What’s New in Fireware v12.0

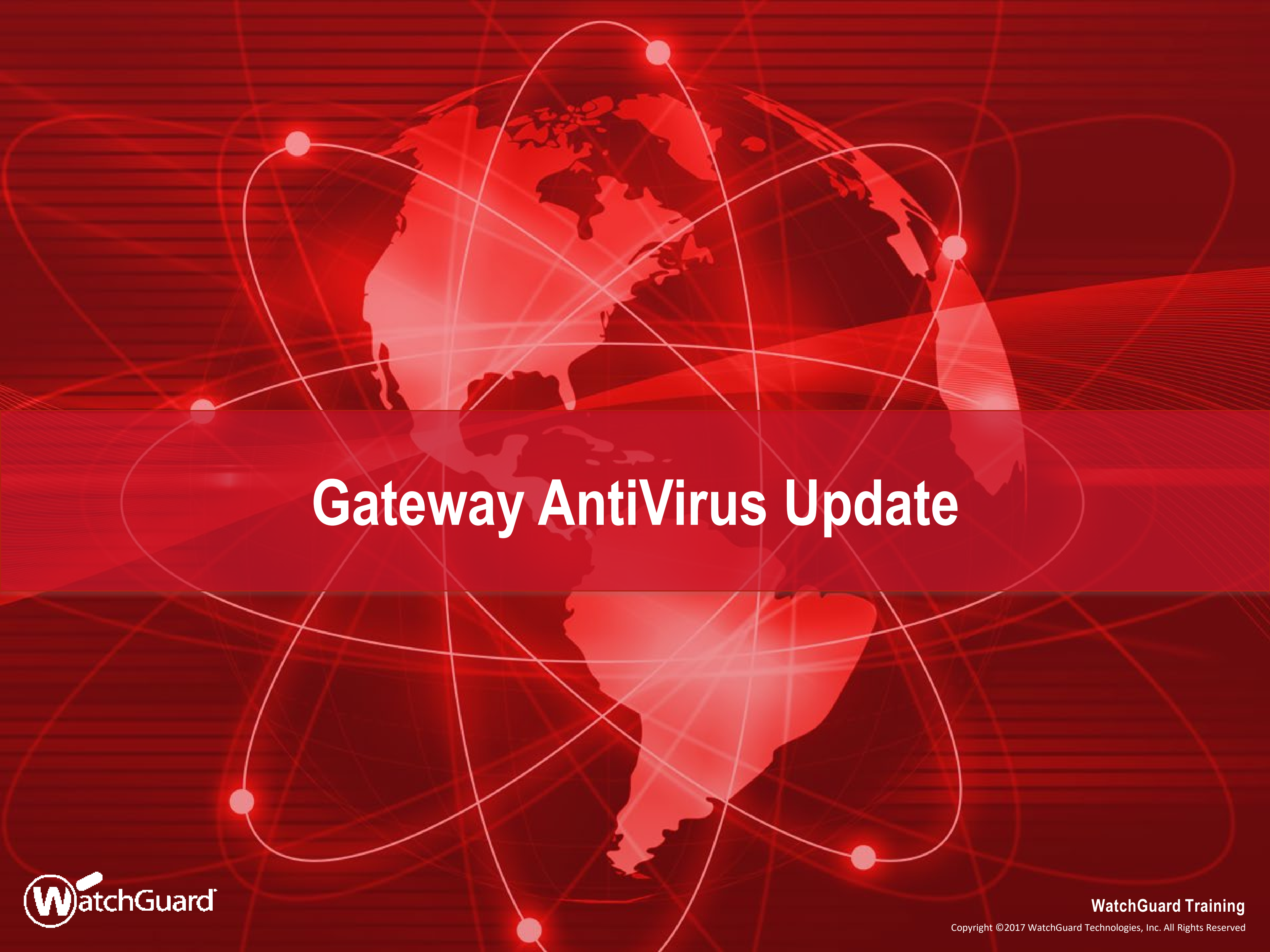
WatchGuard Training

What's New in Fireware v12.0

- Gateway AntiVirus Update
- Content Actions for HTTP and HTTPS
- IMAP Proxy
- OS Compatibility Setting Enhancement
- Gateway Wireless Controller Enhancements
- Mobile VPN with PPTP Feature Removed
- Updated Default VPN Security Settings
- Removed Obsolete Security Settings for Mobile VPN with SSL

What's New in Fireware v12.0

- APT Blocker Enhancements
  - Javascript Scanning of Email Attachments
  - SMTP and IMAP Zero-Day Protection
- WebBlocker Enhancements
- Larger IPS Signature Set
- WatchGuard Cloud on your Firebox
- ConnectWise Integration Enhancements
- Multicast Routing



Gateway AntiVirus Update

WatchGuard Training

Gateway AntiVirus Update

- Gateway AntiVirus has been updated to use a scan engine and signature set from Bitdefender
  - In previous releases, the scan engine and signature set was provided by AVG
  - WatchGuard used virus samples to compare the detection capability of several vendors
    - Bitdefender had the highest detection rate
  - Bitdefender offers high performance and frequent signature updates

Gateway AntiVirus Update

- Gateway AntiVirus signature set sizes vary by model

Gateway AntiVirus Signature Set	Firebox Models
Standard	T10, T30 XTM 25, 26, 33, 330
Enterprise	T50, T70, M200, M300 M370, M400, M440, M470, M500, M570, M670, M4600, M5600 XTM 515, 525, 535, 545, 810, 820, 830, 870, XTM 1050, 1500, 2050, 2520

- Virtual Fireboxes (FireboxV, XTMv, Firebox Cloud) get the Enterprise set if the instance has 2GB or more of memory

Gateway AntiVirus Update

- There are no changes to Gateway AntiVirus configuration settings
- Signature updates are now faster and are all incremental
  - Reduces the download time
  - Reduces the time for FireCluster synchronization of signatures

Gateway AntiVirus Update

- For increased effectiveness, Gateway AV no longer supports partial file scanning
- Gateway AV now automatically uses a scan limit that is much higher than the previous default values so more files get a complete security scan
  - 5 MB — Firebox T10, T30, XTM 25, 26, 33
    - If the Gateway AV File Scan limit is set to less than 5 MB, Gateway AV scans files up to 5 MB in size
  - 10MB — All other Firebox models
    - If the Gateway AV File Scan limit is set to less than 10 MB, Gateway AV scans files up to 10 MB in size

Gateway AntiVirus — Upgrade

- When you upgrade to Fireware v12.0, the old AVG files are removed and the Firebox downloads the new Bitdefender engine and signature set
  - It can take 7–10 minutes to download the files the first time
  - It takes another 5–7 minutes to synchronize a FireCluster
- To minimize downtime, we recommend that you do not schedule the upgrade during business hours

Content Actions and Routing Actions for HTTP and HTTPS Proxy Policies

WatchGuard Training

Content Actions and Routing Actions

- A *content action* is a new type of proxy action for inbound HTTP proxy policies and HTTPS Server proxy actions
- Select a content action to use the same public IP address for multiple public web servers that are behind the Firebox
  - A content action enables the Firebox to route incoming HTTP and HTTPS requests for one public IP address to more than one internal web server
  - This reduces the number of public IP addresses you need for public web servers on your network
- To redirect HTTPS requests based on the domain name without content inspection, you can specify a *routing action* in a domain name rule in the HTTPS Server proxy action

Content Actions and Routing Actions

- Content actions have two main functions:
  - Host Header Redirect
    - Sends inbound HTTP and inspected HTTPS requests to different internal servers based on the path and domain in the HTTP request
  - TLS/SSL Offloading
    - Relieves an internal web server of the processing burden for encryption and decryption of TLS and SSL connections
      - Encrypted (HTTPS) traffic between external clients and the Firebox
      - Clear-text (HTTP) traffic between the Firebox and the internal server
- In an HTTPS Server proxy action, routing actions send inbound HTTPS requests to different servers based on the domain name, without content inspection

