What's New in Fireware v12.4

WatchGuard Training

What's New in Fireware v12.4

- SD-WAN action enhancements
- SD-WAN reporting enhancements
- Link Monitor enhancements
- WebBlocker Warn action
- DNSWatch available in Bridge Mode
- IPv6 support for BOVPN and BOVPN virtual interfaces
- Support for multiple syslog servers
- Proxy support for TLS v1.3
- Enhanced FireCluster Diagnostics page

What's New in Fireware v12.4

- Geolocation Deny message
- Exceptions/Blocked Sites List enhancements
- Synchronize feature key enhancements
- Proxy enhancements for DNSWatch
- FQDN limit increase
- MD5 in Gateway AV/IntelligentAV logs
- RADIUS and SecurID enhancements
- SSO Debug Tool enhancements
- Access Portal RDP enhancements

What's New in Fireware v12.4

- Technology Integrations page updates
- Device configuration template updates
  - QoS
  - DNS/WINS
  - WebBlocker Warn action
- Edit 1-to-1 NAT in the Web UI

SD-WAN Enhancements

WatchGuard Training

SD-WAN Enhancements

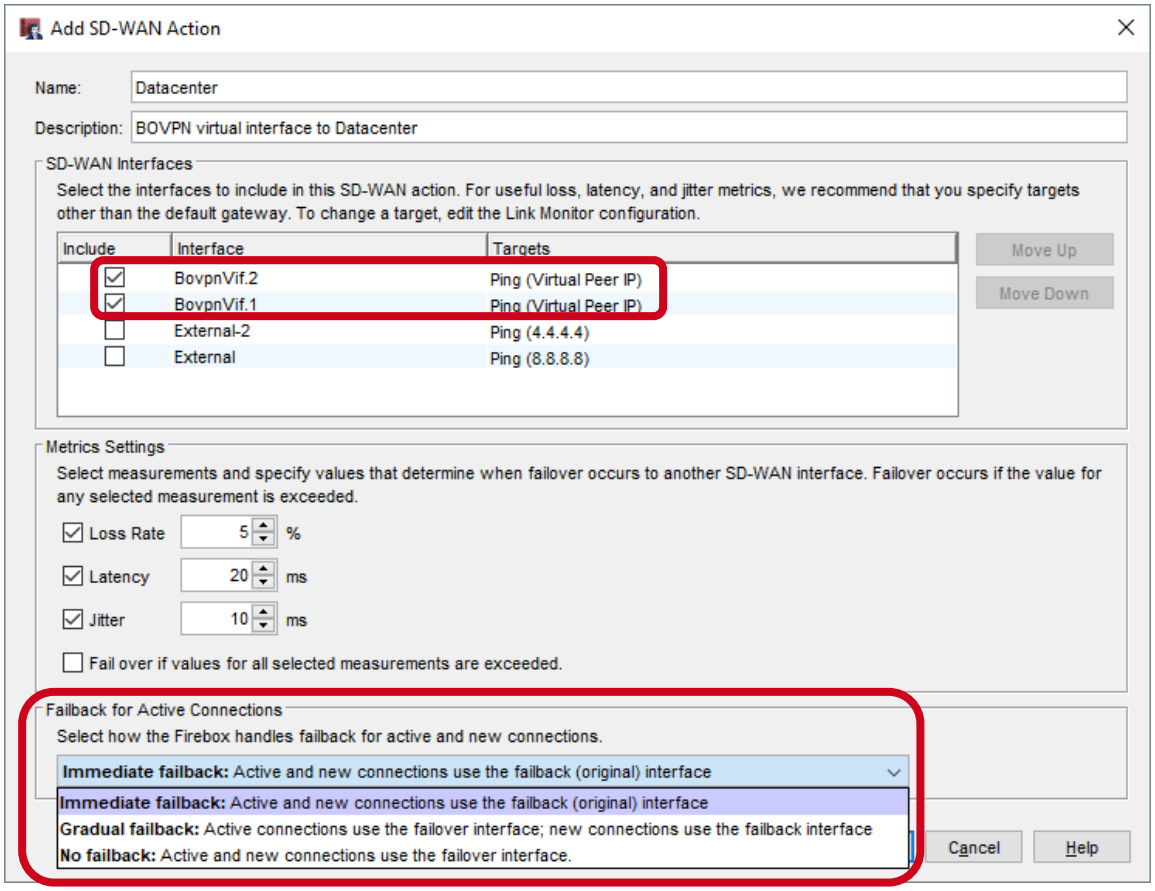
- As development continues on our SD-WAN solution, SD-WAN benefits now extend to more than just external WAN connections
- With these enhancements, you can now downsize or eliminate expensive MPLS connections
  - For example, an SD-WAN implementation with BOVPN virtual interfaces and metrics-based failover gives you encrypted tunnels over the public Internet plus reliability

SD-WAN Enhancements

- SD-WAN actions now support:
  - Multiple BOVPN virtual interfaces
  - Internal interfaces (Trusted, Optional, and Custom)
- With these enhancements, you can now:
  - Measure loss, latency, and jitter on internal interfaces and BOVPN virtual interfaces
  - Fail over based on loss, latency, and jitter for internal interfaces and BOVPN virtual interfaces
  - Use a policy and SD-WAN action to route traffic on any interface
    - This includes internal interfaces configured for private network links

SD-WAN — BOVPN Virtual Interface Failover

- You can now configure BOVPN virtual interface failover in an SD-WAN action



SD-WAN — BOVPN Virtual Interface Failover

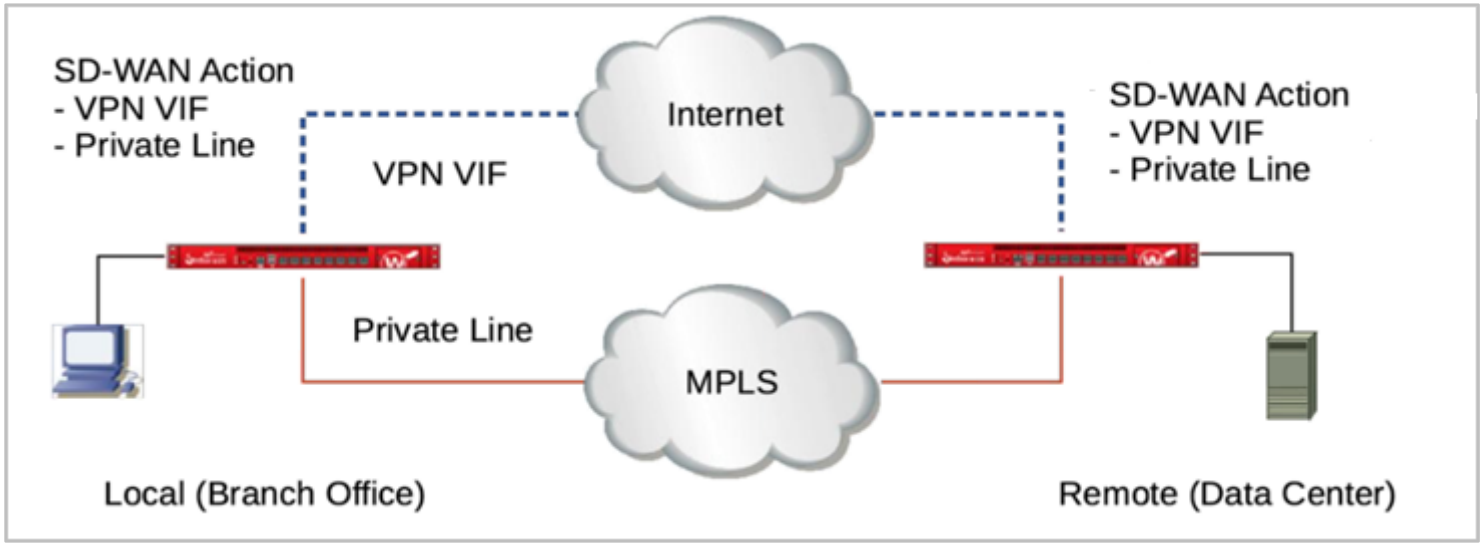
- You can select to fail over based on loss, latency, or jitter measurements
  - If you do not select any measurements, failover occurs if the primary connection fails
- Requirements for BOVPN virtual interface failover:
  - In the BOVPN virtual interface settings for both interfaces, you must configure a virtual peer IP address
  - The virtual peer IP address must be an IP address and not a netmask
  - You must add both interfaces to Link Monitor. For BOVPN virtual interfaces, the link monitor target is the virtual peer IP address and cannot be changed

SD-WAN for Internal Interfaces

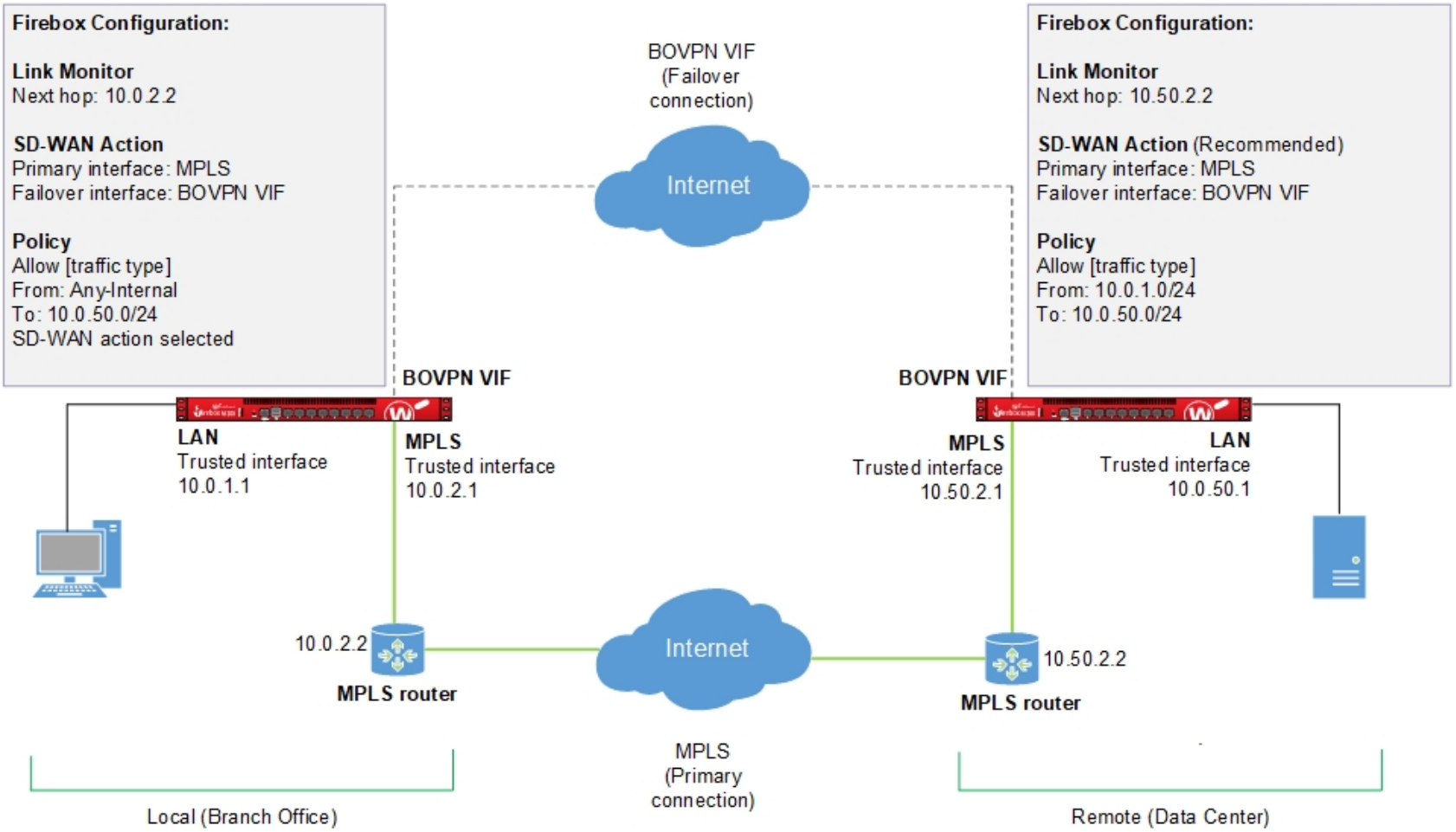
- You can now include internal interfaces in an SD-WAN configuration
  - This includes Trusted, Optional, and Custom interfaces
- If you have a private network connection such as a private line, leased line, or MPLS configured on an internal interface, you can configure SD-WAN failover to another connection

SD-WAN for Internal Interfaces

- Example topology
  - An MPLS connection is the primary connection for traffic to a remote data center
  - The MPLS connection uses an internal interface on the Firebox
  - The BOVPN virtual interface is configured as a failover interface

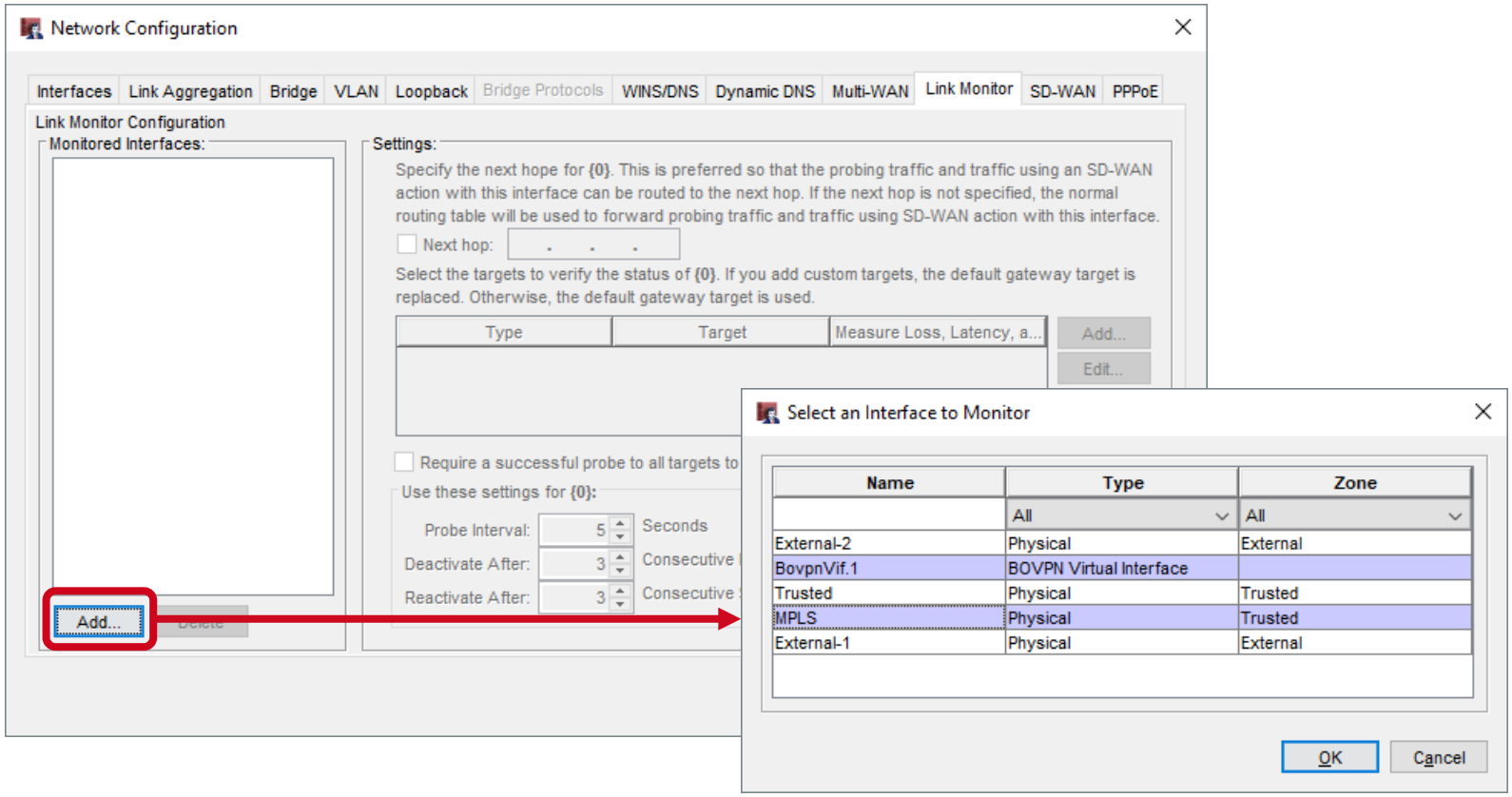


SD-WAN for Internal Interfaces



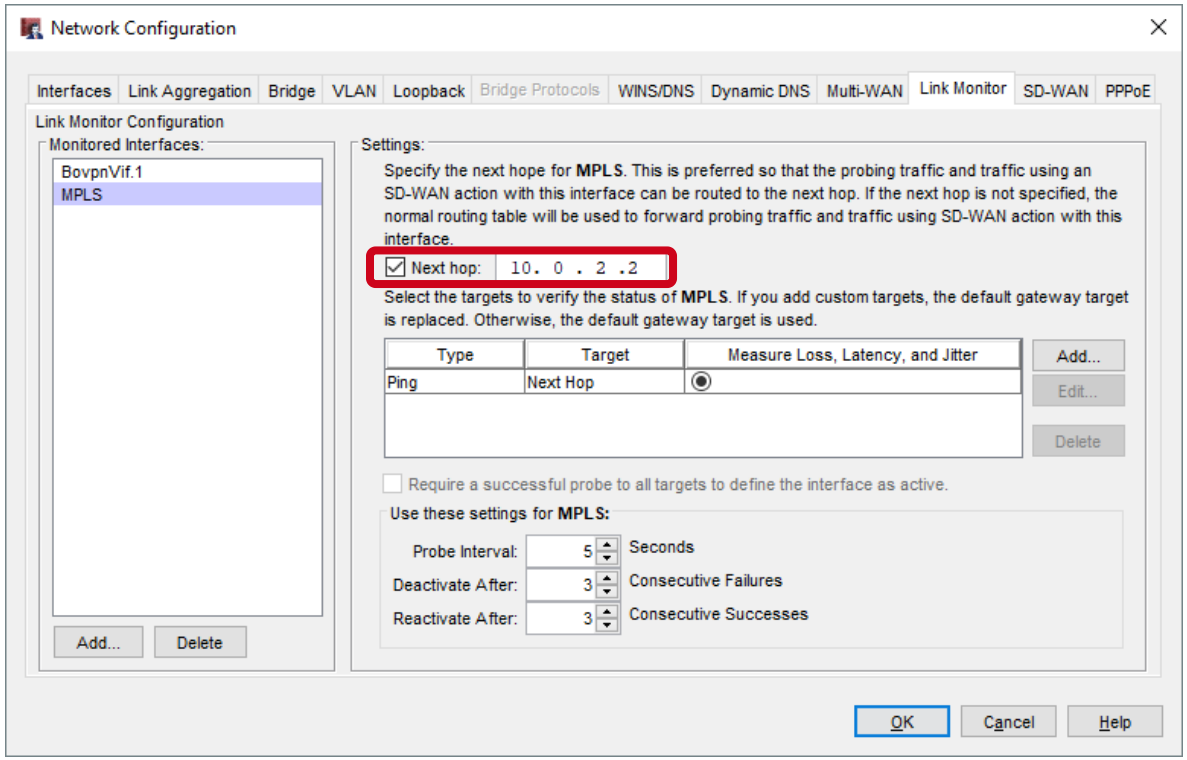
SD-WAN for Internal Interfaces

- Example configuration at the local site (the branch office)
  - In the Link Monitor settings, add the BOVPN virtual interface and the internal interface used for the MPLS connection



