Fireware XTM v11.5.4 Release Notes

Supported Devices	XTMv - All Editions
Fireware XTM OS Build	341871
WatchGuard System Manager Build	341800
Revision Date	26 June 2012

Introduction

WatchGuard is excited to release our new XTMv virtual network appliances. WatchGuard XTMv brings best-in-class network security to the world of virtualization. Designed for a VMware hypervisor environment, the new WatchGuard XTMv series of virtual firewalls provides unparalleled network security, and advanced protection of applications and data.

XTMv is based on Fireware XTM OS and works with the same management and monitoring utilities as our XTM physical appliances. Because of this, both virtual and physical XTM devices share features and functionality and are supported by the same product help system. We recommend that you read the *XTMv Setup Guide* carefully before you install and begin to use this new product. This guide includes important information you need to know as you begin to work with XTMv.

Before You Begin

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

- VMware ESXi 4.1 or 5.0 host installed on any supported server hardware.
- VMware vSphere Client 4.1 or 5.0 installed on a supported Windows computer.
- A serial number for your XTMv device. The serial number is supplied to you when you purchase XTMv.

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

Localization

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

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

Fireware XTM Web UI

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

WatchGuard System Manager

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

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

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

Fireware XTM and WSM v11.5.4 Operating System Compatibility

Revised May 2012

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

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

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

**** Microsoft Windows Server 2003 SP2 required.*

Authentication Support

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

✓ — Fully supported by WatchGuard

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

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

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

WSM 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

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 on a supported Windows computer. You can also 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 check box and search for available Software Downloads. Select the XTMv Software Downloads article.

There are several software files available for download. See the descriptions below so you know what software packages you will need for your upgrade.

Fireware XTM OS

Use this WatchGuard XTMv OVF template file to deploy your XTMv virtual appliance. For installation and deployment instructions, see the *XTMv Setup Guide*.

```
xtmv_11_5_4.ova
```

WatchGuard System Manager

With this software package you can install WSM and the WatchGuard Server Center software:

```
WSM11_5_4s.exe
```

Single Sign-On Software

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

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

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

Terminal Services Authentication Software

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

Mobile VPN with SSL Client for Windows and Mac

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

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

Mobile VPN with IPSec client for Windows

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

Known Issues and Limitations

These are known issues for Fireware XTM v11.5.4 and all management applications, for all devices that run Fireware XTM, including XTMv. Where available, we include a way to work around the issue.

General

- 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]*
- When you use the **Policy Manager > File > Backup** or **Restore** features, the process can take a long time but does complete successfully. *[35450]*
- 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]*

XTMv

- 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.
- To work correctly, some Fireware XTM features require that you configure the virtual switch (vSwitch) on your network in promiscuous mode. These features are:
  - Bridge mode network configuration
  - Drop-in mode network configuration
  - Network/LAN bridge
  - Mobile VPN with SSL with the Routed VPN Traffic setting

WatchGuard System Manager

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

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

- WatchGuard System Manager does not display the correct IP address for the default gateway of an XTM device that has no External interface. *[56385]*
- When you install WatchGuard System Manager or any server software on a computer running Microsoft Windows XP, compatibility mode should not be enabled even if prompted by Windows, for any of the WSM applications, including the installer. *[56355]*
- Remote managed Firebox or XTM devices configured in Drop-in Mode may not be able to connect to a Management Server that is behind a gateway Firebox or XTM device also configured in Drop-in Mode. *[33056]*
- If you restore a backup image to a managed client device managed by a Management Server, it is possible that the shared secret becomes out of sync.

Workaround
Connect to the Management Server from WSM. Select the managed device and select **Update Device**. Select the radio button **Reset server configuration (IP address/ Hostname, shared secret**).