Content Actions and Routing Actions

- Content actions
  - Match the host header/path for each HTTP request
  - Send an HTTP request to a specific server IP address and port
  - Content actions do not rewrite data in the request or response
- Use cases for content actions:
  - Redirect HTTP requests based on the domain and host
  - Redirect HTTPS requests with content inspection
  - SSL offloading for HTTPS requests with content inspection
- Use case for routing actions in the HTTPS Server proxy:
  - Redirect HTTPS without content inspection

HTTP Requests and Content Actions

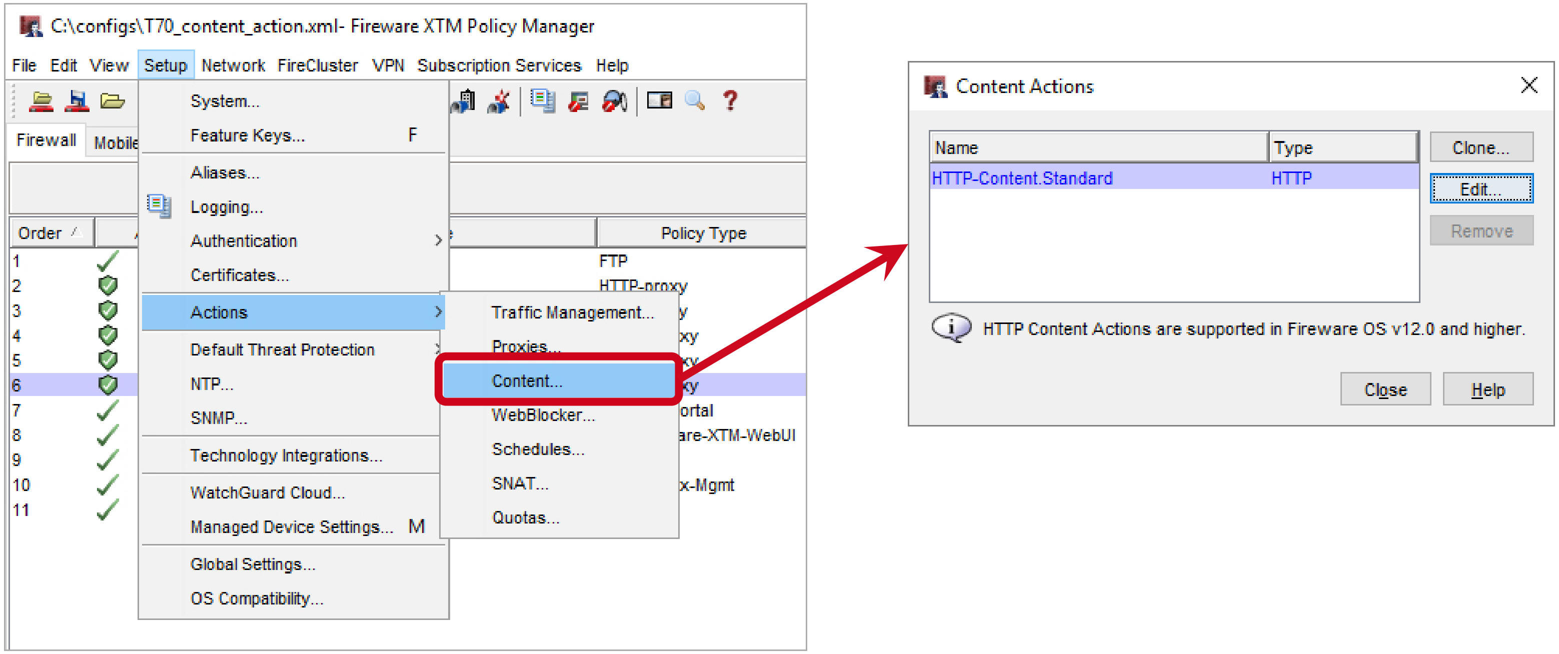
- When a user browses to a URL, the web browser sends the URL as an HTTP request
- The HTTP request includes:
  - A request method (GET or PUT) that specifies the path
  - A host header that specifies the domain name
  - For example, if you browse to the Support section of watchguard.com, the HTTP request includes this information:

```
GET /wgrd-support/overview HTTP/1.1
Host: www.watchguard.com
```

- Content actions review the combination of the domain name and path in the HTTP request to determine which content rule to apply

Content Action Configuration

- Content actions are separate from other proxy actions
- From Policy Manager, select **Setup** > **Actions** > **Content**
- To create a new content action, clone or edit the predefined content action

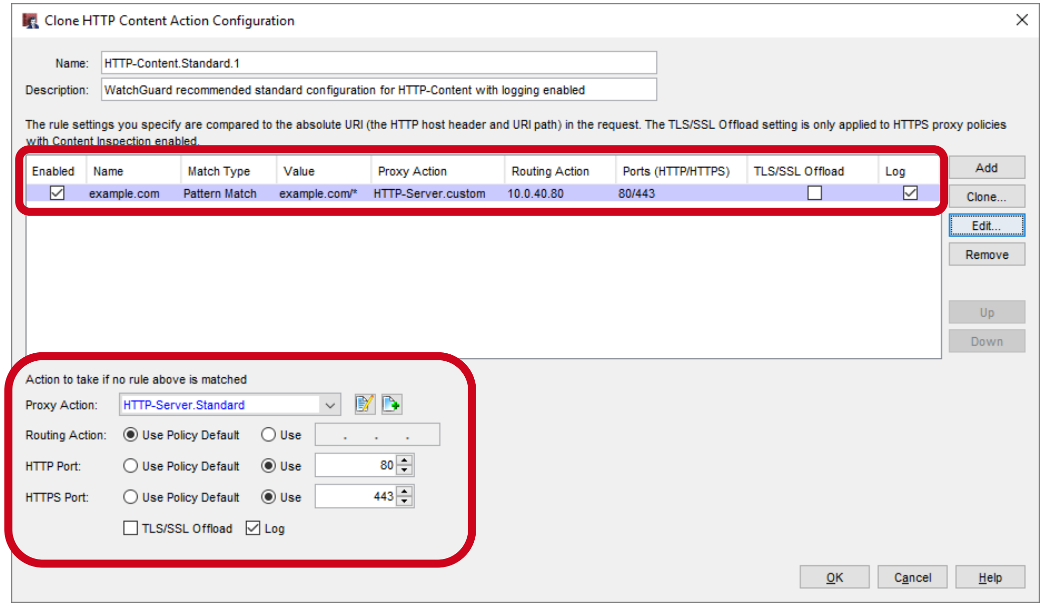


Name	Type
HTTP-Content.Standard	HTTP

HTTP Content Actions are supported in Fireware OS v12.0 and higher.

Content Action Configuration

- In a content action, you can configure:
  - Content rules to define the action for each destination, based on whether content in the host header or SNI matches the specified domain and path
  - The action to take if no content rule is matched



Clone HTTP Content Action Configuration

Name: HTTP-Content.Standard.1

Description: WatchGuard recommended standard configuration for HTTP-Content with logging enabled

The rule settings you specify are compared to the absolute URI (the HTTP host header and URI path) in the request. The TLS/SSL Offload setting is only applied to HTTPS proxy policies with Content Inspection enabled.

Enabled	Name	Match Type	Value	Proxy Action	Routing Action	Ports (HTTP/HTTPS)	TLS/SSL Offload	Log
☑	example.com	Pattern Match	example.com/*	HTTP-Server.custom	10.0.40.80	80/443	□	☑

Action to take if no rule above is matched

Proxy Action: HTTP-Server.Standard

Routing Action: ● Use Policy Default ○ Use . . .

