Fireware XTM v11.3.7
Release Notes

Supported Devices	Firebox X Peak e-Series Firebox X Core e-Series Firebox X Edge e-Series
Fireware XTM OS Build	433175
WatchGuard System Manager Build	N/A *WatchGuard recommends you use WatchGuard System Manager v11.8 to manage Fireware XTM v11.3.7.*
Revision Date	22 May 2014

Introduction

Fireware XTM v11.3.7 is the newest operating system software release for Firebox X Peak, Core, and Edge e-Series appliances. This release provides several bug fixes and stability improvements for our Firebox e-Series customers, including improvements to spamBlocker. Leveraging technology from Commtouch, spamBlocker now offers higher efficacy and reduced false positives measured in testing, as well as an updated UI for Bulk mail handling, Virus Outbreak Detection, and Proactive Patterns.

There is no new WatchGuard System Manager release for Fireware XTM v11.3.7. You can use WatchGuard System Manager v11.4.x - v11.8 to connect to a Firebox X e-Series device that runs Fireware XTM v11.3.7. We recommend that you use the most current version of WatchGuard System Manager available to you.

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

Before You Begin

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

- A Firebox X Core or Peak e-Series device running Fireware v10.2.x or higher, or a Firebox X Edge e-Series device running v10.2.9 or higher. If this is a new device, make sure you follow the instructions in the *Quick Start Guide* that ships with your device before you try to upgrade to v11.3.7.
- The required hardware and software components as shown in the Systems Requirements table below.
- An active LiveSecurity subscription.
- Feature key for your Firebox – If you upgrade your Firebox e-Series from an earlier version of Fireware or Edge appliance software, you can use your existing feature key.
- Online documentation system for this product is available at www.watchguard.com/help/documentation
- See the Resolved Issues section below for a complete list of resolved issues.

Localization

The Fireware XTM v11.3.7 Web UI is localized, however changes to the user interface added after v11.3 remain in English. Supported languages are:

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

> ***Note*** *In addition to these languages, we introduced localized Web UI support for Korean and Traditional Chinese with the v11.3.1 release. Only the Web UI itself has been localized. WSM, and all help files and user documentation, remain in English.*

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

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. The web pages for Reporting Web UI, CA Manager, Quarantine Web UI, and Wireless Hotspot automatically display in whatever language preference you have set in your web browser.

Fireware XTM and WSM Operating System Compatibility

The information provided here is for WatchGuard System Manager v11.4.x and Fireware XTM v11.3.7. To see system requirements for other versions of WatchGuard System Manager, go to the relevant release notes.

WSM/ Fireware XTM Component	Microsoft Windows XP SP2 (32-bit)	Microsoft Windows Vista (32-bit)	Microsoft Windows Vista (64-bit)	Microsoft Windows 7 (32-bit & 64-bit)	Microsoft Windows Server 2003 (32-bit)	Microsoft Windows Server 2008 & 2008 R2*	Mac OS X v10.5 & v10.6
WatchGuard System Manager Application	✓	✓	✓	✓	✓	✓	
Fireware XTM Web UI Supported Browsers: IE 7 and 8, Firefox 3.x	✓	✓	✓	✓	✓	✓	✓
WatchGuard Servers	✓	✓	✓	✓	✓	✓	
Single Sign-On Agent Software					✓	✓	
Single Sign-On Client Software	✓	✓	✓	✓	✓	✓	
Mobile VPN with IPSec Client Software (WatchGuard client and Shrew Soft VPN client)	✓	✓	✓	✓			
Mobile VPN with SSL Client Software	✓	✓	✓	✓	✓		✓ **

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

*** Mac OS X support for the SSL VPN client is for 32-bit mode only.*

System Requirements

	If you have WatchGuard System Manager client software only installed	If you install WatchGuard System Manager and WatchGuard Server software
Minimum CPU	Intel Pentium IV 1GHz	Intel Pentium IV 2GHz
Minimum Memory	1 GB	2 GB
Minimum Available Disk Space	250 MB	1 GB
Minimum Recommended Screen Resolution	1024x768	1024x768

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

To use WatchGuard System Manager or the WatchGuard Server Center with Fireware XTM v11.3.7, we recommend that you use the most current version of WatchGuard System Manager available to you. There is no WatchGuard System Manager v11.3.7.

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.

