



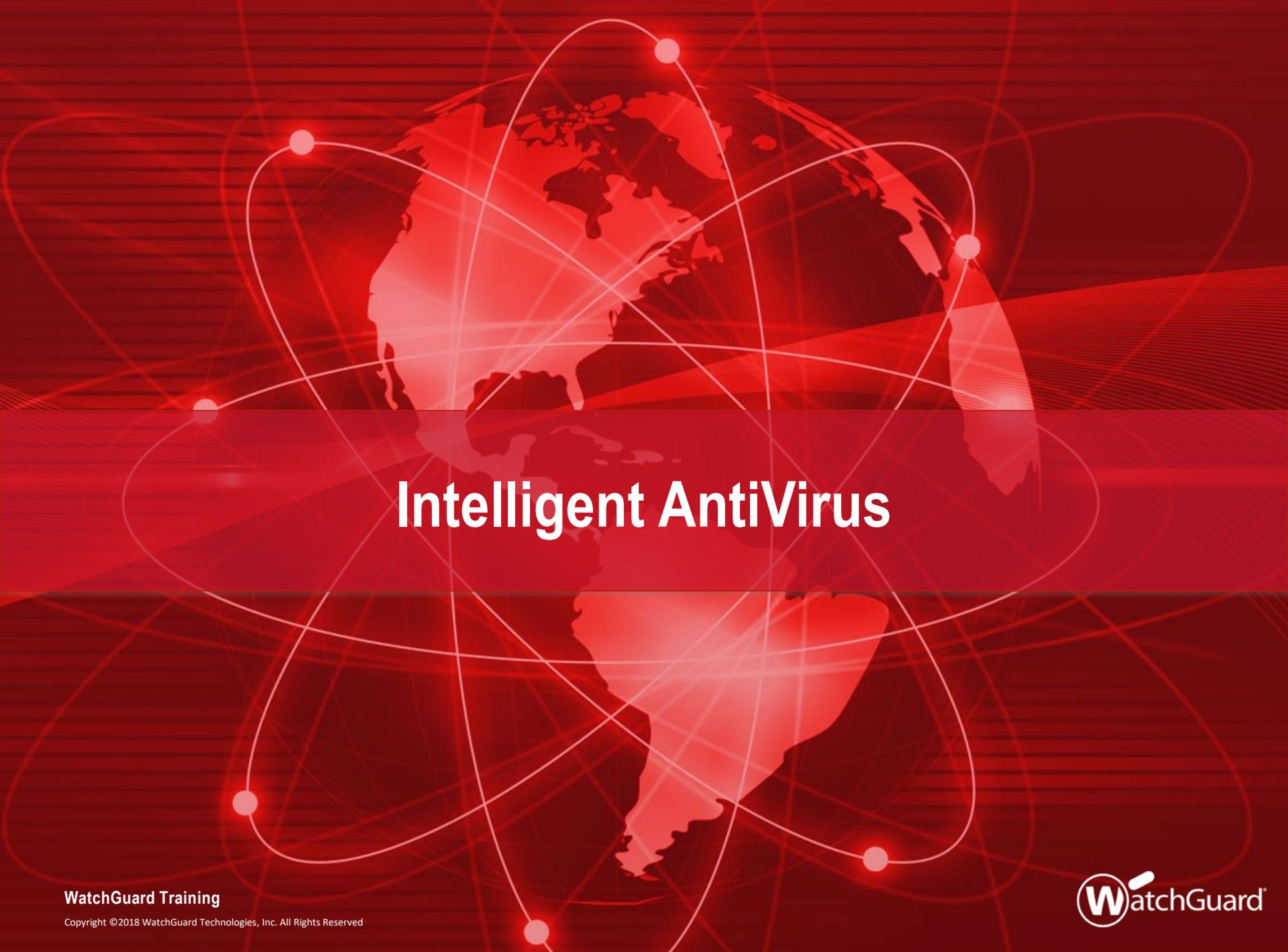
What's New in Fireware v12.2

What's New in Fireware v12.2

- Intelligent AntiVirus
- Geolocation by Policy
- TLS profiles for SMTP & POP3 proxies
- Restore configuration file from Web UI
- Firebox Cloud Enhancements
- WebBlocker Usability Enhancements
- On-premises WebBlocker Server
- FQDN Enhancements

What's New in Fireware v12.2

- Control Firebox-generated traffic
- AES-GCM support
- Secondary IP addresses for BOVPN gateways
- Mobile VPN with SSL and Access Portal settings
- Redundant single sign-on
- Certificate Management Enhancements
- Gateway Wireless Controller Enhancements
- Other Enhancements



Intelligent AntiVirus

Intelligent AntiVirus

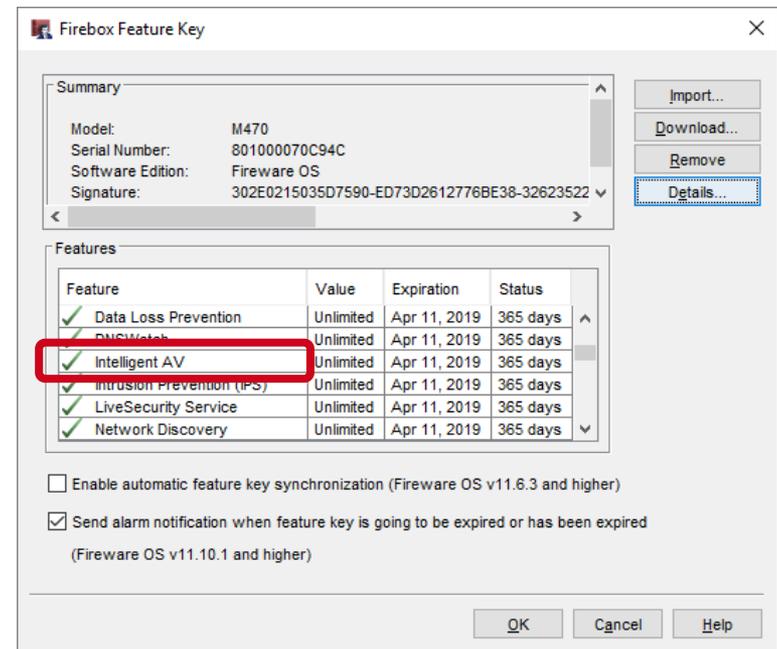
- Intelligent AntiVirus is a new subscription service that enhances the ability of Gateway AntiVirus to detect new threats and polymorphic malware
 - WatchGuard has partnered with Cylance to provide this as a supplemental scanning solution for our higher-end Firebox models
 - Intelligent AntiVirus uses artificial intelligence and mathematical models to examine and characterize millions of file attributes to determine if a file is a threat

Intelligent AntiVirus and Gateway AntiVirus

- Intelligent AntiVirus adds another layer of protection to the Gateway AV security service
- With Intelligent AntiVirus enabled, Gateway AntiVirus uses two scan engines
 - BitDefender — Gateway AntiVirus scan engine
 - Cylance — Intelligent AntiVirus scan engine
- These scan engines work together to increase the ability of the Firebox to detect and block malware before it can enter your network

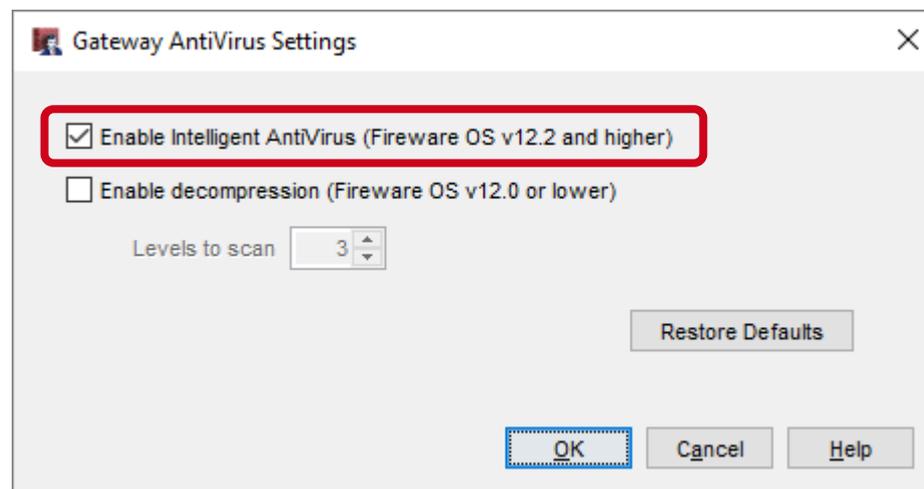
Intelligent AntiVirus Models and Licensing

- Intelligent AntiVirus is supported on these Firebox models:
 - Firebox M370 and higher
 - Firebox Cloud
 - Firebox V
- Intelligent AntiVirus is included in Total Security subscription for Firebox models that support it
 - To enable this feature, the feature key must include the feature **Intelligent AV**



Intelligent AntiVirus Configuration

- When Intelligent AntiVirus is licensed, you can enable it in Gateway AntiVirus global settings
 - Select **Enable Intelligent AntiVirus**



Intelligent AntiVirus Configuration

- In the **Update Server** settings for services, enable automatic signature updates for **Intelligent AntiVirus Signatures**

Update Server

Automatic Update

Enable automatic update Interval: 1 hour(s)

Intrusion Prevention and Application Control Signatures

Gateway AntiVirus Signatures

Intelligent AntiVirus Signatures (Fireware OS v12.2 and higher)

Data Loss Prevention Signatures

Botnet Detection Sites Database (Fireware OS v11.11 and higher)

Geolocation Database (Fireware OS v11.12 and higher)

Server

Type the URL for the update server

https://services.watchguard.com

HTTP Proxy Server

Connect to the update server with an HTTP proxy server

Specify an IPv4 or IPv6 address, or a host name. To use an IPv6 address, your Firebox must run Fireware OS v11.12 or higher.

Server address: IPv4 Address . . .

Server port: 8080

Server authentication: None

User name:

Domain:

Password:

Restore Defaults

OK Cancel Help

Intelligent AntiVirus Status

- In Firebox System Manager, Intelligent AntiVirus status and statistics are available on the Subscription Services tab

The screenshot displays the Firebox System Manager interface. The 'Subscription Services' tab is selected and highlighted with a red box. Within this tab, the 'Intelligent AntiVirus' section is also highlighted with a red box. This section shows the following data:

Activity since last restart		Updates	
Viruses found:	0	Installed version:	20180501.1300
Objects scanned:	0	Last update:	May 1, 2018 2:52:20 PM PDT
Objects not scanned:	0	Version available:	20180501.1300

Buttons for 'History' and 'Update' are visible next to the update information.

Below the Intelligent AntiVirus section, the 'Application Control and Intrusion Prevention Service' section is visible, showing statistics for intrusion prevention and application control, along with update information for its signatures.

At the bottom of the interface, there is a 'Refresh Interval' dropdown set to '60 seconds' and a 'Pause' button.

Intelligent AntiVirus Status

- In Fireware Web UI, Intelligent AntiVirus status and statistics are available on the Subscription Services dashboard

The screenshot shows the WatchGuard Fireware Web UI interface. The left sidebar contains navigation options: DASHBOARD, Front Panel, Subscription Services (highlighted with a red box), FireWatch, Interfaces, Traffic Monitor, Gateway Wireless Controller, Geolocation, Mobile Security, Network Discovery, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, VPN, and SYSTEM. The main content area is titled 'Subscription Services' and includes a 'User: admin' header with a help icon and a refresh button. Below the header, there are four service status cards: Gateway AntiVirus, Intelligent AntiVirus (highlighted with a red rounded rectangle), Intrusion Prevention Service, and WebBlocker. Each card displays a line graph for 'Activity since last restart' and a table for 'Signatures'. The Intelligent AntiVirus card shows 0 viruses found, 0 objects scanned, and 0 objects not scanned. The Intrusion Prevention Service card shows 0 scans performed, 0 intrusions detected, and 0 intrusions prevented. The WebBlocker card shows 0 total requests and 0 denied requests. Each card has an 'UPDATE' button.

Subscription Services

Gateway AntiVirus

Activity since last restart

Viruses found: 0
Objects scanned: 0
Objects not scanned: 0

Signatures

Installed version: 20180412.900
Last update: Thu, Apr 12 2018 11:10:32 AM
Version available: 20180412.900
[UPDATE](#)

Intelligent AntiVirus

Activity since last restart

Virus found: 0
Objects scanned: 0
Objects not scanned: 0

Signatures

Installed version:
Last update: Wed, Dec 31 1969 04:00:00 PM
Version available:
[UPDATE](#)

Intrusion Prevention Service

Activity since last restart

Scans performed: 0
Intrusions detected: 0
Intrusions prevented: 0

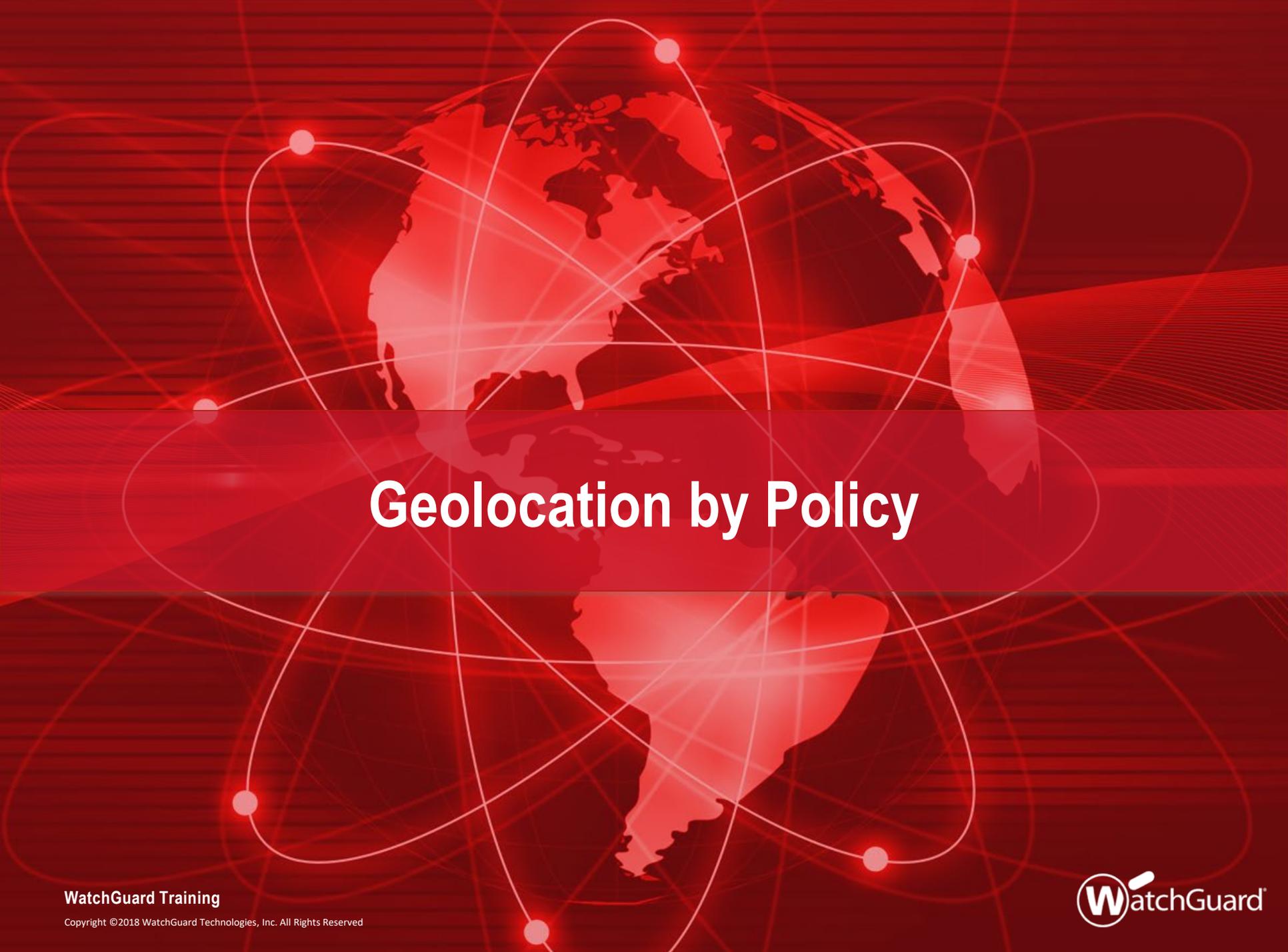
Signatures

Installed version: 4.822
Last update: Tue, Apr 10 2018 10:40:20 AM
Version available: 4.822
[UPDATE](#)

WebBlocker

Activity since last restart

Total requests: 0
Denied requests: 0
[CLEAR CACHE](#)



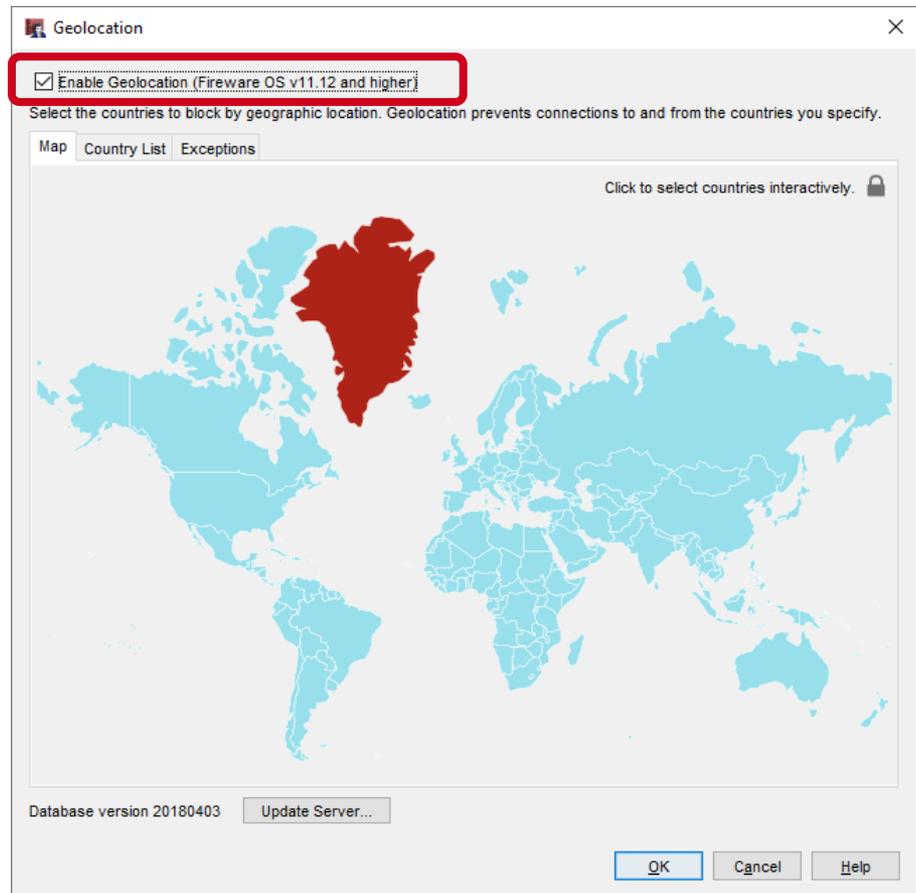
Geolocation by Policy

Geolocation by Policy

- You can now enable Geolocation at the policy level
- This provides you with more granular control over the types of connections the Firebox denies based on geographic location

Geolocation by Policy

- Geolocation prevents connections to and from the countries you specify
- When you enable the Geolocation subscription service, Geolocation is automatically enabled in all policies



Geolocation by Policy

- You can enable or disable Geolocation in policy settings

Firewall Policies / Edit

Name: HTTP-proxy Enable

Settings Application Control Traffic Management Proxy Action Scheduling

Advanced

Connections are: Allowed

Policy Type: HTTP-proxy

PORT	PROTOCOL
80	TCP

FROM: Any-Trusted

TO: Any-External

ADD REMOVE

ADD REMOVE

Enable Geolocation

Enable Intrusion Prevention

Enable bandwidth and time quotas

Edit Policy Properties

Name: HTTP-proxy Enable

Policy Properties Advanced

HTTP-proxy connections are... Allowed Send TCP RST

From: Any-Trusted

Add... Edit... Remove

To: Any-External

Add... Edit... Remove

Enable Application Control: Global

Enable Geolocation

Enable IPS for this policy

Enable bandwidth and time quotas (Fireware OS v11.10 and higher)