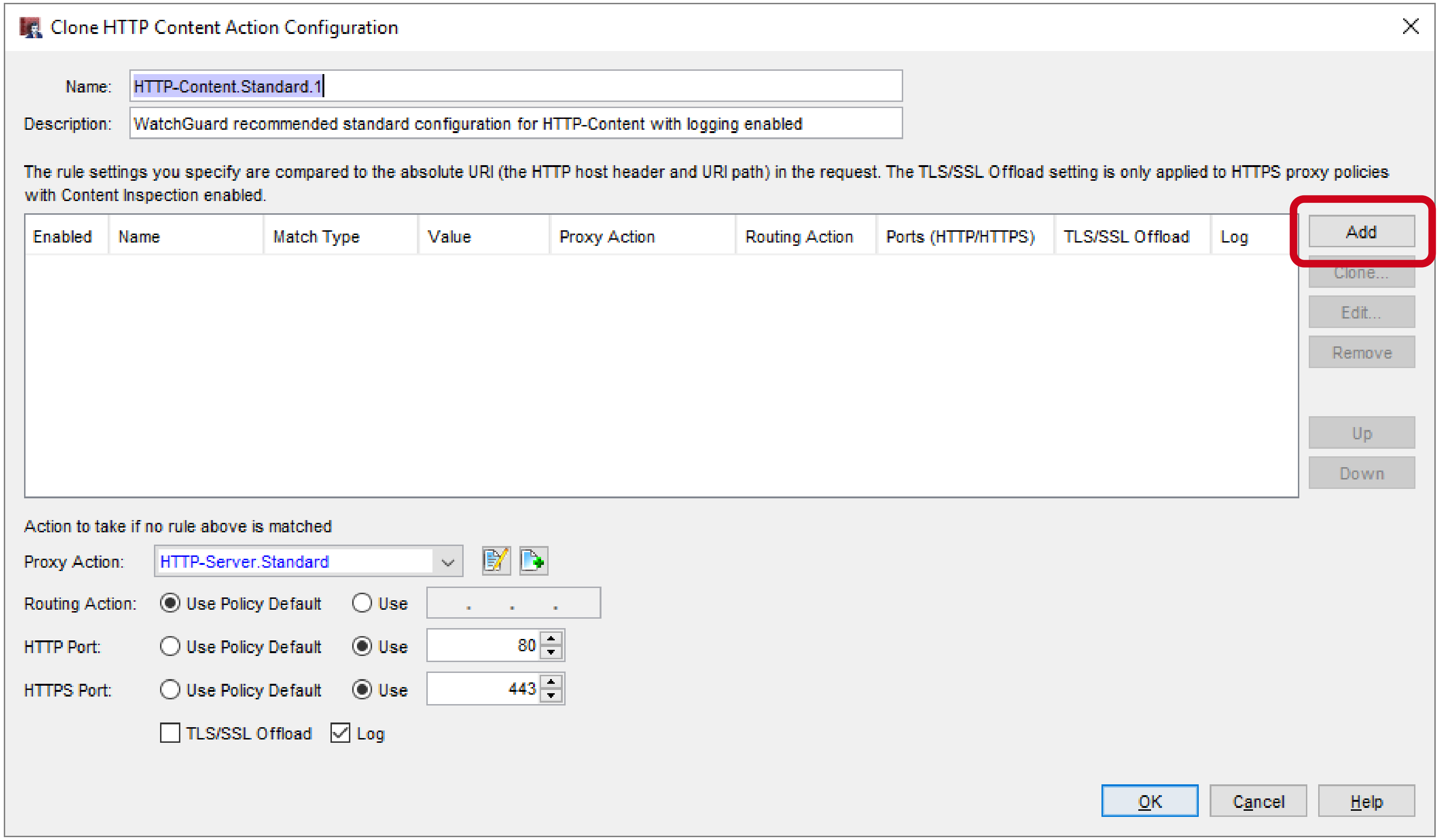
HTTP Port: ○ Use Policy Default ● Use 80

HTTPS Port: ○ Use Policy Default ● Use 443

□ TLS/SSL Offload ☑ Log

Content Action Configuration

- In a content action, click **Add** to create a new content rule



Clone HTTP Content Action Configuration

Name: HTTP-Content.Standard.1

Description: WatchGuard recommended standard configuration for HTTP-Content with logging enabled

The rule settings you specify are compared to the absolute URI (the HTTP host header and URI path) in the request. The TLS/SSL Offload setting is only applied to HTTPS proxy policies with Content Inspection enabled.

Enabled	Name	Match Type	Value	Proxy Action	Routing Action	Ports (HTTP/HTTPS)	TLS/SSL Offload	Log

Action to take if no rule above is matched

Proxy Action: HTTP-Server.Standard

Routing Action: ● Use Policy Default ○ Use . . .

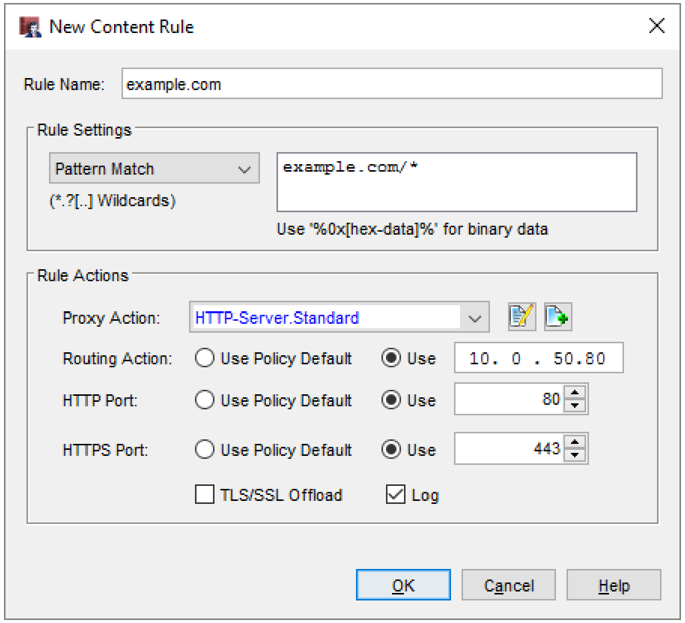
HTTP Port: ○ Use Policy Default ● Use 80

HTTPS Port: ○ Use Policy Default ● Use 443

□ TLS/SSL Offload ☑ Log

Content Rules

- Each content rule specifies:
  - A pattern to match
  - HTTP proxy action
  - Routing action (IP address)
  - HTTP and HTTPS ports
  - TLS/SSL Offload setting
  - Log setting



Rule Name: example.com

Rule Settings

Pattern Match (*.?[..] Wildcards)

example.com/*

Use '%0x[hex-data]%' for binary data

Rule Actions

Proxy Action: HTTP-Server.Standard

Routing Action: ○ Use Policy Default ● Use 10. 0 . 50.80

HTTP Port: ○ Use Policy Default ● Use 80

HTTPS Port: ○ Use Policy Default ● Use 443

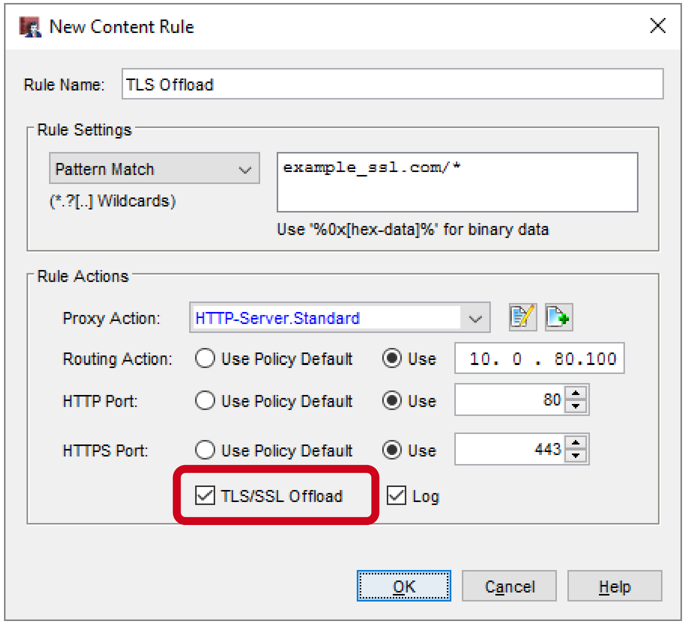
□ TLS/SSL Offload ☑ Log

- Pattern match against domain and host:

