What's New in Fireware v12.2

WatchGuard Training

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

WatchGuard Training

Intelligent AntiVirus

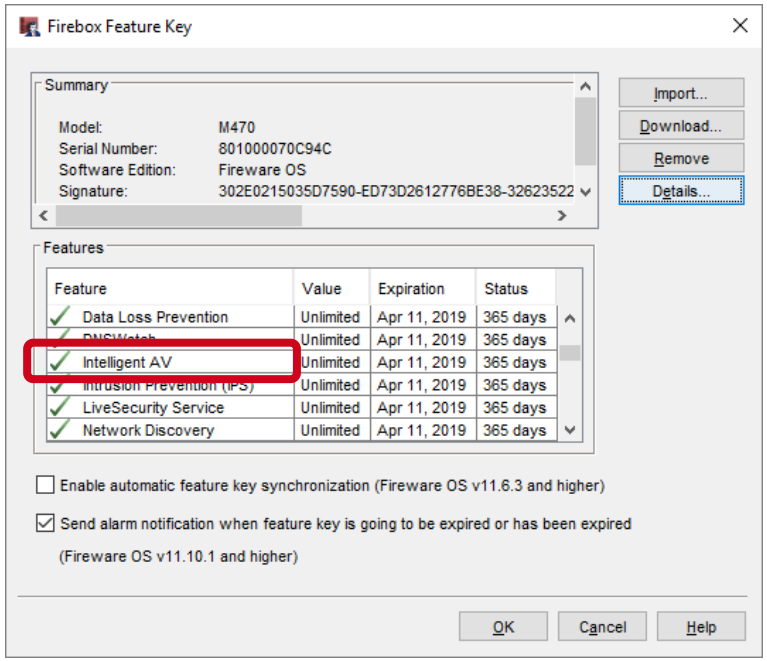
- Intelligent AntiVirus is a new subscription service that enhances the ability of Gateway AntiVirus to detect new threats and polymorphic malware
  - WatchGuard has partnered with Cylance to provide this as a supplemental scanning solution for our higher-end Firebox models
  - Intelligent AntiVirus 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

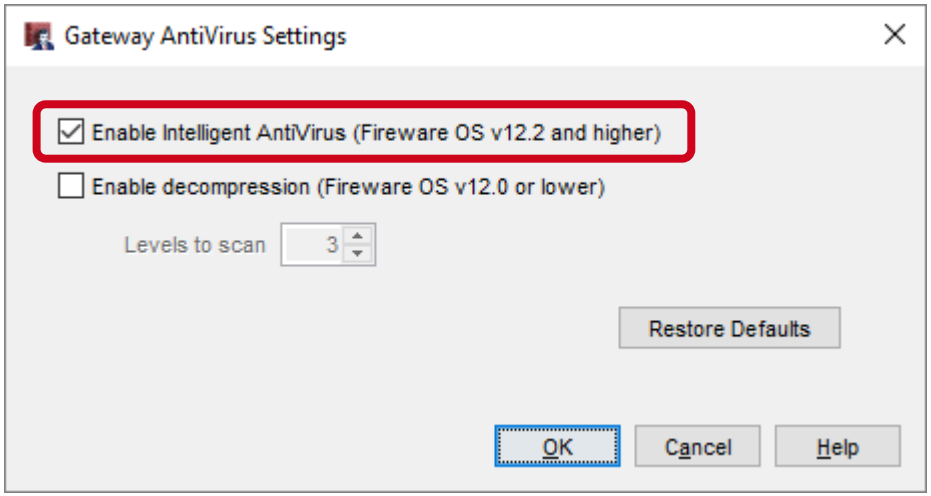
Intelligent AntiVirus Models and Licensing

- 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**



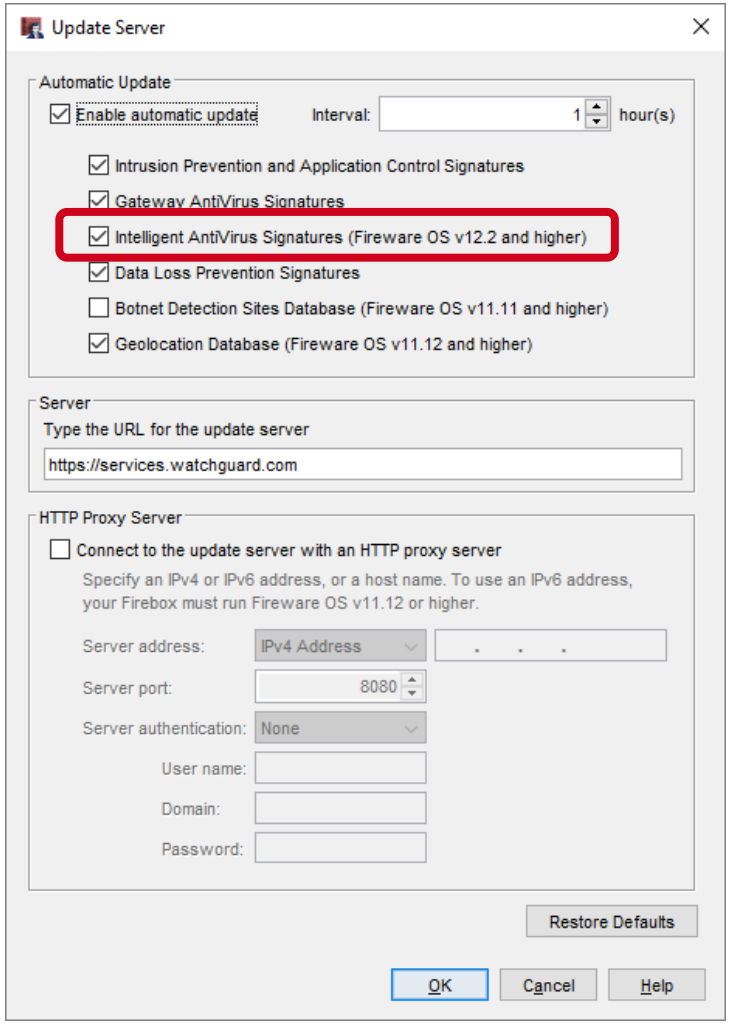
Intelligent AntiVirus Configuration

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



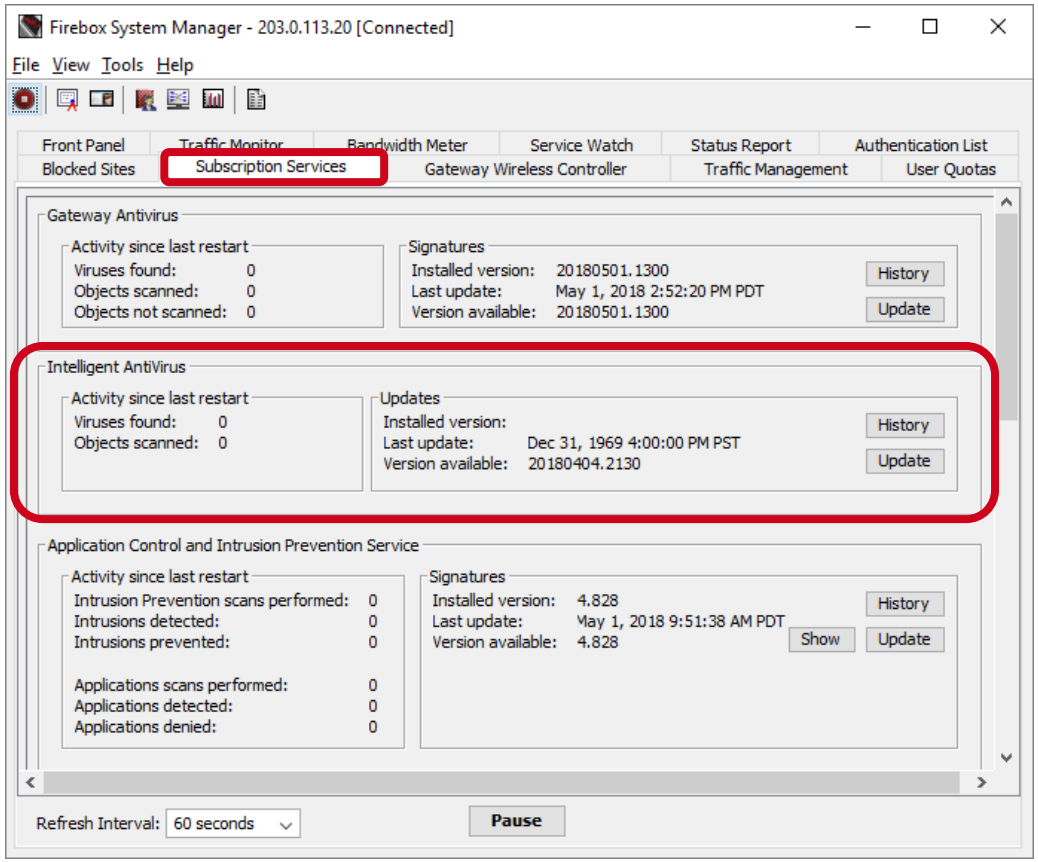
Intelligent AntiVirus Configuration

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



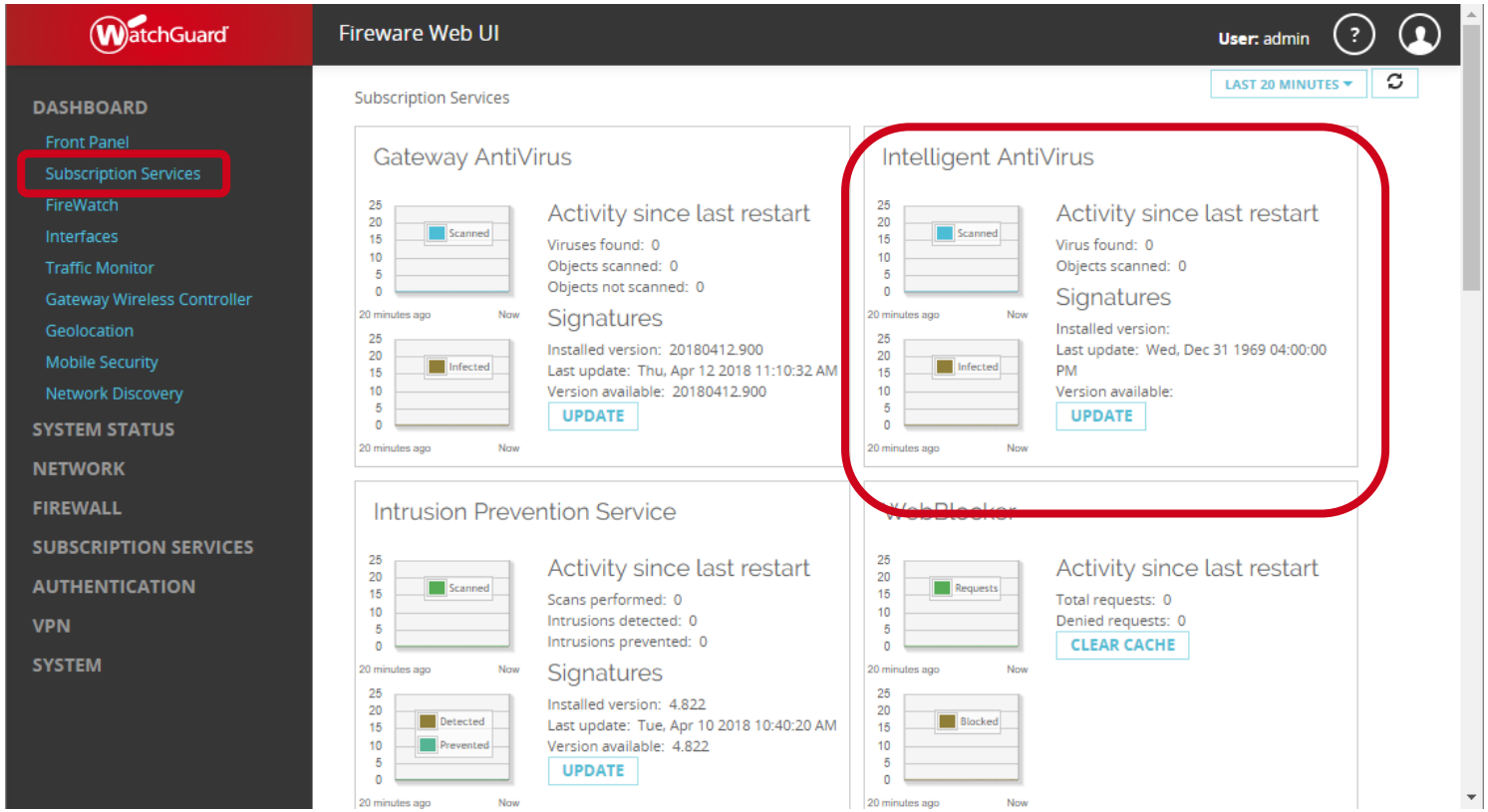
Intelligent AntiVirus Status

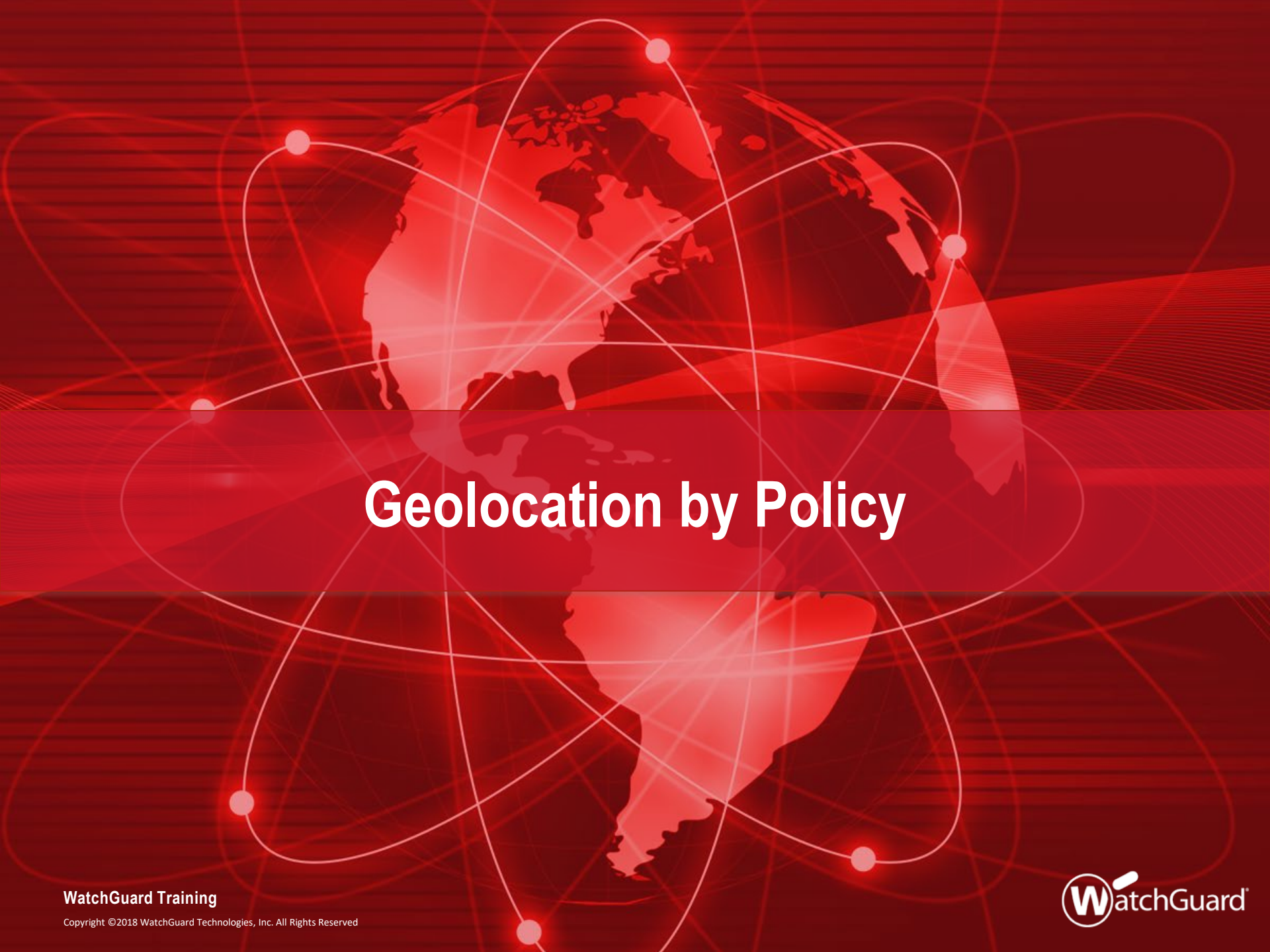
- In Firebox System Manager, Intelligent AntiVirus status and statistics are available on the Subscription Services tab



Intelligent AntiVirus Status

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





WatchGuard Training

Geolocation by Policy

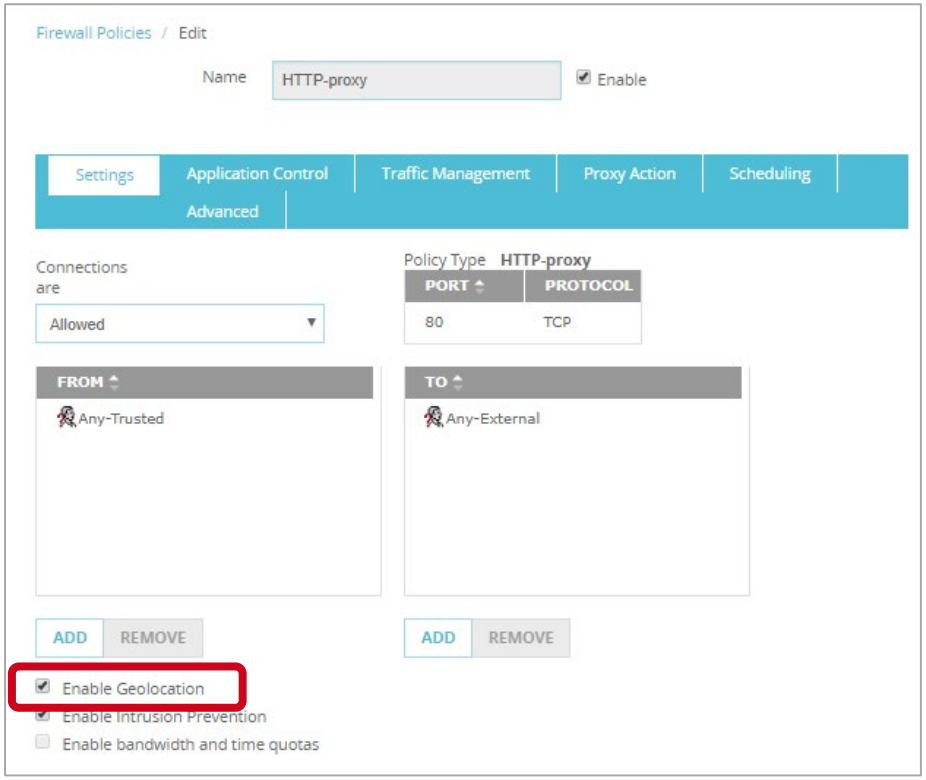
- You can now enable Geolocation at the policy level
- This provides you with more granular control over the types of connections the Firebox denies based on geographic location

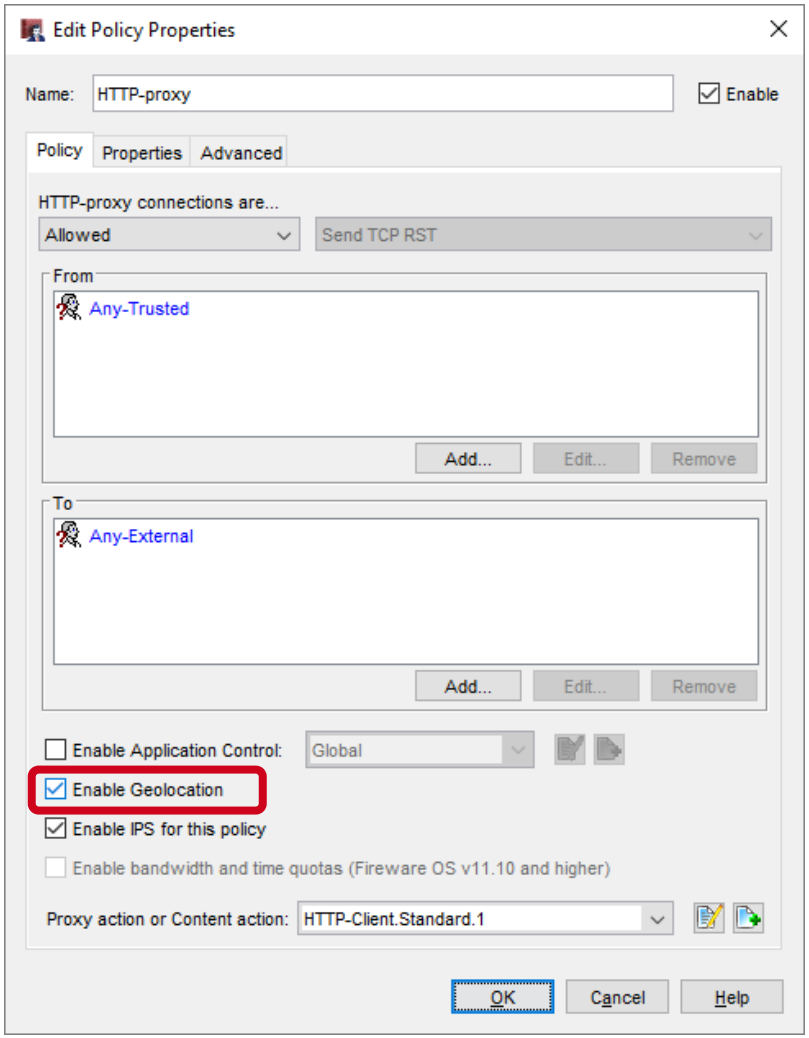
Geolocation by Policy

- 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





SMTP and POP3 over TLS

SMTP and POP3 over TLS

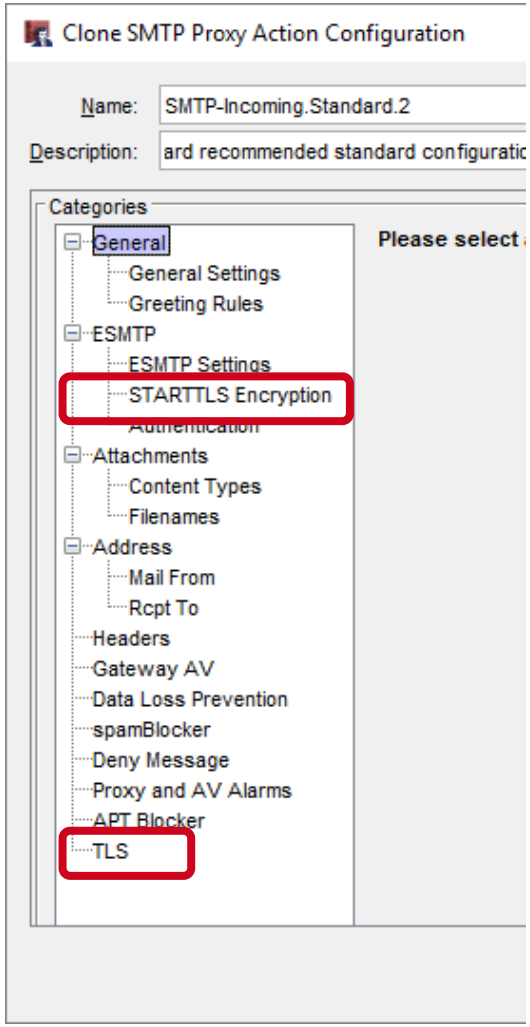
- This release extends TLS profile support to the POP3 and SMTP proxies
  - TLS profiles were previously supported only for the IMAP and HTTPS proxies
- This update enables POP3 and SMTP proxies to inspect mail traffic encrypted with TLS on implicit secure ports:
  - POP3 over TLS
  - SMTP over TLS
-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

