



What's New in Fireware v12.4

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

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

Add SD-WAN Action

Name:

Description:

SD-WAN Interfaces
Select the interfaces to include in this SD-WAN action. For useful loss, latency, and jitter metrics, we recommend that you specify targets other than the default gateway. To change a target, edit the Link Monitor configuration.

Include	Interface	Targets
<input checked="" type="checkbox"/>	BovpnVif.2	Ping (Virtual Peer IP)
<input checked="" type="checkbox"/>	BovpnVif.1	Ping (Virtual Peer IP)
<input type="checkbox"/>	External-2	Ping (4.4.4.4)
<input type="checkbox"/>	External	Ping (8.8.8.8)

Move Up
Move Down

Metrics Settings
Select measurements and specify values that determine when failover occurs to another SD-WAN interface. Failover occurs if the value for any selected measurement is exceeded.

Loss Rate %

Latency ms

Jitter ms

Fail over if values for all selected measurements are exceeded.

Failback for Active Connections
Select how the Firebox handles failback for active and new connections.

Immediate failback: Active and new connections use the failback (original) interface

Immediate failback: Active and new connections use the failback (original) interface

Gradual failback: Active connections use the failover interface; new connections use the failback interface

No failback: Active and new connections use the failover interface.

Cancel Help

SD-WAN — BOVPN Virtual Interface Failover

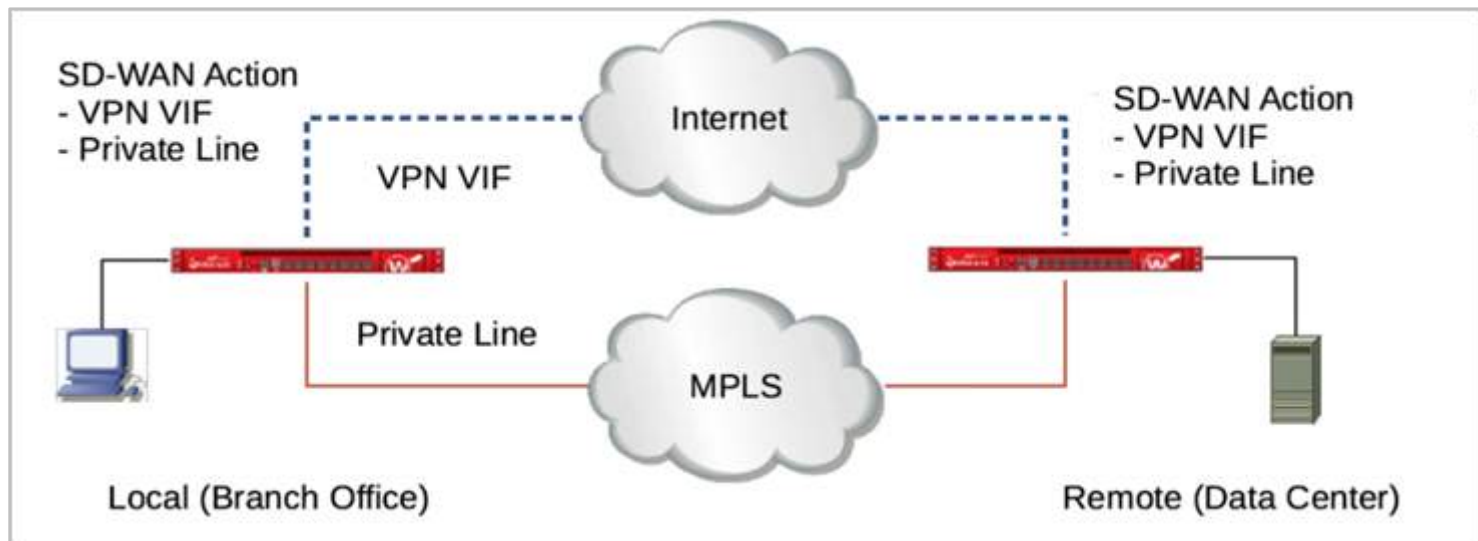
- You can select to fail over based on loss, latency, or jitter measurements
 - If you do not select any measurements, failover occurs if the primary connection fails
- Requirements for BOVPN virtual interface failover:
 - In the BOVPN virtual interface settings for both interfaces, you must configure 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

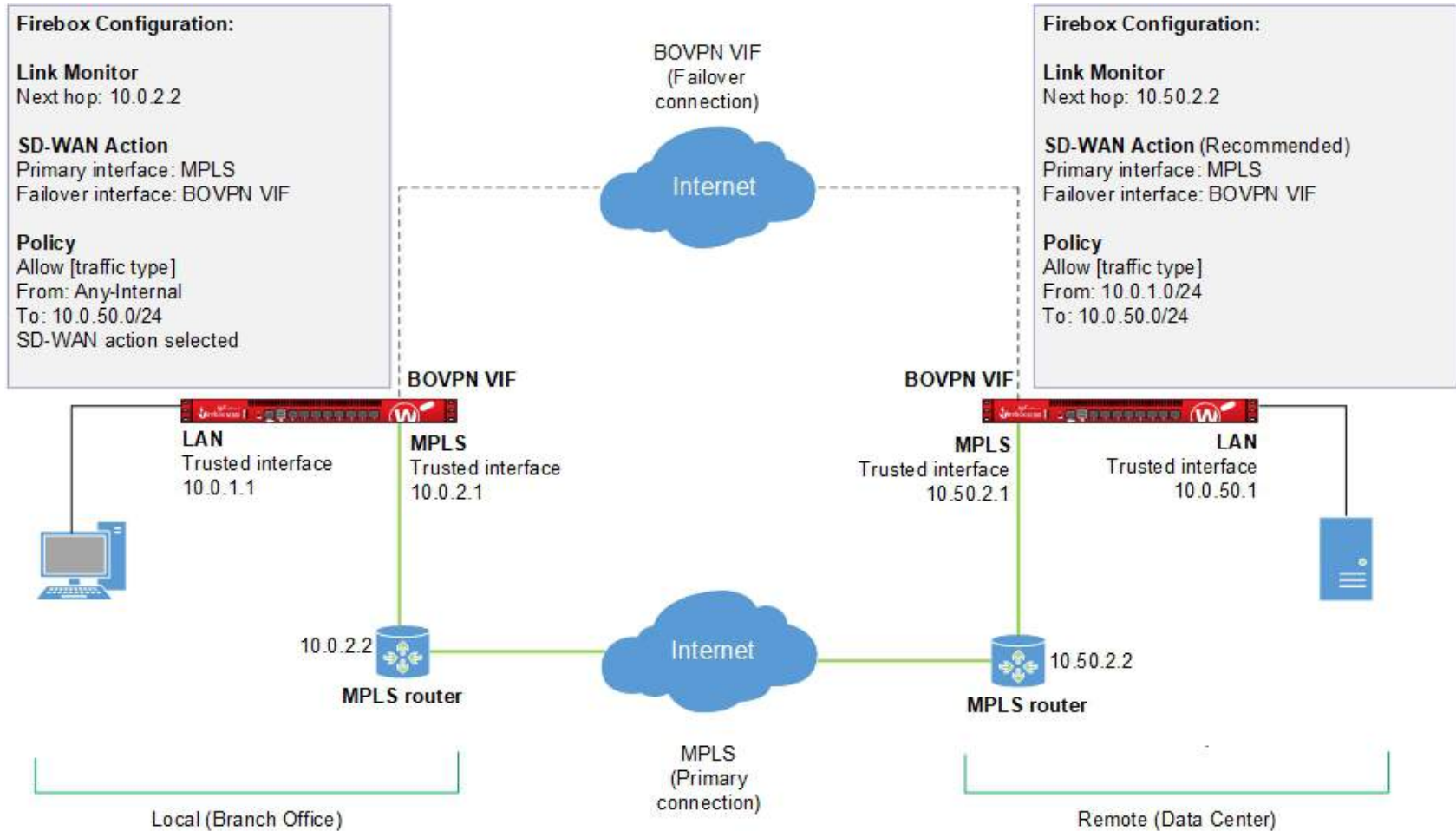
- You can now include internal interfaces in an SD-WAN configuration
 - This includes Trusted, Optional, and Custom interfaces
- If you have a private network connection such as a private line, leased line, or MPLS configured on an internal interface, you can configure SD-WAN failover to another connection

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

Network Configuration

Link Monitor Configuration

Monitored Interfaces:

Settings:

Specify the next hop for {0}. This is preferred so that the probing traffic and traffic using an SD-WAN action with this interface can be routed to the next hop. If the next hop is not specified, the normal routing table will be used to forward probing traffic and traffic using SD-WAN action with this interface.

Next hop: . . .

Select the targets to verify the status of {0}. If you add custom targets, the default gateway target is replaced. Otherwise, the default gateway target is used.

Type	Target	Measure Loss, Latency, a...	Add...
			Edit...

Require a successful probe to all targets to

Use these settings for {0}:

Probe Interval: 5 Seconds

Deactivate After: 3 Consecutive

Reactivate After: 3 Consecutive

Add...

Select an Interface to Monitor

Name	Type	Zone
	All	All
External-2	Physical	External
BovpnVif.1	BOVPN Virtual Interface	
Trusted	Physical	Trusted
MPLS	Physical	Trusted
External-1	Physical	External

OK Cancel

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

Network Configuration

Interfaces Link Aggregation Bridge VLAN Loopback Bridge Protocols WINS/DNS Dynamic DNS Multi-WAN Link Monitor SD-WAN PPPoE

Link Monitor Configuration

Monitored Interfaces:

- BovpnVif.1
- MPLS

Settings:

Specify the next hope for **MPLS**. This is preferred so that the probing traffic and traffic using an SD-WAN action with this interface can be routed to the next hop. If the next hop is not specified, the normal routing table will be used to forward probing traffic and traffic using SD-WAN action with this interface.

Next hop: 10.0.2.2

Select the targets to verify the status of **MPLS**. If you add custom targets, the default gateway target is replaced. Otherwise, the default gateway target is used.

Type	Target	Measure Loss, Latency, and Jitter
Ping	Next Hop	<input checked="" type="radio"/>

Require a successful probe to all targets to define the interface as active.

