



# What's New in Fireware v12.2.1

# 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

# 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

The screenshot shows the 'Edit Mobile VPN with IPsec' configuration window. The 'Group Name' is set to 'test'. The 'Advanced' tab is selected, showing the 'DNS Settings' section. The 'DNS Settings' section is highlighted with a red circle. It contains the following options:

- Assign system settings to mobile clients
- Do not assign any related settings to mobile clients (Fireware OS v12.2.1 and higher)
- Assign the following settings to mobile clients (Fireware OS v12.2.1 and higher)

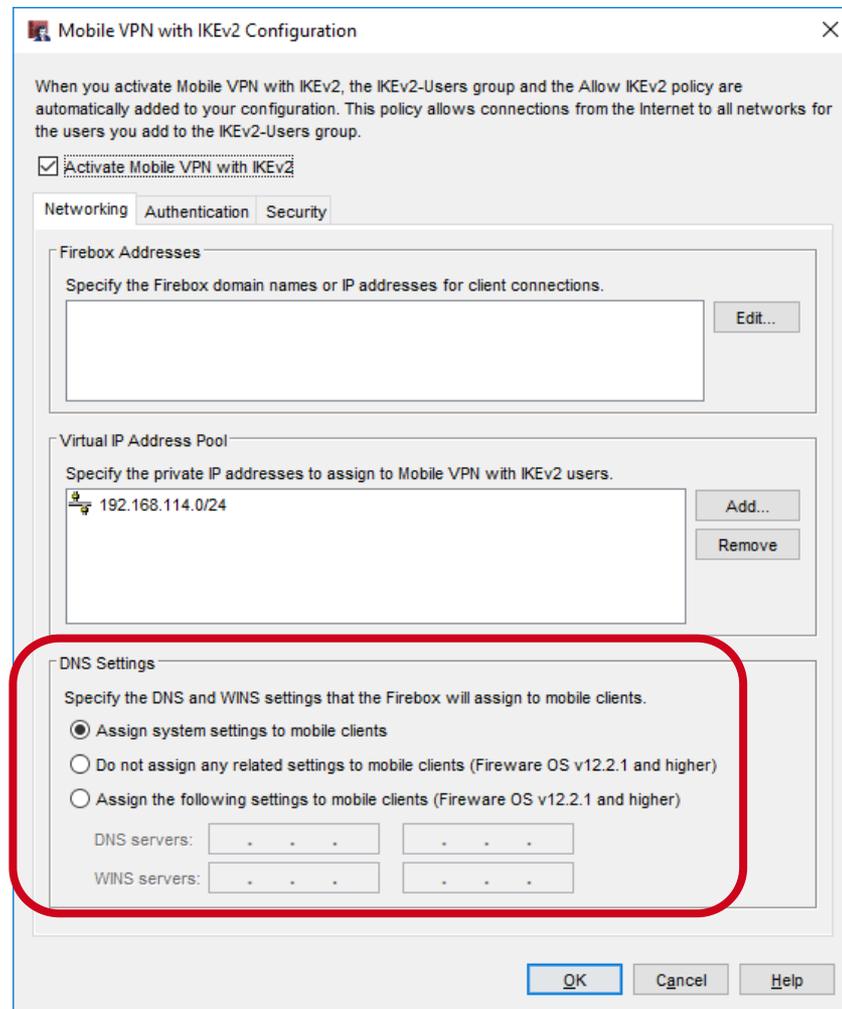
Below the radio buttons, there are input fields for:

- Domain name: [ ]
- DNS servers: [ ] [ ]
- WINS servers: [ ] [ ]

The 'Line Management' section above shows 'Connection mode' set to 'Manual' and 'Inactivity timeout' set to 0 seconds. The 'OK', 'Cancel', and 'Help' buttons are at the bottom right.

# DNS Enhancements for Mobile VPN

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



**Mobile VPN with IKEv2 Configuration**

When you activate Mobile VPN with IKEv2, the IKEv2-Users group and the Allow IKEv2 policy are automatically added to your configuration. This policy allows connections from the Internet to all networks for the users you add to the IKEv2-Users group.

Activate Mobile VPN with IKEv2

Networking Authentication Security

**Firebox Addresses**  
Specify the Firebox domain names or IP addresses for client connections.  
[Text Field] [Edit...]

**Virtual IP Address Pool**  
Specify the private IP addresses to assign to Mobile VPN with IKEv2 users.  
[List Item: 192.168.114.0/24] [Add...]  
[Remove]

**DNS Settings**  
Specify the DNS and WINS settings that the Firebox will assign to mobile clients.

Assign system settings to mobile clients

Do not assign any related settings to mobile clients (Fireware OS v12.2.1 and higher)

Assign the following settings to mobile clients (Fireware OS v12.2.1 and higher)

DNS servers: [Text Field] [Text Field]

WINS servers: [Text Field] [Text Field]

[OK] [Cancel] [Help]

# 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

**Mobile VPN with L2TP Configuration**

When you activate mobile VPN with L2TP, the "L2TP-Users" group and the "WatchGuard L2TP" policy are created to allow Mobile VPN with L2TP connections from the Internet to the external interface.

**Activate Mobile VPN with L2TP**

Networking Authentication IPsec

**Virtual IP Address Pool**

Enter the list of private IP addresses to be assigned to the L2TP users.

Add... Remove

**Network Settings**

Keep Alive Timeout: 60 seconds

Retransmission Timeout: 5 seconds

Maximum Retries: 5

Maximum Transmission Unit (MTU): 1400 bytes

Maximum Receive Unit (MRU): 1400 bytes

**DNS Settings**

Specify the DNS settings that the Firebox will assign to mobile clients.

Assign system settings to mobile clients

Do not assign any related settings to mobile clients (Fireware OS v12.2.1 and higher)

Assign the following settings to mobile clients (Fireware OS v12.2.1 and higher)

DNS servers: . . . . .

OK Cancel Help

# 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

The screenshot shows the "Mobile VPN with SSL Configuration" dialog box. The "Advanced" tab is selected, and the "Activate Mobile VPN with SSL" checkbox is checked. The "DNS Settings" section is highlighted with a red circle. It contains the following options:

Specify the DNS and WINS settings that the Firebox will assign to mobile clients.

- Assign system settings to mobile clients (Fireware OS v12.2.1 and higher)
- Do not assign any settings to mobile clients
- Assign the following settings to mobile clients

Below these options are input fields for:

- Domain name: [ ]
- DNS servers: [ ] [ ]
- WINS servers: [ ] [ ]

At the bottom right of the dialog box, there are buttons for "Restore Defaults", "OK", "Cancel", and "Help".