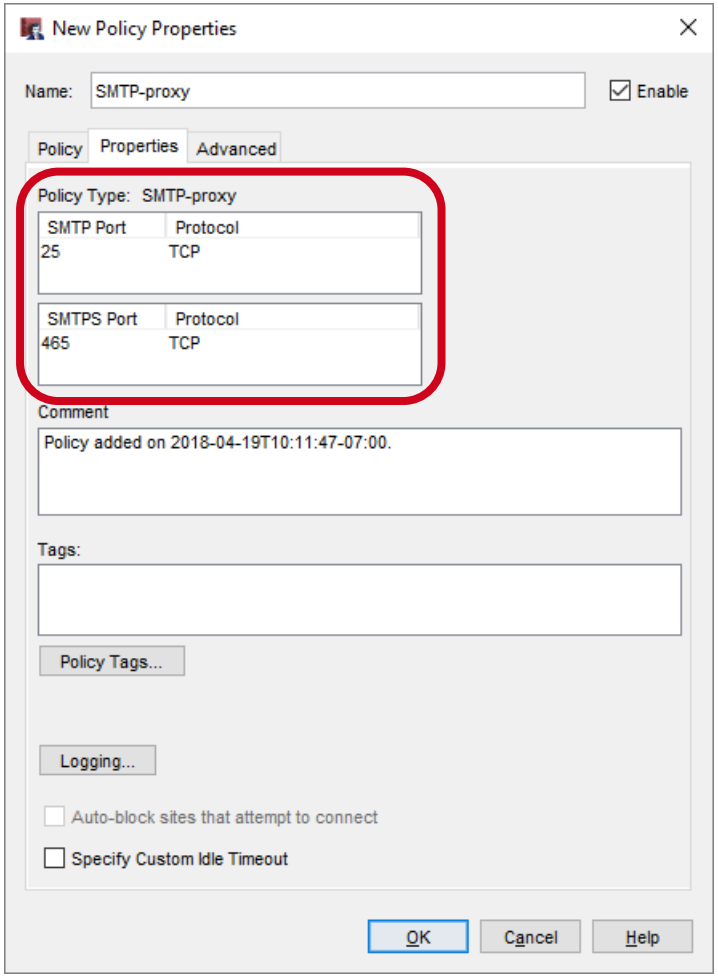
SMTP Proxy — TLS

- 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



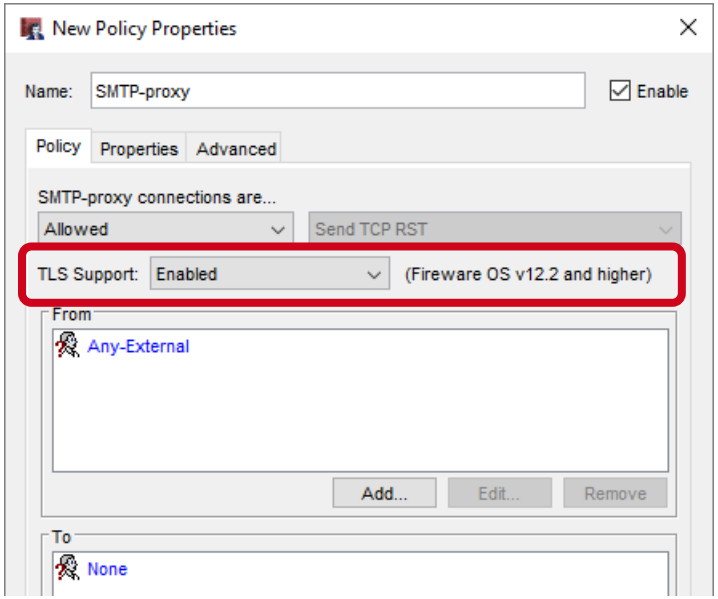
Secure SMTP (SMTPS)

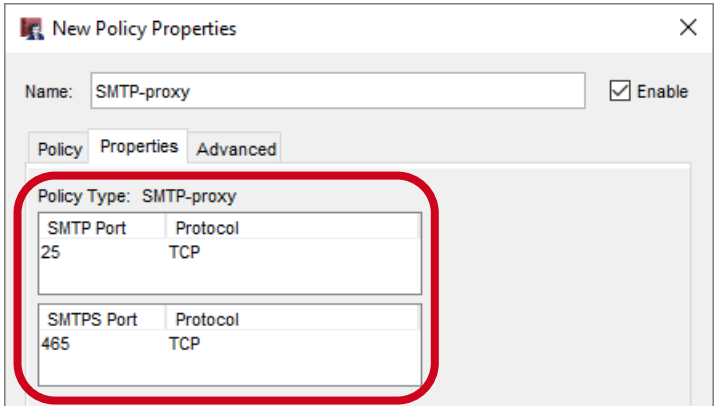
- The SMTP proxy now supports Secure SMTP (SMTPS)
- The SMTP proxy supports:
  - SMTP on TCP port 25
  - SMTPS on TCP port 465 (new)



SMTP Proxy — TLS Support

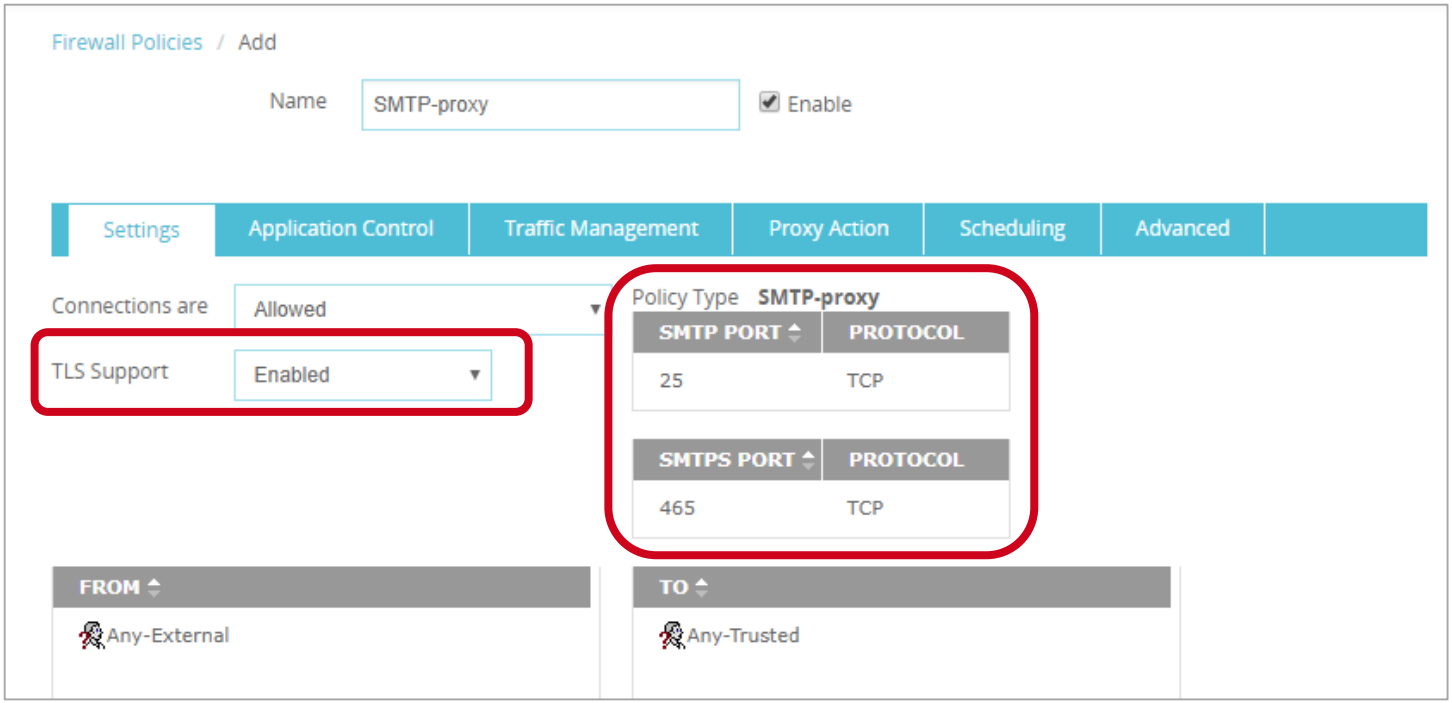
- The **TLS Support** option controls which ports the SMTP proxy listens on:
  - **Disabled** — SMTP proxy listens on port 25 only
  - **Enabled** (default) — SMTP proxy listens on ports 25 and 465
  - **Required** — SMTP proxy listens on port 465 only
- The port list depends on the TLS Support option





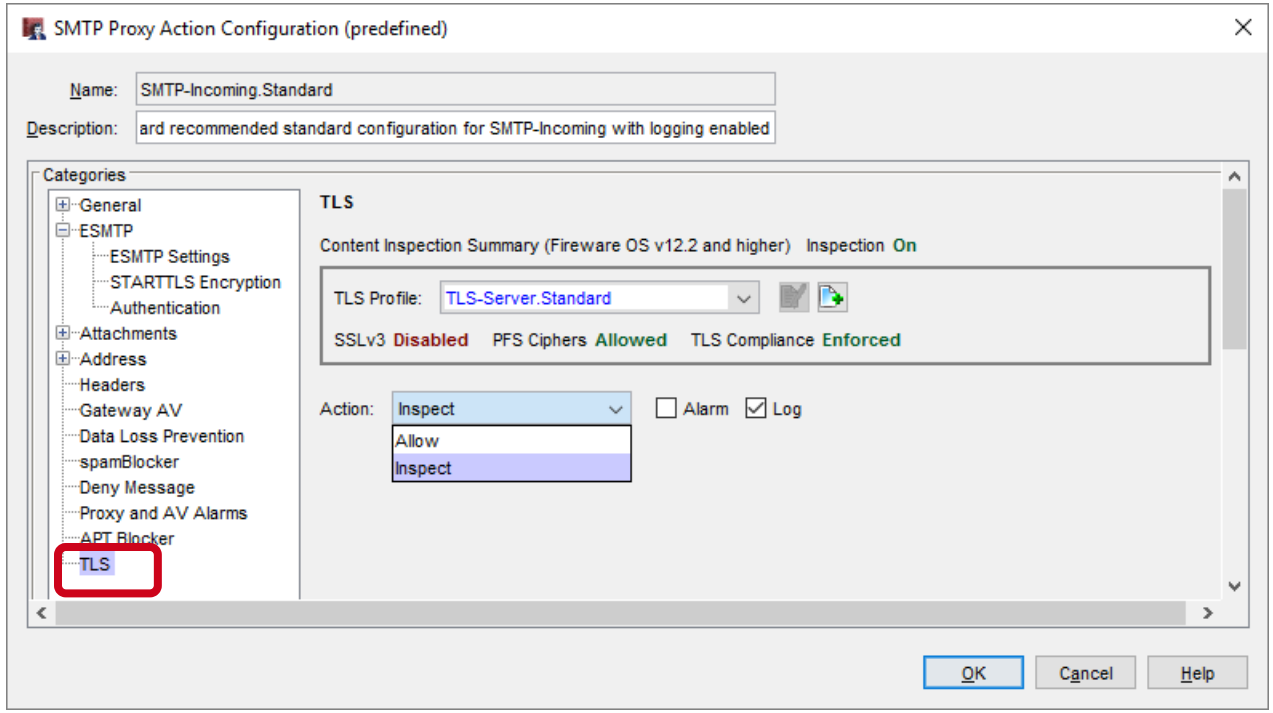
SMTP Proxy — TLS Support

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



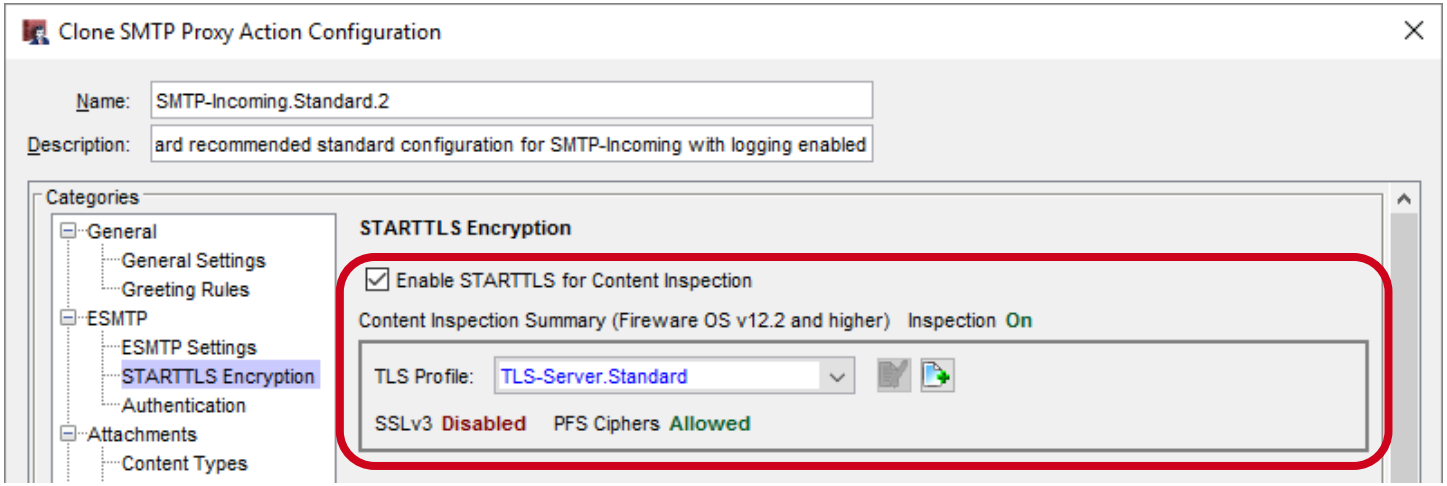
SMTP Proxy Action — TLS Settings

- 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



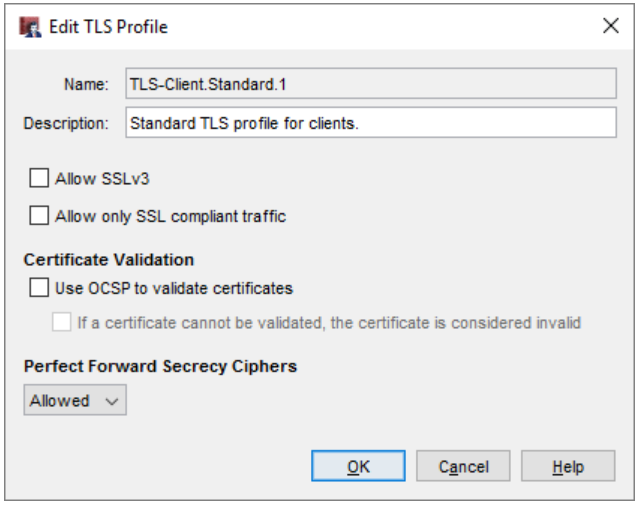
SMTP Proxy Action — STARTTLS Encryption

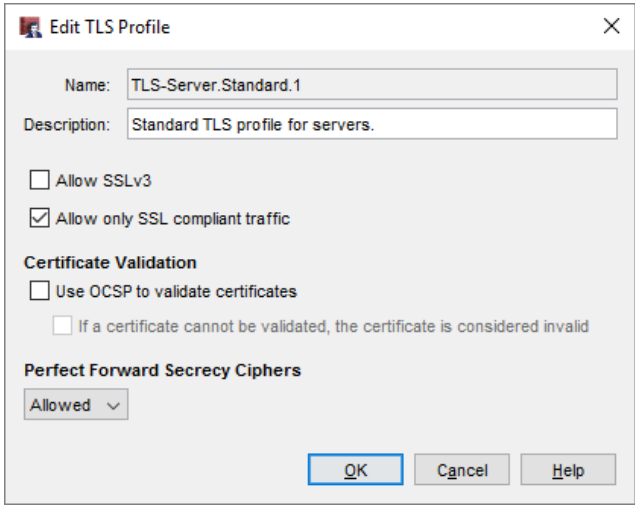
- In the ESMTP settings, the TLS Encryption settings are now called STARTTLS Encryption
  - These settings also use a TLS profile
  - The TLS profile you select in the STARTTLS Encryption settings can be different from the TLS profile in the TLS settings



SMTP and POP3 over TLS

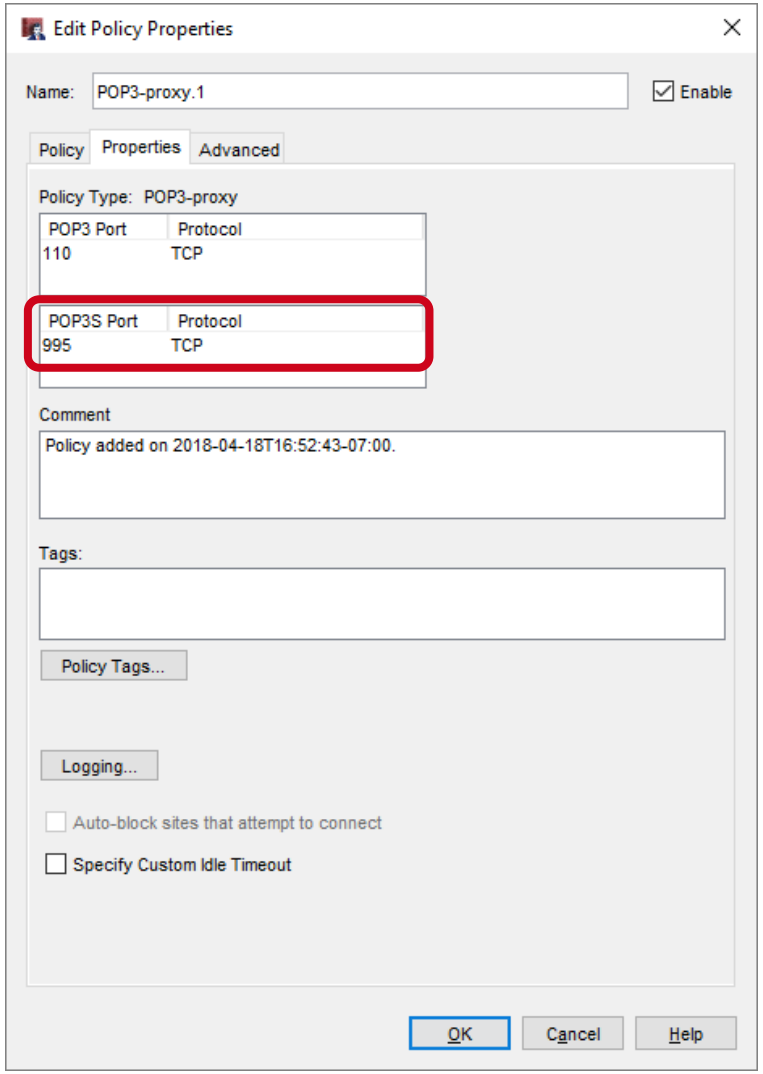
- A TLS profile is a collection of TLS-related security settings:
  - Allow SSLv3
  - Allow only SSL compliant traffic
  - Certificate Validation (OCSP)
  - Perfect Forward Secrecy Ciphers
- The POP3 and SMTP proxies now use the same client and server TLS profiles previously supported for other proxies





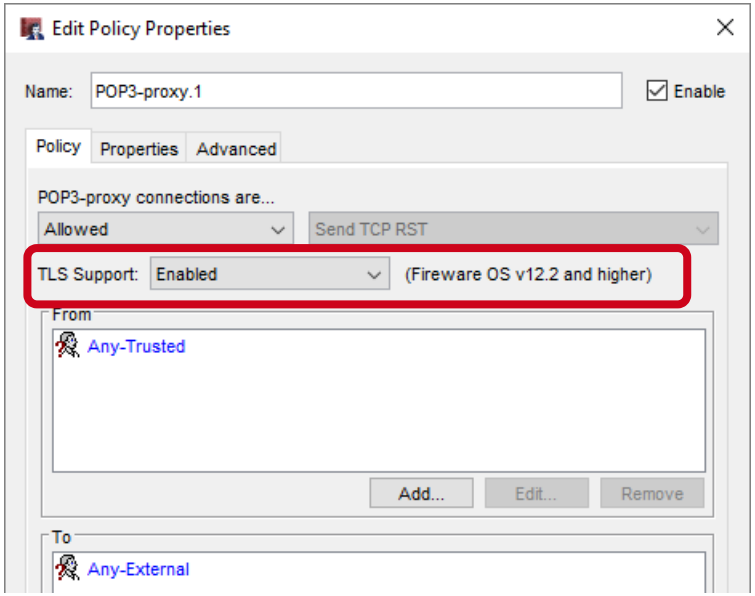
Secure POP3 (POP3S)

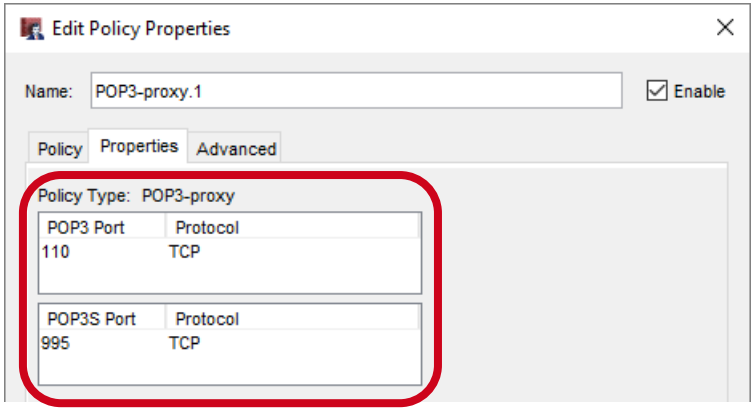
- The POP3 proxy now supports Secure POP3 (POP3S)
- The POP3 proxy supports:
  - POP3 on TCP port 110
  - POP3S on TCP port 995 (new)