Use these settings for **MPLS**:

Probe Interval: 5 Seconds

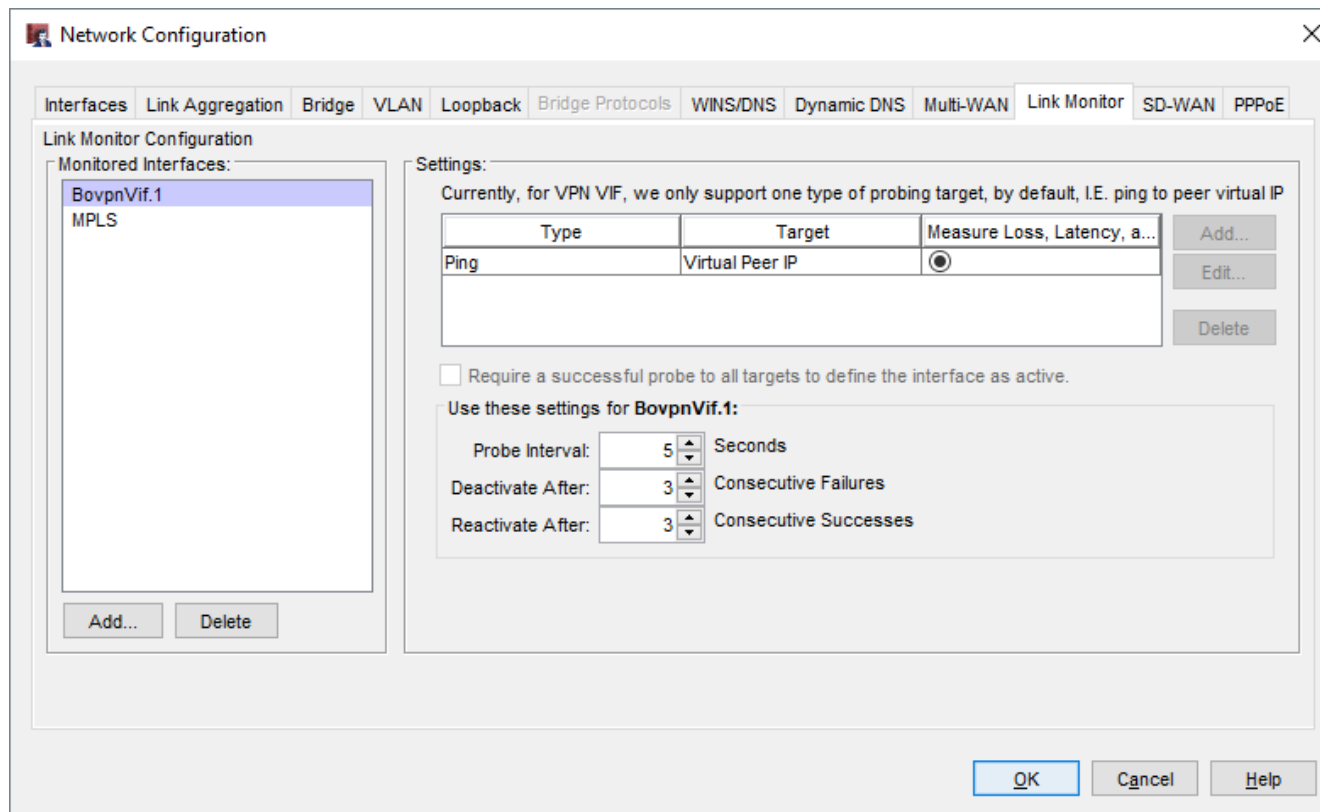
Deactivate After: 3 Consecutive Failures

Reactivate After: 3 Consecutive Successes

OK Cancel Help

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

Add SD-WAN Action
✕

Name:

Description:

SD-WAN Interfaces

Select the interfaces to include in this SD-WAN action. For useful loss, latency, and jitter metrics, we recommend that you specify targets other than the default gateway. To change a target, edit the Link Monitor configuration.

Include	Interface	Targets
<input checked="" type="checkbox"/>	BovpnVif.1	Ping (Virtual Peer IP)
<input checked="" type="checkbox"/>	MPLS	Ping (Next Hop)
<input type="checkbox"/>	External	Ping (4.2.2.1) Ping (8.8.8.8)

Metrics Settings

Select measurements and specify values that determine when failover occurs to another SD-WAN interface. Failover occurs if the value for any selected measurement is exceeded.

Loss Rate %

Latency ms

Jitter ms

Fail over if values for all selected measurements are exceeded.

Failback for Active Connections

Select how the Firebox handles failback for active and new connections.

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

New Policy Properties

Name: SIP-ALG Enable

Policy Properties Advanced

SIP-ALG connections are...

Allowed Send TCP RST

From

10.0.1.0/24

Add... Edit... Remove

To

10.0.50.0/24

Add... Edit... Remove

Route outbound traffic using SD-WAN Based Routing (Fireware OS v12.3 or higher)