If you have….	Select from these Fireware XTM OS packages
Firebox X Core or Peak e-Series	XTM_OS_Core_Peak_11_3_7.exe XTM_Core_Peak_11_3_7.zip utm_core_peakdown2fw.zip - Use this file to downgrade a Firebox X Core or Peak e-Series from v11.3.7 to Fireware v10.2.x.
Firebox X Edge e-Series	XTM_Edge_11_3_7.exe - Use this file to upgrade from previous versions of Fireware XTM 11.x to v11.3.7. XTM_Edge_11_3_7.zip - No configuration conversion is possible if you use this file. edge_11_3_7.exe - Use this file to upgrade your OS and configuration from v10.2.9 or higher to Fireware XTM.

Single Sign-On Software

There are two files available for download if you use Single Sign-On. the SSO Agent software has been updated for this releaase.

- `WG-Authentication-Gateway_11_7_4.exe` (SSO Agent software - required for Single Sign-on)
- `WG-Authentication-Client_11_7.msi` (SSO Client software - optional)

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

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_3_5.exe` (Client software for Windows)
- `WG-MVPN-SSL_11_3_5.dmg` (Client software for Mac)

Mobile VPN with IPSec client for Windows

With this release, we now support the Shrew Soft VPN client for Windows v2.2, which you can download from our web site. Shrew Soft has recently released a v2.2.1 client, available on their web site, which introduces a new "Pro" version available at an extra cost with additional features. WatchGuard recommends you use the no-cost Standard version of the client as it includes all functionality supported in the v2.2 VPN client. If you want to use the v2.2.1 client, we recommend you read this Knowledge Base article first.

Upgrade from Fireware XTM v11.x to v11.3.7

Before you upgrade from Fireware XTM v11.x to Fireware XTM v11.3.7, go to the WatchGuard Portal > Articles & Software tab. Download and save the file that matches the WatchGuard device you want to upgrade. You can use Policy Manager or the Web UI to complete the upgrade procedure. We strongly recommend that you back up your device configuration before you upgrade.

> ***Note*** *If you are currently running v11.0 or v11.0.1 on your Firebox X Edge e-Series, you must upgrade to v11.0.2 before you upgrade to v11.3.7 to avoid possible file system corruption. This issue does not apply to any other model.*

Upgrade to Fireware XTM v11.3.7 from Web UI

1. Go to **System > Backup Image** 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_[model].sysa-dl to the default location of C:\Program Files\Common files\WatchGuard\resources\FirewareXTM\11.3.7\[model].
3. Connect to your XTM device with the Web UI and select **System > Upgrade OS**.
4. Browse to the location of the xtm_[model].sysa-dl file from Step 2 and click **Upgrade**.

Upgrade to Fireware XTM v11.3.7 from WSM/Policy Manager

1. Select **File > Backup** to back up your current configuration file.
2. On your management computer, launch the OS executable file you downloaded from the WatchGuard Software Downloads Center. This installation extracts an upgrade file called xtm_[model].sysa-dl to the default location of C:\Program Files\Common files\WatchGuard\resources\FirewareXTM\11.3.7\[model].
3. Install and open WatchGuard System Manager. Connect to your XTM device and launch Policy Manager.
4. From Policy Manager, select **File > Upgrade**. When prompted, browse to and select the xtm_[model].sysa-dl file from Step 2.

Upgrade from Fireware or Edge v10.x to Fireware XTM v11.3.7

There are special instructions in the WatchGuard Knowledge Base to help you upgrade Firebox X Peak, Core, and Edge e-Series devices to Fireware XTM v11.3.7. These same knowledge base articles also explain how to downgrade to v10.2.x if necessary, and how to upgrade a Fireware v10.x FireCluster to Fireware XTM

- Upgrade a Firebox X Edge e-Series device from v10.2.x to Fireware XTM v11.3.x
- Upgrade a Firebox X Core or Peak e-Series device from Fireware v10.2.x to Fireware XTM v11.3.x

Downgrade Instructions

If you want to downgrade from Fireware XTM v11.3.x to an earlier version of Fireware XTM, you either:

- Restore a previously created full backup image to complete the downgrade (for Firebox X Core and Peak e-Series devices only); or
- Reset your Firebox or XTM device to its factory-default settings and then run the Quick Setup Wizard with the older version of Fireware XTM already installed on your management computer. You can then restore the backup image you created before you upgraded to Fireware XTM v11.3.x.