POP3 Proxy — TLS Support

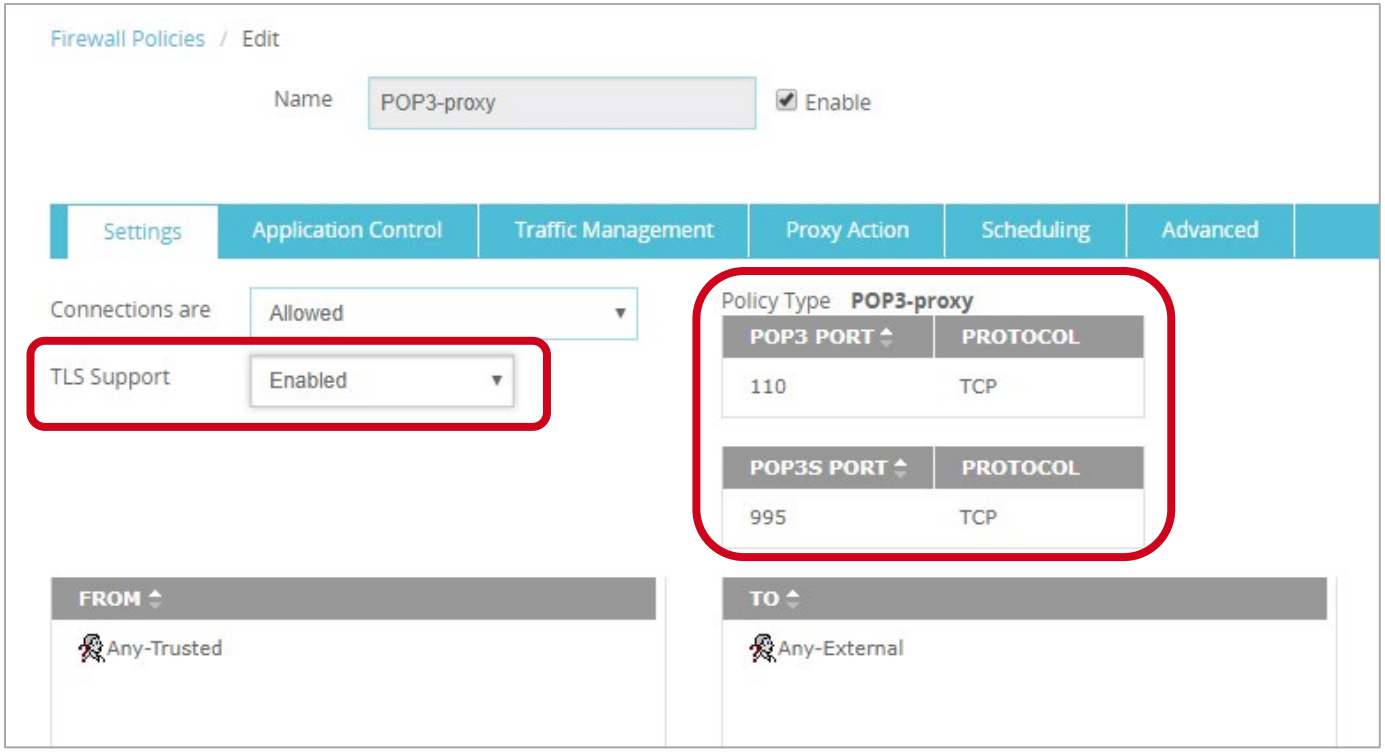
- The **TLS Support** option controls which ports the POP3 proxy listens on:
  - **Disabled** — POP3 proxy listens on port 110 only
  - **Enabled** (default) — POP3 proxy listens on ports 110 and 995
  - **Required** — POP3 proxy listens on port 995 only
- The port list depends on the TLS Support option





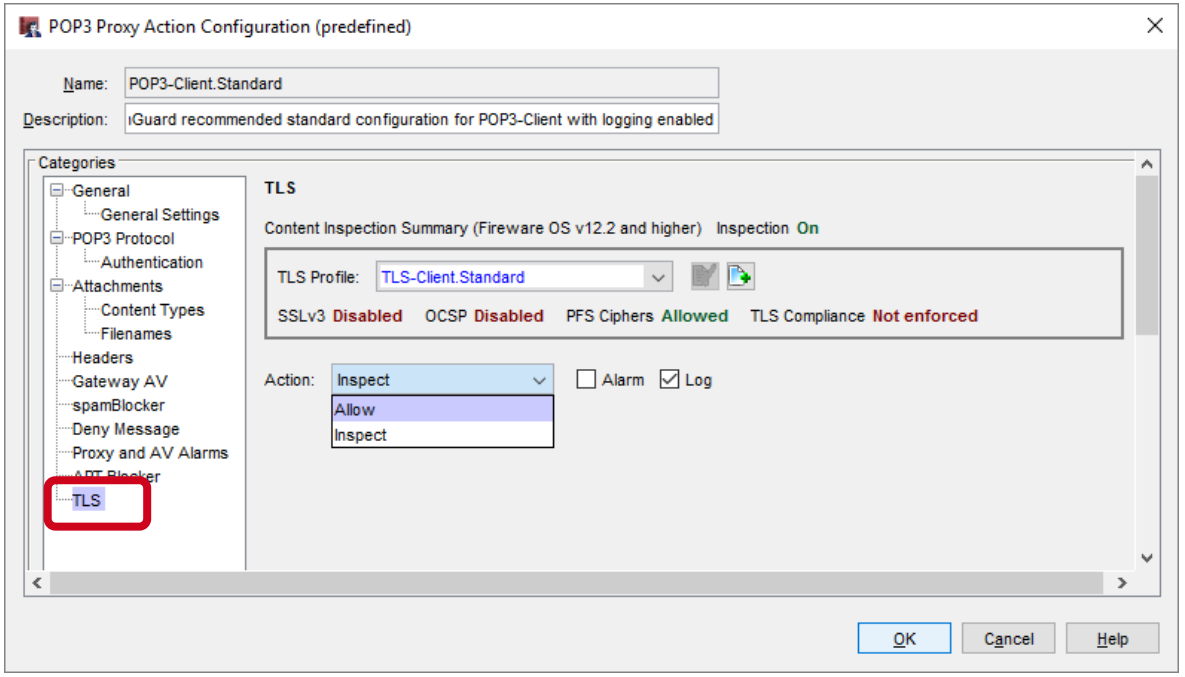
POP3 Proxy — TLS Support

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



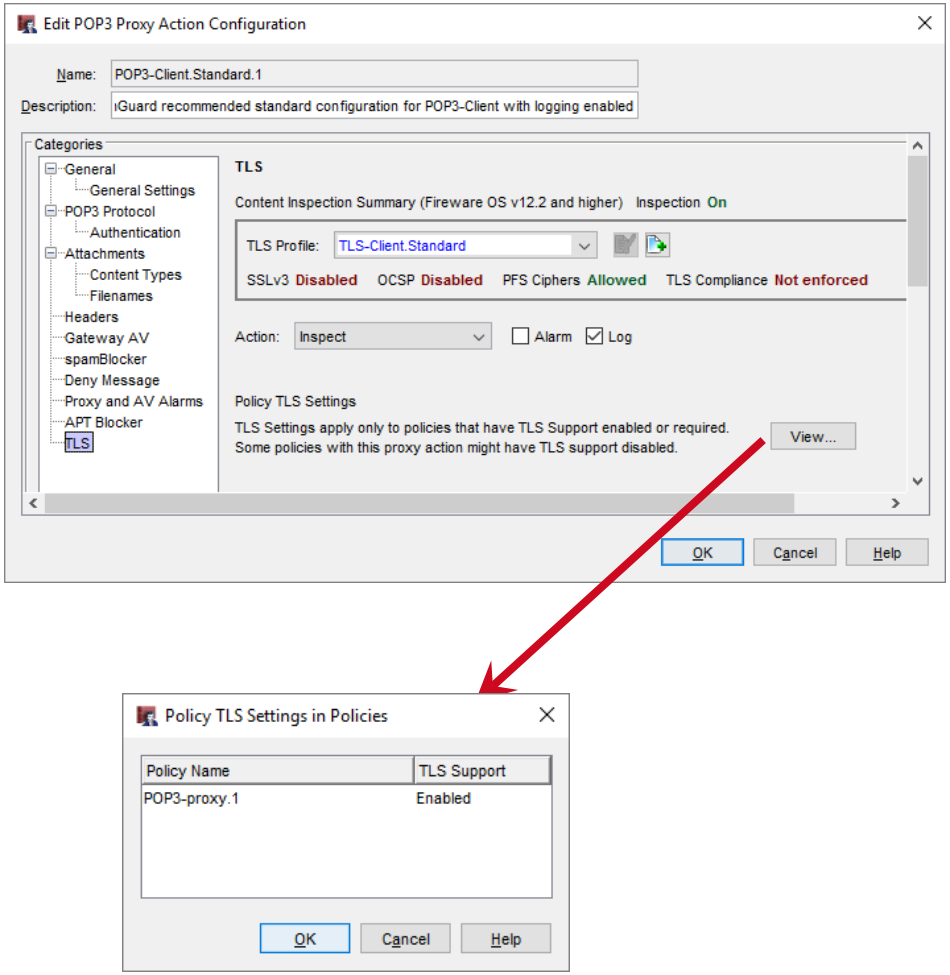
POP3 Proxy Action — TLS Settings

- 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



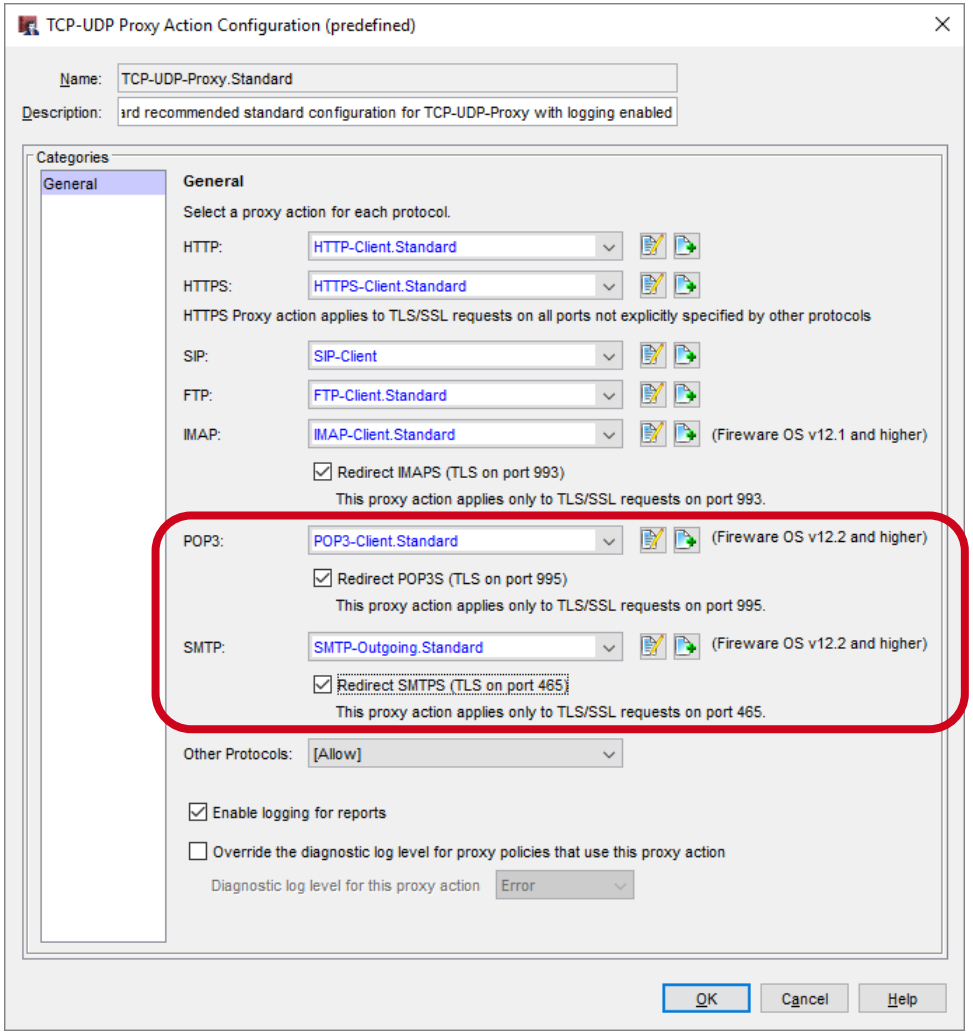
POP3 Proxy Action TLS Settings

- 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



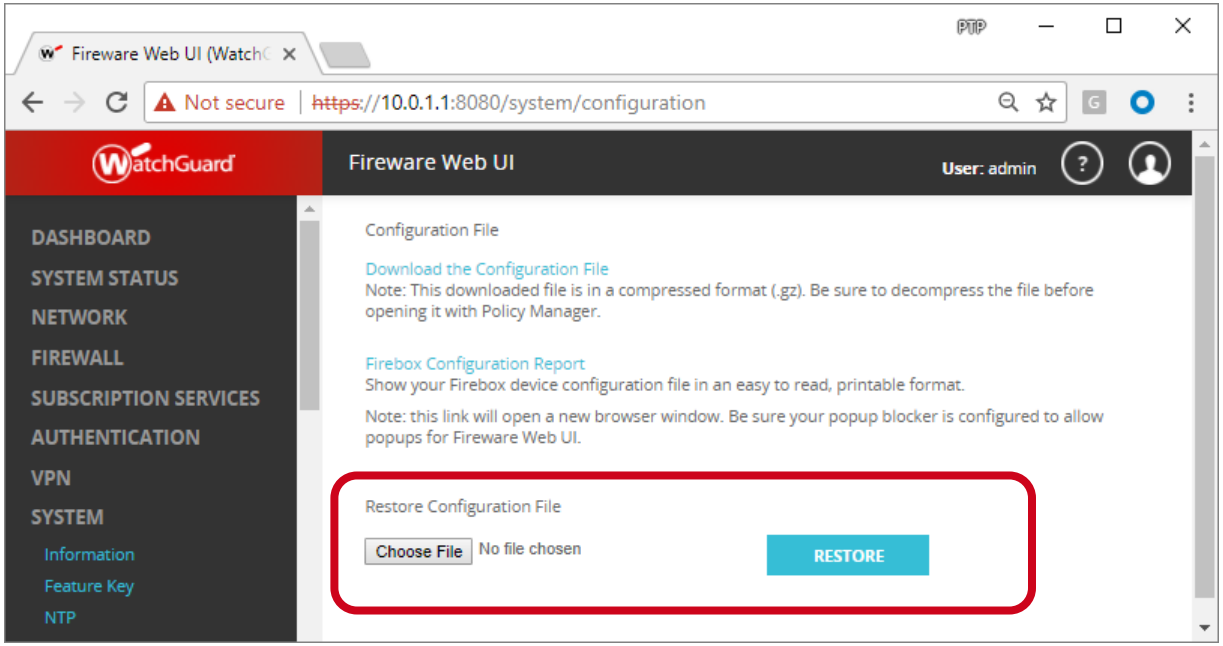
Restore Configuration from Fireware Web UI

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

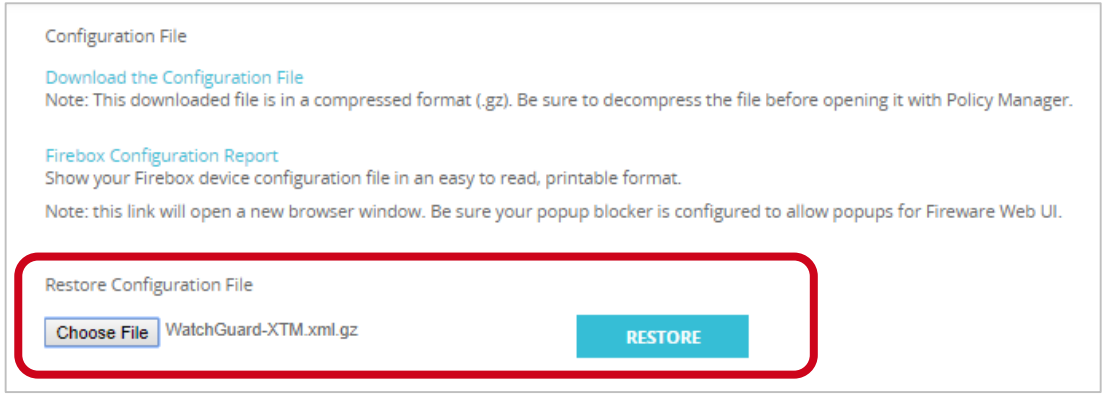
Restore Configuration from Fireware Web UI

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



Restore Configuration from Fireware Web UI

- To restore a saved configuration file:
  1. In Fireware 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**



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

WatchGuard Training

Firebox Cloud Enhancements

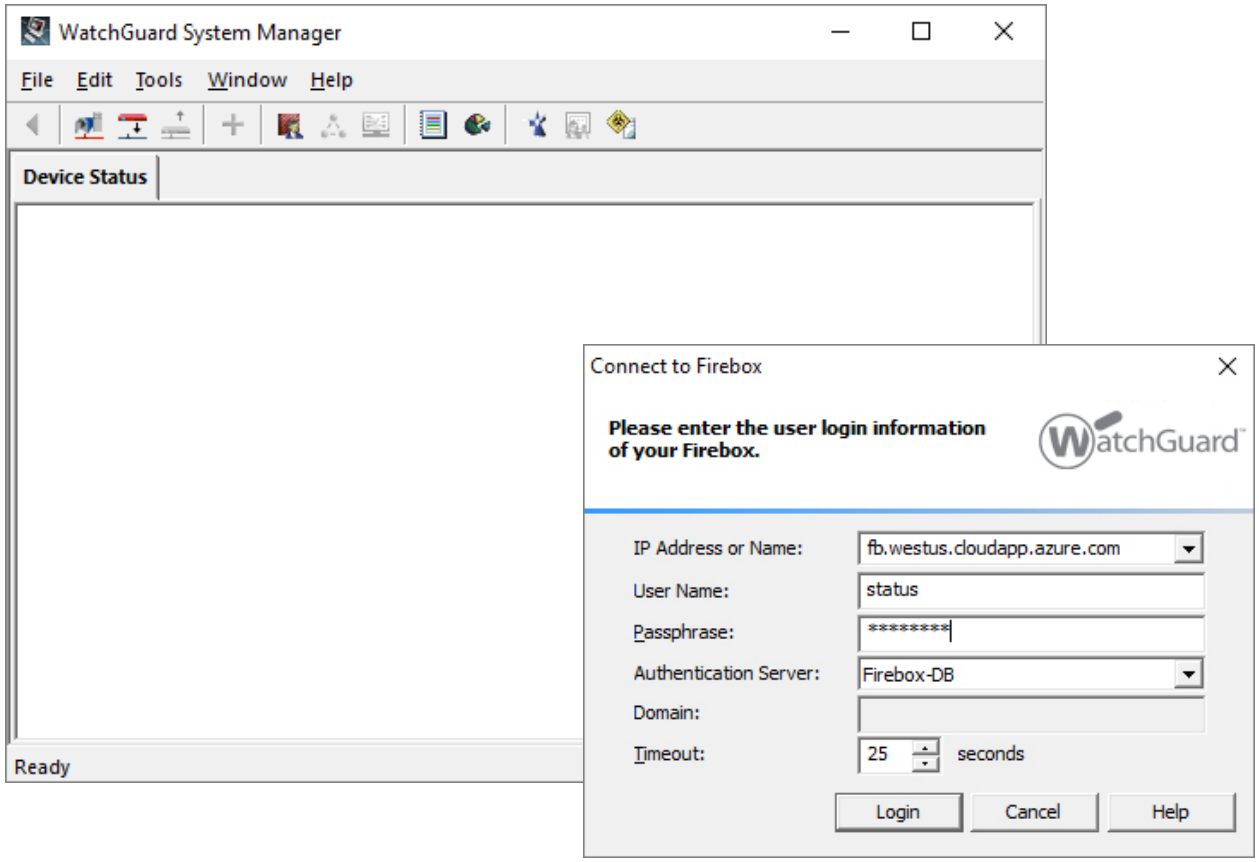
- WatchGuard System Manager and WSM Management Server can now manage Firebox Cloud
- Firebox Cloud now supports these features:
  - Single Sign-On (SSO)
  - spamBlocker
  - Quarantine Server
- Firebox Cloud for Azure will support an hourly license option

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

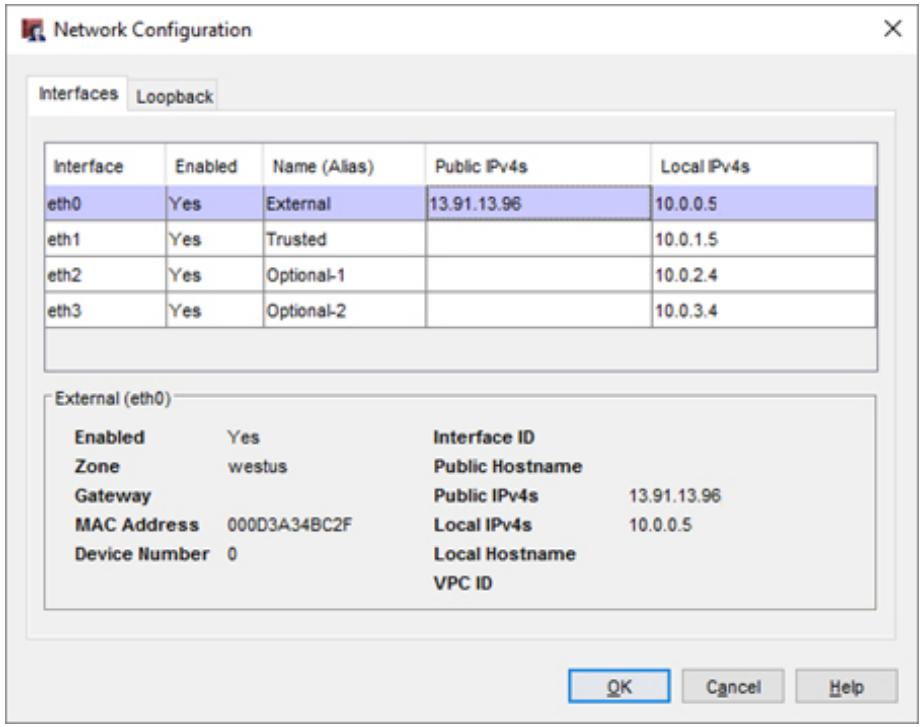


Firebox Cloud — Policy Manager

- 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)

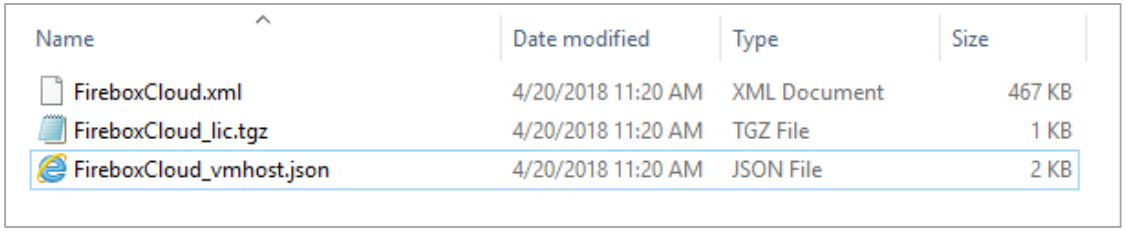
Firebox Cloud — Policy Manager

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



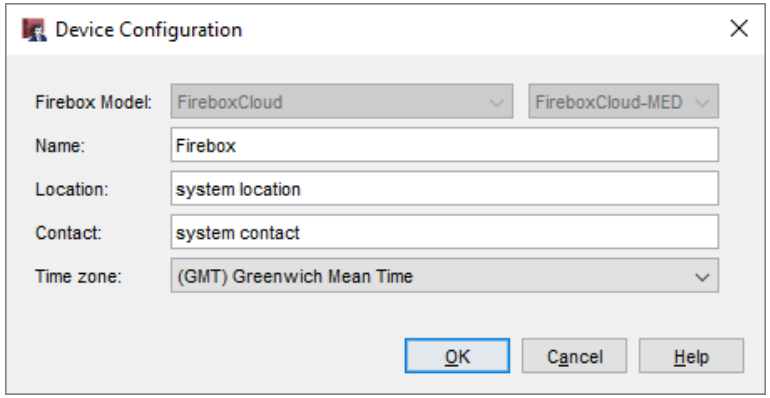
Firebox Cloud — Policy Manager

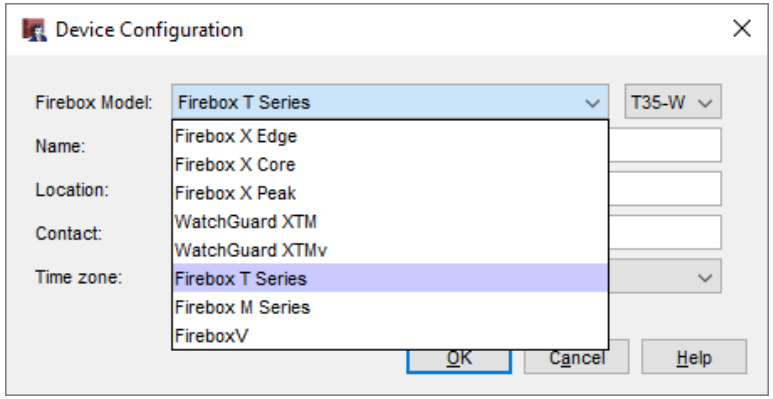
- When you save the Firebox Cloud configuration to a file, Policy Manager saves three files:
  - The configuration file (.xml)
  - The feature key file (_lic.tgz)
  - The VM information file (_vmhost.json)



