What's New in Fireware v12.2.1

WatchGuard Training

What's New in Fireware v12.2.1

- DNS enhancements for mobile VPN
- WAN interface monitors
- Loopback IP address support
- Certificate management enhancements
- DF bit setting for BOVPN gateways
- Password length control for Firebox-DB accounts
- Gateway Wireless Controller enhancements
- Backup and restore enhancements

What's New in Fireware v12.2.1

- SafeSearch enforcement level for YouTube
- Deny action added for Gateway AV & VOD in SMTP proxy
- WebBlocker usability updates
- WatchMode updates (for WatchGuard Partners only)
- WatchGuard IPSec Mobile VPN Client updates
- File Exceptions statistics

DNS Enhancements for Mobile VPN

WatchGuard Training

DNS Enhancements for Mobile VPN

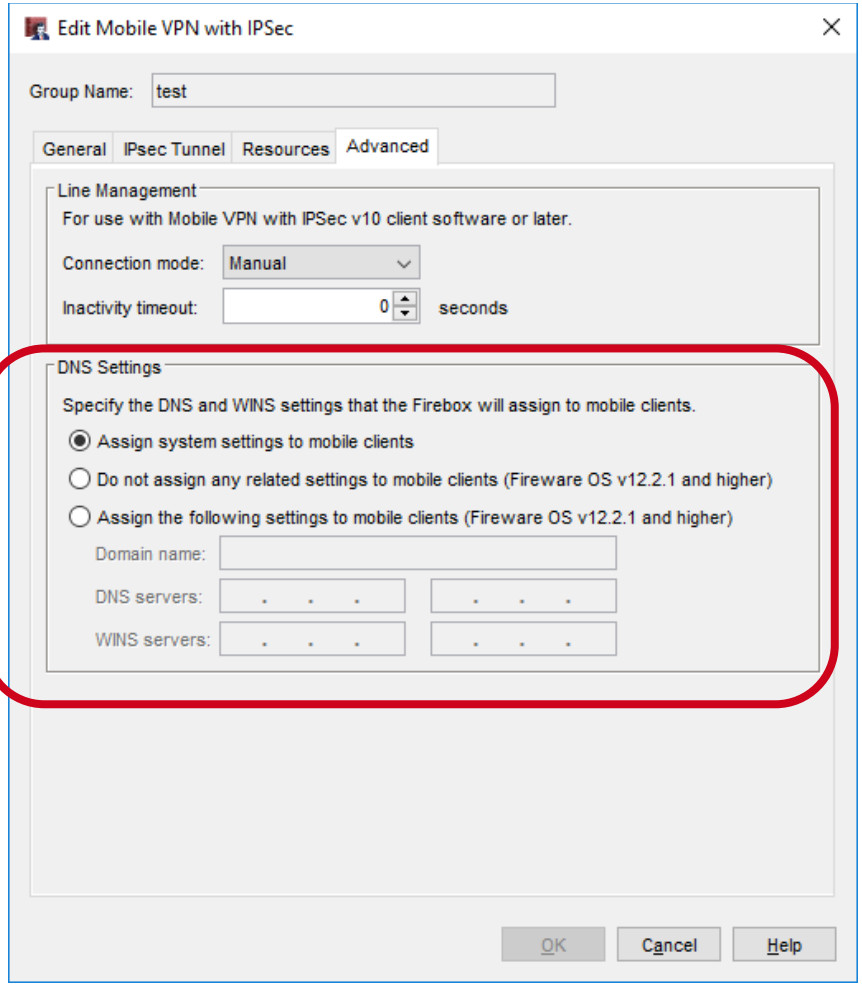
- You can now configure more granular DNS settings for different types of Mobile VPN
- Makes it easier to handle segmented networks
- Provides a more flexible solution to address mobile VPN corner cases

DNS Enhancements for Mobile VPN

- You can now configure these settings in the IPSec, IKEv2, and L2TP mobile VPN configurations:
  - Mobile IPSec – DNS servers, WINS servers, domain name
  - Mobile IKEv2 – DNS servers, WINS servers
  - Mobile L2TP – DNS servers
- In all mobile VPN configurations, you can now select to:
  - Assign or not assign the Network (global) DNS/WINS settings to mobile clients
  - Assign settings specified in the mobile VPN configuration to mobile clients

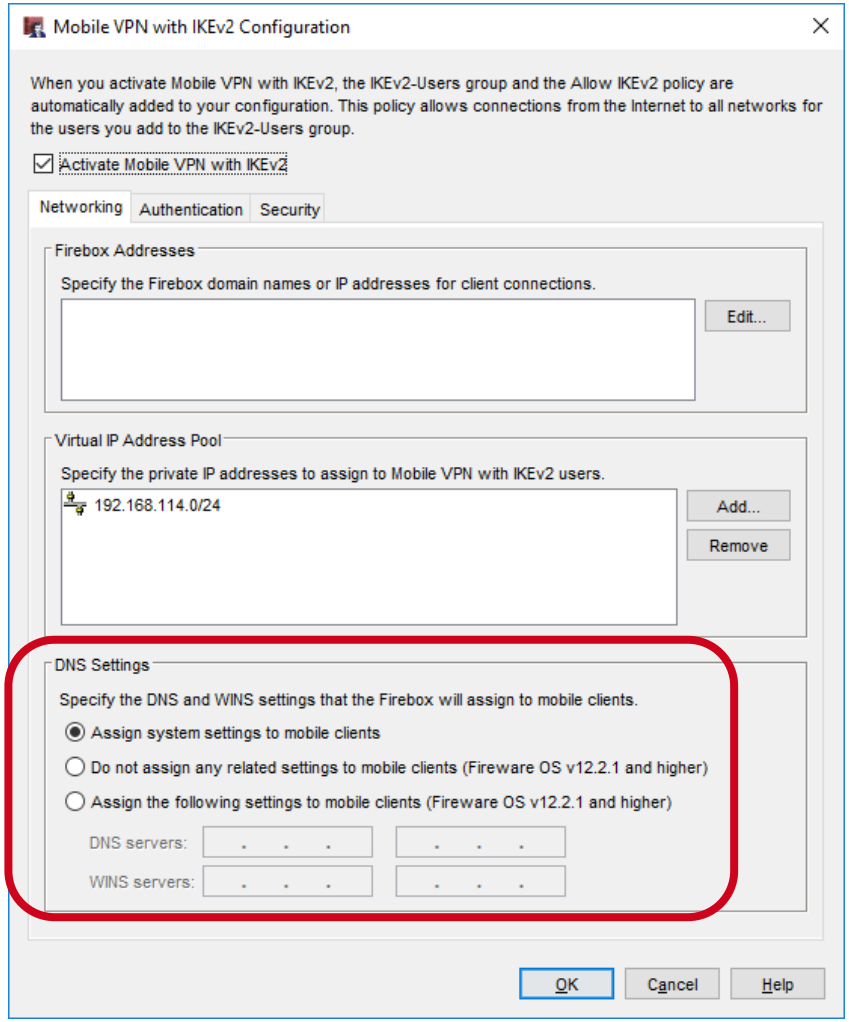
DNS Enhancements for Mobile VPN

- In the Mobile VPN with IPSec configuration, you can specify DNS and WINS servers, and a domain name



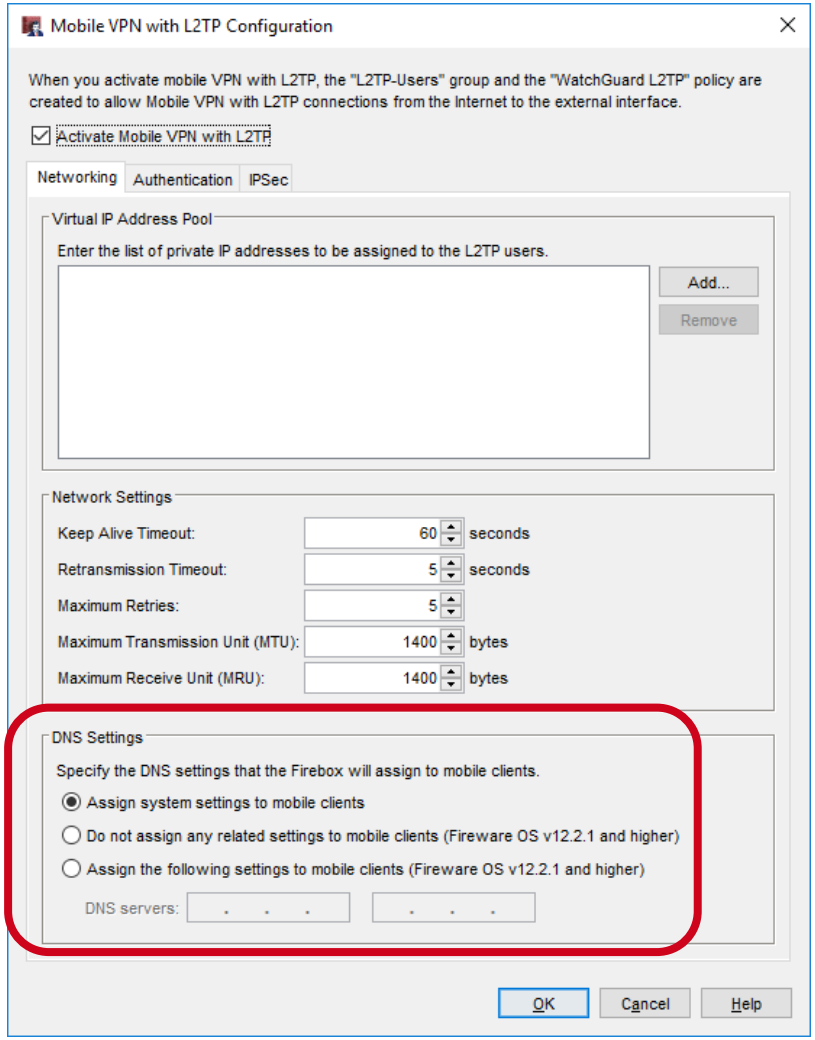
DNS Enhancements for Mobile VPN

- In the Mobile VPN with IKEv2 configuration, you can specify DNS and WINS servers, but not a domain suffix



