WatchGuard® Firebox® X Edge e-Series

Release Notes for Firebox® X Edge e-Series v10.2.12

Release Notes Revision Date: December 14, 2009
Build number: 248909

Introduction

WatchGuard is pleased to announce the release of Firebox® X Edge e-Series v10.2.12.

This release addresses several issues reported by WatchGuard customers and includes bug fixes for issues related to several reported vulnerabilities, Branch Office VPN, and Mobile VPN with SSL. Also, in this release the Mobile VPN with SSL client has been updated to support Windows 7 and Windows 64-bit operating systems.

See the Resolved Issues section for more information.

Appliances Supported with This Release

The Firebox® X Edge e-Series v10.2.12 software works only on Firebox® X Edge e-Series models. It does not operate and cannot be installed on the Edge, SOHO 6, SOHO 6 Wireless, S6, S6 Wireless or SOHO models.

Contact your account manager to purchase a Firebox® X Edge e-Series appliance.

Important Notice on Software Licensing

The Firebox® X Edge e-Series enforces the following software licensing rules:

- **Registration** — You must register the Firebox X Edge e-Series with LiveSecurity to receive a feature key. If you do not have a valid feature key, only one user can connect to the Internet through the Edge.
- **LiveSecurity** — You must have a current LiveSecurity subscription to install software upgrades.
- **WebBlocker** — When the WebBlocker subscription expires, the Edge device denies all outgoing HTTP traffic by default. You can control this behavior through the **WebBlocker > Settings** page.
- **spamBlocker** — When the spamBlocker subscription expires, spamBlocker stops evaluating mail and allows all mail.

Installation

Use these instructions to install the Firebox® X Edge v10.2.12 release. The v10.2.12 appliance software is installed only in English language by default; one additional language pack can be installed on the Edge during the **Edge Upgrade Wizard** as described in the installation instructions below. You can change the language for the Edge user interface on the Administration page in the Edge web interface.

If you use Windows XP (or other non-Vista version of Windows)

1. Go to http://www.watchguard.com/support and log in with your LiveSecurity user name and passphrase. Follow the link to the **Software Downloads** page and save the `Edge_10_2_12.exe` file to your hard disk.
2. We recommend that you reboot your Edge before you upgrade to Edge v10.2.12.
3. Double-click the `Edge_10_2_12.exe` file you downloaded in step 1 and complete the instructions in the **Upgrade Wizard** dialog box.
4. If you want to install a language pack, select the appropriate language during the Upgrade Wizard. You select the language for the Edge user interface in the Quick Setup Wizard or on the Administration page in the Edge web user interface.

If you use Windows Vista or another non-Windows operating system

1. Go to http://www.watchguard.com/support and log in with your LiveSecurity user name and passphrase. Follow the link to the **Software Downloads** page and save the `Edge_10_2_12.zip` file to your hard disk. Decompress the file.
2. We recommend that you reboot your Edge before you upgrade to Edge v10.2.12.
3. Connect to the Firebox® X Edge System Status page.
   To do this, type https:// in the browser address bar, and the IP address of the Edge trusted interface.
   The default URL is: https://192.168.111.1
4. On the System Status page, click **Update**.
5. Click **Browse**. Find and select the `yakfw.sysa-dl` file, then click **Open**.
6. Click **Update**. To complete the installation, you must restart the Firebox Edge.
7. To install a language pack, repeat Steps 3-5, but select one of the following files in Step 4:

French:	`lang-fr-10.2.12-arm.wgpkg-dl`
Japanese:	`lang-ja-10.2.12-arm.wgpkg-dl`
Simplified Chinese:	`lang-zh-10.2.12-arm.wgpkg-dl`

8. After the Edge restarts, go to the Administration page to change the language in the user interface.

After the update, the System Status page shows the new version as: `10.2.12 Nov 23 2009 Build 248909`

> ***Note*** If you currently use Edge v8.0.x software on your Edge, there is a specific upgrade path that you must follow to install this release. Use this chart to determine your upgrade path:

If you are currently running:	Install in this order:
Edge e-Series v8.0	Edge e-Series v8.0.1 → v8.0.3 → v8.6.2 → v10.2 → v10.2.12
Edge e-Series v8.0.3 or later	Edge e-Series v8.6.2 → v10.2 → v10.2.12

If you are not sure what version of software is currently installed on your Edge, log in to the administrative interface of your Edge and look at the System Status page. To get Edge e-Series v8.0.3 software, contact WatchGuard Technical Support.

