Management Server crea una nueva revisión de la configuración para el dispositivo sólo si la nueva revisión va a ser diferente de la revisión actual. Además, tampoco hay comentarios acerca del motivo por el cual no se creó una nueva revisión de la configuración. *[57934]*

FireCluster

- La hora en el principal de respaldo de FireCluster puede salir de sincronización con el clúster principal, aún cuando NTP esté activado. *[66134]*

> **Workaround**
> Sincronice manualmente la hora del principal de respaldo. Conecte el clúster, inicie Firebox System Manager y luego seleccione Herramientas > Sincronizar hora. Esto sincroniza la hora en ambos clúster miembros a la hora en el equipo de administración.

- Cuando se activa el protocolo de árbol de expansión (STP) en algunos conmutadores, una conmutación por error de FireCluster puede tomar 10 segundos o más. *[66180]*

> **Workaround**
> Desactive STP en el conmutador, configure el conmutador para usar STO rápido o utilice un conmutador diferente.

- Puede que necesite volver a importar el certificado HTTPS DPI luego de que realice la actualización del sistema operativo Fireware XTM para FireCluster. [65280]
- No puede utilizar la dirección IP secundaria de una interfaz de dispositivo XTM para administrar un FireCluster que se configuró en modo activo/activo. *[64184]*

Workaround
Utilice la dirección IP primaria de un dispositivo XTM para todas las conexiones de administración para un FireCluster activo/activo.

- Los usuarios que otorgaron acceso para monitorear FireCluster a través de la administración basada en roles no pueden visualizar el dispositivo FireCluster en Log y Report Manager. *[65398]*
- El principal de respaldo de FireCluster puede desactivarse cuando Mobile VPN with SSL o PPTP se configura para usar un grupo de direcciones IP que incluye la dirección IP del clúster. *[63762]*

Workaround
Evite utilizar un grupo virtual desde dirección IP que produzca conflictos con las direcciones IP del clúster.

- Si no se puede acceder al Log Server desde las direcciones IP de administración, solo se podrá conectar el principal de FireCluster actual. Esto puede ocurrir si el Log Server está conectado mediante una red externa, pero las direcciones IP de administración están en una red opcional o de confianza. *[64482]*
- Si cambia la configuración de red de un FireCluster de modo enrutado a modo directo y luego lo cambia nuevamente a modo enrutado, la dirección IP de la interfaz del clúster no se muestra correctamente en el cuadro de diálogo de Policy Manager **Red > Configuración** . Las interfaces del clúster correctas se muestran en el cuadro de diálogo de configuración de FireCluster. *[63905]*
- Las actualizaciones de puertas de enlace AV en un sistema que tiene poca memoria pueden generar una conmutación por error de FireCluster *[62222]*

Workaround
Reduzca la frecuencia con la que el sistema verifica las actualizaciones de puertas de enlace AV para minimizar las posibilidades de que esto ocurra.

- Si un enlace monitoreado falla en los dos miembros de FireCluster, el miembro no maestro se cambia a modo pasivo y en consecuencia no procesa el tráfico. La conmutación por error de WAN múltiple provocada por una conexión con fallas hacia un host de monitor de enlace no desencadena la conmutación por error del FireCluster. La conmutación por error del FireCluster ocurre solamente cuando la interfaz física está desactivada o no responde.
- Cada dispositivo XTM tiene un conjunto de direcciones IP predeterminadas asignado a las interfaces del dispositivo en un rango que va desde 10.0.0.1. La dirección IP predeterminada más elevada depende de la cantidad de interfaces. Si configura la dirección IP de la interfaz del clúster Principal o De respaldo como una de las direcciones IP predeterminadas, ambos dispositivos se reinician y el maestro de respaldo queda inactivo. *[57663]*

Workaround
No utilice ninguna de las direcciones IP predeterminadas como la dirección IP de interfaz del clúster Principal o De respaldo.

- Cuando tiene un FireCluster activo/activo y utiliza la función de cancelación de WebBlocker, se le puede solicitar que ingrese su contraseña de cancelación dos veces. *[39263]*

- Cada interfaz de red activada en un FireCluster está monitoreada automáticamente por FireCluster. Debe asegurarse de que todas las interfaces activadas estén físicamente conectadas a un dispositivo de red.
- Si utiliza conmutadores HP ProCurve, es posible que no pueda configurar su FireCluster en modo activo/activo dado que estos conmutadores pueden no admitir la adición de entradas de ARP estáticas. *[41396]*
- Si utiliza el cliente Mobile VPN with IPSec para la misma red que la dirección de red externa configurada en su FireCluster, es posible que algo de tráfico no pase por el túnel VPN. *[38672]*
- Los usuarios de Mobile VPN with PPTP no aparecen en Firebox System Manager cuando está conectado a un miembro FireCluster pasivo. PPTP sólo está conectado a Firebox activo cuando utiliza un FireCluster activo/pasivo. *[36467]*
- No se puede utilizar una dirección IP de la interfaz VLAN para una dirección IP de administración del FireCluster. [45159]
- Para realizar una actualización manual de un FireCluster de v11.3.x a v11.5.1, el equipo de administración debe estar en la misma red que las direcciones IP de la administración de FireCluster. [63278]