Proxy action or Content action: HTTP-Client.Standard.1

OK Cancel Help

SMTP and POP3 over TLS

SMTP and POP3 over TLS

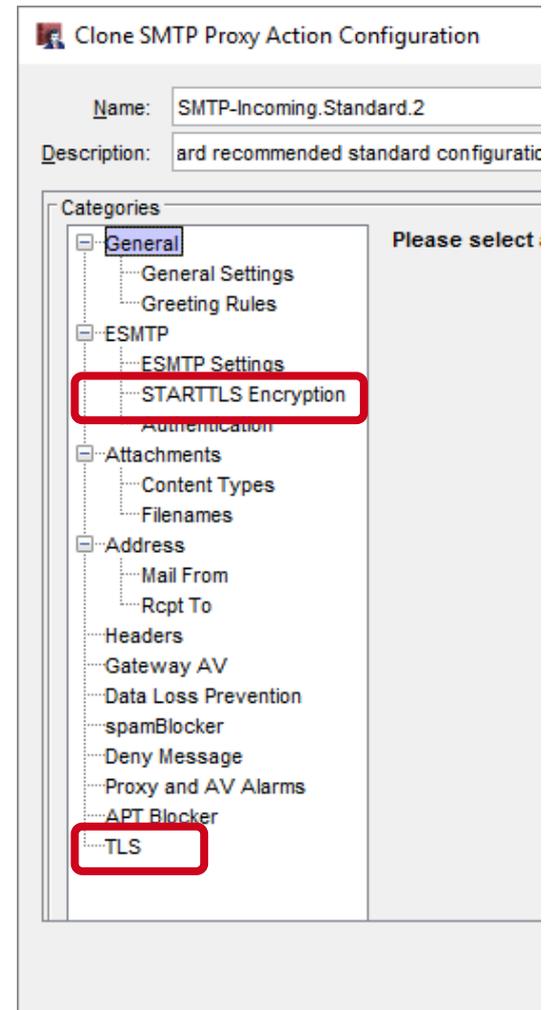
- This release extends TLS profile support to the POP3 and SMTP proxies
 - TLS profiles were previously supported only for the IMAP and HTTPS proxies
- This update enables POP3 and SMTP proxies to inspect mail traffic encrypted with TLS on implicit secure ports:
 - POP3 over TLS
 - SMTP over TLS
- STARTTLS settings for SMTP also now use TLS profiles

Explicit and Implicit TLS

- Transport Layer Security (TLS) is a protocol that provides encryption and security for data sent over a network
- TLS can be explicit or implicit
 - Explicit TLS
 - Server converts a non-TLS connection to a TLS connection when it receives the STARTTLS command
 - Implicit TLS
 - Server expects TLS based on the port
 - IMAPS: port 993 (support added to IMAP proxy in Fireware v12.1)
 - SMTPS: port 465 (support added to SMTP proxy in Fireware v12.2)
 - POP3S: port 995 (support added to POP3 proxy in Fireware v12.2)

SMTP Proxy — TLS

- The SMTP proxy now supports both implicit and explicit TLS
 - Explicit TLS (STARTTLS Encryption)
 - Supported in previous releases
 - STARTTLS now uses a TLS profile
 - Implicit TLS (SMTPS)
 - New in Fireware v12.2
 - Uses a TLS profile
- You can select a separate TLS profile for STARTTLS and SMTPS



Secure SMTP (SMTPS)

- The SMTP proxy now supports Secure SMTP (SMTPS)
- The SMTP proxy supports:
 - SMTP on TCP port 25
 - SMTPS on TCP port 465 (new)

New Policy Properties

Name: SMTP-proxy Enable

Policy Properties Advanced

Policy Type: SMTP-proxy

SMTP Port	Protocol
25	TCP

SMTPS Port	Protocol
465	TCP

Comment
Policy added on 2018-04-19T10:11:47-07:00.

Tags:

Policy Tags...

Logging...

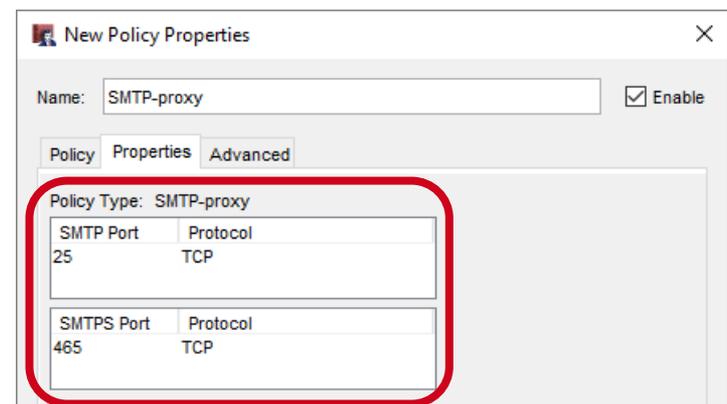
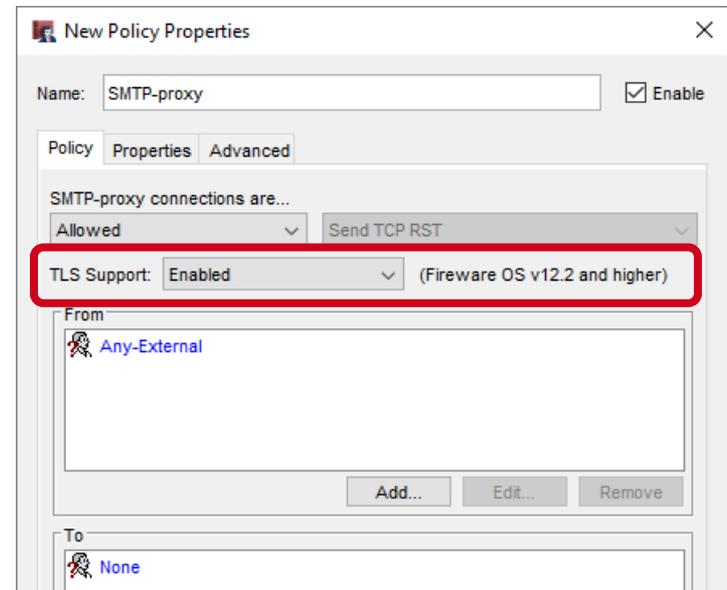
Auto-block sites that attempt to connect

Specify Custom Idle Timeout

OK Cancel Help

SMTP Proxy — TLS Support

- The **TLS Support** option controls which ports the SMTP proxy listens on:
 - **Disabled** — SMTP proxy listens on port 25 only
 - **Enabled** (default) — SMTP proxy listens on ports 25 and 465
 - **Required** — SMTP proxy listens on port 465 only
- The port list depends on the TLS Support option



SMTP Proxy — TLS Support

- In Fireware Web UI, the TLS Support option and ports appear together on the Settings tab

Firewall Policies / Add

Name Enable

Settings Application Control Traffic Management Proxy Action Scheduling Advanced

Connections are Policy Type **SMTP-proxy**

TLS Support

SMTP PORT	PROTOCOL
25	TCP

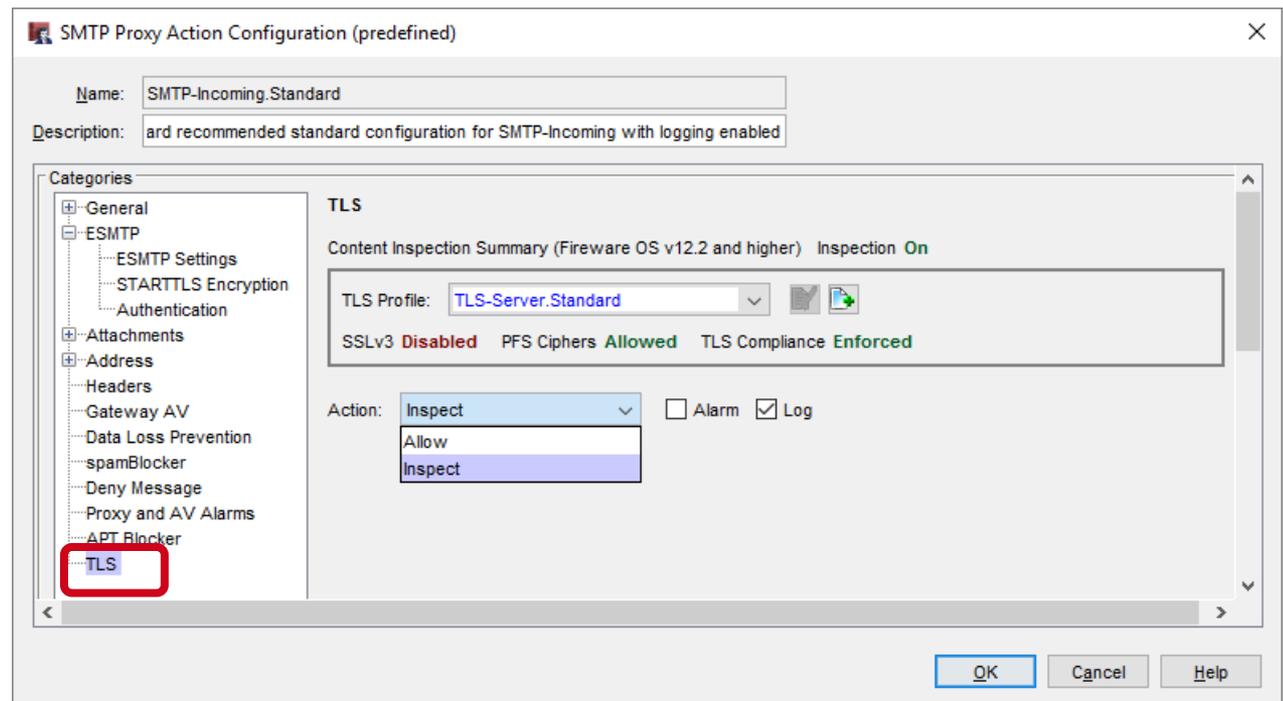
SMTPS PORT	PROTOCOL
465	TCP

FROM

TO

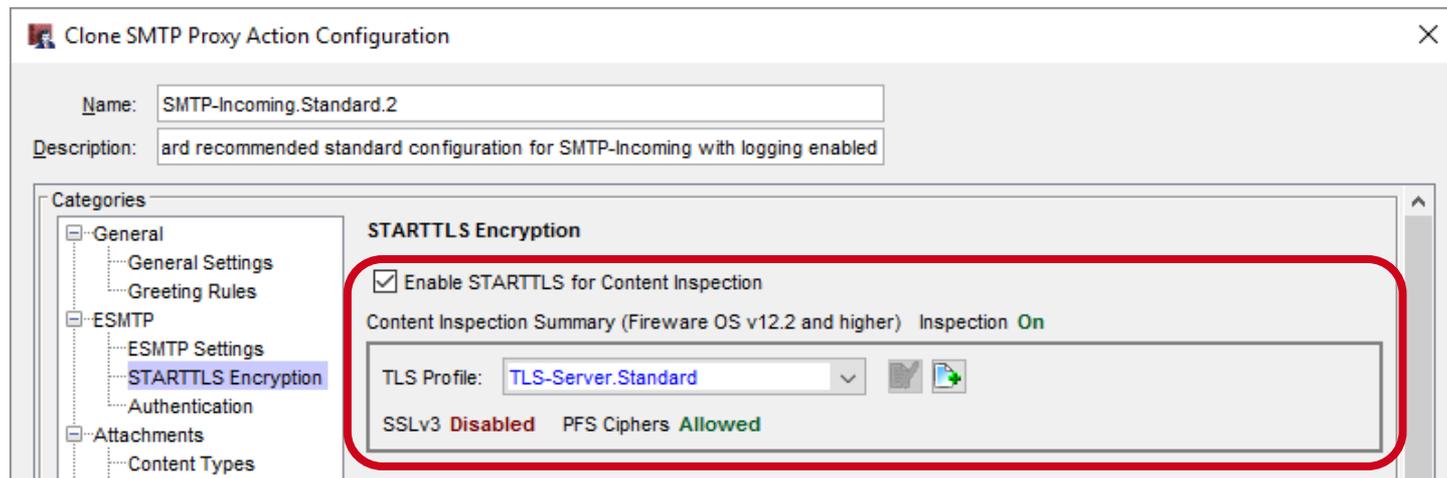
SMTP Proxy Action — TLS Settings

- SMTP proxy actions now include TLS settings
 - TLS settings apply only when TLS Support is set to **Enabled** or **Required** in the SMTP policy
- The TLS settings in the proxy action include:
 - **TLS Profile**
 - **Action**
 - Allow
 - Inspect



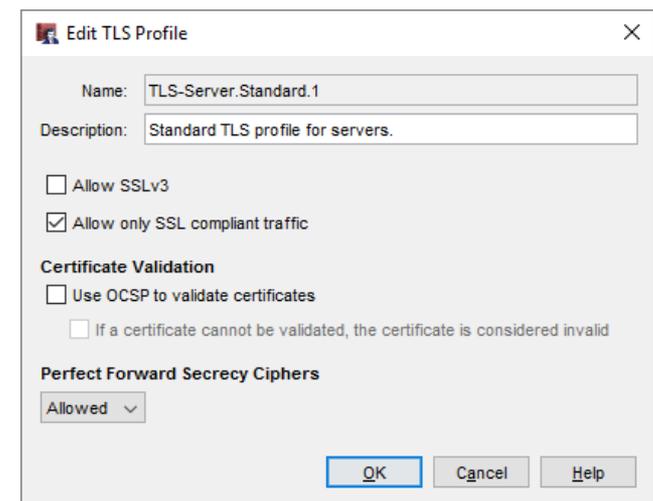
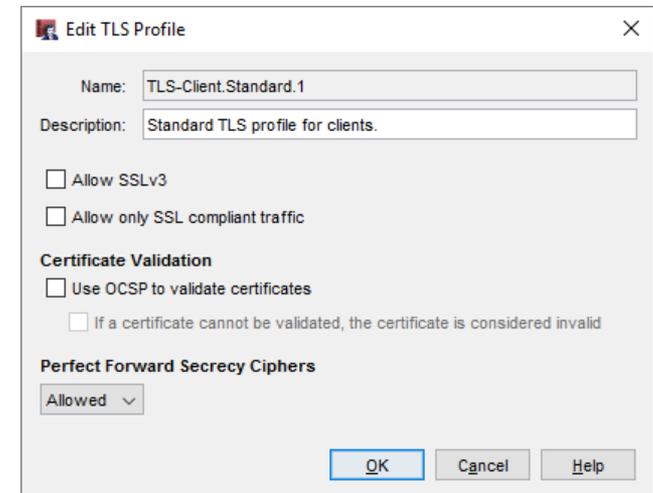
SMTP Proxy Action — STARTTLS Encryption

- In the ESMTP settings, the TLS Encryption settings are now called STARTTLS Encryption
 - These settings also use a TLS profile
 - The TLS profile you select in the STARTTLS Encryption settings can be different from the TLS profile in the TLS settings



SMTP and POP3 over TLS

- A TLS profile is a collection of TLS-related security settings:
 - Allow SSLv3
 - Allow only SSL compliant traffic
 - Certificate Validation (OCSP)
 - Perfect Forward Secrecy Ciphers
- The POP3 and SMTP proxies now use the same client and server TLS profiles previously supported for other proxies



Secure POP3 (POP3S)

- The POP3 proxy now supports Secure POP3 (POP3S)
- The POP3 proxy supports:
 - POP3 on TCP port 110
 - POP3S on TCP port 995 (new)

Edit Policy Properties

Name: POP3-proxy.1 Enable

Policy Properties Advanced

Policy Type: POP3-proxy

POP3 Port	Protocol
110	TCP
POP3S Port	Protocol
995	TCP

Comment

Policy added on 2018-04-18T16:52:43-07:00.

Tags:

Policy Tags...

Logging...

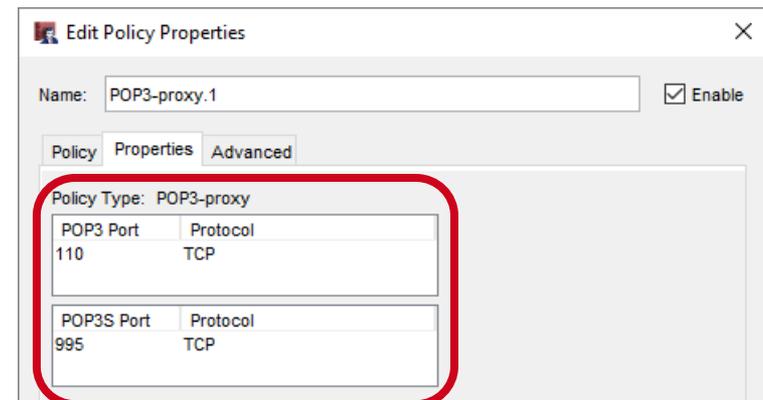
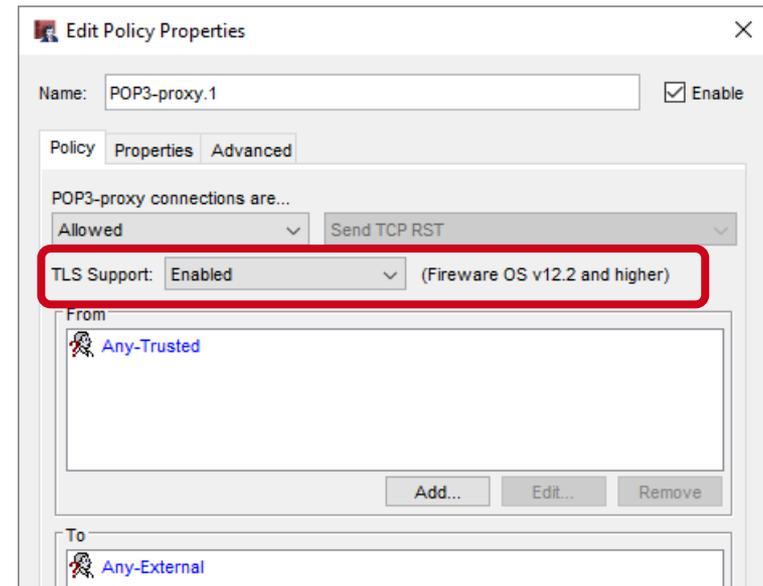
Auto-block sites that attempt to connect

Specify Custom Idle Timeout

OK Cancel Help

POP3 Proxy — TLS Support

- The **TLS Support** option controls which ports the POP3 proxy listens on:
 - **Disabled** — POP3 proxy listens on port 110 only
 - **Enabled** (default) — POP3 proxy listens on ports 110 and 995
 - **Required** — POP3 proxy listens on port 995 only
- The port list depends on the TLS Support option



POP3 Proxy — TLS Support

- In Fireware Web UI, the TLS Support option and ports appear together on the Settings tab