To install the v10.2 Mobile VPN with IPSec client software

There is no new Mobile VPN with IPSec client for this release. You can continue to use the v10.2 client, which you can download from the WatchGuard Software Downloads web site. The name of the file is `WatchGuard_EntryCl_Win_1010_059.exe`.

Or, you can use the v11.1 Mobile VPN with IPSec client from the software download page. Follow the installation instructions in the release notes for the v11.1 Mobile VPN with IPSec client.

To install the Mobile VPN with SSL v10.2.12 client for Windows

The v10.2.12 Mobile VPN with SSL client is integrated into the Fireware 10.2.12 appliance software. Mobile VPN with SSL users can choose to download the v10.2.12 client from the Firebox or download the v10.2.12 client from the WatchGuard web site if the remote users do not have access to the Firebox on port 4100.

When a SSL client computer running an earlier version of the client software connects to a Firebox running v10.2.12, the user sees a prompt to upgrade the SSL client version to 1.17. Select **Yes** to upgrade the Mobile VPN client version to v10.2.12. Mobile VPN with SSL continues to operate if the user chooses not to upgrade, however, the user does not receive the fixes available in the v10.2.12 Mobile VPN with SSL client.

To install Single Sign-On (SSO) software

There are no updates for the Single Sign-On client or agent software with this release. You can continue to use the v10.2.9 software. If you are upgrading from an SSO implementation installed prior to v10.2.9, you must first uninstall the existing SSO agent.

To install v10.2.9 Single Sign-On agent software

- Go to http://www.watchguard.com/support and log in with your LiveSecurity user name and passphrase. Follow the link to the Software Downloads page and download the WatchGuard Single Sign-On Agent v10.2.9. Save the WG-Authentication-Gateway.exe file to your hard disk.
- Install the file on a domain computer with a static IP address running Microsoft Windows 2003, Windows XP, or Windows Vista. It is a good idea to install the SSO agent software on your domain controller. Complete the setup wizard. For more setup instructions see the product help system.

To install v10.2.9 Single Sign-On client software

- Go to http://www.watchguard.com/support and log in with your LiveSecurity user name and passphrase. Follow the link to the Software Downloads page and download the WatchGuard Single Sign-On client v10.2.9. Save the WatchGuard-Authentication-Client.msi file to your hard disk.
- Because the SSO client installer is an MSI file, you can choose to automatically install it on your user's computers when they log on to your domain. You can use Active Directory Group Policy to automatically install software when users log on to your domain. For more information about software installation deployment for Active Directory group policy objects, go to http://www.microsoft.com. You can only install the client software on computers running Microsoft Windows 2003, Windows XP, or Windows Vista.

To install local WebBlocker and Quarantine Server software

> ***Note*** You can only install WebBlocker and Quarantine Server v10.2.3 on top of a previous 10.2 installation. The v10.2.12 release does not include an updated WebBlocker and Quarantine Server.

1. Go to http://www.watchguard.com/support and log in with your LiveSecurity user name and passphrase. Follow the link to the **Software Downloads** page and save the `WGEdge10_2_3QWB.exe` file to your hard disk.

2. Run the `WGEdge10_2_3QWB.exe` on a computer with WebBlocker and Quarantine Server v10.2 already installed. Follow the onscreen installation instructions.

Resolved Issues

General

- Edge v10.2.x uses ISC's DHCP server to assign DHCP IP addresses. Some versions of ISC's DHCP server are affected by a Denial of Service (DoS) vulnerability and cannot handle specially crafted DHCP requests. Edge v10.2.12 updates our implementation of the ISC DHCP server, to correct this issue. For more information about this flaw, see http://xforce.iss.net/xforce/xfdb/51717. [40557,40033]
- Edge v10.2.x uses OpenSSL to implement the Secure Sockets Layer (SSL) protocol. Many SSL implementations, including OpenSSL, are affected by a SSL/TLS renegotiation vulnerability that attackers could leverage in man-in-the-middle (MitM) attacks. Edge v10.2.12 updates our OpenSSL implementation. To correct this problem we disable TLS renegotiation. For more information about this flaw see: https://www.kb.cert.org/vuls/id/120541. [41351,41350]
- This release resolves an issue that caused the Edge to become unresponsive after multiple PPPoE renegotiations. [28695]
- The upgrade wizard now completes correctly when you install the Japanese language files. [40841]
- This release resolves an issue that caused an Edge to crash when you edit a policy. This issue only occurred if the Edge had Branch Office VPN polices added by the Management Server. [38740]