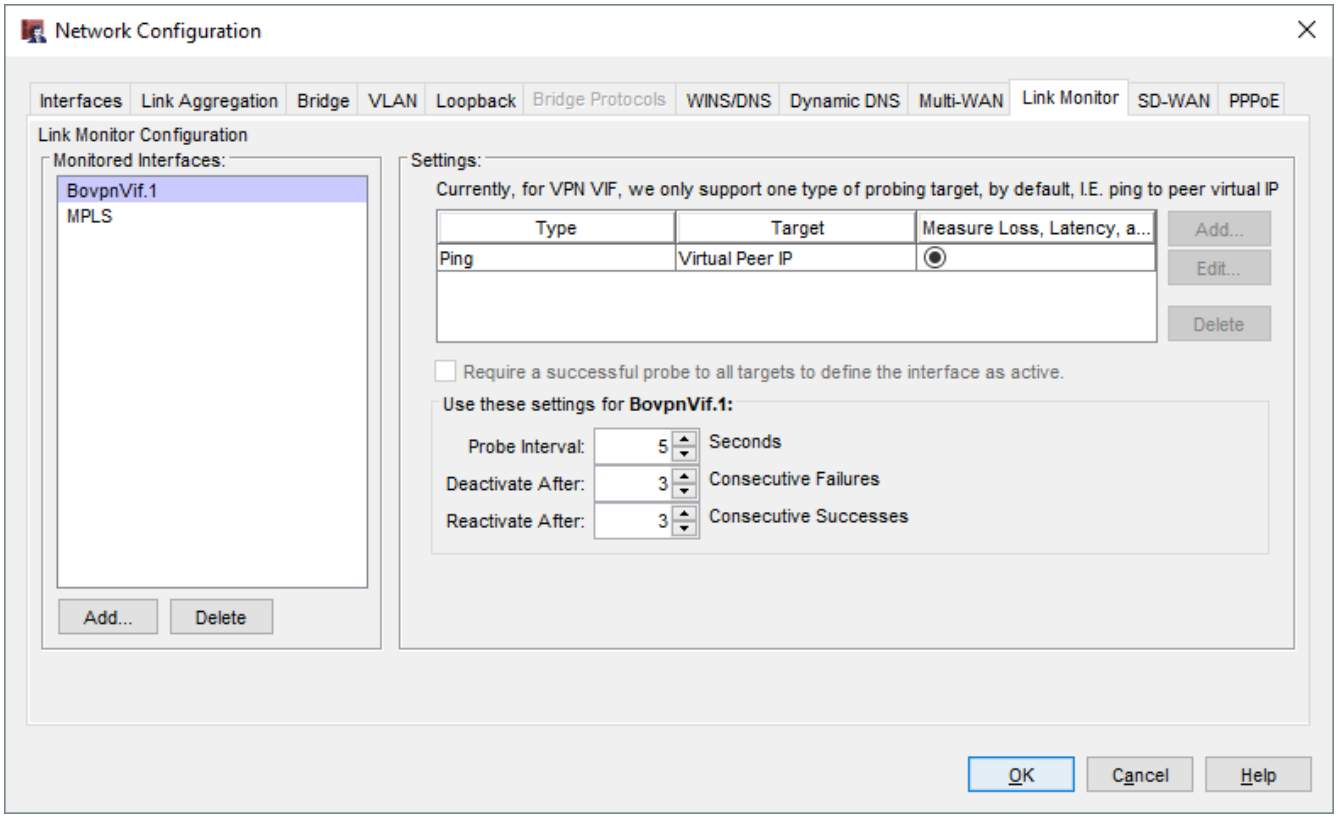
SD-WAN for Internal Interfaces

- For the MPLS interface, specify the IP address of the next hop
  - In our example, the next hop is the local side of the local MPLS router



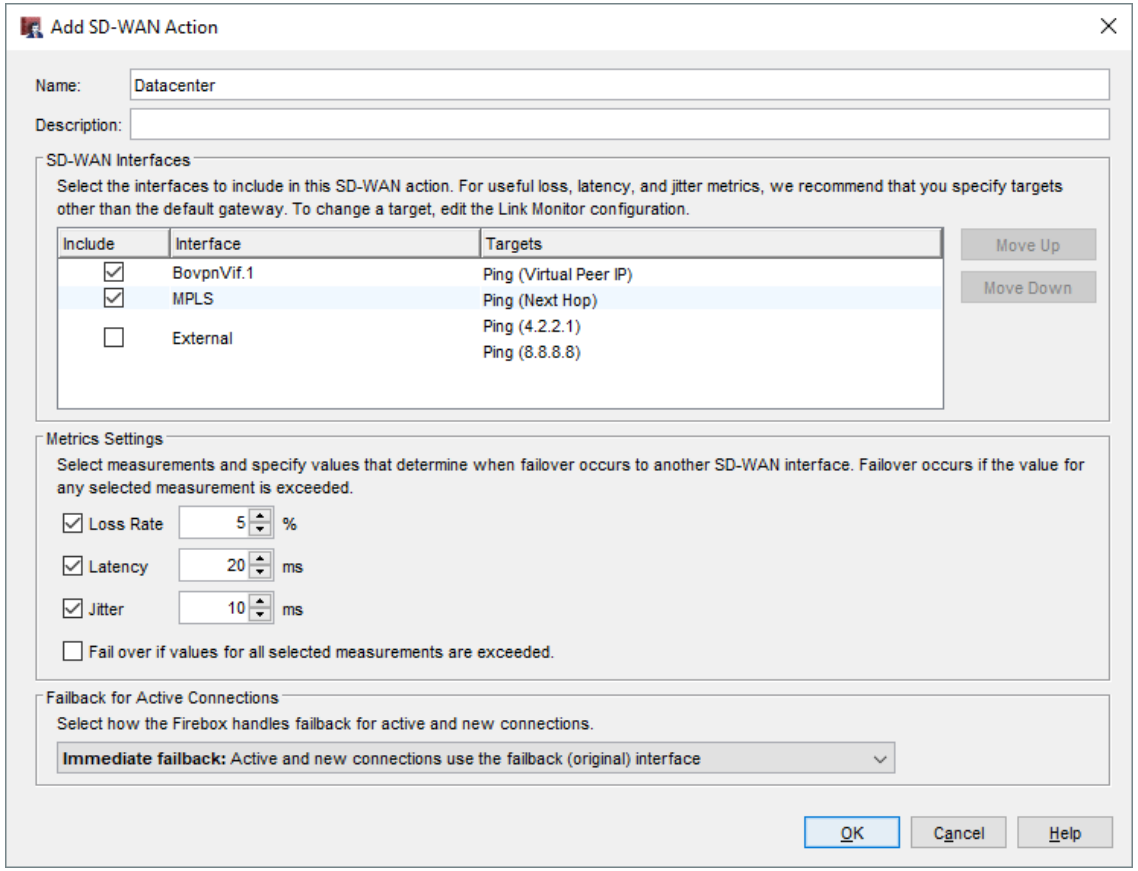
SD-WAN for Internal Interfaces

- The Link Monitor target for the BOVPN virtual interface is the IP address of the remote VPN peer



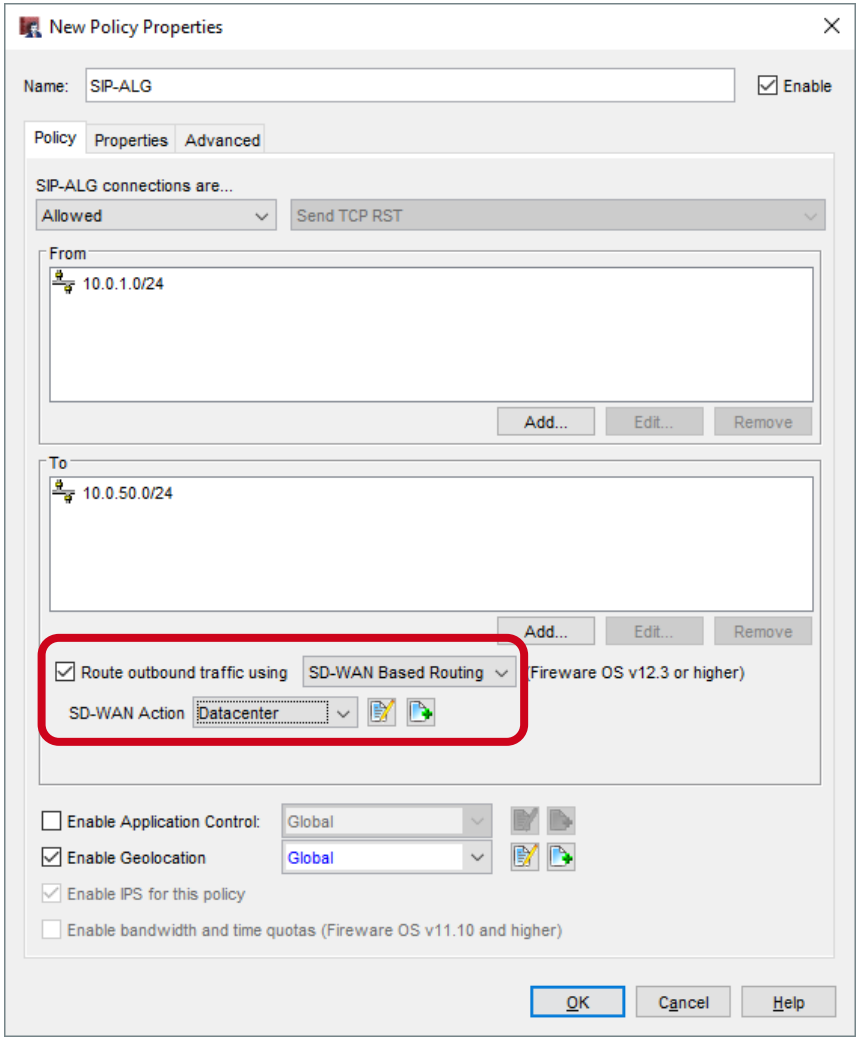
SD-WAN for Internal Interfaces

- Next, add an SD-WAN action that includes the MPLS interface and the BOVPN virtual interface, and specify metric settings



SD-WAN for Internal Interfaces

- Finally, add a policy that specifies the SD-WAN action
  - In our example, traffic that matches this policy is sent over the MPLS connection to the local network at the Datacenter
- If MPLS performance does not meet your requirements, or the link fails, traffic fails over to the BOVPN VIF



SD-WAN for Internal Interfaces

- Static routes and SD-WAN
  - Different factors determine whether static routes are recommended or required
  - **Sites that initiate traffic** — If both sites have Fireboxes configured with SD-WAN actions, you do not have to add a static route on a Firebox that initiates traffic in most cases
  - **Sites that receive traffic** — We recommend that you add static routes on a Firebox at a site that receives traffic
  - You must add a static route if you did not specify a next hop IP address for an internal interface

SD-WAN for Internal Interfaces

- IP Spoof Attack protection and SD-WAN
  - If the global **Drop Spoofing Attacks** setting is enabled, the Firebox monitors inbound traffic on internal and external interfaces for IP spoof attacks
  - If the Firebox determines traffic is not an IP spoof attack, the Firebox sends reply traffic through the same interface as the inbound interface
  - For internal interfaces:
    - If the interface in the routing results does not match the inbound interface, the Firebox considers the inbound traffic to be an IP spoof attack
    - The Firebox drops the inbound traffic and does not send reply traffic
  - If you add static routes, make sure to configure route metrics correctly

SD-WAN

- Restrictions to interface type changes:
  - In most cases, you cannot change the interface type (zone) for an interface included in an SD-WAN action
  - If the interface type is internal (Trusted, Optional, or Custom) you can change the interface type to another internal type
    - For example, if a Trusted interface appears in an SD-WAN action, you can change the interface type to Optional or Custom

SD-WAN Configuration Conversion

- **Important**: Before you upgrade to Fireware v12.4 or higher, review the Release-specific upgrade notes in the WatchGuard Knowledge Base about a change that affects some inbound NAT policies with policy-based routing or an SD-WAN action
  - In Fireware v12.3.1 or lower, the Firebox ignored unnecessary policy-based routing or SD-WAN actions in inbound NAT policies
  - To support SD-WAN enhancements in v12.4, when you upgrade to Fireware v12.4 or higher:
    - For policies with a SNAT action to an RFC1918 address, the Firebox automatically removes policy-based routing or SD-WAN actions to external interfaces unless the action specifies only a BOVPN virtual interface
    - RFC1918 includes the networks `192.168.0.0/16`, `172.16.0.0/12`, and `10.0.0.0/8`

SD-WAN Configuration Conversion

- For policies with 1-to-1 NAT to an internal address:
  - The Firebox does not automatically remove policy-based routing or SD-WAN actions to external interfaces
  - We recommend that you manually remove any policy-based routing or SD-WAN action that is unnecessary

SD-WAN Reporting Enhancements

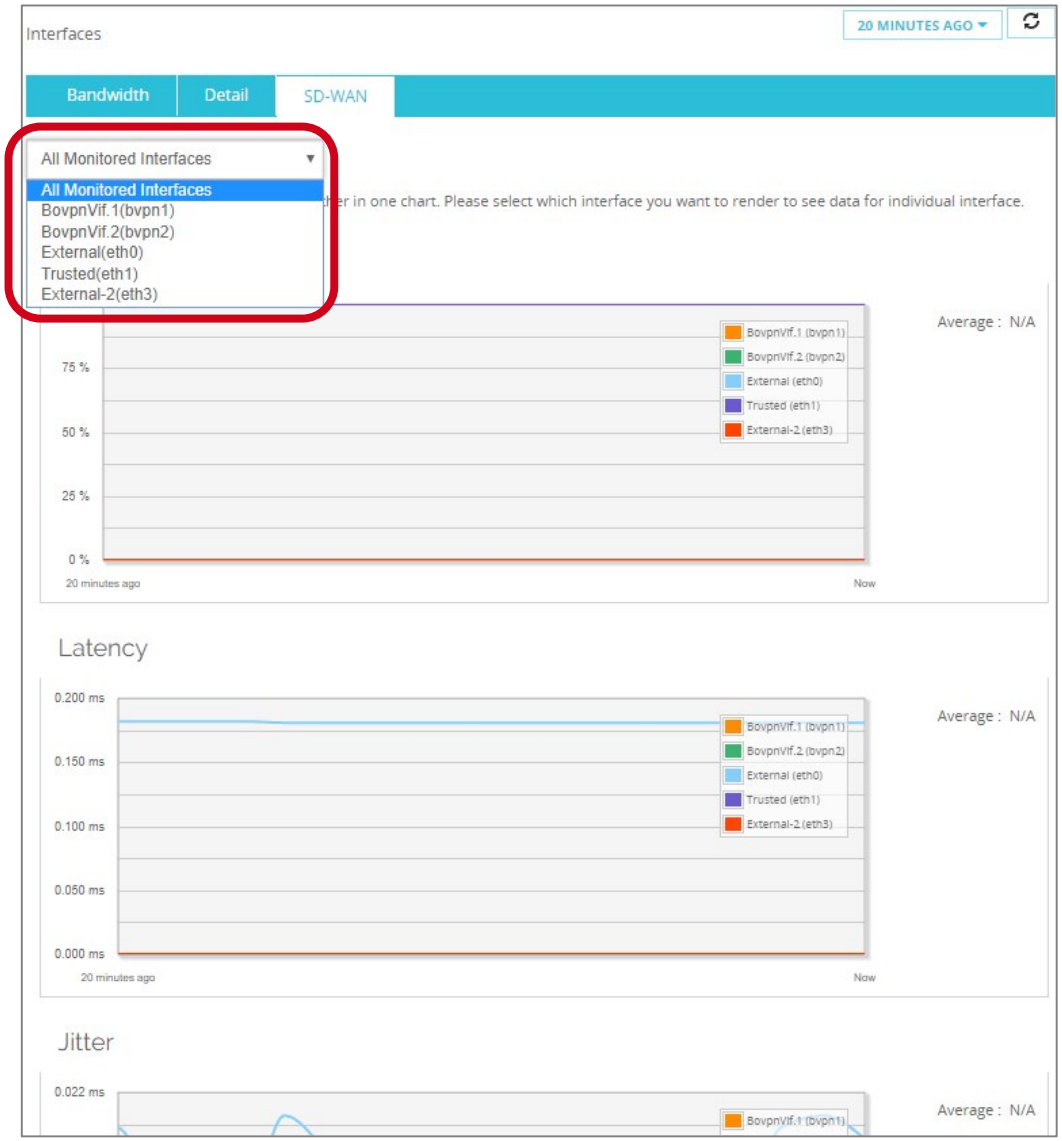
WatchGuard Training

SD-WAN Reporting Enhancements

- On the SD-WAN reporting page:
  - Internal interfaces (Trusted, Optional, and Custom) configured with Link Monitor targets now appear
  - BOVPN virtual interfaces configured with Link Monitor targets now appear
  - Interfaces are grouped by type instead of alphabetically
  - A maximum of 64 interfaces can appear in the Monitored Interfaces list
  - A maximum of 15 interfaces can appear simultaneously on each chart