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

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

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

Web UI

- The Fireware XTM Web UI does not support the configuration of some features. These features include:
  - FireCluster
  - Certificate export
  - You cannot turn on or off notification of BOVPN events
  - You cannot add or remove static ARP entries to the device ARP table
- You cannot get the encrypted Mobile VPN with IPSec end-user configuration profile, known as the .wgx file. The Web UI generates only a plain-text version of the end-user configuration profile, with file extension .ini.
- You cannot edit the name of a policy, use a custom address in a policy, or use Host Name (DNS lookup) to add an IP address to a policy.
- You may need to reboot your XTM device after you import a third-party web certificate before the certificate will take effect. *[65589]*
- If you configure a policy in the Web UI with a status of Disabled, then open Policy Manager and make a change to the same policy, the action assigned to the policy when it denies packets is changed to Send TCP RST. *[34118]*
- If you use the Web UI to edit an existing proxy policy that has alarm settings enabled, the alarm settings may be disabled when you save your configuration. *[38585]*
- You cannot create read-only Mobile VPN with IPSec configuration files with the Web UI. *[39176]*

Command Line Interface (CLI)

- The CLI does not support the configuration of some features:
  - You cannot add or edit a proxy action.
  - You cannot get the encrypted Mobile VPN with IPSec end user configuration profile, known as the .wgx file. The CLI generates only a plain-text version of the end-user configuration profile, with file extension .ini.
- The CLI performs minimal input validation for many commands.

Proxies

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

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

- The XTM device can store only one HTTPS Proxy Server certificate and can protect only one HTTPS web site at a time. *[41131]*
- When an XTM device is under high load, some proxy connections may not terminate correctly. *[61925, 62503]*
- When you enable both DPI and OCSP in the HTTPS proxy, you may see occasional certificate warnings or error messages. *[63001]*...
- The ability to use an HTTP caching proxy server is not available in conjunction with the TCP-UDP Proxy. *[44260]*
- You cannot make a SIP-based call from Polycom PVX softphone behind a Firebox to a Polycom PVX on the external network. *[38567]*

> **Workaround**
> You can use the H.323 protocol instead of SIP.

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

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

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

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

Security Subscriptions

- The Gateway AV signature update process is memory-intensive. To avoid memory contention or negative side effects resulting from a spike in memory use, we recommend that you extend the signature update interval to 8-24 hours.
- Some IPS signature information, such as the CVE number, is not available in Firebox System Manager. We provide search capabilities and CVE information for IPS signatures on a web security portal for IPS on the WatchGuard web site, which you can access at http://www.watchguard.com/SecurityPortal/ThreatDB.aspx

- Skype detection blocks only new Skype sessions. If a user is already logged in to Skype and a Skype session is already started when Application Control is enabled, Application Control may not detect the activity.
- It is not possible to assign a role for Application Control management from the WatchGuard System Manager role-based administration feature. *[59204]*
- You cannot use a WebBlocker Server through a branch office VPN tunnel. *[56319]*

Networking

- An apostrophe in a DHCP reservation name causes the DHCP reservation fail. *[65529]*
- You cannot configure traffic management actions or use QoS marking on VLANs. *[56971, 42093]*
- You cannot bridge a wireless interface to a VLAN interface. *[41977]*
- 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 XTM device 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 HTTP redirect feature is configurable from the user interface but does not work in this release. *[38870]*
- Static MAC/IP address binding does not work when your XTM device is configured in Bridge mode. *[36900*
- When you change your configuration mode from Mixed Routing to Bridge or from Bridge to Mixed Routing, the CLI and Web UI may continue to show the previous configuration mode. *[38896]*
- The dynamic routing of RIPv1 does not work. *[40880]*
- When an IP address is added to the Temporary Blocked Site list by the administrator through the Firebox System Manager > Blocked Sites tab, the expiration time is constantly reset when traffic is received from the IP address. *[42089]*

Multi-WAN

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

Authentication

- Clientless SSO is not supported on a TLS-Enabled Active Directory environment.
- If you use Terminal Services authentication, no authentication verification is done against traffic of any protocol that is not TCP or UDP. This includes DNS, NetBIOS, and ICMP traffic.
- Terminal Services authentication support does not work with Single Sign-On.