# DNS Enhancements for Mobile VPN

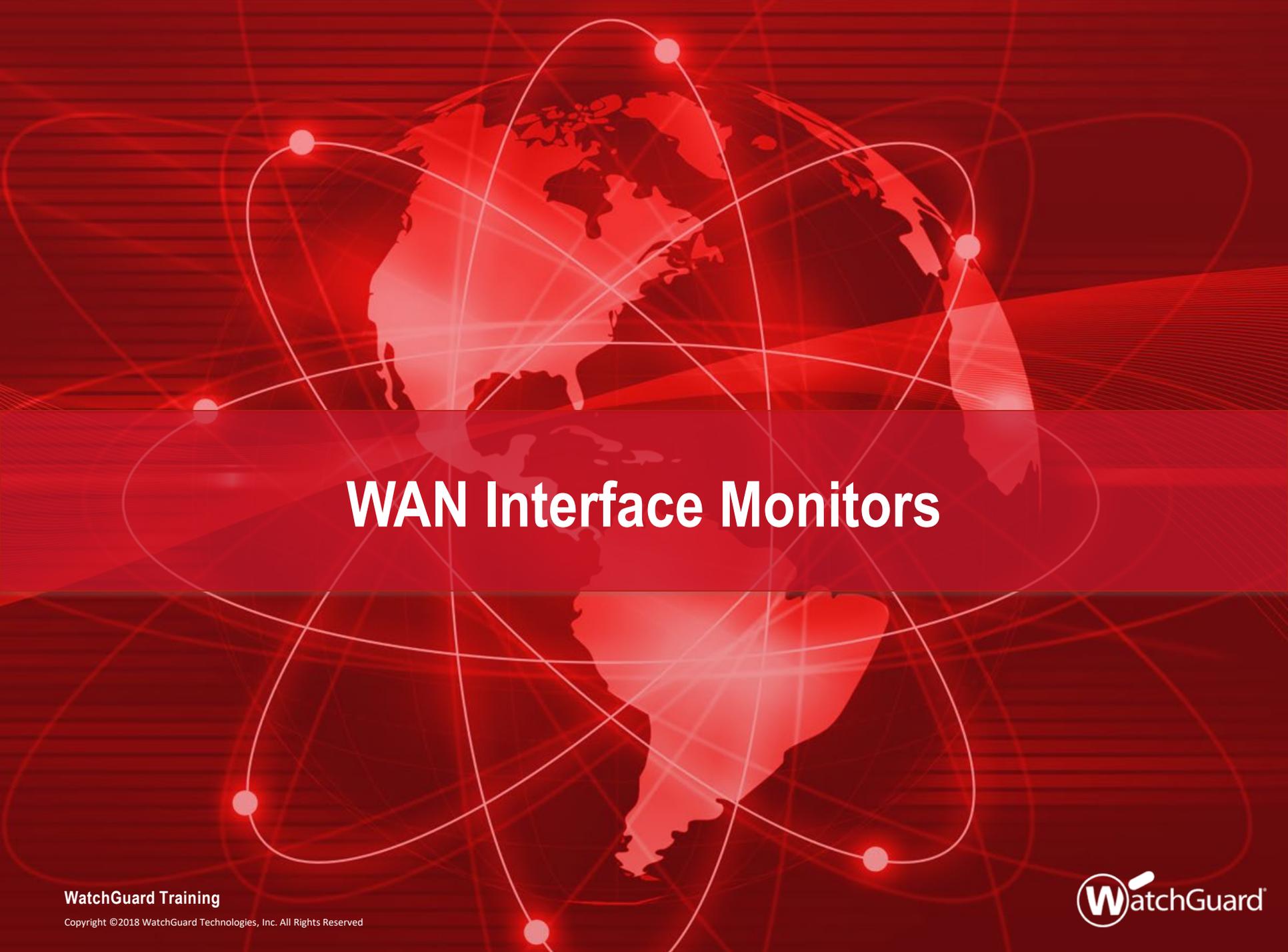
- If you select the **Assign the Network DNS/WINS Server settings to mobile clients**, mobile VPN clients receive the settings configured in the Network (global) DNS/WINS settings
- For example, if you specify the DNS server 203.0.113.50 in the Network DNS settings, mobile VPN clients receive 203.0.113.50 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

# 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

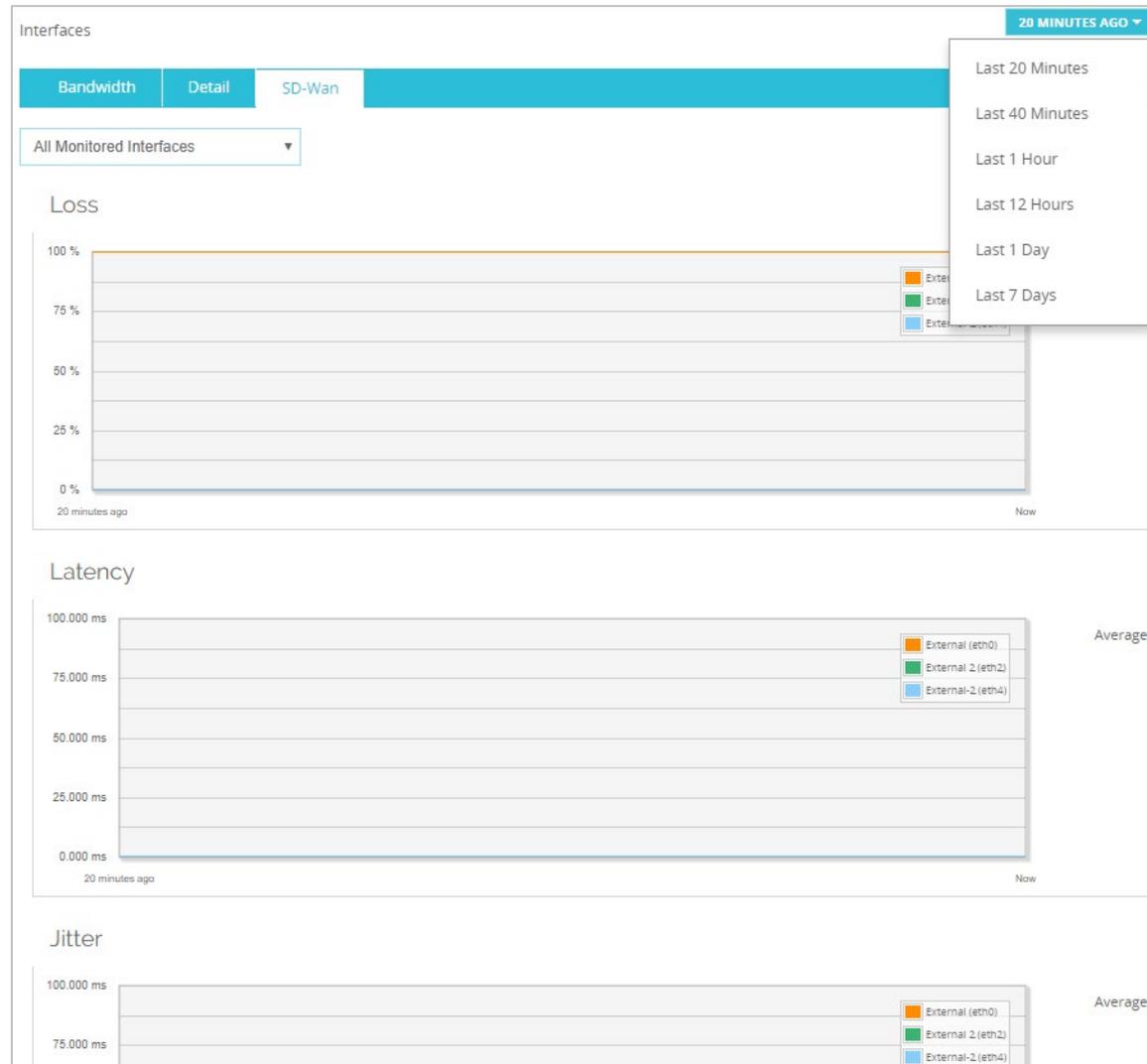
- You can now monitor WAN interfaces on the Firebox for:
  - **Loss** — Percentage of packets lost
  - **Latency** — Packet delivery delay, measured in milliseconds (ms)
  - **Jitter** — Difference in packet delivery delay, measured in ms
- To see data for a WAN interface, you must configure the interface 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