Firebox Cloud — Policy Manager

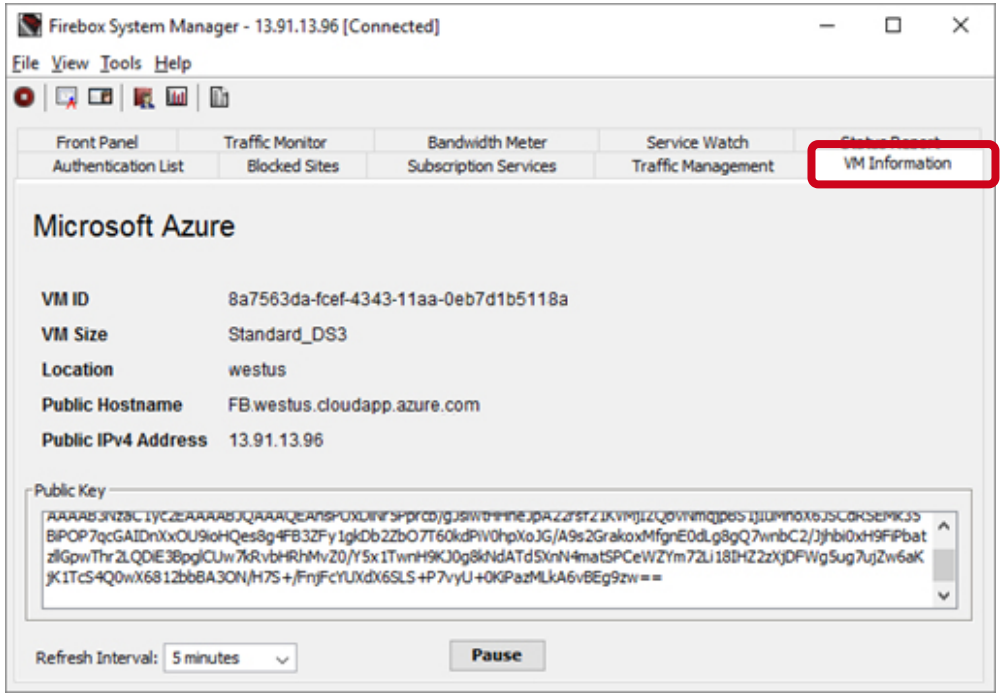
- Firebox Cloud configuration files are not compatible with other Firebox models
  - On the **Setup > System** page for Firebox Cloud, you cannot change the Firebox Model
  - On the **Setup > System** page for any other Firebox model, you cannot change the model to Firebox Cloud
  - In Policy Manager,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





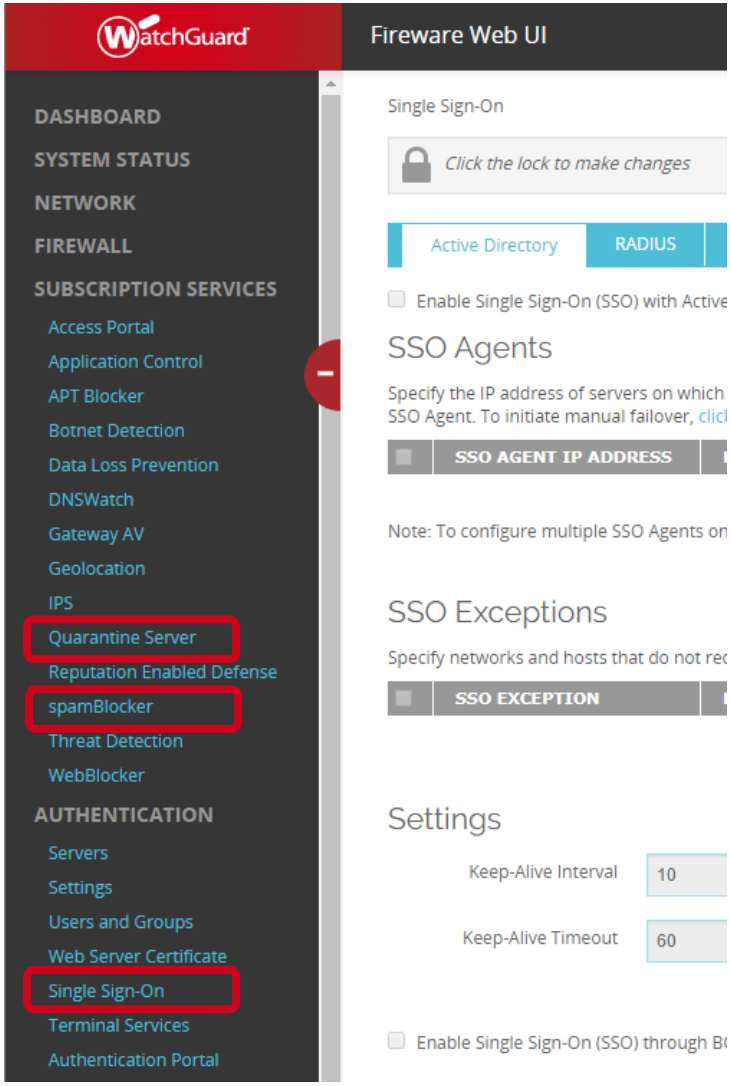
Firebox Cloud — Firebox System Manager

- 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



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



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

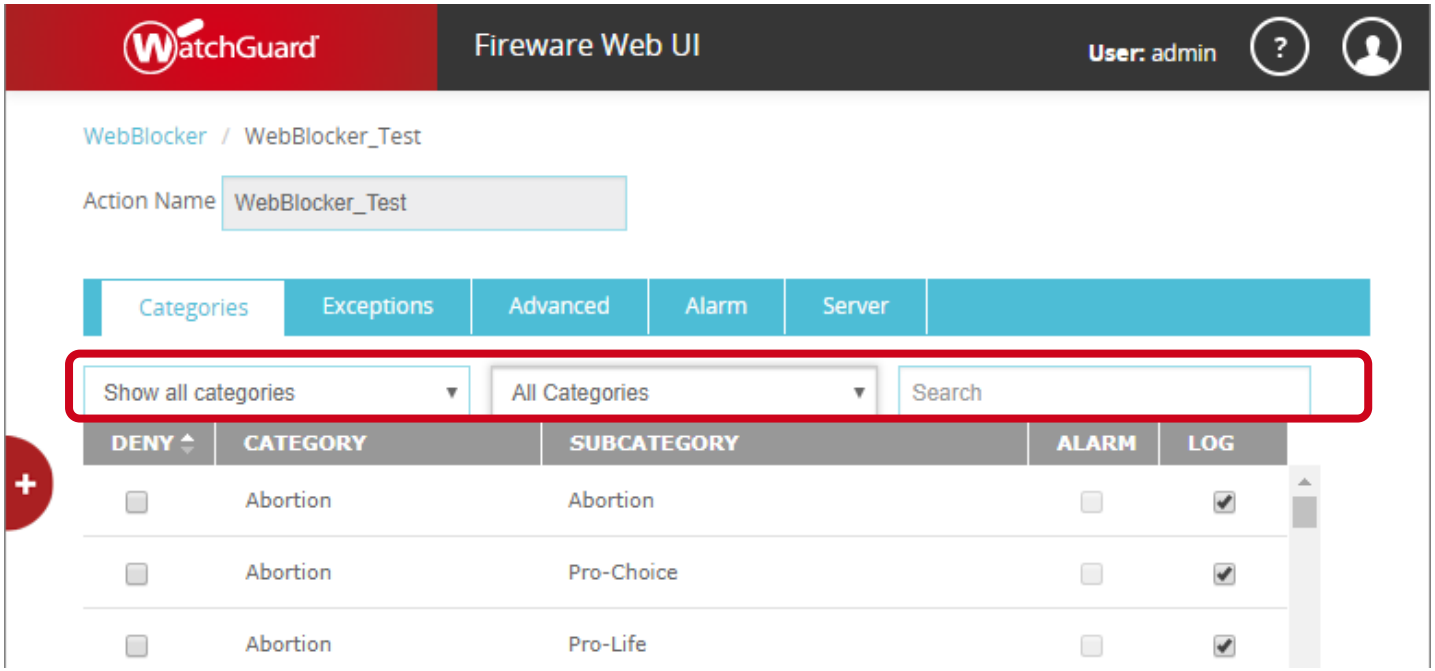
WatchGuard Training

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

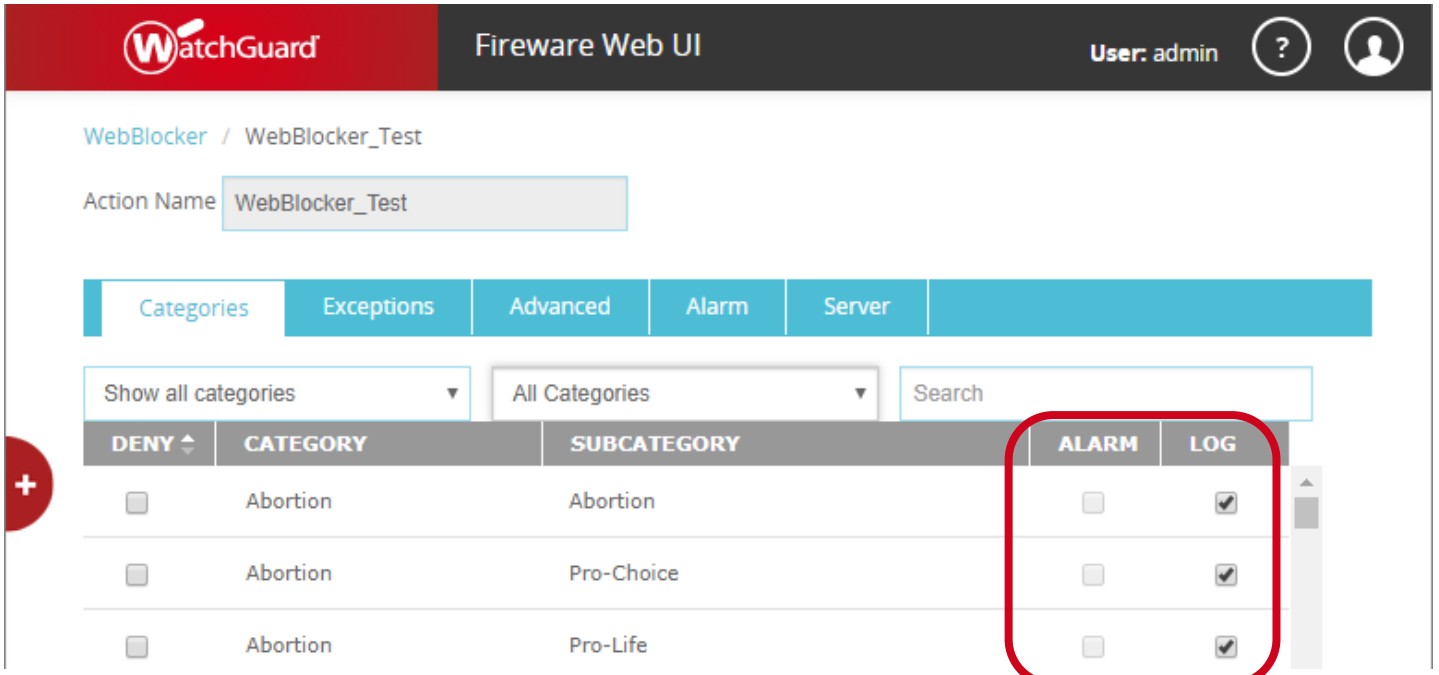
WebBlocker Usability Enhancements

- 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



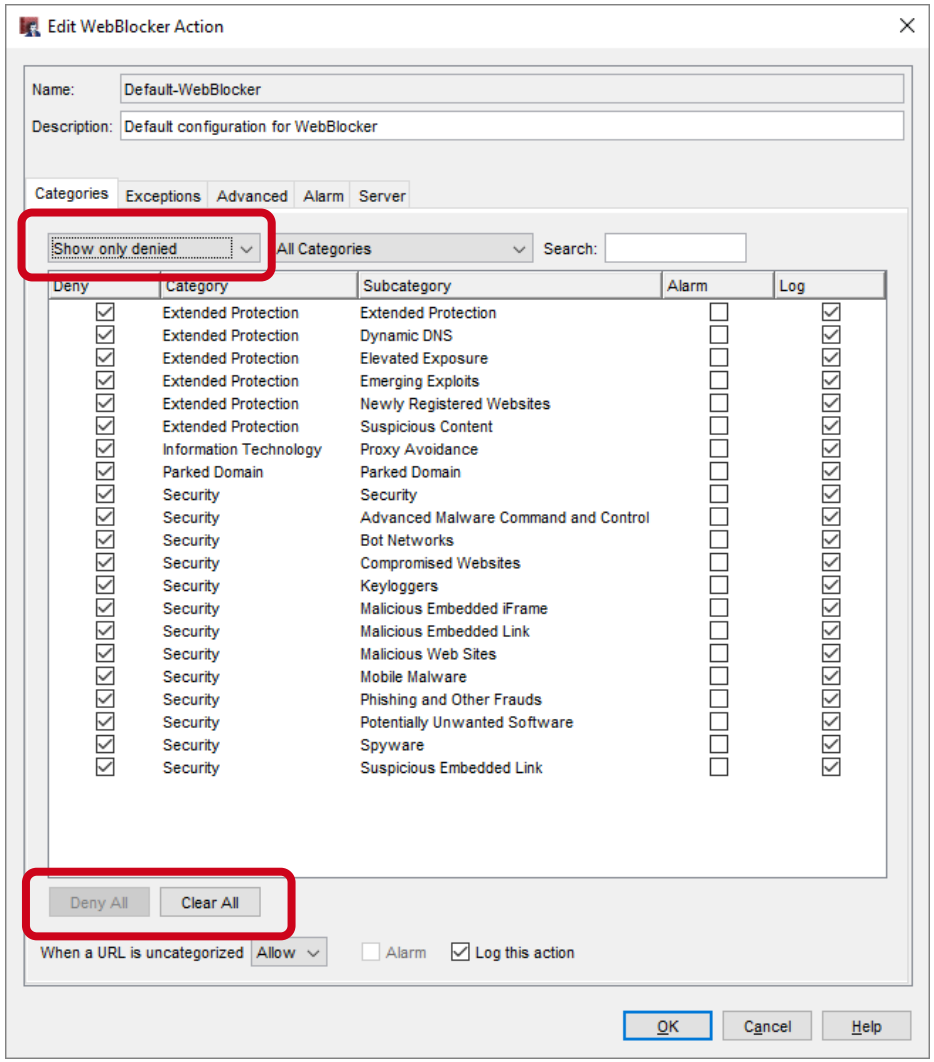
WebBlocker Usability Enhancements

- 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**



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

WatchGuard Training

On-Premises WebBlocker Server

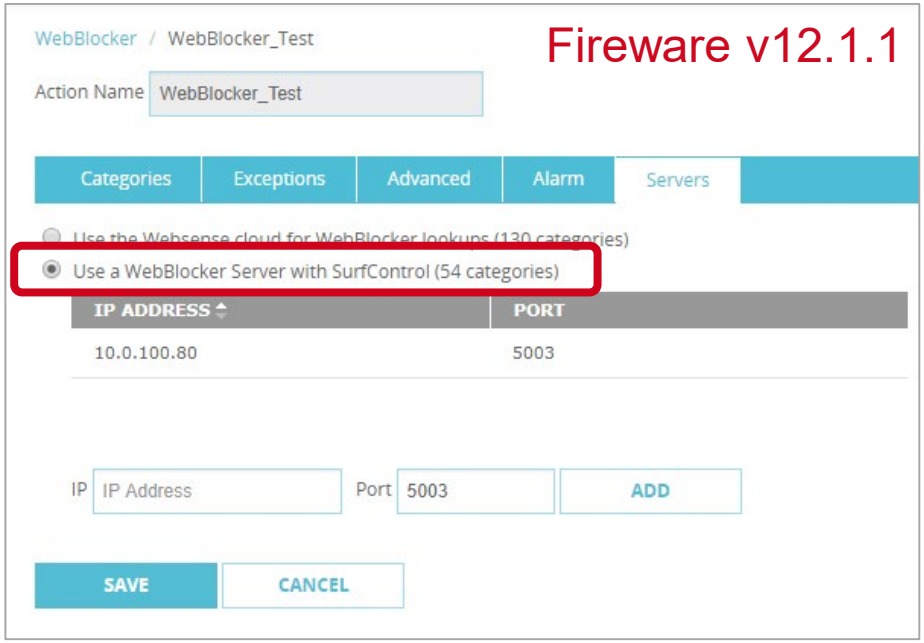
- Fireware now supports an on-premises WebBlocker Server with the same set of content categories as Websense cloud (now called WebBlocker cloud)
  - Supports more content categories than the WebBlocker Server previously available for local installation with WSM
  - New UI available in Fireware v12.2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

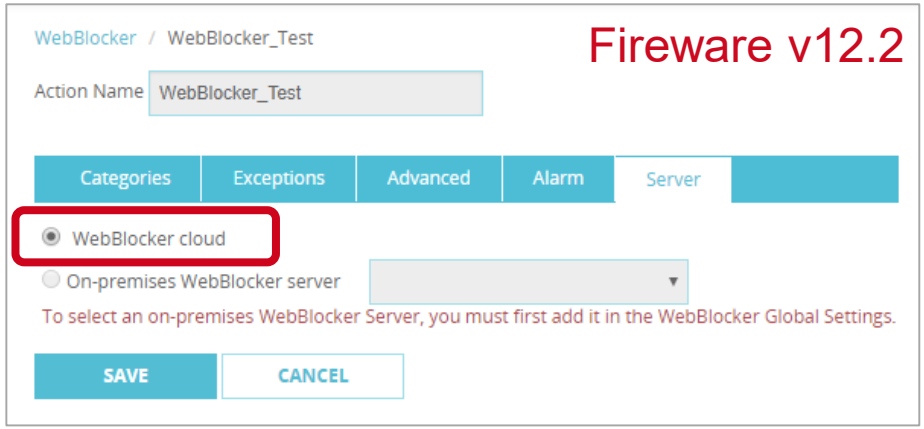
On-Premises WebBlocker Server

- 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





On-Premises WebBlocker Server Licensing

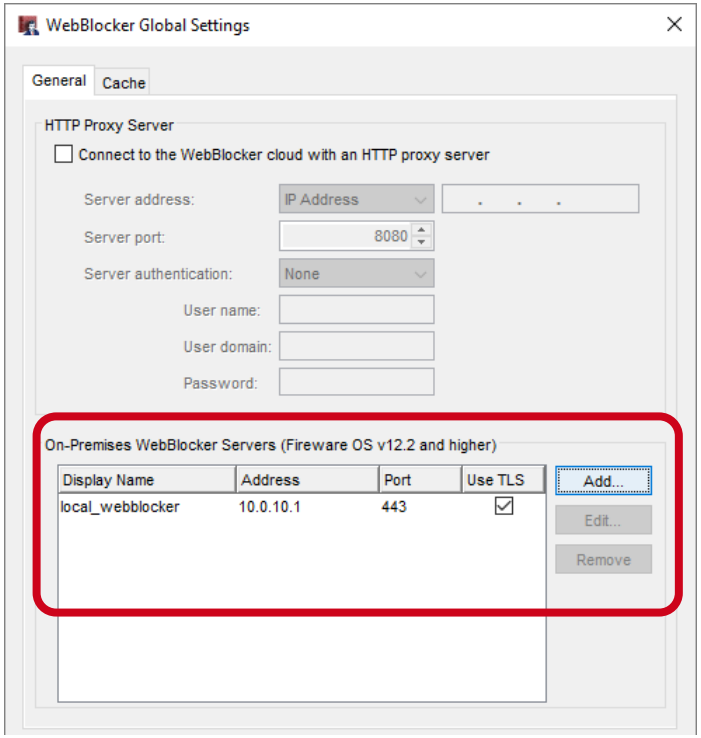
- The on-premises WebBlocker Server is licensed as part of a WebBlocker subscription
- To activate an on-premises WebBlocker Server, you must have a Firebox with an active Total Security or WebBlocker subscription
- If the WebBlocker subscription expires, the WebBlocker Server activation also expires

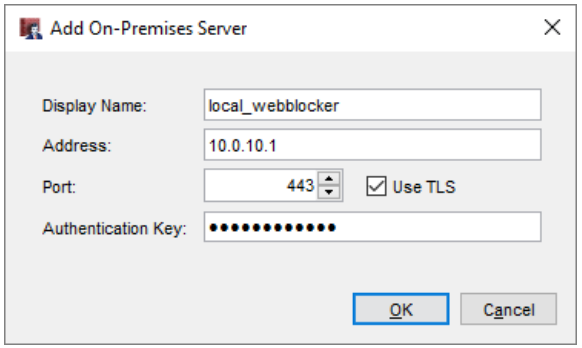
On-Premises WebBlocker Server Setup

- 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

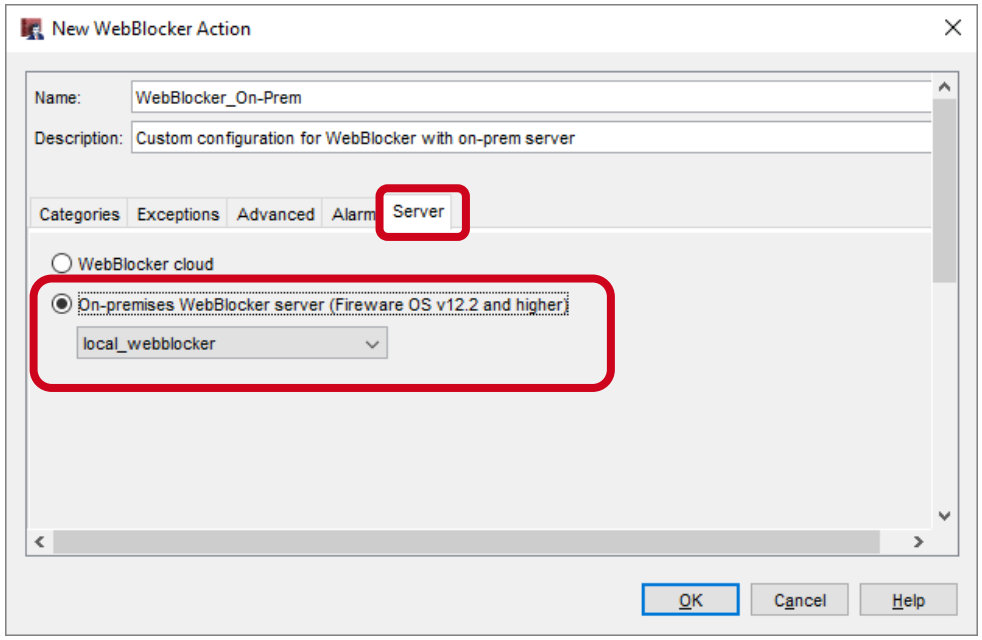
- To add an on-premises WebBlocker Server to the Firebox configuration, edit WebBlocker Global settings
  - WebBlocker Server Properties:
    - **Display Name** — The server name as it appears in the WebBlocker configuration
    - **Address** — WebBlocker Server host name or IP address
    - **Port**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