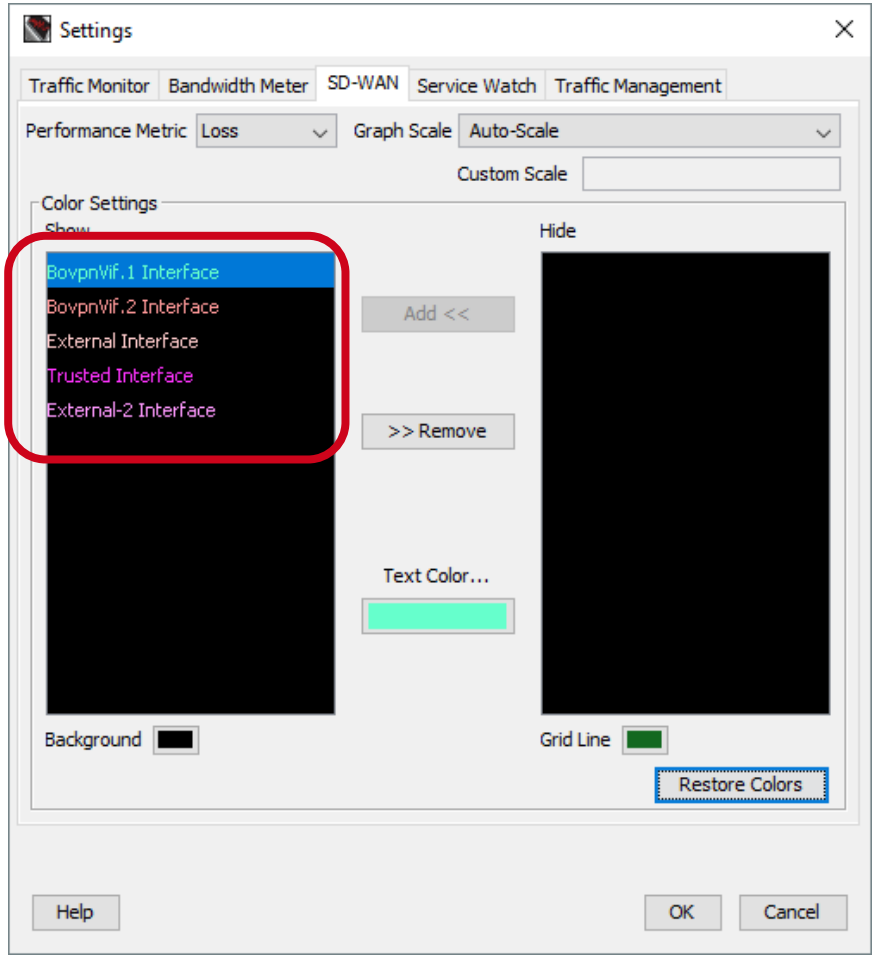
SD-WAN Reporting Enhancements

- SD-WAN reporting page in the Web UI



SD-WAN Reporting Enhancements

- SD-WAN reporting page in Firebox System Manager



Link Monitor Enhancements

WatchGuard Training

Link Monitor — Enhancements

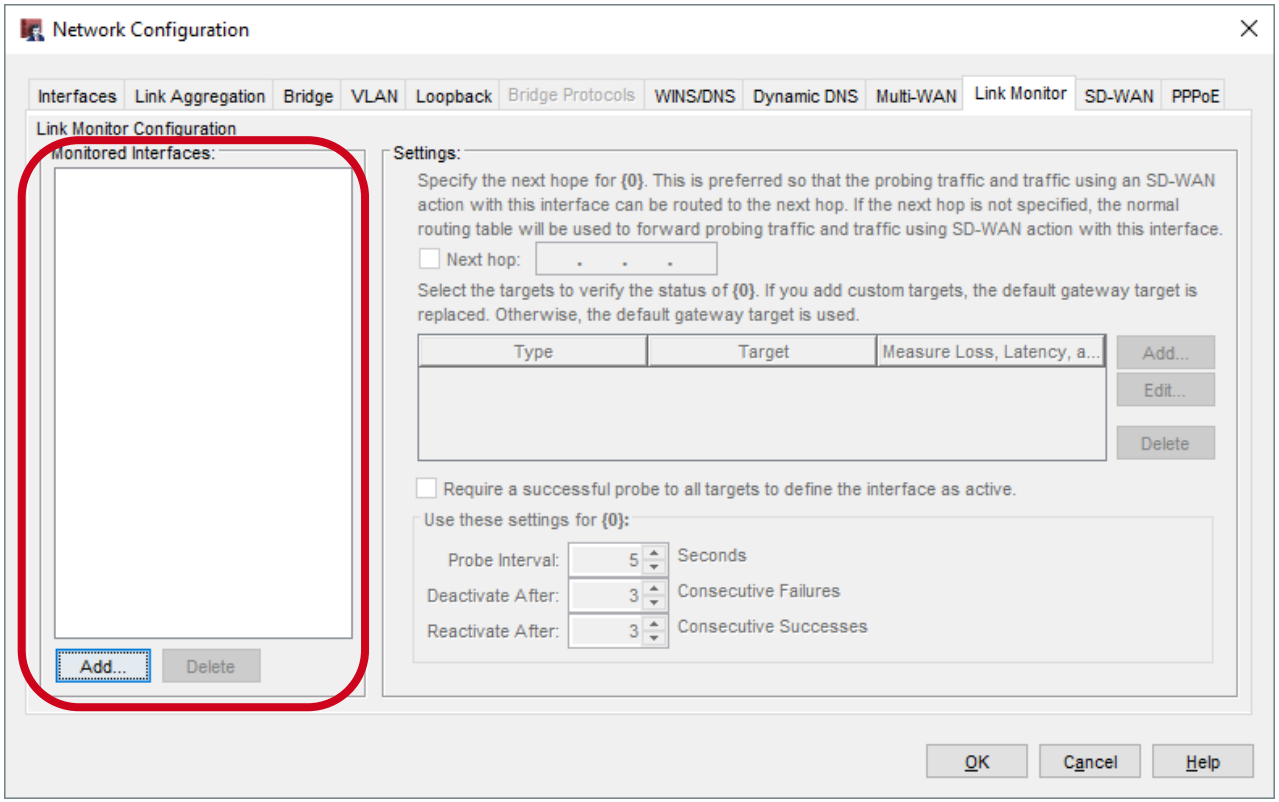
- Link Monitor has these enhancements:
  - You can now add Internal interfaces (Trusted, Optional, and Custom) and BOVPN virtual interfaces to Link Monitor
    - For example, you can monitor an internal interface that is used for a private network link such as an MPLS connection, private line, or leased line
  - You can now select to monitor single WAN interfaces in Link Monitor
  - Link Monitor is not enabled by default for interfaces

Link Monitor — Interfaces List

- In the Link Monitor configuration, now only monitored interfaces appear
  - Monitored interfaces are interfaces for which a target is configured
  - For example, if the interface **External-2** does not have a Link Monitor target, **External-2** does not appear in the Link Monitor interfaces list
- When you configure a new interface on the Firebox, Link Monitor is not automatically enabled for that interface
  - For example, if you add a new External interface, you must manually add that interface to Link Monitor
  - For External interfaces, we recommend that you configure a target other than the default gateway

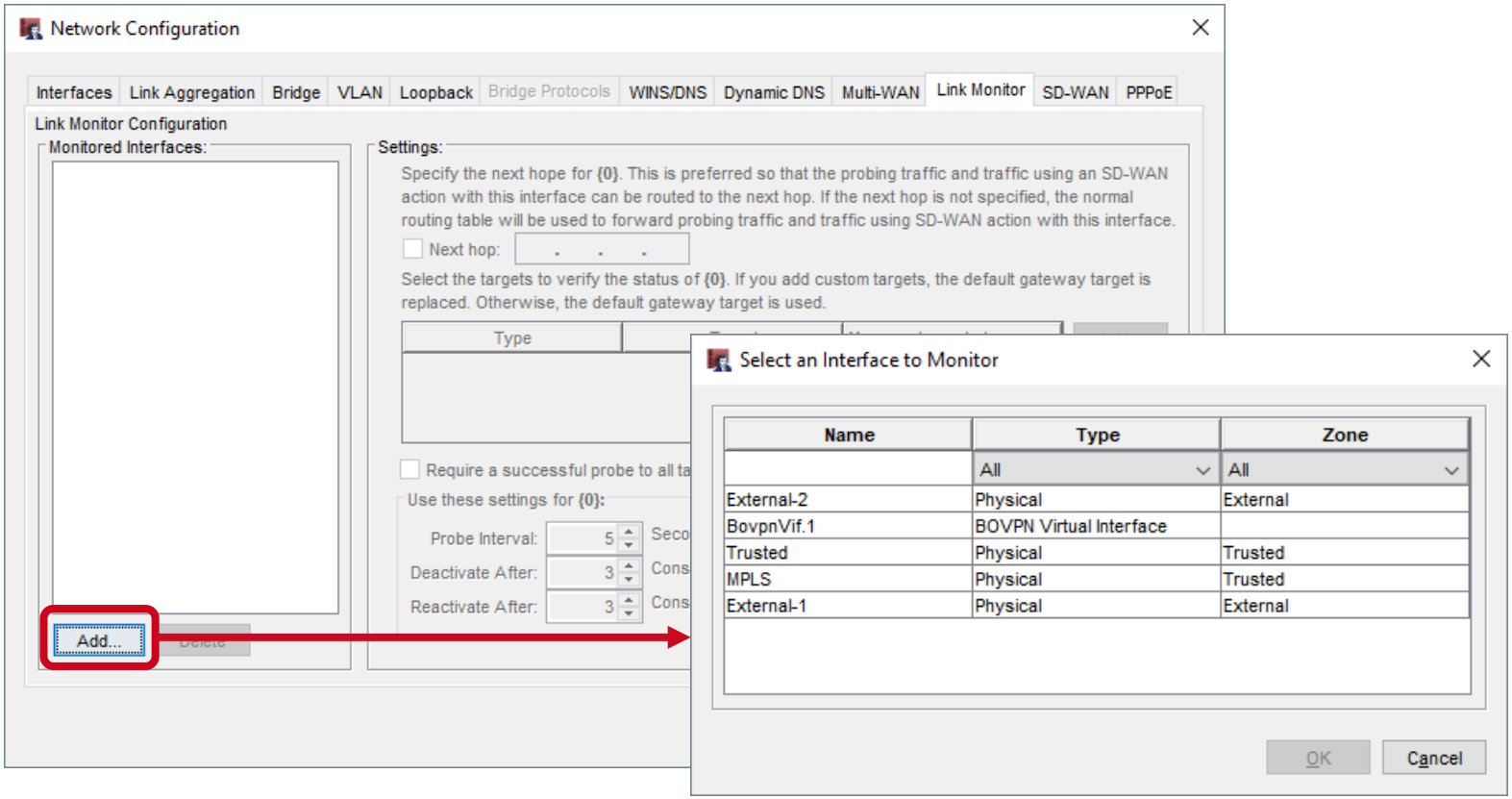
Link Monitor — Interfaces List

- Interfaces list in Link Monitor



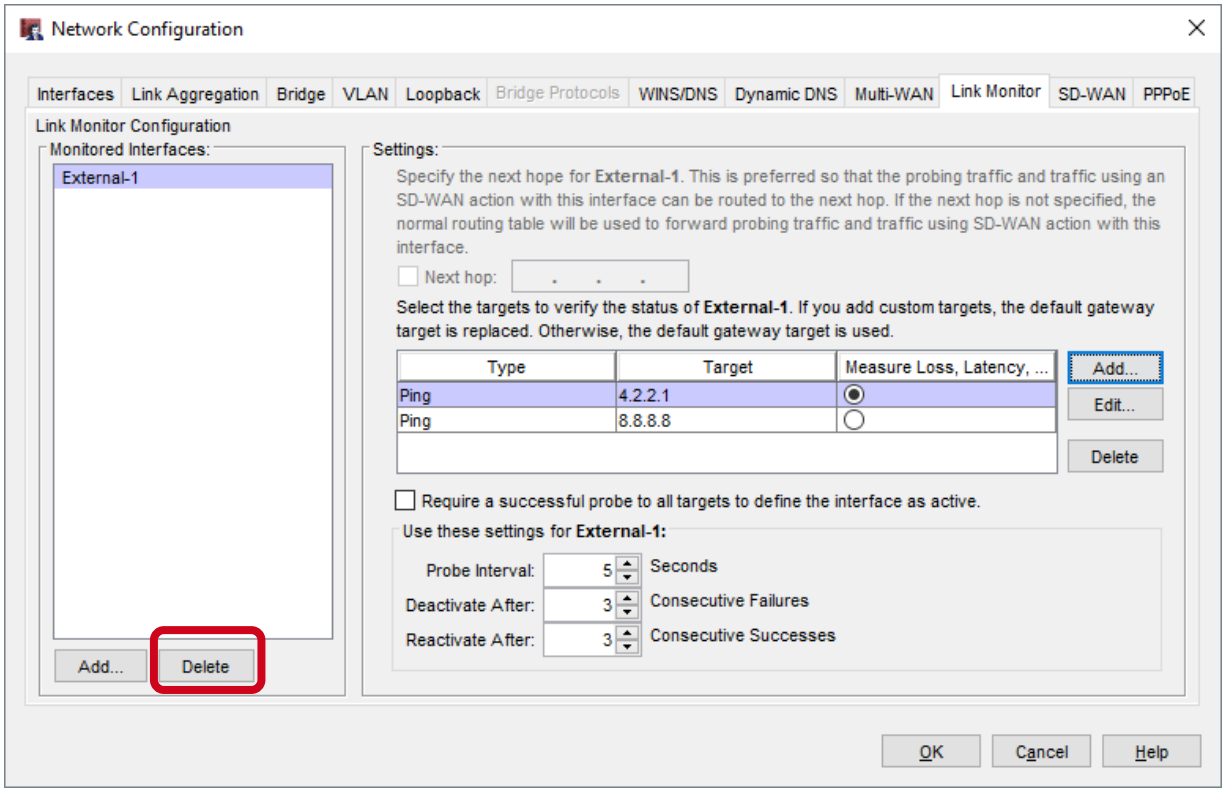
Link Monitor — Interfaces List

- To configure a target for an interface, you must first add the interface to the Link Monitor interfaces list
- Add an interface to the list of monitored interfaces