Resolved Issues

This release resolves several issues reported in earlier versions of Fireware XTM OS, including:

- This release resolves a reported buffer overflow vulnerability in the WGagent code supporting the web management UI. *[76815]*
- A problem that caused network interface status to display incorrectly in WatchGuard System Manager and Firebox System Manager when using an active/passive FireCluster has been resolved. *[61346]*
- This release resolves a memory leak in the `certd` process that occurred in a FireCluster environment. *[62605]*
- The Firebox no longer ignores DHCPREQUEST messages when a host moves from one subnet to another. It now responds with DHCP NACK when requests are for different subnet. *[64456]*
- This release resolves a problem that caused high CPU load for a Firebox configured to use a multi-WAN FireCluster configuration with domain name-based probes. *[64614]*
- A problem that caused high CPU load and excessive memory use when a Firebox was configured for SNMP has been resolved. *[68374]*
- A memory leak associated with management connections to the Firebox has been fixed. *[70019]*
- A buffer overflow vulnerability has been resolved. *[76815]*
- The backup master in an active/passive FireCluster no longer responds to ARP requests for IP addresses configured on its network interfaces. *[71986]*
- A problem that caused a system crash in a FireCluster under heavy load has been resolved. *[77040]*
- Inbound data through an FTP proxy with SNAT applied is now processed correctly. *[65368]*

Known Issues and Limitations

These are known issues for Fireware XTM v11.3.7 and all management applications. Where available, we include a way to work around the issue.

General

- If you use WSM v11.4.x to manage a Firebox X Edge e-Series device that runs Fireware XTM v11.3.5, you cannot use the backup and restore functions in Policy Manager. You must use the WatchGuard System Manager v11.3.2 or the Web UI to back up and restore your Edge configuration. *[59873, 59887]*
- If your Firebox X Edge e-Series device is connected to a modem, it may not boot correctly if you try to set your Edge to its factory default settings. *[30284]*
- When you use the **Policy Manager > File > Backup** or **Restore** features, the process can take a long time but does complete successfully. *[35450]*
- Fireware XTM does not support BGP connections through an IPSec VPN tunnel to Amazon Web Services. VPN tunnels that do not use BGP are supported. *[41534]*
- Policy Manager opens the locally stored copy of your configuration, instead of the configuration from the device, when you use a status passphrase with a "-" character as the first character in the passphrase (for example: "-1234567"). *[42616]*

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

Upgrade Issues

- After you upgrade to Fireware XTM v11.3.5, it is possible to modify your TCP connection idle timeout with the Web UI. If you modify this setting and then try to open your configuration with WSM v11.3.2's Policy Manager, your configuration can be corrupted.

Workaround
You can open the configuration with WSM v11.4.x with no issue. If you change this setting through the Web UI, and want to continue to use WSM v11.3.2, you can save your configuration to a file. Then, open your configuration file in an XML editor and remove all lines in the section between <traffic-flow-timers> and </traffic-flow-timers>, but keep <tcp-timeout-established>.

- After you upgrade a Firebox X Edge from v10.2.x, it is important to know that you must use the user name "admin" when you want read/write access to the Edge. In versions older than v11.0 of Edge appliance software, you could use a name other than "admin" in your administrative credentials, but this is no longer possible in Fireware XTM. You must log in to the Edge with the user name "admin" and the read/write passphrase you set during the upgrade.
- The disk space occupied by data in the Report Server database before you upgrade to v11.2.x is not freed until after the number of days specified in the **Keep reports on the Report Server** setting in your Report Server configuration. Because of this, the Report Server database consumes more disk space until this number of days pass.
- If you upgrade to Fireware XTM from an earlier version of Fireware and used a branch office VPN Phase 2 encryption setting of **None**, this setting is not correctly converted during the configuration upgrade. You must edit your Phase 2 encryption setting manually when the upgrade is complete to select an appropriate encryption setting.
- If you have special characters (, ;) in the policy names of your v10.x configuration, you must remove them from your policy names after you upgrade to Fireware XTM v11 so that reporting and monitoring operate correctly. *[36577]*

- In WSM v10.x, you could create a Traffic Management action that set both incoming and outgoing traffic bandwidth for an external interface. This action could operate on a policy that managed traffic to and from a trusted network. To reproduce this feature in Fireware XTM v11.x, you must create a Traffic Management action that sets the maximum upload speed on the external interface and the maximum download speed on the trusted interface.
- The Firebox X Edge **Require user authentication** and **Trusted Hosts** features do not exist in Fireware XTM, because of the increased granularity available when you configure policies for Edge users. During the Edge upgrade, the users are added to a local group called Local-Users. If you previously had **Require user authentication** enabled, you must use this group in your policies to enforce user authentication. The **Trusted Hosts** feature is no longer necessary.
- The DNS suffix and second DNS server entries are not converted when you upgrade from v10.2.x to v11.x on Firebox X Edge e-Series. *[40774]*