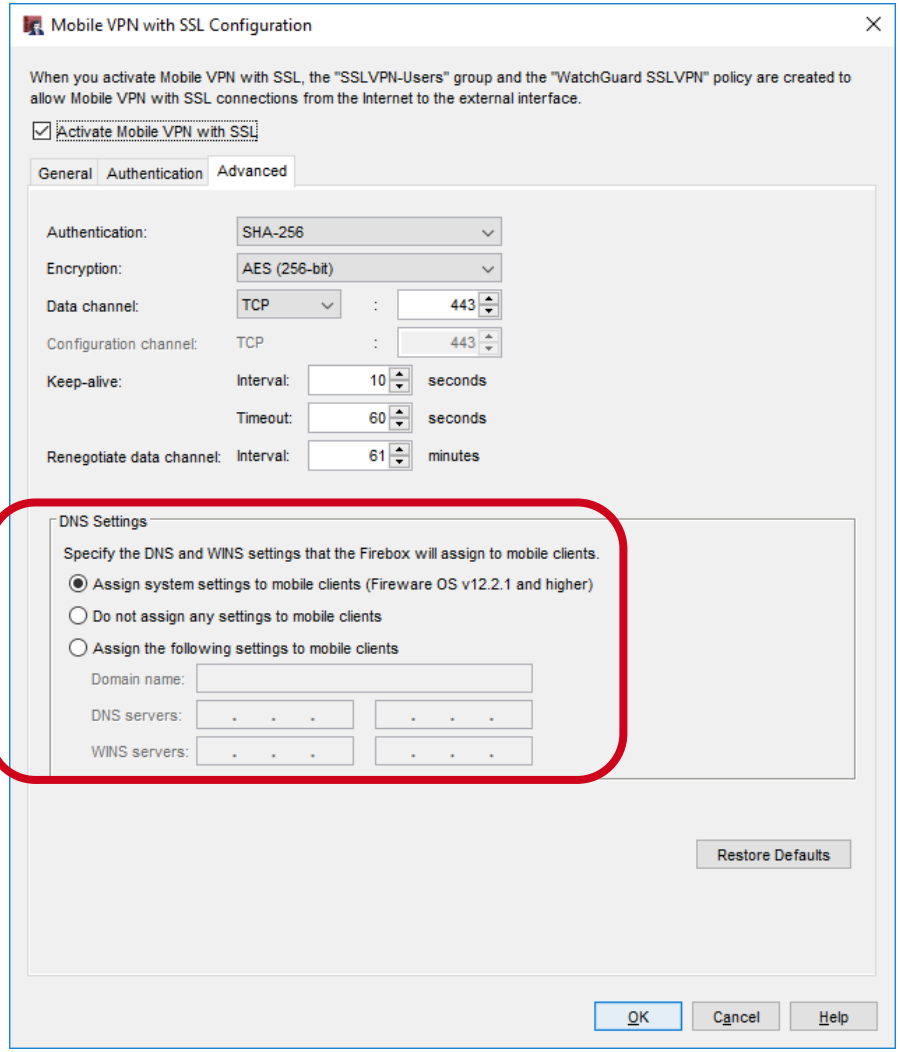
DNS Enhancements for Mobile VPN

- In the Mobile VPN with L2TP configuration, you can specify DNS servers, but not WINS servers or a domain suffix



DNS Enhancements for Mobile VPN

- In the Mobile VPN with SSL configuration, DNS, WINS, and domain name settings that appear in Fireware v12.2 or lower remain
- In the DNS Settings section, only the radio button options are new in Fireware v12.2.1



DNS Enhancements for Mobile VPN

- If you select the **Assign the Network DNS/WINS Server settings to mobile clients**, mobile VPN clients receive the settings configured in the Network (global) DNS/WINS settings
- For example, if you specify the DNS server 203.0.113.50 in the Network DNS settings, mobile VPN clients receive 203.0.113.50 as a DNS server
  - Network DNS/WINS settings appear in these locations:
    - In Fireware Web UI: **Network** > **Interfaces** > **DNS/WINS**
    - In Policy Manager: **Network** > **Configuration** > **DNS/WINS**
- By default, the **Assign the Network DNS/WINS Server settings to mobile clients** setting is selected for new mobile VPN configurations

DNS Enhancements for Mobile VPN

- If you select the **Assign these settings to mobile clients** option, you can specify these settings:
  - DNS servers
  - WINS servers (Mobile VPN with IPSec, SSL, and IKEv2 only)
  - Domain name suffix (Mobile VPN with IPSec and SSL only)
- Settings are not inherited from the global Network DNS settings if you select the **Assign these settings to mobile clients** option
  - For example, if you select this option and only specify a DNS server, clients only receive the DNS server. If a WINS server and domain name are configured in the Network DNS settings, clients do not receive those settings.

DNS Enhancements for Mobile VPN

- Mobile VPN with SSL configuration conversion
  - If your configuration does not specify DNS, WINS, or domain name settings, after you upgrade to Fireware v12.2.1, the **Do not assign DNS or WINS settings to mobile clients** option is selected

WAN Interface Monitors

WatchGuard Training

WAN Interface Monitors

- View loss, latency, and jitter for WAN interfaces to better understand WAN network performance
- The first of several new SD-WAN related features planned for upcoming Fireware releases
- For example, in a future release, you will be able to use this new monitoring functionality to configure actions for policy failover

WAN Interface Monitors

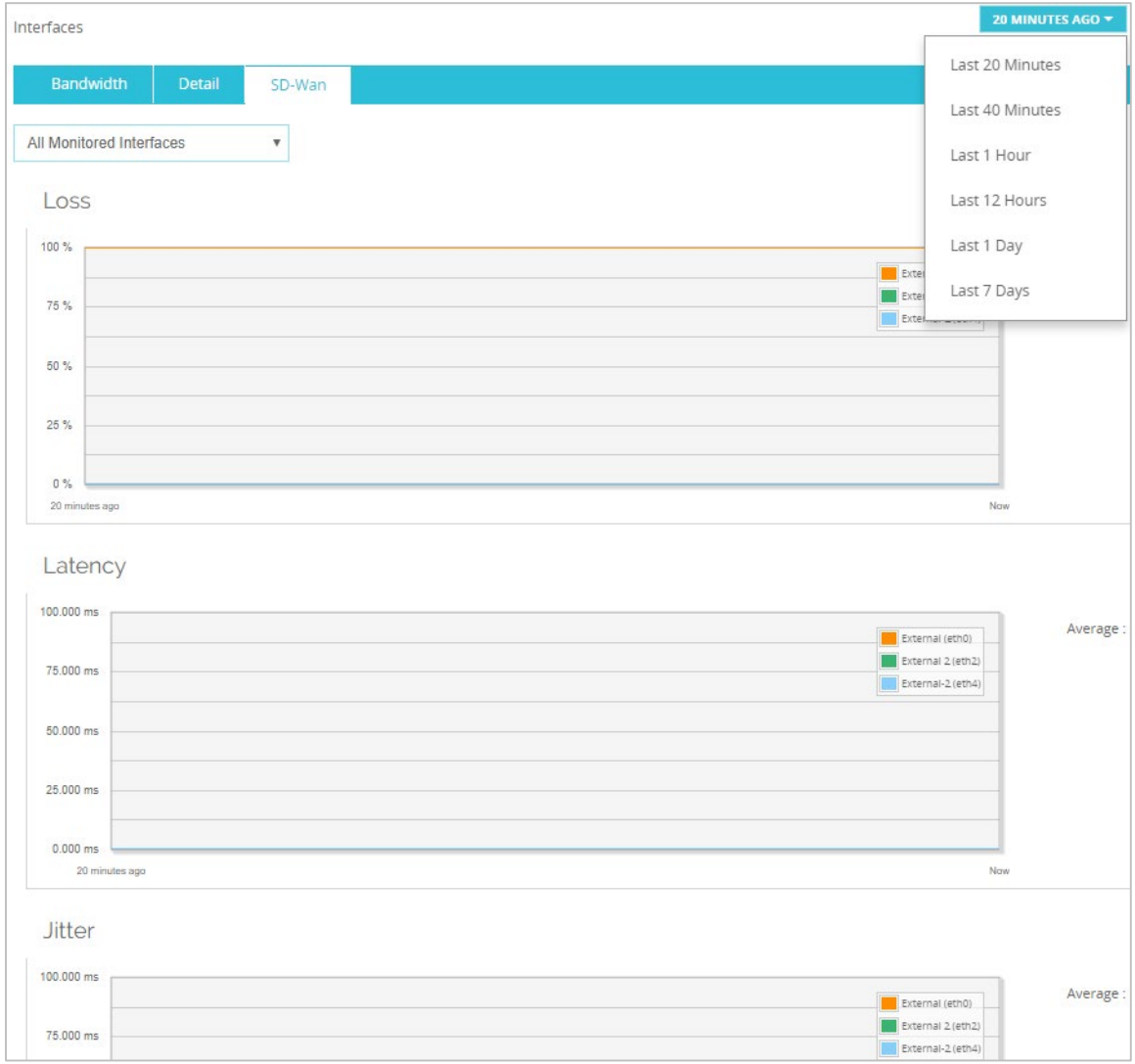
- You can now monitor WAN interfaces on the Firebox for:
  - **Loss** — Percentage of packets lost
  - **Latency** — Packet delivery delay, measured in milliseconds (ms)
  - **Jitter** — Difference in packet delivery delay, measured in ms
- To see data for a WAN interface, you must configure the interface as a multi-WAN member and enable link monitor
  - Data is based on responses from link monitor targets
  - For meaningful data, specify a target other than the default gateway
- Fireware Web UI shows historical data
- Firebox System Manager shows real-time data

WAN Interface Monitors

- Data appears in a graph here:
  - Web UI — **Dashboard > Interfaces > SD-WAN**
  - Firebox System Manager — **SD-WAN** tab

WAN Interface Monitors

- Web UI

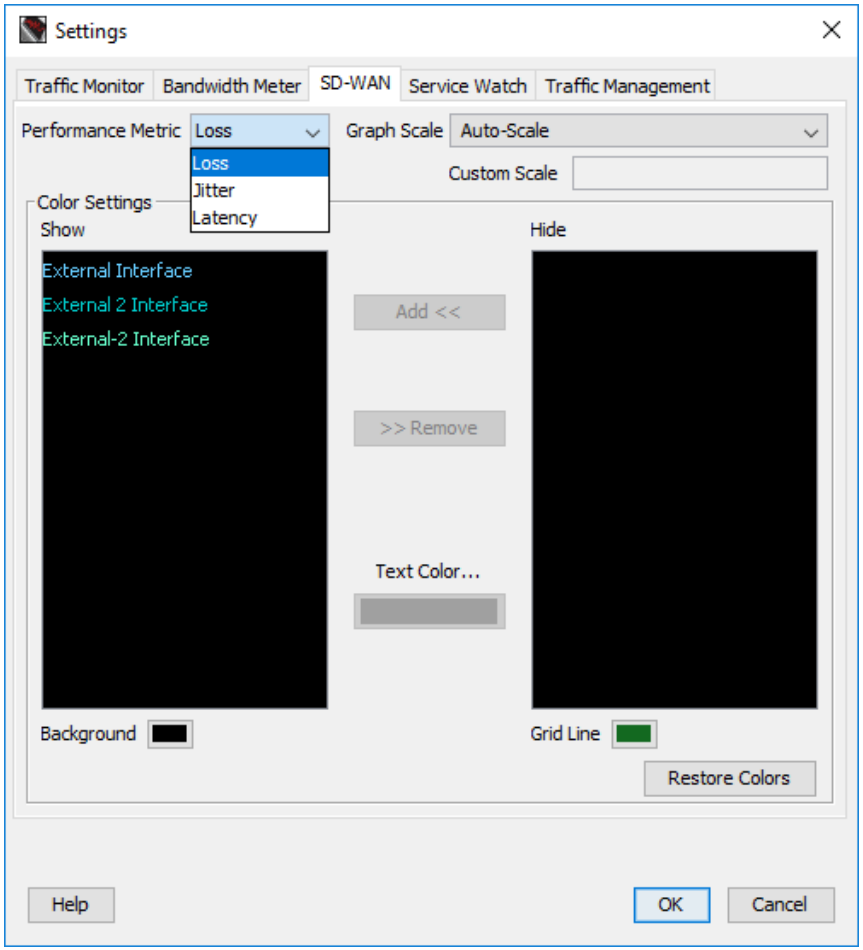


WAN Interface Monitoring Enhancements

- To customize Web UI graph, you can:
  - Select to show data for all monitored interfaces or individual interfaces
  - Select to show data from the last 20 minutes, 40 minutes, hour, 12 hours, day, or 7 days
  - Select to immediately refresh the page