Firewall Policies / Edit

Name Enable

Settings Application Control Traffic Management Proxy Action Scheduling Advanced

Connections are

TLS Support

Policy Type **POP3-proxy**

POP3 PORT	PROTOCOL
110	TCP

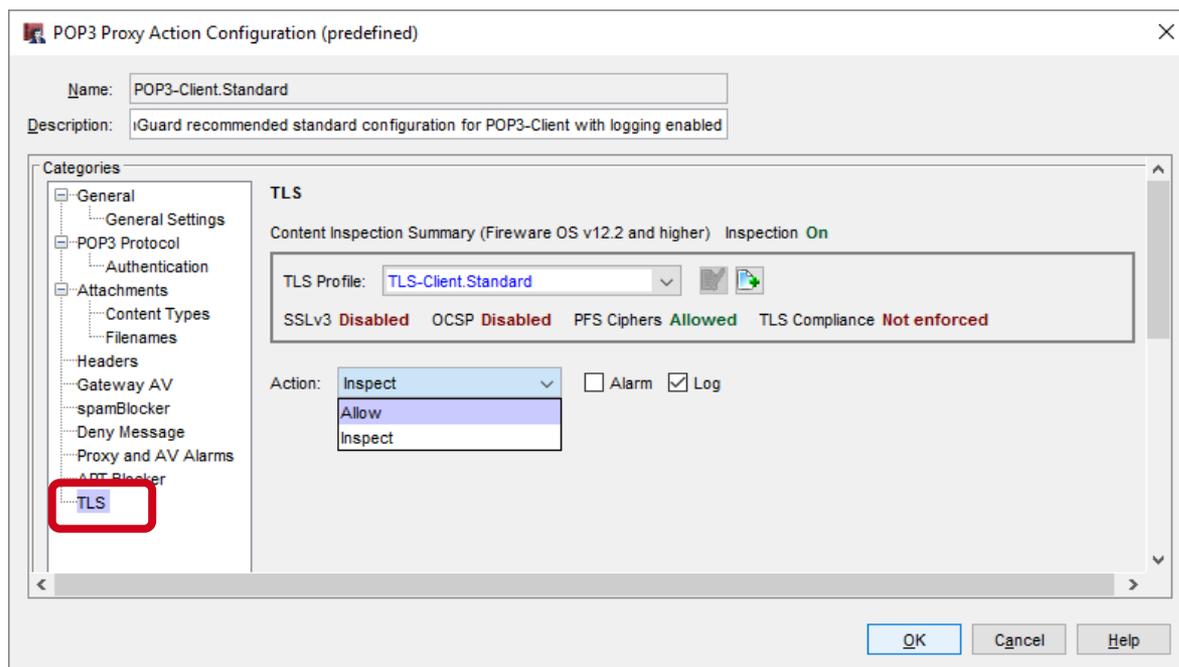
POP3S PORT	PROTOCOL
995	TCP

FROM

TO

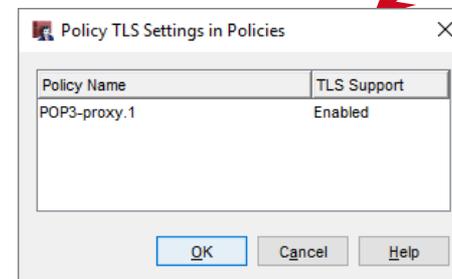
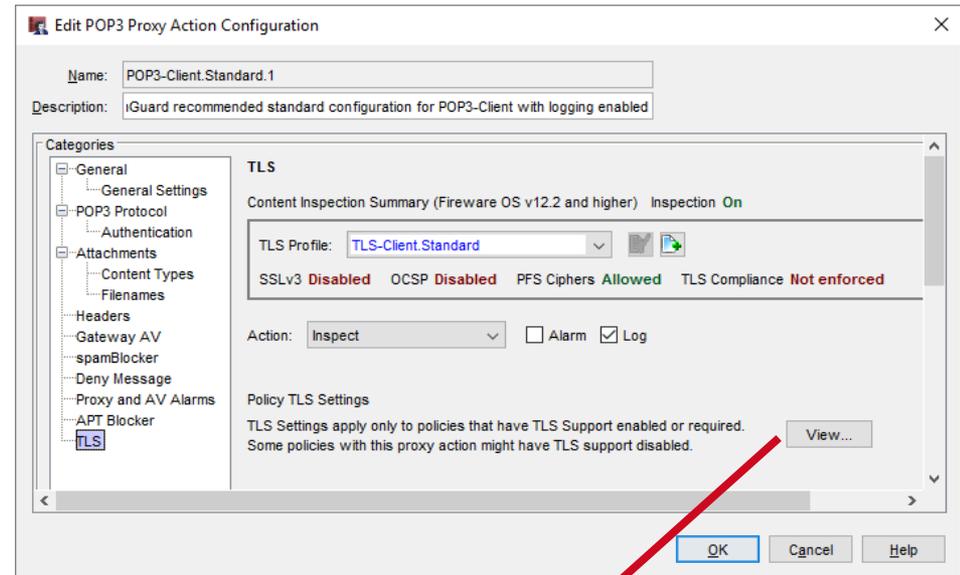
POP3 Proxy Action — TLS Settings

- POP3 proxy actions now include TLS settings
 - TLS settings apply only when TLS Support is set to **Enabled** or **Required** in the POP3 policy
- The TLS settings in the proxy action include:
 - **TLS Profile**
 - **Action**
 - Allow
 - Inspect



POP3 Proxy Action TLS Settings

- TLS settings apply only when TLS Support is enabled or required in a policy
- If you edit the proxy action from the **Proxy Actions** list, click **View** to see whether TLS is enabled for policies that use the proxy action



TCP/UDP Proxy Action

- The TCP-UDP proxy action now applies to POP3 and SMTP
 - The POP3 proxy action applies only to TLS/SSL requests on port 995
 - The SMTP proxy action applies only to TLS/SSL requests on port 465
 - The HTTPS proxy action applies to TLS/SSL requests on all ports not specified by other protocols

TCP-UDP Proxy Action Configuration (predefined)

Name: TCP-UDP-Proxy.Standard

Description: Ird recommended standard configuration for TCP-UDP-Proxy with logging enabled

Categories

General

Select a proxy action for each protocol.

HTTP: HTTP-Client.Standard

HTTPS: HTTPS-Client.Standard
HTTPS Proxy action applies to TLS/SSL requests on all ports not explicitly specified by other protocols

SIP: SIP-Client

FTP: FTP-Client.Standard

IMAP: IMAP-Client.Standard (Fireware OS v12.1 and higher)
 Redirect IMAPS (TLS on port 993)
This proxy action applies only to TLS/SSL requests on port 993.

POP3: POP3-Client.Standard (Fireware OS v12.2 and higher)
 Redirect POP3S (TLS on port 995)
This proxy action applies only to TLS/SSL requests on port 995.

SMTP: SMTP-Outgoing.Standard (Fireware OS v12.2 and higher)
 Redirect SMTPS (TLS on port 465)
This proxy action applies only to TLS/SSL requests on port 465.

Other Protocols: [Allow]

Enable logging for reports

Override the diagnostic log level for proxy policies that use this proxy action
 Diagnostic log level for this proxy action: Error

OK Cancel Help

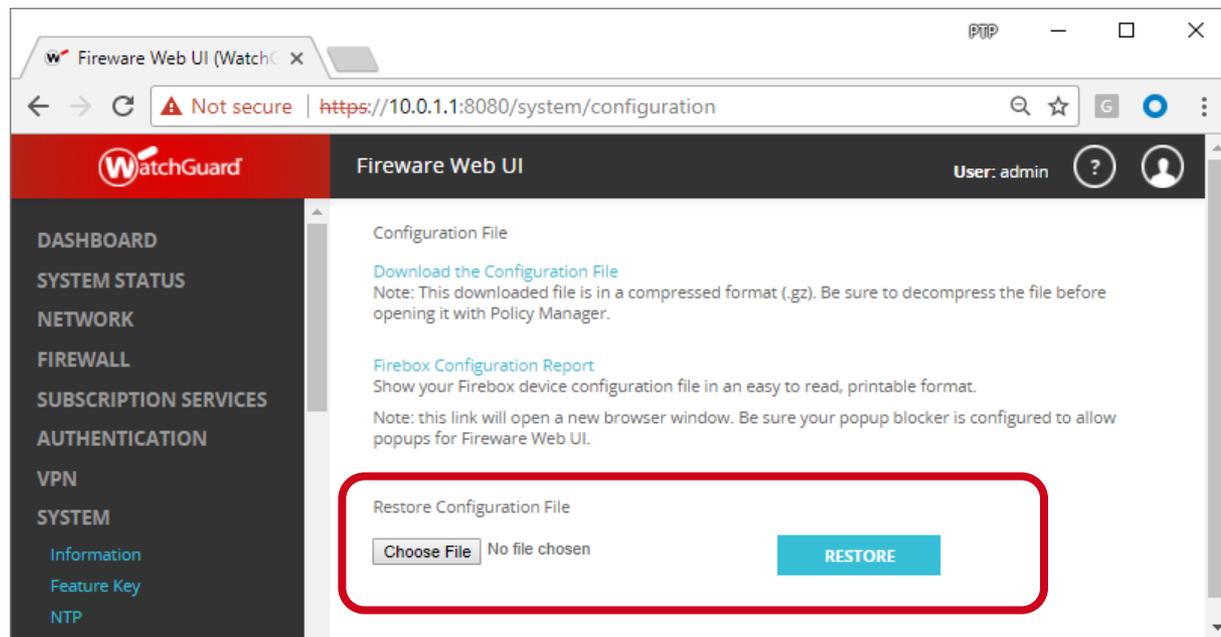
Restore Configuration from Firewall Web UI

Restore Configuration from Fireware Web UI

- In previous versions of Fireware, you could save the configuration to a file from Fireware Web UI
- You can now restore the saved configuration file from Fireware Web UI

Restore Configuration from Firewall Web UI

- In Firewall Web UI, you can restore a saved configuration file from the Configuration File page



Restore Configuration from Firewall Web UI

- To restore a saved configuration file:
 1. In Firewall Web UI, select **System > Configuration**
 2. Select a saved configuration file for the same Firebox model
The configuration file can be one of these types:
 - Compressed (.gz) configuration file downloaded from the Web UI
 - Configuration file (.xml) saved from Policy Manager or extracted from the .gz file
 3. Click **Restore**

Configuration File

[Download the Configuration File](#)
Note: This downloaded file is in a compressed format (.gz). Be sure to decompress the file before opening it with Policy Manager.

[Firebox Configuration Report](#)
Show your Firebox device configuration file in an easy to read, printable format.
Note: this link will open a new browser window. Be sure your popup blocker is configured to allow popups for Firewall Web UI.

Restore Configuration File

WatchGuard-XTM.xml.gz

Restore Configuration from Fireware Web UI

- When you restore a configuration file, the Firebox checks the file to verify compatibility
- The Firebox does not restore the configuration file if:
 - Firebox model does not match
 - OS compatibility setting is newer than the installed OS version
- When you restore a configuration file, there is no change to the Firebox feature key
 - If you restore a configuration that enables subscription services that are missing or expired in the feature key, or if the Firebox does not have a feature key, the behavior for those services is the same as when a feature key expires



Firebox Cloud Enhancements

Firebox Cloud Enhancements

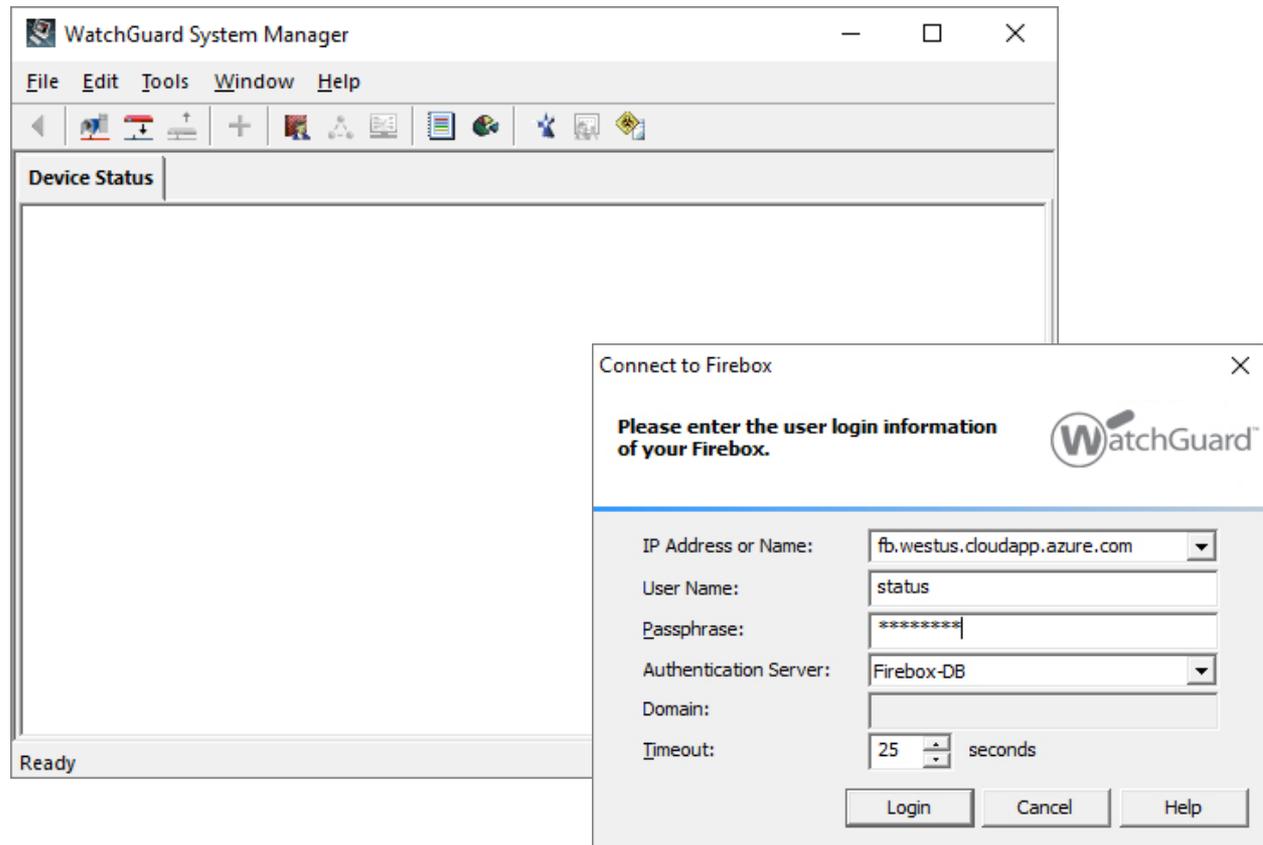
- WatchGuard System Manager and WSM Management Server can now manage Firebox Cloud
- Firebox Cloud now supports these features:
 - Single Sign-On (SSO)
 - spamBlocker
 - Quarantine Server
- Firebox Cloud for Azure will support an hourly license option

Firebox Cloud — WSM Support

- WatchGuard System Manager (WSM) now supports management of Firebox Cloud
 - WatchGuard System Manager
 - Policy Manager
 - Firebox System Manager
 - WSM Management Server now supports management of Firebox Cloud for:
 - Management of multiple Firebox OS updates
 - Drag-and-drop VPNs
 - Templates
- WSM Quick Setup Wizard is not supported for Firebox Cloud

Firebox Cloud — WSM Support

- To connect to Firebox Cloud from WatchGuard System Manager, use the Firebox Cloud IP address or DNS name

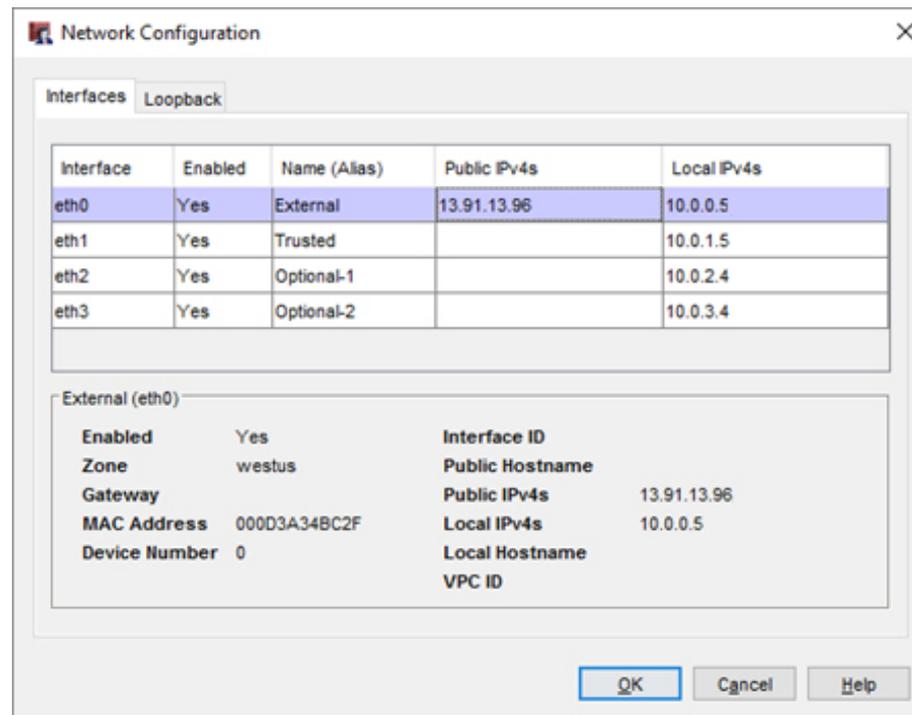


Firebox Cloud — Policy Manager

- Policy Manager does not allow you to configure features and options that are not supported by Firebox Cloud, such as:
 - Most networking features (manage network settings in the VM configuration)
 - Gateway Wireless Controller
 - Quotas
 - Mobile VPN with SSL Bridge VPN option
 - Services: Network Discovery, Mobile Security, DNSWatch
 - Hotspot
 - Explicit Proxy (not currently hidden, but not supported)

Firebox Cloud — Policy Manager

- On the **Network > Configuration** page:
 - The **Interfaces** tab shows read-only interface information
 - On the **Loopback** tab you can configure a loopback interface



Firebox Cloud — Policy Manager

- When you save the Firebox Cloud configuration to a file, Policy Manager saves three files:
 - The configuration file (.xml)
 - The feature key file (_lic.tgz)
 - The VM information file (_vmhost.json)

Name	Date modified	Type	Size
 FireboxCloud.xml	4/20/2018 11:20 AM	XML Document	467 KB
 FireboxCloud_lic.tgz	4/20/2018 11:20 AM	TGZ File	1 KB
 FireboxCloud_vmhost.json	4/20/2018 11:20 AM	JSON File	2 KB

Firebox Cloud — Policy Manager

- Firebox Cloud configuration files are not compatible with other Firebox models
 - On the **Setup > System** page for Firebox Cloud, you cannot change the Firebox Model
 - On the **Setup > System** page for any other Firebox model, you cannot change the model to Firebox Cloud
 - In Policy Manager, you cannot create a new Firebox Cloud configuration

Device Configuration

Firebox Model: FireboxCloud FireboxCloud-MED

Name: Firebox

Location: system location

Contact: system contact

Time zone: (GMT) Greenwich Mean Time

OK Cancel Help

Device Configuration

Firebox Model: Firebox T Series T35-W

Name: Firebox X Edge

Location: Firebox X Core

Contact: Firebox X Peak

Time zone: WatchGuard XTM

WatchGuard XTMv

Firebox T Series

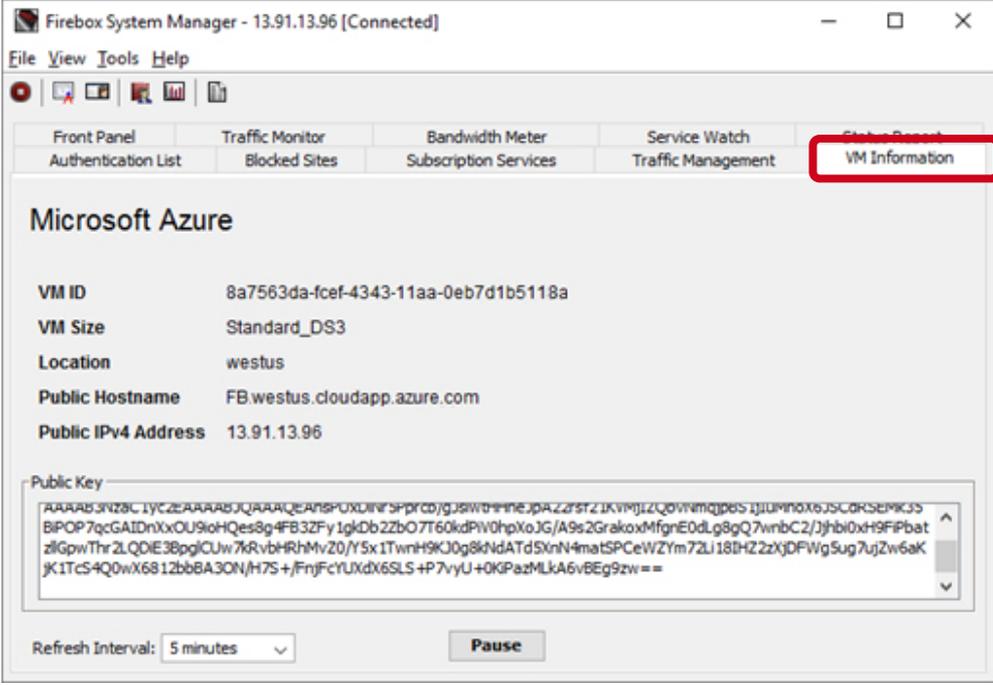
Firebox M Series

FireboxV

OK Cancel Help

Firebox Cloud — Firebox System Manager

- In Firebox System Manager, the **VM Information** tab shows information about the Firebox Cloud virtual machine
 - This is the same information available in Fireware Web UI on the **System Status > VM Information** page



The screenshot shows the Firebox System Manager interface. The window title is "Firebox System Manager - 13.91.13.96 [Connected]". The menu bar includes "File", "View", "Tools", and "Help". Below the menu bar is a toolbar with icons for Home, Refresh, Stop, Start, and Log. The main content area has a navigation bar with tabs: "Front Panel", "Traffic Monitor", "Bandwidth Meter", "Service Watch", and "VM Information" (which is highlighted with a red box). Below the tabs, the "VM Information" section is titled "Microsoft Azure" and displays the following details:

VM ID	8a7563da-fcef-4343-11aa-0eb7d1b5118a
VM Size	Standard_DS3
Location	westus
Public Hostname	FB.westus.cloudapp.azure.com
Public IPv4 Address	13.91.13.96

Below the table is a "Public Key" section with a text area containing a long string of characters:

```
AAAAAB3NzBc1YcZcAAAAABJQAAAQeANSFOXDInr3Pprcbjg8iwrHinejpaZzsrzZlXVmjZcQoVnmqpeS1j1uVnOx6JScCRSEPK3S  
BIPOP7qcGAIDnXxOU9ioHQes8g4FB3ZFy1gkDb2ZbO7T60kdPIW0hpXoJG/A9s2GrakoxMfgrE0dLg8gQ7wnbC2/Jjhb10xH9FFPbat  
zllGpwThrZLQDIE3BpglCUw7kRvbHrHmVz0/Y5x1TwnH9KJ0g8kNdATd5XnN4matSPCeWZYm72Lj18DHZ2zXJDFWg5ug7ujZw6aK  
JK1TcS4Q0wX6812bb8A3ON/H7S+/FnyFcYUXdx6SLS+P7vyU+OKPazMLkA6vBEg9zw==
```

At the bottom of the page, there is a "Refresh Interval" dropdown menu set to "5 minutes" and a "Pause" button.