SD-WAN Action Datacenter

Enable Application Control: Global

Enable Geolocation: Global

Enable IPS for this policy

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

OK Cancel Help

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



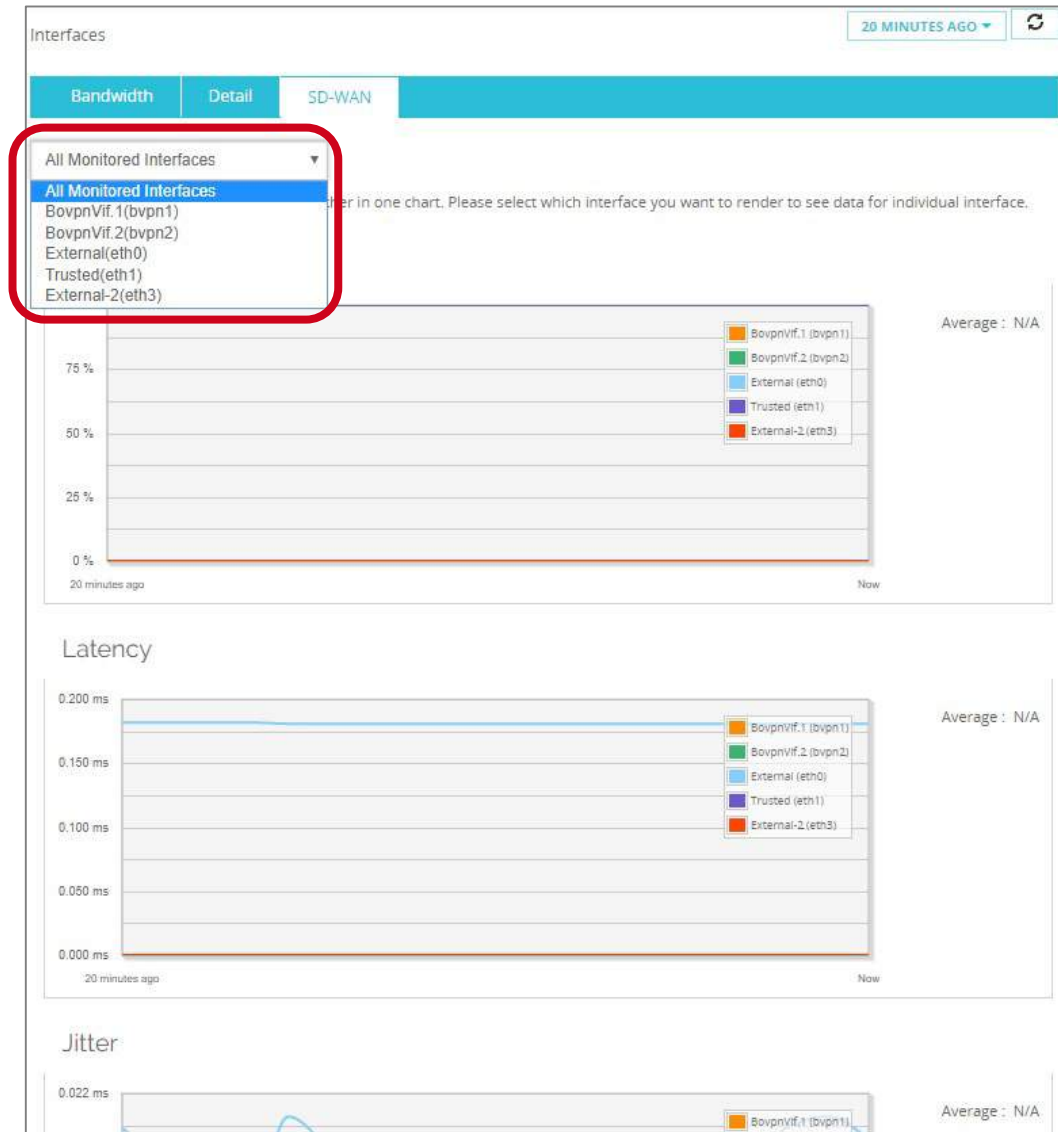
SD-WAN Reporting Enhancements

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

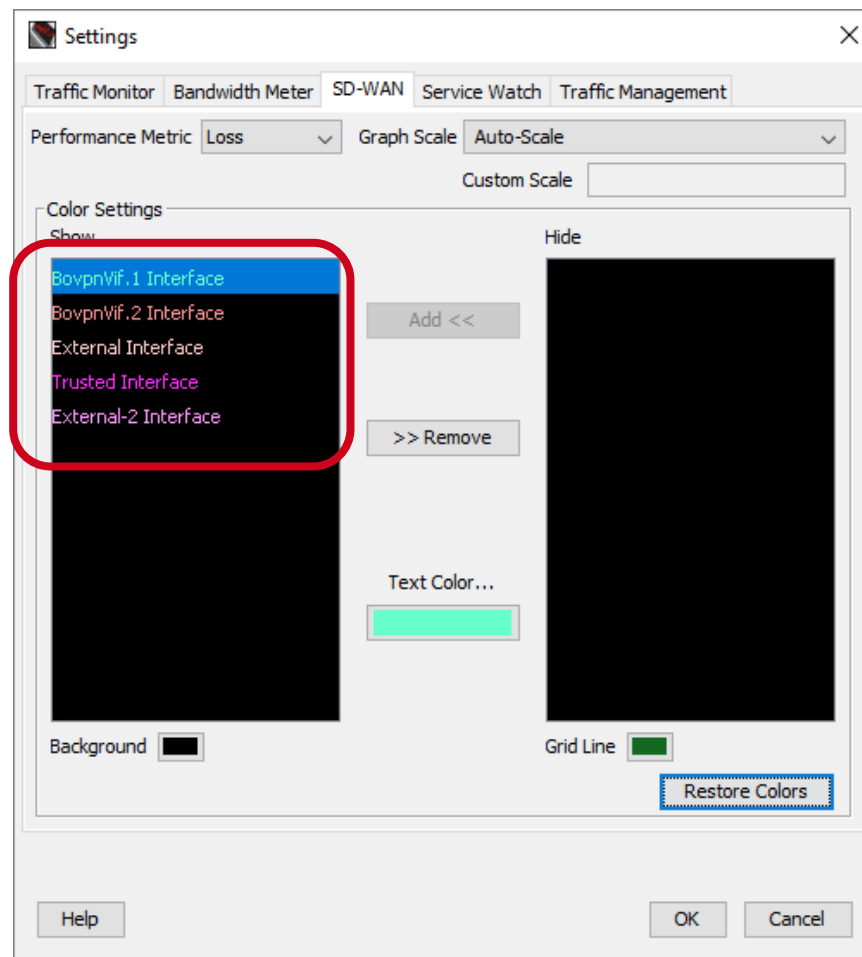
SD-WAN Reporting Enhancements

- SD-WAN reporting page in the Web UI



SD-WAN Reporting Enhancements

- SD-WAN reporting page in Firebox System Manager





Link Monitor Enhancements

Link Monitor — Enhancements

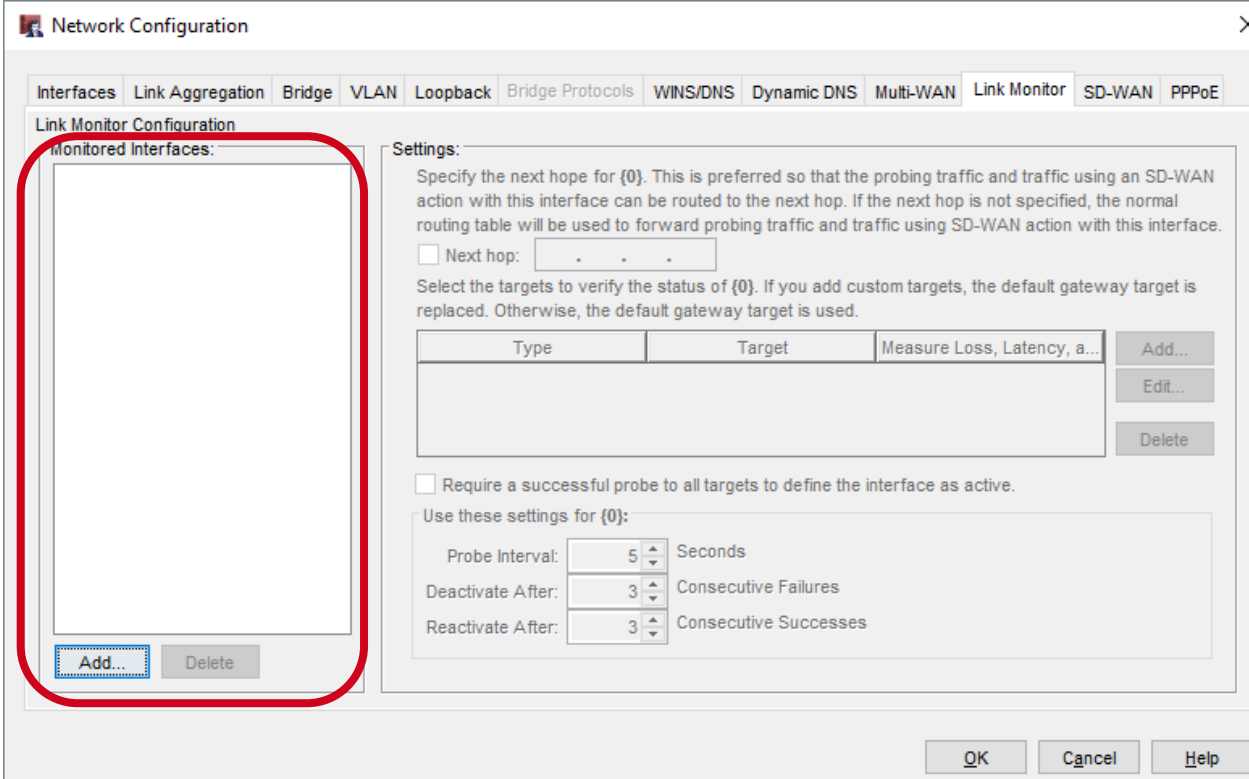
- Link Monitor has these enhancements:
 - You can now add Internal interfaces (Trusted, Optional, and Custom) and BOVPN virtual interfaces to Link Monitor
 - For example, you can monitor an internal interface that is used for a private network link such as an MPLS connection, private line, or leased 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



Network Configuration

Interfaces | Link Aggregation | Bridge | VLAN | Loopback | Bridge Protocols | WINS/DNS | Dynamic DNS | Multi-WAN | **Link Monitor** | SD-WAN | PPPoE

Link Monitor Configuration

Monitored Interfaces:

Settings:

Specify the next hope for {0}. This is preferred so that the probing traffic and traffic using an SD-WAN action with this interface can be routed to the next hop. If the next hop is not specified, the normal routing table will be used to forward probing traffic and traffic using SD-WAN action with this interface.

Next hop: . . .

Select the targets to verify the status of {0}. If you add custom targets, the default gateway target is replaced. Otherwise, the default gateway target is used.

Type	Target	Measure Loss, Latency, a...	Add...
			Edit...
			Delete

Require a successful probe to all targets to define the interface as active.

Use these settings for {0}:

Probe Interval: 5 Seconds

Deactivate After: 3 Consecutive Failures

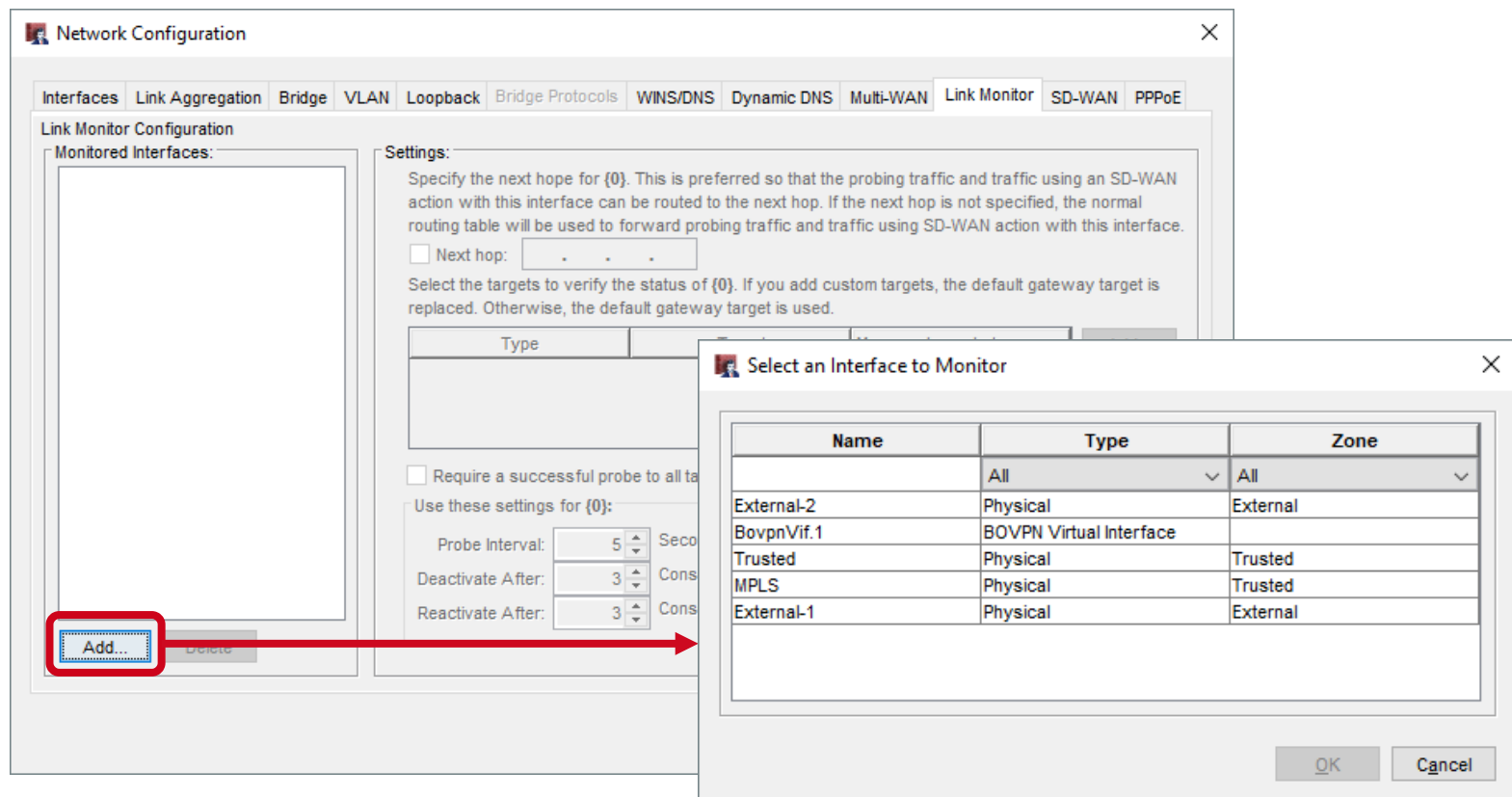
Reactivate After: 3 Consecutive Successes

Add... Delete

OK Cancel Help

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



Network Configuration

Interfaces | Link Aggregation | Bridge | VLAN | Loopback | Bridge Protocols | WINS/DNS | Dynamic DNS | Multi-WAN | **Link Monitor** | SD-WAN | PPPoE

Link Monitor Configuration

Monitored Interfaces:

Settings:

Specify the next hope for {0}. This is preferred so that the probing traffic and traffic using an SD-WAN action with this interface can be routed to the next hop. If the next hop is not specified, the normal routing table will be used to forward probing traffic and traffic using SD-WAN action with this interface.

Next hop: . . .

Select the targets to verify the status of {0}. If you add custom targets, the default gateway target is replaced. Otherwise, the default gateway target is used.

Require a successful probe to all targets

Use these settings for {0}:

Probe Interval: 5 Sec

Deactivate After: 3 Cons

Reactivate After: 3 Cons

Add... Delete

Select an Interface to Monitor

Name	Type	Zone
External-2	Physical	External
BovpnVif.1	BOVPN Virtual Interface	
Trusted	Physical	Trusted
MPLS	Physical	Trusted
External-1	Physical	External

OK Cancel

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

Network Configuration

Interfaces | Link Aggregation | Bridge | VLAN | Loopback | Bridge Protocols | WINS/DNS | Dynamic DNS | Multi-WAN | **Link Monitor** | SD-WAN | PPPoE

Link Monitor Configuration

Monitored Interfaces:

- External-1

Settings:

Specify the next hop for **External-1**. This is preferred so that the probing traffic and traffic using an SD-WAN action with this interface can be routed to the next hop. If the next hop is not specified, the normal routing table will be used to forward probing traffic and traffic using SD-WAN action with this interface.

Next hop: . . .