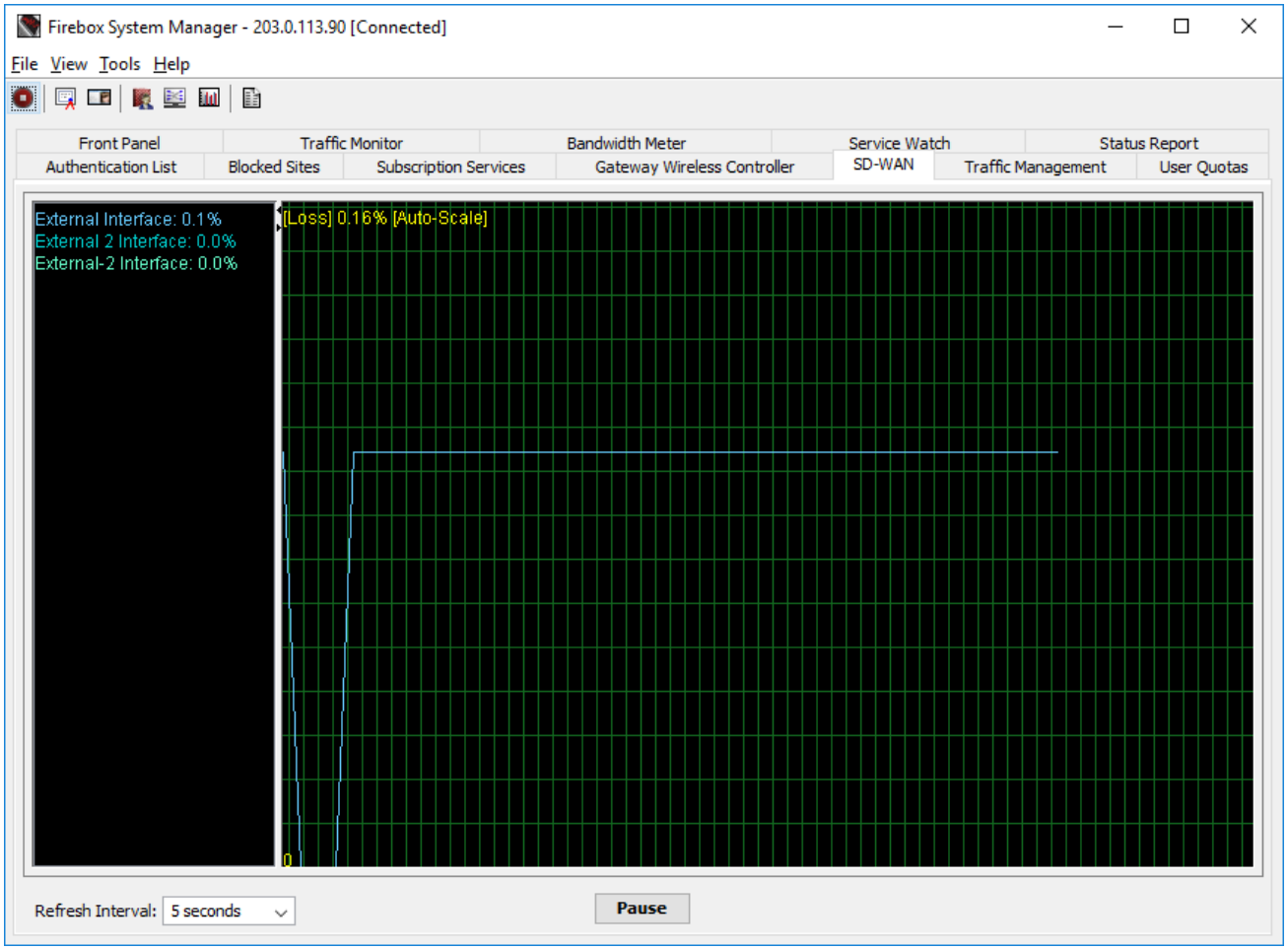
WAN Interface Monitors

- SD-WAN settings in Firebox System Manager



WAN Interface Monitors

- SD-WAN graph in Firebox System Manager



WAN Interface Monitors

- To customize the Firebox System Manager graph, you can:
  - Select to show data for all monitored interfaces or individual interfaces
  - Select a refresh interval of 5, 10, 30, or 60 seconds, or 2 or 5 minutes
  - Select custom colors for the background, text, and grid line
  - Specify a custom scale value
  - Select to pause data collection

Loopback IP Address Support

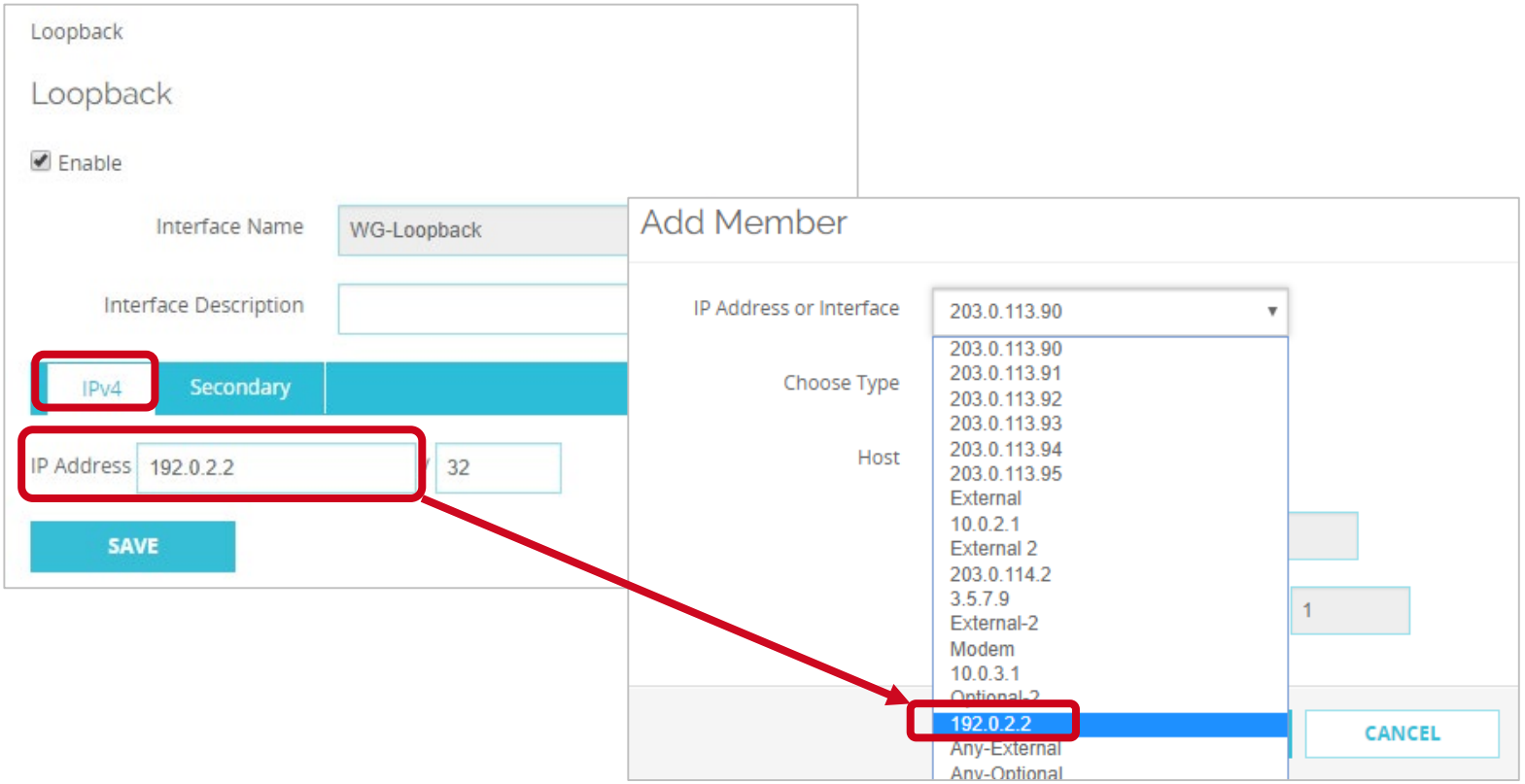
WatchGuard Training

Loopback IP Address Support

- You can now specify a loopback IP address in static NAT actions
- If your configuration includes a loopback IP address, you can specify the primary or secondary IP address of the loopback interface in a static NAT action