Firebox Cloud — New Supported Features

- Fireware v12.2 for Firebox Cloud now supports configuration of these features in both Web UI and Policy Manager:
 - Single Sign-On
 - spamBlocker
 - Quarantine Server

The screenshot displays the WatchGuard Fireware Web UI. The left sidebar contains a navigation menu with the following categories and items:

- DASHBOARD
- SYSTEM STATUS
- NETWORK
- FIREWALL
- SUBSCRIPTION SERVICES
 - Access Portal
 - Application Control
 - APT Blocker
 - Botnet Detection
 - Data Loss Prevention
 - DNSWatch
 - Gateway AV
 - Geolocation
 - IPS
 - Quarantine Server
 - Reputation Enabled Defense
 - spamBlocker
 - Threat Detection
 - WebBlocker
- AUTHENTICATION
 - Servers
 - Settings
 - Users and Groups
 - Web Server Certificate
 - Single Sign-On
 - Terminal Services
 - Authentication Portal

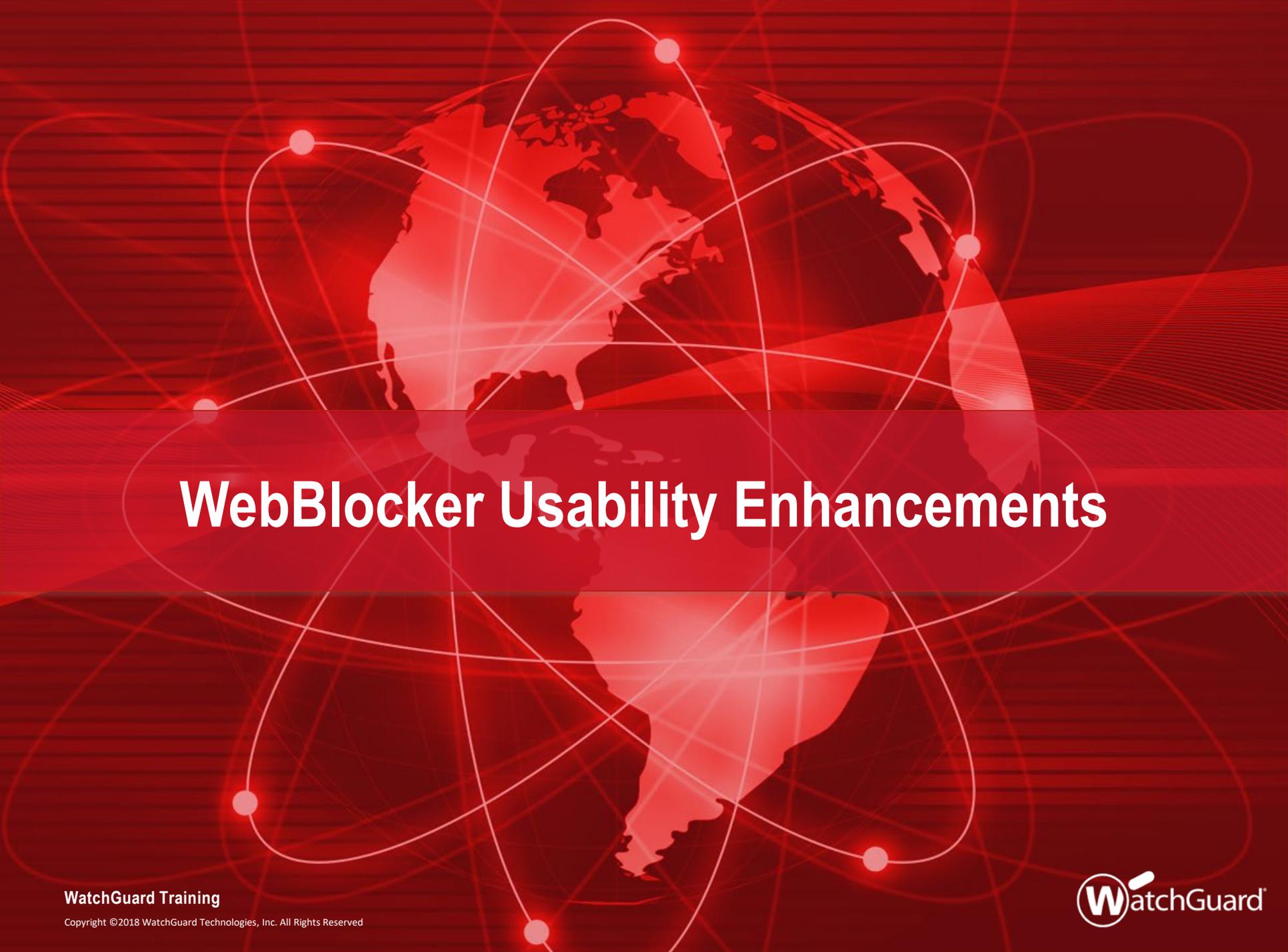
The main content area shows the configuration for Single Sign-On. It includes a lock icon and the text "Click the lock to make changes". Below this, there are tabs for "Active Directory" and "RADIUS". A checkbox labeled "Enable Single Sign-On (SSO) with Active" is present. The "SSO Agents" section includes a text input field for "SSO AGENT IP ADDRESS" and a note: "Note: To configure multiple SSO Agents on". The "SSO Exceptions" section includes a text input field for "SSO EXCEPTION". The "Settings" section includes two input fields: "Keep-Alive Interval" set to 10 and "Keep-Alive Timeout" set to 60. A checkbox labeled "Enable Single Sign-On (SSO) through B" is at the bottom.

Firebox Cloud — Feature Key Visibility

- Firebox Cloud with an hourly license does not require a feature key from WatchGuard
 - The cost of Firebox Cloud and all security services is included in the hourly price
- For Firebox Cloud with an hourly (pay as you go) license, the Feature Keys page is now visible in Fireware Web UI
 - Select **System > Feature Key**
 - The Feature Key page shows only the list of licensed features
 - There is no expiration date for each feature
 - The Feature Key page is read-only

Firebox Cloud — Azure Hourly License

- Previously, Firebox Cloud was available in the Microsoft Azure Marketplace only with a BYOL license
- Firebox Cloud v12.2 will be available for Azure with both BYOL and hourly license options
 - The hourly license includes a free 30 day trial
 - No hourly software charges for the instance during the trial
 - Azure infrastructure charges still apply
 - The trial converts to a paid hourly subscription upon expiration
- Firebox Cloud with both license options will be available in Azure Marketplace shortly after general availability (GA) of Fireware v12.2



WebBlocker Usability Enhancements

WebBlocker Usability

- WebBlocker has been updated to make it easier to see and manage denied categories in WebBlocker actions
- The UI for category management in WebBlocker is now more consistent with category management in Application Control

WebBlocker Usability Enhancements

- In a WebBlocker action you can now:
 - Filter categories by deny status or by top-level category
 - Search for a category by name
 - Click a column heading to sort the list by that column

WatchGuard Fireware Web UI

User: admin

WebBlocker / WebBlocker_Test

Action Name: WebBlocker_Test

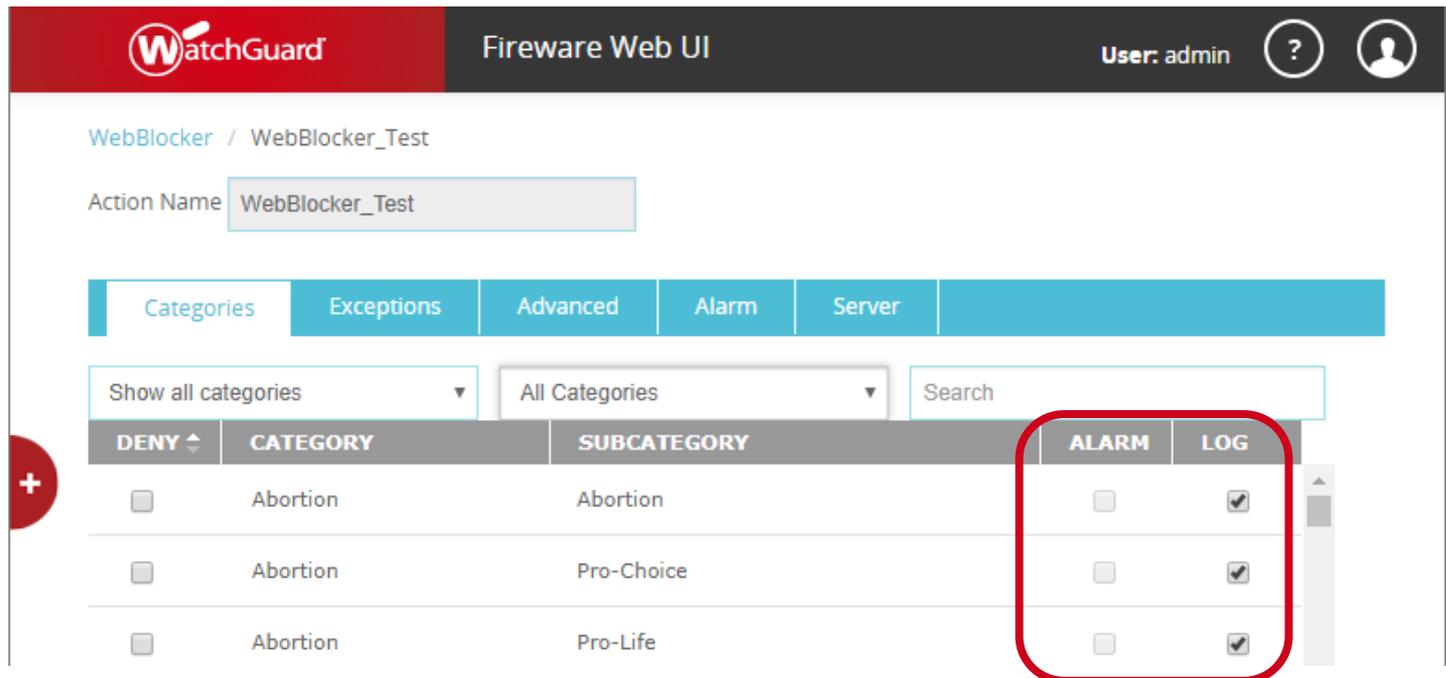
Categories | Exceptions | Advanced | Alarm | Server

Show all categories | All Categories | Search

DENY	CATEGORY	SUBCATEGORY	ALARM	LOG
<input type="checkbox"/>	Abortion	Abortion	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Abortion	Pro-Choice	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Abortion	Pro-Life	<input type="checkbox"/>	<input checked="" type="checkbox"/>

WebBlocker Usability Enhancements

- You can now configure **Alarm** and **Log** options per category
 - To receive notification when WebBlocker denies content for a category, select **Alarm**
 - To generate a log message when WebBlocker denies content for a category, select **Log**



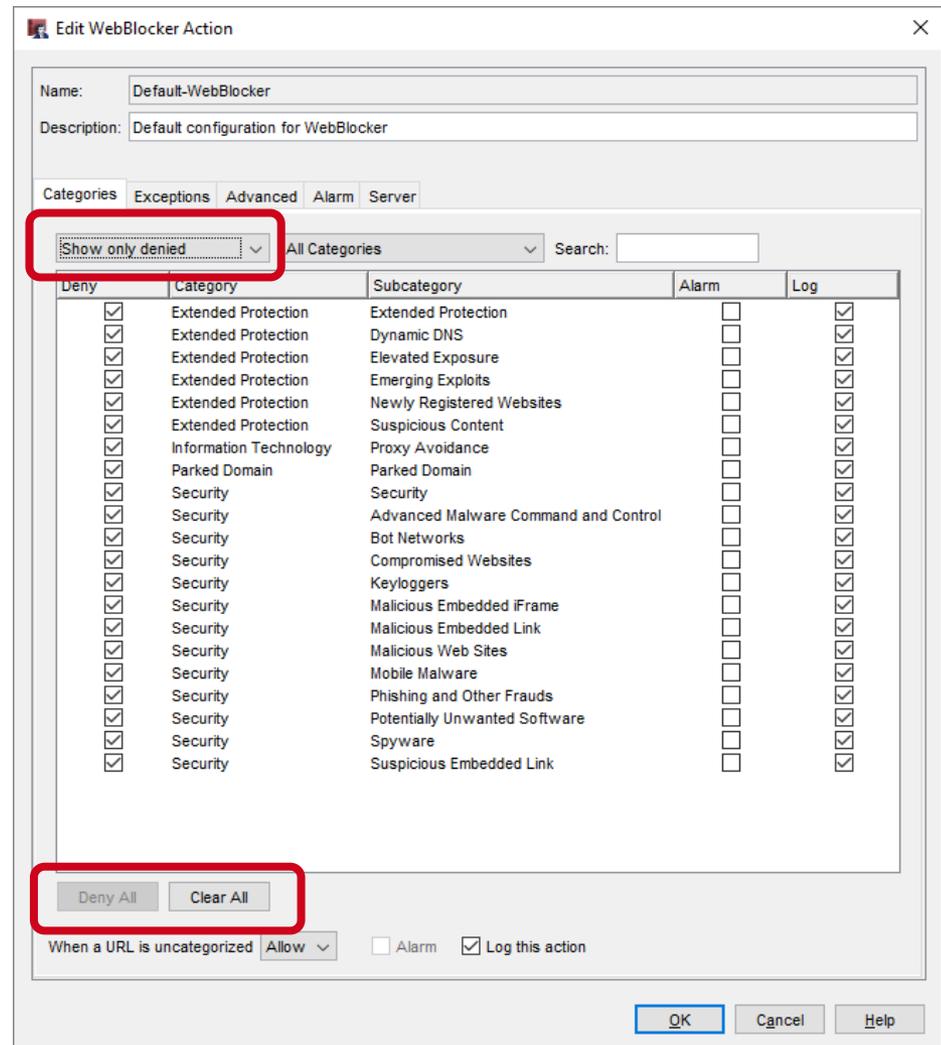
The screenshot shows the WatchGuard Fireware Web UI interface. The top navigation bar includes the WatchGuard logo, the text "Fireware Web UI", and the user "User: admin". The breadcrumb trail is "WebBlocker / WebBlocker_Test". The "Action Name" field is set to "WebBlocker_Test".

The main content area has a tabbed interface with "Categories" selected. Below the tabs, there are dropdown menus for "Show all categories" and "All Categories", and a search field. The table below shows the configuration for various categories, with the "ALARM" and "LOG" columns highlighted by a red box.

DENY	CATEGORY	SUBCATEGORY	ALARM	LOG
<input type="checkbox"/>	Abortion	Abortion	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Abortion	Pro-Choice	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Abortion	Pro-Life	<input type="checkbox"/>	<input checked="" type="checkbox"/>

WebBlocker Usability Enhancements

- WebBlocker action configuration in Policy Manager
- To see a list of denied categories, select the filter **Show only denied**
- To deny all categories in the filtered list, click **Deny All**
- To clear the Deny check box for all categories in the filtered list, click **Clear All**





On-Premises WebBlocker Server

On-Premises WebBlocker Server

- Firewall now supports an on-premises WebBlocker Server with the same set of content categories as Websense cloud (now called WebBlocker cloud)
 - Supports more content categories than the WebBlocker Server previously available for local installation with WSM
 - New UI available in Firewall v12.2 Beta, but feature not yet available

On-Premises WebBlocker Server

- The on-premises WebBlocker Server must be installed as a virtual machine
 - Supported environments:
 - Microsoft Hyper-V System Center VMM 2012 and higher
 - VMware vCenter 5.0 and higher
- The WebBlocker Server previously available in WatchGuard Server Center has been removed

On-Premises WebBlocker Server — Upgrade

- When you upgrade to Fireware v12.2:
 - WebBlocker actions that use a WebBlocker Server with SurfControl are updated to use WebBlocker Cloud
 - Previously configured content categories are automatically converted to equivalent categories in WebBlocker cloud

WebBlocker / WebBlocker_Test Fireware v12.1.1

Action Name

Categories Exceptions Advanced Alarm Servers

Use the Websense cloud for WebBlocker lookups (130 categories)

Use a WebBlocker Server with SurfControl (54 categories)

IP ADDRESS	PORT
10.0.100.80	5003

IP Port

WebBlocker / WebBlocker_Test Fireware v12.2

Action Name

Categories Exceptions Advanced Alarm Server

WebBlocker cloud

On-premises WebBlocker server

To select an on-premises WebBlocker Server, you must first add it in the WebBlocker Global Settings.

On-Premises WebBlocker Server Licensing

- The on-premises WebBlocker Server is licensed as part of a WebBlocker subscription
- To activate an on-premises WebBlocker Server, you must have a Firebox with an active Total Security or WebBlocker subscription
- If the WebBlocker subscription expires, the WebBlocker Server activation also expires

On-Premises WebBlocker Server Setup

- WebBlocker Server installation files:
 - .OVA file for installation on VMWare
 - .VHD file for installation on Hyper-V
- Installation:
 - Use the .OVA or .VHD file to create a virtual machine
 - Connect and run the WebBlocker Server Setup Wizard

On-Premises WebBlocker Server Setup

- To add an on-premises WebBlocker Server to the Firebox configuration, edit WebBlocker Global settings
 - WebBlocker Server Properties:
 - **Display Name** — The server name as it appears in the WebBlocker configuration
 - **Address** — WebBlocker Server host name or IP address
 - **Port** and **TLS** options — Default settings match the defaults for the on-premises WebBlocker Server
 - **Authentication Key** — the Authentication Key on the WebBlocker Server

WebBlocker Global Settings

General Cache

HTTP Proxy Server

Connect to the WebBlocker cloud with an HTTP proxy server

Server address: IP Address . . .