Select the targets to verify the status of **External-1**. If you add custom targets, the default gateway target is replaced. Otherwise, the default gateway target is used.

Type	Target	Measure Loss, Latency, ...	Add...
Ping	4.2.2.1	<input checked="" type="radio"/>	Edit...
Ping	8.8.8.8	<input type="radio"/>	Delete

Require a successful probe to all targets to define the interface as active.

Use these settings for **External-1**:

Probe Interval: 5 Seconds

Deactivate After: 3 Consecutive Failures

Reactivate After: 3 Consecutive Successes

Buttons: Add... (highlighted), Delete (highlighted with red box), OK, Cancel, Help

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

Network Configuration

Interfaces | Link Aggregation | Bridge | VLAN | Loopback | Bridge Protocols | WINS/DNS | Dynamic DNS | Multi-WAN | **Link Monitor** | SD-WAN | PPPoE

Link Monitor Configuration

Monitored Interfaces:

- BovpnVif.1
- MPLS**

Settings:

Specify the next hope for **MPLS**. This is preferred so that the probing traffic and traffic using an SD-WAN action with this interface can be routed to the next hop. If the next hop is not specified, the normal routing table will be used to forward probing traffic and traffic using SD-WAN action with this interface.

Next hop: 10.0.2.2

Select the targets to verify the status of **MPLS**. If you add custom targets, the default gateway target is replaced. Otherwise, the default gateway target is used.

Type	Target	Measure Loss, Latency, and Jitter	Add...
Ping	Next Hop	<input checked="" type="radio"/>	Edit...
			Delete

Require a successful probe to all targets to define the interface as active.

Use these settings for **MPLS**:

Probe Interval: 5 Seconds

Deactivate After: 3 Consecutive Failures

Reactivate After: 3 Consecutive Successes

OK Cancel Help

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

Network Configuration

Interfaces Link Aggregation Bridge VLAN Loopback Bridge Protocols WINS/DNS Dynamic DNS Multi-WAN Link Monitor SD-WAN PPPoE

Link Monitor Configuration

Monitored Interfaces:

- MPLS
- BovpnVif.1

Settings:

Specify the next hop for MPLS. This is preferred so that the probing traffic and traffic using an SD-WAN action with this interface can be routed to the next hop. If the next hop is not specified, the normal routing table will be used to forward probing traffic and traffic using SD-WAN action with this interface.

Next hop: . . .

Select the targets to verify the status of MPLS. If you add custom targets, the default gateway target is replaced. Otherwise, the default gateway target is used.

Type	Target	Measure Loss, Latency, and Jitter
Ping	4.2.2.1	<input checked="" type="radio"/>

Require a successful probe to all targets to define the interface as active.

Use these settings for MPLS:

Probe Interval: 5 Seconds

Deactivate After: 3 Consecutive Failures

Reactivate After: 3 Consecutive Successes

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

Interface

Assign virtual interface IP addresses (required for dynamic routing)

Local IP address: 10.0.49.1

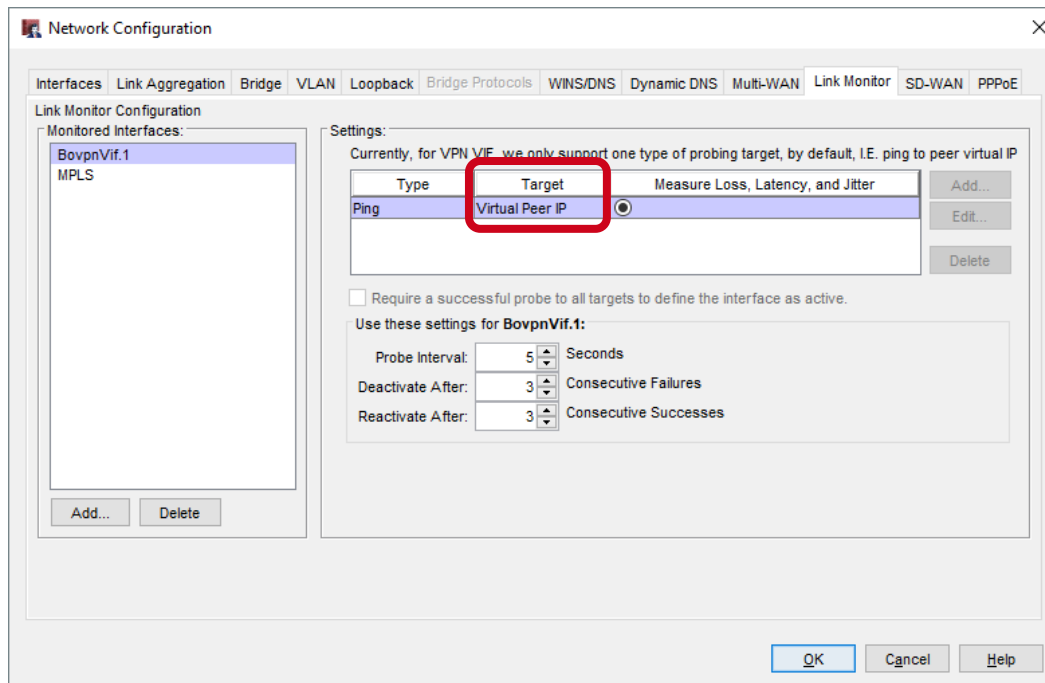
Peer IP address or netmask: 10.0.50.1

Use a netmask for a VPN to a third-party endpoint. (Fireware OS v11.11 and higher)

OK Cancel Help

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

Network Configuration

Interfaces | Link Aggregation | Bridge | VLAN | Loopback | Bridge Protocols | WINS/DNS | Dynamic DNS | Multi-WAN | **Link Monitor** | SD-WAN | PPPoE

Link Monitor Configuration

Monitored Interfaces:

External

Add... Delete

Settings:

Specify the next hope for External. This is preferred so that the probing traffic and traffic using an SD-WAN action with this interface can be routed to the next hop. If the next hop is not specified, the normal routing table will be used to forward probing traffic and traffic using SD-WAN action with this interface.

Next hop: . . .

Select the targets to verify the status of External. If you add custom targets, the default gateway target is replaced. Otherwise, the default gateway target is used.

Type	Target	Measure Loss, Latency, and Jitter
Ping	203.0.113.1	<input checked="" type="radio"/>

Add... Edit... Delete

Require a successful probe to all targets to define the interface as active.

Use these settings for External:

Probe Interval: 5 Seconds

Deactivate After: 3 Consecutive Failures

Reactivate After: 3 Consecutive Successes

OK Cancel Help

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



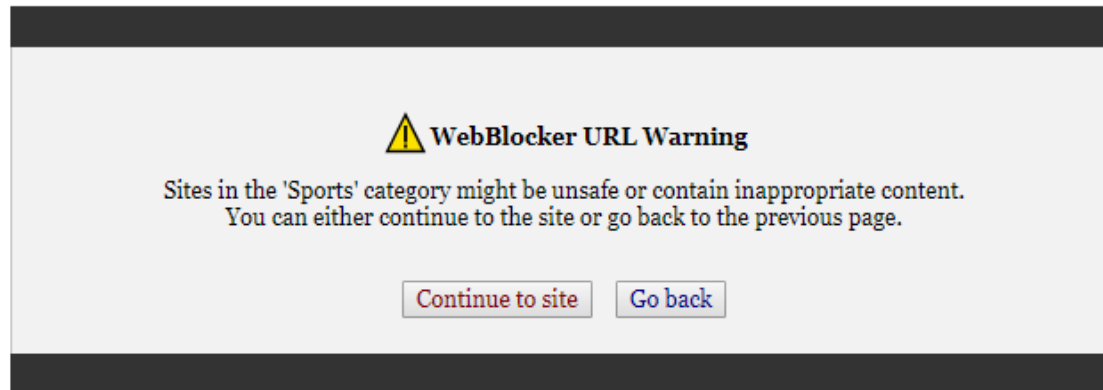
WebBlocker Warn Action

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

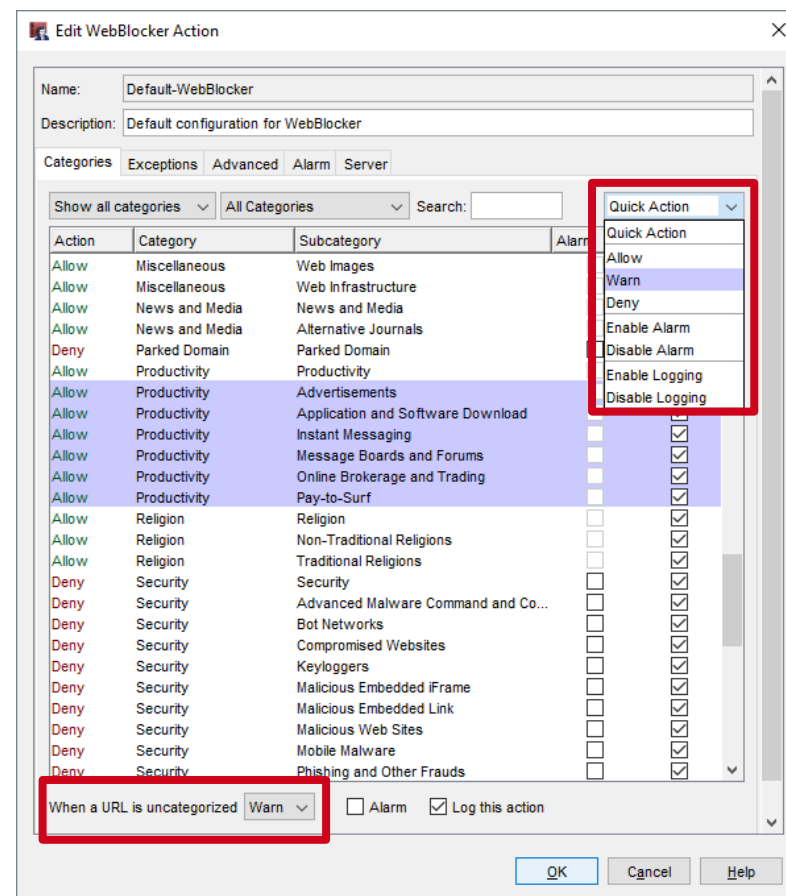


- Users can click **Continue to site** to open the website or **Go back** to return to the previous page
- The warning page includes the WebBlocker category and cannot be customized