Domain only	wiki.example.net/*
Path	*/blog/*
Domain and path	blog.example.net/resource/*

TLS/SSL Offloading

- To enable TLS/SSL offloading for HTTPS, in the content rule action, select the **TLS/SSL Offload** check box
- With TLS/SSL offloading:
  - HTTPS is used between external clients and the Firebox
  - HTTP is used between the Firebox and the internal server



New Content Rule

Rule Name: TLS Offload

Rule Settings

Pattern Match (*.?[..] Wildcards) — example_ssl.com/*

Use '%0x[hex-data]%' for binary data

Rule Actions

Proxy Action: HTTP-Server.Standard

Routing Action: ○ Use Policy Default ● Use 10. 0 . 80.100

HTTP Port: ○ Use Policy Default ● Use 80

HTTPS Port: ○ Use Policy Default ● Use 443

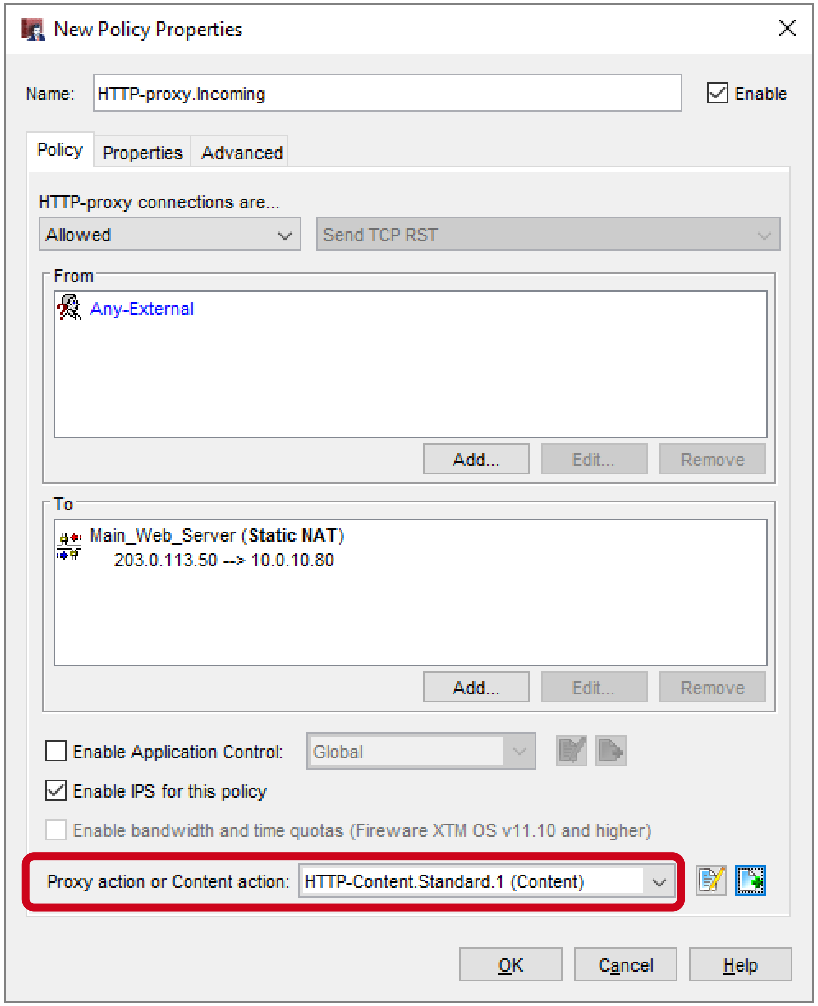
☑ TLS/SSL Offload ☑ Log

TLS/SSL Offloading

- If you use TLS/SSL offloading, you might need to change configuration settings on your server application
  - Some server applications must be configured to use HTTPS in links/redirects even if incoming requests use HTTP
    - $_SERVER[‘HTTPS’]=‘on’; (Wordpress)
  - Some server applications recognize the *Upgrade-Insecure-Requests* Header
    - Upgrade-Insecure-Requests: 1

Content Action in an HTTP Proxy

- In an HTTP proxy policy, select a content action
  - The drop-down list includes both proxy actions and content actions
- In the policy **To** list, add a **Static NAT** rule, or use 1-to-1 NAT
  - Policy NAT settings are not used unless a routing action in the content action specifies *Use Policy Default*



New Policy Properties

Name: HTTP-proxy.Incoming ☑ Enable

HTTP-proxy connections are... Allowed

Send TCP RST

From: Any-External

To: Main_Web_Server (**Static NAT**) 203.0.113.50 --> 10.0.10.80

□ Enable Application Control: Global

☑ Enable IPS for this policy

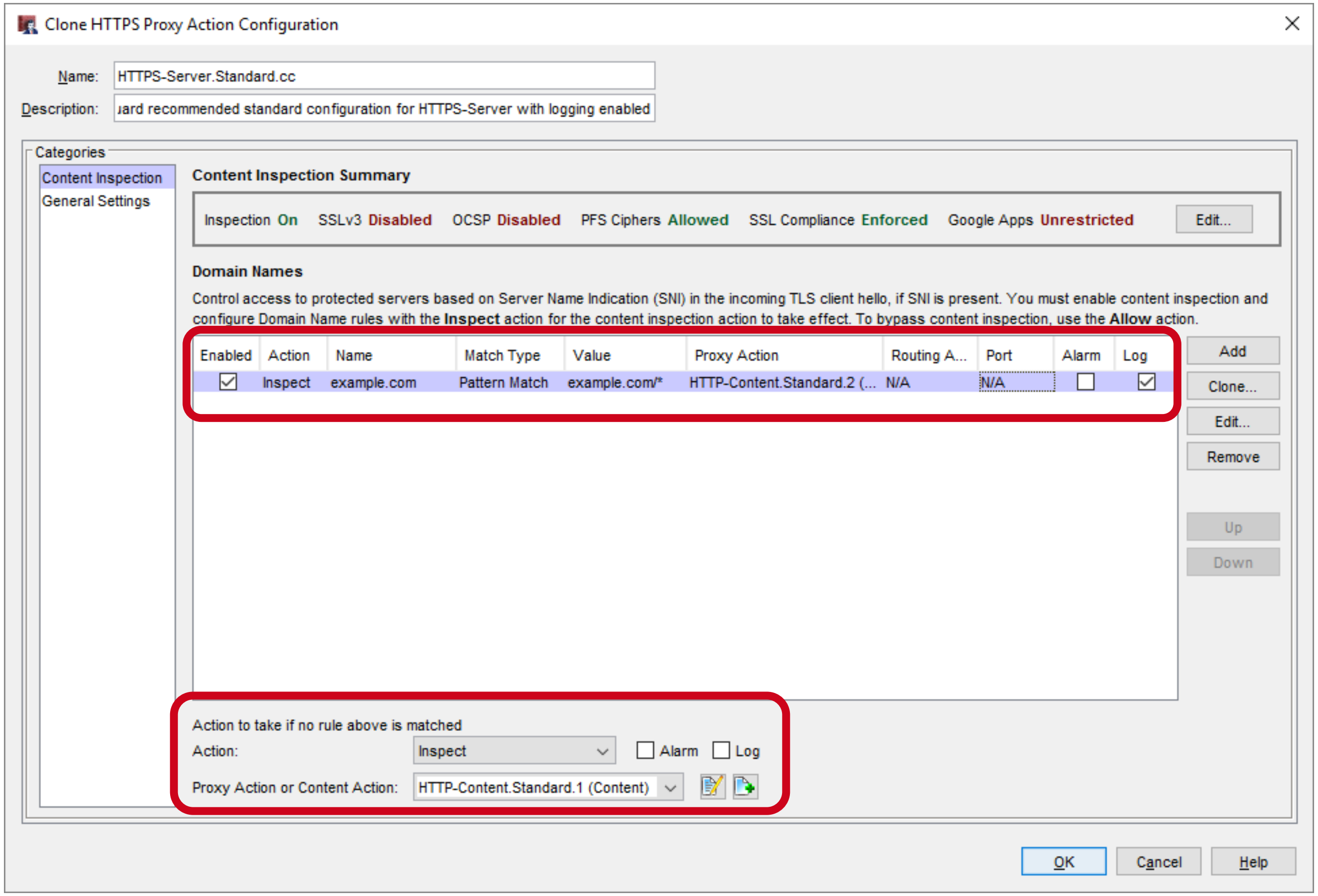
□ Enable bandwidth and time quotas (Fireware XTM OS v11.10 and higher)