Branch Office VPN

- This release resolves an issue that caused branch office VPN tunnels to fail with the log message: `ipsec_input.c408 in resume_stack_dec_esp IPSEC Error: !(ntohs(iph->tot_len)==skb->len)` [40782]

Mobile VPN with SSL

- The Windows SSL VPN client has been updated to support Window7 and Windows 64-bit operating systems. [39841]
- The Mobile VPN with SSL client now successfully connects to a backup Firebox IP address if one is configured. [35256]
- If the `openvpn` process dies or is manually stopped, the Mobile VPN with SSL client no longer uses up 100% of the CPU on the client computer. [39997] [41424]
- This release resolves an issue that caused the SSL client logon to fail if the user connected and disconnected the SSL client multiple times without closing the SSL client. [41425]
- This release resolves an issue that prevented the SSL client from releasing the assigned IP address. [39004]

Proxies

- When you use a caching proxy server, the Firebox no longer prevents an FTP session from a web browser from succeeding because of an HTTP proxy line parsing error. [41018]

Known Issues and Limitations

Network Configuration

- The Wireless Client configuration tab for WAN1 is visible on all Edge e-Series models. Do not use this tab or make changes to the wireless settings if you do not have a Firebox X Edge e-Series Wireless. [23910]

DHCP

- DHCP relay server settings do not take priority over the Edge DHCP server. [16796]
- DHCP lease times are always reported in GMT. [15431]
- If you use the legacy MUVPN with IPSec client software and create a Mobile VPN default route (0.0.0.0/0) tunnel for a DHCP internal client, the client cannot renew its IP address and the connection terminates when the DHCP lease times out. If you use this configuration, we recommend that you set the DHCP lease timeout to be greater than 8 hours. [15912]

Multi-WAN/Policy-based Routing

- BOVPN tunnel failover may not operate correctly if WAN1 and the remote IPSec gateway are on the same subnet. [15935]
- Ping intervals are 2 seconds longer than the configured interval. [15598]
- IPSec tunnels always try to negotiate using WAN1. If the Edge is configured for multi-WAN, all IPSec tunnels use WAN1 unless a failover occurs. [23704]
- When you use multi-WAN, you can use the policy-based routing feature to select the external interface you want traffic for any policy to use. By default, the external interface is selected and load balancing is applied. If you select either WAN1 or WAN2, you must reboot the Edge for the change to take effect. [23519]
- When the Edge is configured for WAN failover to a modem, IPSec tunnel connections can fail to correctly re-key when a large amount of traffic is sent. [23560]

Authentication

- When the **Require user authentication (enable local user accounts)** setting is not selected, anonymous users that get access to the Internet are not identified as an "Active session" but use one of the available user licenses. [26493]
- When you install the Single Sign-On agent on Windows Vista, remote computers that try to enumerate the current users get an "Access denied" message. [23590]
- When a user authenticates to the Edge and the Edge is configured for Single Sign-On, the user cannot log off from the Edge. [23708]

  Workaround

  Use the **Enable automatic session termination** setting to enforce short authentication sessions if necessary.

- You must use Active Directory authentication for Single Sign-On to work. LDAP authentication is not supported for Single Sign-On.
- Windows 2000 Server no longer works for AD authentication.
- Users and groups must be in the search base, where previously only the user had to be within the search base.

Proxies

- The POP3 proxy setting **Deny unsafe URL patterns** is incorrectly labeled. The correct label for this field is **Deny unsafe file name patterns**.
- Initial BitTorrent connections are successfully blocked by the TCP-UDP (outgoing) proxy. If BitTorrent tries a subsequent connection using TCP port 80, it is allowed by the HTTP proxy or an HTTP filter policy. [27474]
- When you use the unsafe file name pattern feature of the HTTP proxy, file name patterns are applied to the full URI and may block some redirects. [23758]

Workaround

Allow unsafe file types and rely on content type blocking, or eliminate specified unsafe file name patterns from the default list when they cause a problem.

- When you enable the Outgoing proxy, outbound SIP connections are not correctly sent to the SIP proxy. [23546, all platforms]

Workaround

Configure the SIP proxy to directly handle SIP connections.