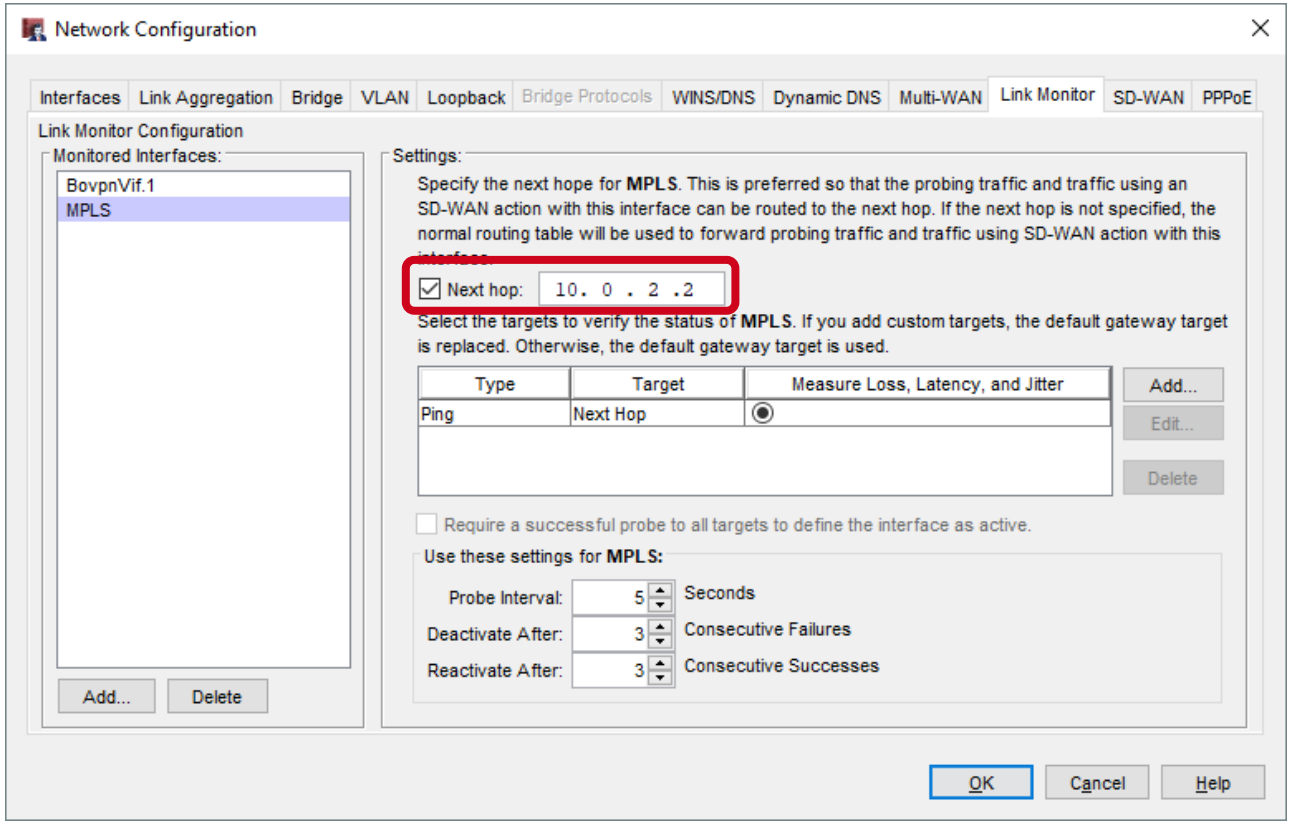
Link Monitor — Interfaces List

- Only the interfaces you add appear in the list
- To remove monitoring for an interface, you can delete the interface from the Link Monitor interfaces list



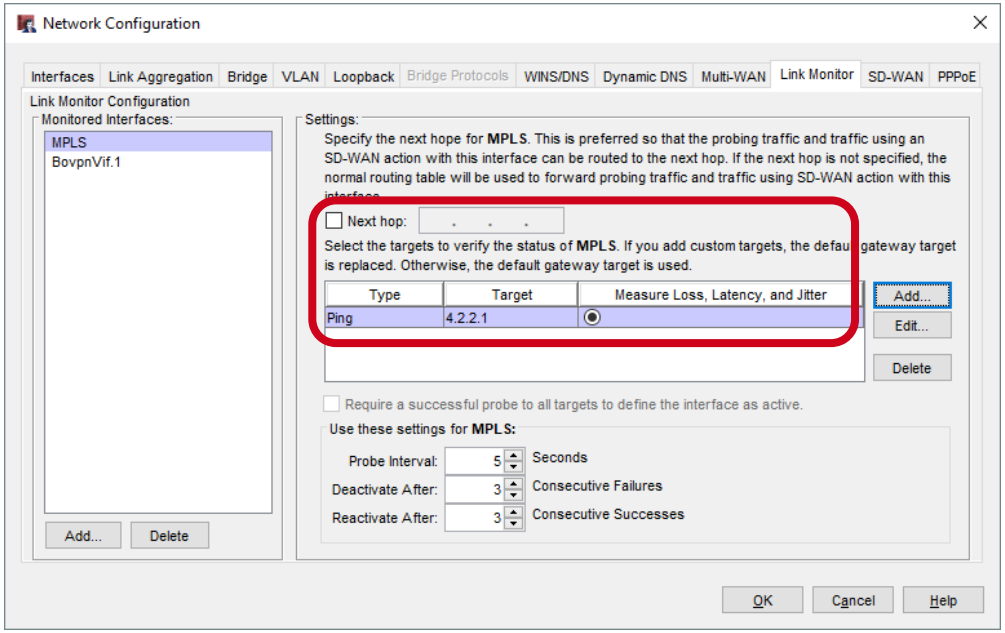
Link Monitor — Internal Interfaces

- When you add a Trusted, Custom, or Optional interface to Link Monitor, you must specify either a next hop IP address or a custom target



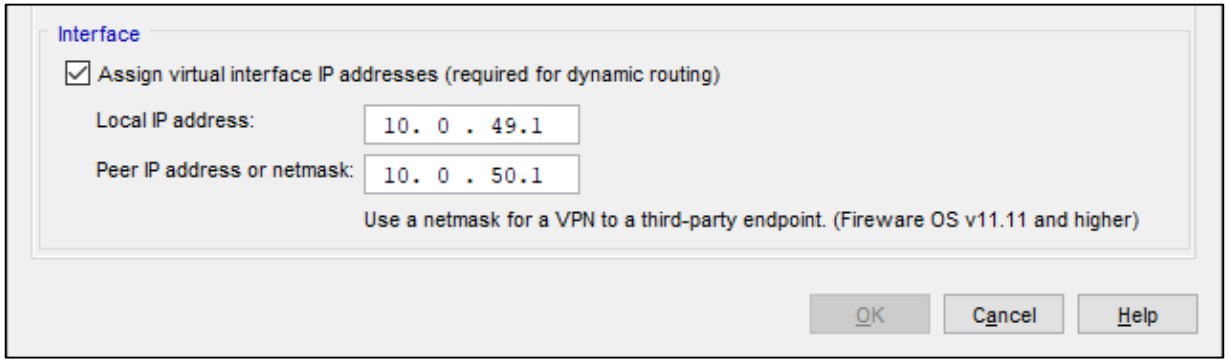
Link Monitor — Internal Interfaces

- The next hop IP address tells the Firebox where to route:
  - Traffic to the link monitor target
  - Traffic that uses an SD-WAN action
- If you do not specify a next hop IP address for an internal interface, you must specify a custom target



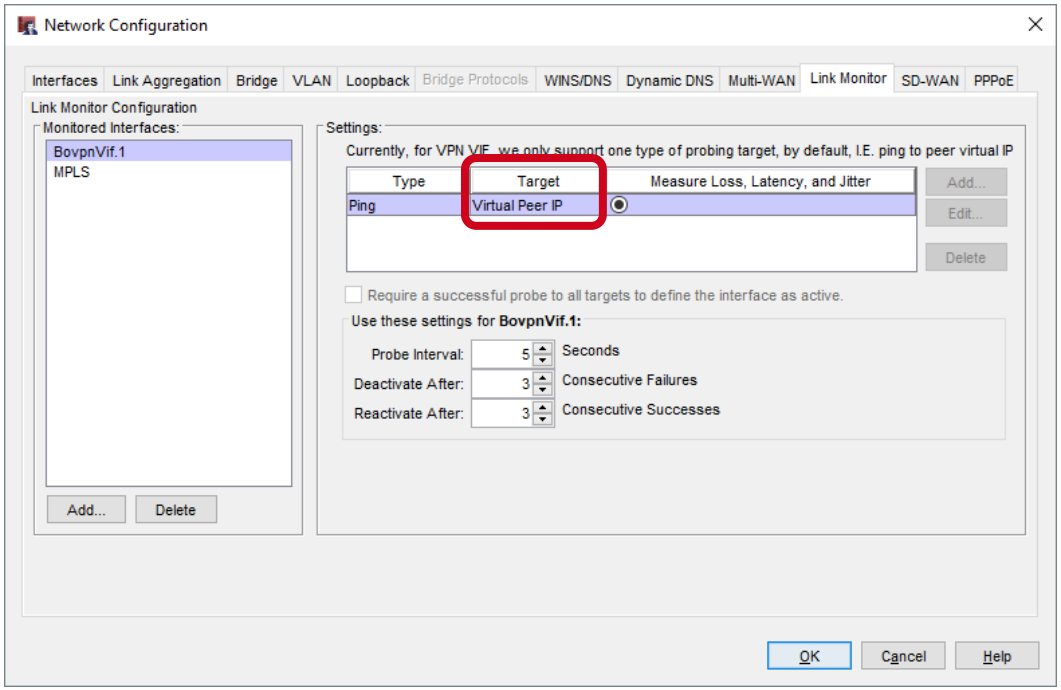
Link Monitor — BOVPN Virtual Interfaces

- To monitor a BOVPN virtual interface, you must first:
  - Configure a virtual peer IP address in the BOVPN virtual interface settings
  - Use an IP address for the peer and not a netmask



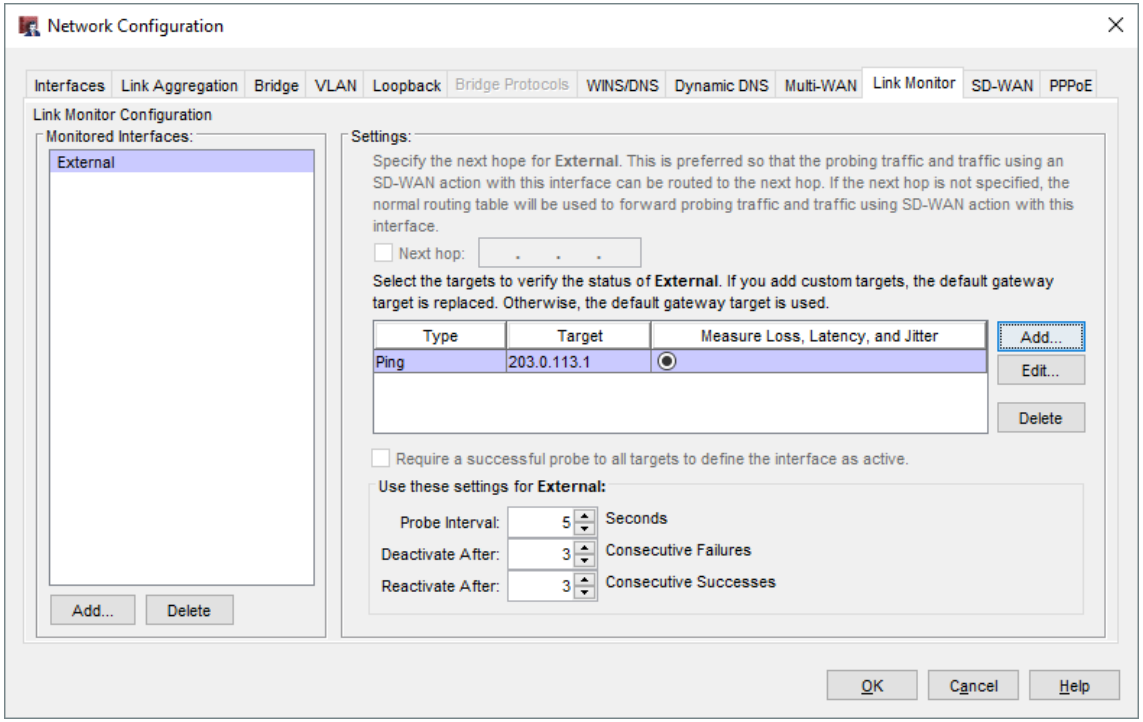
Link Monitor — BOVPN Virtual Interfaces

- In Link Monitor, add the BOVPN virtual interface
  - A target to the virtual peer IP address is automatically configured
  - You cannot change or remove this target, and you cannot specify additional targets



Link Monitor — Single WAN Interfaces

- You can now monitor single WAN interfaces
  - In Policy Manager, this functionality was added in Fireware v12.4
  - In Web UI, this functionality was added in Fireware v12.3



Link Monitor — Interface Changes

- If an interface has Link Monitor targets but is not used by any SD-WAN actions:
  - If you disable the interface, Link Monitor is disabled automatically
  - For an internal interface, if you change the interface type to Bridge, VLAN, or Link Aggregation, Link Monitor is disabled automatically
  - Link Monitor is enabled automatically if you change a non-external interface to an external interface:
    - Interface type changed from internal to external
    - Interface type changed from Bridge, VLAN, or Link Aggregation to external

WebBlocker Warn Action

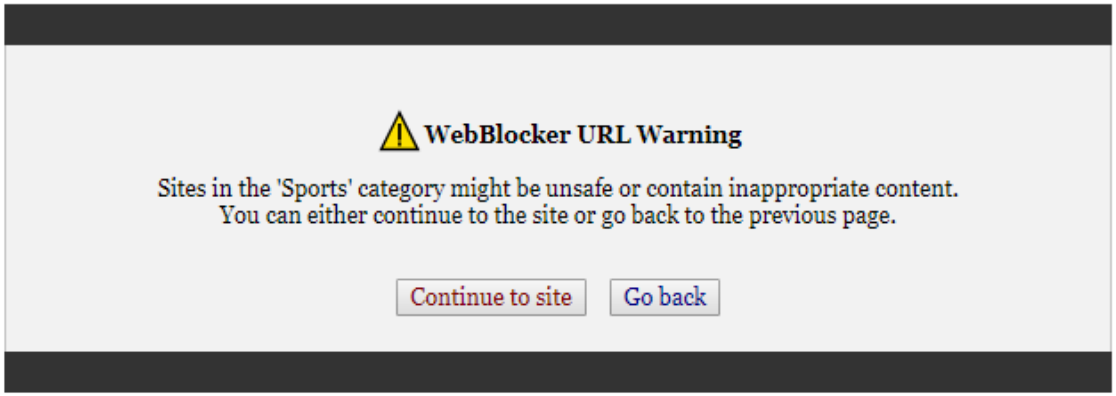
WatchGuard Training

WebBlocker Warn Action

- WebBlocker now includes a new Warn action
- Gives administrators more flexibility to enforce acceptable usage policies
- No longer need to block traffic that is borderline acceptable
- Increases employee awareness of policies in cases where the Deny action is too strict

WebBlocker Warn Action

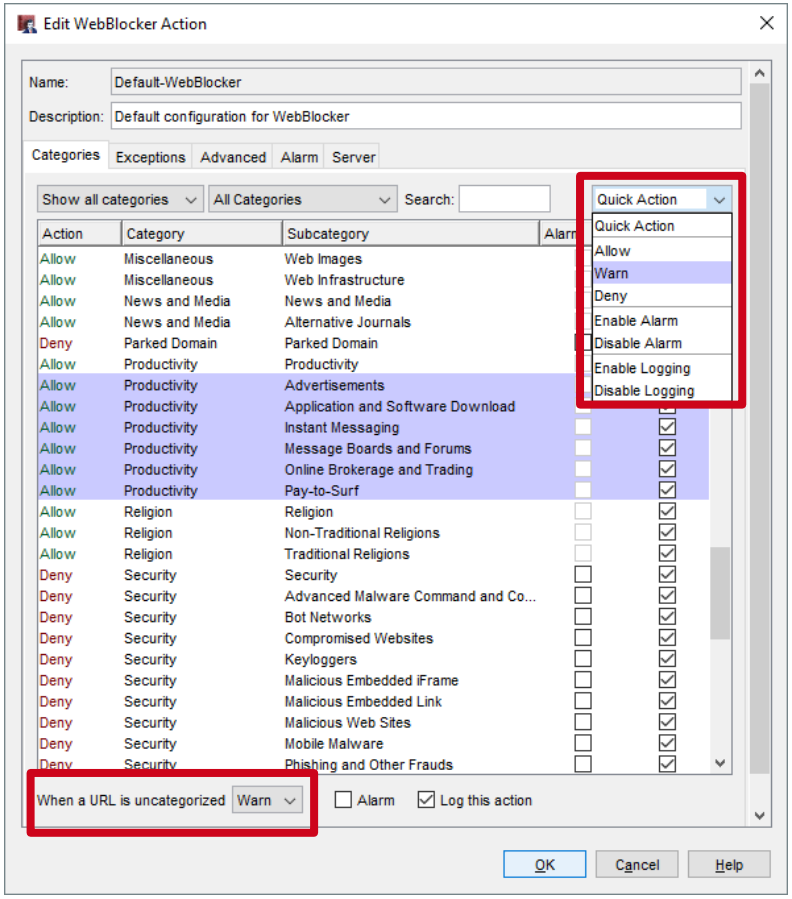
- When users try to get access to a website in a WebBlocker category that has the Warn action assigned, a new warning page appears



- Users can click **Continue to site** to open the website or **Go back** to return to the previous page
- The warning page includes the WebBlocker category and cannot be customized

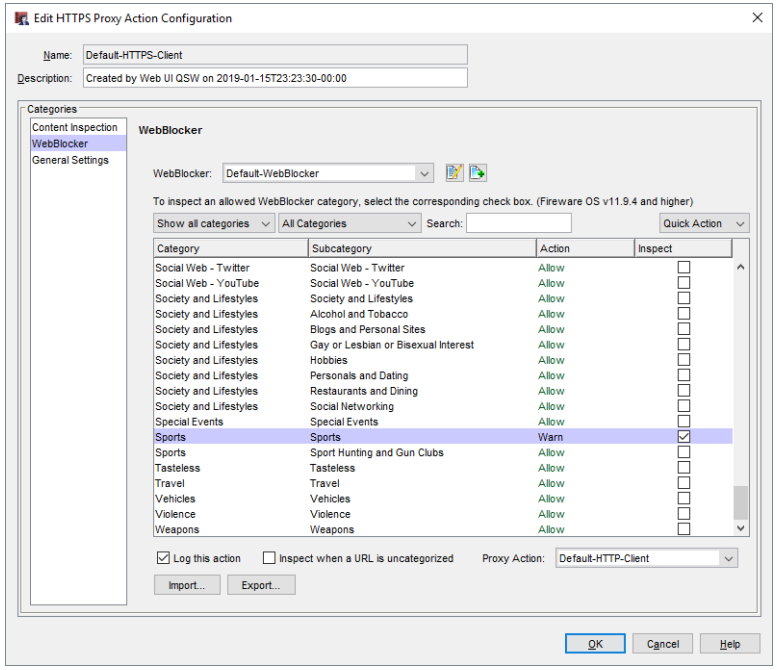
WebBlocker Warn Action

- To assign the Warn action to a WebBlocker category:
  1. Edit a WebBlocker action
  2. In the **Categories** tab, select the category
  3. From the **Quick Action** drop-down list, select **Warn**
- To assign the Warn action to all uncategorized URLs:
  1. From the **When a URL is uncategorized** drop-down list, select **Warn**