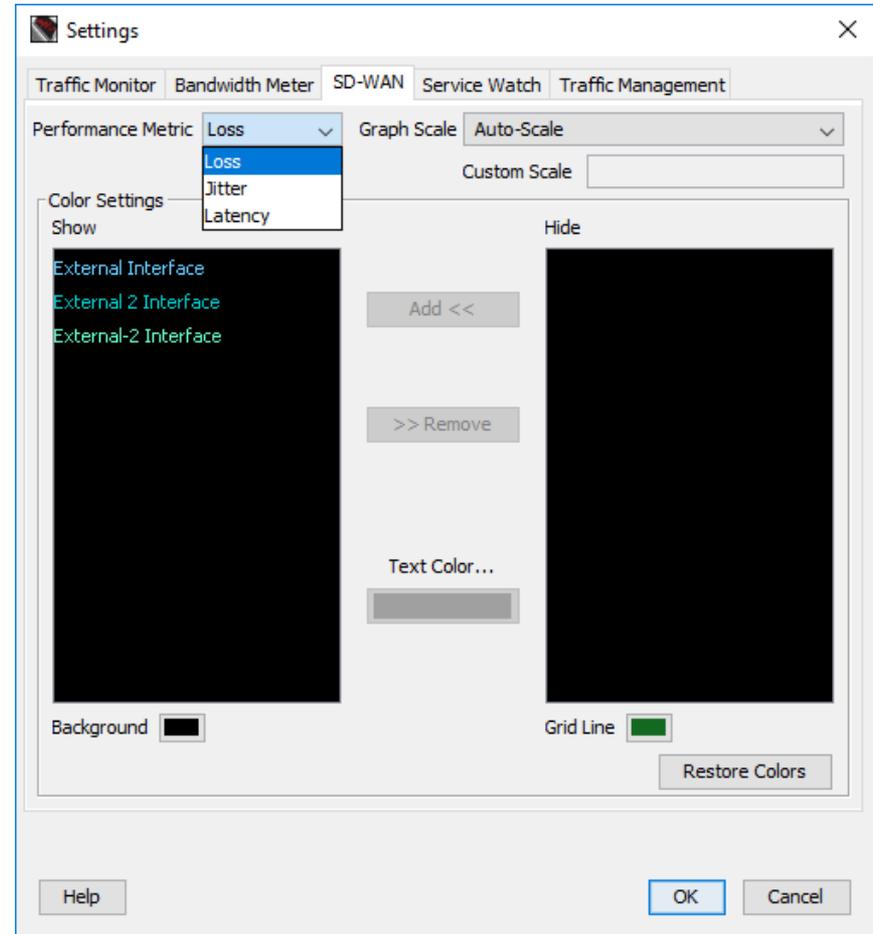


# WAN Interface Monitoring Enhancements

- 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

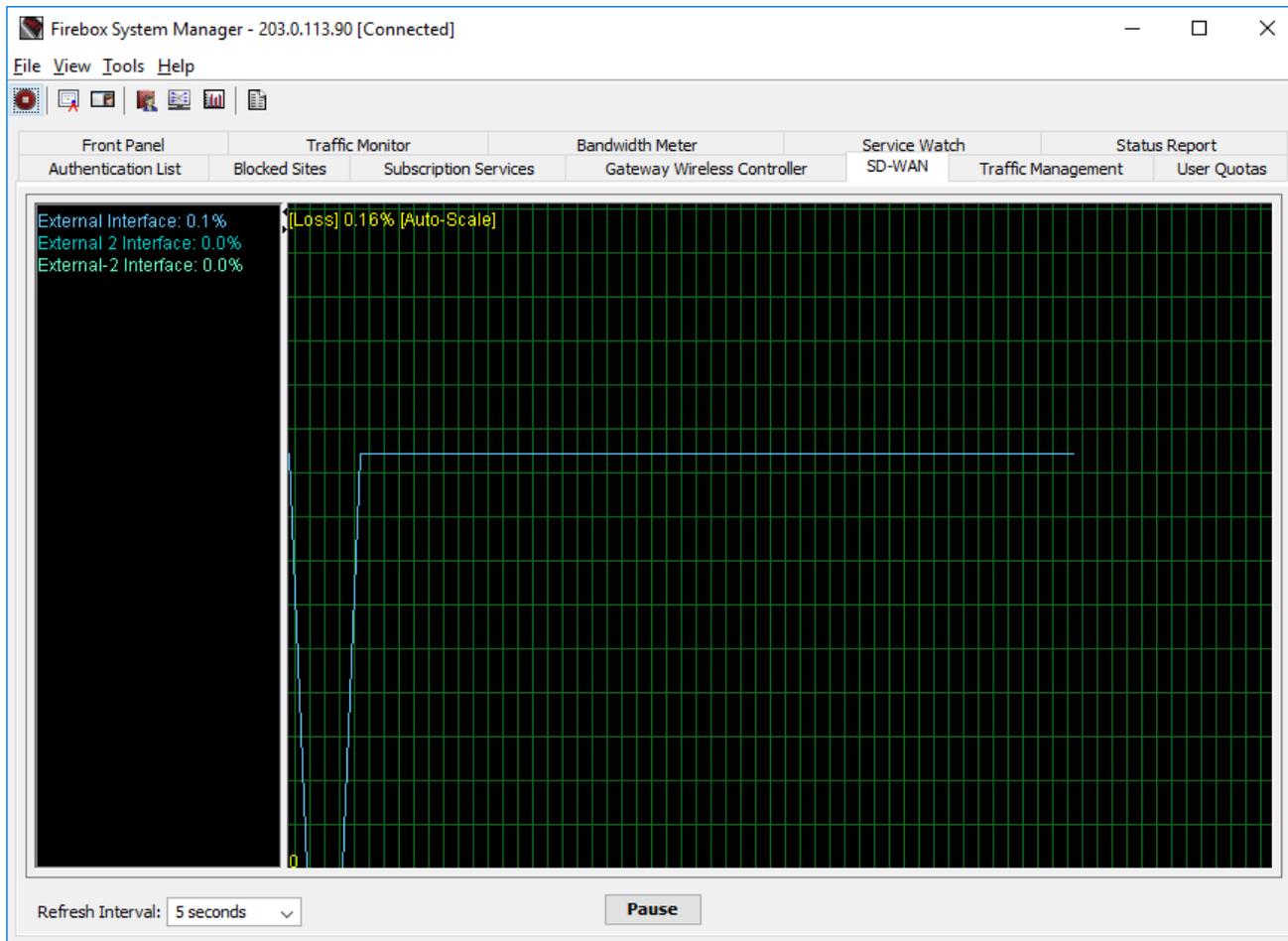
# WAN Interface Monitors

- SD-WAN settings in Firebox System Manager



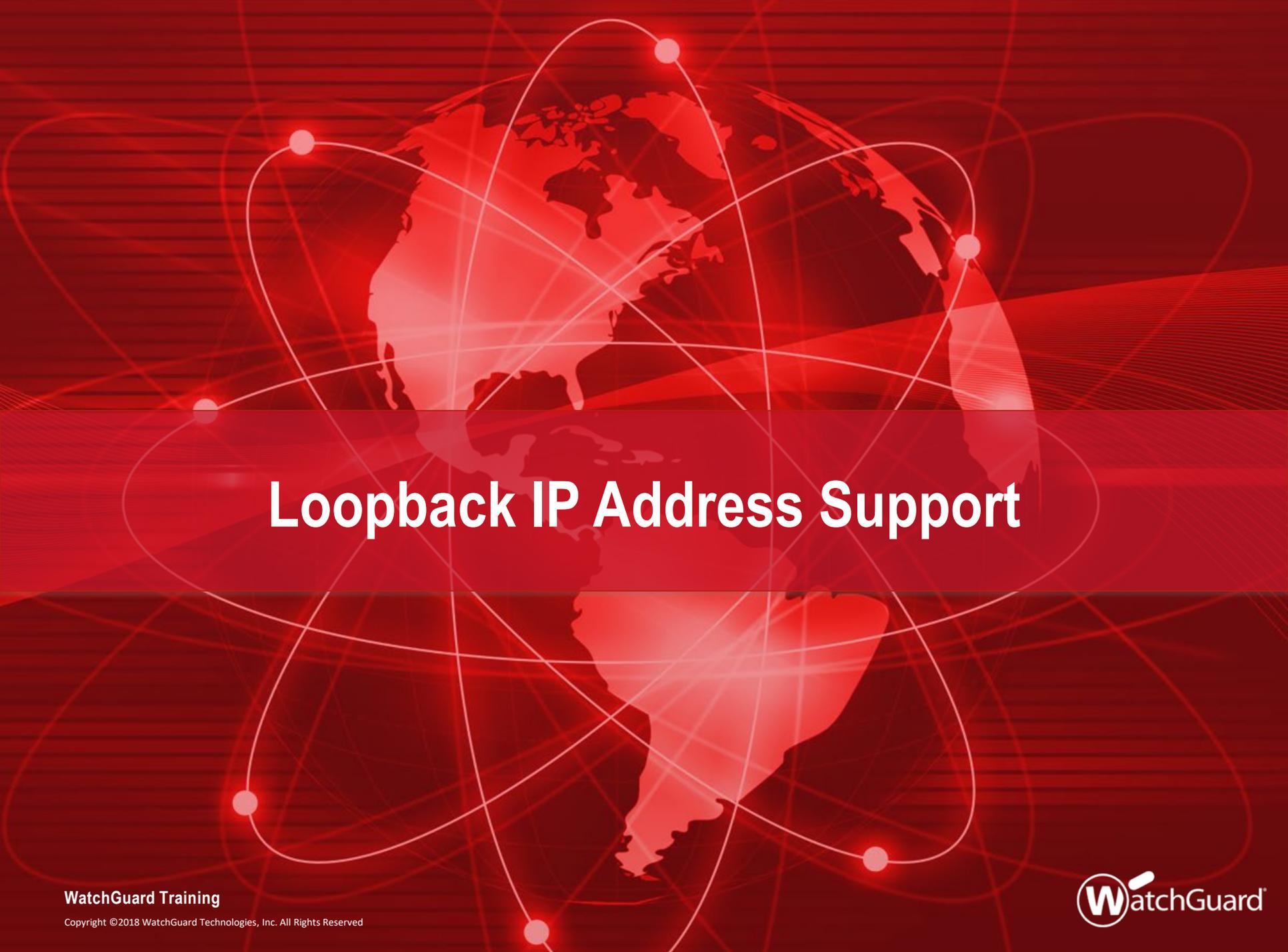
# WAN Interface Monitors

- 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

# 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

The screenshot displays the WatchGuard Web UI configuration for a Loopback interface. The main configuration area shows the following details:

- Loopback: Loopback
- Enable
- Interface Name: WG-Loopback
- Interface Description: (empty)
- Protocol: IPv4 (highlighted with a red box)
- Role: Secondary
- IP Address: 192.0.2.2 (highlighted with a red box)
- Subnet Mask: 32
- SAVE button

An "Add Member" dialog is overlaid on the right side of the screen. It shows a list of IP addresses and interface types. The IP address 192.0.2.2 is selected and highlighted with a blue bar and a red box. A red arrow points from the IP address field in the main configuration to this selection in the dialog.