Proxy action or Content action: HTTP-Content.Standard.1 (Content)

Content Action in an HTTPS Server Proxy

- To use a content action in a Domain Name rule or in the action to take if no rule is matched:
  1. Select the **Inspect** action
  2. Select a content action

Content Action in an HTTPS Server Proxy



Clone HTTPS Proxy Action Configuration

Name: HTTPS-Server.Standard.cc

Description: ɹard recommended standard configuration for HTTPS-Server with logging enabled

Categories

- Content Inspection
- General Settings

Content Inspection Summary

Inspection On SSLv3 Disabled OCSP Disabled PFS Ciphers Allowed SSL Compliance Enforced Google Apps Unrestricted

Domain Names

Control access to protected servers based on Server Name Indication (SNI) in the incoming TLS client hello, if SNI is present. You must enable content inspection and configure Domain Name rules with the **Inspect** action for the content inspection action to take effect. To bypass content inspection, use the **Allow** action.

Enabled	Action	Name	Match Type	Value	Proxy Action	Routing A...	Port	Alarm	Log
☑	Inspect	example.com	Pattern Match	example.com/*	HTTP-Content.Standard.2 (...	N/A	N/A	☐	☑

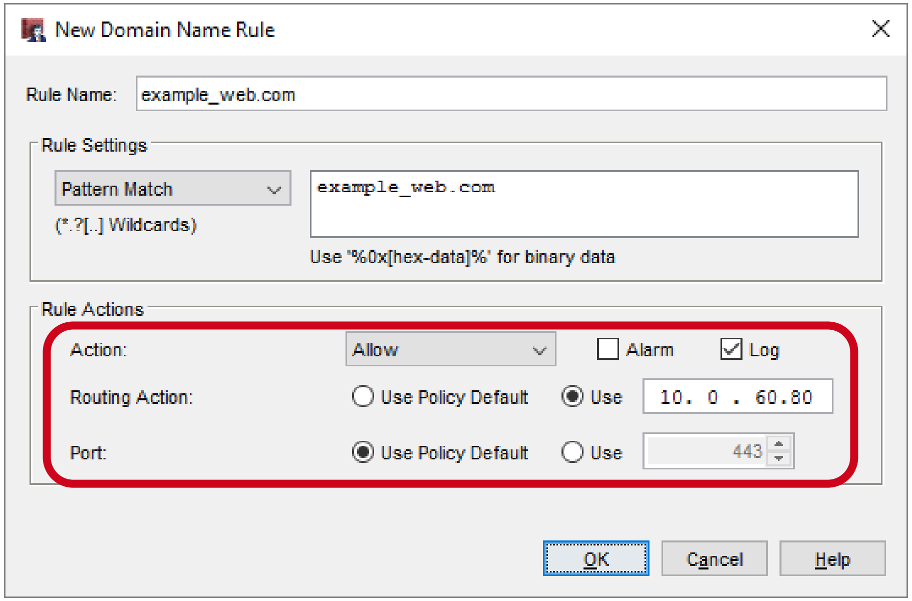
Action to take if no rule above is matched

Action: Inspect ☐ Alarm ☐ Log

Proxy Action or Content Action: HTTP-Content.Standard.1 (Content)

Routing Action in an HTTPS Server Proxy

- To route HTTPS requests without content inspection, in a Domain Name Rule or in the action to take if no rule is matched:
  1. Select the **Allow** action
  2. Configure a Routing Action and Port



New Domain Name Rule

Rule Name: example_web.com

Rule Settings

Pattern Match

(*.?[..] Wildcards)

example_web.com

Use '%0x[hex-data]%' for binary data

Rule Actions

Action: Allow □ Alarm ☑ Log

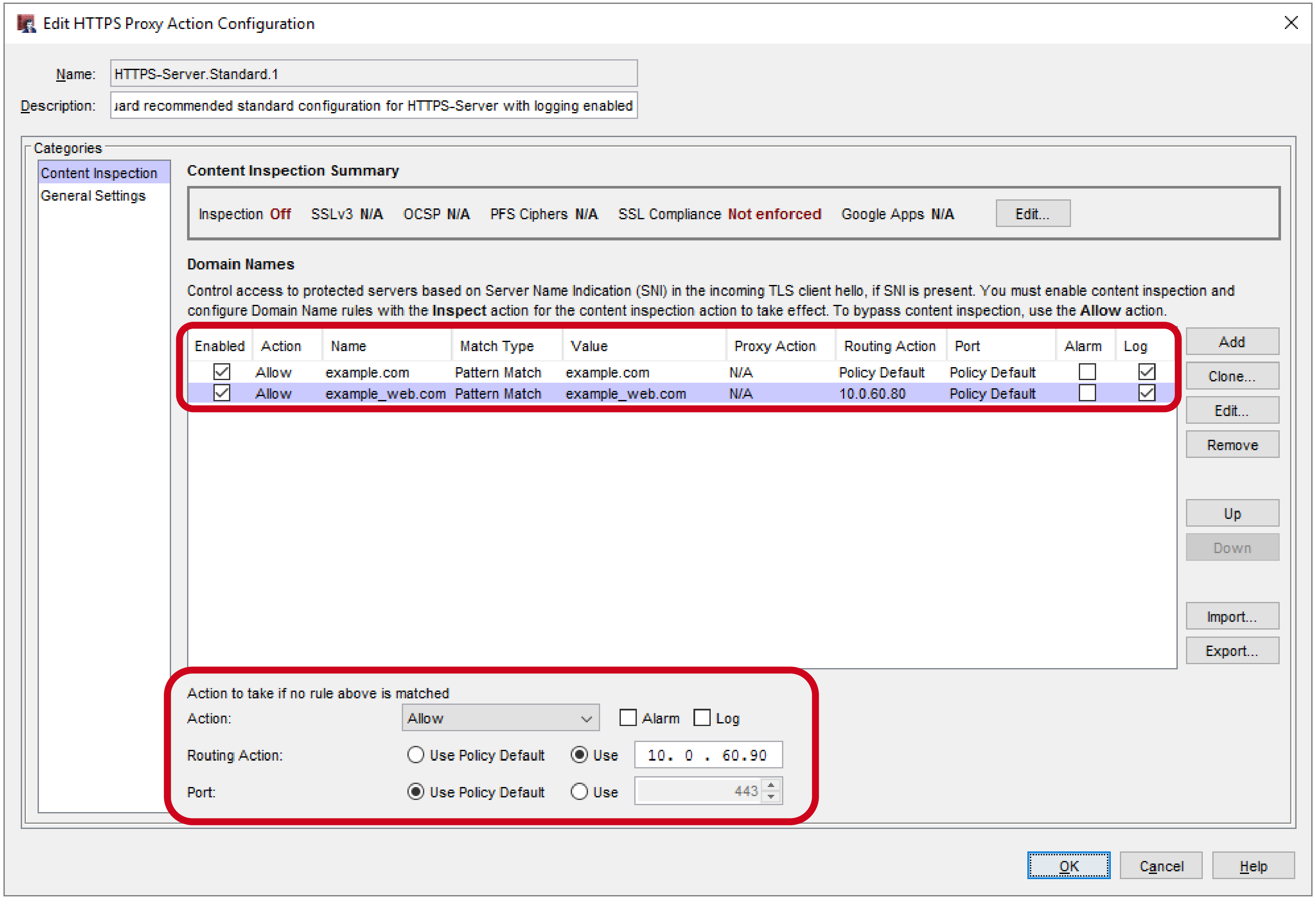
Routing Action: ○ Use Policy Default ● Use 10. 0 . 60.80

Port: ● Use Policy Default ○ Use 443

Routing Action in an HTTPS Server Proxy

- The routing action compares the domain name you specify in a domain name action with the domain name in the TLS Server Name Indication (SNI), or the Common Name of a server in the server certificate
  - For HTTPS requests, the SNI in the TLS handshake specifies the domain and path of the destination server
  - SNI is described in RFC 6066 TLS Extensions

Routing Action in an HTTPS Server Proxy



Edit HTTPS Proxy Action Configuration

Name: HTTPS-Server.Standard.1

Description: ıard recommended standard configuration for HTTPS-Server with logging enabled

Categories

- Content Inspection
- General Settings

Content Inspection Summary

Inspection Off SSLv3 N/A OCSP N/A PFS Ciphers N/A SSL Compliance Not enforced Google Apps N/A Edit...