WebBlocker Warn Action

- In HTTPS proxy actions, you can perform content inspection on WebBlocker categories with the Warn action
- Select the check box in the **Inspect** column
- When you do not enable content inspection, the HTTPS proxy allows categories with the Warn action and the Warn message does not appear



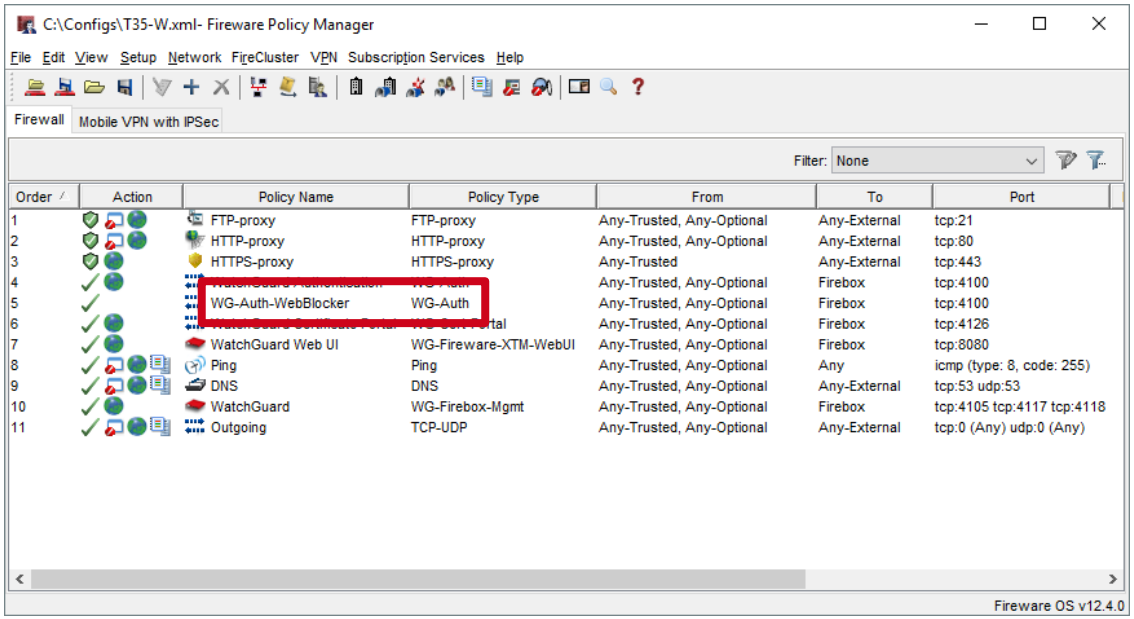
WebBlocker Warn Action

- When users try to get access to a website in a WebBlocker category that has the Warn action assigned, the Firebox writes a log message that includes the text **ProxyWarn**:

2019-03-15 15:42:38 Allow 10.0.1.2 34.232.27.44 http/tcp 50111 80 1-Trusted 0-External **ProxyWarn: HTTP Request categories** (HTTP-proxy-00) Default-HTTP-Client proc_id="http-proxy" rc="602" msg_id="1AFF-0021" proxy_act="Default-HTTP-Client" cats="Sports" op="GET" dstname="www.espn.com" arg="/favicon.ico" geo_dst="USA" Traffic:

WebBlocker Warn Action

- When you assign the Warn action to a WebBlocker category, the **WG-Auth-WebBlocker** policy is added to the configuration automatically
- This is the same policy that is added automatically when you enable the WebBlocker local override feature



WebBlocker Warn Action

- If the Firebox uses a self-signed certificate for authentication, users will receive a certificate warning for the new warning page
- To resolve this, install a trusted certificate on the Firebox, or import the self-signed certificate on each client device

DNSWatch in Bridge Mode

WatchGuard Training

Firebox supports DNSWatch in Bridge Mode

- Can only be configured in Web UI, not CLI or WatchGuard System Manager
- Prerequisite – Firebox system IP address must be able to connect to the DNSWatch Server
  - This system IP address is the source IP address in DNS request packets redirected to the DNSWatch DNS server
- Provides the same types of information as Mixed Routing Mode but is called Global Bridge
- Known Issue - Local domains can’t be resolved even when a local DNS server is specified
  - Workaround – Create DNS Forwarding Rules for local domains

IPv6 Support for BOVPN and BOVPN Virtual Interfaces

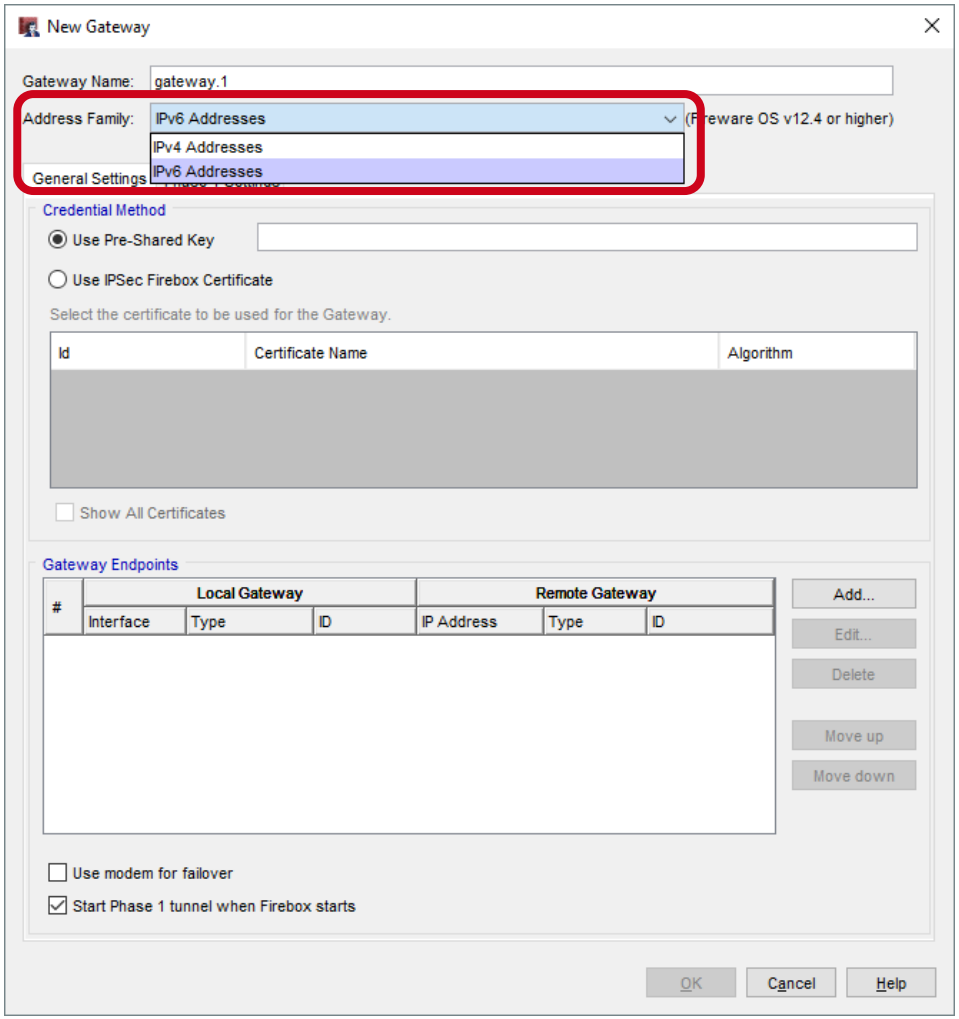
WatchGuard Training

IPv6 Support for BOVPN and BOVPN VIFs

- You can now create VPN tunnels directly between two IPv6 addresses
  - Tunneling over IPv4 is not required
- If an ISP provides only IPv6 addresses, you can now continue to deploy Fireboxes in those environments

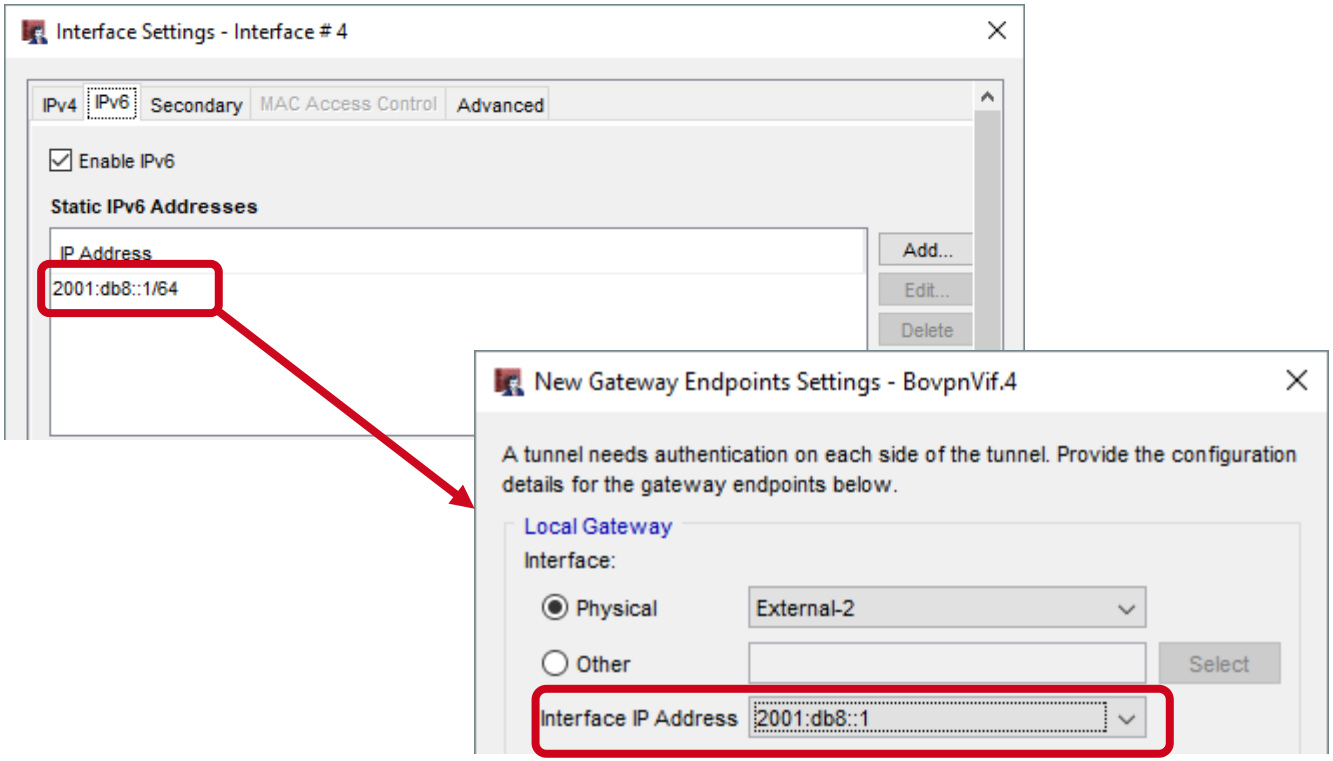
IPv6 Support for BOVPN and BOVPN VIFs

- BOVPN and BOVPN virtual interface configurations now support IPv6
- In the **Address Family** drop-down list, if you select **IPv6 Addresses**, you must specify an IPv6 address for all other BOVPN settings that require an IP address



IPv6 Support for BOVPN and BOVPN VIFs

- The interface you select for the local gateway must have a static IPv6 interface IP address, or the interface must be enabled as a DHCPv6 client



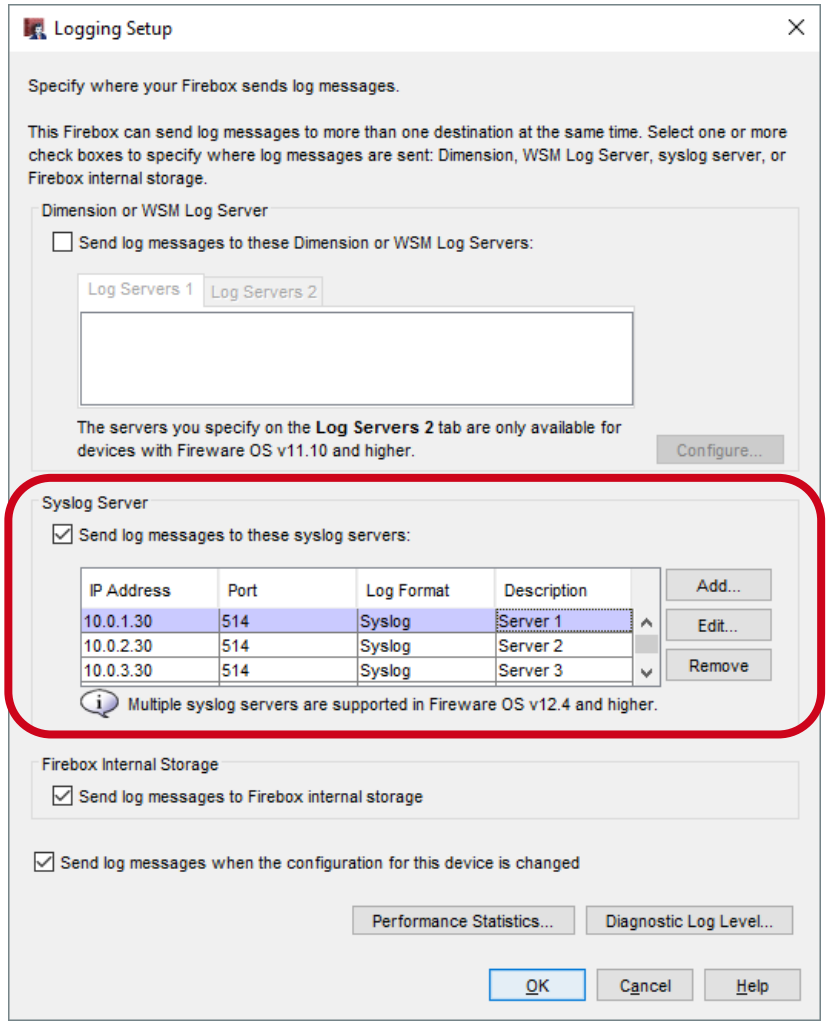
IPv6 Support for BOVPN and BOVPN VIFs

- These BOVPN and BOVPN virtual interface settings are not supported for IPv6 tunnels:
  - Multicast
  - Modem failover
  - NAT and direction
  - Broadcast routing
  - **Attempt to resolve domain** setting

Syslog Servers

Support for Multiple Syslog Servers

- You can now configure a Firebox to send log messages to a maximum of three syslog servers



Proxy Support for TLS 1.3

WatchGuard Training

Proxy Support for TLS 1.3

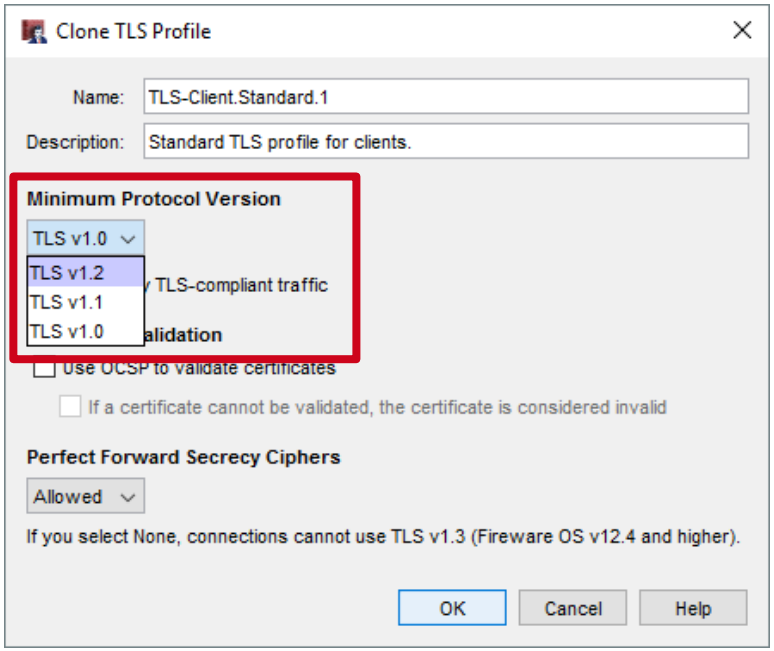
- Fireware now supports TLS 1.3 protocol
- Provides compliance and support for the latest standards
- Allows full inspection of HTTPS traffic
- TLS 1.3 connections are now supported and not downgraded to TLS 1.2

Proxy Support for TLS 1.3

- These proxies now support the TLS 1.3 protocol:
  - HTTPS
  - SMTP
  - IMAP
  - POP3
- Proxies no longer support the SSL v3 protocol. When SSL v3 protocol is specified by the client:
  - Connections are now denied immediately
  - Proxies do not allow negotiation to a different protocol