The "Add Member" dialog includes the following fields and options:

- IP Address or Interface: 203.0.113.90
- Choose Type: (dropdown menu)
- Host: (input field)
- CANCEL button

IP Address or Interface
203.0.113.90
203.0.113.91
203.0.113.92
203.0.113.93
203.0.113.94
203.0.113.95
External
10.0.2.1
External 2
203.0.114.2
3.5.7.9
External-2
Modem
10.0.3.1
Optional 2
<b>192.0.2.2</b>
Any-External
Any-Optional

# Loopback IP Address Support

- Web UI – Secondary loopback IP address

The screenshot displays the WatchGuard Web UI configuration for a Loopback interface. The main configuration area shows the following details:

- Loopback** section:  Enable
- Interface Name:** WG-Loopback
- Interface Description:** (empty)
- IPv4** section: **Secondary** (highlighted with a red box)
- Secondary Networks** section: **SECONDARY NETWORKS** (highlighted with a red box), listing **198.51.100.2/32** (highlighted with a red box)
- Input fields for IP address and subnet mask (32) and an **ADD** button.

An **Add Member** dialog box is open, showing a list of IP addresses and interface types. The **IP Address or Interface** dropdown is set to **203.0.113.90**. The list includes:

- 203.0.113.90
- 203.0.113.91
- 203.0.113.92
- 203.0.113.93
- 203.0.113.94
- 203.0.113.95
- External
- 10.0.2.1
- External 2
- 203.0.114.2
- 3.5.7.9
- External-2
- Modem
- 10.0.3.1
- Optional-2
- 192.0.2.2
- 198.51.100.2** (highlighted with a red box)

The **Host** field is set to **1**. A **CANCEL** button is visible at the bottom right of the dialog. A red arrow points from the **198.51.100.2/32** entry in the main configuration to the **198.51.100.2** entry in the dialog.



# Certificate Management Enhancements

# Certificate Import Wizard

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

Certificates

[IMPORT CERTIFICATE](#) [IMPORT CRL](#) [CREATE CSR](#) All Certificates (except...)

STATUS	IMPORT DATE	TYPE	AL
Signed	N/A	Web Server	RS
Signed	2018-07-10 15:50	Web Client	RS
Signed*	2018-07-10 15:50	CA Cert	RS

Certificates / Import Certificate

Welcome to the Certificate Import Wizard

WatchGuard™

Use this wizard to import a certificate for use by the Firebox.

[NEXT](#)

Certificates / Import Certificate

### Certificate Function

What is the function of this certificate?

General Use  
This option is for these certificate types: root or intermediate CA, VPN tunnel, Firebox web server, or other.

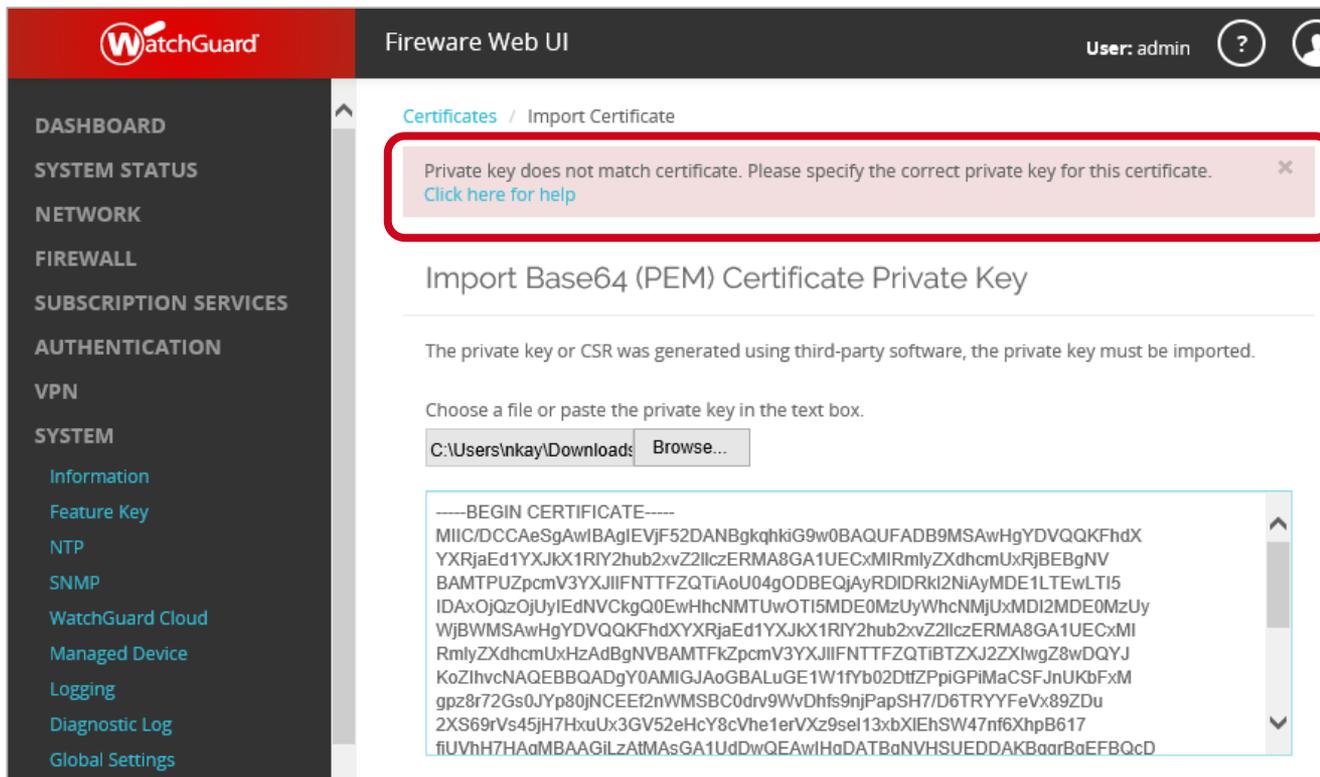
Proxy Authority  
This option is for a re-signing CA certificate for outbound content inspection.

Proxy Server  
This option is for a server certificate for inbound content inspection.

[BACK](#) [NEXT](#)

# Certificate Import Wizard

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



The screenshot displays the WatchGuard Fireware Web UI interface. The top navigation bar includes the WatchGuard logo, the title "Fireware Web UI", and the user "User: admin". The left sidebar contains a menu with categories: DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, VPN, and SYSTEM. The main content area is titled "Certificates / Import Certificate". A red-bordered box highlights an error message: "Private key does not match certificate. Please specify the correct private key for this certificate. Click here for help". Below the error message, the page title is "Import Base64 (PEM) Certificate Private Key". A note states: "The private key or CSR was generated using third-party software, the private key must be imported." Below this, there is a text input field with the path "C:\Users\inkay\Downloads\" and a "Browse..." button. A large text area contains a Base64-encoded PEM certificate, starting with "-----BEGIN CERTIFICATE-----" and ending with "fiUVhH7HHAqMBAAGIzAtMA8GA1UdDwQEAwIHaDATBaNVHSUEDDAKBaBaEFBQcD".