- You cannot call from one trusted endpoint to another trusted endpoint behind the same Firebox using an external PBX. This is commonly known as NAT “hairpinning.” [23872]
- The SMTP proxy does not completely strip Uuencoded and BinHex attachments. A small section of the attachment header remains in the body of the email together with the deny message. [22989]
- VoIP deployments are often complex and use many standard and proprietary protocols. Our current proxies only support standards-based traffic using the H.323 and SIP protocols, for basic voice, video, and data transfer. In VoIP industry terminology, these new proxies are more accurately called Application Layer Gateways (ALGs). Some proxy features, services, and configurations may not be supported with all types of VoIP hardware. These features include chat, whiteboarding, and fax transmission. Specific configuration limitations are noted below for each protocol. We strongly recommend that you perform compatibility and interoperability tests within your own organization before you deploy the H.323 or SIP proxy in a production environment.
- The H.323 proxy supports NAT traversal for voice and video traffic. However, support for H.323 Gatekeeper (PBX hosting/trunking) and T.120 multimedia is not included in this release. This limits use of the H.323 ALG to point-to-point scenarios, such as video conferences, that do not use an H.323 Gatekeeper server. While compatibility and interoperability cannot be guaranteed, point-to-point audio/video connectivity has been demonstrated with common software clients and video hardware.
- The SIP proxy supports NAT traversal for voice and video traffic. It does not provide the PBX registration capabilities of a typical standalone SIP Registrar-Proxy, but instead is transparent to SIP traffic. You must have your own Registrar-Proxy server to route PBX traffic, and this Registrar-Proxy server must be located on an external network. While compatibility and interoperability cannot be guaranteed, point-to-point audio/video connectivity and hosted audio connections have been demonstrated with common software clients.

WebBlocker

- No deny message is sent to the client when an HTTPS connection is correctly blocked because of your WebBlocker configuration. Blocked HTTPS connections are recorded in the log file. [22515]

spamBlocker

- On the **Quarantine Server > Edit-Auto Remove Rule** dialog box, changes to the **Auto Remove messages with specific text in the subject** rule are not saved to the Quarantine Server. While the UI shows that the rule has been deleted, it remains effective. The only way to make that rule ineffective is to clear the check box for **Auto Remove messages with specific text in the subject**. [26796]
- If you use both spamBlocker with Virus Outbreak Detection (VOD) enabled and Gateway AV to scan your email, and the SMTP proxy detects an email message that is both spam and a virus, the SMTP proxy applies the action that is configured for VOD to the message. Specifically, if the VOD action is set to **Strip**, then the attachment(s) are removed from the message and cannot be recovered. If the VOD action is set to **Lock**, the attachment is locked in the quarantined message. [23709, 23711]
- When spamBlocker finds a Virus Outbreak Detection (VOD) indication for an email message, all of the email's attachments are stripped or quarantined. If the email was sent in HTML format, this includes the message body.
- When an infected email message with multi-part attachments (i.e., embedded email messages) is detected and spamBlocker is configured to use the **Strip** action, a small section of the email header in the attachment remains in the delivered attachment, together with the deny message for the attachment. Virus content is always stripped. [23550]
- spamBlocker does not operate if the Edge cannot reach the primary DNS server. [18159]

Gateway AV/IPS

- Signature update log messages show the previous time and date information after a time zone change. The correct time zone is not used for these log messages until you restart the Edge. [17754]

Wireless

- Some wireless client hardware and software may not show all available wireless networks when the client has connected to one of those networks already. If you need to connect to another Edge Wireless network, you may need to disable and re-enable your wireless network adapter.
- When the WAN1 interface is configured as a wireless client, the Traffic Control feature does not operate correctly. [23757]
- Wireless clients that use Windows XP SP1 may not be able to connect when the Edge is configured to use "WPA2 ONLY" for wireless authentication. [23808]
- The WAP light on the front panel of the Edge is lit either when the Edge is configured as a Wireless Access point or when the External WAN1 interface is configured as a wireless client. [23121]
- When you activate the Wireless Guest account you may see the Edge DHCP server stop three times when the Edge restarts. The DHCP server operates correctly within two minutes after the Edge has restarted. 23792]
- You cannot use an XBOX 360 wireless client to establish a wireless connection to the Edge. [27481]
- If your Edge is running an earlier version of Wireless Guest Services (Edge v8.0 through Edge v8.5), you must reconfigure Guest Services after you upgrade to Edge v10.2.12.