Server port: 8080

Server authentication: None

User name:

User domain:

Password:

On-Premises WebBlocker Servers (Fireware OS v12.2 and higher)

Display Name	Address	Port	Use TLS
local_webblocker	10.0.10.1	443	<input checked="" type="checkbox"/>

Add... Edit... Remove

Add On-Premises Server

Display Name: local_webblocker

Address: 10.0.10.1

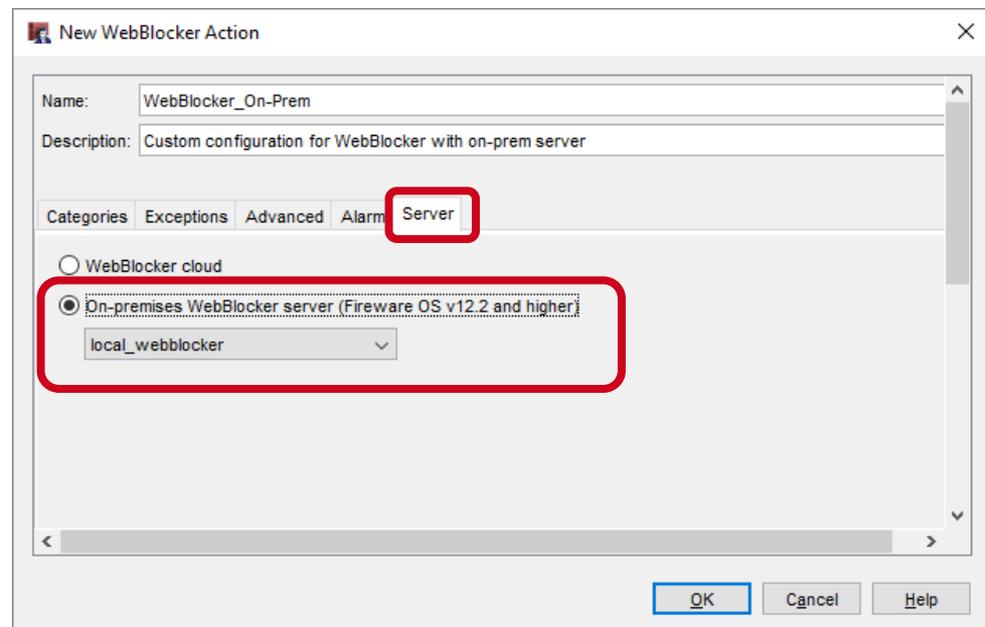
Port: 443 Use TLS

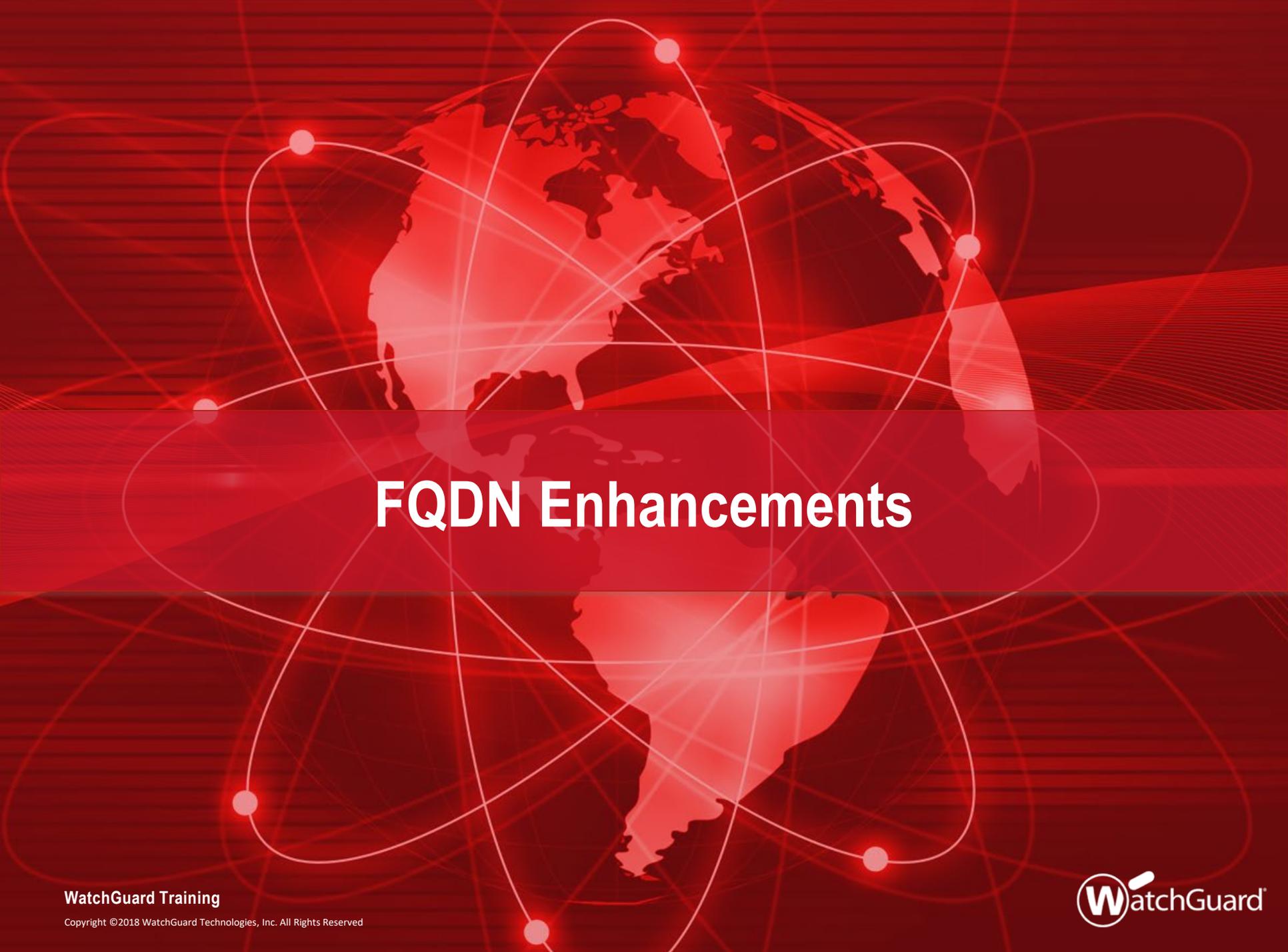
Authentication Key:

OK Cancel

On-Premises WebBlocker Server Setup

- By default, all WebBlocker actions use WebBlocker cloud
- To use an on-premises WebBlocker Server
 - Create or edit a WebBlocker action
 - On the Server tab, select the on-premises WebBlocker Server





FQDN Enhancements

FQDN Improvements

- FQDN support has been extended to provide greater granularity and flexibility
 - You can now use a wildcard FQDN with multi-level subdomains
 - More than one FQDN can now resolve to the same IP address
 - You can use the same FQDN in more than one policy
 - FQDN support for SNAT

FQDN Subdomain Wildcard Support

- Multi-level wildcard subdomain support for FQDNs in policies, aliases, and any feature that supports FQDN input
- Previously only supported 2 levels (*.example.com)
- For example, you can now specify an FQDN as:
 - *.b.example.com
 - *.a.b.example.com

FQDN Wildcard Support

- Overlapping addresses in FQDN wildcards are resolved by policy precedence
- For example, *a.b.example.com* is applicable to all three of these FQDN entries:
 - *.example.com
 - *.b.example.com
 - a.b.example.com
- The policy that is applied is based on the policy precedence order
- If a policy with the FQDN **.example.com* appears first in the policy order, *a.b.example.com* will be applicable to that policy

Multiple FQDN Resolution to One IP Address

- Multiple FQDNs can resolve to the same IP address
 - For example:
 - *.blog.example.com
 - *.example.com
- Previously, Fireware mapped the IP address only to the first FQDN that resolved to it
 - This created limitations because FQDNs can be used in many places in the configuration
 - This becomes a more common issue with wildcard FQDNs
- Now an IP address can be mapped to more than one FQDN
 - The FQDN that appears in traffic log messages depends on policy precedence

FQDN in Multiple Policies

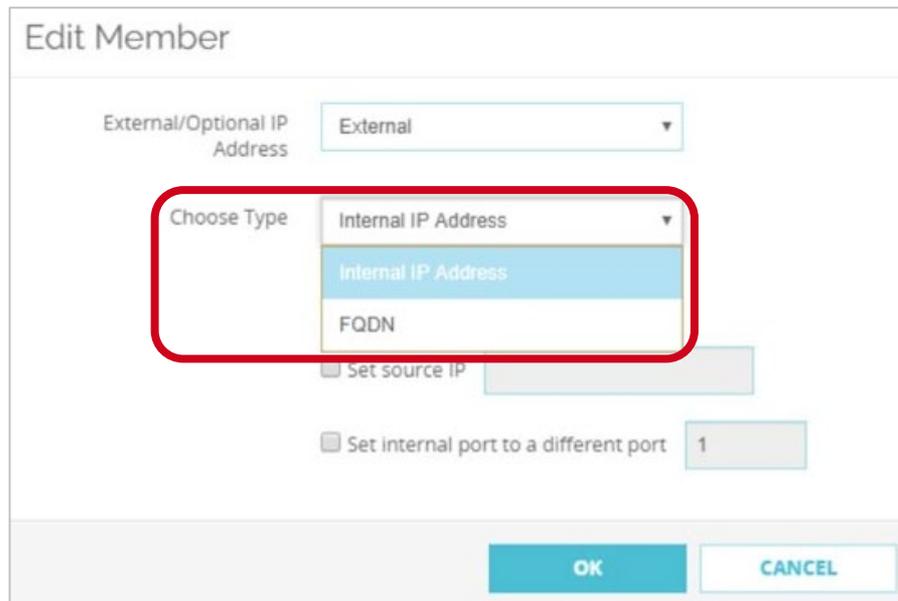
- The same FQDN can be used in more than one policy
- Prevents issues with multiple FQDN matches in different packet level features, such as packet filter policies, blocked sites, and blocked sites exceptions
- Policy order precedence decides the FQDN resolution

FQDN Support for SNAT

- You can now specify an FQDN in a static NAT (SNAT) action to help make policy management easier and to avoid downtime from IP address changes
- For example, if your Firebox is configured to process SMTP traffic from an Office 365 mail server, you can specify an FQDN instead of IP addresses for Office 365
 - If the Office 365 IP addresses change, you no longer need to update the SNAT entry

FQDN Support for SNAT

- When you add or edit a SNAT member, a new drop-down list appears that includes an **FQDN** option:



The screenshot shows the 'Edit Member' dialog box. The 'External/Optional IP Address' dropdown is set to 'External'. The 'Choose Type' dropdown is open, showing three options: 'Internal IP Address' (selected), 'Internal IP Address', and 'FQDN'. The 'FQDN' option is highlighted in blue. Below the dropdown, there are two checkboxes: 'Set source IP' and 'Set internal port to a different port' (set to 1). At the bottom, there are 'OK' and 'CANCEL' buttons.

FQDN Support for SNAT

- Example – Hybrid mail environment with a local mail server and Office 365 in the cloud
 - On the Firebox, configure an SMTP-proxy policy for port 25 traffic from the External interface
 - Add an SNAT entry that specifies an FQDN for the Office 365 mail server



Control Firebox-Generated Traffic

Control Firebox-Generated Traffic

- New enhancements give you control over traffic generated by the Firebox:
 - Enable a global setting to configure policies for Firebox-generated traffic
 - Configure policy-based routing for Firebox-generated traffic
 - Set a different source IP address for Firebox-generated traffic
 - Specify the loopback IP address as the source in dynamic NAT policies

Control Firebox-Generated Traffic

- These enhancements have many uses:
 - You can apply global NAT, per-policy NAT, policy-based routing, traffic management, and QoS to policies for Firebox-generated traffic
- Examples of Firebox-generated traffic:
 - Signature-based cloud services, such as Gateway AntiVirus, Intrusion Prevention Service, Application Control, Data Loss Prevention, Botnet Detection, and Geolocation
 - Tunnels not tied to an interface (SSL management and BOVPN TLS clients)
 - Log traffic from the Firebox to a Dimension server

Control Firebox-Generated Traffic

- To add new policies for Firebox-generated traffic, you must first select the **Enable configuration of policies for traffic generated by the Firebox** global setting

Control Firebox-Generated Traffic

- Web UI

Global Settings

General Networking

Web UI Port

8080

Automatic Reboot

Schedule time for reboot Daily 0 (Hour) 0 (Minute)

Device Feedback

Device feedback helps WatchGuard improve products and features. The feedback that your device sends to WatchGuard includes information about how your device is used, but does not include identifying information about your company or your company data.

Send device feedback to WatchGuard

Fault Report

Fault Reports include data about errors that occur on your device. WatchGuard will use this information to help improve the device OS and hardware.

Send Fault Reports to WatchGuard daily

Device Administrator Connections

Enable more than one Device Administrator to log in at the same time

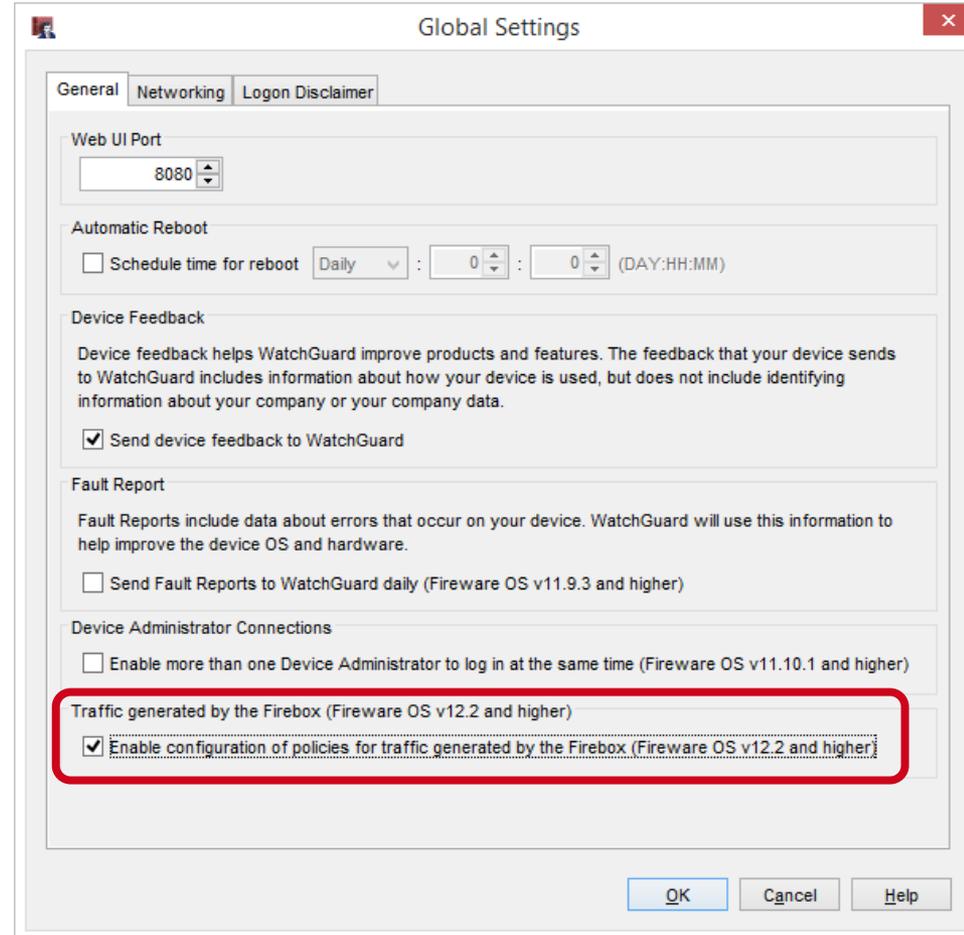
Traffic generated by the Firebox

Enable configuration of policies for traffic generated by the Firebox

SAVE

Control Firebox-Generated Traffic

- Policy Manager



Control Firebox-Generated Traffic

- When the **Enable configuration of policies for traffic generated by the Firebox** check box is selected:
 - The *Any-From-Firebox* policy appears in the list of policies. This policy cannot be modified or removed.
 - You can add new policies that apply to Firebox-generated traffic
 - When the list of policies is configured for auto-order mode, policies that specify Firebox-generated traffic appear before all other policies
 - Policies that you add for Firebox-generated traffic appear before the *Any-From-Firebox* policy because they are more granular

Control Firebox-Generated Traffic

- Web UI

Policies

ACTION ▾ ADD POLICY

Filter None ▾

	ORDE	ACTION	POLICY NAME	TYPE	FROM	TO	PORT	PBR	APP CONTROL	TAGS
<input type="checkbox"/>	1		Any From Firebox	Any	Firebox	Any	Any			

Control Firebox-Generated Traffic

- Policy Manager

untitled.xml *- Fireware Policy Manager

File Edit View Setup Network FireCluster VPN Subscription Services Help

Firewall Mobile VPN with IPSec

Filter: No

Order /	Action	Policy Name	Policy Type	From	To	Port
1	✓	Any From Firebox	Any	Firebox	Any	any
2	✓	FTP	FTP	Any-Trusted, Any-Optional	Any-External	tcp:21
3	✓	WatchGuard Web UI	WG-Fireware-XTM-WebUI	Any-Trusted, Any-Optional	Firebox	tcp:8080
4	✓	Ping	Ping	Any-Trusted, Any-Optional	Any	icmp (type: 8, code: 255)
5	✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-Optional	Firebox	tcp:4105 tcp:4117 tcp:4118
6	✓	Outgoing	TCP-UDP	Any-Trusted, Any-Optional	Any-External	tcp:0 (Any) udp:0 (Any)

Control Firebox-Generated Traffic

- Logging for the *Any-From-Firebox* policy is controlled by the **Enable logging for traffic sent from this device** check box
 - This check box appears in the global logging settings:
 - Web UI — **System > Logging > Settings**
 - Policy Manager — **Setup > Logging > Diagnostic Log Level**
- Logging for policies that you create is controlled in those policies

Control Firebox-Generated Traffic

- Use cases
 - For multi-WAN, you can control which WAN interface is used for Firebox-generated traffic to cloud-based WatchGuard subscription services
 - This helps you prevent subscription services traffic to unintended or expensive interfaces
 - Example: On a connection with limited bandwidth, force WebBlocker traffic to use a specific interface so WebBlocker traffic does not reduce the bandwidth available to VoIP traffic
 - Example: Force traffic from the Firebox to your Log Server to use a specific interface rather than the VPN tunnel

Control Firebox-Generated Traffic

- Use cases
 - For BOVPN virtual interface tunnels configured as zero route, you can create exceptions
 - Example: If the local Firebox requests signature updates, the request is sent through the tunnel. If the remote Firebox does not allow DNS requests, the signature updates fail
 - To avoid this issue, you can force traffic to cloud-based WatchGuard subscription services to use a WAN interface instead of the VPN tunnel
 - You can force traffic that matches local, static, or policy-based routing routes to take precedence over routes specified in your BOVPN configuration

Control Firebox-Generated Traffic

- Use cases
 - Configure the Firebox to use provider-independent IP addresses
 - Example: You have a provider-independent block of IP addresses and multiple ISPs. The external Firebox interface has a public IP address that is not part of the provider-independent IP address block.
 - To use provider-independent addresses for Firebox-generated traffic or traffic that passes through the Firebox, set the source IP address in a DNAT rule to one or more IP addresses from the provider-independent block
 - A provider-independent IP address you specify as the source IP address is not bound to a specific interface

Control Firebox-Generated Traffic

- Use cases
 - Apply Quality of Service (QoS) and traffic management to traffic generated by the Firebox
 - Example: Apply QoS and traffic management to Firebox-generated traffic to make sure emergency calls placed over VoIP are not interrupted



AES-GCM Support

AES-GCM Support

- Firewall now supports AES-GCM for IPSec and SSL/TLS VPN and mobile VPN tunnels
- GCM (Galois/Counter Mode) is an authenticated encryption algorithm known for its security, efficiency, and performance
 - Encryption and data integrity check occur simultaneously
 - Performance increases on Intel-based Fireboxes without hardware crypto support (T55 and T70)
 - Performance increases on FireboxV and Firebox Cloud for any processor models that support AES-NI
- GCM is required by NSA Suite B, a standard specified by the United States government and adopted worldwide for data security

AES-GCM Support

- AES-GCM is supported for these features:
 - BOVPN (IPSec and TLS)
 - BOVPN virtual interfaces
 - Mobile VPN with IKEv2
 - Mobile VPN with SSL
- These options are supported:
 - AES-GCM-128
 - AES-GCM-192
 - AES-GCM-256

AES-GCM Support

- Mobile VPN example — Mobile VPN with SSL

Mobile VPN with SSL

When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" policy are created to allow Mobile VPN with SSL connections from the Internet to the external interface.