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

WatchGuard Training

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

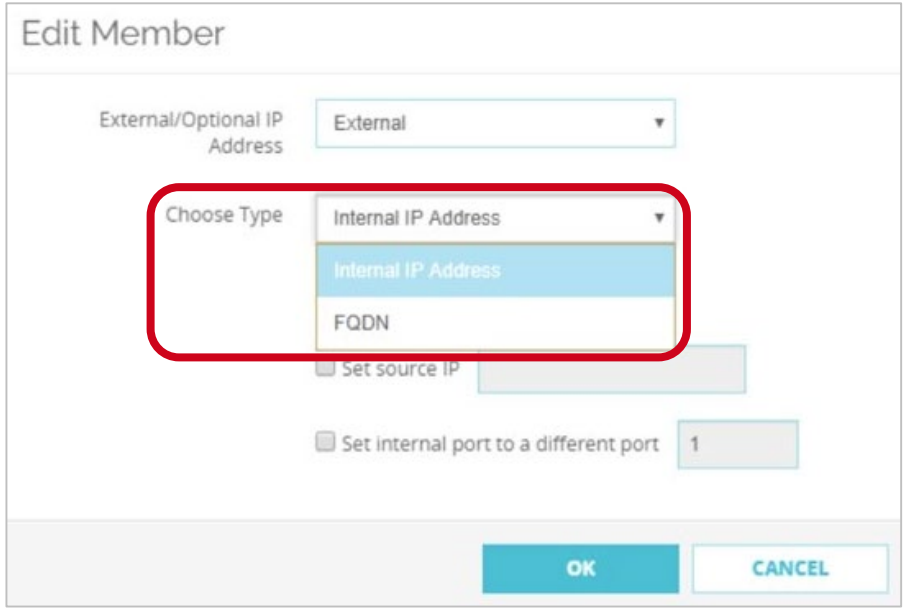
- The same FQDN can be used in more than one policy
- Prevents issues with multiple FQDN matches in different packet level features, such as packet filter policies, blocked sites, and blocked sites exceptions
- Policy order precedence decides the FQDN resolution

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:



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

WatchGuard Training

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

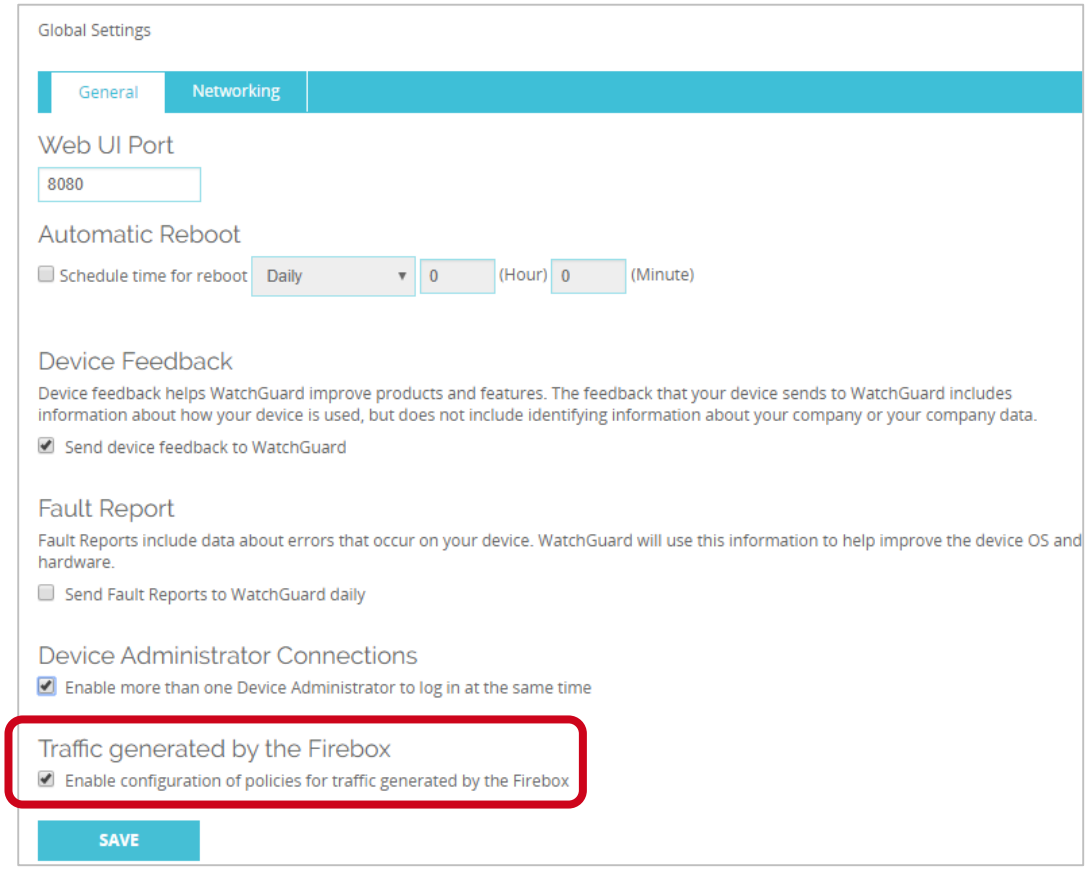
- These enhancements have many uses:
  - You can apply global NAT, per-policy NAT, policy-based routing, traffic management, and QoS to policies for Firebox-generated traffic
- Examples of Firebox-generated traffic:
  - Signature-based cloud services, such as Gateway AntiVirus, Intrusion Prevention Service, 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

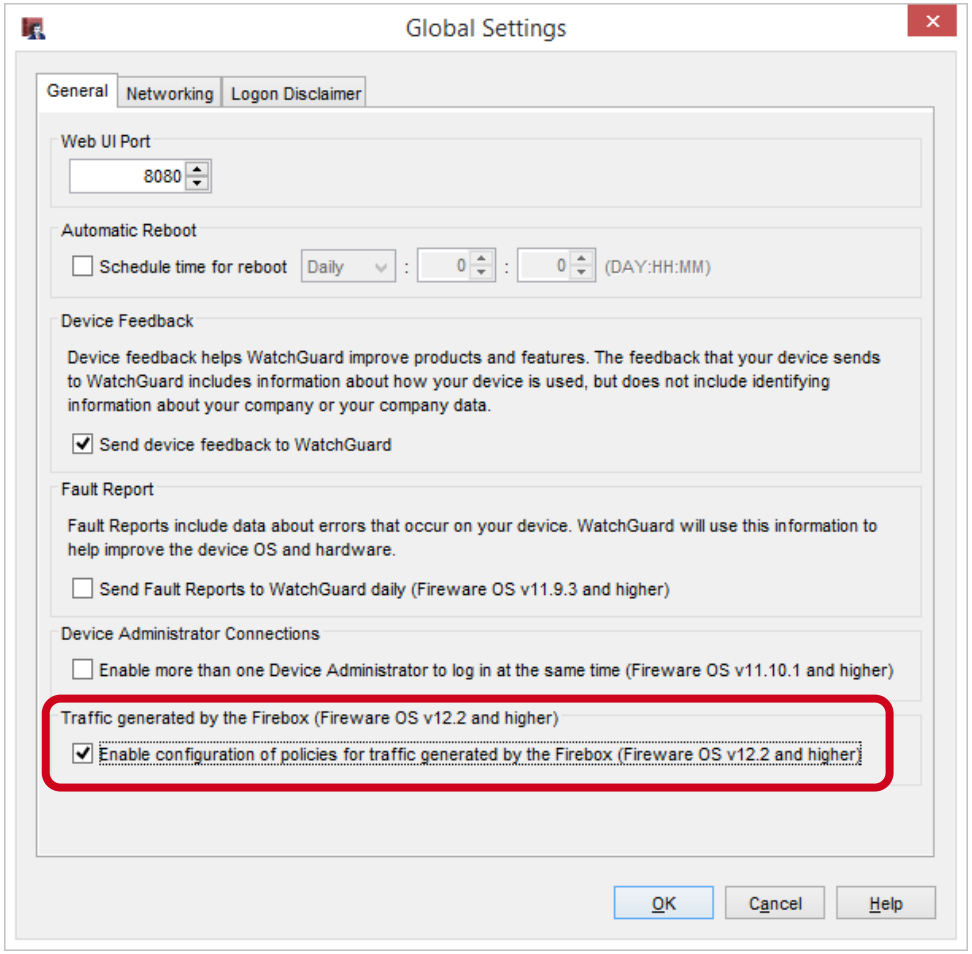
Control Firebox-Generated Traffic

- Web UI



Control Firebox-Generated Traffic

- Policy Manager

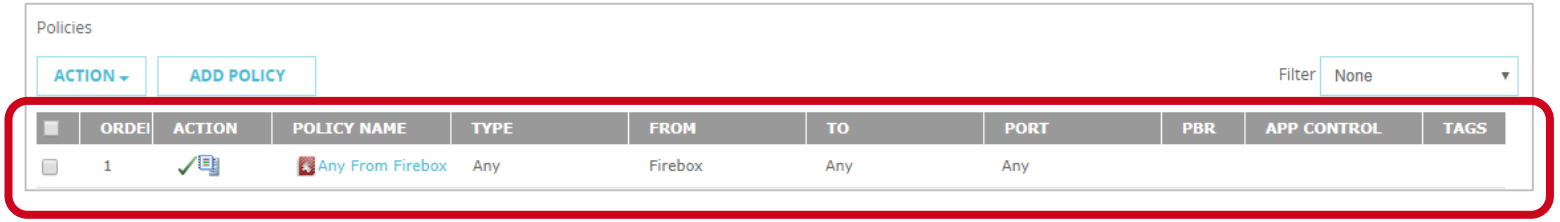


Control Firebox-Generated Traffic

- 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

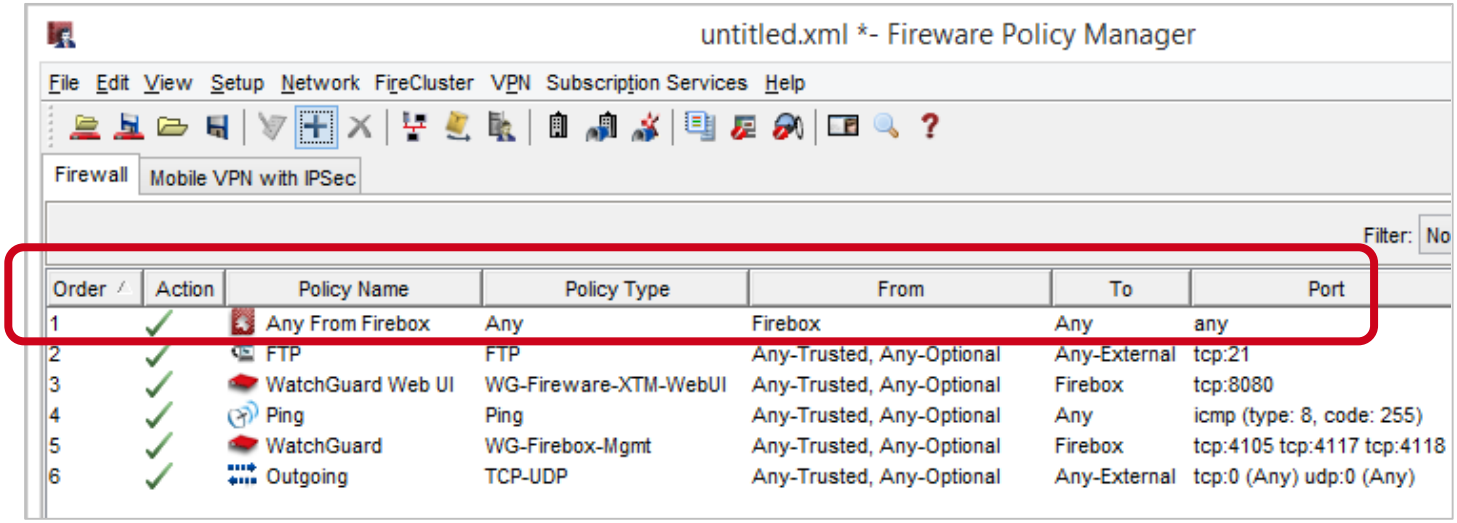
Control Firebox-Generated Traffic

- Web UI



Control Firebox-Generated Traffic

- Policy Manager



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

WatchGuard Training

AES-GCM Support

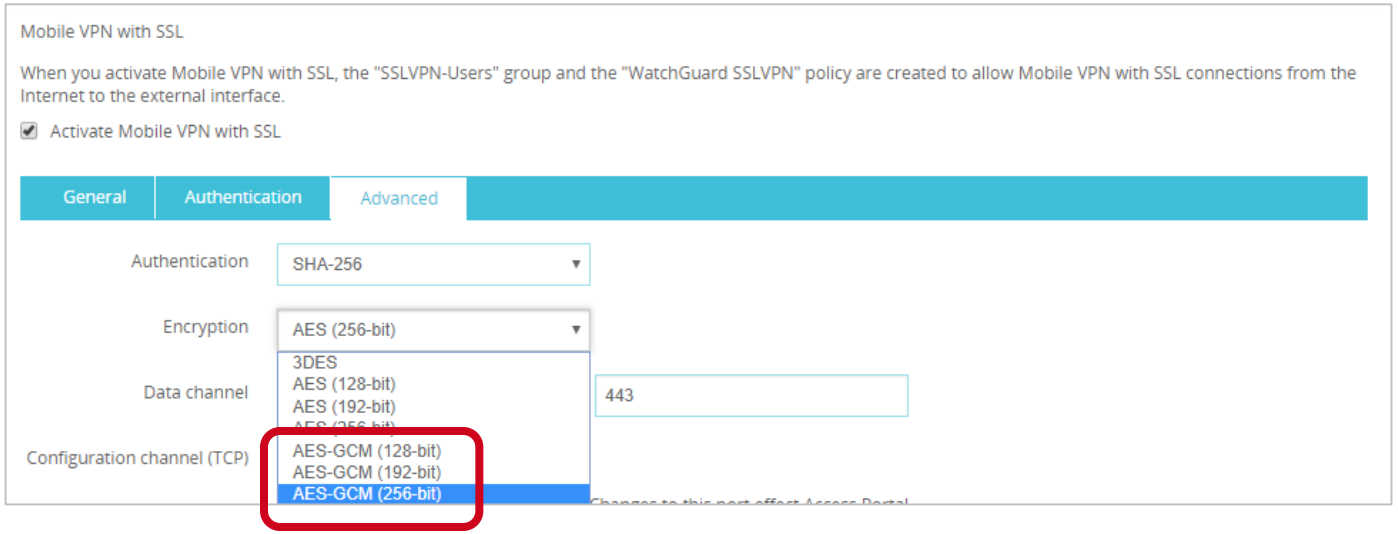
- Fireware now supports AES-GCM for IPSec and SSL/TLS VPN and mobile VPN tunnels
- GCM (Galois/Counter Mode) is an authenticated encryption algorithm known for its security, efficiency, and performance
  - Encryption and data integrity check occur simultaneously
  - Performance increases on Intel-based 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

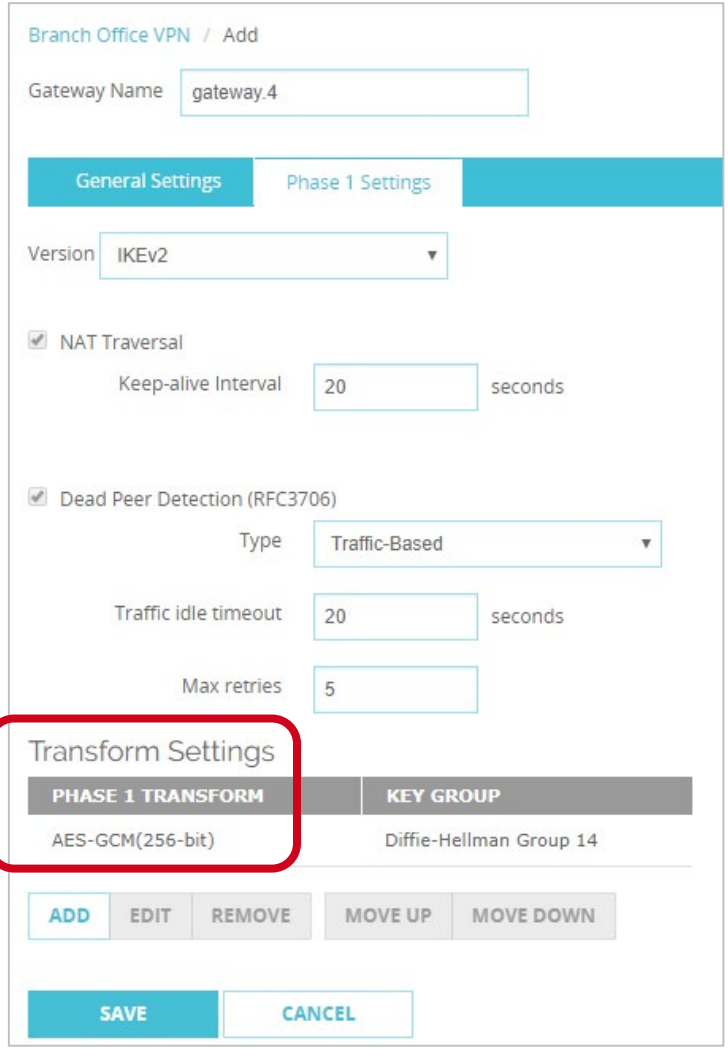
AES-GCM Support

- Mobile VPN example — Mobile VPN with SSL



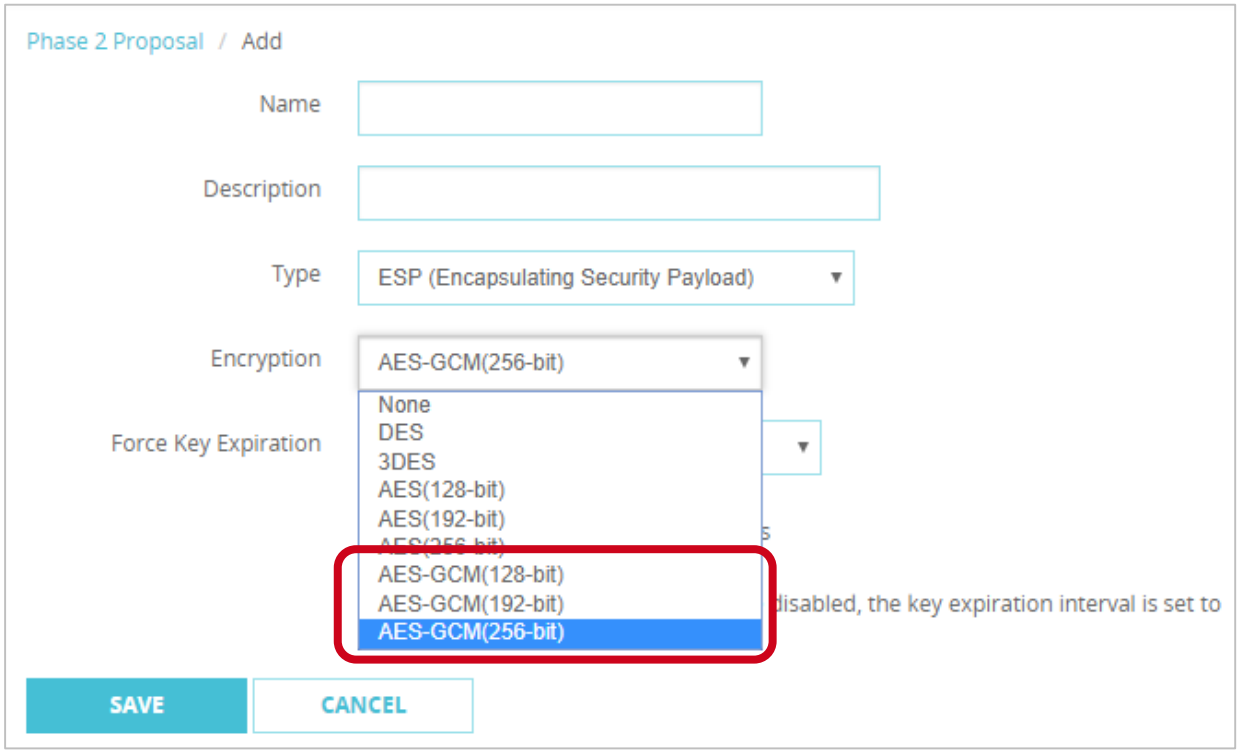
AES-GCM Support

- BOVPN example — Phase 1 settings



AES-GCM Support

- BOVPN example — Phase 2 settings



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

- Fireware 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

WatchGuard Training

Secondary IP Addresses for BOVPN Gateways

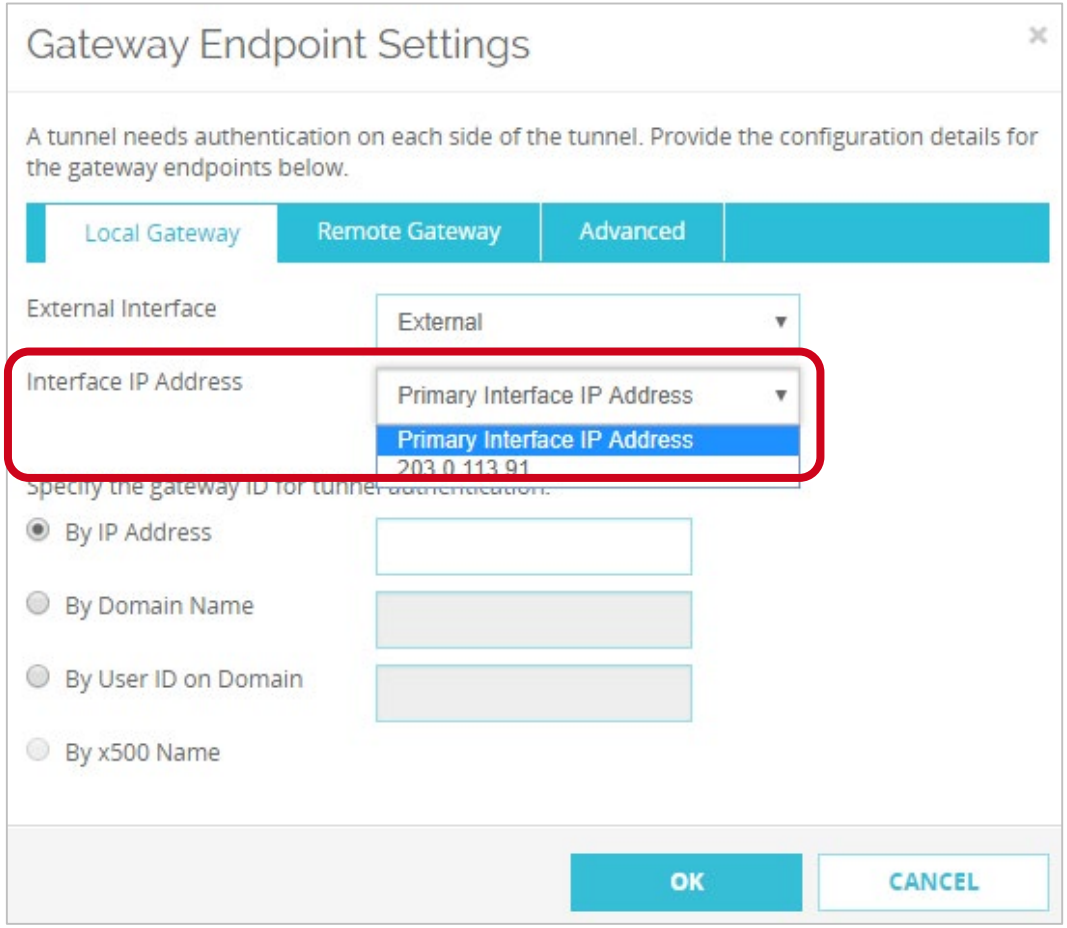
- To configure BOVPN and BOVPN virtual interface connections in more complex environments, you can now specify a secondary IP address as the local gateway IP address