VPN

- The Edge uses more memory when IKE renegotiations are configured to occur frequently. This can cause slow Edge management connections. If you change the default IPSec settings, make sure that the tunnel does not exchange keys more than two times per hour. [24221]

- An Edge using v8.6.2 under WSM Centralized Management shows a red exclamation mark for tunnels that have exchanged new keys based on time expiration if no traffic has passed through that tunnel since the key exchange. Once traffic is sent through this tunnel, the red exclamation mark disappears and the tunnel operates correctly. [22412]
- Outgoing Mobile VPN with IPSec connections through the Edge may not operate correctly when using a Cisco VPN Client. [19183]

Mobile VPN with SSL

- The Mobile VPN with SSL client v11.x is not compatible with a Firebox X Edge e-Series device running v10.2.x.
- After the Mobile VPN with SSL client first connects, any subsequent changes made to the Mobile VPN with SSL configuration cause a connection problem with Windows Vista SP1 clients. The client appears to connect correctly; however, the client sends a log message that it unsuccessfully flushed the ARP table. [29621]

Workaround

There are 2 options to work around this issue:

1. Disable User Account Control (UAC) on the Vista PC; or

2. Go to Program Files >WatchGuard >WatchGuard Mobile VPN with SSL and right-click `wgsslvpnc`. Select **Run as Administrator**.

- If an SSL client is connected to the Edge and the administrator changes the Mobile VPN with SSL configuration, the SSL client is not disconnected from the Edge. Each user must manually disconnect and then reconnect to get the new SSL configuration file. [23921]
- You cannot install the Mobile VPN with SSL client on a Windows 2000 Professional computer. [23667]
- The Mobile VPN with SSL client cannot connect to the Edge from the trusted network. [22547]

Workaround

Configure Mobile VPN with SSL clients to connect to the Edge from the optional network.

- The Mobile VPN with SSL Mac OS X client does not check for its configuration when its connection to the Firebox is lost (not disconnected). You must disconnect and reconnect to establish the VPN connection again. [23109]
- The Mobile VPN with SSL client can fail to stay connected if the client computer has more than one active network interface. [27112]
- The Mobile VPN with SSL client can fail to connect when it is configured to have routes to 12 or more networks. The client has a limit to the number of routes it can support related to the client configuration size. The route limit is not exact, but, depending on data in the configuration the limit is approximately 12 to 25 routes. [24226]

SNMP

- When you configure the Edge to use SNMP v3, the password must be eight (8) characters or more to operate correctly. [23531]

Traffic Control

- Traffic Control for IPSec uses the VPN-ANY rule instead of the most specific rule. [24206]

Logging and Real-time Monitoring

- When you look at the Edge System Status page, you may see this error in your log files: `httpd doInclude: INCLUDE failed for "lang.inc" result code was -1.` The log message is informational and can be ignored. [27322]
- Log messages appear truncated when the Edge sends log messages to a legacy WatchGuard Security Event Processor Log Server. [27430]
- Traffic between the trusted and optional networks is not shown in the event log file. [15611]
- When you enable **Log traffic prioritization** on the **Network > Traffic Control** page, the prioritization is not included in log messages generated by any proxy policy. [23164]

Resetting an Edge to Factory Default Settings

- The configuration file is not erased when you restore the factory default settings. [15174]

> **Workaround**
>
> When you restore the Edge to factory default settings, make sure you hold the reset button on the Firebox X Edge e-Series for 45 seconds to erase the configuration file.

User Interface

- During the Quick Setup Wizard, a second login prompt is requested after you enter your feature key. [21994]
- You may need to clear your browser cache after you update the Edge from v8.x to v10.x to see new user interface options and all new features. [20457]
- If you use Internet Explorer 7 or Mozilla Firefox 3 to manage your Firebox X Edge e-Series, you see a Certificate Security warning. This warning appears because the self-signed certificate used by each Firebox X Edge by default does not contain the correct information for your network. While previous versions of these browsers show a similar warning, the new versions are more strongly worded. If you use Internet Explorer, you can disregard the message and continue. If you use Firefox, you must add a certificate exception for the Firebox X Edge on each client computer. [14434]

User Documentation

Documentation changes for the Edge v10.2.12 release are included in the most current English help system available at www.watchguard.com/help/documentation. There is no updated Edge User Guide for this release.

Technical Assistance

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

Issues Resolved in Earlier 10.2.x Releases

For your convenience, this section shows a list of resolved issues from the release notes of all versions of 10.2.x prior to this one. For installation information, tech notes, and known issues for each of these releases, download the complete release notes for that specific release.