Activate Mobile VPN with SSL

General Authentication **Advanced**

Authentication: SHA-256

Encryption: AES (256-bit)

Data channel: 3DES, AES (128-bit), AES (192-bit), AES (256-bit)

Configuration channel (TCP): AES-GCM (128-bit), AES-GCM (192-bit), **AES-GCM (256-bit)**

443

Changes to this port affect Access Portal

AES-GCM Support

- BOVPN example — Phase 1 settings

Branch Office VPN / Add

Gateway Name

General Settings | Phase 1 Settings

Version

NAT Traversal

Keep-alive Interval seconds

Dead Peer Detection (RFC3706)

Type

Traffic idle timeout seconds

Max retries

Transform Settings

PHASE 1 TRANSFORM	KEY GROUP
AES-GCM(256-bit)	Diffie-Hellman Group 14

AES-GCM Support

- BOVPN example — Phase 2 settings

Phase 2 Proposal / Add

Name

Description

Type ESP (Encapsulating Security Payload) ▼

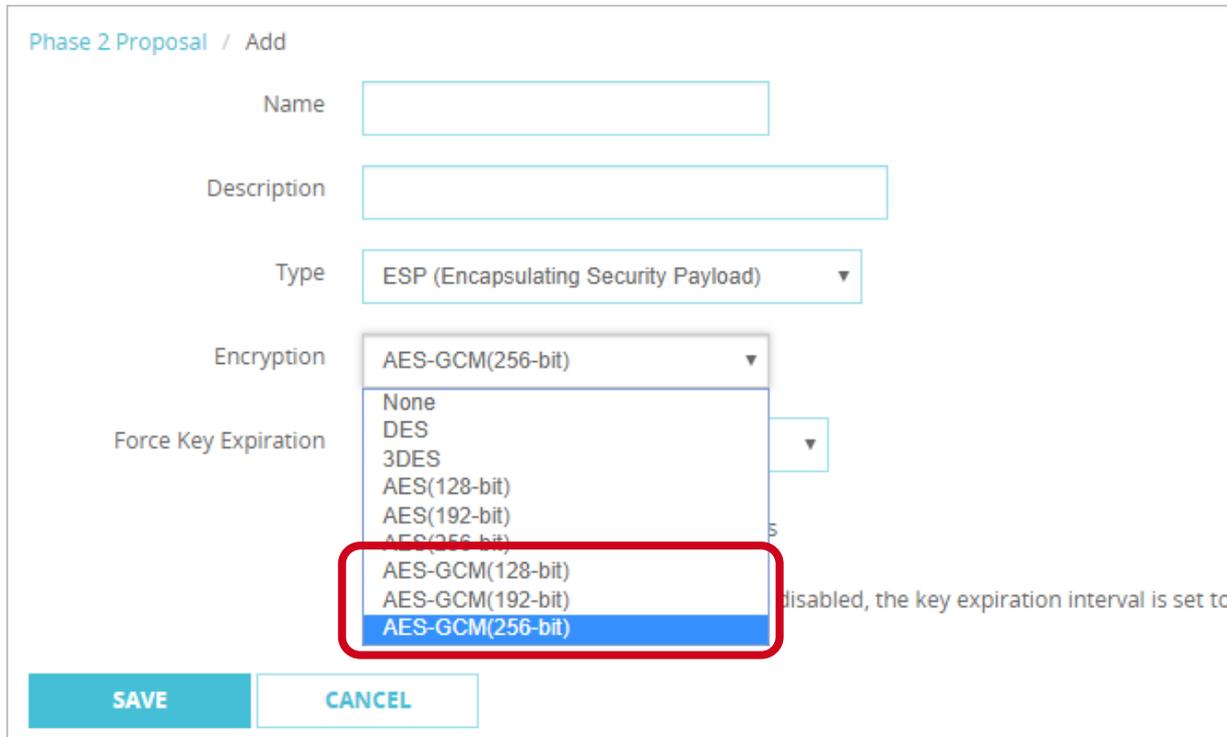
Encryption AES-GCM(256-bit) ▼

Force Key Expiration

None
DES
3DES
AES(128-bit)
AES(192-bit)
AES(256-bit)
AES-GCM(128-bit)
AES-GCM(192-bit)
AES-GCM(256-bit)

disabled, the key expiration interval is set to

SAVE CANCEL

The image shows a configuration window for a Phase 2 Proposal. The 'Encryption' dropdown menu is open, displaying a list of encryption algorithms. The 'AES-GCM(256-bit)' option is highlighted in blue, and a red rectangle is drawn around the entire list of options. The 'Force Key Expiration' field is currently empty. At the bottom of the window, there are 'SAVE' and 'CANCEL' buttons.

AES-GCM Support

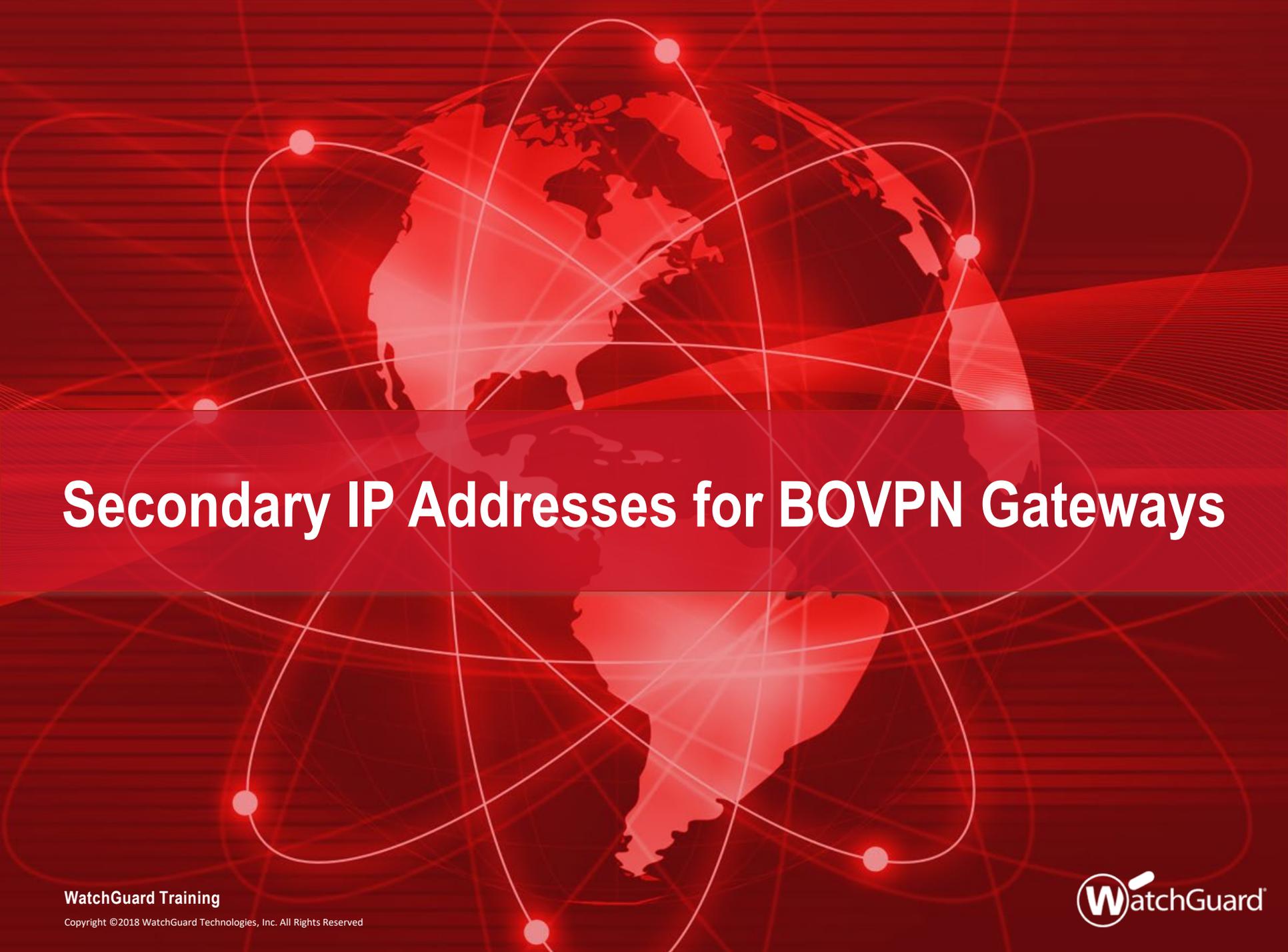
- AES-GCM support details
 - IPSec BOVPN and BOVPN virtual interface configurations:
 - AES-GCM is supported for IKE proposals only when you select IKEv2
 - AES-GCM is supported for IPSec proposals in both IKEv1 and IKEv2
 - Mobile VPN with IKEv2 clients:
 - Windows supports all AES-GCM options, but only for IPSec proposals
 - macOS and iOS support AES-GCM-128 and AES-GCM-256 for IKE and IPSec proposals. AES-GCM-192 is not supported.
 - Android supports all AES-GCM options in for IKE and IPSec proposals

AES-GCM Support

- AES-GCM support details
 - Mobile VPN with SSL
 - Windows and MacOS clients can support all AES-GCM options
 - Mobile SSLVPN servers can support all AES-GCM options
 - BOVPN over TLS
 - Client and Server mode support all AES-GCM options
 - Unsupported features
 - Management tunnels over SSL
 - Mobile VPN with IPSec
 - Mobile VPN with L2TP

AES-GCM Support

- Firewall supports a 16-byte Integrity Check Value (ICV) to verify data integrity
 - 16-byte ICV is required by GCM
 - 8- and 12-byte ICVs are not supported



Secondary IP Addresses for BOVPN Gateways

Secondary IP Addresses for BOVPN Gateways

- To configure BOVPN and BOVPN virtual interface connections in more complex environments, you can now specify a secondary IP address as the local gateway IP address

Secondary IP Addresses for VPN Gateways

- A new drop-down list named **Interface IP Address** now appears in the gateway settings in the BOVPN and BOVPN virtual interface configurations
- To specify a secondary IP address for a BOVPN or BOVPN virtual interface gateway, the interface you select as the **Interface IP Address** must already be configured with a secondary IP address

Secondary IP Addresses for VPN Gateways

- Web UI — BOVPN configuration

Gateway Endpoint Settings

A tunnel needs authentication on each side of the tunnel. Provide the configuration details for the gateway endpoints below.

Local Gateway Remote Gateway Advanced

External Interface External

Interface IP Address Primary Interface IP Address
Primary Interface IP Address
203.0.113.91

Specify the gateway ID for tunnel authentication.

By IP Address

By Domain Name

By User ID on Domain

By x500 Name

OK CANCEL

Secondary IP Addresses for VPN Gateways

- Web UI — BOVPN virtual interface configuration

Gateway Endpoint Settings

A tunnel needs authentication on each side of the tunnel. Provide the configuration details for the gateway endpoints below.

Local Gateway Remote Gateway Advanced

Interface

Physical External

Other SELECT

Interface IP Address Primary Interface IP Address
Primary Interface IP Address
203.0.113.91

Specify the gateway ID for tunnel authentication.

By IP Address

By Domain Name

By User ID on Domain

By x500 Name

OK CANCEL

Secondary IP Addresses for VPN Gateways

- Policy Manager — BOVPN configuration

New Gateway Endpoints Settings - gateway.1

A tunnel needs authentication on each side of the tunnel. Provide the configuration details for the gateway endpoints below.

Local Gateway

External Interface: External

Interface IP Address: Primary Interface IP Address

Specify the gateway: Primary Interface IP Address
203.0.113.91

By IP Address

IP Address: . . .

By Domain Information [Configure...](#)

Remote Gateway

Specify the remote gateway IP address for a tunnel.

Static IP address

IP Address: . . .

Dynamic IP address

Specify the remote gateway ID for tunnel authentication.

By IP Address

IP Address: . . .

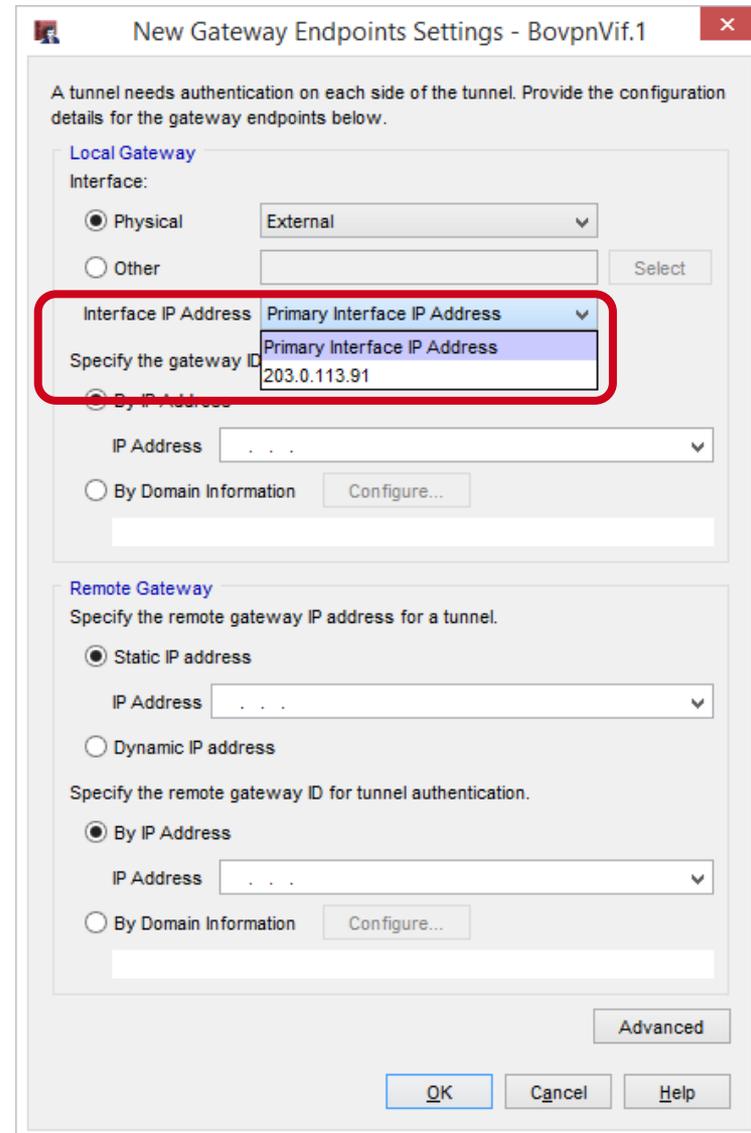
By Domain Information [Configure...](#)

[Advanced](#)

[OK](#) [Cancel](#) [Help](#)

Secondary IP Addresses for VPN Gateways

- Policy Manager — BOVPN virtual interface configuration



New Gateway Endpoints Settings - BovpnVif.1

A tunnel needs authentication on each side of the tunnel. Provide the configuration details for the gateway endpoints below.

Local Gateway

Interface:

Physical External

Other Select

Interface IP Address Primary Interface IP Address

Specify the gateway ID Primary Interface IP Address

By IP Address 203.0.113.91

IP Address . . .

By Domain Information

Remote Gateway

Specify the remote gateway IP address for a tunnel.

Static IP address

IP Address . . .

Dynamic IP address

Specify the remote gateway ID for tunnel authentication.

By IP Address

IP Address . . .

By Domain Information

Advanced

OK Cancel Help



Mobile VPN with SSL and Access Portal Settings

Mobile VPN with SSL & Access Portal

- In Fireware v12.1, the VPN Portal was added to consolidate settings shared by Mobile VPN with SSL and the Access Portal
 - This configuration created challenges and generated customer feedback
- For a better user experience, in Fireware v12.2:
 - The VPN Portal configuration page is removed
 - Settings that appeared on the VPN Portal page now appear in the Mobile VPN with SSL and Access Portal configurations
 - VPN Portal Port is now named Access Portal Port
 - The WG-VPN-Portal alias is removed

Mobile VPN with SSL & Access Portal

- Mobile VPN with SSL and the Access Portal continue to share these settings:
 - Authentication servers
 - Configuration Channel (known as the Access Portal Port in the Access Portal configuration)
- SSL/TLS settings precedence remains unchanged for Firebox features that share the same OpenVPN server
 - For information about settings precedence for Firebox features that share the same OpenVPN server, see *Fireware Help*

Mobile VPN with SSL & Access Portal

- Mobile VPN with SSL
 - Firebox settings for Mobile VPN with SSL now appear as they did before Fireware v12.1
 - On the **Authentication** tab, the **Authentication Server** list now appears
 - On the **Advanced** tab, the **Configuration Channel** text box now appears
 - These items were removed:
 - On **Authentication** tab, information about VPN Portal interfaces and authentication servers
 - A link to the **VPN Portal** page

Mobile VPN with SSL & Access Portal

- Web UI — Authentication Server Settings list

Mobile VPN with SSL

When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" policy are created to allow Mobile VPN with SSL connections from the Internet to the external interface.

Activate Mobile VPN with SSL

General Authentication Advanced

Authentication Server Settings

Specify the authentication servers to use for connections to Mobile SSL with VPN. The first authentication server in the list is the default server.

AUTHENTICATION SERVER	
Firebox-DB (default)	
example.com	
Firebox-DB ▼	ADD REMOVE
	MOVE UP MOVE DOWN

Note: These authentication servers are also used by the Access Portal. Changes to this list effect Access Portal.

Mobile VPN with SSL & Access Portal

- Web UI — **Configuration Channel** text box

Activate Mobile VPN with SSL

General	Authentication	Advanced
Authentication	SHA-256	
Encryption	AES (256-bit)	
Data channel	UDP	447
Configuration channel (TCP)	443	
This port is also the Access Portal port. Changes to this port effect Access Portal.		
Keep-Alive Interval	10	seconds
Keep-Alive Timeout	60	seconds
Renegotiate Data Channel	480	minutes

Mobile VPN with SSL & Access Portal

- Policy Manager — Authentication Server Settings list

Mobile VPN with SSL Configuration

When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" policy are created to allow Mobile VPN with SSL connections from the Internet to the external interface.

Activate Mobile VPN with SSL

General Authentication **Advanced**

Authentication Server Settings

Select one or more authentication servers. The first server in the list is the default authentication server. To configure additional authentication servers, click **Configure**.

Select	Authentication Server	Configure...
<input checked="" type="checkbox"/>	Firebox-DB (Default)	Make Default

Auto reconnect after a connection is lost

Force users to authenticate after a connection is lost

Allow the Mobile VPN with SSL client to remember password
(Fireware OS v11.8 and higher)

Define users and groups to authenticate with Mobile VPN with SSL. The users and groups you define are automatically included in the "SSLVPN-Users" group.

Name	Type	Authentication Server	Remove
SSLVPN-Users	Group	Any	

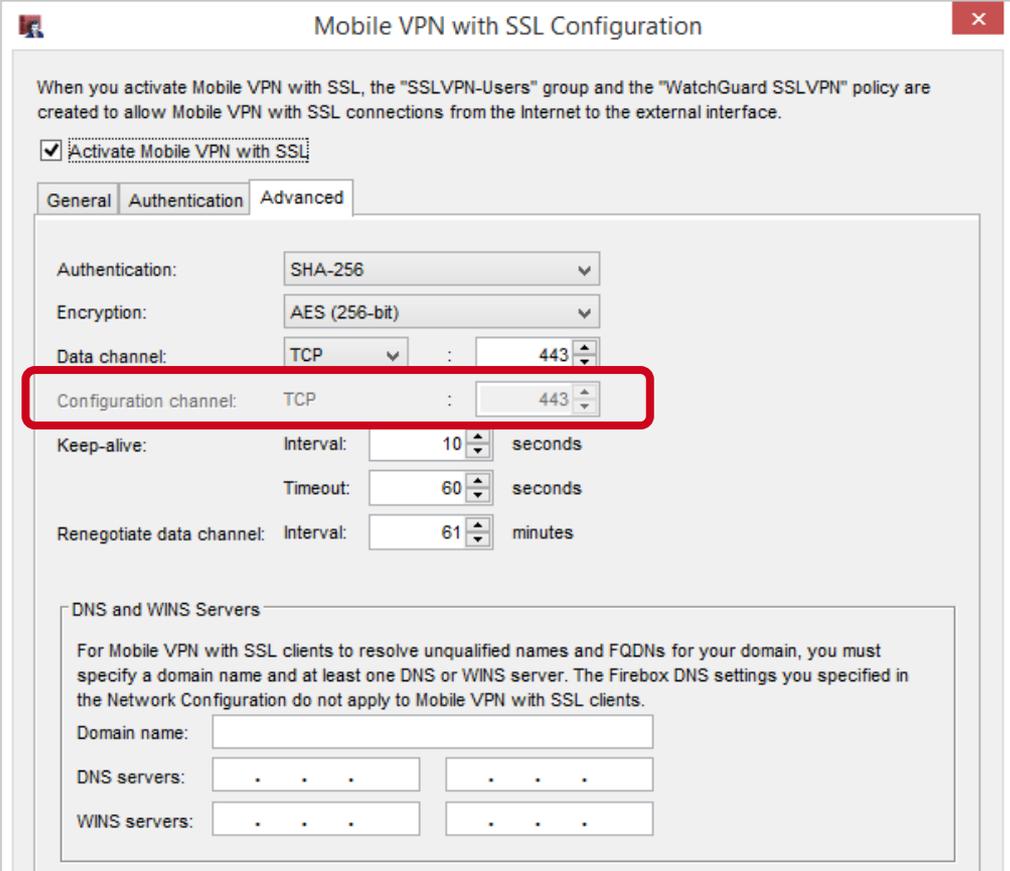
Type: Group User

Name:

Authentication Server:

Mobile VPN with SSL & Access Portal

- Policy Manager — **Configuration Channel** text box



Mobile VPN with SSL Configuration

When you activate Mobile VPN with SSL, the "SSLVPN-Users" group and the "WatchGuard SSLVPN" policy are created to allow Mobile VPN with SSL connections from the Internet to the external interface.