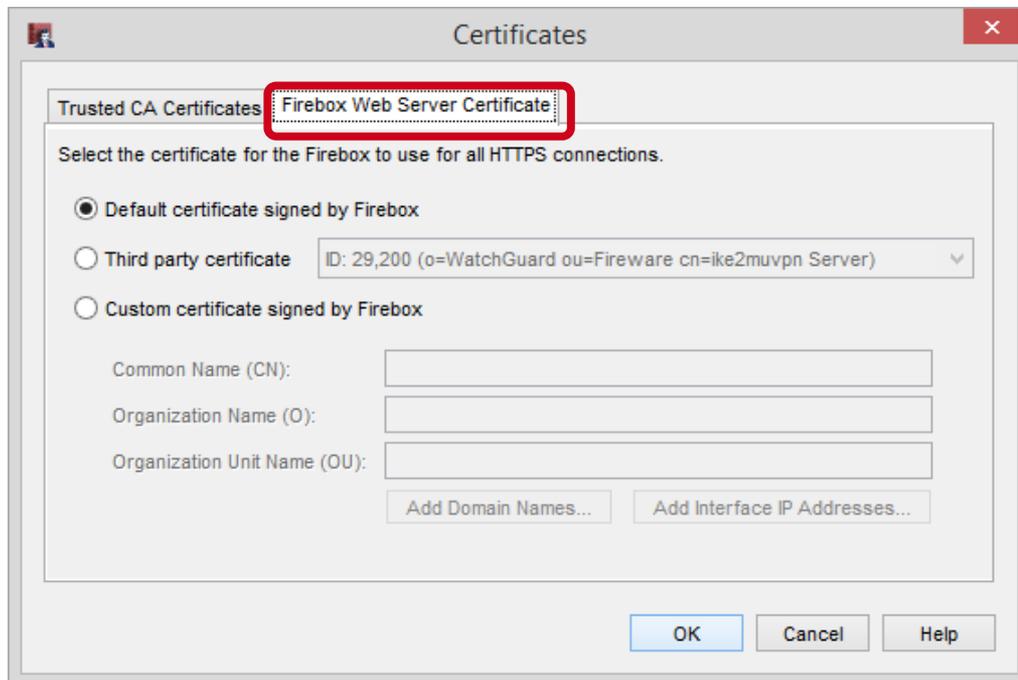
# Firebox Web Server Certificate Management

- 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

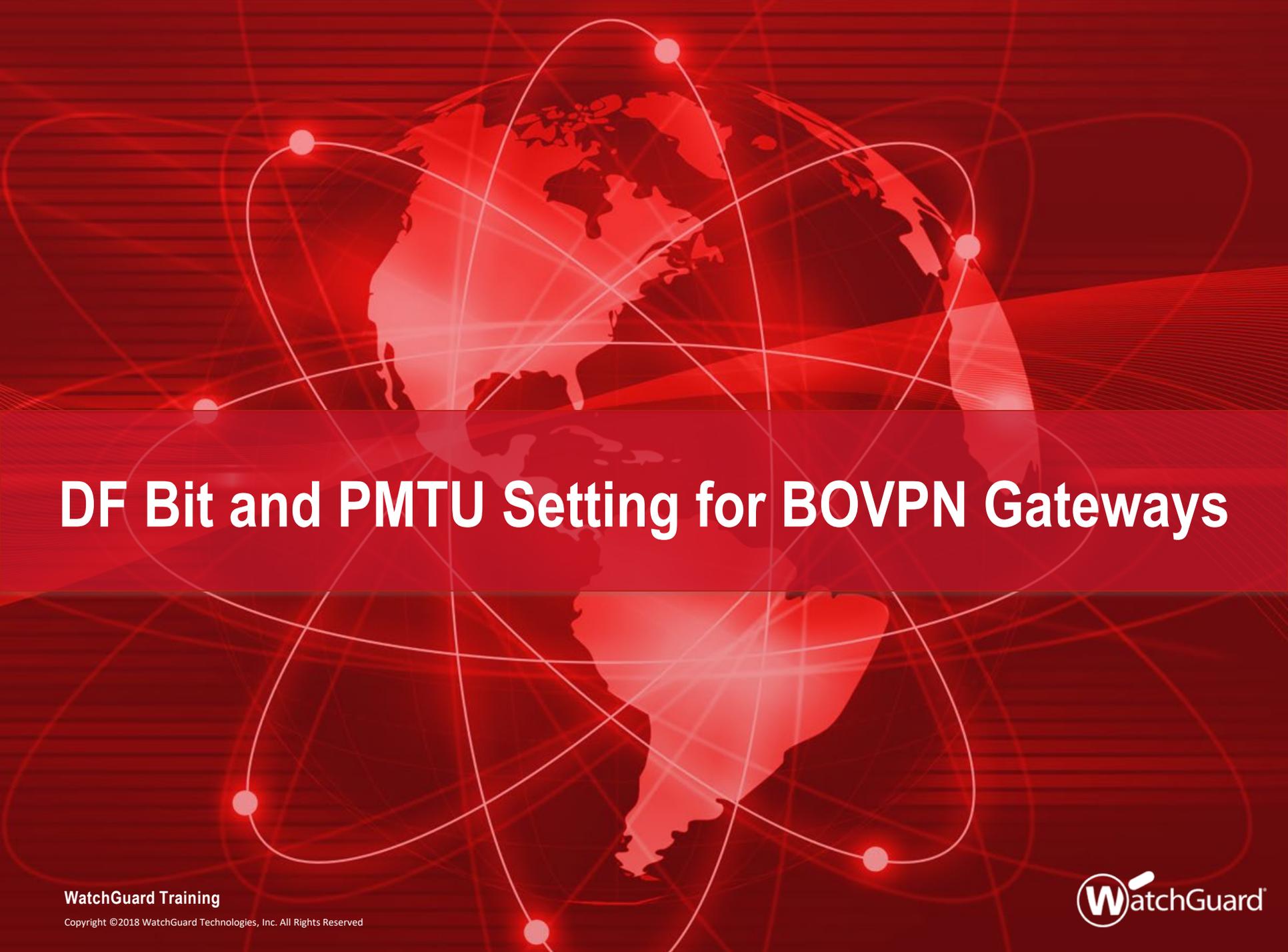
The screenshot displays the WatchGuard Fireware Web UI interface. The top navigation bar shows the WatchGuard logo, the title 'Fireware Web UI', and the user 'admin'. The left sidebar contains a menu with categories: DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, VPN, and SYSTEM. The 'SYSTEM' category is expanded, showing sub-items like Information, Feature Key, NTP, SNMP, WatchGuard Cloud, Managed Device, Logging, Diagnostic Log, Global Settings, and Certificates. The 'Certificates' sub-item is highlighted with a red box. The main content area is titled 'Certificates' and shows a breadcrumb 'Certificates > Firebox Web Server Certificate', where 'Firebox Web Server Certificate' is highlighted with a red box. Below the breadcrumb, there are three radio button options: 'Default Certificate signed by Firebox' (selected), 'Third party certificates', and 'Custom certificate signed by Firebox'. The 'Third party certificates' option has a dropdown menu showing 'ID: 29200 o=WatchGuard ou=Fireware cn=ike2muvpn Server'. The 'Custom certificate signed by Firebox' option has three input fields for 'Common Name (CN)', 'Organization Name (O)', and 'Organization Unit Name (OU)'. Below these options is a section for 'Domain Names' with a text area and a 'DOMAIN NAME' button.

# 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**



The screenshot shows a window titled "Certificates" with a close button in the top right corner. The window contains a tab labeled "Trusted CA Certificates" and a sub-tab labeled "Firebox Web Server Certificate", which is highlighted with a red box. Below the tabs, there is a text prompt: "Select the certificate for the Firebox to use for all HTTPS connections." There are three radio button options: "Default certificate signed by Firebox" (which is selected), "Third party certificate" (with a dropdown menu showing "ID: 29,200 (o=WatchGuard ou=Fireware cn=ike2muvpn Server)"), and "Custom certificate signed by Firebox". Below these options are three text input fields for "Common Name (CN)", "Organization Name (O)", and "Organization Unit Name (OU)". At the bottom of the input fields are two buttons: "Add Domain Names..." and "Add Interface IP Addresses...". At the bottom right of the window are three buttons: "OK", "Cancel", and "Help".



# DF Bit and PMTU Setting for BOVPN Gateways

# 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

Gateway Endpoint Settings

Local Gateway Remote Gateway Advanced

Pre-Shared Key

Specify a different pre-shared key for each gateway endpoint

Pre-Shared Key

**Don't Fragment (DF) Bit**

Enable DF bit settings for this gateway endpoint

Copy - Original DF bit setting of the IPsec packet is copied to the encapsulating header

Set - Firebox cannot fragment IPsec packets regardless of the original bit setting

Clear - Firebox can fragment IPsec packets regardless of the original bit setting