WebBlocker Warn Action

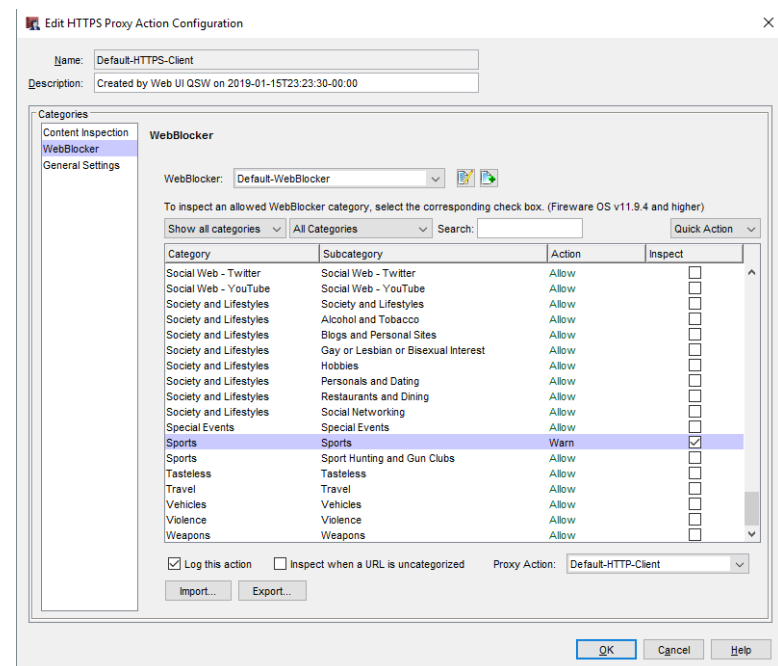
- To assign the Warn action to a WebBlocker category:
 1. Edit a WebBlocker action
 2. In the **Categories** tab, select the category
 3. From the **Quick Action** drop-down list, select **Warn**

- 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

The screenshot shows the WatchGuard Firewall Policy Manager interface. The main window displays a list of policies with columns for Order, Action, Policy Name, Policy Type, From, To, and Port. The policy 'WG-Auth-WebBlocker' is highlighted with a red box.

Order	Action	Policy Name	Policy Type	From	To	Port
1	FTP-proxy	FTP-proxy	FTP-proxy	Any-Trusted, Any-Optional	Any-External	tcp:21
2	HTTP-proxy	HTTP-proxy	HTTP-proxy	Any-Trusted, Any-Optional	Any-External	tcp:80
3	HTTPS-proxy	HTTPS-proxy	HTTPS-proxy	Any-Trusted	Any-External	tcp:443
4	WebBlocker Warn	WG-Auth-WebBlocker	WG-Auth	Any-Trusted, Any-Optional	Firebox	tcp:4100
5	WebBlocker Warn	WG-Auth-WebBlocker	WG-Auth	Any-Trusted, Any-Optional	Firebox	tcp:4100
6	WebBlocker Warn	WG-Auth-WebBlocker	WG-Auth	Any-Trusted, Any-Optional	Firebox	tcp:4126
7	WatchGuard Web UI	WG-Fireware-XTM-WebUI	WG-Fireware-XTM-WebUI	Any-Trusted, Any-Optional	Firebox	tcp:8080
8	Ping	Ping	Ping	Any-Trusted, Any-Optional	Any	icmp (type: 8, code: 255)
9	DNS	DNS	DNS	Any-Trusted, Any-Optional	Any-External	tcp:53 udp:53
10	WatchGuard	WG-Firebox-Mgmt	WG-Firebox-Mgmt	Any-Trusted, Any-Optional	Firebox	tcp:4105 tcp:4117 tcp:4118
11	Outgoing	TCP-UDP	TCP-UDP	Any-Trusted, Any-Optional	Any-External	tcp:0 (Any) udp:0 (Any)

Fireware OS v12.4.0

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

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

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

New Gateway

Gateway Name: gateway.1

Address Family: IPv6 Addresses (Firmware OS v12.4 or higher)

General Settings

Credential Method

Use Pre-Shared Key

Use IPsec Firebox Certificate

Select the certificate to be used for the Gateway.

Id	Certificate Name	Algorithm

Show All Certificates

Gateway Endpoints

#	Local Gateway			Remote Gateway		
	Interface	Type	ID	IP Address	Type	ID

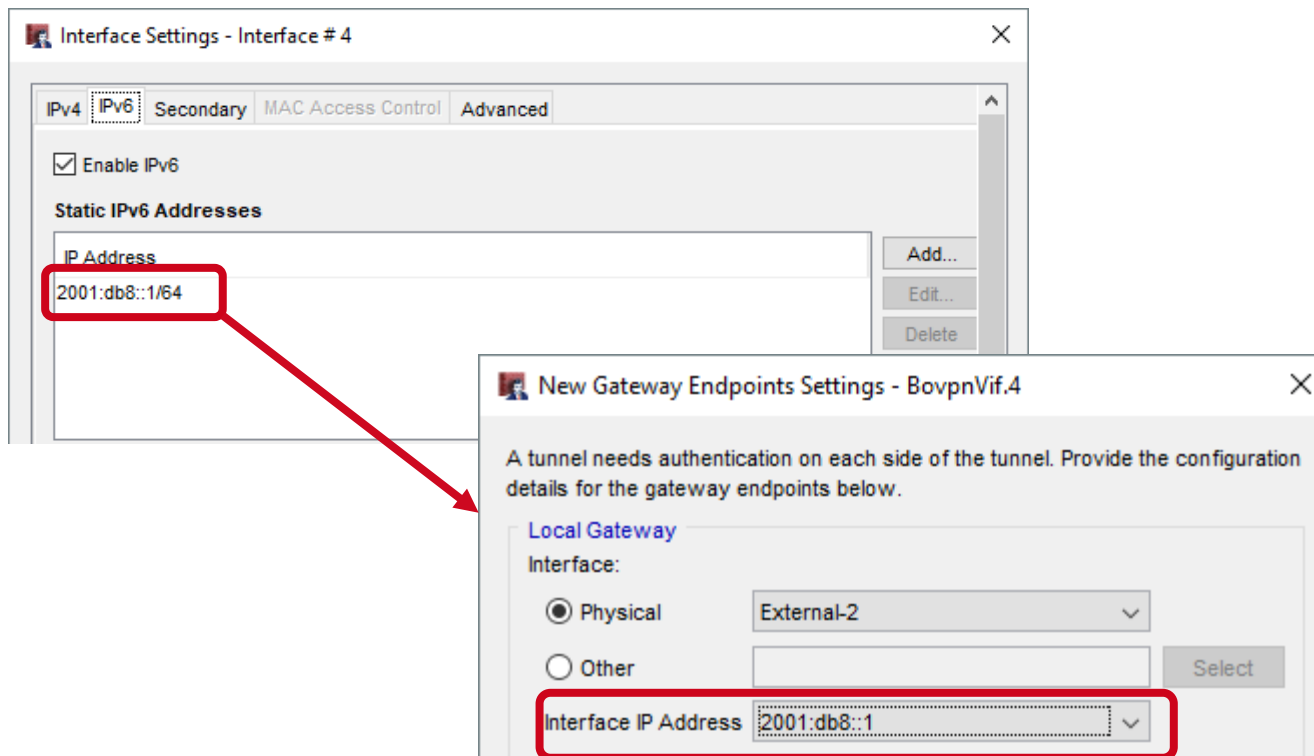
Use modem for failover

Start Phase 1 tunnel when Firebox starts

OK Cancel Help

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

Logging Setup

Specify where your Firebox sends log messages.

This Firebox can send log messages to more than one destination at the same time. Select one or more check boxes to specify where log messages are sent: Dimension, WSM Log Server, syslog server, or Firebox internal storage.

Dimension or WSM Log Server

Send log messages to these Dimension or WSM Log Servers:

Log Servers 1 Log Servers 2

The servers you specify on the **Log Servers 2** tab are only available for devices with Fireware OS v11.10 and higher. Configure...

Syslog Server

Send log messages to these syslog servers:

IP Address	Port	Log Format	Description	
10.0.1.30	514	Syslog	Server 1	^
10.0.2.30	514	Syslog	Server 2	
10.0.3.30	514	Syslog	Server 3	v

Info Multiple syslog servers are supported in Fireware OS v12.4 and higher.

Firebox Internal Storage

Send log messages to Firebox internal storage

Send log messages when the configuration for this device is changed

Performance Statistics... Diagnostic Log Level...

OK Cancel Help



Proxy Support for TLS 1.3

Proxy Support for TLS 1.3

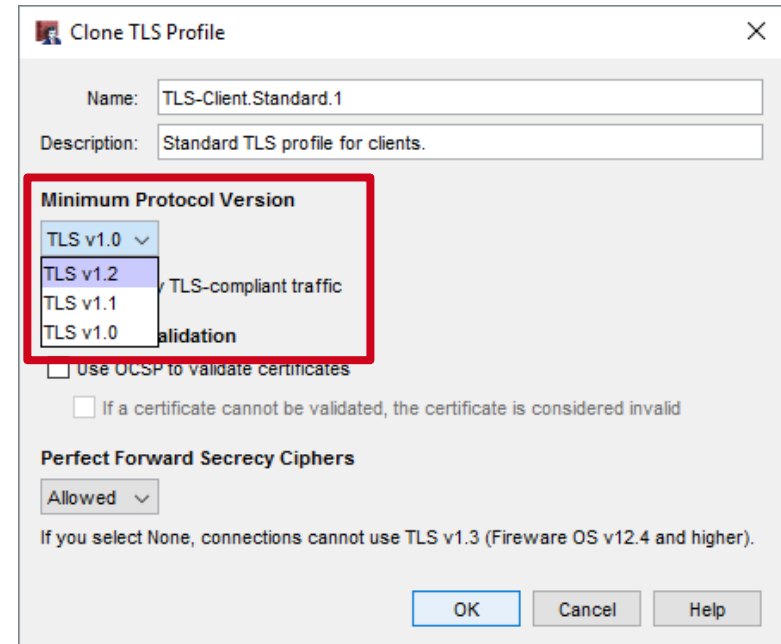
- Firewall now supports TLS 1.3 protocol
- Provides compliance and support for the latest standards
- Allows full inspection of HTTPS traffic
- TLS 1.3 connections are now supported and not downgraded to TLS 1.2

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

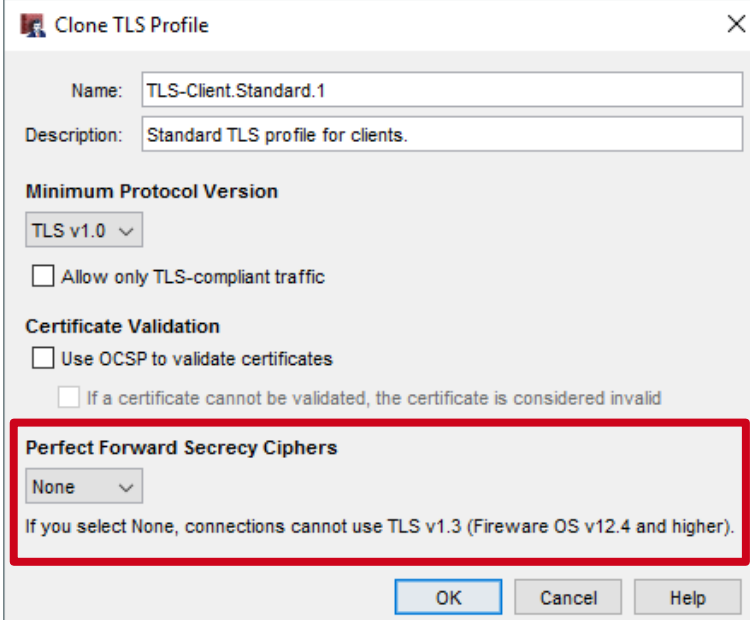
TLS Profile Updates

- 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



Clone TLS Profile

Name: TLS-Client.Standard.1

Description: Standard TLS profile for clients.