Domain Names

Control access to protected servers based on Server Name Indication (SNI) in the incoming TLS client hello, if SNI is present. You must enable content inspection and configure Domain Name rules with the **Inspect** action for the content inspection action to take effect. To bypass content inspection, use the **Allow** action.

Enabled	Action	Name	Match Type	Value	Proxy Action	Routing Action	Port	Alarm	Log
☑	Allow	example.com	Pattern Match	example.com	N/A	Policy Default	Policy Default	□	☑
☑	Allow	example_web.com	Pattern Match	example_web.com	N/A	10.0.60.80	Policy Default	□	☑

Action to take if no rule above is matched

Action: Allow □ Alarm □ Log

Routing Action: ○ Use Policy Default ● Use 10. 0 . 60.90

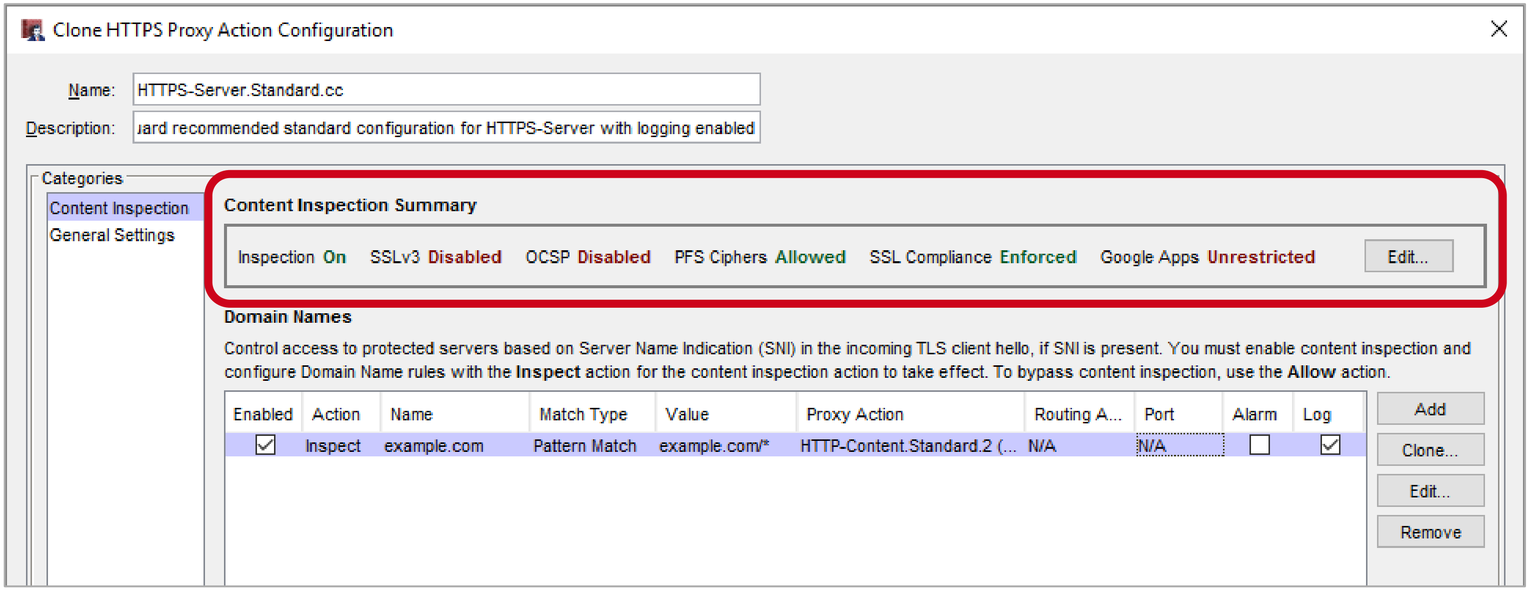
Port: ● Use Policy Default ○ Use 443

Proxy Action Changes

- Some proxy action settings were removed from the HTTP Server and HTTPS Server proxy actions because they are not applicable to inbound connections to a web server
  - HTTP Server proxy actions now do not include:
    - WebBlocker
    - Reputation Enabled Defense
  - HTTPS Server proxy actions now do not include:
    - WebBlocker
    - OCSP (Online Certificate Status Protocol)
      - No certificate validation in HTTPS proxy server actions

HTTPS Proxy Action Changes

- WebBlocker is removed from the **Categories** list
- Content Inspection and Domain Names settings are now combined in the **Content Inspection** category
- To change content inspection settings, in the **Content Inspection Summary** section, click **Edit**



Clone HTTPS Proxy Action Configuration

Name: HTTPS-Server.Standard.cc

Description: ıard recommended standard configuration for HTTPS-Server with logging enabled

Categories

- Content Inspection
- General Settings

Content Inspection Summary

Inspection On SSLv3 Disabled OCSP Disabled PFS Ciphers Allowed SSL Compliance Enforced Google Apps Unrestricted

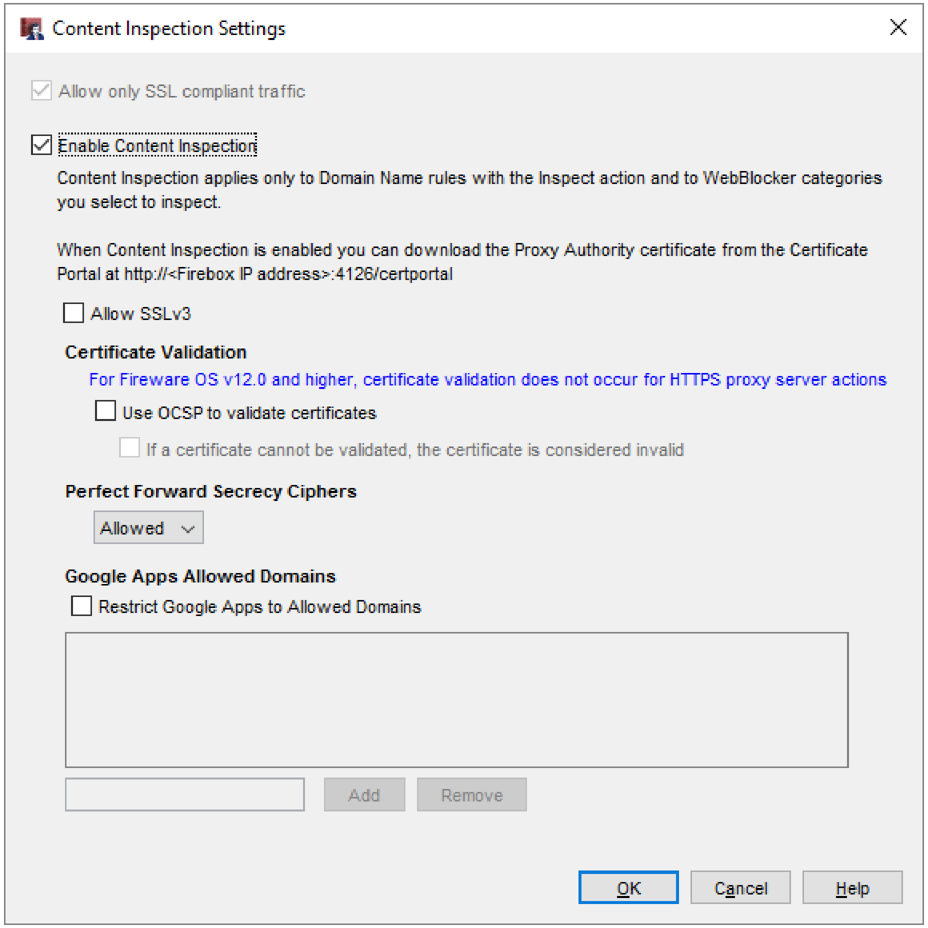
Domain Names

Control access to protected servers based on Server Name Indication (SNI) in the incoming TLS client hello, if SNI is present. You must enable content inspection and configure Domain Name rules with the **Inspect** action for the content inspection action to take effect. To bypass content inspection, use the **Allow** action.