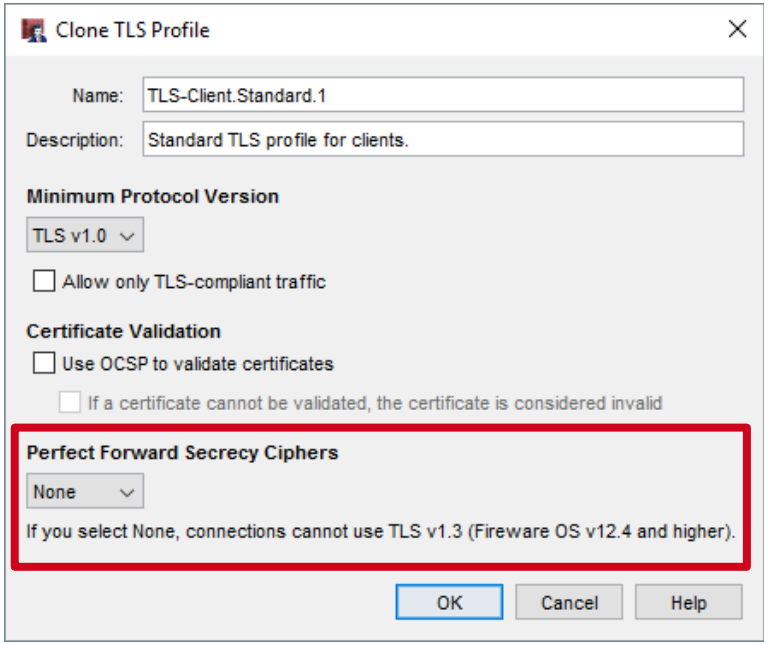
TLS Profile Updates

- Minimum Protocol Version changes
  - TLS v1.2 added
  - SSLv3 removed
- When you upgrade to Fireware v12.4, any existing TLS Profiles with SSLv3 as the Minimum Protocol Version are updated to use TLS v1.0 automatically



TLS Profile Updates

- TLS 1.3 always uses Perfect Forward Secrecy (PFS) Ciphers
- If you select **None** from the **Perfect Forward Secrecy Ciphers** drop-down list:
  - TLS 1.3 is disabled for proxy content inspection negotiation
  - TLS v1.2 and below can be negotiated based on Client/Server support and the **Minimum Protocol Version** in the TLS profile



Enhanced FireCluster Diagnostics

WatchGuard Training

Enhanced FireCluster Diagnostics

- An enhanced FireCluster Diagnostics page shows you more details upfront with better organization

Enhanced FireCluster Diagnostics

- This information now appears on the main FireCluster Diagnostics page:
  - Cluster mode (active/passive or active/active)
  - Cluster ID
- Detailed information is now organized in three tabs:
  - Diagnostics — Heartbeat, interface up/down status, health indexes, and more
  - File Objects — Sync status of objects such as the password, license, and signatures
  - Event History — A list of past cluster events

Enhanced FireCluster Diagnostics

- A status indicator on each tab lets you know whether a cluster member requires attention:
  - If the indicator is green, the cluster functionality is normal
  - If the indicator is red, one or more cluster issues are present
  - To find an issue, look for a red status indicator in each tab section. For example, if the Hardware Health Index has a value considered as unhealthy, the Health section of the Diagnostics tab has a red indicator

Enhanced FireCluster Diagnostics

- Main page and **Diagnostic** tab

FireCluster

30 SECONDS

FireCluster

✓ Synchronized

Cluster enabled for:	1d 1h 13m 40s
Cluster Mode:	active-passive
Cluster ID:	118
Connections:	55
Connections per second:	0

More Details

MEMBER ROLE	SERIAL NUMBER	STATUS	UPTIME	CPU	MEMORY
Master	801002DAA2FEB	Online	1h 18m 6s	0%	29%
Backup	801002DFD1C29	Online	1h 15m 7s	0%	27%

✗ Diagnostic | ✓ File Object | Event History

✗ Backup - 801002DFD1C29

✓ FireCluster State

Heartbeat:	Yes
Management Interface:	Up
Primary Cluster Interface:	Up

✓ Health — More Details

System Health Index:	100
Monitored Ports Health Index:	100
Weighed Avg Index:	100

✗ Monitored Interfaces — More Details

eth0:	Up
eth1:	Up
eth10:	Down
eth11:	Down

Runtime Objects

BOVPN Tunnels:	0
CONNTRACK:	10

Enhanced FireCluster Diagnostics

- **File Object** tab

FireCluster

30 SECONDS

FireCluster

✓ Synchronized

Cluster enabled for:	1d 1h 16m 0s
Cluster Mode:	active-passive
Cluster ID:	118
Connections:	32
Connections per second:	1

More Details

MEMBER ROLE	SERIAL NUMBER	STATUS	UPTIME	CPU	MEMORY
Master	801002DAA2FEB	Online	1h 20m 26s	0%	29%
Backup	801002DFD1C29	Online	1h 17m 27s	0%	27%

✗ Diagnostic | ✓ File Object | Event History

✓ File Objects

Configuration:	Matched
Password:	Matched
Certificate:	Matched
License:	Matched
IPS Signature:	Matched
GAV Signature:	Matched
IAV Signature:	Matched
DLP Signature:	Matched
Botnet:	Matched
Geolocation:	Matched
Hostile Sites and Ports:	Matched

Enhanced FireCluster Diagnostics

- **Event History** tab

FireCluster

30 SECONDS

FireCluster

✓ Synchronized

Cluster enabled for:	1d 1h 16m 20s
Cluster Mode:	active-passive
Cluster ID:	118
Connections:	26
Connections per second:	0

More Details

MEMBER ROLE	SERIAL NUMBER	STATUS	UPTIME	CPU	MEMORY
Master	801002DAA2FEB	Online	1h 20m 46s	0%	29%
Backup	801002DFD1C29	Online	1h 17m 47s	0%	27%

✗ Diagnostic | ✓ File Object | Event History

Cluster Member History

LAST 7 DAYS

Failovers:	0
Faults:	0
Cluster Downtime:	0d 0h 0m

CLUSTER STATUS	PERCENTAGE	TIME
Both Members Up	100.000%	7d 0h 0m
Single Member Up	0.000%	0d 0h 0m
Both Members Down	0.000%	0d 0h 0m

History from 2019-01-18 12:00:00 AM to 2019-01-25 10:33:20 AM

12 PM | Sat 19 | 12 PM | Jan 20 | 12 PM | Mon 21 | 12 PM | Tue 22 | 12 PM | Wed 23 | 12 PM | Thu 24 | 12 PM | Fri 25

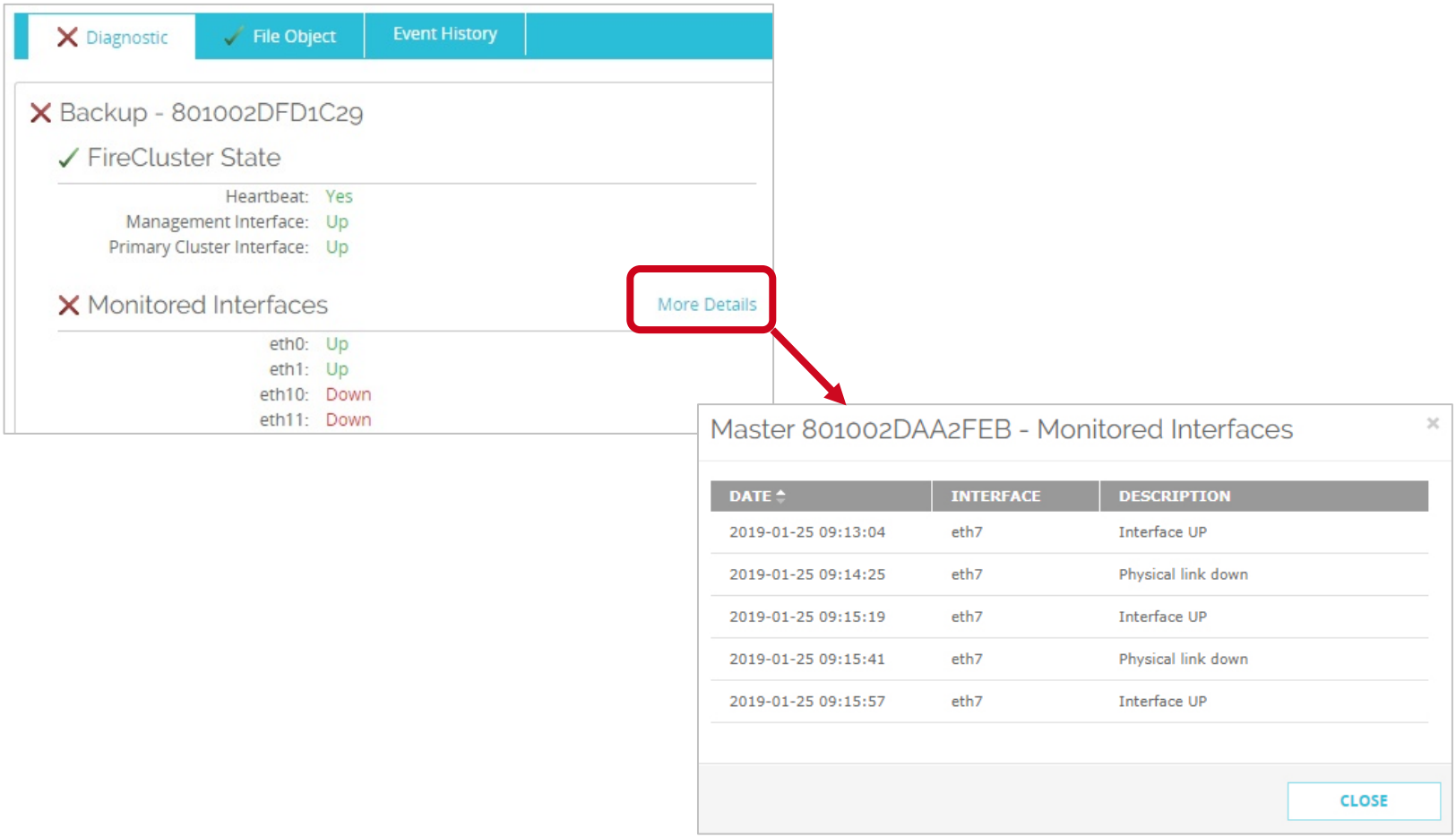
DATE	EVENT	REASON	DURATION

Enhanced FireCluster Diagnostics

- The **More Details** link in each section shows you a list of associated events.
  - For example, if you click the **More Details** link in the **Monitored Interfaces** section, you see a list of interface events (“Interface Up” and “Interface Down”)

Enhanced FireCluster Diagnostics

- **More Details** link

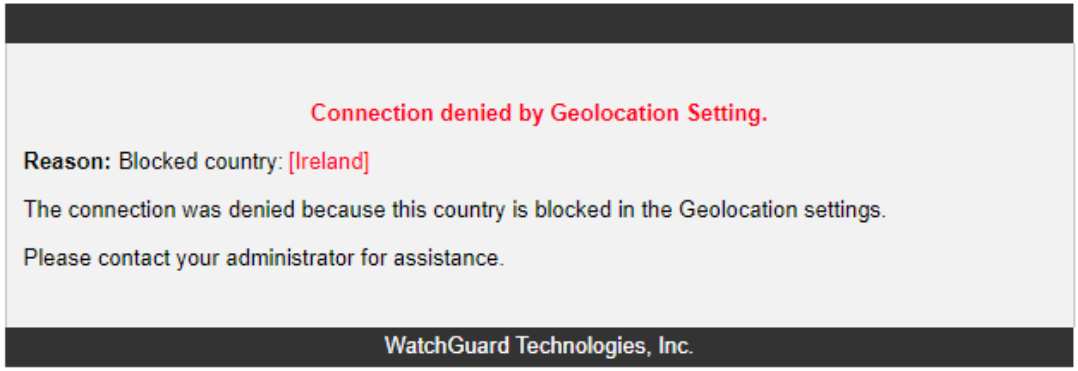


Geolocation Deny Message

WatchGuard Training

Geolocation Deny Message

- A new *Deny* message now appears when Geolocation blocks access to a website
- In previous releases, the connection would timeout



- The message includes the name of the blocked country and cannot be customized

Exception/Blocked Site List Enhancements

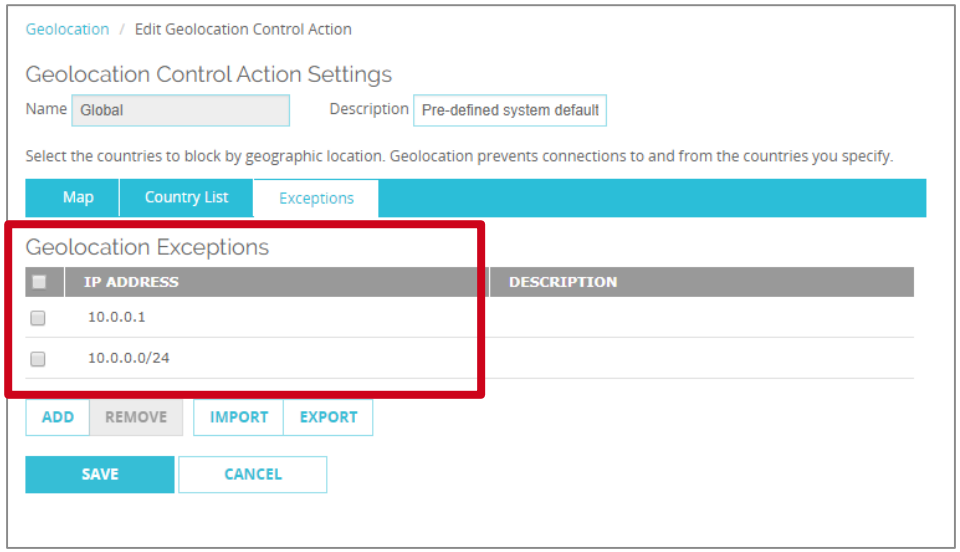
WatchGuard Training

Exceptions/Blocked Site List Enhancements

- In Fireware Web UI and CLI, you can now add IP addresses, Network IP address ranges, and Host IP address ranges that overlap to these lists:
  - Blocked Sites
  - Blocked Sites Exceptions
  - Botnet Site Exceptions
  - Geolocation Exceptions
  - RADIUS SSO Exceptions
- This feature was already supported in Policy Manager
- Domain names that overlap are not allowed

Exceptions/Blocked Site List Enhancements

- For example, you can now add these exceptions to a Geolocation action:
  - Host IPv4: 10.0.0.1
  - Network IPv4: 10.0.0.0/24

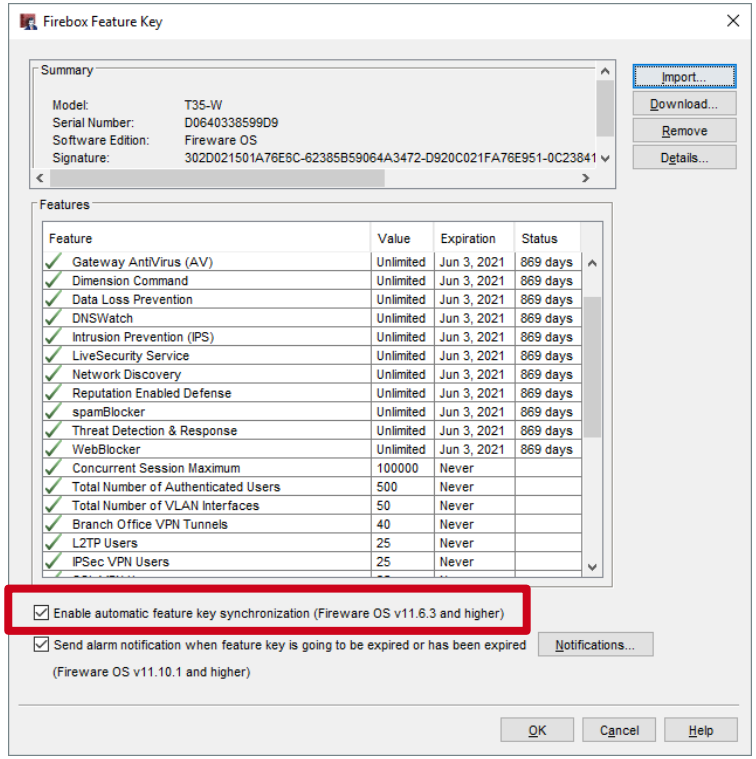


Synchronize Feature Key Enhancements

WatchGuard Training

Synchronize Feature Key Enhancements

- If **Automatic Feature Key Synchronization** is enabled, the Firebox now automatically synchronizes the feature key after you:
  - Restore a Backup Image (with or without Fireware OS)
  - Upgrade Fireware OS
  - Downgrade Fireware OS
- Benefits:
  - Makes sure the feature key includes support for new features after you upgrade
  - Updates the feature key if you restore a backup image that includes an expired license