Minimum Protocol Version

TLS v1.0

Allow only TLS-compliant traffic

Certificate Validation

Use OCSP to validate certificates

If a certificate cannot be validated, the certificate is considered invalid

Perfect Forward Secrecy Ciphers

None

If you select None, connections cannot use TLS v1.3 (Fireware OS v12.4 and higher).

OK Cancel Help



Enhanced FireCluster Diagnostics

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
[More Details](#)

✓ FireCluster State

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

✗ Monitored Interfaces [More Details](#)

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

✓ Health [More Details](#)

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

Runtime Objects

BOVPN Tunnels:	0
CONNTRACK:	10

Enhanced FireCluster Diagnostics

- **File Object tab**

The screenshot displays the FireCluster diagnostics interface. At the top right, there is a refresh button labeled "30 SECONDS" and a pause button. The main header shows "FireCluster" and "FireCluster". Below this, a status indicator shows "✓ Synchronized".

On the left side, there are several metrics:

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

A "More Details" link is located below these metrics.

In the center, there is a table with the following data:

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

At the bottom, there is a navigation bar with four tabs: "Diagnostic" (with a red X), "File Object" (with a checkmark and highlighted by a red box), "Event History", and "Event History".

Below the navigation bar, the "File Objects" section is expanded, showing a list of items, all of which are "Matched":

- 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

Diagnostic | File Object | Event History

Backup - 801002DFD1C2g

FireCluster State

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

Monitored Interfaces

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

More Details

Master 801002DAA2FEB - Monitored Interfaces

DATE ↑	INTERFACE	DESCRIPTION
2019-01-25 09:13:04	eth7	Interface UP
2019-01-25 09:14:25	eth7	Physical link down
2019-01-25 09:15:19	eth7	Interface UP
2019-01-25 09:15:41	eth7	Physical link down
2019-01-25 09:15:57	eth7	Interface UP

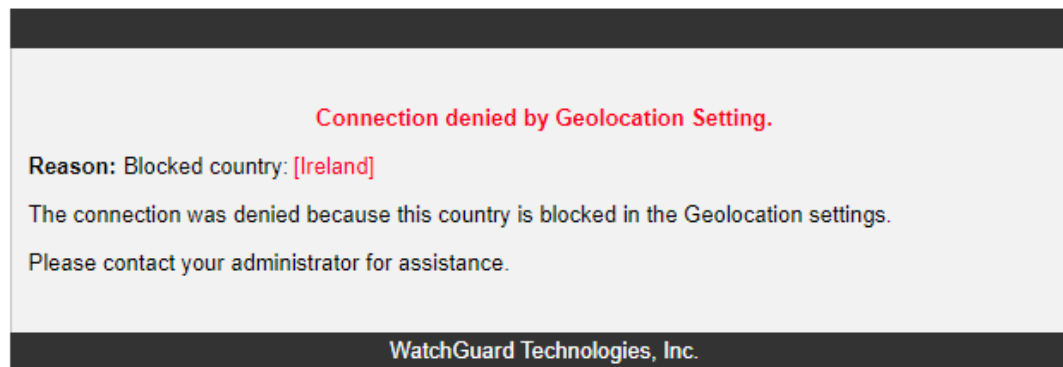
CLOSE



Geolocation Deny Message

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



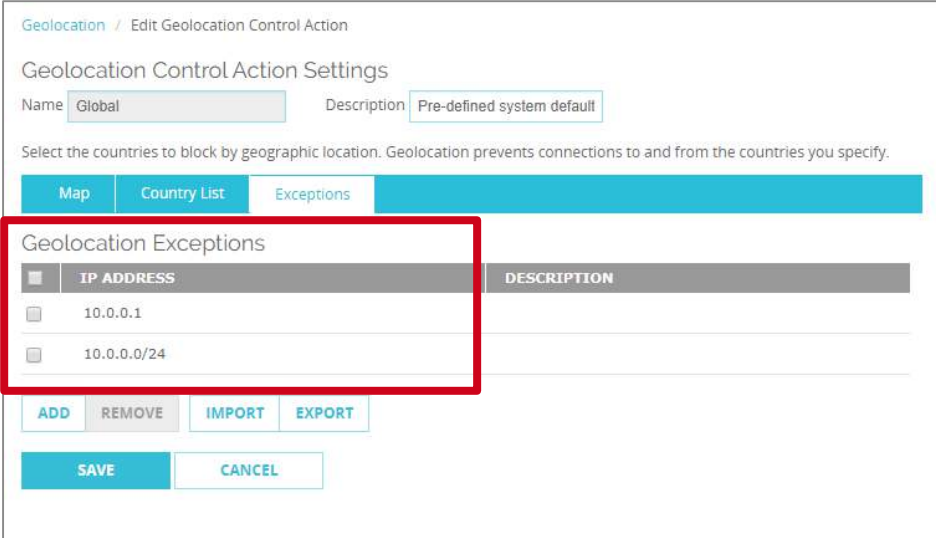
Exception/Blocked Site List Enhancements

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



Geolocation / Edit Geolocation Control Action

Geolocation Control Action Settings

Name: Global Description: Pre-defined system default

Select the countries to block by geographic location. Geolocation prevents connections to and from the countries you specify.

Map Country List Exceptions

Geolocation Exceptions

IP ADDRESS	DESCRIPTION
<input type="checkbox"/> 10.0.0.1	
<input type="checkbox"/> 10.0.0.0/24	

ADD REMOVE IMPORT EXPORT

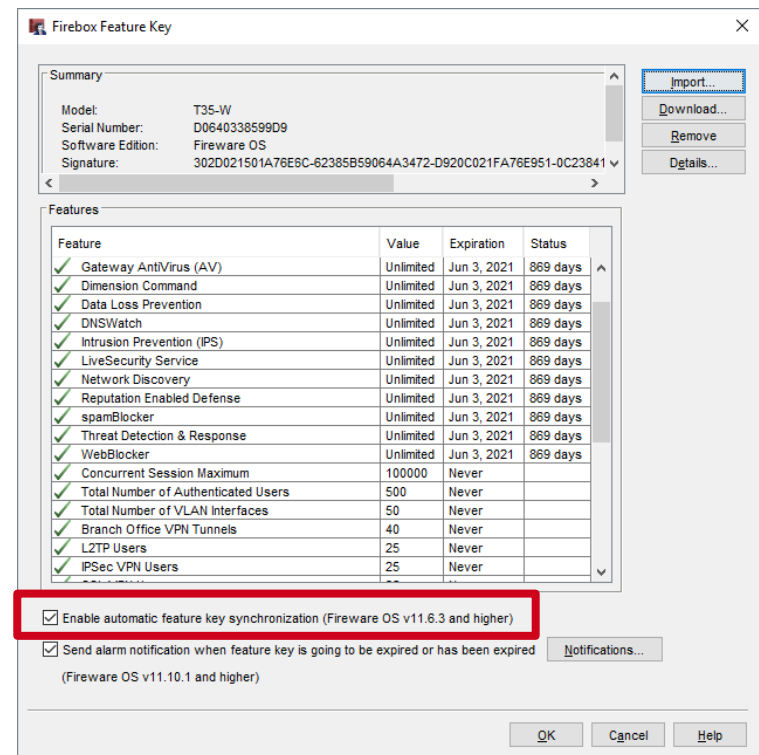
SAVE CANCEL



Synchronize Feature Key Enhancements

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





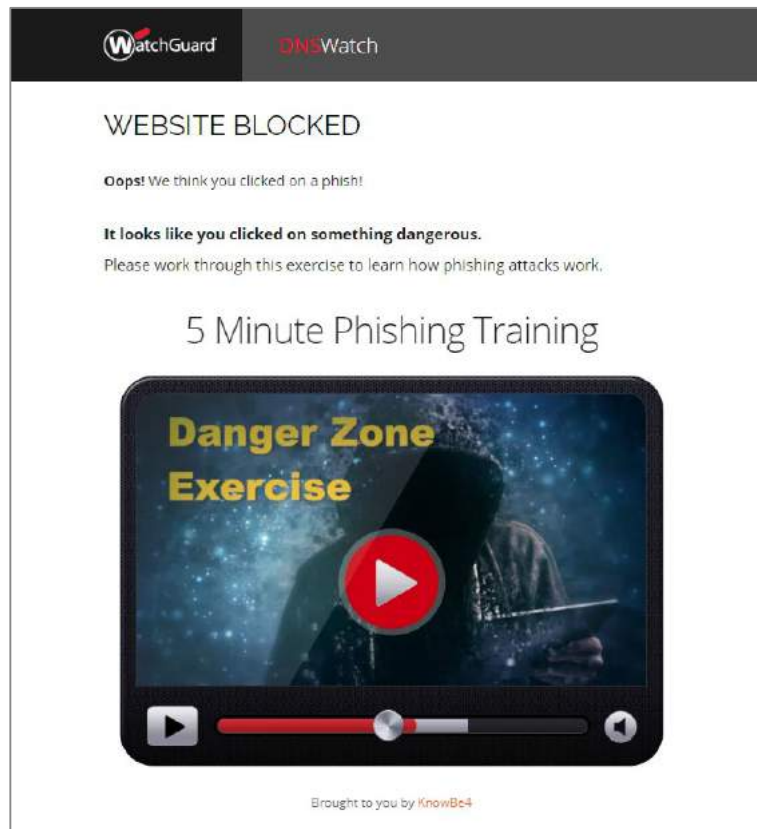
Proxy Enhancements for DNSWatch

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

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

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

SSO Agent Debug Tool Enhancements

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

The screenshot shows the 'Status' window of the SSO Agent. It includes a 'Debug Log' section set to 'On' with a 'Refresh Interval' of '5 seconds'. The 'SSO Agent version' is '12.4.0.31059 B585506'. The main content is divided into three sections, each highlighted with a red box:

ELM, EM and SSO client status:

Domain Name	IP Address	Type	Status	Version	Build
[Redacted]	[Redacted]	ELM	connected	12.3.1.0	585506
[Redacted]	[Redacted]	EM	disconnected		

Authentication Info: Success: 2. From ELM:2, EM:0, SSO Client:0, AD:0

Domain Name	IP Address	Type	User Name	Authentication Time
ssolqdn.com	[Redacted]	ELM	administrator	1/22/2019 1:40:04 PM
ssolqdn.com	[Redacted]	ELM	ssotest1	1/22/2019 2:22:46 PM

Processing IP list: 54

IP Address	Type
1.1.1.77	ELM
1.1.2.77	ELM
1.1.1.78	ELM
1.1.2.78	ELM
1.1.1.79	ELM
1.1.2.79	ELM

Pending IP list: 38

IP Address
1.1.2.2
1.1.1.3
1.1.2.3
1.1.1.4
1.1.2.4
1.1.1.5

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



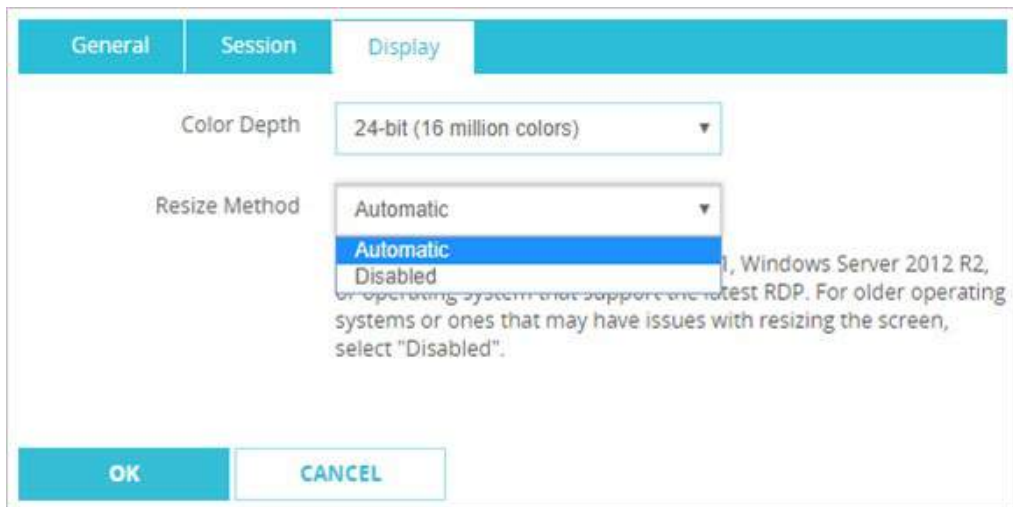
Access Portal Enhancements

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

Authentication Servers

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

AUTHENTICATION SERVER	
example.com (default)	
Firebox-DB	

Firebox-DB ▼ ADD REMOVE MOVE UP MOVE DOWN

Default domain

ADF

Or login with:

username

LOG IN

Alternative domain

ADF

Or login with:

Domain\username

LOG IN



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

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

Servers / RADIUS

Before you configure your Firebox device to use a RADIUS authentication server, make sure the server can successfully accept and process RADIUS authentication requests.

Primary Server Settings

Enable RADIUS Server

IP Address: 2001.4860.4860.:8888

Port: 1812

Shared Secret:

Confirm Secret:

Timeout: 10 seconds

Retries: 3

Dead Time: 3 Minutes

Group Attribute: 11

Authentication Servers

Firebox-DB RADIUS SecurID LDAP Active Directory

Make sure that the users can successfully authenticate to the SecurID server.

Primary Server Settings

Enable SecurID server

IP Address: 2001.4860.4860.:8888

Port: 1812

Shared Secret:

Confirm Secret:

Timeout: 10 seconds

Retry: 3

Dead Time: 3 minutes

Group Attribute: 11

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

Servers / RADIUS

Before you configure your Firebox device to use a RADIUS authentication server, make sure the server can successfully accept and process RADIUS authentication requests.

Primary Server Settings

Enable RADIUS Server

IP Address: 2001:4860:4860::8888

Port: 1812

Shared Secret:

Confirm Secret:

Timeout: 10 seconds

Retries: 3

Dead Time: 3 Minutes

Group Attribute: 11

Authentication Servers

Firebox-DB RADIUS SecurID LDAP Active Directory

Make sure that the users can successfully authenticate to the SecurID server.

Primary Server Settings

Enable SecurID server

IP Address: 2001:4860:4860::8888

Port: 1812

Shared Secret:

Confirm Secret:

Timeout: 10 seconds

Retry: 3

Dead Time: 3 minutes

Group Attribute: 11




Technology Integrations Page Updates

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

Technology Integrations

WatchGuard partners with industry-leading technology companies to develop tight integrations for stronger security, easier deployments, and better interoperability in your IT environments. To enable and configure Firebox integration with a technology partner, click the configure button. You can configure the Firebox to integrate with more than one third party product at the same time.




Autotask

Autotask Corporation helps IT organizations worldwide work smarter with a complete, cloud-based IT business management platform that enables efficiency, accountability and access to the metrics that drive intelligent business decisions.

Integration: WatchGuard Firebox appliances integrate with Autotask PSA for integrated, closed-loop service ticketing and auto synchronization of asset information.

[CONFIGURE](#) [INTEGRATION GUIDE](#) [LEARN MORE](#) [SOLUTION BRIEF](#)




ConnectWise

Made for companies that sell, service, and support technology, ConnectWise is the leading business management platform worldwide that enables technology companies to achieve the highest level of profitability and service to their clients.

Integration: WatchGuard Firebox appliances and WatchGuard Dimension integrate with ConnectWise for service ticketing, security asset synchronization, and automated reporting directly from ConnectWise.

[CONFIGURE](#) [INTEGRATION GUIDE](#) [LEARN MORE](#) [SOLUTION BRIEF](#)



Tigerpaw

Tigerpaw deliver complete business automation and management across all aspects of your business: organizing and streamlining operations, building a marketing and sales pipeline, optimizing your customer's experience and understanding your metrics.

Integration: WatchGuard Firebox appliances integrate with Tigerpaw PSA for integrated, closed-loop service ticketing and auto synchronization of asset information.

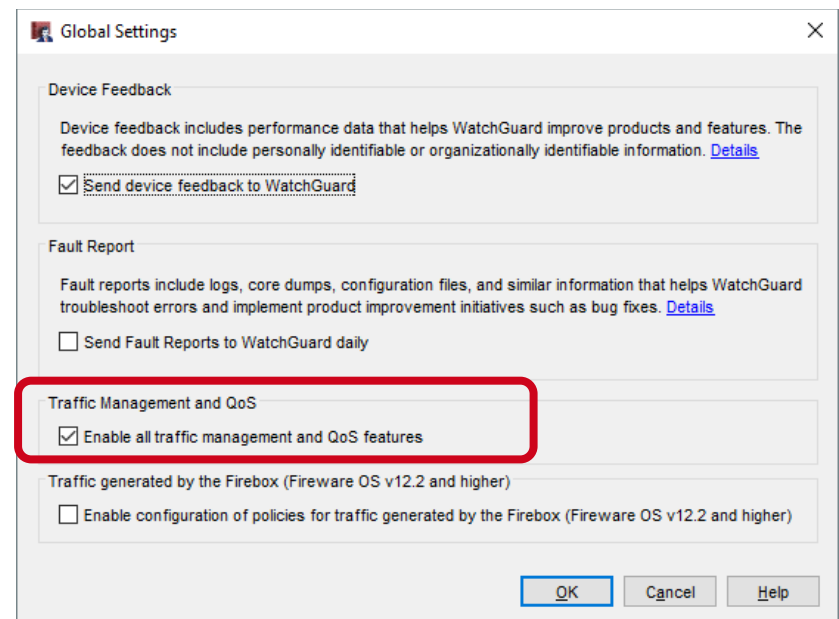
[CONFIGURE](#) [INTEGRATION GUIDE](#)



Device Configuration Template Updates

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

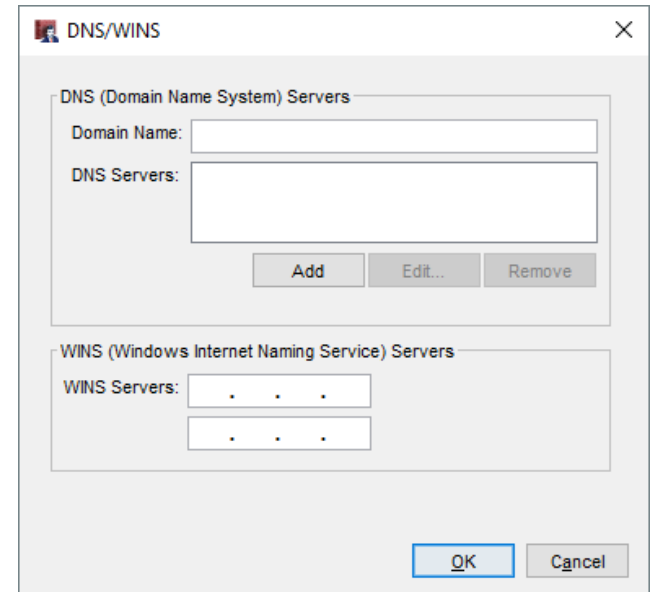
The screenshot shows the 'New Policy Properties' dialog box in a firewall configuration tool. The 'Advanced' tab is selected, and the 'QoS' section is highlighted with a red rounded rectangle. The 'Name' field is set to 'FTP-proxy' and the 'Enable' checkbox is checked. The 'Schedule' is set to 'Always On'. Under 'Traffic Management Actions', both 'Forward (From > To)' and 'Reverse (To > From)' are set to 'Default (No Limits)'. The 'Connection Rate (per second)' is set to 'No Limit', and the 'Alarm when capacity exceeded' checkbox is unchecked. Under 'ICMP Error Handling', 'Use global setting' is selected. The 'QoS' section is expanded, showing the following settings:

Setting	Value
Override per-interface settings	<input checked="" type="checkbox"/>
Marking Type	DSCP
Marking Method	Preserve
Value	0 (Best Effort)
Prioritize Traffic Based On	Custom Value
Value	0 (Normal)

At the bottom of the dialog, there are 'OK', 'Cancel', and 'Help' buttons.