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

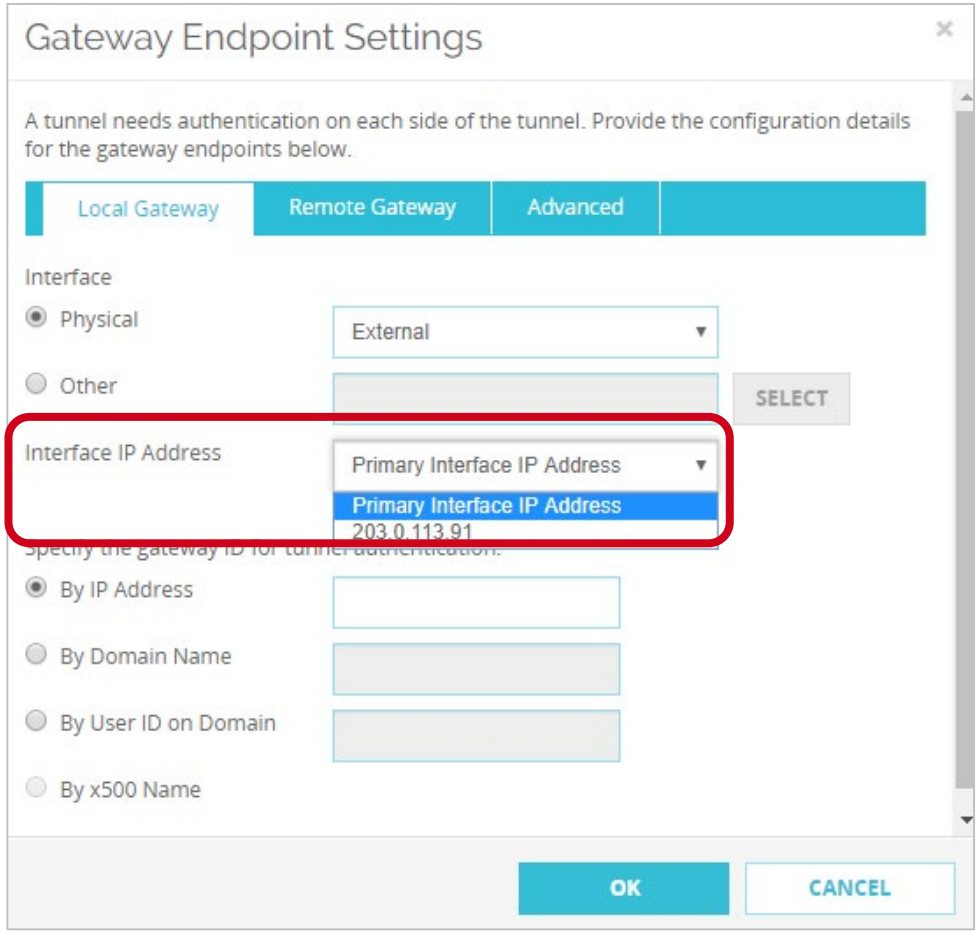
Secondary IP Addresses for VPN Gateways

- Web UI — BOVPN configuration



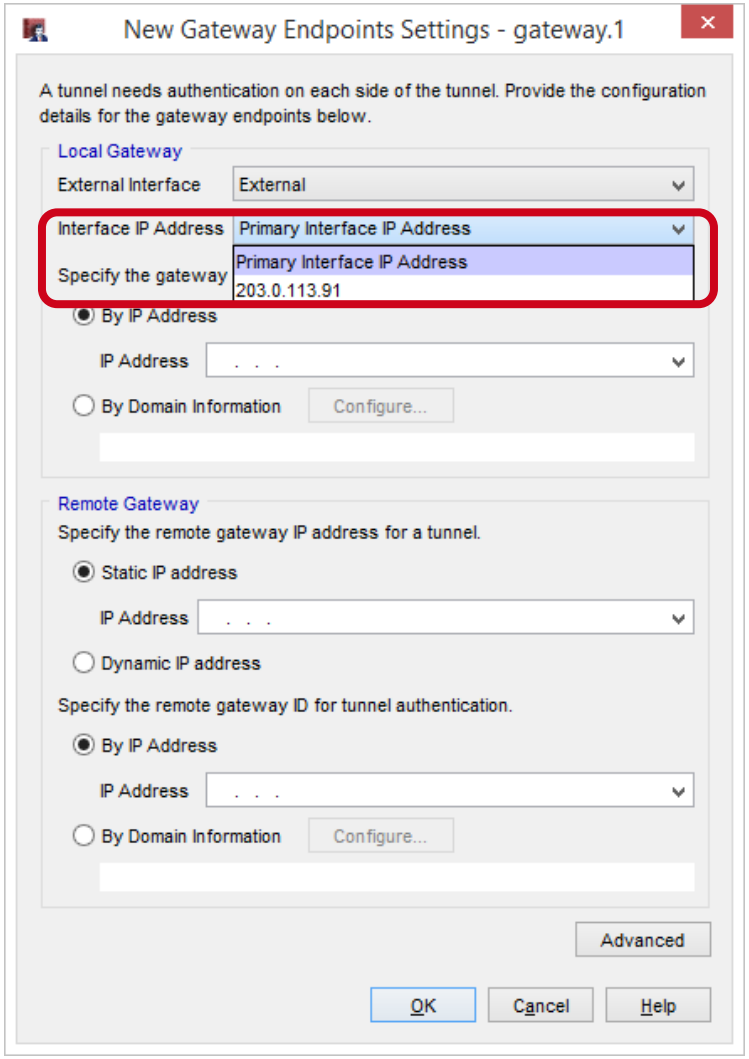
Secondary IP Addresses for VPN Gateways

- Web UI — BOVPN virtual interface configuration



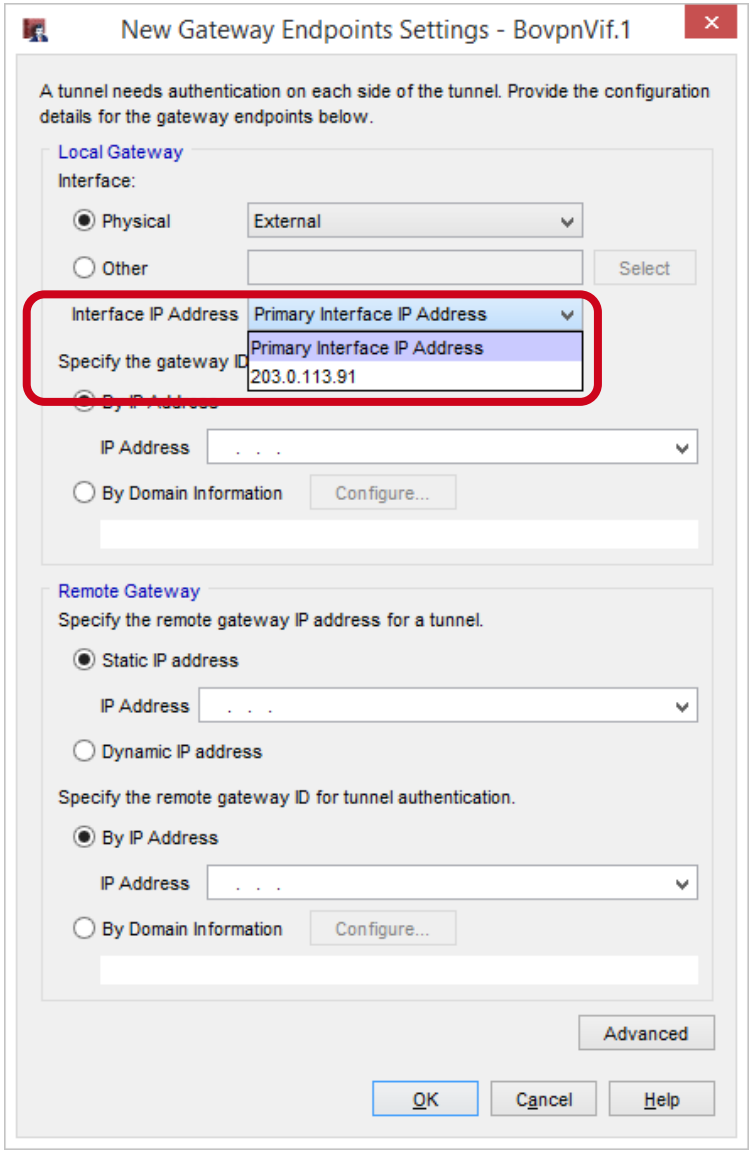
Secondary IP Addresses for VPN Gateways

- Policy Manager — BOVPN configuration



Secondary IP Addresses for VPN Gateways

- Policy Manager — BOVPN virtual interface configuration



Mobile VPN with SSL and Access Portal Settings

WatchGuard Training

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

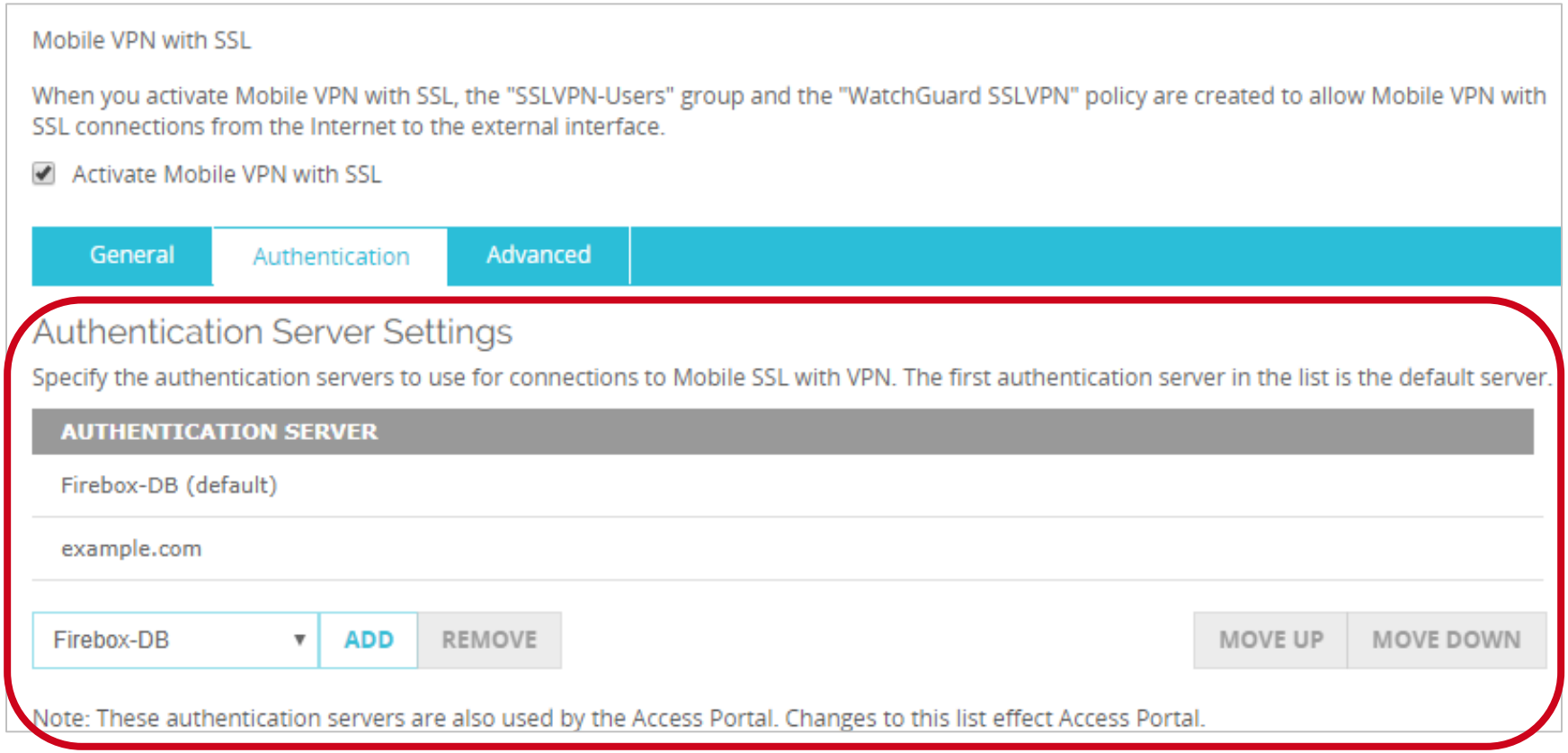
- Mobile VPN with SSL and the Access Portal continue to share these settings:
  - Authentication servers
  - Configuration Channel (known as the Access Portal Port in the Access Portal configuration)
- SSL/TLS settings precedence remains unchanged for Firebox features that share the same OpenVPN server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

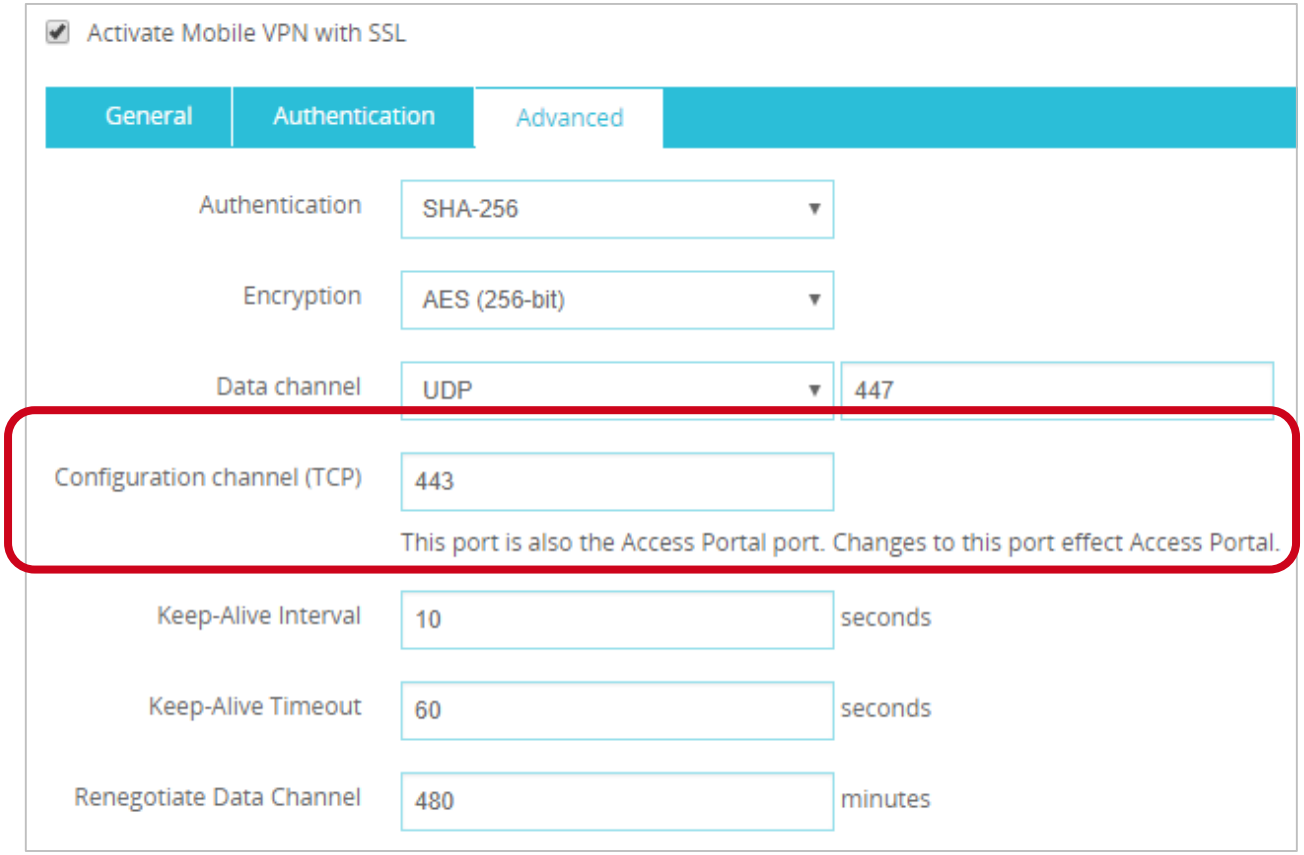
Mobile VPN with SSL & Access Portal

- Web UI — **Authentication Server Settings** list



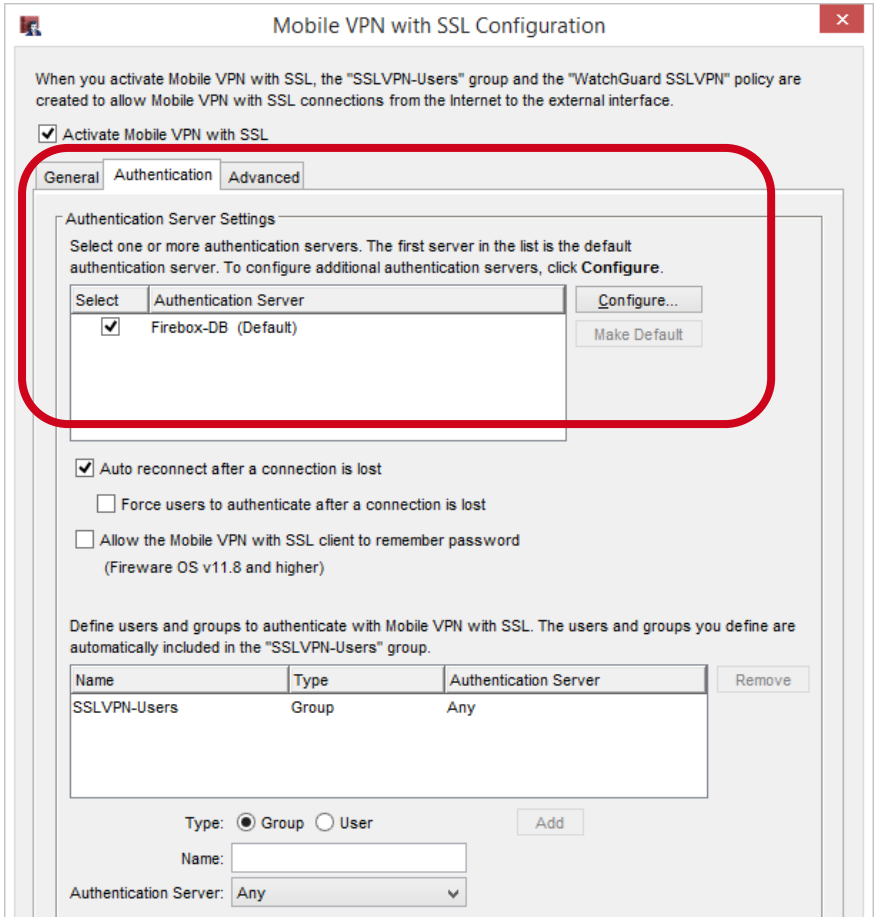
Mobile VPN with SSL & Access Portal

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



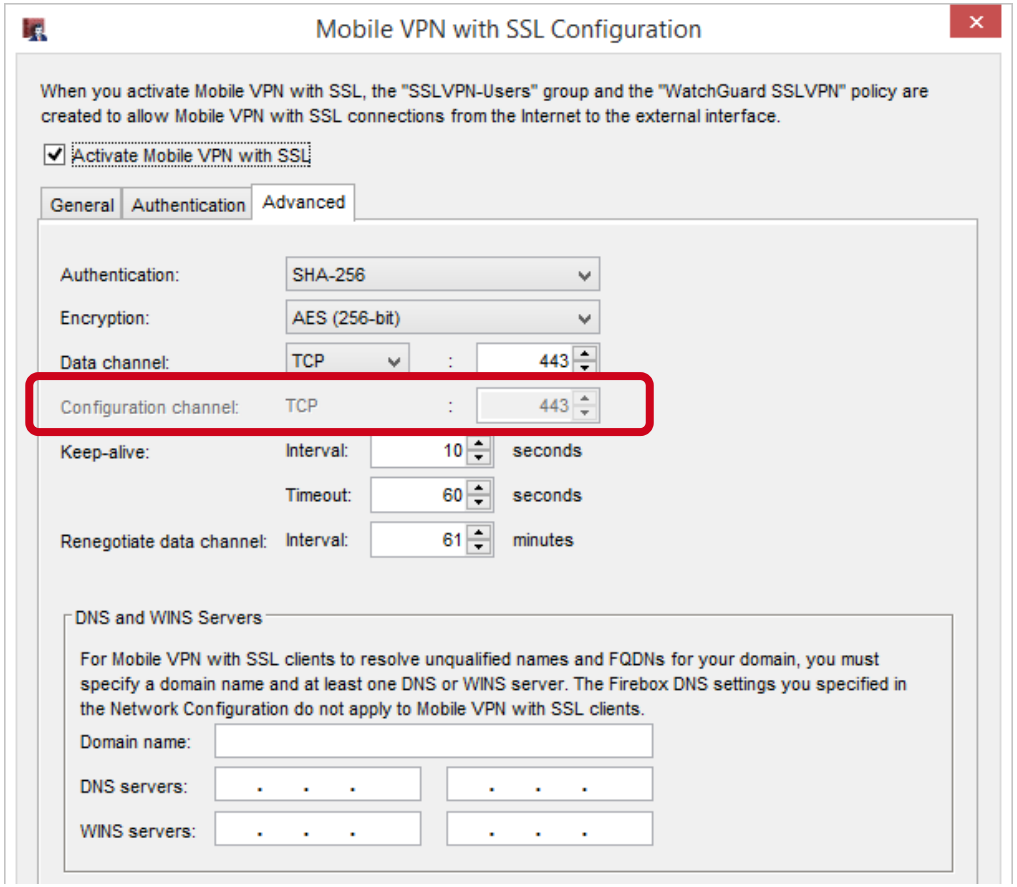
Mobile VPN with SSL & Access Portal

- Policy Manager — **Authentication Server Settings** list



Mobile VPN with SSL & Access Portal

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



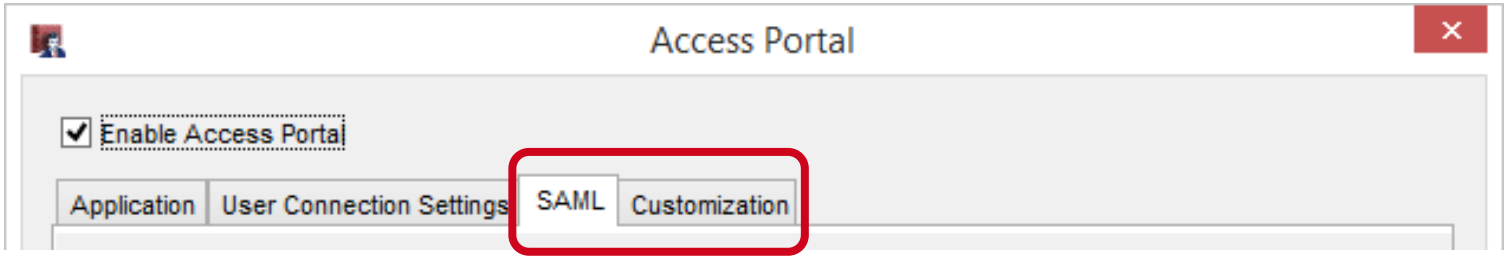
Mobile VPN with SSL & Access Portal

- 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

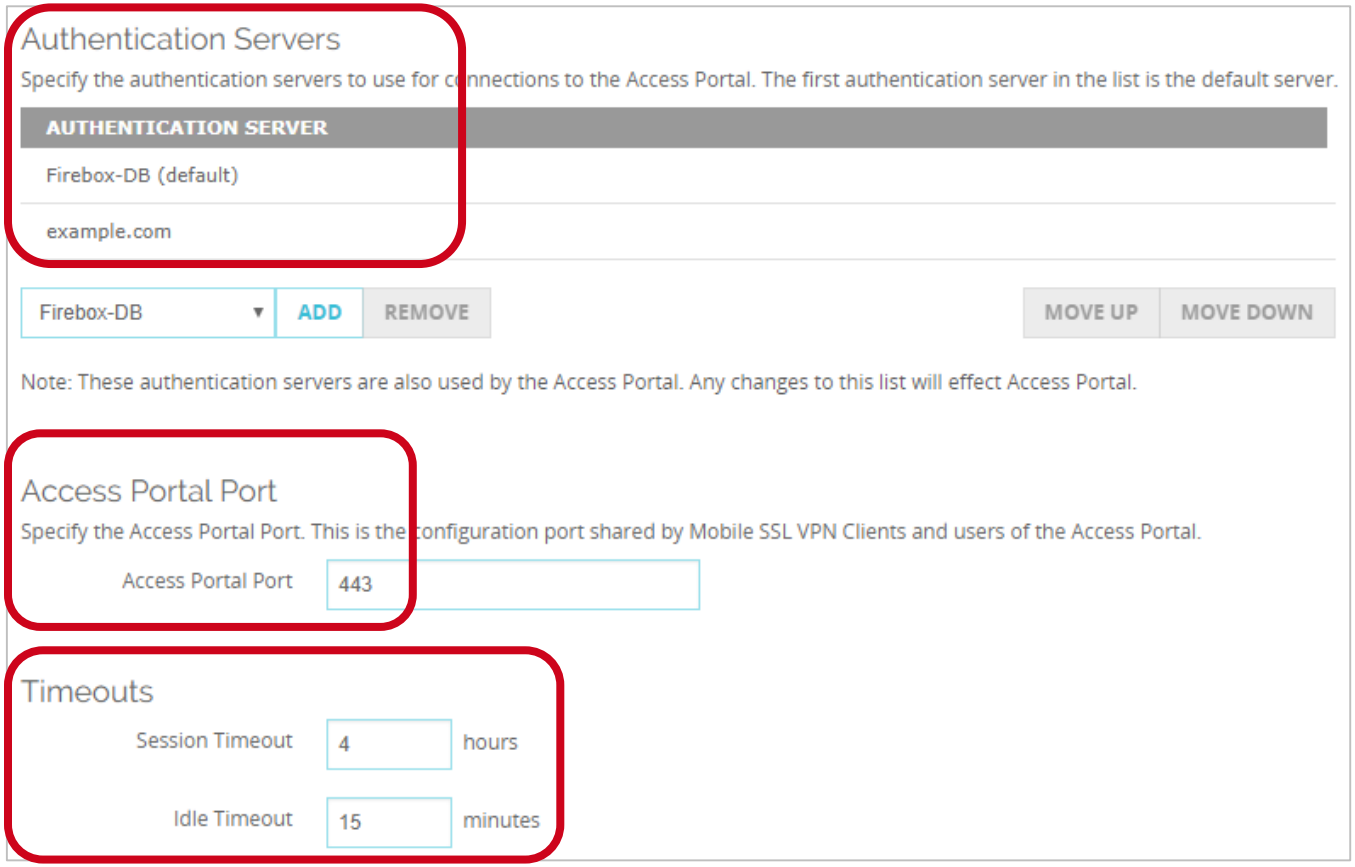
- Web UI — **SAML** and **Customization** tabs