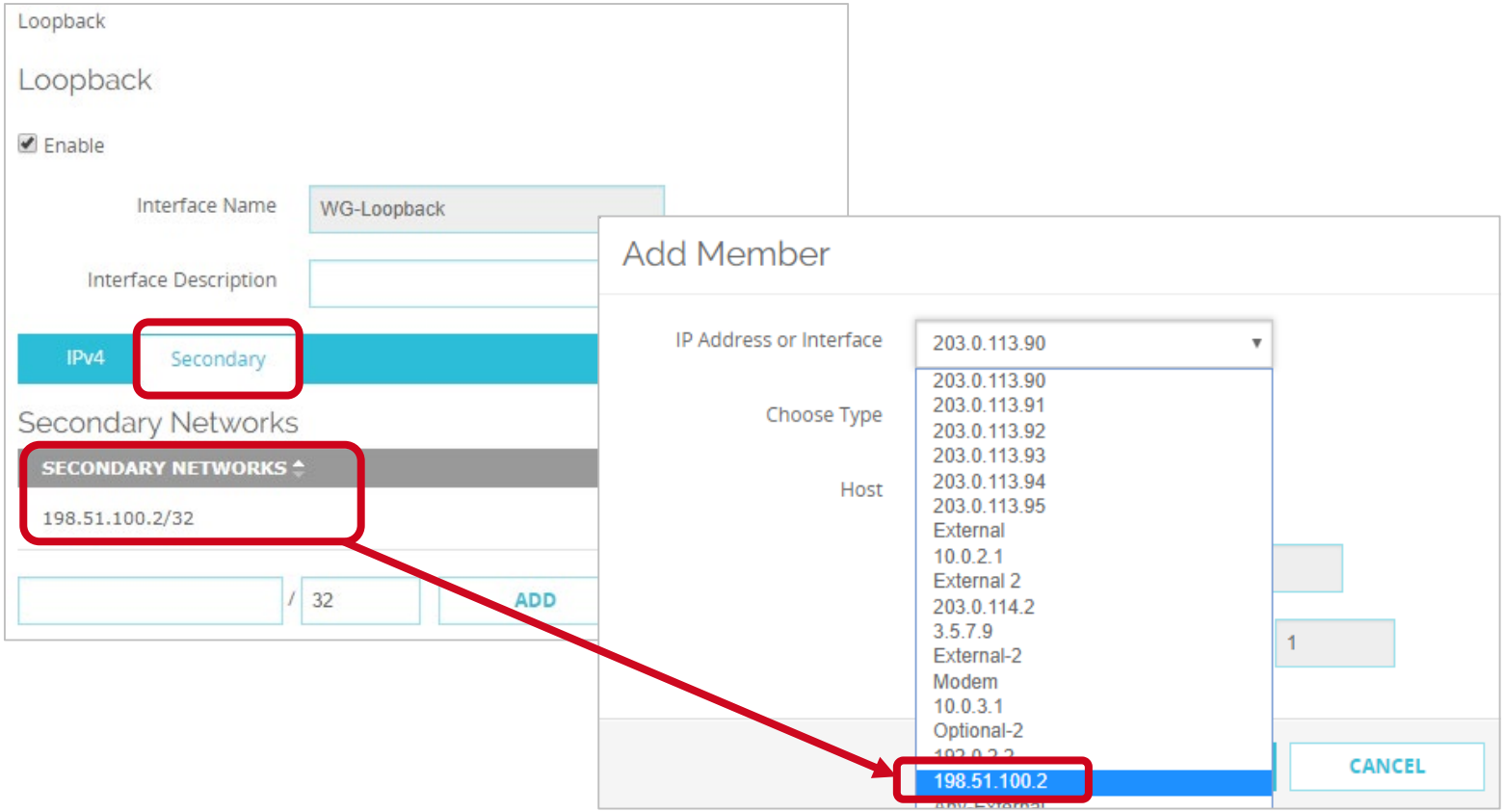
Loopback IP Address Support

- Web UI — Primary loopback IP address



Loopback IP Address Support

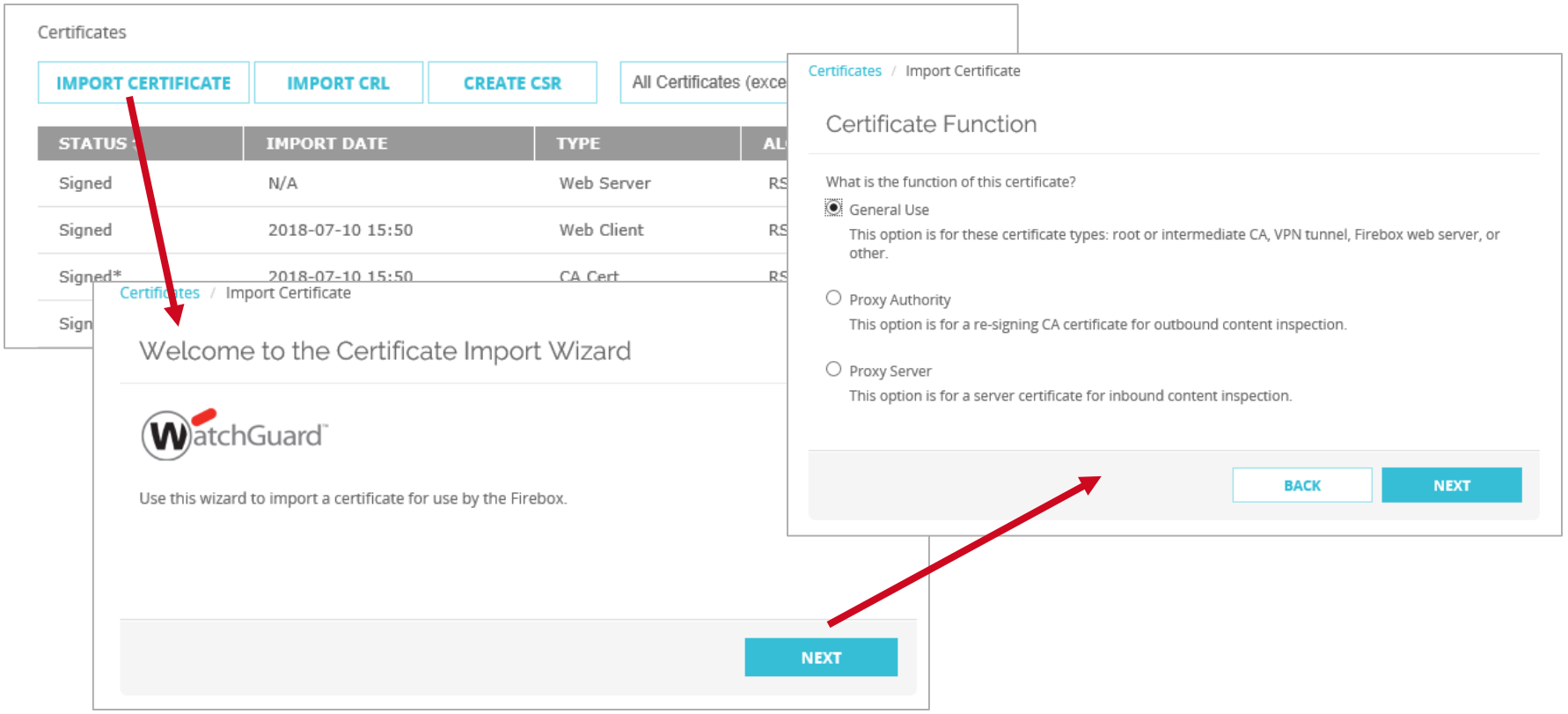
- Web UI — Secondary loopback IP address



WatchGuard Training

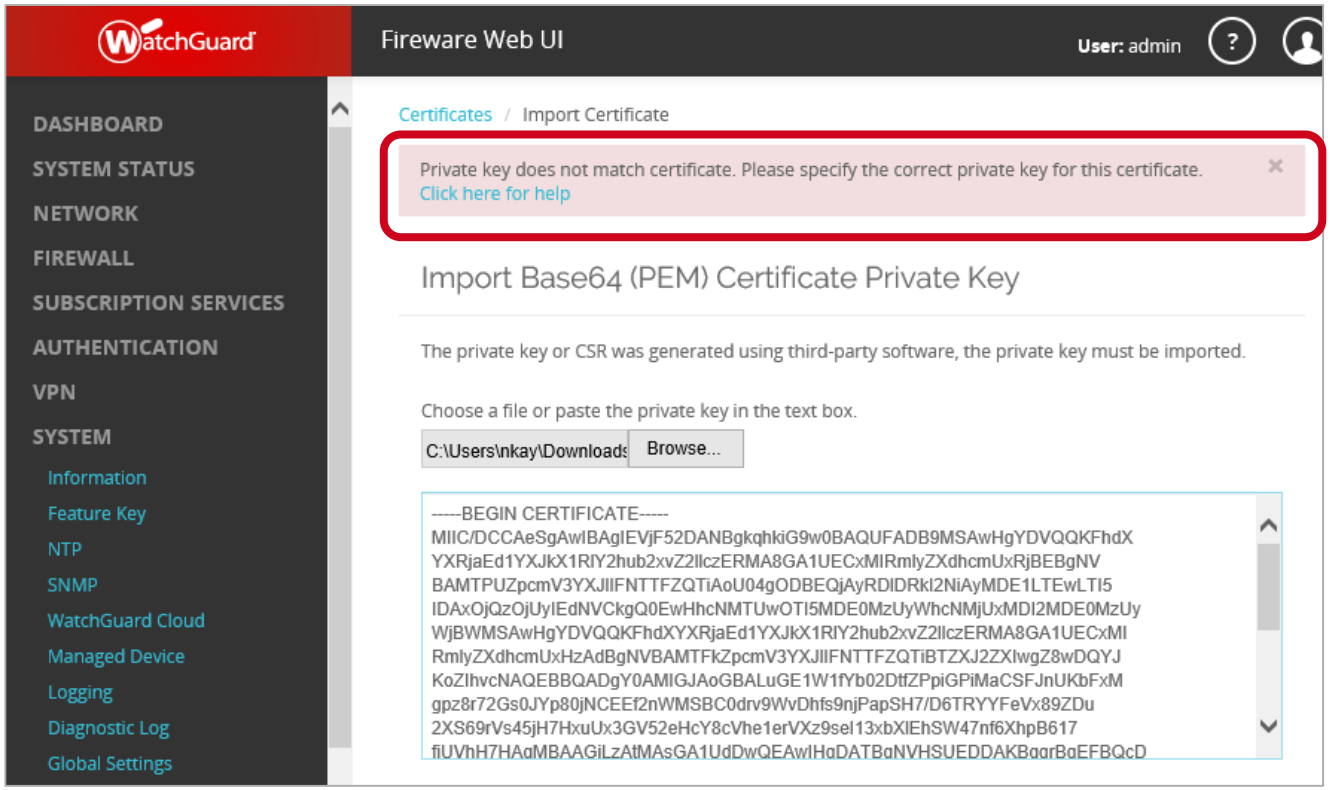
Certificate Import Wizard

- New certificate import wizard helps you import certificates in the correct functional category and provides improved feedback about certificate import issues