Enabled	Action	Name	Match Type	Value	Proxy Action	Routing A...	Port	Alarm	Log
☑	Inspect	example.com	Pattern Match	example.com/*	HTTP-Content.Standard.2 (...	N/A	N/A	☐	☑

HTTPS Proxy Action Changes

- Content inspection settings are the same as in Fireware v11.x, except that you do not select an HTTP Client proxy action
- Now you specify an HTTP Client proxy action each time you select the **Inspect** action
  - You can use different HTTP proxy actions for each domain name rule and for WebBlocker



Content Inspection Settings

☑ Allow only SSL compliant traffic

☑ Enable Content Inspection

Content Inspection applies only to Domain Name rules with the Inspect action and to WebBlocker categories you select to inspect.

When Content Inspection is enabled you can download the Proxy Authority certificate from the Certificate Portal at http://<Firebox IP address>:4126/certportal

□ Allow SSLv3

Certificate Validation

For Fireware OS v12.0 and higher, certificate validation does not occur for HTTPS proxy server actions

□ Use OCSP to validate certificates

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

Perfect Forward Secrecy Ciphers

Allowed

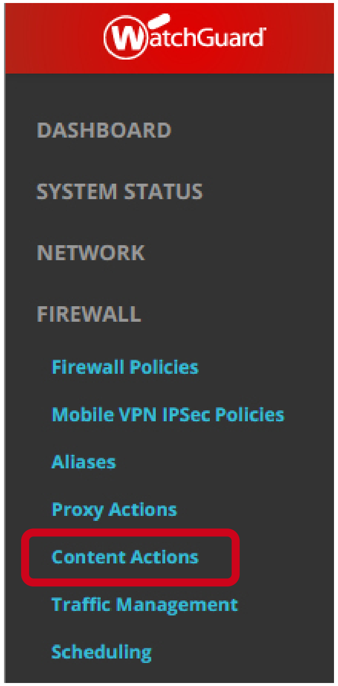
Google Apps Allowed Domains

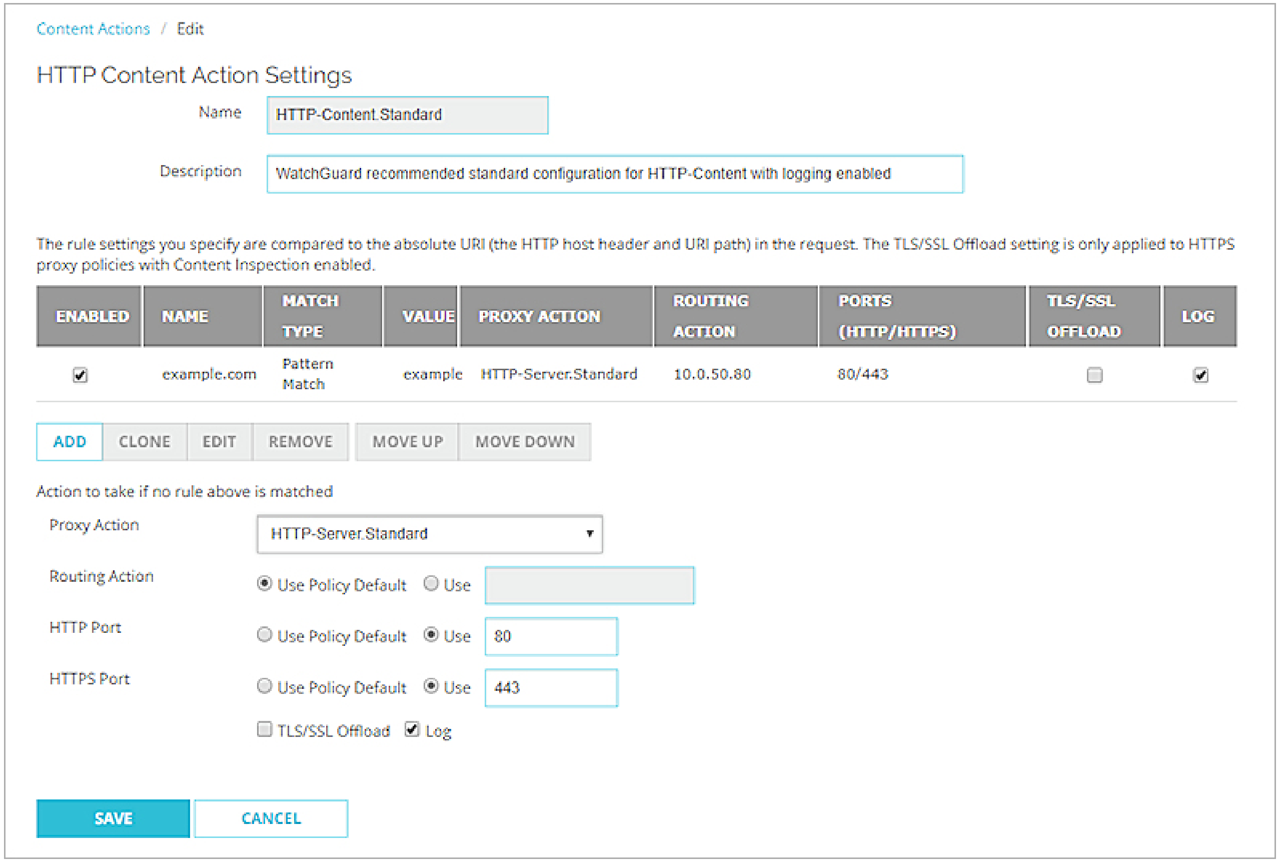
□ Restrict Google Apps to Allowed Domains

WatchGuard Training

Content Actions in Fireware Web UI

- To configure content actions in Fireware Web UI, select **Firewall > Content Actions**





HTTP Content Action Settings

Name: HTTP-Content.Standard

Description: WatchGuard recommended standard configuration for HTTP-Content with logging enabled

The rule settings you specify are compared to the absolute URI (the HTTP host header and URI path) in the request. The TLS/SSL Offload setting is only applied to HTTPS proxy policies with Content Inspection enabled.

ENABLED	NAME	MATCH TYPE	VALUE	PROXY ACTION	ROUTING ACTION	PORTS (HTTP/HTTPS)	TLS/SSL OFFLOAD	LOG
☑	example.com	Pattern Match	example	HTTP-Server.Standard	10.0.50.80	80/443	□	☑