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



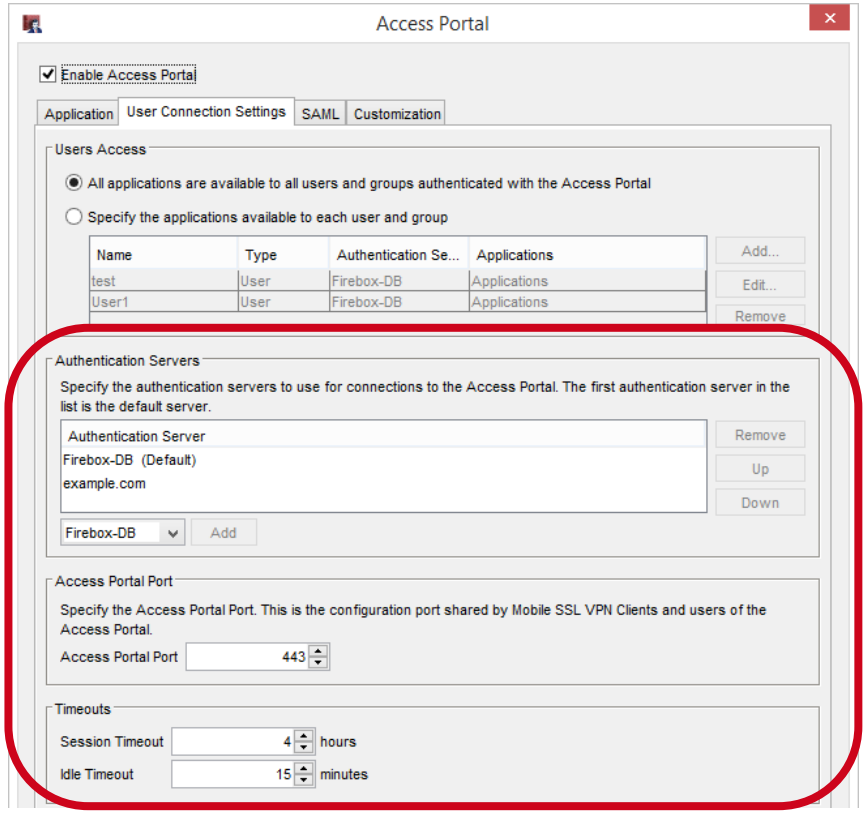
Mobile VPN with SSL & Access Portal

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



Mobile VPN with SSL & Access Portal

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



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

WatchGuard Training

Redundant Single Sign-On

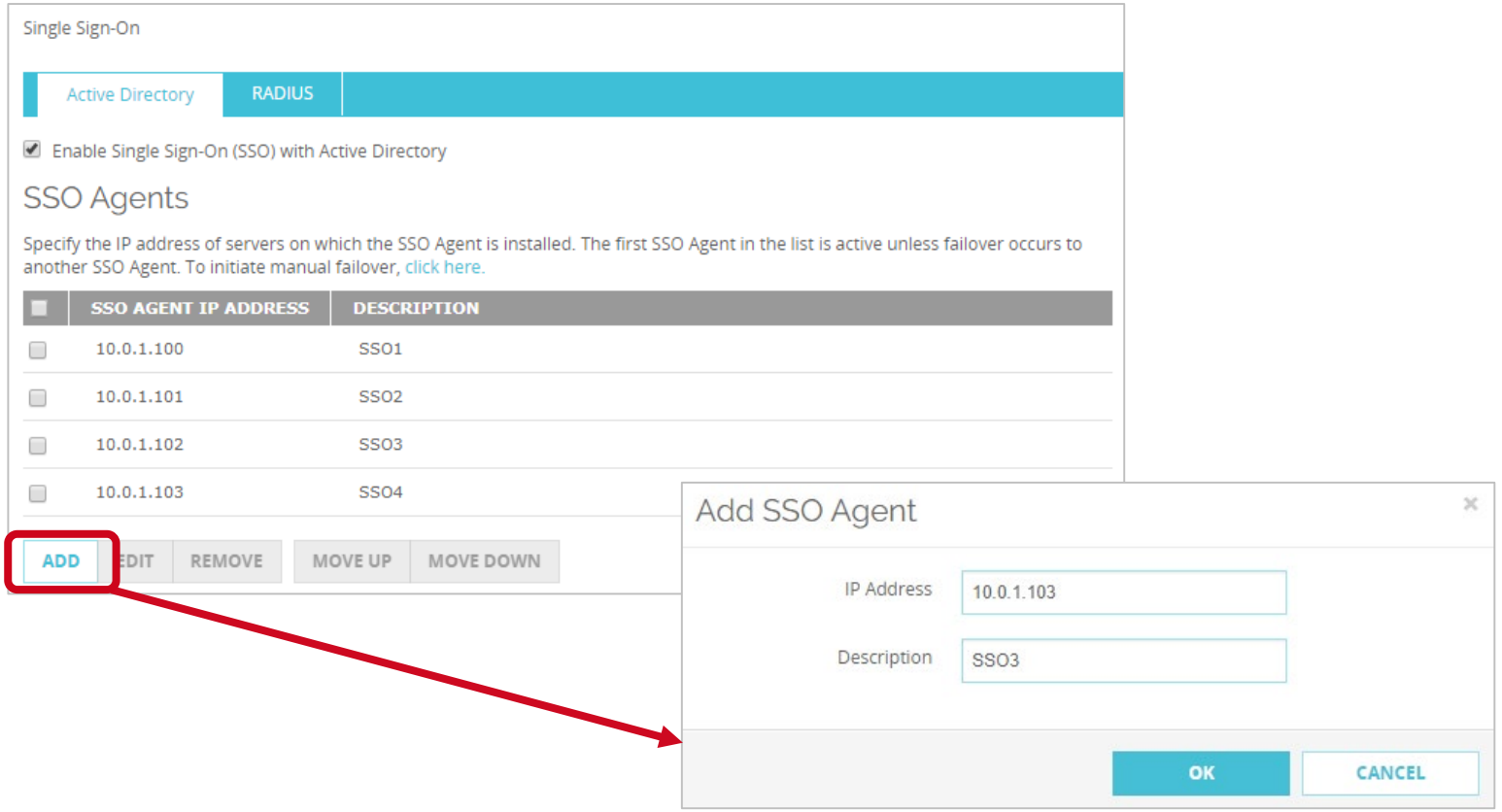
- To eliminate a single point of failure for Single Sign-On (SSO), you can now configure more than one SSO agent
- For example, you can install an SSO agent on a secondary domain controller so users can continue to authenticate if you must reboot the primary domain controller

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

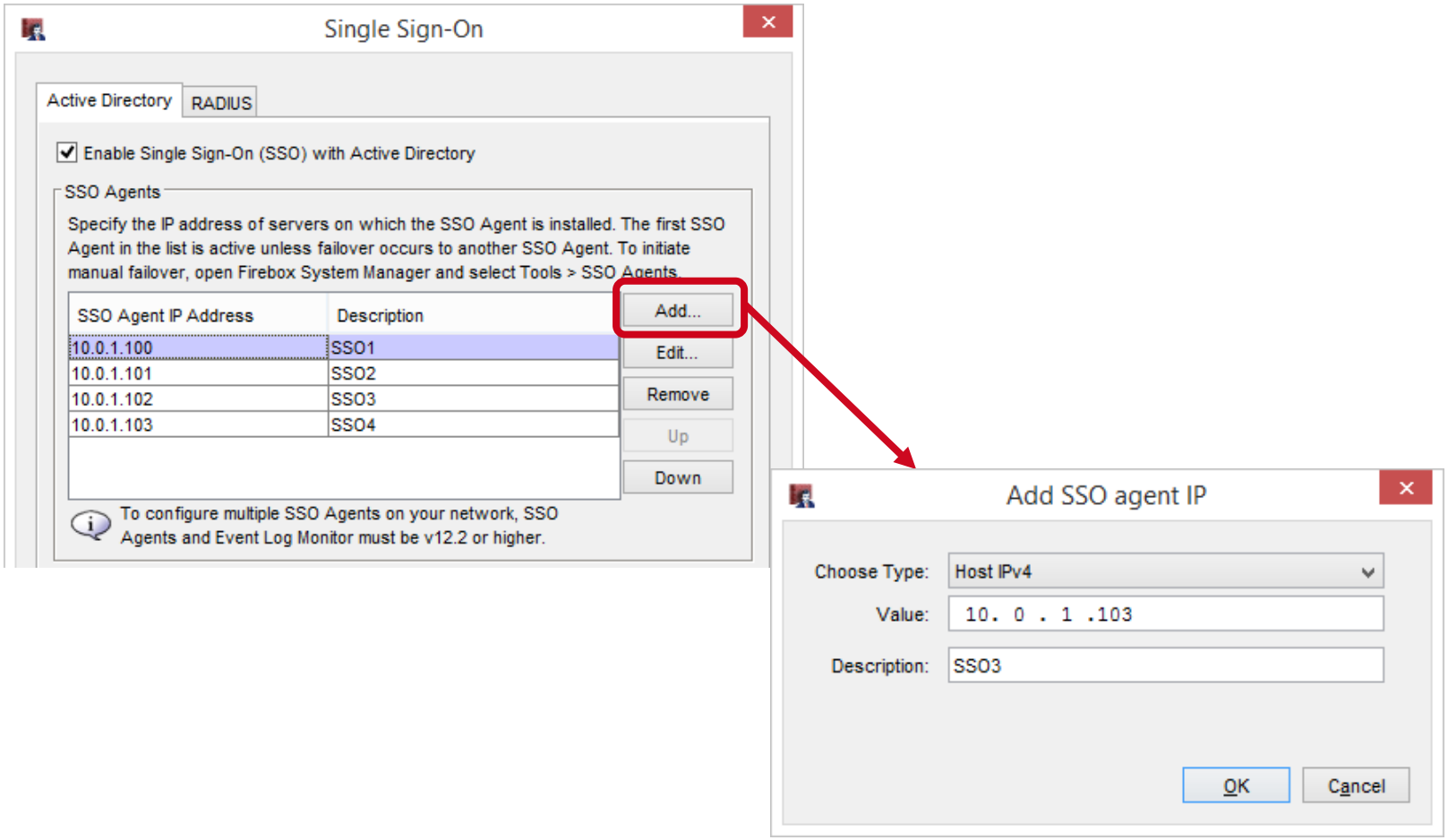
Redundant Single Sign-On

- Web UI — Add an SSO agent



Redundant Single Sign-On

- Policy Manager — Add an SSO agent

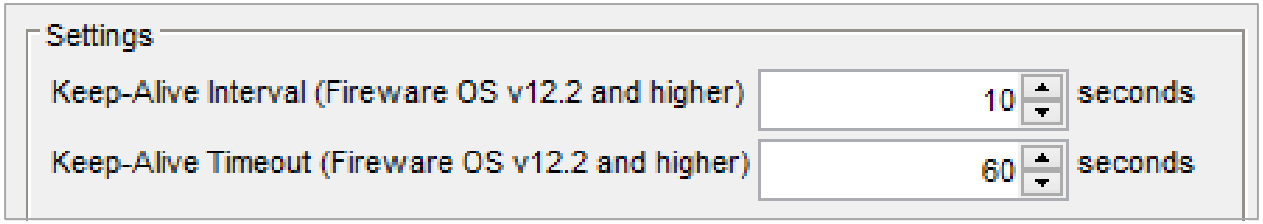


Redundant Single Sign-On

- 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



Redundant Single Sign-On

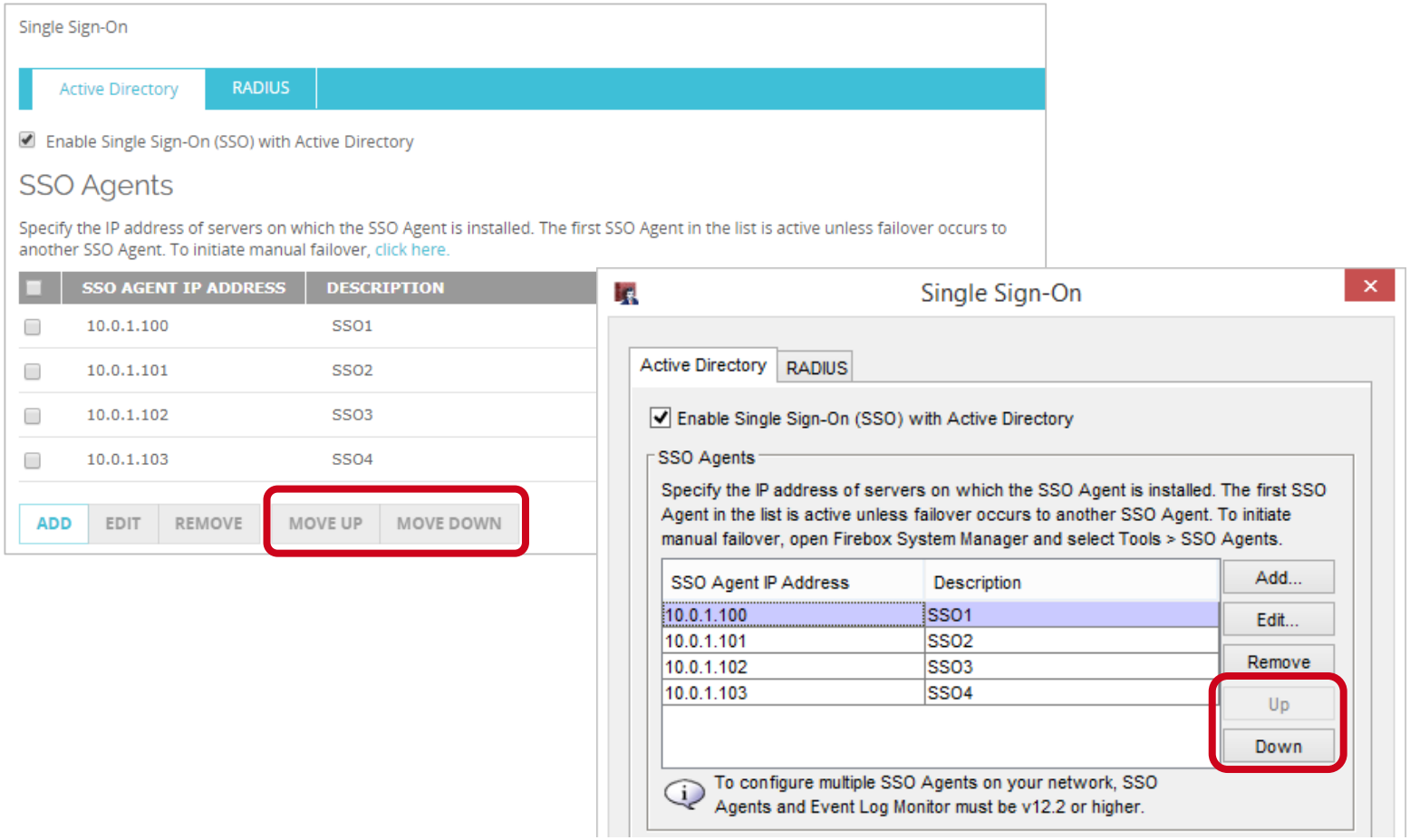
- Failover to a different SSO agent occurs automatically when:
  - The connection to an SSO agent is lost or closed
  - The SSO agent does not respond to keep-alive messages in the specified amount of time
  - You remove the SSO agent from the Firebox configuration
  - You manually initiate a failover 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.