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

Web UI

- The Fireware XTM Web UI does **not** support the configuration of some features. These features include:
  - FireCluster
  - The editing of static NAT rules
  - 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, as well as the .vpn profile for the Shrew Soft VPN client.
  - You cannot edit the name of a policy, use a custom address in a policy, or use Host Name (DNS lookup) to add an IP address to a policy.
- If you configure a policy in the Web UI with a status of **Disabled**, then open Policy Manager and make a change to the same policy, the action assigned to the policy when it denies packets is changed to **Send TCP RST**. *[34118]*
- If you use the Web UI to edit an existing proxy policy that has alarm settings enabled, the alarm settings may be disabled when you save your configuration. *[38585]*
- You cannot create read-only Mobile VPN with IPSec configuration files with the Web UI. *[39176]*

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 as well as the .vpn profile for the Shrew Soft VPN client.
- The CLI performs minimal input validation for many commands.

Multi-WAN

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

- When you enable Multi-WAN in round-robin mode, you cannot use the HTTP Proxy Caching Server option. *[57561]*

Networking

- 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]*
- After you enable the MAC access control list or add a new MAC address, you must reboot your Firebox before the change takes effect. *[39987]*
- You must make sure that any disabled network interfaces do not have the same IP address as any active network interface or routing problems can occur. *[37807]*
- If you enable the MAC/IP binding with the **Only allow traffic sent from or to these MAC/IP addresses** check box, but do not add any entries to the table, the MAC/IP binding feature does not become active. This is to help make sure administrators do not accidentally block themselves from their own Firebox. *[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 Firebox with a Mixed Routing Mode configuration, any bridged interfaces show their interface and default gateway IP address as 0.0.0.0 in the Web UI. *[39389]*
- When you configure your Firebox in Bridge Mode, the LCD display on your Firebox shows the IP address of the bridged interfaces as 0.0.0.0. *[39324]*
- When you configure your Firebox in Bridge Mode, the HTTP redirect feature is configurable from the user interface but does not work in this release. *[38870]*
- Static MAC/IP address binding does not work when your Firebox is configured in Bridge mode. *[36900]*
- When your Firebox is configured to use Bridge mode, the physical interface of the Firebox does not appear correctly in log messages. Instead, the interface is represented as "tbrX". *[36783]*
- When you change your configuration mode from Mixed Routing to Bridge or from Bridge to Mixed Routing, the CLI and Web UI may continue to show the previous configuration mode. *[38896]*
- The dynamic routing of RIPv1 does not work. *[40880]*
- 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]*

Firebox X Edge e-Series Wireless

- When a Firebox X Edge e-Series is configured as both a wireless access point and as a Mobile VPN with SSL endpoint, the wireless connection does not work correctly if the SSL VPN address pool is configured on the same subnet as the wireless access point. *[42429]*
- When you set the external interface as a wireless client and configure static NAT to use the Eth0 interface as its source IP address, inbound static NAT does not operate correctly. *[38239]*
- The MAC Address Override feature is not available on a Firebox X Edge that has a wireless interfaced configured as an external interface. *[38241]*

FireCluster

- Each Firebox has a set of default IP addresses assigned to the device interfaces in the range 10.0.0.1 – 10.0.11.1. 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 cannot configure your FireCluster in active/active mode because these switches may not support the addition of static ARP entries. *[41396]*
- FireCluster is not supported if you use Bridge network configuration mode on your WatchGuard devices. *[37287]*
- If you use the Mobile VPN with IPSec client from the same network as the external network address configured on your FireCluster, some traffic may not go through the VPN tunnel. *[38672]*
- Mobile VPN with PPTP users do not appear in Firebox System Manager when you are connected to a passive FireCluster member. PPTP is only connected to the active Firebox when using an active/passive FireCluster. *[36467]*
- FireCluster does not support dynamic routing. *[39442]*

Authentication

- If your XTM device runs Fireware XTM OS v11.3.5, and you use the v11.5.1 SSO Agent, you can use clientless SSO with only a single domain. The v11.5.1 SSO Agent configuration settings allow you to specify additional domains, but only one domain is supported with this version of Fireware XTM OS.
- 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]*

Proxies

- The ability to use an HTTP caching proxy server is not available in conjunction with the TCP-UDP Proxy. *[44260]*
- Application Blocker can only block the initial login to Skype. It cannot block traffic for a Skype client that has previously logged in. If a user with a laptop logs in to Skype when the computer is not connected to your network, and then the user connects to your network while the Skype client is still active, Application Blocker cannot block the Skype traffic until the user exits and logs out of the Skype application.
- Application Blocker does not stop all BitTorrent connections. It does stop most connections, which causes BitTorrent throughput to be significantly reduced. *[44288]*
- 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.