Activate Mobile VPN with SSL

General Authentication Advanced

Authentication: SHA-256

Encryption: AES (256-bit)

Data channel: TCP : 443

Configuration channel: TCP : 443

Keep-alive: Interval: 10 seconds
Timeout: 60 seconds

Renegotiate data channel: Interval: 61 minutes

DNS and WINS Servers

For Mobile VPN with SSL clients to resolve unqualified names and FQDNs for your domain, you must specify a domain name and at least one DNS or WINS server. The Firebox DNS settings you specified in the Network Configuration do not apply to Mobile VPN with SSL clients.

Domain name:

DNS servers:

WINS servers:

Mobile VPN with SSL & Access Portal

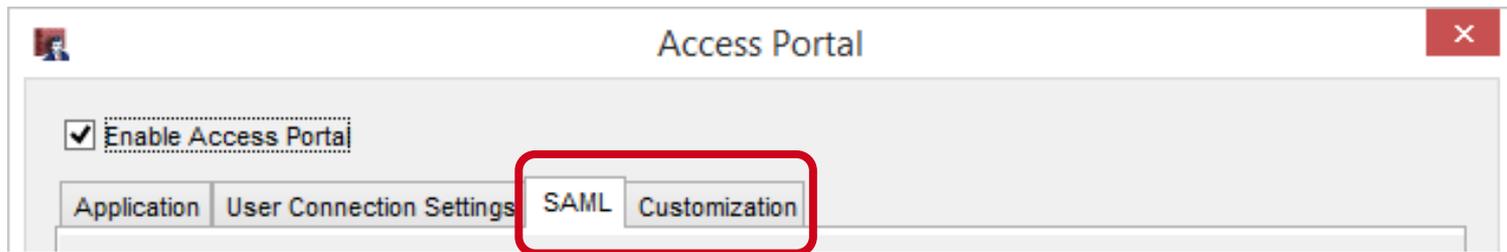
- Access Portal configuration
 - **SAML** and **Customization** tabs
 - These settings now appear on the **User Connection Settings** page:
 - **Authentication Servers**
 - **Access Portal Port**
 - **Timeouts**
 - **VPN Portal Port** is now named **Access Portal Port**
 - These items were removed from **User Connection Settings** page:
 - Information about VPN Portal interfaces and authentication servers
 - A link to the **VPN Portal** page

Mobile VPN with SSL & Access Portal

- Web UI — **SAML** and **Customization** tabs



- Policy Manager — **SAML** and **Customization** tabs



Mobile VPN with SSL & Access Portal

- Web UI — **Authentication Servers, Access Portal Port, and Timeouts** settings

Authentication Servers

Specify the authentication servers to use for connections to the Access Portal. The first authentication server in the list is the default server.

AUTHENTICATION SERVER
Firebox-DB (default) example.com

Firebox-DB ▼ [ADD](#) [REMOVE](#) [MOVE UP](#) [MOVE DOWN](#)

Note: These authentication servers are also used by the Access Portal. Any changes to this list will effect Access Portal.

Access Portal Port

Specify the Access Portal Port. This is the configuration port shared by Mobile SSL VPN Clients and users of the Access Portal.

Access Portal Port

Timeouts

Session Timeout hours

Idle Timeout minutes

Mobile VPN with SSL & Access Portal

- Policy Manager — **Authentication Servers, Access Portal Port, and Timeouts** settings

Access Portal

Enable Access Portal

Application | User Connection Settings | SAML | Customization

Users Access

All applications are available to all users and groups authenticated with the Access Portal

Specify the applications available to each user and group

Name	Type	Authentication Se...	Applications
test	User	Firebox-DB	Applications
User1	User	Firebox-DB	Applications

Authentication Servers

Specify the authentication servers to use for connections to the Access Portal. The first authentication server in the list is the default server.

Authentication Server: Firebox-DB (Default) example.com

Firebox-DB Add

Access Portal Port

Specify the Access Portal Port. This is the configuration port shared by Mobile SSL VPN Clients and users of the Access Portal.

Access Portal Port: 443

Timeouts

Session Timeout: 4 hours

Idle Timeout: 15 minutes

Mobile VPN with SSL & Access Portal

- Alias change
 - If the *WG-VPN-Portal* alias appears in your configuration, when you upgrade to v12.2, this alias is removed from the *WatchGuard SSLVPN* policy
 - Interfaces that appeared in the *WG-VPN-Portal* alias appear in the *WatchGuard SSLVPN* policy, which means the policy will match the same traffic
 - To add or remove interfaces for Mobile VPN with SSL or the Access Portal, edit the *WatchGuard SSLVPN* policy
 - The default interface in the From field of the *WatchGuard SSLVPN* policy is **Any-External**

Mobile VPN with SSL & Access Portal

- Known issue
 - If you use WSM v12.2 or higher to manage a Firebox with Fireware v12.1 or v12.1.1, and you enable the Access Portal in WSM:
 - Inaccurate interface information appears in the Web UI
 - Changes you make to VPN Portal interfaces are not applied to the WatchGuard SSLVPN policy
 - To avoid this issue, we recommend that you upgrade your Firebox to Fireware v12.2 if you use Mobile VPN with SSL or the Access Portal
 - You cannot upgrade XTM devices to Fireware v12.2. These devices are not supported with this release.



Redundant Single Sign-On

Redundant Single Sign-On

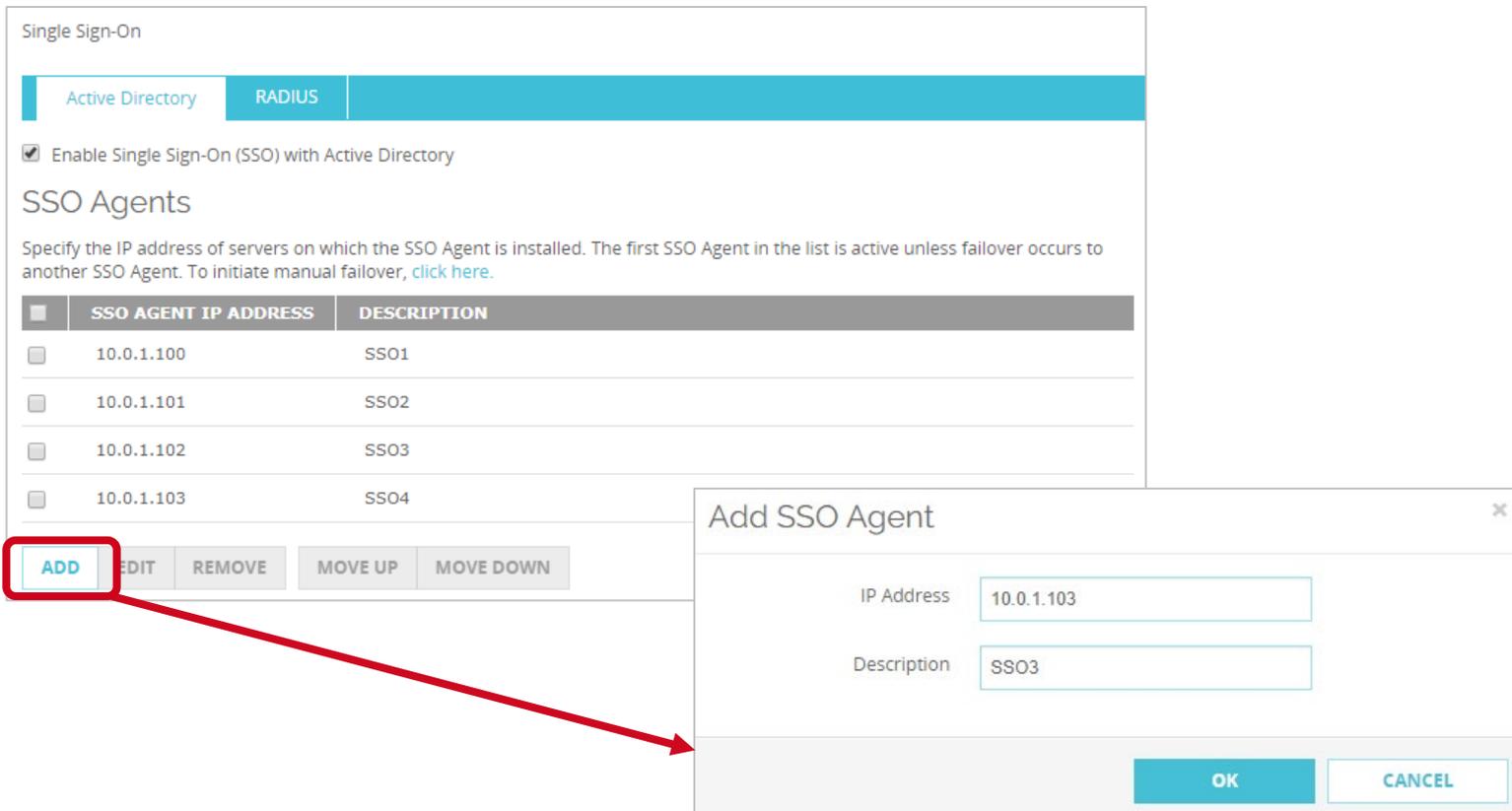
- To eliminate a single point of failure for Single Sign-On (SSO), you can now configure more than one SSO agent
- For example, you can install an SSO agent on a secondary domain controller so users can continue to authenticate if you must reboot the primary domain controller

Redundant Single Sign-On

- You can configure up to four SSO agents in your Firebox configuration
- If an SSO agent becomes unavailable, failover to the next SSO agent in the list automatically occurs
 - You can also manually fail over to an agent you specify

Redundant Single Sign-On

- Web UI — Add an SSO agent



Single Sign-On

Active Directory RADIUS

Enable Single Sign-On (SSO) with Active Directory

SSO Agents

Specify the IP address of servers on which the SSO Agent is installed. The first SSO Agent in the list is active unless failover occurs to another SSO Agent. To initiate manual failover, [click here](#).

<input type="checkbox"/>	SSO AGENT IP ADDRESS	DESCRIPTION
<input type="checkbox"/>	10.0.1.100	SS01
<input type="checkbox"/>	10.0.1.101	SS02
<input type="checkbox"/>	10.0.1.102	SS03
<input type="checkbox"/>	10.0.1.103	SS04

ADD EDIT REMOVE MOVE UP MOVE DOWN

Add SSO Agent

IP Address: 10.0.1.103

Description: SS03

OK CANCEL

Redundant Single Sign-On

- Policy Manager — Add an SSO agent

The image shows two overlapping windows from a management console. The background window is titled "Single Sign-On" and has tabs for "Active Directory" and "RADIUS". The "RADIUS" tab is active, and the "Enable Single Sign-On (SSO) with Active Directory" checkbox is checked. Below this is the "SSO Agents" section, which includes a table of agents and a list of control buttons. The "Add..." button is highlighted with a red box, and a red arrow points from it to a smaller dialog box in the foreground titled "Add SSO agent IP".

Single Sign-On - SSO Agents Table

SSO Agent IP Address	Description
10.0.1.100	SS01
10.0.1.101	SS02
10.0.1.102	SS03
10.0.1.103	SS04

Add SSO agent IP Dialog

Choose Type: Host IPv4
Value: 10.0.1.103
Description: SS03

Buttons: OK, Cancel

Redundant Single Sign-On

- You can now configure keep-alive timers for SSO agent connections
- The **Keep-Alive Interval** specifies how often the Firebox tries to contact the SSO agent to determine whether the agent is available
 - This value must be between 1 and 120 seconds
- The **Keep-Alive Timeout** specifies how long the Firebox waits for a response from the SSO agent before the Firebox tries to connect to the next available SSO agent
 - This value must be between 10 and 1200 seconds, and it must be at least twice as long as the **Keep-Alive Interval**

Redundant Single Sign-On

- Configure the keep-alive timers in the Web UI and Policy Manager

Settings

Keep-Alive Interval	<input type="text" value="10"/>	seconds
Keep-Alive Timeout	<input type="text" value="60"/>	seconds

Settings

Keep-Alive Interval (Fireware OS v12.2 and higher)	<input type="text" value="10"/>	<input type="button" value="▲"/>	<input type="button" value="▼"/>	seconds
Keep-Alive Timeout (Fireware OS v12.2 and higher)	<input type="text" value="60"/>	<input type="button" value="▲"/>	<input type="button" value="▼"/>	seconds

Redundant Single Sign-On

- Failover to a different SSO agent occurs automatically when:
 - The connection to an SSO agent is lost or closed
 - The SSO agent does not respond to keep-alive messages in the specified amount of time
 - You remove the SSO agent from the Firebox configuration
 - You manually initiate a failover to a different SSO agent
- Failover occurs sequentially:
 - If the first SSO agent in the list that is active and becomes unavailable, failover occurs to the second SSO agent in the list
 - If the last SSO agent in the list is active and becomes unavailable, failover occurs to the first SSO agent in the list

Redundant Single Sign-On

- Failback does not occur
 - For example, if the first agent in the list becomes unavailable, failover occurs to the second agent in the list
 - If the first agent becomes available again, the second agent remains the active agent. Failback does not occur to the first agent.

Redundant Single Sign-On

- You can move SSO agents up and down in the list

The image shows two screenshots of the Single Sign-On configuration interface. The left screenshot shows the main configuration page with the 'RADIUS' tab selected. The 'SSO Agents' section contains a table with four entries: SS01 (10.0.1.100), SS02 (10.0.1.101), SS03 (10.0.1.102), and SS04 (10.0.1.103). Below the table are buttons for 'ADD', 'EDIT', 'REMOVE', 'MOVE UP', and 'MOVE DOWN'. The 'MOVE UP' and 'MOVE DOWN' buttons are highlighted with a red box. The right screenshot is a modal dialog titled 'Single Sign-On' with the 'RADIUS' tab selected. It contains the same 'SSO Agents' section, but the 'MOVE UP' and 'MOVE DOWN' buttons are also highlighted with a red box. The modal dialog also includes an 'Add...' button, an 'Edit...' button, and a 'Remove' button. At the bottom of the modal, there is an information icon and text: 'To configure multiple SSO Agents on your network, SSO Agents and Event Log Monitor must be v12.2 or higher.'

Single Sign-On

Active Directory RADIUS

Enable Single Sign-On (SSO) with Active Directory

SSO Agents

Specify the IP address of servers on which the SSO Agent is installed. The first SSO Agent in the list is active unless failover occurs to another SSO Agent. To initiate manual failover, [click here](#).

SSO AGENT IP ADDRESS	DESCRIPTION
<input type="checkbox"/> 10.0.1.100	SS01
<input type="checkbox"/> 10.0.1.101	SS02
<input type="checkbox"/> 10.0.1.102	SS03
<input type="checkbox"/> 10.0.1.103	SS04

ADD EDIT REMOVE MOVE UP MOVE DOWN

Single Sign-On

Active Directory RADIUS

Enable Single Sign-On (SSO) with Active Directory

SSO Agents

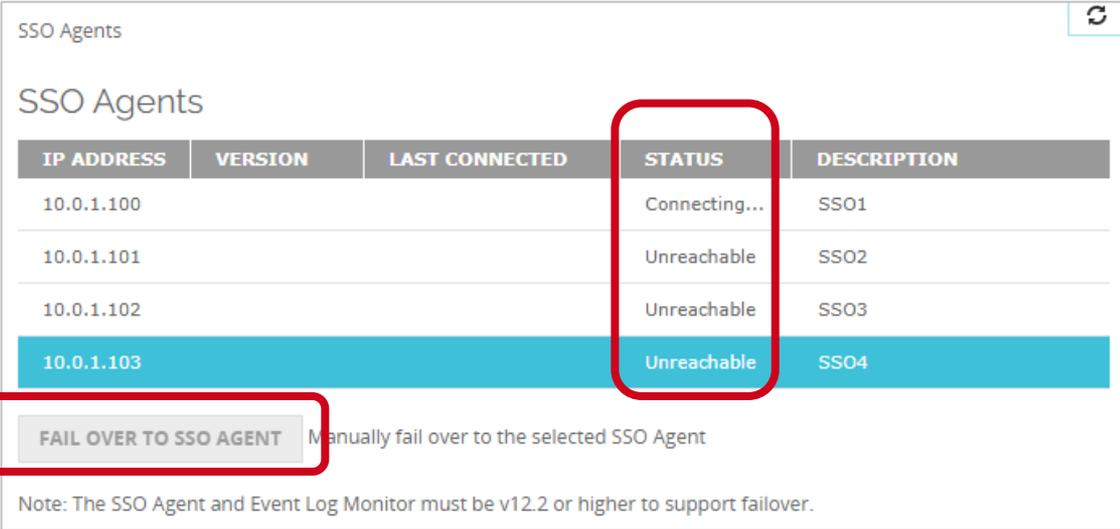
Specify the IP address of servers on which the SSO Agent is installed. The first SSO Agent in the list is active unless failover occurs to another SSO Agent. To initiate manual failover, open Firebox System Manager and select Tools > SSO Agents.

SSO Agent IP Address	Description	Add...
10.0.1.100	SS01	Edit...
10.0.1.101	SS02	Remove
10.0.1.102	SS03	Up
10.0.1.103	SS04	Down

To configure multiple SSO Agents on your network, SSO Agents and Event Log Monitor must be v12.2 or higher.

Redundant Single Sign-On

- To view the status of SSO agents or to manually fail over to an agent that you specify:
 - Web UI — select **System Status > SSO Agents**



The screenshot displays the 'SSO Agents' web interface. It features a table with the following columns: IP ADDRESS, VERSION, LAST CONNECTED, STATUS, and DESCRIPTION. The table lists four agents: SS01 (10.0.1.100, Connecting...), SS02 (10.0.1.101, Unreachable), SS03 (10.0.1.102, Unreachable), and SS04 (10.0.1.103, Unreachable). The SS04 row is highlighted in blue. Below the table is a button labeled 'FAIL OVER TO SSO AGENT' with a tooltip that reads 'Manually fail over to the selected SSO Agent'. A note at the bottom states: 'Note: The SSO Agent and Event Log Monitor must be v12.2 or higher to support failover.' Red boxes highlight the 'STATUS' column and the 'FAIL OVER TO SSO AGENT' button.