**PMTU**

Enable PMTU settings for this gateway endpoint

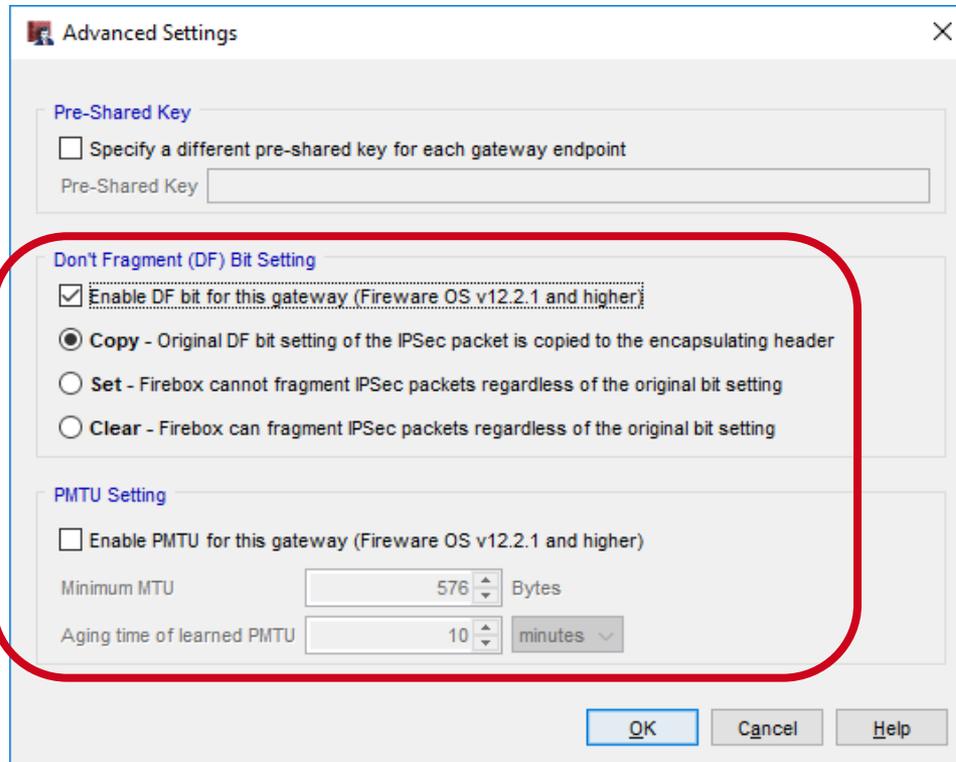
Minimum MTU  bytes

Aging time of learned PMTU  minutes

OK CANCEL

# DF Bit and PMTU for BOVPN Gateways

- Policy Manager



Advanced Settings

Pre-Shared Key

Specify a different pre-shared key for each gateway endpoint

Pre-Shared Key

Don't Fragment (DF) Bit Setting

Enable DF bit for this gateway (Fireware OS v12.2.1 and higher)

Copy - Original DF bit setting of the IPSec packet is copied to the encapsulating header

Set - Firebox cannot fragment IPSec packets regardless of the original bit setting

Clear - Firebox can fragment IPSec packets regardless of the original bit setting

PMTU Setting

Enable PMTU for this gateway (Fireware OS v12.2.1 and higher)

Minimum MTU  Bytes

Aging time of learned PMTU  minutes

OK Cancel Help



# Password Length Control for Firebox-DB Accounts

# 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:

**Inheritance Settings**

Select the template settings that a Firebox can override.

- Policies
- Policy Types
- Schedules
- Aliases
- Proxy Actions
- Content Actions
- TLS Profiles
- HTTPS Exception Overrides
- Application Control
- Data Loss Prevention
- WebBlockers
- Traffic Management
- SNAT
- Authentication Servers
- Authorized Users / Groups
- Quotas Rule
- Quotas Action
- Other

Other

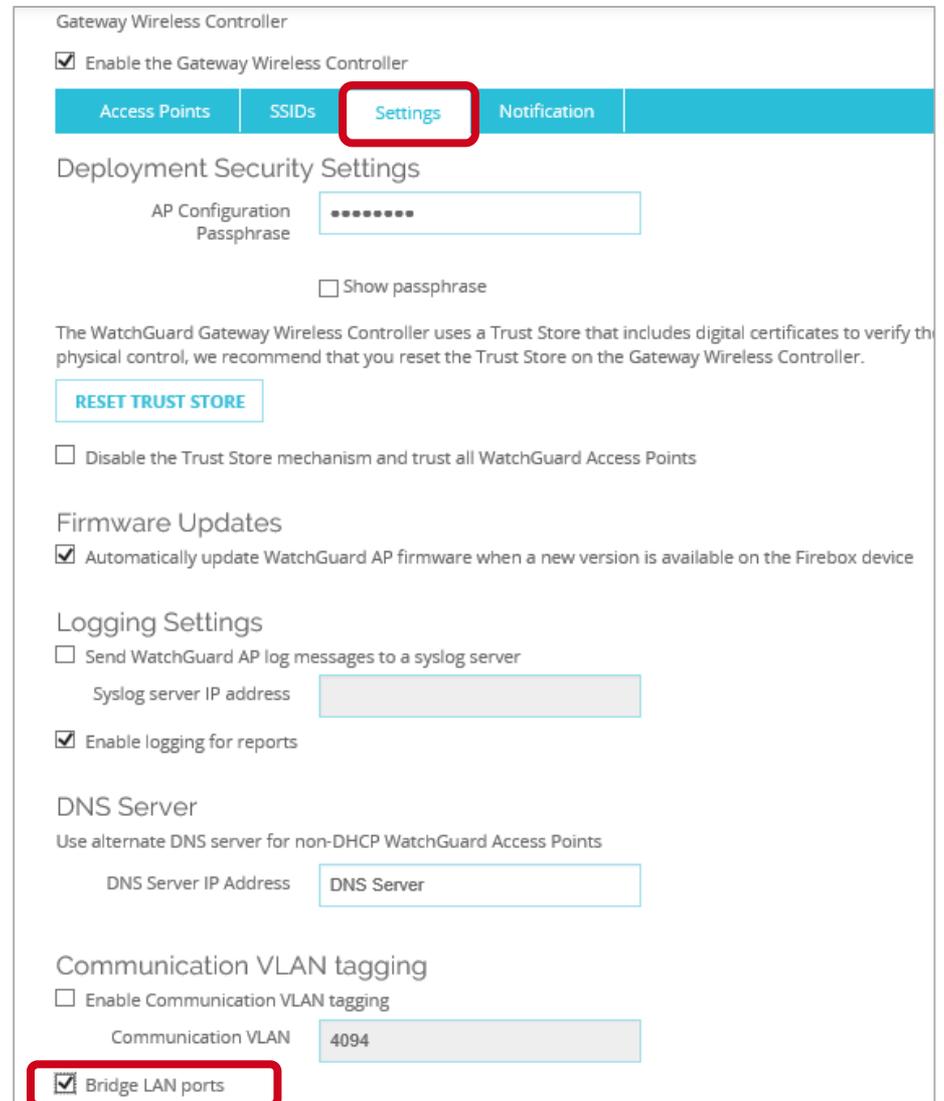
Allow Override	Settings
<input type="checkbox"/>	Account settings for Firebox authentication (Fireware OS v11.12.2 and higher)
<input checked="" type="checkbox"/>	APT Blocker Settings
<input checked="" type="checkbox"/>	Automatic feature key synchronization setting
<input checked="" type="checkbox"/>	Autotask Settings (Fireware OS v12.0.1 and higher)
<input checked="" type="checkbox"/>	Botnet Detection (Fireware OS v11.11 and higher)
<input checked="" type="checkbox"/>	ConnectWise Settings (Fireware OS v11.12 and higher)
<input checked="" type="checkbox"/>	Control of Firebox Generated Traffic (Fireware OS v12.2 and higher)
<input checked="" type="checkbox"/>	Device Administrator Connections setting (Fireware OS v11.10.1 and higher)
<input checked="" type="checkbox"/>	Device Feedback setting
<input checked="" type="checkbox"/>	Diagnostic Log Level
<input checked="" type="checkbox"/>	DLP Global Settings
<input checked="" type="checkbox"/>	DNSWatch (Fireware OS v12.1.1 and higher)
<input checked="" type="checkbox"/>	Enable automatic update of trusted CA certificates (Fireware OS v11.10 and higher)
<input checked="" type="checkbox"/>	Enable feature keys expired notification (Fireware OS v11.10.1 and higher)
<input checked="" type="checkbox"/>	Fault Report setting
<input checked="" type="checkbox"/>	Gateway AntiVirus 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



Gateway Wireless Controller

Enable the Gateway Wireless Controller

Access Points | SSIDs | **Settings** | Notification

Deployment Security Settings

AP Configuration Passphrase

Show passphrase

The WatchGuard Gateway Wireless Controller uses a Trust Store that includes digital certificates to verify the physical control, we recommend that you reset the Trust Store on the Gateway Wireless Controller.