- If deep inspection of HTTPS content is enabled in an HTTPS proxy policy, some sites may not load correctly unless SSL v3 is enabled in the browser. *[59831]*

Workaround
You can use an HTTPS packet filter policy instead of an HTTPS proxy policy for sites that do not work correctly.

- 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 Firebox.

Security Subscriptions

- The Trusted Email Forwarders feature does not work when you use spamBlocker with Mailshell. *[71489]*
- You cannot use a WebBlocker Server through a branch office VPN tunnel. *[56319]*
- To optimize performance of web browsing on the Firebox X Edge e-Series, Gateway AntiVirus does not scan the following content types when used with the HTTP proxy: text/*, image/*, audio/*, video/*, application/javascript, application/x-javascript, and application/x-shockwave-flash. The content types appear in the HTTP-Client proxy action configuration for the Edge, but Gateway AV does not scan for these content types. All other content types, including executable files, are scanned. Gateway AntiVirus also does not use code emulation capabilities of the AV engine on Firebox X Edge e-series appliances.
- On newly installed appliances, Intrusion Prevention will fail to scan any objects. The error "unable to init ips context" may be printed in the log file. *[56470*

Workaround
Reboot the appliance.

Mobile VPN with SSL

- Users who try to upgrade their Mobile VPN with SSL client from Fireware XTM v11.2.1 to a more recent version of the client will fail. The failure does not damage the v11.2.1 client installation. *[43970]*

Workaround
To upgrade your Mobile VPN with SSL client from v11.2.1 to v11.3, use your web browser to connect to `https://<IP address of a Firebox or XTM device>/sslvpn.html`. You can then download and install the new client software. Or, you can download the client software from the Software Downloads page and email it your users to install on their computer.

- The Macintosh SSL VPN client may not be able to connect to a Firebox when the authentication algorithm is set to SHA 256. *[35724]*
- When the Macintosh SSL VPN client disconnects or is stopped manually, the client disables the AirPort wireless adapter on the Mac. *[39914]*

Mobile VPN with IPSec

- Shrew Soft VPN client connections can drop if there are multiple cilents connected to a Firebox 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 Firebox to 23 hours -- one hour shorter than the rekey hard-coded in the Shrew Soft client configuration. This forces the Firebox to initiate the rekey, and gives the client a notification that the tunnel must be re-established. *[60260, 60259]*
- 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]*
- A continuous FTP session over a Mobile VPN with IPSec connection could get terminated if an IPSec rekey occurs during the FTP transfer. *[32769]*

> **Workaround**
> Increase the rekey byte count.

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

Branch Office VPN

- When you configure your Firebox 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 Firebox or XTM device. *[41822]*
- Managed branch office VPN tunnels cannot be established if the CRL distribution point (for example, the WatchGuard Management Server or a third-party CRL distribution site you use) is offline. *[55946]*
- The use of Any in a BOVPN tunnel route is changed in Fireware XTM. If a branch office VPN tunnel uses Any for the Local part of a tunnel route, Fireware XTM interprets this to mean network 0.0.0.0 and subnet mask 0.0.0.0 (in slash notation, 0.0.0.0/0). If the remote IPSec peer does not send 0.0.0.0/0 as its Phase 2 ID, Phase 2 negotiations fail. *[40098]*

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

- The VPN Keep-Alive feature is not available for the Firebox X Edge e-Series. *[37769]*
- If you have a large number of branch office VPN tunnels in your configuration, the tunnels may take a long time to appear in Policy Manager. *[35919]*
- When you set the Phase 2 SA expiration to zero by setting both the Life-time and Life-size values to 0, the Firebox changes the rekey life-time to 8 hours. *[37209]*

Using the CLI

The Fireware XTM CLI (Command Line Interface) is fully supported for v11.x releases. For information on how to start and use the CLI, see the CLI Command Reference Guide for Fireware XTM v11.3.x. You can download the CLI guide from the documentation web site at http://www.watchguard.com/help/documentation/fireware.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