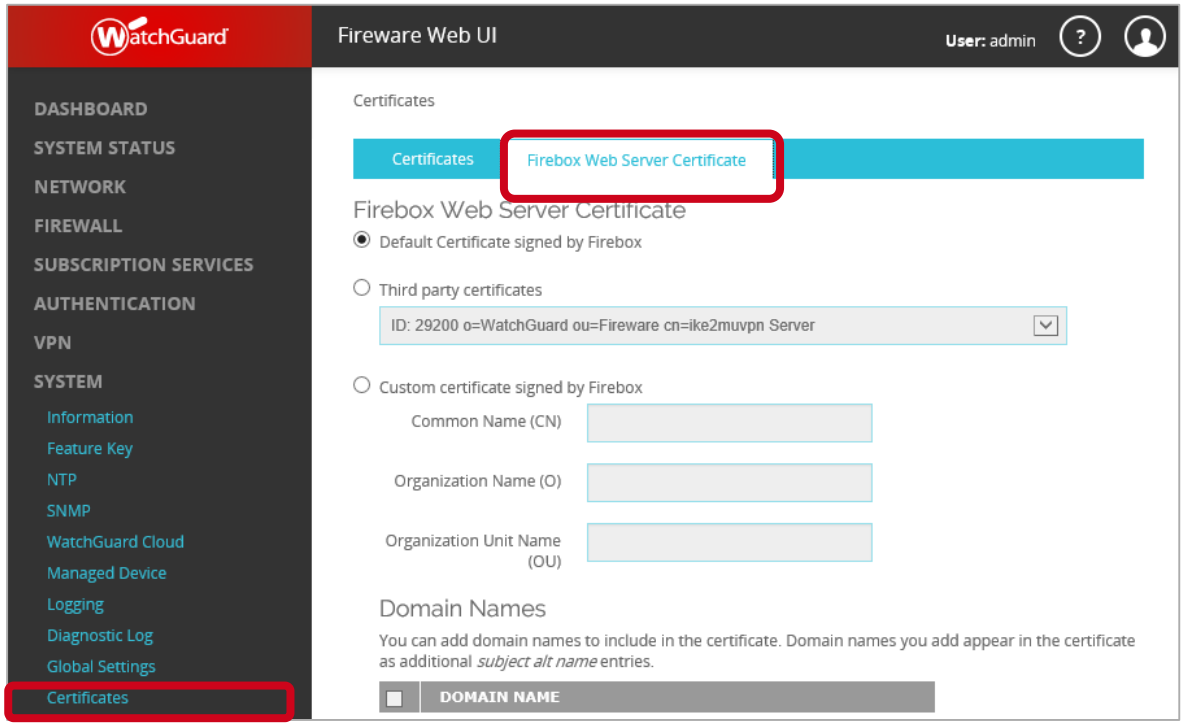
Certificate Import Wizard

- Certificate import error messages provide detailed feedback
  - For example: Private key does not match, missing intermediate or CA certificate, certificate import order issues, etc.



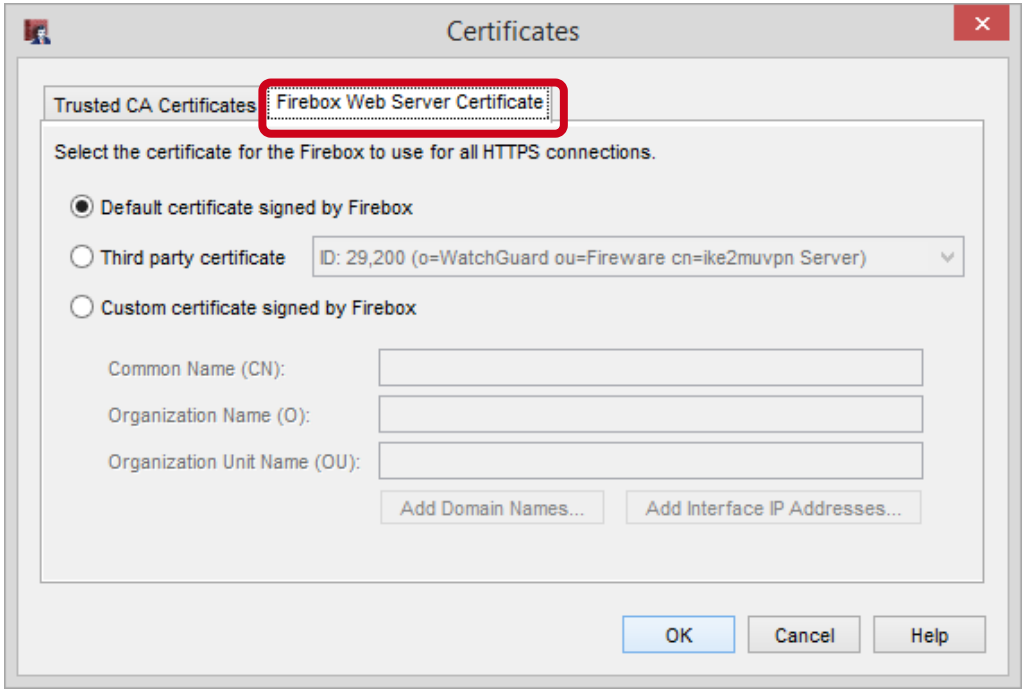
Firebox Web Server Certificate Management

- In Fireware Web UI, Firebox web server certificate management is now located on the **System > Certificates** page on a separate tab
- Previously located on the **Authentication** page



Firebox Web Server Certificate Management

- In Policy Manager, Firebox web server certificate management is now located on the **Setup > Certificates > Firebox Web Server Certificate** tab
- Previously located in **Setup > Authentication**



DF Bit and PMTU Setting for BOVPN Gateways

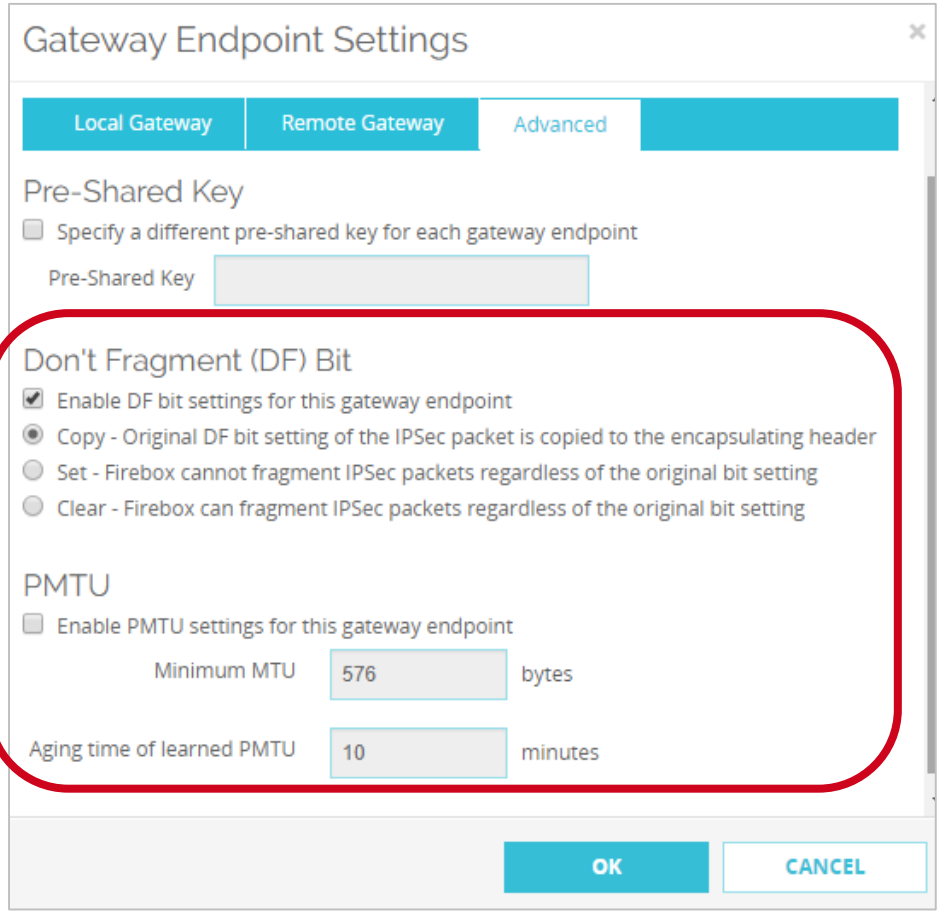
WatchGuard Training

DF Bit and PMTU for BOVPN Gateways

- The **DF (Don't Fragment) Bit** and **PMTU** settings now appear in the BOVPN and BOVPN virtual interface gateway configuration
  - You can configure the DF Bit and PMTU settings per gateway
  - For example, you can specify the **Copy** option for one gateway, and the **Set** option for another gateway
- The global DF Bit and PMTU settings remain in the external interface configuration
  - The gateway DF Bit and PMTU settings take precedence over the interface DF Bit and PMTU settings
- When you enable the DF Bit setting, it defaults to the **Copy** option

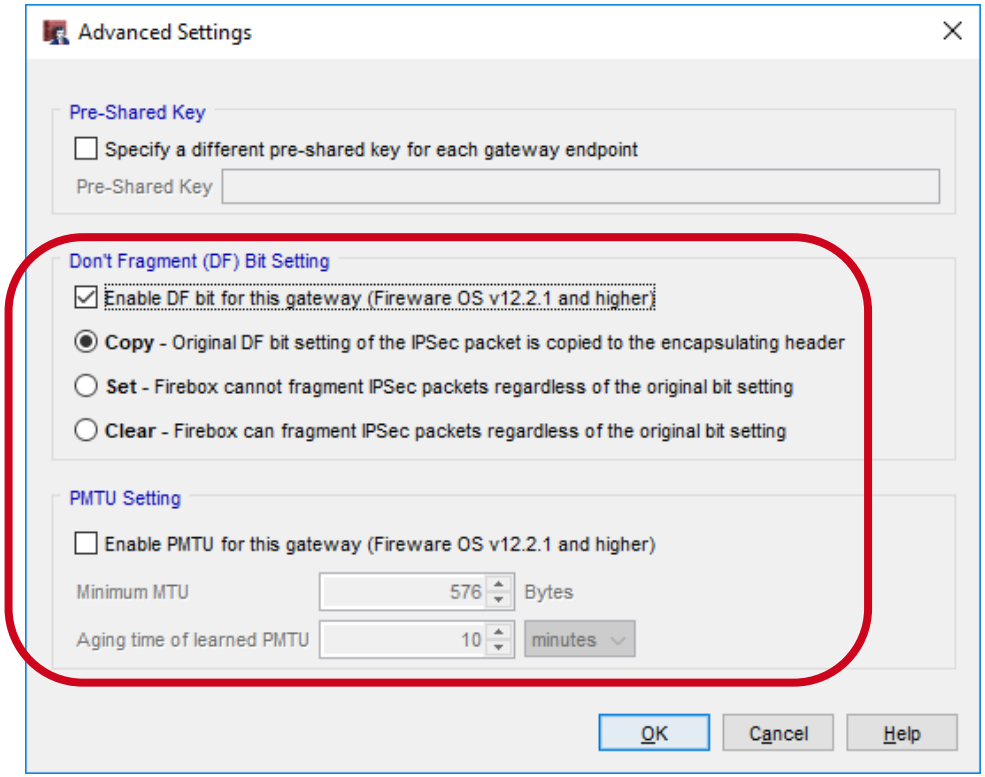
DF Bit and PMTU for BOVPN Gateways

- Fireware Web UI



DF Bit and PMTU for BOVPN Gateways

- Policy Manager



Password Length Control for Firebox-DB Accounts

WatchGuard Training

Password Length Control

- New **Minimum password length** setting lets you specify the minimum password length for Firebox-DB accounts
- Longer passwords are more secure and harder to crack
- Increasing password length is considered to be a more effective security measure than using special characters and cases