Edge v10.2.1 Resolved Issues

General

- The Edge now saves the list of Allowed MAC Addresses when the configuration is updated. [27242]
- The error message: `SSL VPN Protocol/Port (udp:80) conflicts with HTTP` no longer occurs when UDP port 80 is selected on the Mobile VPN with SSL setup page Advanced tab. [27702]
- You can now enable Mobile VPN with SSL when the Edge is also configured for 1-to-1 NAT using a secondary IP address and the same port/protocol as SSL VPN. [27863]

Proxies

- You can now allow BinHex attachments through the SMTP and POP3 proxy policies. [27927]
- The SMTP proxy and POP3 proxy no longer strip attachments with extra padding characters from base64-encoded messages. [27445]

spamBlocker

- You can now add up to 80 entries to the spamBlocker exception list. [27098]

Edge v10.2.2 Resolved Issues

General

- The help links in the Quick Setup Wizard now work correctly. [23489]
- Resolved issue that caused an error message to occur when you ran the *Edge_10_2_2.exe installer for Chinese, French, or Japanese.* [28121]

VPN

- The BOVPN default settings are now the same for Edge v10.2.2 and Fireware v10.2.2. [28389]

Mobile VPN with SSL

- You can now use Mobile VPN with SSL with an Edge that has NAT applied. [27844]

Edge v10.2.3 Resolved Issues

General

- Resolved an upgrade issue that prevented the VPN-ANY policy from being created when upgrading from v8.6.2 or older. [29321]
- You can now enable Dead Peer Detection for Mobile VPN with IPSec. [23498]

Mobile VPN with SSL

- The Mobile VPN with SSL client now supports Window Vista SP1. [27901]

- The Mobile VPN with SSL client and gateway now protect against "Man in the Middle" attacks. The Mobile VPN with SSL gateway generates a self-signed x.509 certificate when an IP address is assigned to the external interface of the Firebox. The gateway presents this certificate the first time a v10.2.3 client connects.
  Because the certificate is self-signed, all Mobile VPN with SSL users see a warning message about an “un-trusted” certificate the first time they connect to the Firebox. The user is given the option to confirm the certificate as trusted and save the certificate locally. When you accept the certificate as “trusted,” it allows the Mobile VPN with SSL client to warn the user if the certificate changes to alert the user of a possible Man in the Middle attack. [27304]

Quarantine Server

- Resolved an issue that caused quarantined email in HTML or Rich Text to show up as plain text when released from the Quarantine Server. [28058]

SMTP Proxy

- The SMTP proxy now sends a 200 success message when spamBlocker is configured to send email to a Quarantine Server when it matches a spamBlocker exception. A 200 success message is also sent when spamBlocker is configured to quarantine email classified as spam, bulk, suspect or VOD. Sending a 200 success message back to the sending email client helps to prevent duplicate emails on the Quarantine Server. [29332] [29333]

Single Sign-On

- Non-ASCII characters in the domain name no longer cause authentication to fail with log message `Malformed "list" response from SSO Agent.` [27198]

Edge v10.2.4 Resolved Issues

General

- This release includes a fix for an authentication bypass vulnerability present in Firebox X Edge devices running v10.2.3 or earlier. For complete information about the vulnerability, go to www.watchguard.com/archive/broadcasts.asp
- Language packs now install correctly. [29986]
- Authentication on port 4100 no longer supports SSLv2 and now meets Payment Card Industry (PCI) compliance standards. [29794]
- You can now set a PPPoE authentication retry timeout. [29829]

HTTPS Proxy

- The idle timeout in the HTTPS proxy is no longer treated as a session timeout. [28706]

Multi-WAN/Policy-based Routing

- Traffic that matches a policy-based routing rule now consistently follows the correct policy routing action. [27601] [27602] [25791]
- When using multi-WAN, all outgoing packets sent through WAN2 (ETH3) are no longer shown in the log files as sent from the initial interface ETH1 (for trusted) or ETH2 (for optional). [27519]

Single Sign-On

- The Single Sign-On solution is improved with the v10.2.4 release. A Single Sign-On client is now available to install on each computer in a network to improve the accuracy of who is authenticated. See the client installation instructions above for more information.

Edge v10.2.5 Resolved Issues

General

- This release includes a fix for an authentication bypass vulnerability present in Firebox X Edge devices running v10.2.3 or earlier. For complete information about the vulnerability, go to https://www.watchguard.com/archive/showhtml.asp?pack=78373
- Language packs now install correctly. [29986]
- Authentication on port 4100 no longer supports SSLv2 and now meets Payment Card Industry (PCI) compliance standards. [29794]
- You can now set a PPPoE authentication retry timeout. [29829]

HTTP Proxy

- The HTTP proxy no longer performs a body scan for both IPS and Gateway AV when both security features are enabled. When both Gateway AV and IPS are enabled, body scanning occurs only for Gateway AV. This improves throughput. [28002]

HTTPS Proxy

- The idle timeout in the HTTPS proxy is no longer treated as a session timeout. [28706]