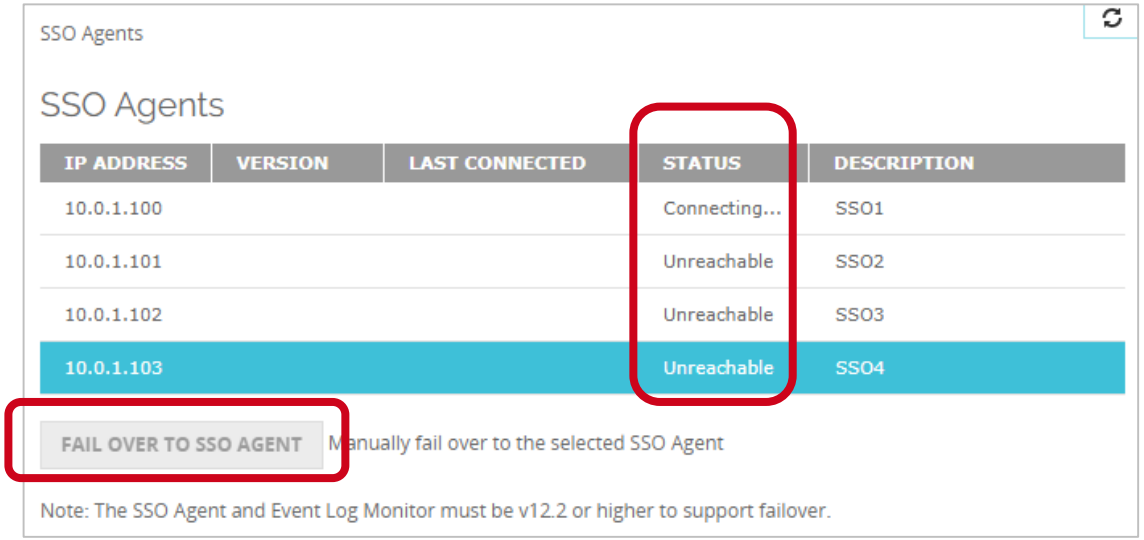
Redundant Single Sign-On

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



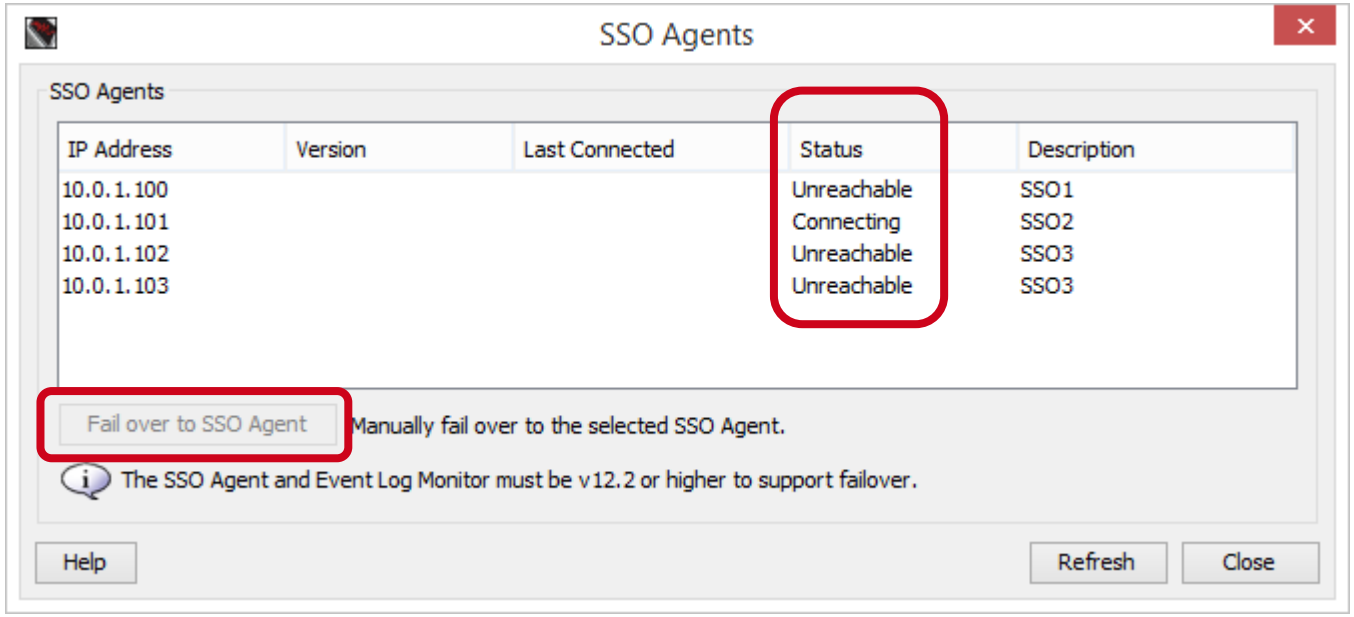
Redundant Single Sign-On

- 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**



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

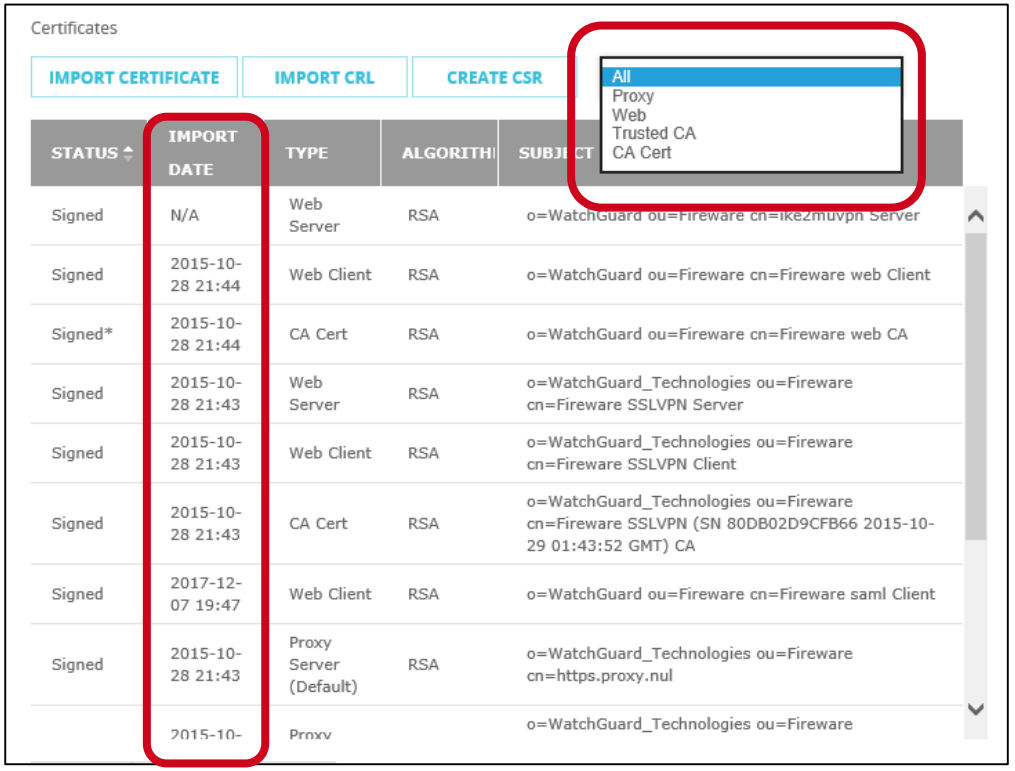
Certificate Management Enhancements

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

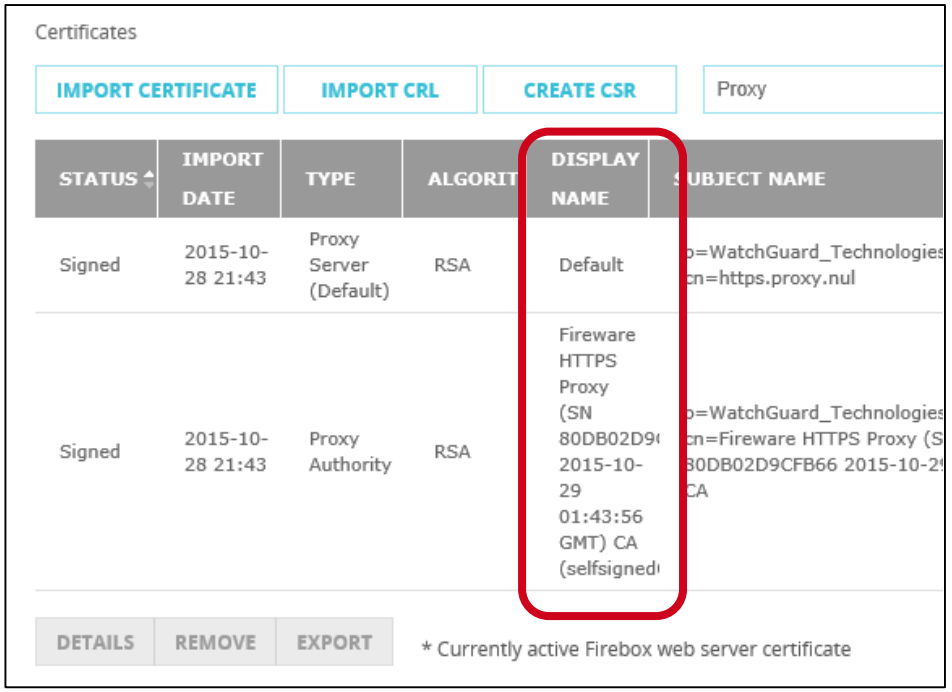
Certificate Management Enhancements

- 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



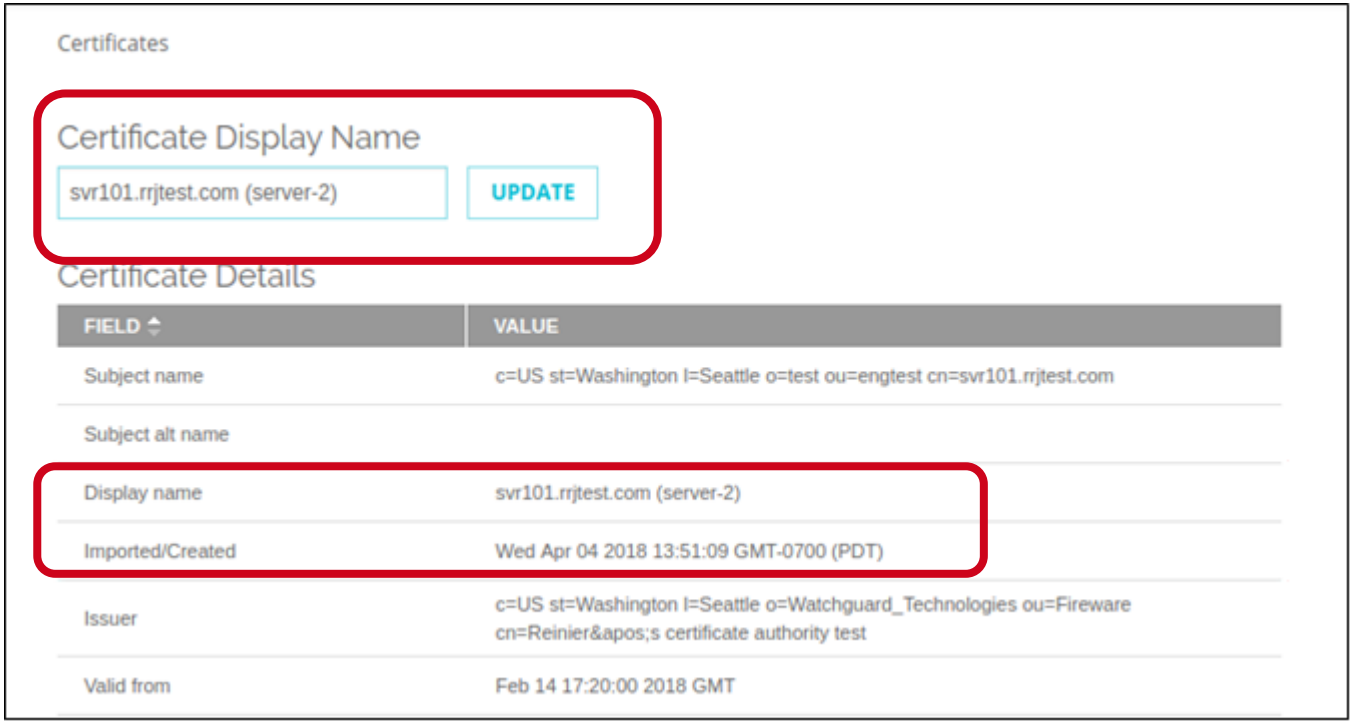
Improved Certificate Management

- 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



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

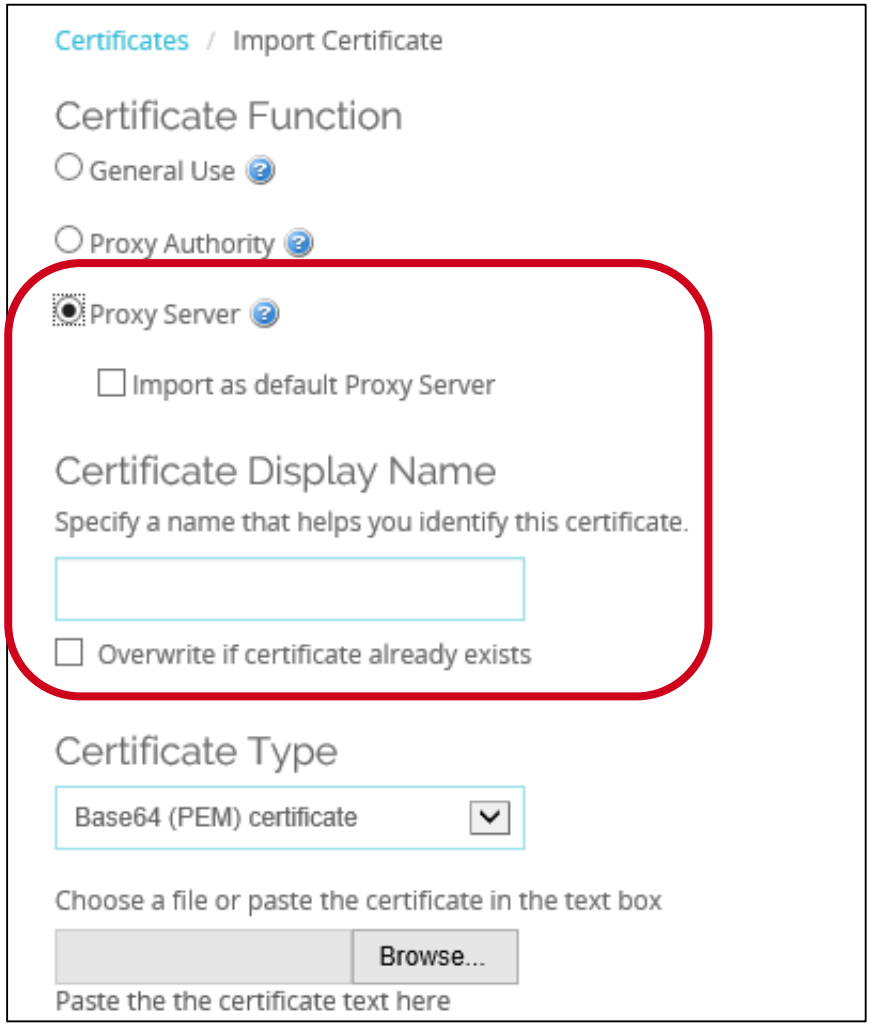


Certificate Import Enhancements

- 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



Certificate Import Enhancements

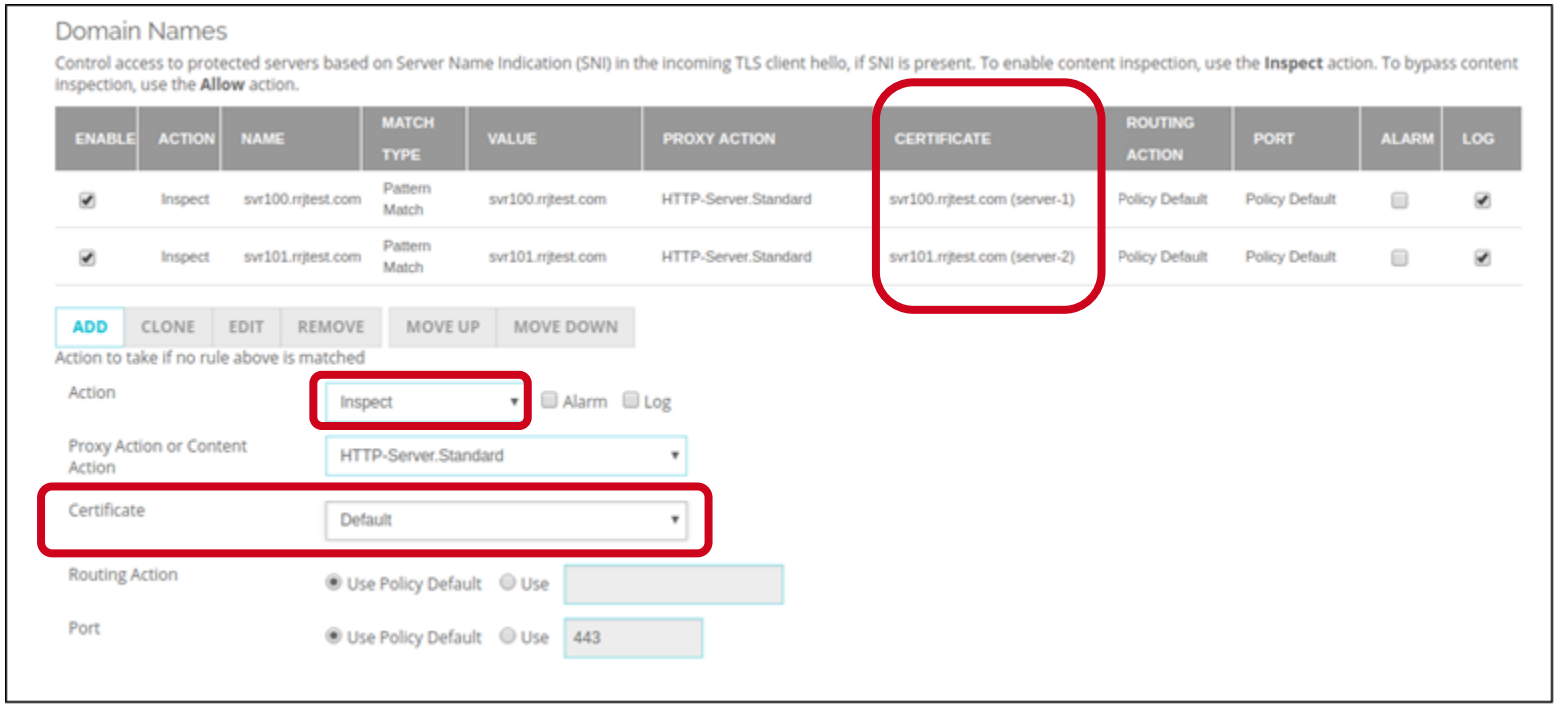
- **Certificate Display Name** and **Overwrite if certificate already exists** check box
  - Only visible when you import a Proxy Server certificate
  - Select **Overwrite** if the certificate to import will overwrite a certificate with the same display name
  - If **Overwrite** is not selected, you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

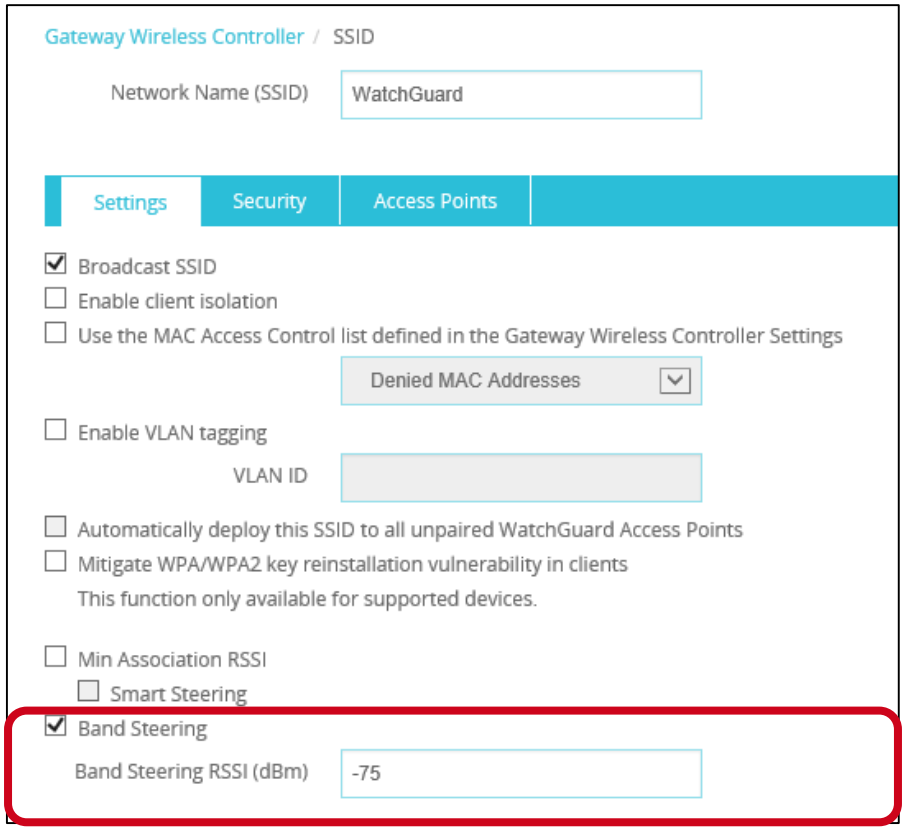
- Certificates are assigned to inbound HTTPS proxy domain name rules
- When you edit domain name rules, you can use a new **Certificate** drop-down list when the action is **Inspect**



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



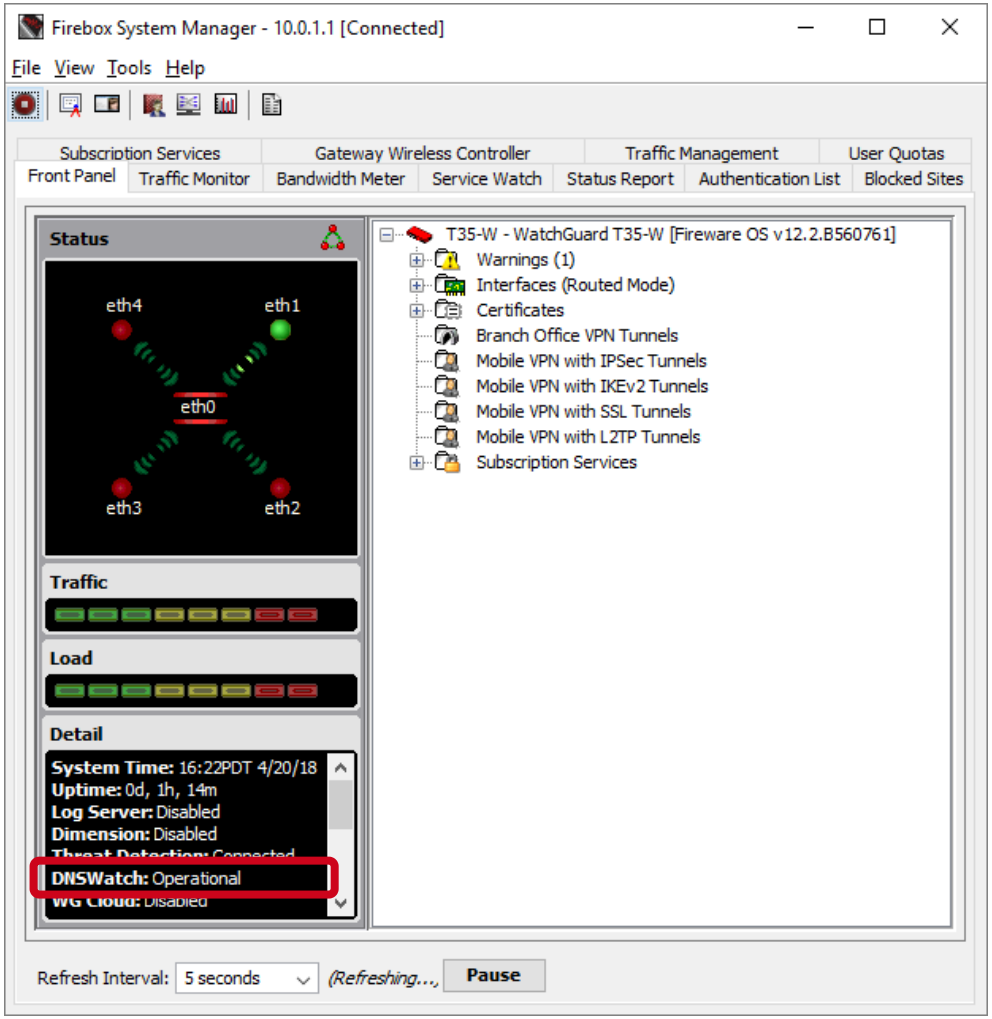
AP125 Support

- 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

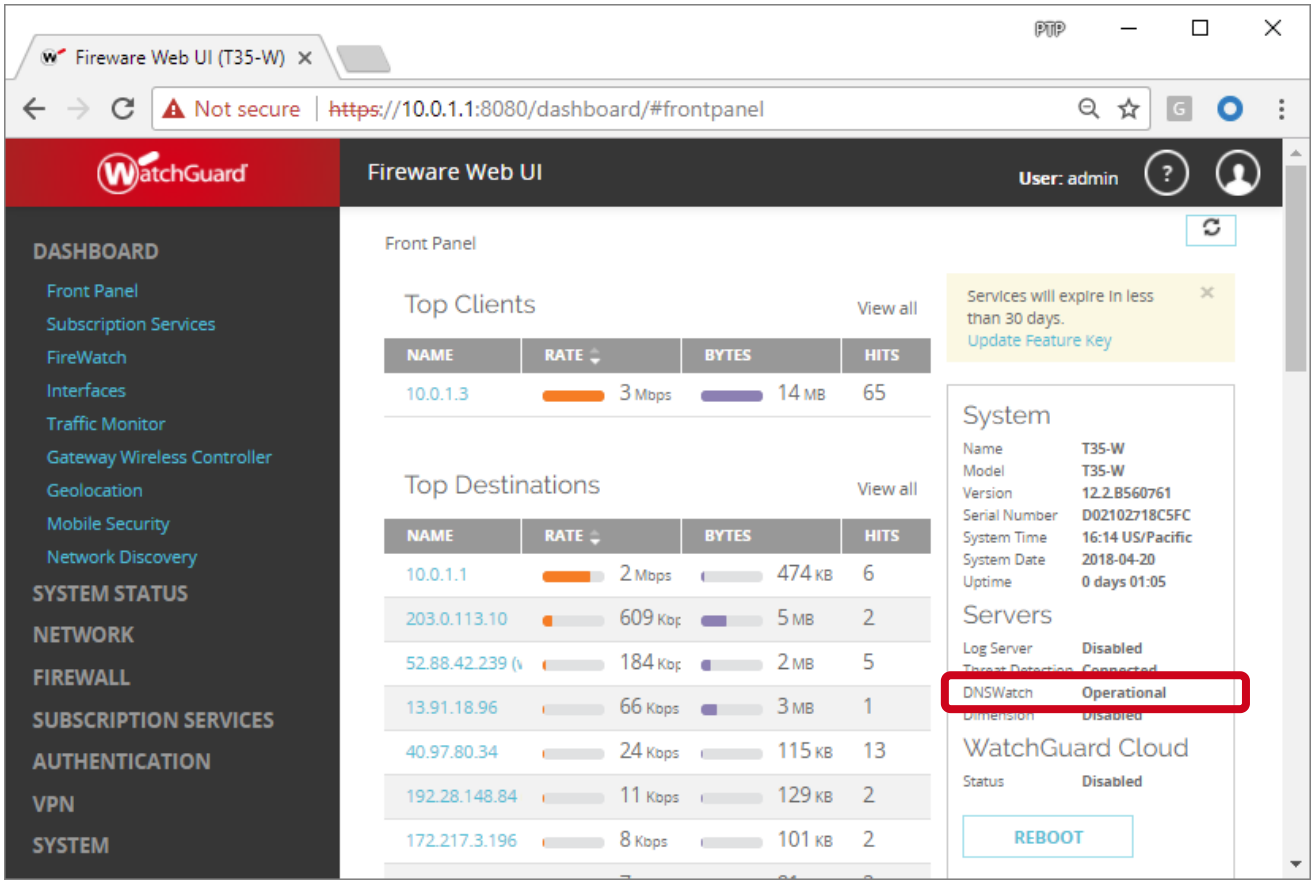
DNSWatch Status in FSM Front Panel

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



DNSWatch Status in Web UI Front Panel

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



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!