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**



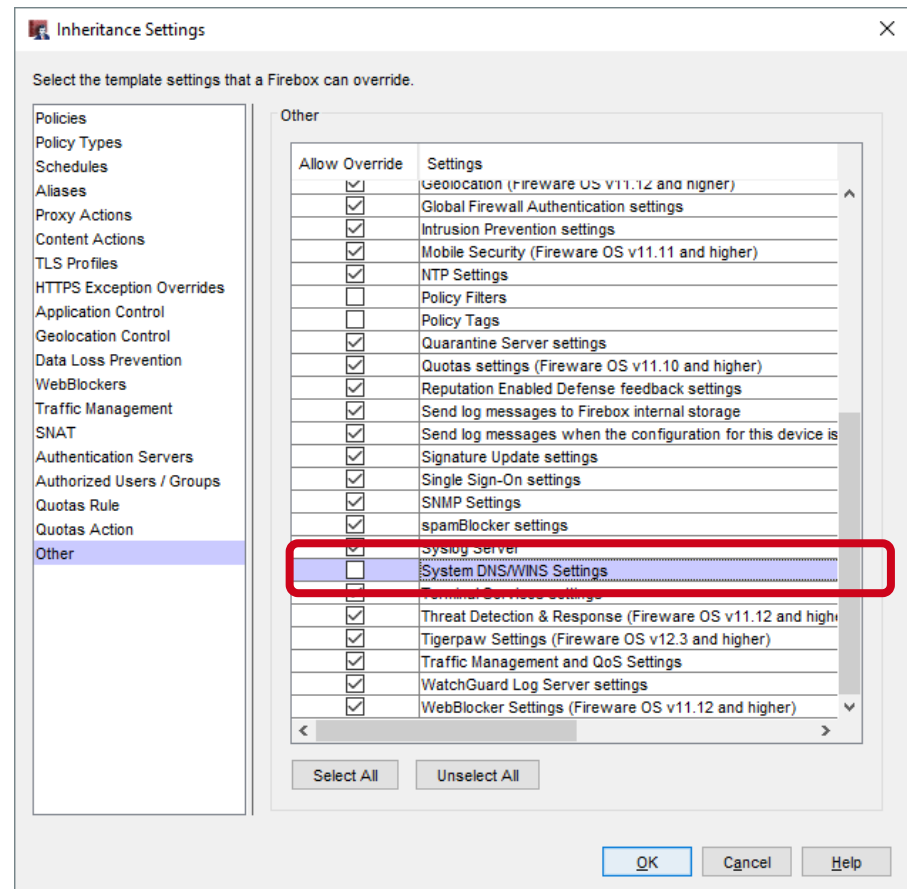
The screenshot shows a dialog box titled "DNS/WINS" with a close button (X) in the top right corner. The dialog is divided into two main sections:

- DNS (Domain Name System) Servers:** This section contains a "Domain Name:" text input field, a "DNS Servers:" list box, and three buttons: "Add", "Edit...", and "Remove".
- WINS (Windows Internet Naming Service) Servers:** This section contains a "WINS Servers:" label followed by two rows of text input fields, each containing three dots (". . .") to indicate IP address entry.

At the bottom right of the dialog, there are "OK" and "Cancel" buttons.

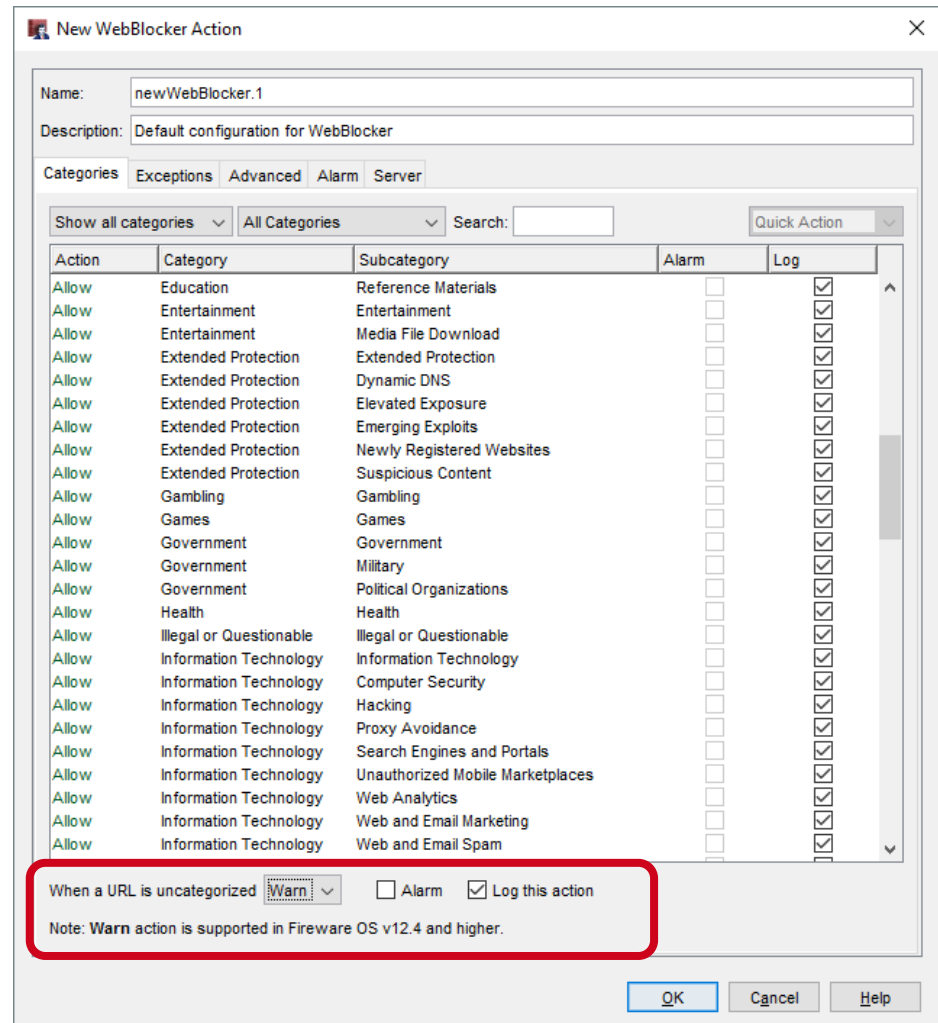
Device Configuration Template – DNS/WINS

- 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 Firewall v12.4 and higher





Edit 1-to-1 NAT

Edit 1-to-1 NAT

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

1-to-1 NAT

1-to-1 NAT rewrites and redirects packets sent to one range of IP Addresses to another range of addresses.

INTERFACE	# OF HOSTS	NAT BASE	REAL BASE
External	1	192.0.2.15	10.0.1.15

ADD EDIT REMOVE

SAVE

NAT / 1-to-1 NAT Configuration

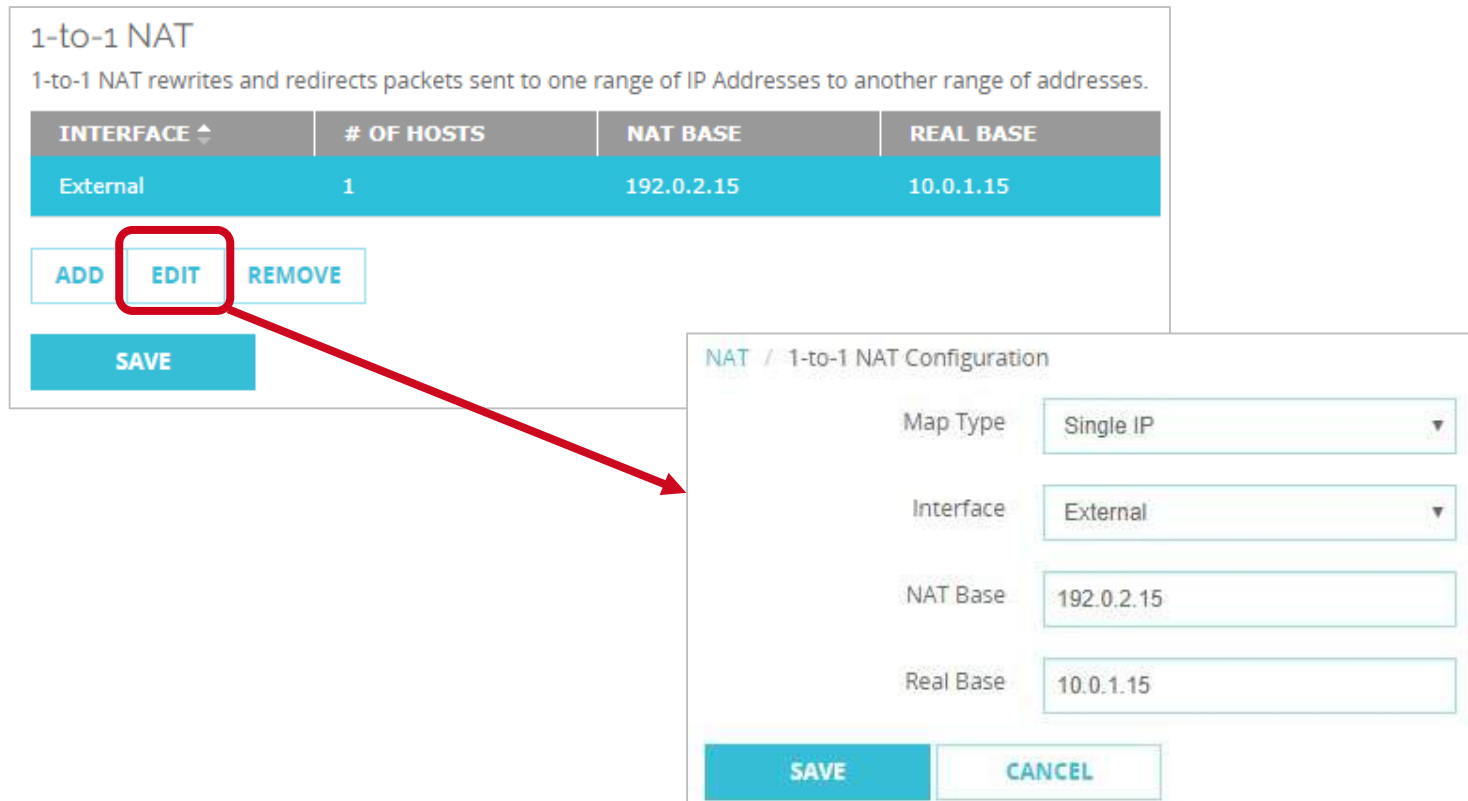
Map Type: Single IP

Interface: External

NAT Base: 192.0.2.15

Real Base: 10.0.1.15

SAVE CANCEL



Thank You!