BOVPN

- The Edge no longer prevents administration access to the trusted interface when a branch office VPN is configured with a remote network that overlaps with the Edge local network (for example: remote network 10.0.0.0/8, Edge local network 10.0.2.0/24). [28352] [27106]

Mobile VPN with SSL

- Mobile VPN with SSL client connections no longer fail. This issue occurred after an upgrade to Edge v10.2.4. [30951]
- When you edit the "Default" group from the Firebox Users page, the **Allow remote access with Mobile VPN with SSL** check box no longer appears selected. [23449]

Multi-WAN/Policy-based Routing

- Traffic that matches a policy-based routing rule now consistently follows the correct policy routing action. [27601] [27602] [25791]
- When using multi-WAN, all outgoing packets sent through WAN2 (ETH3) are no longer shown in the log files as sent from the initial interface ETH1 (for trusted) or ETH2 (for optional). [27519]
- Resolved 10.2.4 issue causing traffic matching a policy based route and a BOVPN Tunnel to not route through the BOVPN tunnel. [31015]

Single Sign-On

- The Single Sign-On solution is improved with the v10.2.5 release. A v10.2.4 Single Sign-On client is now available to install on each computer in a network to improve the accuracy of who is authenticated. See the client installation instructions above for more information.

Edge v10.2.6 Resolved Issues

General

- The Edge no longer stops sending authentication attempts after receiving the first CHAP failure message from the ISP during PPPoE re-authentication. [29564]

- The Schedule Reboot option is now available when you use French, Japanese or Chinese language packs. [29361]

BOVPN

- BOVPN tunnels between two Edge Firebox devices, both with dynamic external interfaces and both using dynamic DNS, now negotiate correctly after the external IP address changes on one or both Edges. [28100]
- The Edge no longer crashes when an Avaya phone that uses H.323 sends H.323 traffic through a BOVPN tunnel. [24191]

Mobile VPN with SSL

- The Edge no longer sends a log message that includes the password of the Mobile VPN with SSL user during authentication. [27572]
- When you start the Mobile VPN with SSL client, the DNS client service on that computer now stops and restarts to update the computer to use the DNS server IP address provided in the Mobile VPN with SSL client configuration. [28120]

NAT

- 1-to-1 NAT now operate correctly when applied to an incoming policy that uses the same port as another incoming policy. [31243]

Edge v10.2.7 Resolved Issues

General

- In the HTTP proxy settings, the **Deny unsafe file name patterns** option has been renamed to **Deny unsafe URL patterns** to more accurately describe the function of this setting. [23758]

spamBlocker

- The spamBlocker exception limit now supports up to 150 exceptions. [28385]

Mobile VPN with SSL

- The Windows SSL VPN client no longer fails to install on Windows XP with a Runtime Error message. [31932]
- The Windows SSL VPN client now operates correctly after a computer returns from sleep mode. [31523]

Authentication

- The Edge now correctly enforces SSL VPN user authentication based on Active Directory group membership. [27363]

Edge v10.2.8 Resolved Issues

General

- VPN and configuration updates no longer fail when you enable syslog through a VPN tunnel when WAN1 to get its IP address with PPPoE. [29965]
- The Chinese installer now works correctly. [30997]

NAT

- You can now masquerade traffic using 1-to1 NAT through an IPSec VPN tunnel with IKE Keepalive. [20649][RFE20649]

Wireless

- Several bugs affecting wireless performance under heavy load have been fixed. [34619] [34621] [31637]
- You can now download files through a wireless connection without a kernel crash. [31132]
- The CPU no longer grows to 100% usage after a few hours on a wireless Edge. [34514]

Single Sign-On

- The SSO agent no longer crashes with Windows Event message: `EventType clr20r3`. [32775]
- The SSO client now returns the correct domain name whether the domain filter is empty or not.
- The SSO client and agent now handle both AD domain name information and NetBIOS domain name information correctly.
- The SSO client and agent now respond correctly to unexpected disconnections that occur within 10 seconds.