Generación de registros y presentación de informes

- Cuando cambie el nivel de registro de su WatchGuard Log Server y haga clic en Aplicar, el cambio tiene efecto. *[60088]*

> **Workaround**
> 1. En WatchGuard Server Center, en la pestaña Log Server Logging, cambie el nivel de registro para los mensajes de registro desde Log Server y haga clic en **Aplicar.**.
> 2. En el árbol de Servidores, haga clic con el botón derecho en Log Server y seleccione **Detener el Servidor**. En el mensaje de confirmación, seleccione **Sí**.
> 3. Haga clic con el botón derecho nuevamente en Log Server y seleccione **Iniciar el Servidor**.

- El Informe de resumen de paquetes denegados todavía no se encuentra disponible en el Log y Report Manager. *[63192]*
- La salida del informe de Tendencia de actividad web en PDF no incluye etiquetas de tiempo en el eje X cuando se visualiza en Log and Report Manager. La información de fechas y horarios se incluye en la tabla que aparece debajo del informe. *[64162]*
- Cuando realiza una actualización de Fireware XTM v11.4.x a v11.5.1, es posible que los informes generados cerca del horario de la actualización no aparezcan en Log and Report Manager. *[64325]*
- Si un nombre del cronograma de informe diario incluye dos puntos u otros ciertos caracteres (por ejemplo: "1:35"), el sistema devuelve un error. *[63427]*

> **Workaround**
> Asegúrese de que sus nombres de cronograma de informe utilicen solamente caracteres que sean válidos en los nombres de archivo Windows. Puede encontrar caracteres válidos en artículos como http://msdn.microsoft.com/en-us/library/windows/desktop/aa365247%28v=vs.85%29.aspx .

- El log collector se bloqueará cuando alcance el tamaño virtual límite de 2 GB en sistemas Windows de 32 bits. *[64249]*

- Hay dos problemas de ordenamiento en el nuevo Log and Report Manager. Cuando ordena por Destino, el campo ordena por la dirección IP y no por el nombre de host del destino (si existe). Cuando ordena por Disposición, algunos elementos en el estado "denegar" no se ordenan adecuadamente dentro de los grupos. *[62879]*
- Cualquier "Informe archivado" que tenga configurado como diario o semanal en su configuración de v11.3 se convertirá automáticamente en informes programados después de que realice la actualización a WSM v11.4 o superior.

Mobile VPN

- No puede generar un archivo de configuración Mobile VPN with IPSec cuando el nombre de grupo contiene caracteres como el asterisco o el punto (*, .). *[66815]*
- Si configura el nivel de registro de diagnóstico para tráfico Mobile VPN with SSL a nivel de "depuración", los mensajes de registro se detendrán en Firebox System Manager > Administrador de tráfico. *[65165]*

> **Workaround**
> Configure el nivel de registro de diagnóstico para Mobile VPN with SSL a cualquier nivel de registro menos granular que el de "depuración".

- Si agrega una tecla de función nueva que agrega licencias Mobile VPN with SSL para su dispositivo XTM, debe reiniciar su dispositivo XTM para habilitar a los usuarios adicionales de Mobile VPN with SSL. *[65620]*
- Cuando conecte un cliente Mobile VPN with SSL v11.5.1 por primera vez con un dispositivo XTM actualizado a v11.5.2, a veces la actualización del cliente falla. *[65635]*

> **Workaround**
> Instalar el cliente Mobile VPN with SSL manualmente.

- No puede establecer una conexión Mobile VPN with SSL desde un equipo basado en Windows cuando la cuenta del sistema Windows es china. *[58208]*
- Cuando utilice el cliente IPSec incorporado desde un iPhone o iPad, la conexión del cliente se desconectará cuando la duración de aquella alcance 1 horas y 45 minutos. Esto ocurre a causa de una limitación en el cliente Cisco utilizado por iPhone/iPad. Debe reconectar el cliente IPSec para restablecer el túnel VPN. *[63147]*
- Las conexiones de Mobile VPN with PPTP desde dispositivos móviles Android no funcionan consistentemente en redes móviles 3G. *[63451]*
- Las conexiones del cliente Mobile VPN with IPSec pueden enrutar a través de una interfaz externa incorrecta cuando el dispositivo XTM está configurado para red de área ancha (WAN) múltiple con modo de operación por turnos. *[64386]*
- No puede configurar Mobile VPN with SSL para conectar el tráfico de red a una interfaz puenteada. *[61844]*
- Los usuarios de Mobile VPN with SSL no pueden conectarse a algunos recursos de red a través de un túnel VPN para sucursales que finaliza en FireCluster activo/activo. *[61549]*
- No puede hacer ping a la dirección IP de la interfaz del dispositivo XTM a la cual un cliente Shrew Soft VPN estableció un túnel VPN. Puede hacer ping en equipos en esa red, pero no en la interfaz misma de la dirección IP. *[60988]*
- Las conexiones de cliente Shrew Soft VPN pueden fallar si hay varios clientes conectados a un dispositivo XTM al mismo tiempo, otorgando claves de Fase 2. *[60261*]