[RESET TRUST STORE](#)

Disable the Trust Store mechanism and trust all WatchGuard Access Points

Firmware Updates

Automatically update WatchGuard AP firmware when a new version is available on the Firebox device

Logging Settings

Send WatchGuard AP log messages to a syslog server

Syslog server IP address

Enable logging for reports

DNS Server

Use alternate DNS server for non-DHCP WatchGuard Access Points

DNS Server IP Address

Communication VLAN tagging

Enable Communication VLAN tagging

Communication VLAN

Bridge LAN ports



# Backup and Restore Enhancements

# Backup and Restore Enhancements

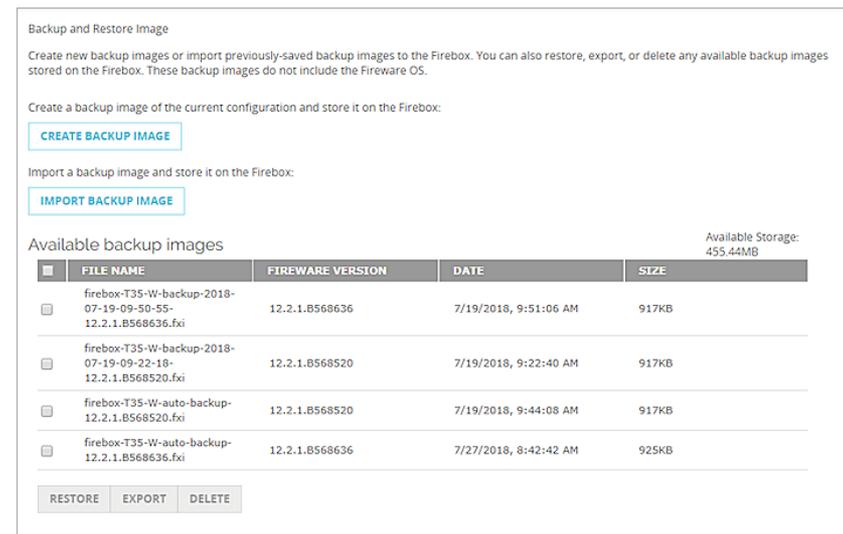
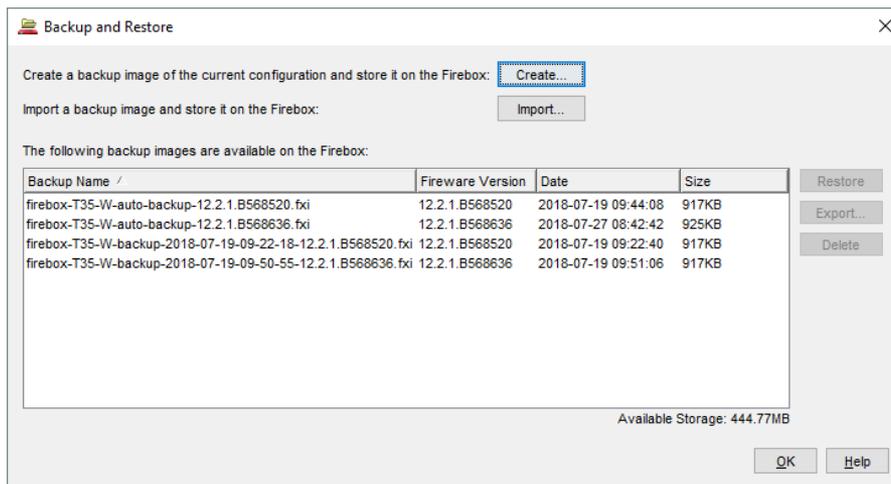
- Fireware v12.2.1 includes these backup image enhancements:
  - New Backup and Restore Image page to create, restore, and manage backup image files
  - Backup images are now stored on the Firebox
  - Backup images no longer include the Fireware OS
  - Backup images are now created automatically every 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**



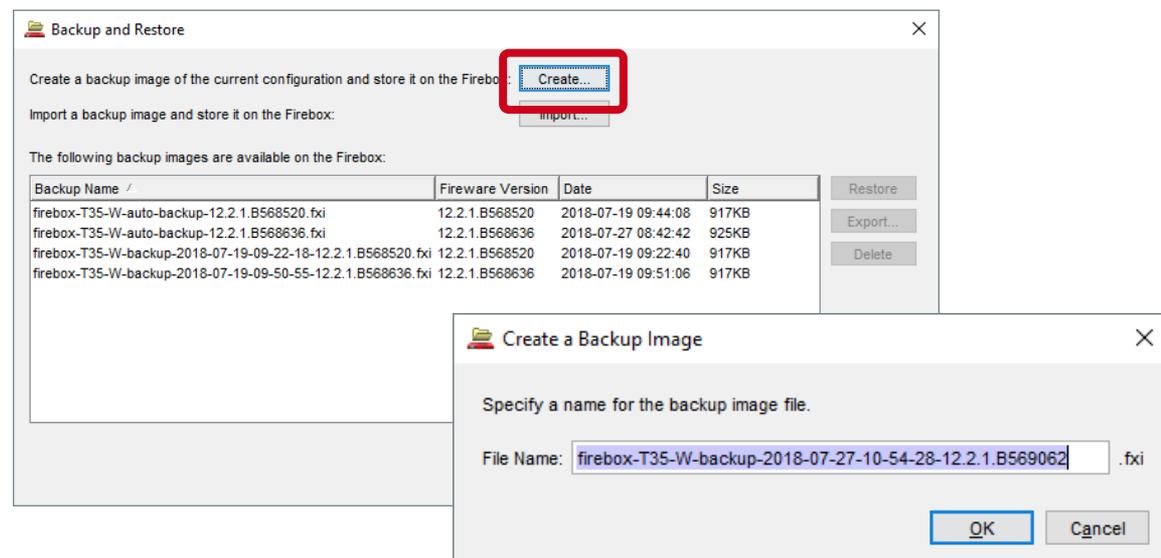
# Backup and Restore Image

- 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



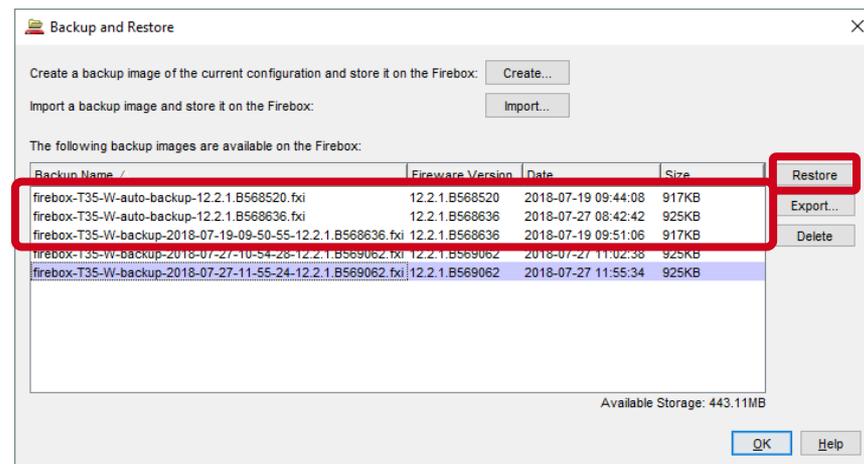
# Create New Backup Image

- 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



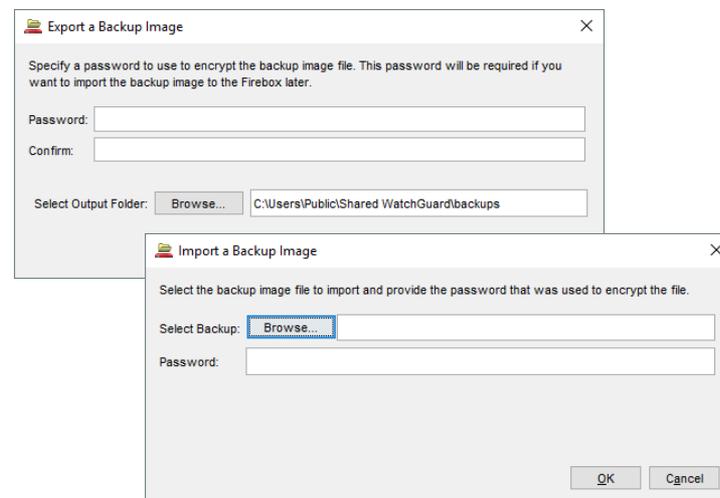
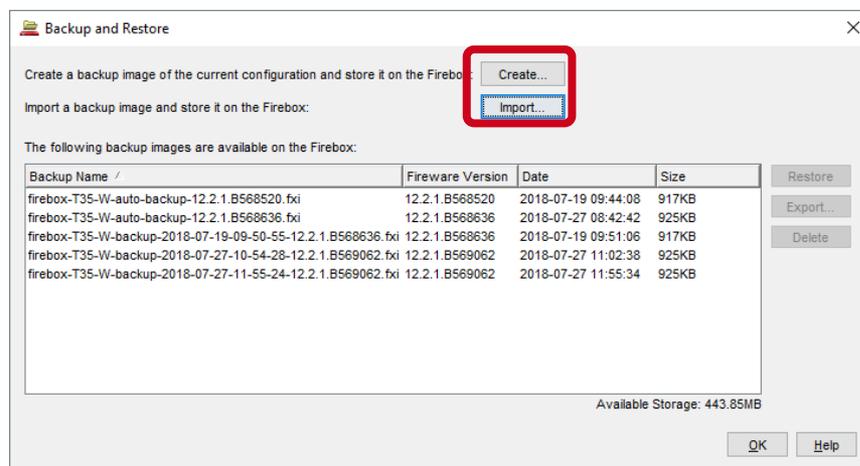
# Restore Backup Images