Password Length Control

- You must specify a **Minimum password length** for Firebox-DB accounts
- This setting applies to:
  - Firebox-DB accounts added in the Firebox-DB server, Access Portal, and Mobile VPN with IKEv2 configurations
  - Firebox management accounts (*admin* and *status* accounts)
  - Support Access accounts

Password Length Control

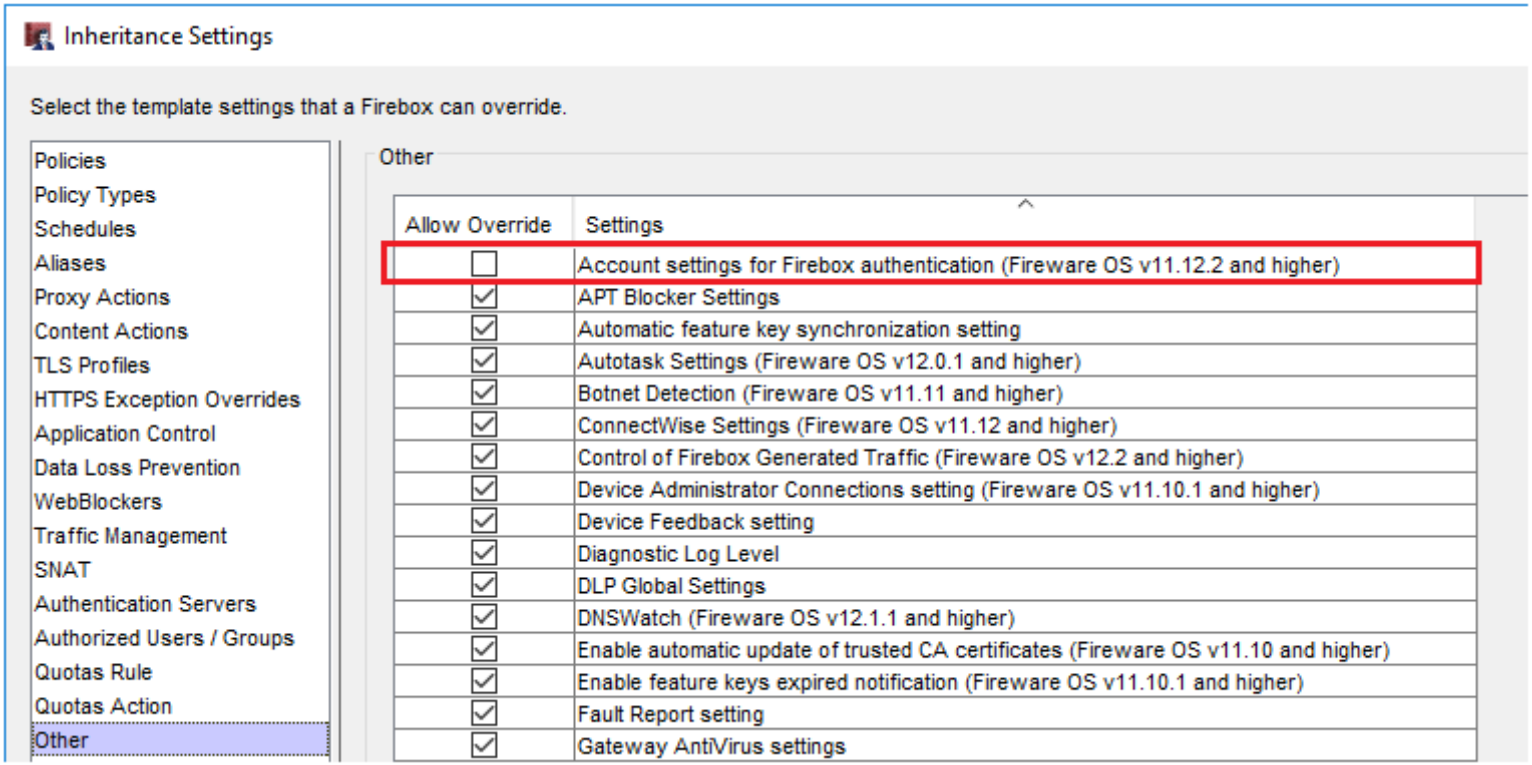
- The minimum password length must be between 8 and 32 characters
  - The maximum password length is 32 characters
- The minimum length you specify applies to passwords for new users
- Passwords for current users are not changed, but any new password must meet the minimum length requirement
  - For example, if you unlock a user account and select the option to reset the password, the new password must meet the minimum length requirement

Password Length Control

- If you use a WSM Management Server to manage your Fireboxes:
  - In the device configuration template, you can control whether the minimum password length setting overrides the same setting on a Firebox
  - To configure the password settings in a template to override the password settings on a Firebox, keep the **Account settings for Firebox authentication** check box clear

Password Length Control

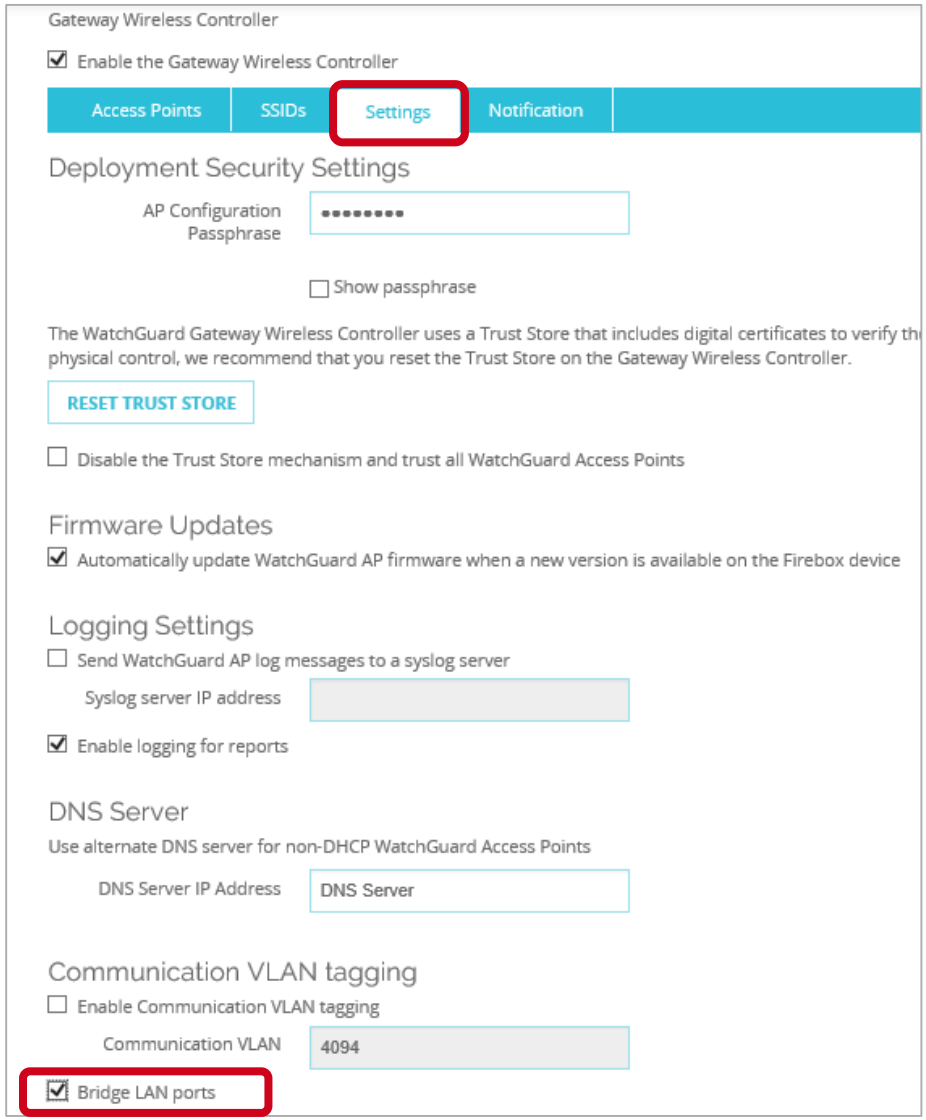
- Device configuration template settings:



Gateway Wireless Controller Enhancements

Bridge LAN Ports on APs

- You can now bridge together the LAN ports on AP models that have two LAN interfaces
- This enables you to extend the wired network on the second LAN interface
- Located in the Gateway Wireless Controller Settings page



Backup and Restore Enhancements

WatchGuard Training

Backup and Restore Enhancements

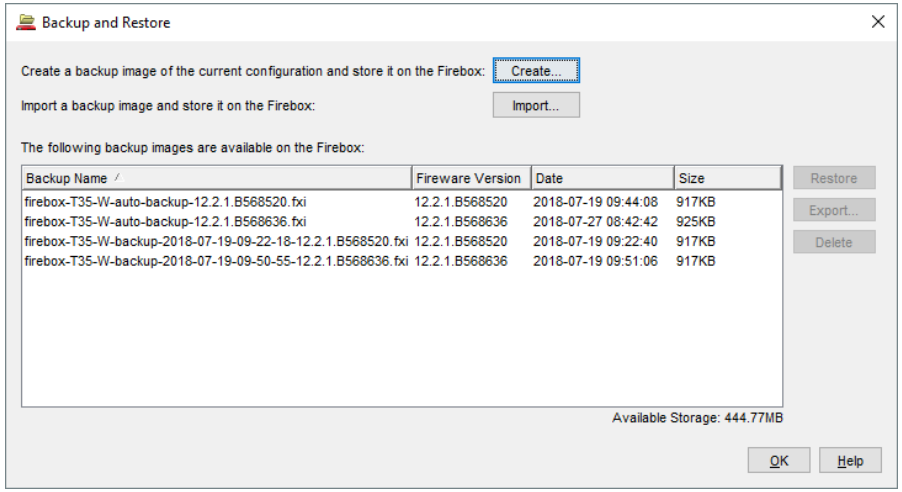
- Fireware v12.2.1 includes these backup image enhancements:
  - New Backup and Restore Image page to create, restore, and manage backup image files
  - Backup images are now stored on the Firebox
  - Backup images no longer include the Fireware OS
  - Backup images are now created automatically every time the Firebox is upgraded
  - Backup images are retained on the Firebox until you delete them manually or reset the Firebox to factory-default settings
  - Backup image files are smaller
  - Backup and restore operations complete faster