Proxy Enhancements for DNSWatch

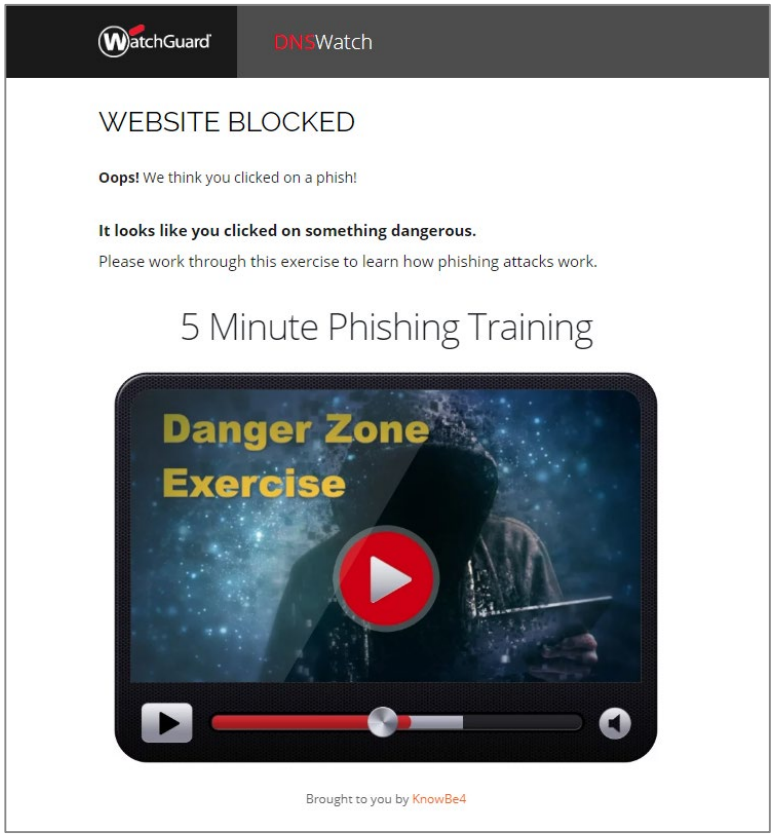
WatchGuard Training

Proxy Enhancements for DNSWatch

- When users try to get access to a domain on the DNSWatch Blackholed domain list:
  - The Firebox now treats the connection to the Blackhole Server educational page as a trusted host connection and allows it
  - The Firebox now writes a log message that includes this text:
    - ProxyDeny: HTTP DNSWatch blackholed domain

Proxy Enhancements for DNSWatch

- When a domain is in both the DNSWatch Blackholed Domain list and a denied WebBlocker category, the Blackhole Server page now appears instead of a WebBlocker Deny message



FQDN Limit Increase

WatchGuard Training

FQDN Limit Increase

- You can now configure up to a total of 2048 Fully Qualified Domain Names (FQDNs) on these devices:
  - Firebox Cloud
  - FireboxV
  - M Series: M200, M270, M300, M370, M400, M440, M470, M500, M570, M670, M4600, M5600
  - T Series: T55, T55-W, T70
- All other devices continue to support up to 1024 FQDNs

MD5 in Gateway AV/IntelligentAV Logs

WatchGuard Training

MD5 in Gateway AV and IntelligentAV Logs

- Gateway AntiVirus and IntelligentAV log messages now include the MD5 hash values of malicious and suspicious files

Gateway AntiVirus:

Nov 28 14:54:25 2018 M400 local1.info http-proxy[2674]: msg_id="1AFF-0028" Deny 1-Internal 0-External-1 tcp 10.0.1.106 100.100.100.121 60912 80 msg="ProxyDrop: HTTP Virus found" proxy_act="HTTP-Client.Standard.1" **md5="dea724a49e3ab3e0b0857150217fd743**" virus="WM.DMV.A" host="100.100.100.121" path="/gav/virus.doc" (HTTP-proxy-00)

IntelligentAV:

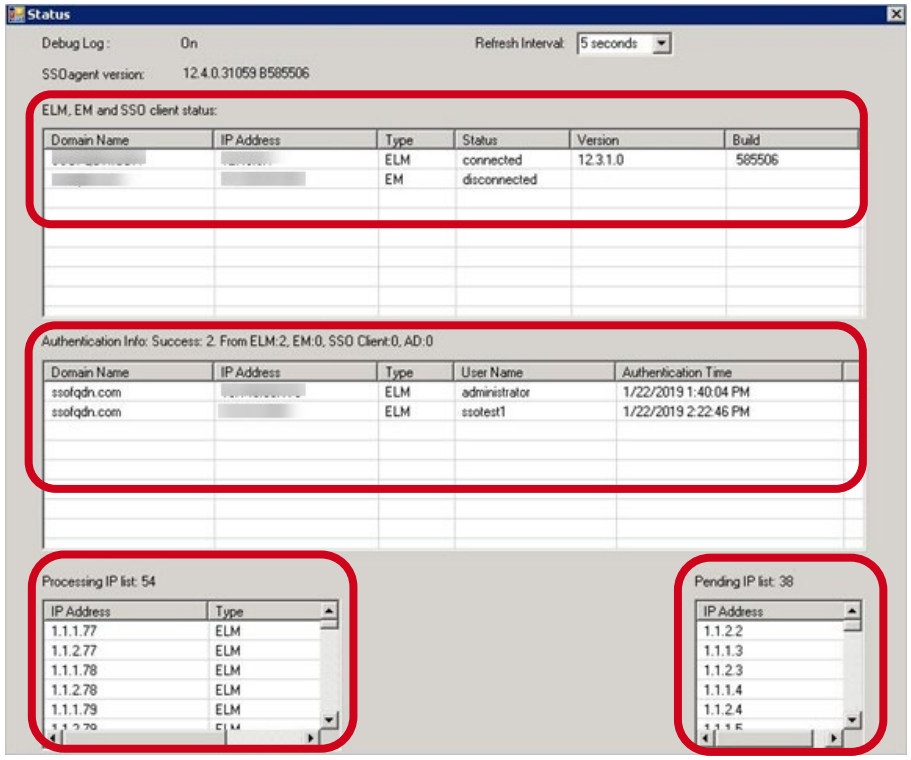
2018-11-28 15:06:09 Deny 10.0.1.106 100.100.100.121 http/tcp 60940 80 1-Internal 0-External-1 ProxyDrop: HTTP Virus found (HTTP-proxy-00) proc_id="http-proxy" rc="594" msg_id="1AFF-0028" proxy_act= "HTTP-Client.Standard.1" host="100.100.100.121" path="/iavtest/virus.doc" virus="malicious" **md5="1c0bd146af6358ad929f3e4b2bd14f8d"**

SSO Agent Debug Tool Enhancements

WatchGuard Training

SSO Agent Debug Tool Enhancements

- Status detail now shows connection information to help you troubleshoot SSO issues



SSO Agent Debug Tool Enhancements

- Connection information:
  - **ELM, EM, and SSO Client Status** – Connection status information
  - **Authentication Info Success** – Information about current users who have successfully authenticated
  - **Pending IP list** – Indicates requests sent to SSO Agent but not processed
  - **Processing IP list** – The information request is in process with ELM, EM, SSO Client or Active Directory
  - **Refresh interval** is configurable for 5 second, 10 second, 30 second, 60 second, 2 minute, and 5 minute intervals

SSO Agent Debug Tool

- Provides easy visibility into the SSO authentication process
- Pending or Processing lists are usually empty because the requests typically process in less time than the refresh rate
- When a client tries to authenticate, the request is sent to the Firebox
- The Firebox forwards the request to the SSO Agent
- The request to the SSO Agent appears in the Pending IP List
  - If an IP address is in the Pending IP List, begin to investigate with the SSO Agent

SSO Agent Debug Tool

- When a request starts processing in ELM, EM, AD, or the SSO Client, the IP address appears in the Processing IP List
  - If an IP address is in the Processing IP List, look at the ELM, EM, AD, SSO Client, or SSO Agent
- When an IP has authenticated, it appears in the Authentication Info Success list until the user logs off

Access Portal Enhancements

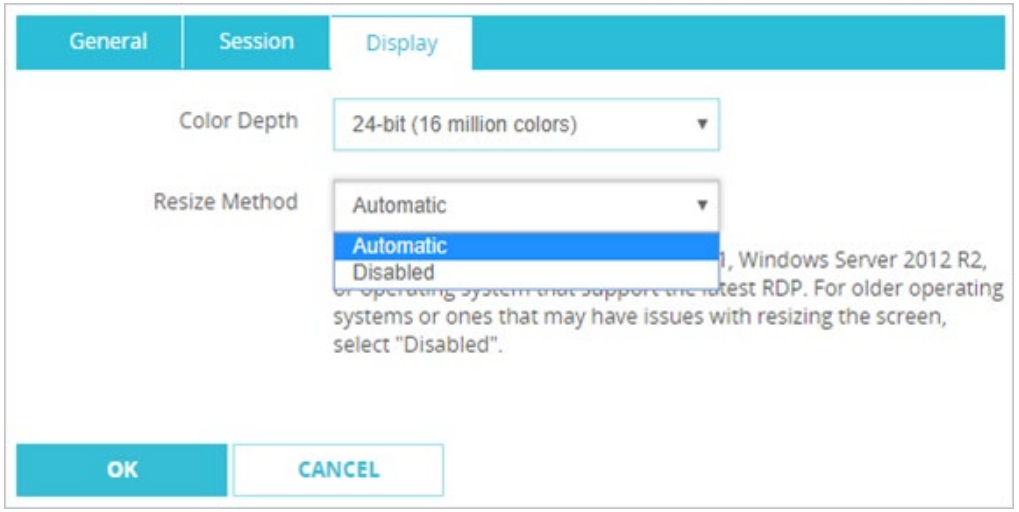
WatchGuard Training

Resize RDP Window Enhancement

- You can now resize the RDP window in your browser without reconnection issues
- The **Automatic** option resizes the RDP window smoothly instead of forcing you to reconnect and, sometimes, re-authenticate
- Added TLS 1.2 support for compliance with environments where TLS 1.0 is prevented
- Support for this feature is dependent on an OS that supports RDP 8.1

Operating Systems Supported

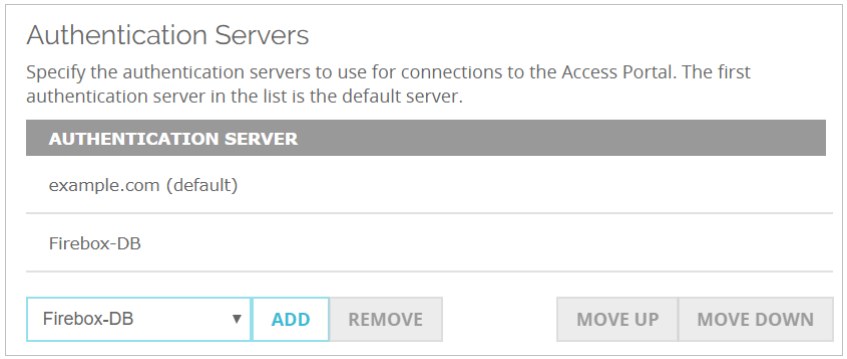
- Windows 7 with RDP 8.1 update
- Windows 8.1 and higher
- Windows Server 2012 R2 and higher



- Versions prior to Windows 8.1 or Windows Server 2012 R2 without RDP 8.1 updates must select **Disabled**

AD Domains Hidden

- Active Directory Domains are now hidden on the Access Portal sign-in page
- The first server in the Authentication Server list is the default server
- User who authenticate with a different server must add <*domain*>\ before their username to authenticate



Default domain

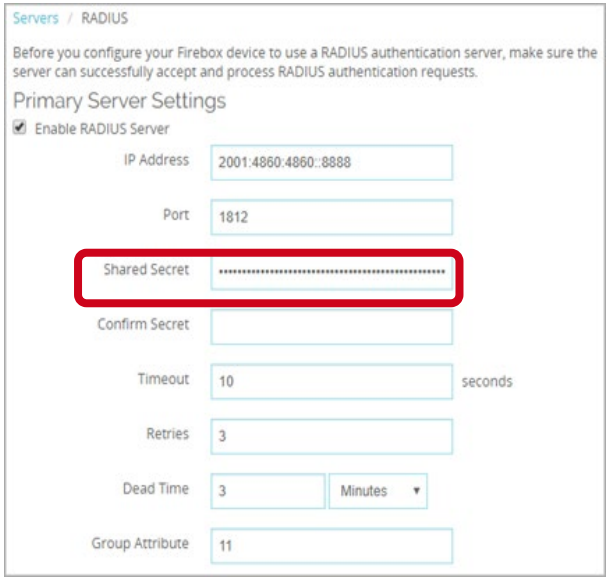
Alternative domain

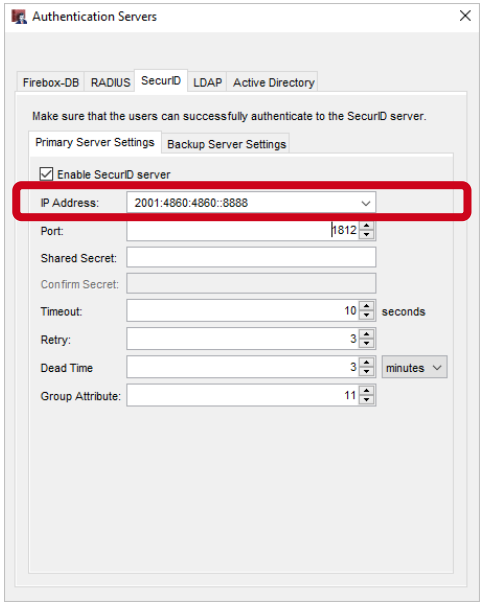
RADIUS and SecurID support for IPv6 and 64-character shared secret

WatchGuard Training

IPv6 Support for RADIUS and SecurID

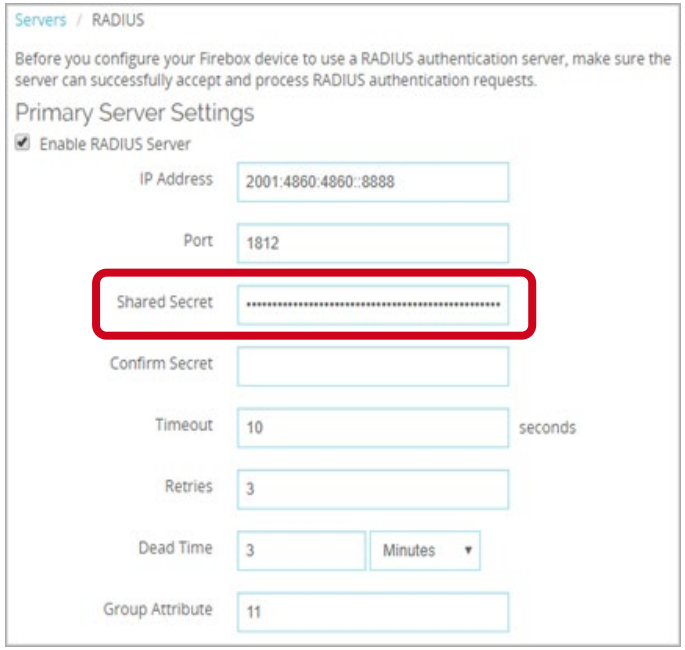
- On the Firebox, you can now configure IPv6 addresses for RADIUS and SecurID servers in both Fireware Web UI and Policy Manager

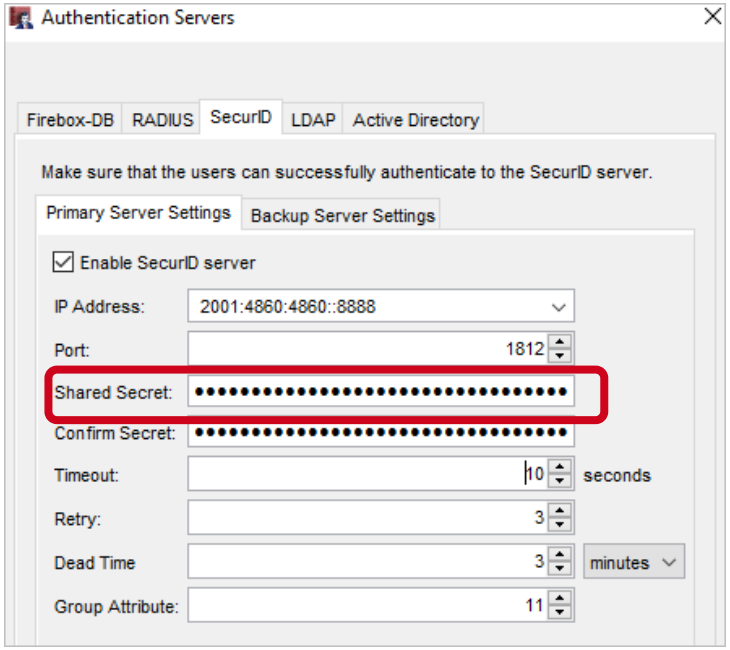




64-Character Shared Secret

- You can now use up to 64 characters in the shared secret for RADIUS and SecurID servers in both Fireware Web UI and Policy Manager