- El reingreso de claves de Fase 1 iniciado por el cliente Shrew Soft VPN provoca la desconexión del cliente, si está conectado por más de 24 horas. En este caso, recomendamos que configure el reingreso de clave en su dispositivo XTM a 23 horas, una hora antes que el reingreso de claves preprogramadas en la configuración del cliente Shrew Soft. Esto obliga al dispositivo XTM a iniciar el reingreso de claves y le envía al cliente una notificación informándole que el túnel debe establecerse nuevamente. *[60260, 60259]*
- Una sesión continua de FTP a través de una conexión de Mobile VPN with IPSec podría finalizarse si se produce una regeneración de clave IPSec durante la transferencia de FTP. *[32769]*

Workaround
Incremente el conteo de bytes de la regeneración de clave.

- El Mobile VPN para cliente SSL Mac puede que no se conecte a un dispositivo XTM cuando el algoritmo de autenticación se establece a SHA 256. *[35724]*

Branch Office VPN

- El VPN para sucursales manual falla cuando la clave precompartida excede los 50 caracteres. *[65215]*
- No use la misma para la Puerta de enlace VPN y para el Túnel VPN . *[66412]*
- No puede usar una clave precompartida mayor que 50 caracteres de longitud para un túnel VPN para sucursales. *[65215]*
- Cuando configure su dispositivo XTM en modo WAN múltiple, debe seleccionar las interfaces que desea incluir en su configuración de WAN múltiple. Si hay alguna interfaz que elige no incluir en su configuración de WAN múltiple (es decir, limpia la casilla de selección para esa interfaz), el sistema no crea una ruta para esa red. Esto puede causar un problema si tiene una VPN de sucursal configurada para incluir la misma interfaz. En este caso, es posible que el túnel VPN no logre negociar con este par remoto. *[57153]*

Workaround
Si utiliza la WAN múltiple y tiene problemas con sus túneles de VPN de sucursal porque éstos no logran negociar con sus pares remotos, debe abrir su configuración de WAN múltiple y seleccionar Configurar en la ubicación adyacente a su modo de configuración de WAN múltiple elegido. Asegúrese de que las interfaces adecuadas estén incluidas en su configuración de WAN múltiple.

- Un túnel VPN de sucursal no pasa el tráfico si existe una política NAT estática entrante que incluye los protocolos IP 50 e IP 51 para la dirección IP externa del dispositivo XTM. [*41822]*
- Los túneles branch office VPN administrados no pueden establecerse si el punto de distribución de la lista de revocación de certificados (CRL) (por ejemplo, el WatchGuard Management Server o un sitio de distribución de CRL de terceros que utilice) está desconectado. *[55946]*
- El uso de *Cualquiera* en una ruta de túnel BOVPN se cambia en Fireware XTM. Si un túnel VPN para sucursales utiliza Cualquiera para la parte Local de una ruta de túnel, Fireware XTM interpreta que esto significa una red 0.0.0.0 y una subnet mask 0.0.0.0 (en notación diagonal, 0.0.0.0/0). Si el punto remoto IPSec no envía 0.0.0.0/0 como su identificación de Fase 2, las negociaciones de Fase 2 fallan. *[40098]*

Workaround
No utilice *Cualquiera* para la parte Local o la parte Remota de la ruta de túnel. Cambie la parte Local de la ruta de túnel. Ingrese las direcciones IP de equipos detrás del dispositivo XTM que participa realmente en el enrutamiento del túnel. Comuníquese con el administrador del punto remoto de IPSec para determinar qué utiliza ese dispositivo para la parte Remota de su ruta de túnel (o la parte Remota de su identificación de Fase 2).

- Si tiene una gran cantidad de túneles VPN para sucursales en la configuración, los túneles pueden requerir bastante tiempo para aparecer en Policy Manager. *[35919]*

Workaround
Desde Policy Manager, seleccione **Visualizar > Resaltado de Políticas**. Borrar el **Resaltado de políticas Firewall que se basan en el tipo de tráfico** seleccione esta casilla de verificación.

Uso de CLI

La CLI (Command Line Interface) de Fireware XTM está totalmente admitida en lanzamientos de v11.x. Para obtener información sobre cómo iniciar y utilizar la CLI, consulte la *Guía de referencia de comandos de la CLI*. Puede descargar la guía de la CLI desde el sitio web de documentación en http://www.watchguard.com/help/documentation/xtm.asp.

Asistencia Técnica

Para recibir asistencia técnica, comuníquese con el Soporte Técnico de WatchGuard por teléfono o inicie sesión en el portal de WatchGuard en la Web en http://www.watchguard.com/support. Cuando se comunica con el soporte técnico, debe proporcionar el número de serie del producto registrado o la identificación de socio.

	Número de teléfono
Usuarios finales de EE. UU.	877.232.3531
Usuarios finales internacionales	+1 206.613.0456
Revendedores autorizados de WatchGuard	206.521.8375