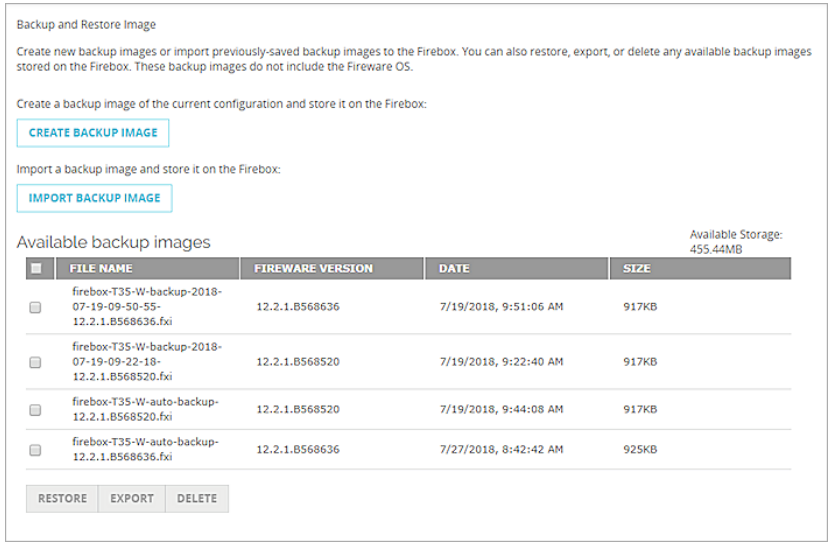
Backup Image Contents

- A backup image is a file you can use to restore your Firebox back to a previous state
- In Fireware v12.2.1, backup images include:
  - Configuration file
  - Feature key
  - DHCP lease file
  - Event notification config
  - Serial Number/Platform/Version information
  - Certificates
  - Passwords file
  - Hotspot guest config files
  - Customer logo
- Backup images no longer include Fireware OS

Backup and Restore Image

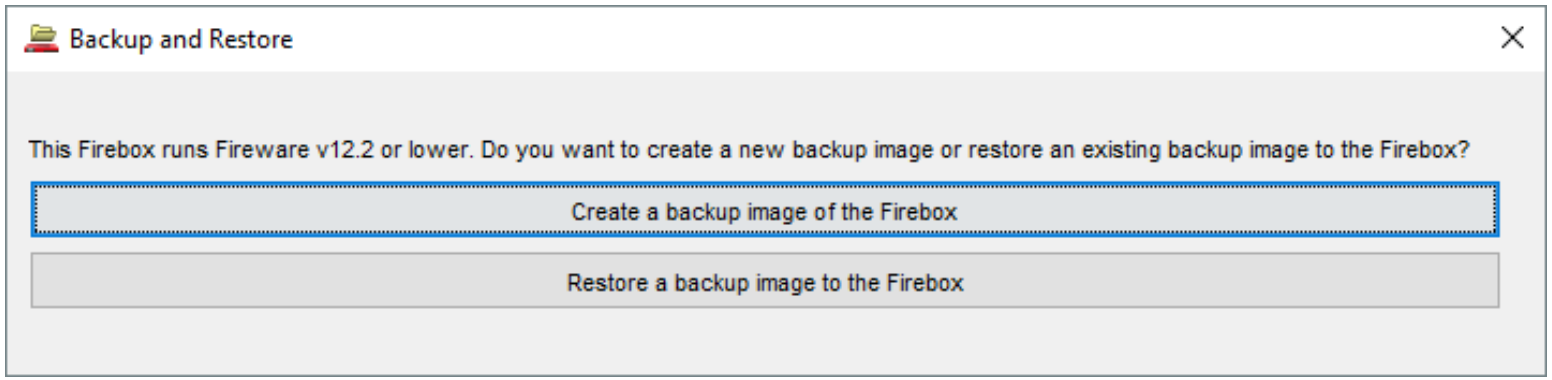
- You can use the new Backup and Restore user interface to view and manage backup images stored on the Firebox
  - In Web UI, select **System > Backup and Restore Image**
  - In Policy Manager, select **File > Backup and Restore Image**





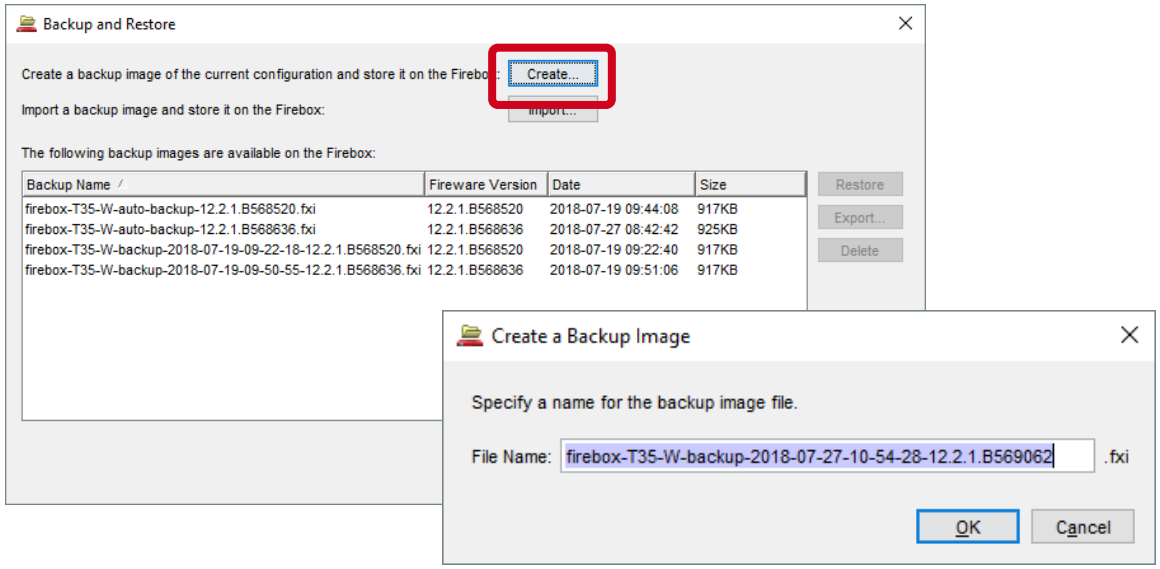
Backup and Restore Image

- If you use Policy Manager to manage a Firebox that runs Fireware v12.2 or lower, when you select **File > Backup and Restore Image** you see the v12.2 backup and restore options instead of the new page



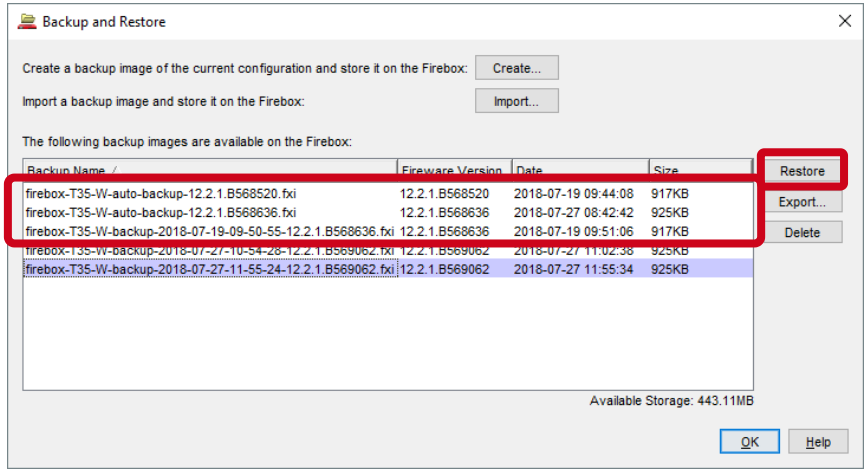
Create New Backup Image

- To create a new backup image and store it on the Firebox, click **Create** and type a name for the backup image file
  - Default file name is based on the Firebox system name, model, current date, and Fireware OS version number
  - Backup images files are permanently retained on the Firebox unless you delete them, or reset the Firebox to factory-default settings



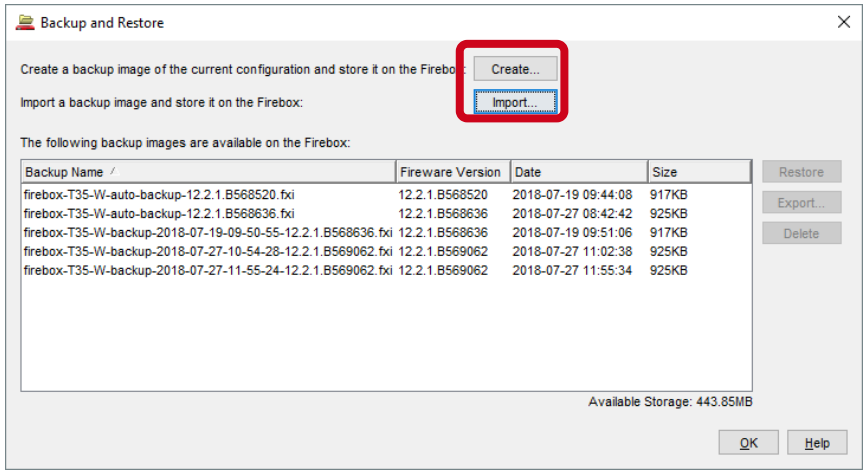
Restore Backup Images

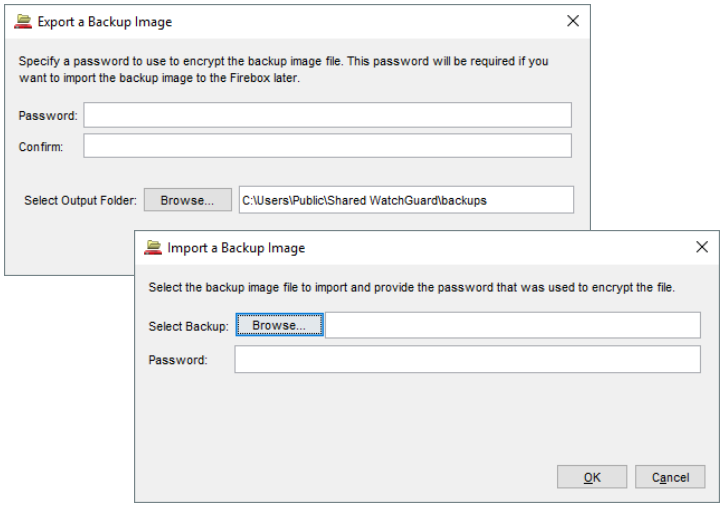
- To restore backup images that are stored on the Firebox
  - Select an available backup image and click **Restore**
  - If a backup image was saved from a lower Fireware OS version, you must restore it as part of the Fireware OS downgrade process instead
  - Because admin credentials are stored in the backup image file, make sure you know the admin passphrase at the time the backup was created before you restore