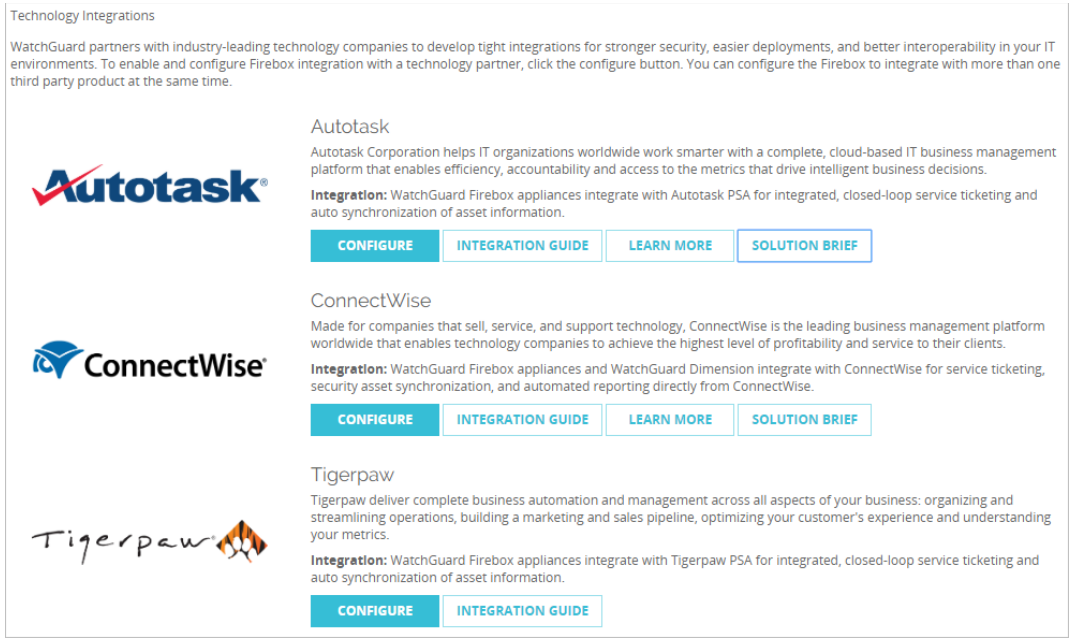


Technology Integrations Page Updates

WatchGuard Training

Updates to Technologies Integrations Page

- New splash page for Technology Integrations
  - **Configure** opens the partner configuration page
  - **Integration Guide** opens the Online Help Integration Guide
  - **Learn More** opens the partner page on WatchGuard.com
  - **Solution Brief** opens a downloadable version of the solution brief

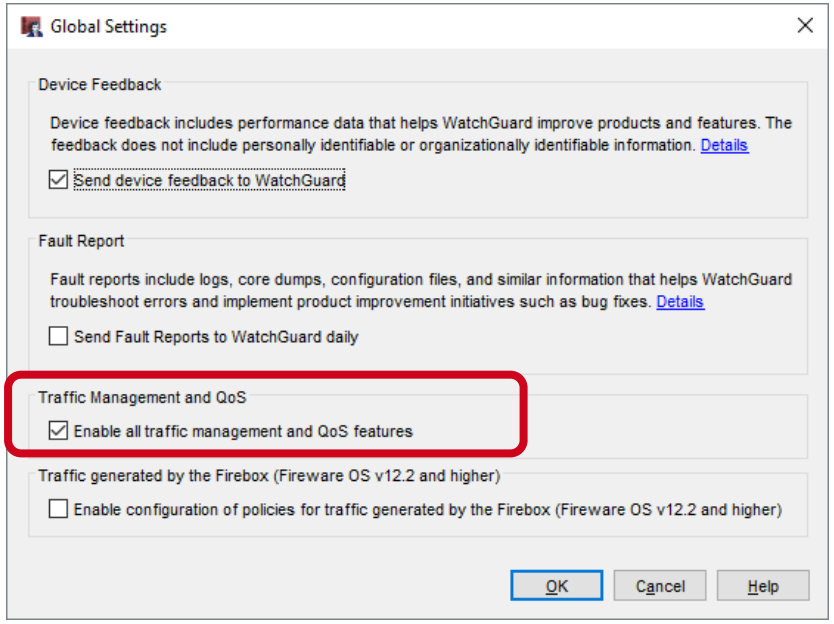


Device Configuration Template Updates

WatchGuard Training

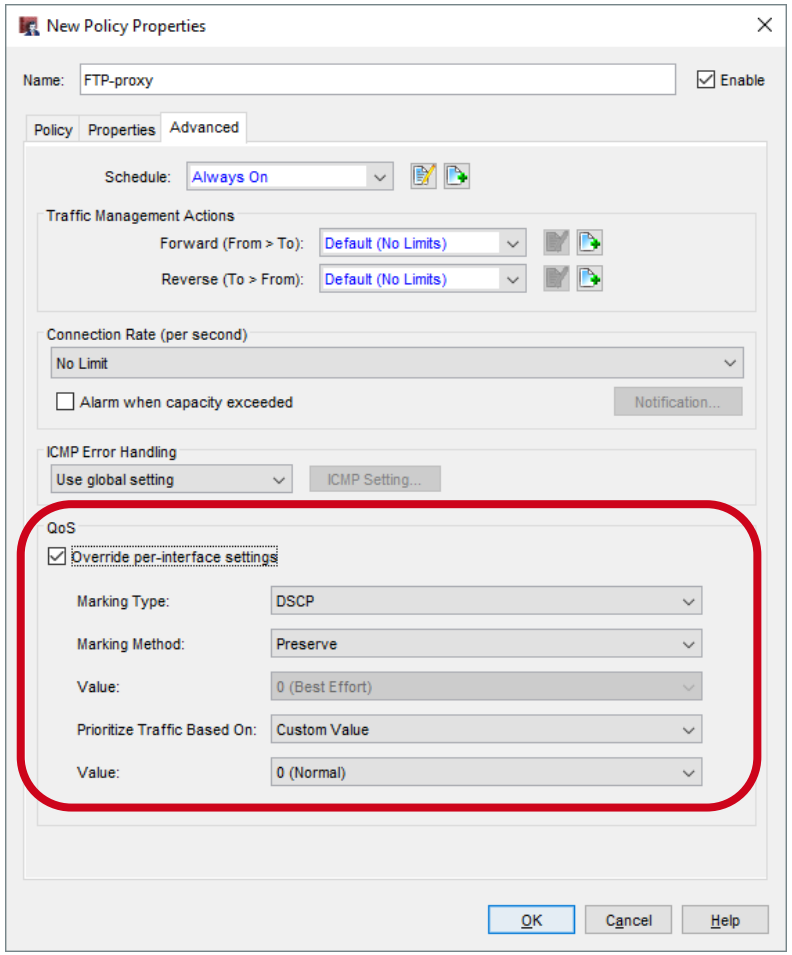
Device Configuration Template – QoS

- In a Device Configuration Template on the Management Server, you can now configure QoS settings
  - Supported in templates for Fireware 12.0 or higher
- Before you can configure QoS in a policy, you must enable all traffic management and QoS features in the Global Settings



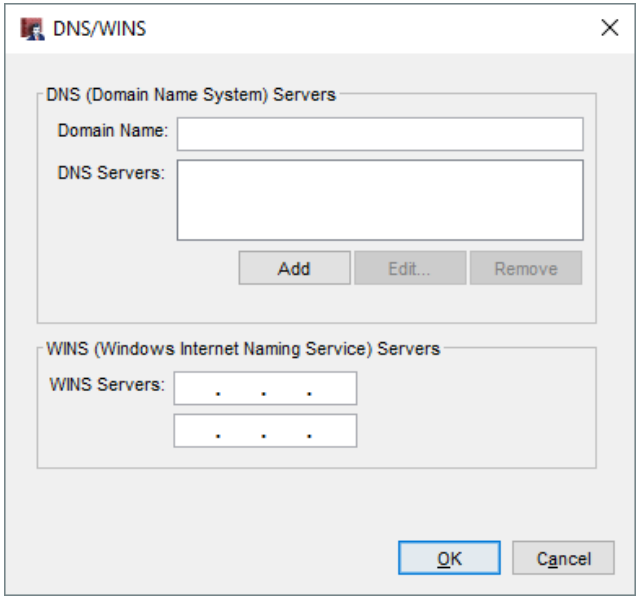
Device Configuration Template – QoS

- When the global setting is enabled, you can configure QoS on the **Advanced** tab in a firewall policy
- QoS settings in a Device Configuration Template are the same as in an individual Firebox configuration



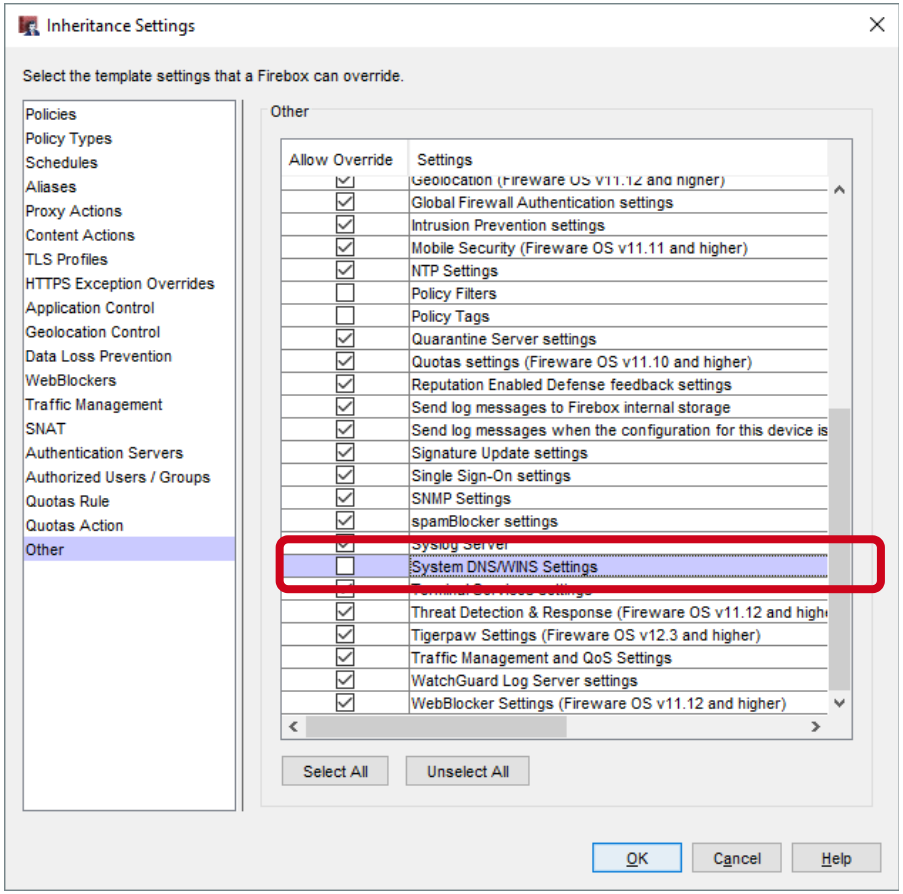
Device Configuration Template – DNS/WINS

- In a Device Configuration Template on the Management Server, you can now configure DNS/WINS settings
  - Supported in templates for Fireware 12.0 or higher
- To specify DNS and WINS settings, edit the Device Configuration Template, and select **Setup > DNS/WINS**



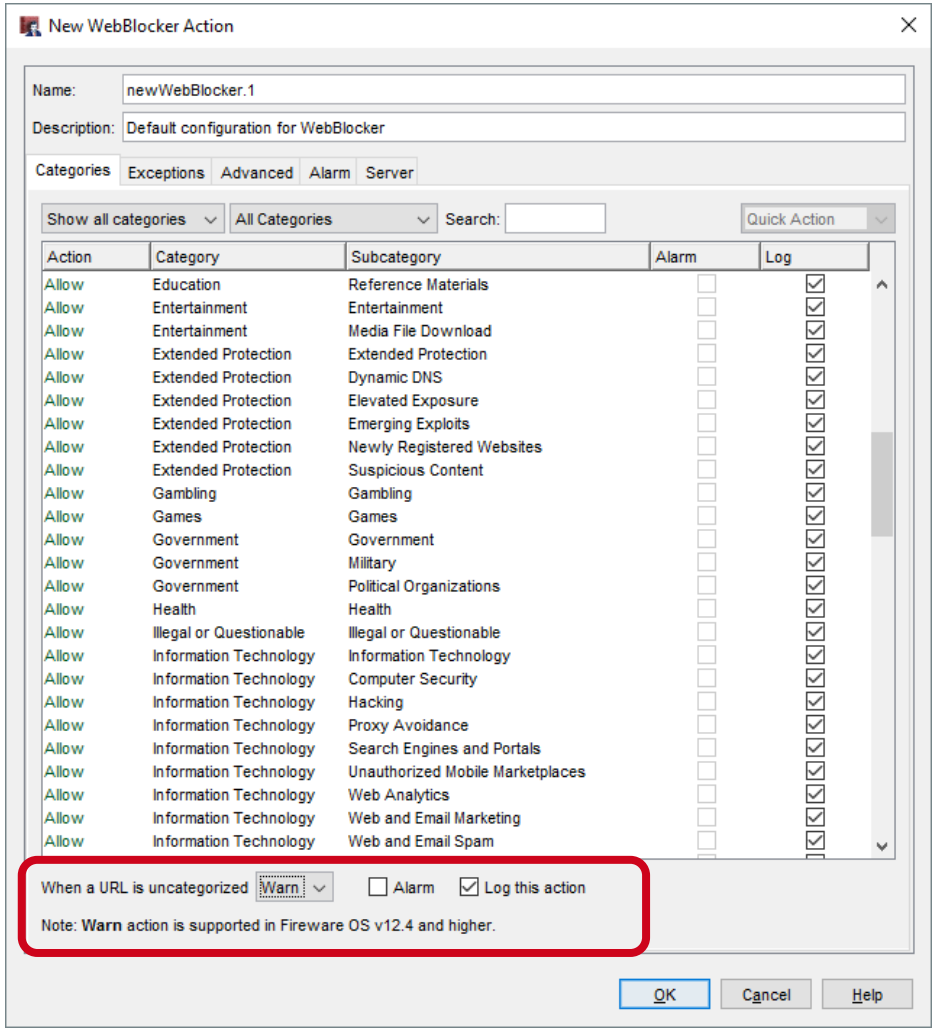
Device Configuration Template – DNS/WINS

- In the Inheritance Settings, the **Other** list now includes **System DNS/WINS Settings**
- To control inheritance of these settings, select or clear the **Allow Override** check box



Device Configuration Template – WebBlocker

- Device Configuration Templates now support the WebBlocker **Warn** action
- Supported for Fireware v12.4 and higher

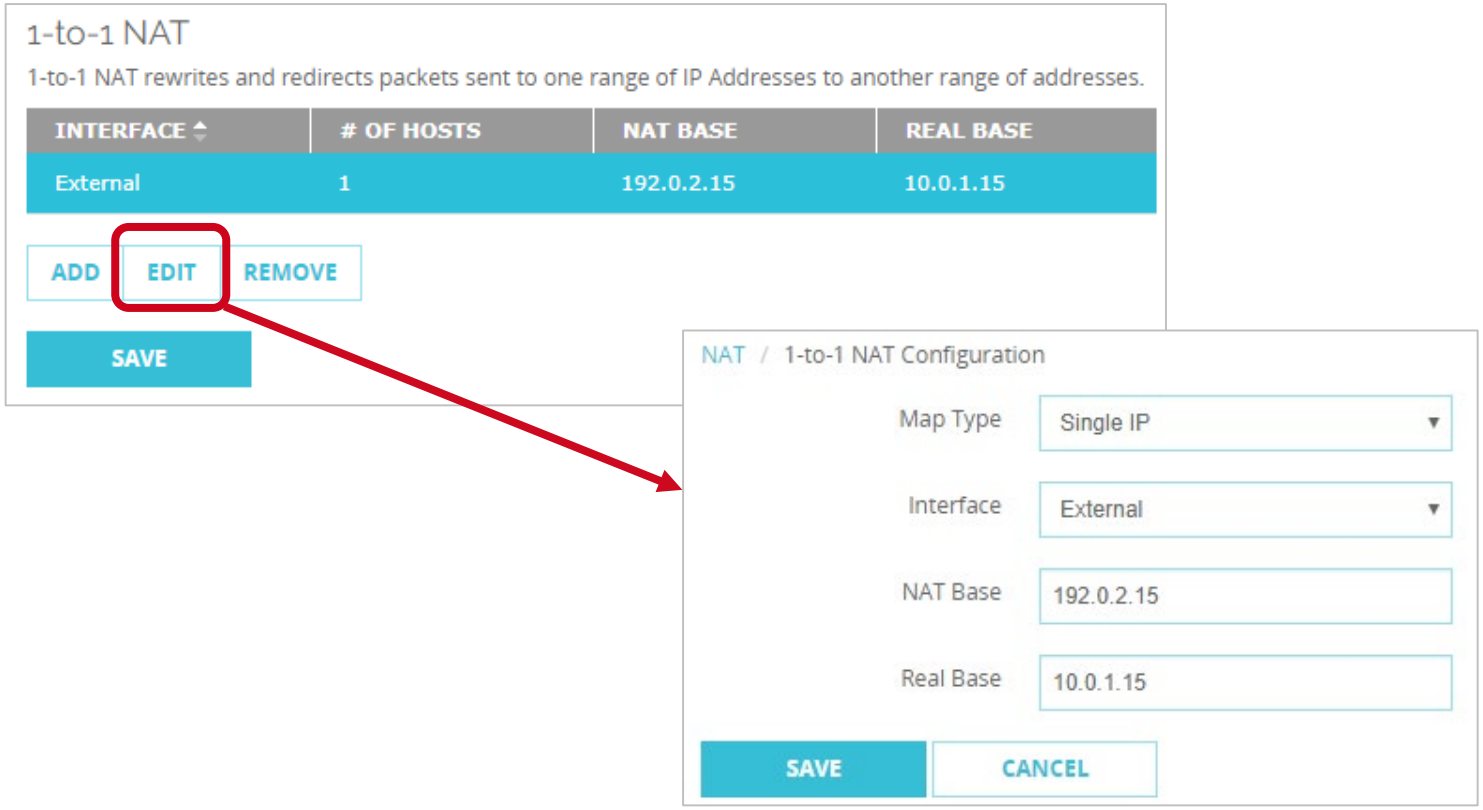


Edit 1-to-1 NAT

WatchGuard Training

Edit 1-to-1 NAT

- You can now edit a 1-to-1 NAT configuration in the Web UI



Thank You!

WatchGuard Training