- 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



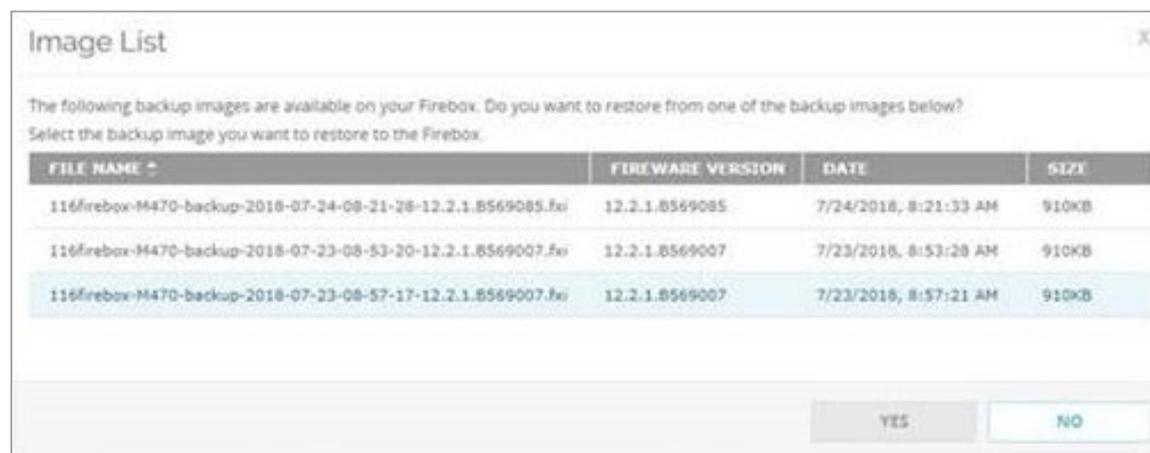
# Export and Import Backup Images

- 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

**SafeSearch**  
You can enforce SafeSearch for major search engines such as Google, Yahoo, Bing, YouTube. You can also select an enforcement level for YouTube.

Enforce SafeSearch  
SafeSearch enforcement level for YouTube: **Strict** (Fireware OS v12.2.1 and higher)

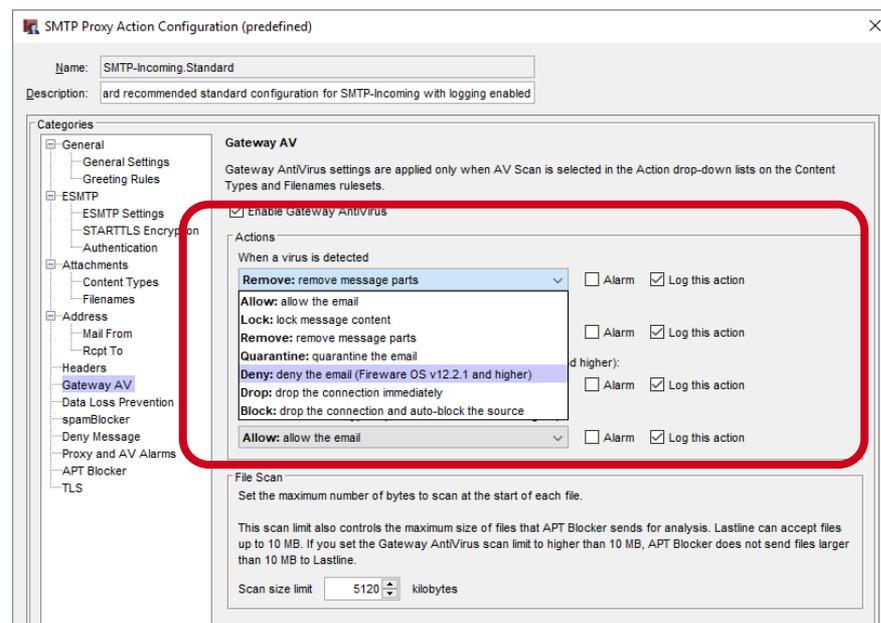
Enable logging for reports

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

# SMTP-proxy Action Updates

# SMTP-proxy Action Updates

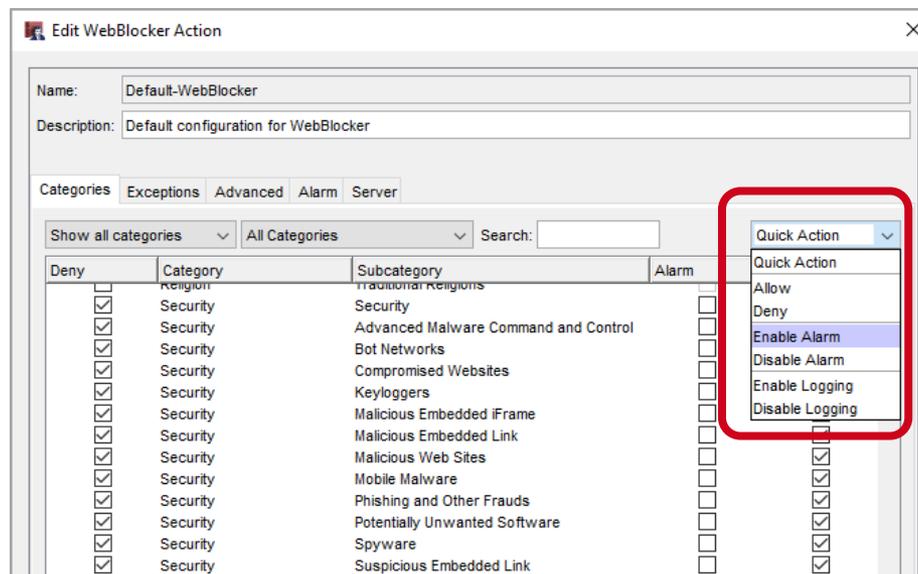
- In SMTP-proxy actions, you can now select **Deny** when you configure the following:
  - Gateway AV actions
  - spamBlocker Virus Outbreak Detection actions
- When Deny is selected, Gateway AV or spamBlocker denies delivery of the message
- The Firebox sends an SMTP 554 Transaction Failed response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

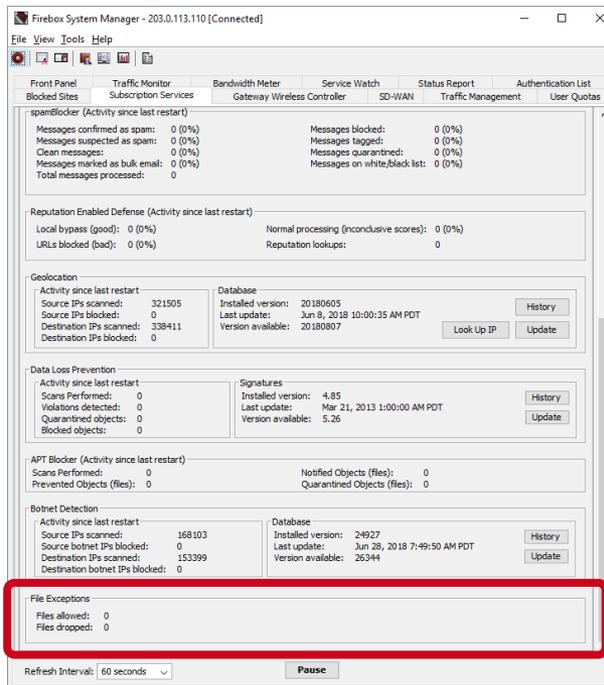
# WatchGuard IPSec Mobile VPN Client

- 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:
  - Firewall Web UI > Dashboard > Subscription Services
  - Firebox System Manager > Subscription Services tab



The screenshot displays the Firebox System Manager interface, specifically the Subscription Services tab. The interface shows various security and performance metrics. At the bottom of the main content area, the 'File Exceptions' section is highlighted with a red box. This section displays the following statistics:

File Exceptions
Files allowed: 0
Files dropped: 0

Below the File Exceptions section, there is a 'Refresh Interval' dropdown menu set to '60 seconds' and a 'Pause' button.



**Thank You!**