Mobile VPN with SSL

- The Mobile VPN with SSL Mac OS X client now shows the Bound IP Address and Gateway Connected IP Address correctly. [34561]
- The Mobile VPN with SSL Mac OS X client now removes the search domain and DNS information when it is disconnected or you exit. [34564]
- The Mobile VPN with SSL Mac OS X client now shows both WINS addresses. [34560] [23635]
- The Mobile VPN with SSL Mac OS X client now sets the default log level to low. [34563]
- Routes of available networks are now correctly added when you install the Mobile VPN with SSL client software on a computer running Windows Vista. [34558]

Edge v10.2.9 Resolved Issues

Authentication

- The administrator or group user level now displays correctly when it is set to **full**. [36257, 36259]

Single Sign On

- The SSO client software now reports both for both the Active Directory domain and a NetBios domain, if a computer participates in both. Now, administrators can specify either the Active Directory name or the NetBios name and Single-Sign On will work correctly. [36307]
- You can now install the SSO client on Microsoft Windows Vista. [35869]
- When you enable SSO, you can now obtain group information even if the SSO agent is not installed on the Domain Controller. [36043]
- When you install the SSO client on Vista, you can now see the build number. [36289]
- SSO client and agent communication is now more reliable and several timeout issues have been resolved. [35199, 35200]
- SSO now ignores group names exceeding 32 characters and continues to process other group names. It no longer returns a "domain name str too log" error. [35988]

VPN

- BOVPN Failover/Failback now works correctly when the gateway fails. [33572]
- A VPN tunnel between Edge and Fireware can now be reliably re-established after Fireware restarts [35361]
- 1-to-1 NAT over branch office VPN tunnels now supports dead peer detection (DPD). [35700]
- You can now add BOVPN routing policies in the Japan and Chinese localized user interfaces. [33874, 27723]

PPPoE

- In a multi-WAN round robin configuration set up with a static IP address and PPPoE, traffic can now fail over to the other WAN when the WAN with PPPoE is disconnected, [33857]
- PPPoE can recover if it is disconnected and reconnected within 3 seconds. [33858]

Proxy

- Incoming SMTP proxy traffic now works with multi-WAN round robin. [32732]
- The IP address in the URL for the WebBlocker override password is now correct when the user is connected through the trusted interface. [36307]

Edge v10.2.10 Resolved Issues

VPN

- You can now bind the built-in SSL VPN server to trusted or optional interfaces in addition to the external interface. [37934]
- The rekey in a BOVPN tunnel no longer fails after the Phase 1 lifetime expires when the Firebox external interface is configured with a dynamic IP address. [38812]
- When you configure a branch office VPN tunnel between an Edge with a static IP address and an Edge configured to use DynDNS, the VPN tunnel can now successfully renegotiate if the DNS record is updated slightly later than when the dynamic IP address changes. [34359]
- The Firebox X Edge now cleans up old security associations (SAs) effectively. This solves a problem because large amounts of old SA information can cause BOVPN tunnels to fail and the Firebox to become unresponsive. [37565]
- The NAT address and local address in 1-to-1 NAT configuration for a BOVPN configuration are now swapped to be consistent with WatchGuard System Manager's Policy Manager In other words, when 1-to-1 NAT is used, the NAT address should be used in the peer’s local-remote pair. [38769]

  > Note: If you currently use 1-to-1 NAT in a branch office configuration on your Edge, you must swap your NAT address and your local address.

NAT

- The Firebox X Edge now supports 16 1-to-1 NAT entries. [19027]
- You can now add a secondary IP address to WAN2 on your Edge. [23443]
- If the external interface field of an incoming policy was changed from External to WAN2 earlier, it will now stay as WAN2 after other changes in the policy. [23769]

User Interface

- The Reboot Request option for Firebox X Edge e-Series Wireless devices is now the same color as the other reboot request options. [23633]
- The user interface option to logout authenticated users now operates correctly when using IE6, IE7, Netscape9, Mozilla1.8, and Mozilla Firefox2.0. [29970]

Edge v10.2.11 Resolved Issues

General

- The support for SSL Weak Encryption Algorithms has been removed to adhere to PCI compliance. [35194]
- The embedded lighttpd module has been upgraded from version 1.4.18 to version 1.4.22 to avoid several reported vulnerabilities in version 1.4.18. [39698]
- The number of cfgfilter processes no longer increases each time the external IP address changes. This prevents excess memory use. [39633]
- This release resolves a memory leak that occurred when SNMP was enabled. [34395]
- The OSS daemon no longer causes the CPU to run at 100%. [34514]
- You can now schedule a Firebox reboot on a weekly schedule. [38173]

VPN

- The IKED process no longer crashes when it initiates DPD over BOVPN. [39444]
- VPN Keep Alive no longer shows as not responding although the tunnel is up and pings to the keep alive host complete successfully. [38988]
- The SSL VPN daemons now start successfully after an upgrade when the Edge primary SSL VPN IP address is not equal to the WAN1 IP address. [39680]

Networking

- You can now use a Secondary IP address on WAN2 for outbound NAT,[39534]
- External wireless status now displays correctly on the **System Status > Wireless Statistics** page. [39380]