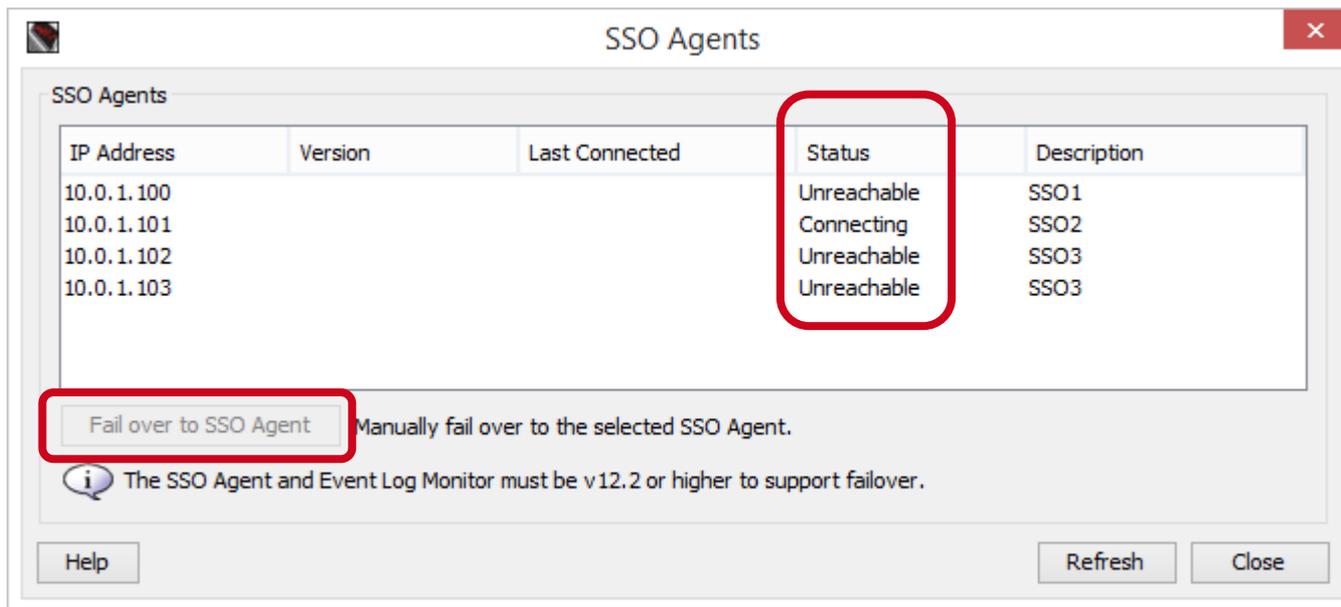
IP ADDRESS	VERSION	LAST CONNECTED	STATUS	DESCRIPTION
10.0.1.100			Connecting...	SS01
10.0.1.101			Unreachable	SS02
10.0.1.102			Unreachable	SS03
10.0.1.103			Unreachable	SS04

FAIL OVER TO SSO AGENT Manually fail over to the selected SSO Agent

Note: The SSO Agent and Event Log Monitor must be v12.2 or higher to support failover.

Redundant Single Sign-On

- To view the status of SSO agents or to manually fail over to an agent that you specify:
 - Firebox System Manager — select **Tools > SSO Agents**



Redundant Single Sign-On

- SSO agents can have these status indicators:
 - **Connecting** — Firebox is trying to connect to the agent
 - **Connected** — Agent is currently active
 - **Standby** — Agent is available, but it is not the currently active agent
 - **Unreachable** — Firebox cannot communicate with the agent
 - **Incompatible** — Agent with a Fireware OS version that does not support redundant SSO

Certificate Management Enhancements

Certificate Management Enhancements

- This release includes several enhancements to certificate management on a Firebox:
 - Improved certificate management
 - Improvements to the certificate list and certificate detail views
 - Ability to define a certificate display name
 - Improvements to the certificate import process
 - Ability to select and use separate certificates for content inspection for an inbound HTTPS proxy

Certificate Management Enhancements

- Drop-down list shows certificate types
- New column for **Import Date**
 - Indicates the file timestamp for non-proxy server certificates
 - Not visible for pending CSRs or items that cannot be exported

Certificates

[IMPORT CERTIFICATE](#)
[IMPORT CRL](#)
[CREATE CSR](#)

STATUS ↑	IMPORT DATE	TYPE	ALGORITHM	SUBJECT
Signed	N/A	Web Server	RSA	o=WatchGuard ou=Fireware cn=ikezmuvpn Server
Signed	2015-10-28 21:44	Web Client	RSA	o=WatchGuard ou=Fireware cn=Fireware web Client
Signed*	2015-10-28 21:44	CA Cert	RSA	o=WatchGuard ou=Fireware cn=Fireware web CA
Signed	2015-10-28 21:43	Web Server	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fireware SSLVPN Server
Signed	2015-10-28 21:43	Web Client	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fireware SSLVPN Client
Signed	2015-10-28 21:43	CA Cert	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fireware SSLVPN (SN 80DB02D9CFB66 2015-10-29 01:43:52 GMT) CA
Signed	2017-12-07 19:47	Web Client	RSA	o=WatchGuard ou=Fireware cn=Fireware saml Client
Signed	2015-10-28 21:43	Proxy Server (Default)	RSA	o=WatchGuard_Technologies ou=Fireware cn=https.proxy.nul
	2015-10-	Proxy		o=WatchGuard_Technologies ou=Fireware

All
 Proxy
 Web
 Trusted CA
 CA Cert

Improved Certificate Management

- A new **Display Name** column is available when you view a Proxy category
- The default display name is comprised of the certificate's Common Name and the internal filename
- If another certificate has the same default display name, a number is appended to the name

Certificates

[IMPORT CERTIFICATE](#)
[IMPORT CRL](#)
[CREATE CSR](#)
Proxy

STATUS	IMPORT DATE	TYPE	ALGORITHM	DISPLAY NAME	SUBJECT NAME
Signed	2015-10-28 21:43	Proxy Server (Default)	RSA	Default	o=WatchGuard_Technologies cn=https.proxy.nul
Signed	2015-10-28 21:43	Proxy Authority	RSA	Fireware HTTPS Proxy (SN 80DB02D91 2015-10-29 01:43:56 GMT) CA (selfsigned)	o=WatchGuard_Technologies cn=Fireware HTTPS Proxy (S 80DB02D9CFB66 2015-10-29 CA

[DETAILS](#)
[REMOVE](#)
[EXPORT](#)
* Currently active Firebox web server certificate

Improved Certificate Management

- Certificate details page now includes the **Import Date** and the **Display Name**
- You can edit the display name for Proxy certificates only

Certificates

Certificate Display Name

svr101.rjtest.com (server-2) [UPDATE](#)

Certificate Details

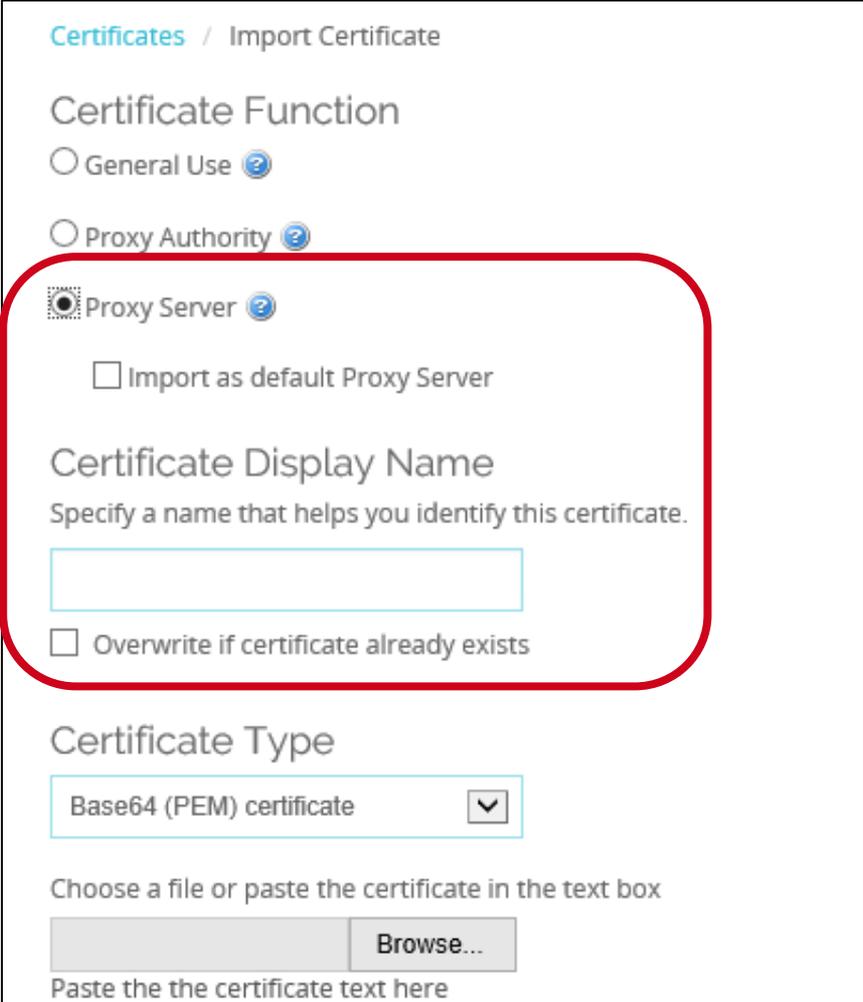
FIELD ↕	VALUE
Subject name	c=US st=Washington l=Seattle o=test ou=engtest cn=svr101.rjtest.com
Subject alt name	
Display name	svr101.rjtest.com (server-2)
Imported/Created	Wed Apr 04 2018 13:51:09 GMT-0700 (PDT)
Issuer	c=US st=Washington l=Seattle o=Watchguard_Technologies ou=Fireware cn=Reinier's certificate authority test
Valid from	Feb 14 17:20:00 2018 GMT

Certificate Import Enhancements

- Provides more information on certificate import requirements, correct import order, and troubleshooting import errors
- Validation of certificate import success
- Improved error messages when the certificate fails to import:
 - Mismatch between private key and certificate
 - Lack of root certificate
 - Incorrect certificate format or type
 - Wrong order of certificate import
 - Certificate has been revoked
 - Incorrect PFX file password
 - Certificate already exists

Certificate Import Enhancements

- New check box to import a certificate as the default Proxy Server certificate
- By default, certificates are imported as a non-default Proxy Server certificate and do not overwrite any existing certificates



Certificates / Import Certificate

Certificate Function

General Use ?

Proxy Authority ?

Proxy Server ?

Import as default Proxy Server

Certificate Display Name

Specify a name that helps you identify this certificate.

Overwrite if certificate already exists

Certificate Type

Base64 (PEM) certificate ▼

Choose a file or paste the certificate in the text box

Browse...

Paste the the certificate text here

Certificate Import Enhancements

- **Certificate Display Name and Overwrite if certificate already exists** check box
 - Only visible when you import a Proxy Server certificate
 - Select **Overwrite** if the certificate to import will overwrite a certificate with the same display name
 - If **Overwrite** is not selected, you cannot import a certificate with the same display name as an existing certificate

Multiple Certificate Support for HTTPS Proxy

- You can now select and use separate certificates for content inspection for an inbound HTTPS proxy
- The ability to use separate certificates for content inspection enables organizations to host several different public-facing web servers and applications behind one Firebox
- Different applications can use different certificates for inbound HTTPS traffic

Multiple Certificate Support for HTTPS Proxy

- Certificates are assigned to inbound HTTPS proxy domain name rules
- When you edit domain name rules, you can use a new **Certificate** drop-down list when the action is **Inspect**

Domain Names

Control access to protected servers based on Server Name Indication (SNI) in the incoming TLS client hello, if SNI is present. To enable content inspection, use the **Inspect** action. To bypass content inspection, use the **Allow** action.

ENABLE	ACTION	NAME	MATCH TYPE	VALUE	PROXY ACTION	CERTIFICATE	ROUTING ACTION	PORT	ALARM	LOG
<input checked="" type="checkbox"/>	Inspect	svr100.rjtest.com	Pattern Match	svr100.rjtest.com	HTTP-Server.Standard	svr100.rjtest.com (server-1)	Policy Default	Policy Default	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Inspect	svr101.rjtest.com	Pattern Match	svr101.rjtest.com	HTTP-Server.Standard	svr101.rjtest.com (server-2)	Policy Default	Policy Default	<input type="checkbox"/>	<input checked="" type="checkbox"/>

ADD CLONE EDIT REMOVE MOVE UP MOVE DOWN

Action to take if no rule above is matched

Action Alarm Log

Proxy Action or Content Action

Certificate

Routing Action Use Policy Default Use

Port Use Policy Default Use



Gateway Wireless Controller Enhancements

Gateway Wireless Controller Enhancements

- You can now specify an RSSI value for the Band Steering feature
 - Previously not configurable and hard coded to -75 dBm
- Client RSSI must be equal to or above this threshold to be steered to the 5 GHz band.
- Clients with weak signal strength cannot operate effectively in the 5 GHz band and should not be steered even if they are capable of operating in 5 GHz

Gateway Wireless Controller / SSID

Network Name (SSID) WatchGuard

Settings Security Access Points

Broadcast SSID

Enable client isolation

Use the MAC Access Control list defined in the Gateway Wireless Controller Settings

Denied MAC Addresses

Enable VLAN tagging

VLAN ID

Automatically deploy this SSID to all unpaired WatchGuard Access Points

Mitigate WPA/WPA2 key reinstallation vulnerability in clients
This function only available for supported devices.

Min Association RSSI

Smart Steering

Band Steering

Band Steering RSSI (dBm) -75

AP125 Support

- Added support for the upcoming AP125
- Indoor, dual radio 2x2:2 MU-MIMO 802.11ac Wave 2 access point for low to medium density deployments

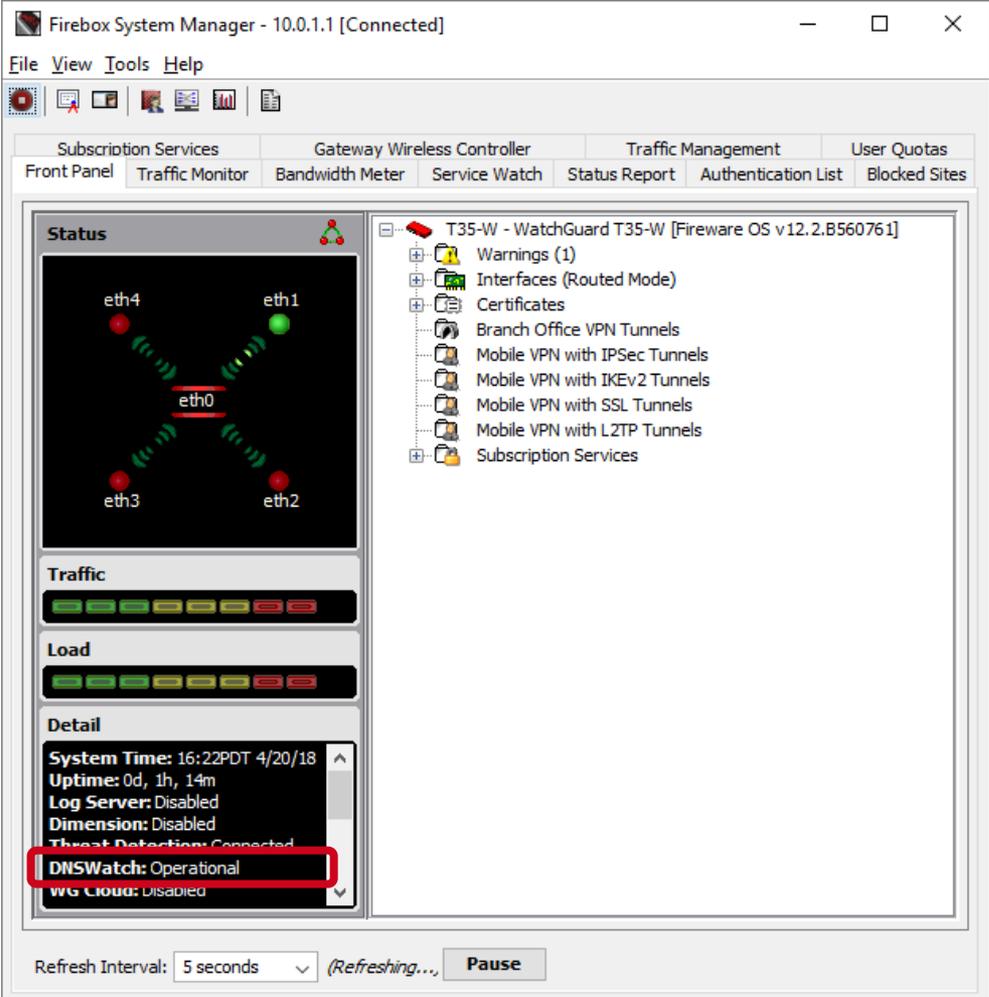




Other Enhancements

DNSWatch Status in FSM Front Panel

- In Firebox System Manager, DNSWatch status now appears in the Front Panel tab



The screenshot displays the Firebox System Manager interface for a WatchGuard T35-W device. The 'Front Panel' tab is active, showing a network diagram with interfaces eth0, eth1, eth2, eth3, and eth4. Below the diagram are sections for Traffic, Load, and Detail. The Detail section shows system information and a red box highlighting 'DNSWatch: Operational'. The right sidebar shows a tree view of system components.

Firebox System Manager - 10.0.1.1 [Connected]

File View Tools Help

Subscription Services Gateway Wireless Controller Traffic Management User Quotas
Front Panel Traffic Monitor Bandwidth Meter Service Watch Status Report Authentication List Blocked Sites

Status

eth4 eth1
eth0
eth3 eth2

Traffic

Load

Detail

System Time: 16:22PDT 4/20/18
Uptime: 0d, 1h, 14m
Log Server: Disabled
Dimension: Disabled
Threat Detection: Connected
DNSWatch: Operational
WG Cloud: Disabled

T35-W - WatchGuard T35-W [Fireware OS v12.2.B560761]

- Warnings (1)
- Interfaces (Routed Mode)
- Certificates
- Branch Office VPN Tunnels
- Mobile VPN with IPsec Tunnels
- Mobile VPN with IKEv2 Tunnels
- Mobile VPN with SSL Tunnels
- Mobile VPN with L2TP Tunnels
- Subscription Services

Refresh Interval: 5 seconds (Refreshing...) Pause

DNSWatch Status in Web UI Front Panel

- In Fireware Web UI, DNSWatch status now appears in the Front Panel dashboard

The screenshot displays the WatchGuard Fireware Web UI Front Panel dashboard. The interface includes a navigation sidebar on the left with categories like DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, and SUBSCRIPTION SERVICES. The main content area shows 'Top Clients' and 'Top Destinations' tables. A 'System' information panel on the right lists details such as Name (T35-W), Version (12.2.B560761), and Uptime (0 days 01:05). A 'Servers' section is also present, where the 'DNSWatch' status is highlighted with a red box and shown as 'Operational'. A 'WatchGuard Cloud' section at the bottom right shows the status as 'Disabled' and a 'REBOOT' button.

Front Panel

Top Clients [View all](#)

NAME	RATE	BYTES	HITS
10.0.1.3	3 Mbps	14 MB	65

Top Destinations [View all](#)

NAME	RATE	BYTES	HITS
10.0.1.1	2 Mbps	474 KB	6
203.0.113.10	609 Kbps	5 MB	2
52.88.42.239 (v)	184 Kbps	2 MB	5
13.91.18.96	66 Kbps	3 MB	1
40.97.80.34	24 Kbps	115 KB	13
192.28.148.84	11 Kbps	129 KB	2
172.217.3.196	8 Kbps	101 KB	2

Services will expire in less than 30 days. [Update Feature Key](#)

System

Name T35-W
Model T35-W
Version 12.2.B560761
Serial Number D02102718C5FC
System Time 16:14 US/Pacific
System Date 2018-04-20
Uptime 0 days 01:05

Servers

Log Server Disabled
Threat Detection Connected
DNSWatch Operational
Dimension Disabled

WatchGuard Cloud

Status Disabled

[REBOOT](#)

Gateway AV Log Message Enhancement

- When Gateway AntiVirus cannot scan a file in a zip archive, the scan error in the traffic log message now includes the name of the file within the archive

- Example log message:

```
Mar 27 11:07:23 2018 xtmv local1.info http-proxy[1678]:  
msg_id="1AFF-003D" Allow 1-Trusted 0-External tcp 10.0.1.2  
203.0.113.3 51770 80 msg="ProxyAllow: HTTP Gateway AV object  
encrypted (password-protected)" proxy_act="HTTP-  
Client.Standard.1" error="Object (password-protected-file.pdf)  
Encrypted" host="example.net" path="/archive.zip"
```

- Previously, the error in this log message would say:
error="Object Encrypted"

Modem Support

- Support is added for these modems:
 - LTE UX302NC USB
 - LTE UX302NC-R USB
 - Fujisoft FS040U
 - Netgear 341U USB

Thank You!