- It is not possible to use the *Auto redirect users to authentication* page for authentication option together with Terminal Services authentication.
- To enable your XTM device to correctly process system-related traffic from your Terminal or Citrix server, the Terminal Services Agent uses a special user account named Backend-Service. Because of this, you may need to add policies to allow traffic from this user account through your XTM device. You can learn more about how Backend-Service operates in the product help system.
- For the Authentication Redirect feature to operate correctly, HTTP or HTTPS traffic cannot be allowed through an outgoing policy based on IP addresses or aliases that contain IP addresses. The Authentication Redirect feature operates only when policies for port 80 and 443 are configured for user or user group authentication. *[37241]*

Centralized Management

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

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

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

Logging and Reporting

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

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

- The Denied Packets Summary report is not yet available in the Log and Report Manager. *[63192]*
- The PDF output of the Web Activity Trend report does not include time labels on the x-axis when viewed in Log and Report Manager. Date and time information is included in the table below the report. *[64162]*
- The User Authentication Denied report does not contain records of denied authentication attempts if you use an authentication server other than Firebox-DB. *[65717]*

- If you use Mobile VPN with PPTP configured to use RADIUS authentication, the User Authentication Denied report does not contain records of denied authentication attempts. It incorrectly includes only allowed authentication attempts. *[65689]*
- In the WatchGuard Server Center > Report Server > Server Settings tab, the name of the server that you type in the ConnectWise Server (Site), is case sensitive. If the ConnectWise server name does not exactly match the name of the server specified in the ConnectWise server certificate, reports fail with 'Error: Certificate validation failed." *[64393]*

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

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

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

- Log collector will crash when it reaches the 2GB virtual size limit on 32-bit Windows systems. *[64249]*
- There are two sorting issues in 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]*.

Mobile VPN

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

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

- If you add a new feature key that adds Mobile VPN with SSL licenses for your XTM device, you must reboot your XTM device to enable the additional Mobile VPN with SSL users. *[65620]*
- 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]*
- Fireware XTM Web UI does not allow you to enable Mobile VPN with SSL if the only external interface is an external VLAN interface. *[63871]*

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

- Connections from the Mobile VPN with IPSec client can route through the wrong external interface when the XTM device is configured for multi-WAN in round-robin mode. *[64386]*
- You cannot configure Mobile VPN with SSL to bridge network traffic to a bridged interface. *[61844]*
- Mobile VPN with SSL users cannot connect to some network resources through a branch office VPN tunnel that terminates on an active/active FireCluster. *[61549]*
- You cannot ping the IP address of the XTM device interface to which a Shrew Soft VPN client established a VPN tunnel. You can ping computers on that network, but not the interface IP address itself. *[60988]*
- Shrew Soft VPN client connections can drop if there are multiple 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

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

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

- A branch office VPN tunnel does not pass traffic if an inbound static NAT policy that includes IP 50 and IP 51 protocols exists for the external IP address of the XTM device. [*41822]*
- Managed branch office VPN tunnels cannot be established if the CRL distribution point (for example, the WatchGuard Management Server or a third-party CRL distribution site you use) is offline. *[55946]*
- The use of *Any* in a BOVPN tunnel route is changed in Fireware XTM. If a branch office VPN tunnel uses Any for the Local part of a tunnel route, Fireware XTM interprets this to mean network 0.0.0.0 and subnet mask 0.0.0.0 (in slash notation, 0.0.0.0/0). If the remote IPSec peer does not send 0.0.0.0/0 as its Phase 2 ID, Phase 2 negotiations fail. *[40098]*

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

- If you have a large number of branch office VPN tunnels in your configuration, the tunnels may take a long time to appear in Policy Manager. *[35919]*

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

Using the CLI

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

Technical Assistance

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

	Phone Number
U.S. End Users	877.232.3531
International End Users	+1 206.613.0456
Authorized WatchGuard Resellers	206.521.8375