Export and Import Backup Images

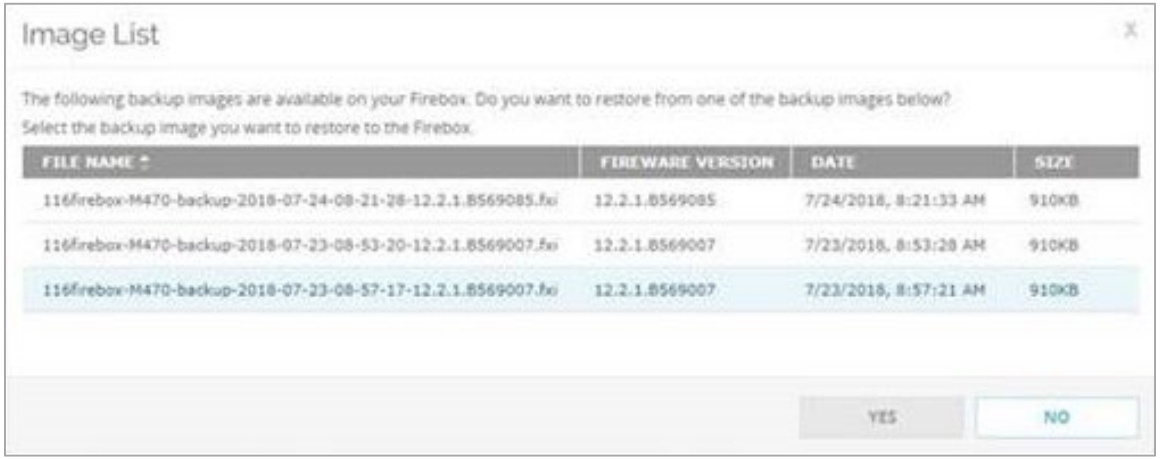
- To import and export backup images to and from the Firebox
  - In the Backup and Restore page, click **Import** or **Export**
  - Exported backup images are encrypted with a password that must be specified when you import it
  - Backup images saved from Fireware v12.2 or lower cannot be stored on the Firebox. If you try to import one, you are asked if you want to restore the backup image





Downgrade OS and Restore Backup Image

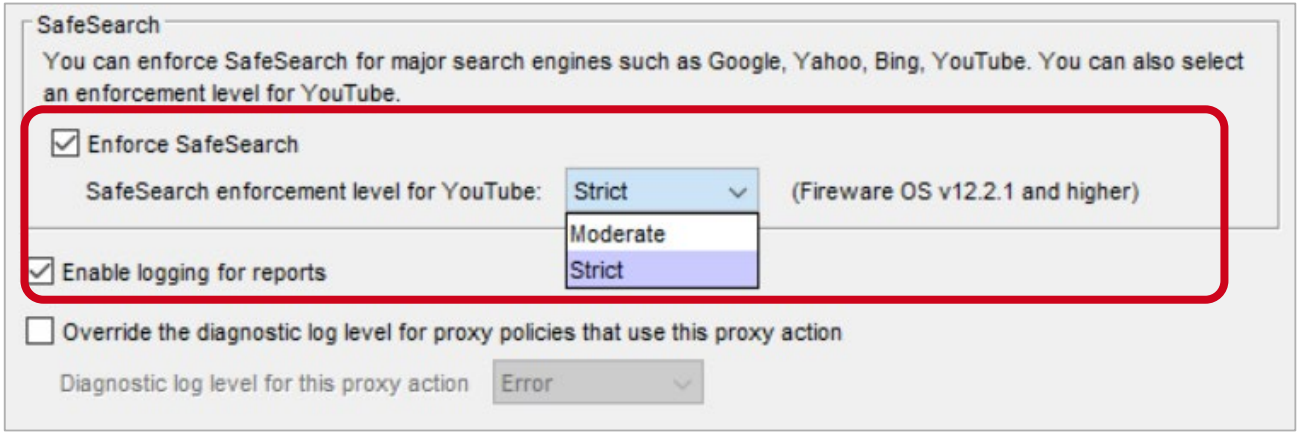
- In future releases, when you downgrade Fireware OS, you will be able to restore a backup image that is stored on your Firebox
- Choose from saved backup images for the specific Fireware OS version
- If you do not choose an image to restore, the Firebox is reset to factory-default settings



SafeSearch Enforcement Level for YouTube

SafeSearch Enforcement Level for YouTube

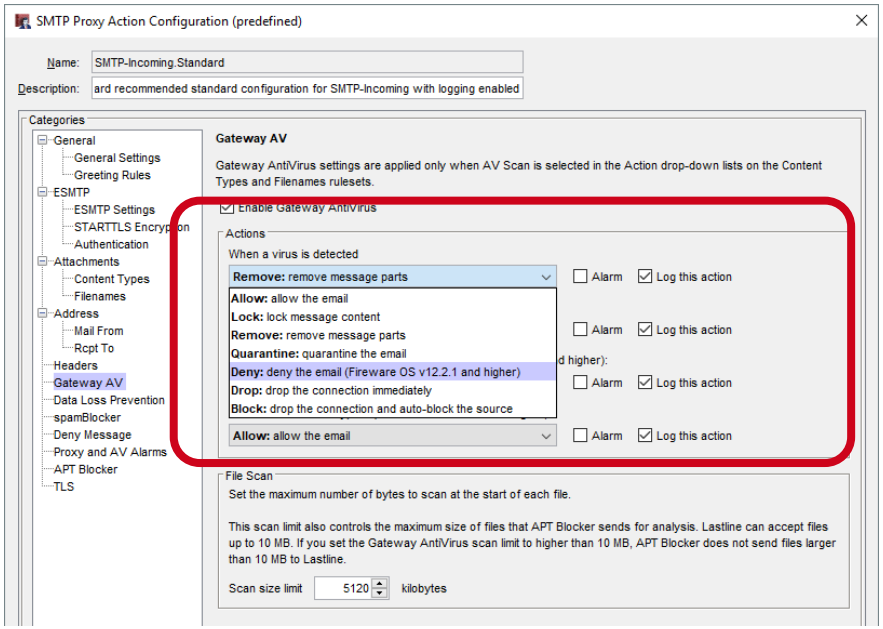
- In HTTP and Explicit proxy actions, you can now specify the level at which SafeSearch is enforced on YouTube
- In the **HTTP Request > General Settings** section, select an option from the **SafeSearch enforcement level for YouTube** drop-down list: Strict or Moderate
- The selected enforcement level only applies to YouTube and does not affect other sites



SMTP-proxy Action Updates

SMTP-proxy Action Updates

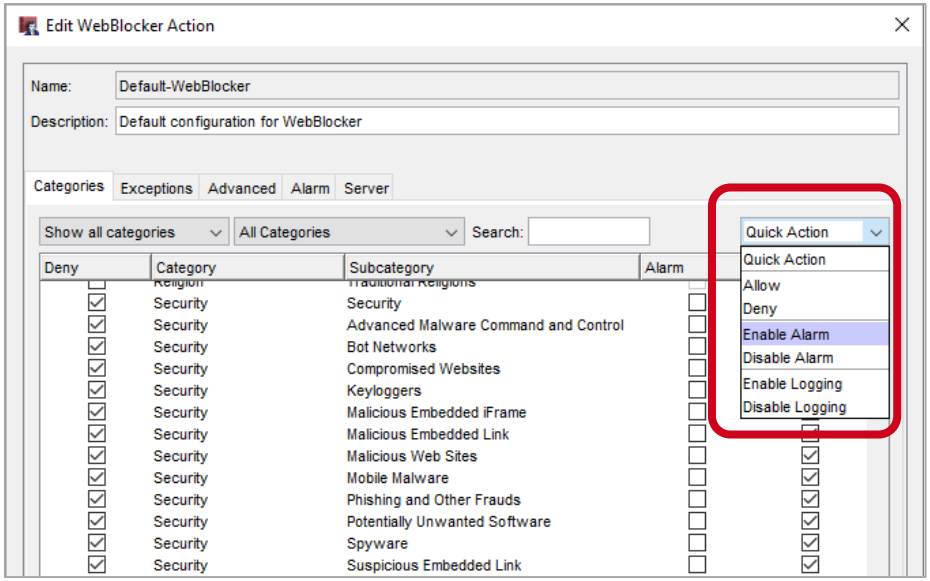
- In SMTP-proxy actions, you can now select **Deny** when you configure the following:
  - Gateway AV actions
  - spamBlocker Virus Outbreak Detection actions
- When Deny is selected, Gateway AV or spamBlocker denies delivery of the message
- The Firebox sends an SMTP 554 Transaction Failed response to the source of the message with the reason the email was denied



WebBlocker Usability Updates

WebBlocker Usability Updates

- In the WebBlocker Action dialog box, Categories tab, you can now select multiple category rows
- When multiple rows are selected, use the Quick Action drop-down list to apply an action to the selected categories
- For example, deny the categories or enable logging



WatchMode Updates

WatchMode Updates

- WatchMode is an audit-only Firebox mode used by WatchGuard Partners to help demonstrate the value of the Firebox to prospective customers
- This release addresses many backend issues that affected the ease of use and reliability of WatchMode
- Application Control, WebBlocker, Gateway AV, and APT Blocker now work reliably, even when there is fragmented TCP/IP traffic

WatchMode Updates

- With Fireware v12.2.1, mirrored traffic can now contain traffic from 802.1Q tagged VLANs
- You can now change these proxy policy settings:
  - Policy name
  - Port
  - From/To addresses can now include IP address ranges or subnets
  - New proxy policies can be added to the WatchMode configuration

WatchGuard IPSec Mobile VPN Client

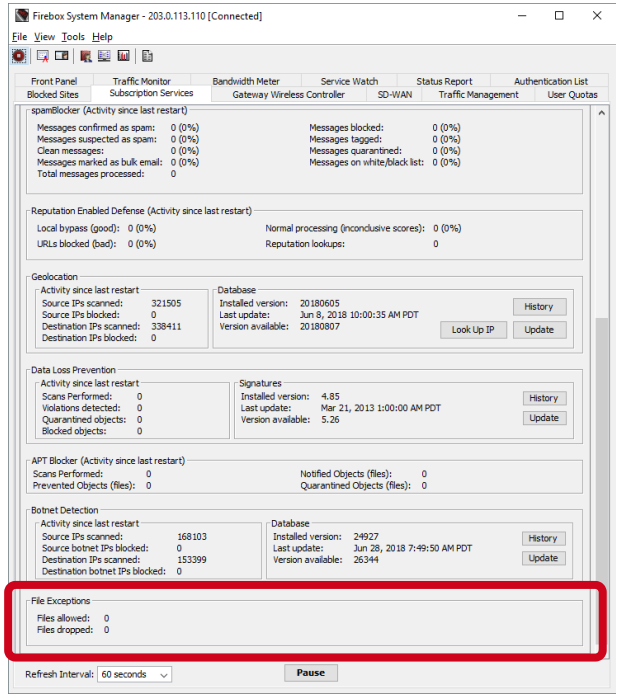
WatchGuard IPSec Mobile VPN Client

- The WatchGuard IPSec mobile VPN client has these enhancements:
  - 64-bit version of each component
  - Updated design to reflect Windows 10 design
  - Connect to a hotspot to start the VPN connection before you log in to Windows

File Exceptions Statistics

File Exceptions Statistics

- The number of files allowed and dropped by the File Exceptions list are now shown in these locations:
  - Fireware Web UI > Dashboard > Subscription Services
  - Firebox System Manager > Subscription Services tab



Thank You!