Action to take if no rule above is matched

Proxy Action: HTTP-Server.Standard

Routing Action: ● Use Policy Default ○ Use

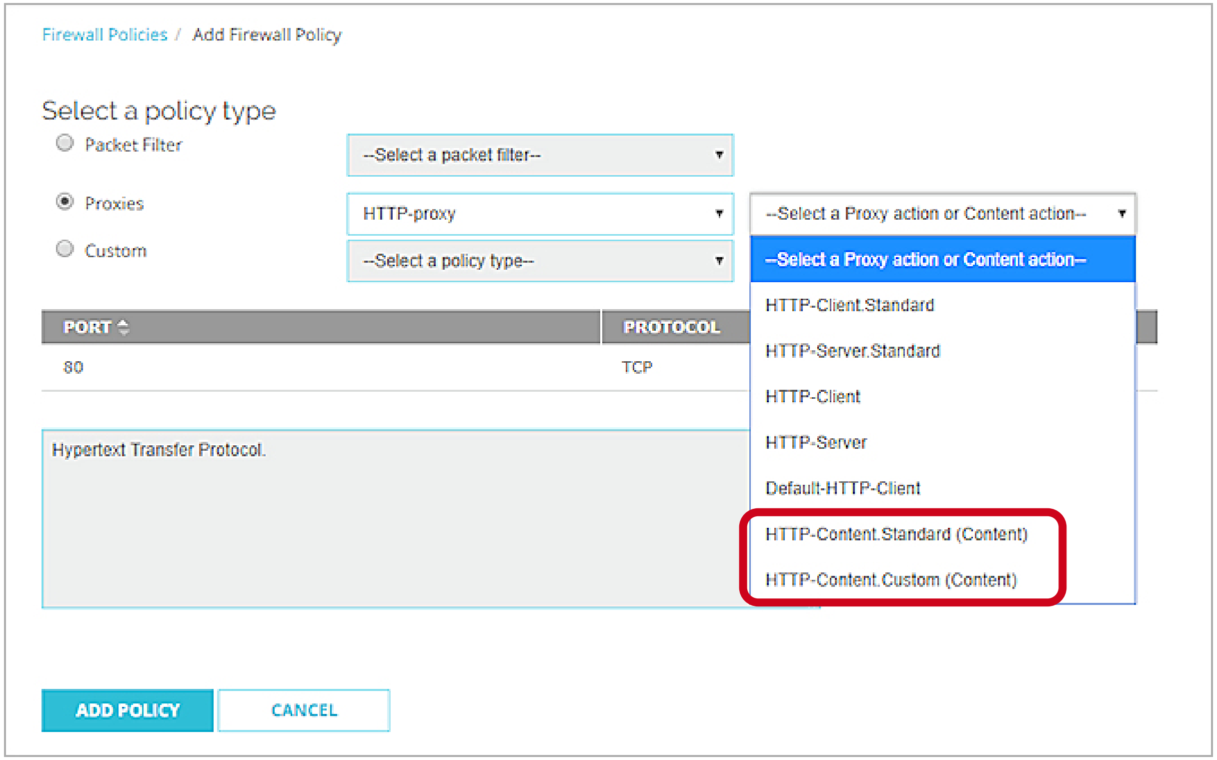
HTTP Port: ○ Use Policy Default ● Use 80

HTTPS Port: ○ Use Policy Default ● Use 443

□ TLS/SSL Offload ☑ Log

Content Actions in Fireware Web UI

- Select a content action when you add an HTTP-proxy policy



Firewall Policies / Add Firewall Policy

Select a policy type

○ Packet Filter — --Select a packet filter--

● Proxies — HTTP-proxy — --Select a Proxy action or Content action--

○ Custom — --Select a policy type--

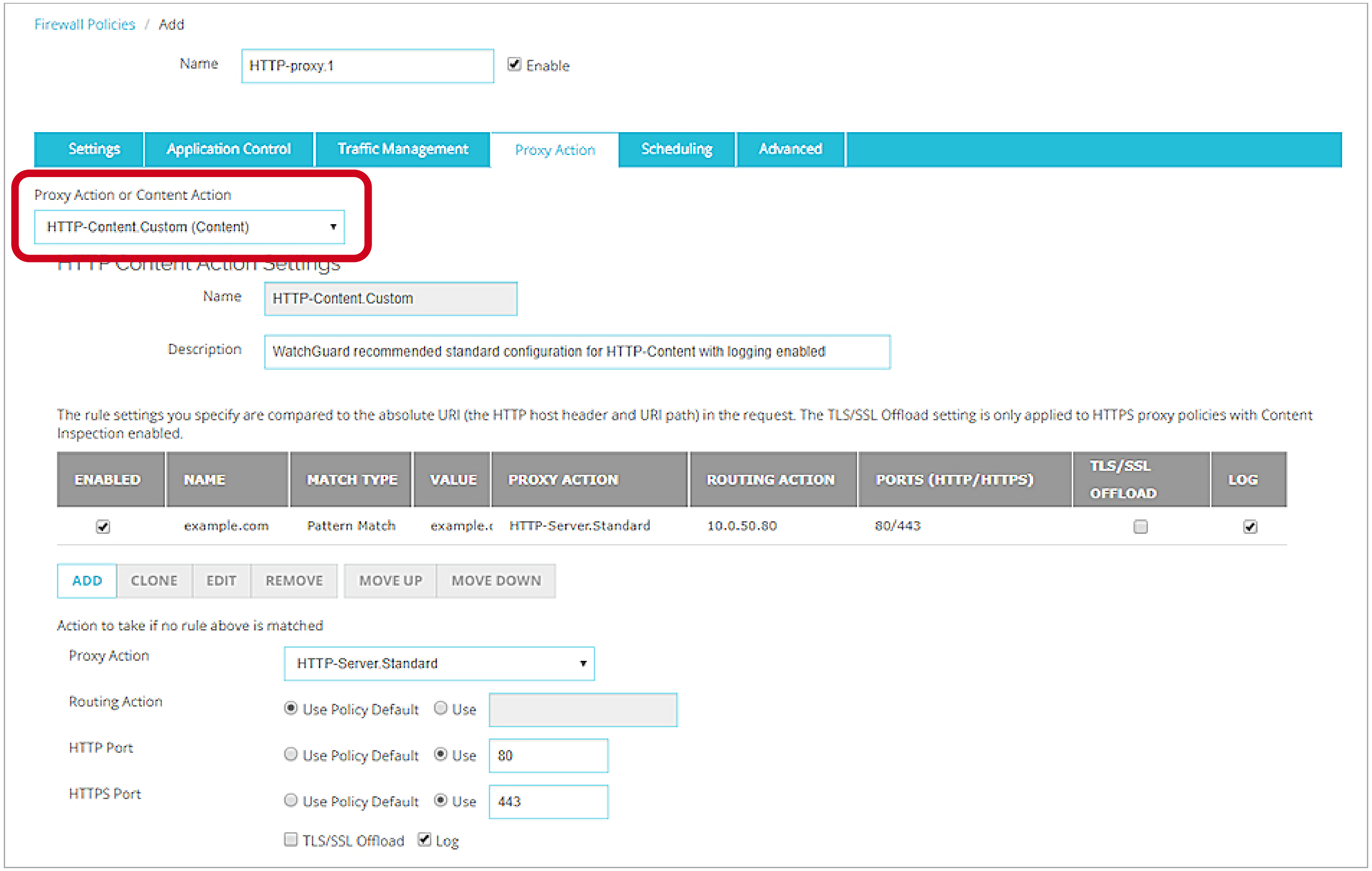
--Select a Proxy action or Content action--
HTTP-Client.Standard
HTTP-Server.Standard
HTTP-Client
HTTP-Server
Default-HTTP-Client
HTTP-Content.Standard (Content)
HTTP-Content.Custom (Content)

PORT	PROTOCOL
80	TCP

Hypertext Transfer Protocol.

Content Actions in Fireware Web UI

- The content action is on the HTTP-proxy **Proxy Action** tab



Firewall Policies / Add

Name: HTTP-proxy.1 ☑ Enable

Proxy Action or Content Action: HTTP-Content.Custom (Content) ▾

HTTP Content Action Settings

Name: HTTP-Content.Custom

Description: WatchGuard recommended standard configuration for HTTP-Content with logging enabled

The rule settings you specify are compared to the absolute URI (the HTTP host header and URI path) in the request. The TLS/SSL Offload setting is only applied to HTTPS proxy policies with Content Inspection enabled.

ENABLED	NAME	MATCH TYPE	VALUE	PROXY ACTION	ROUTING ACTION	PORTS (HTTP/HTTPS)	TLS/SSL OFFLOAD	LOG
☑	example.com	Pattern Match	example.(	HTTP-Server.Standard	10.0.50.80	80/443	□	☑

Action to take if no rule above is matched

Proxy Action: HTTP-Server.Standard ▾

Routing Action: ● Use Policy Default ○ Use

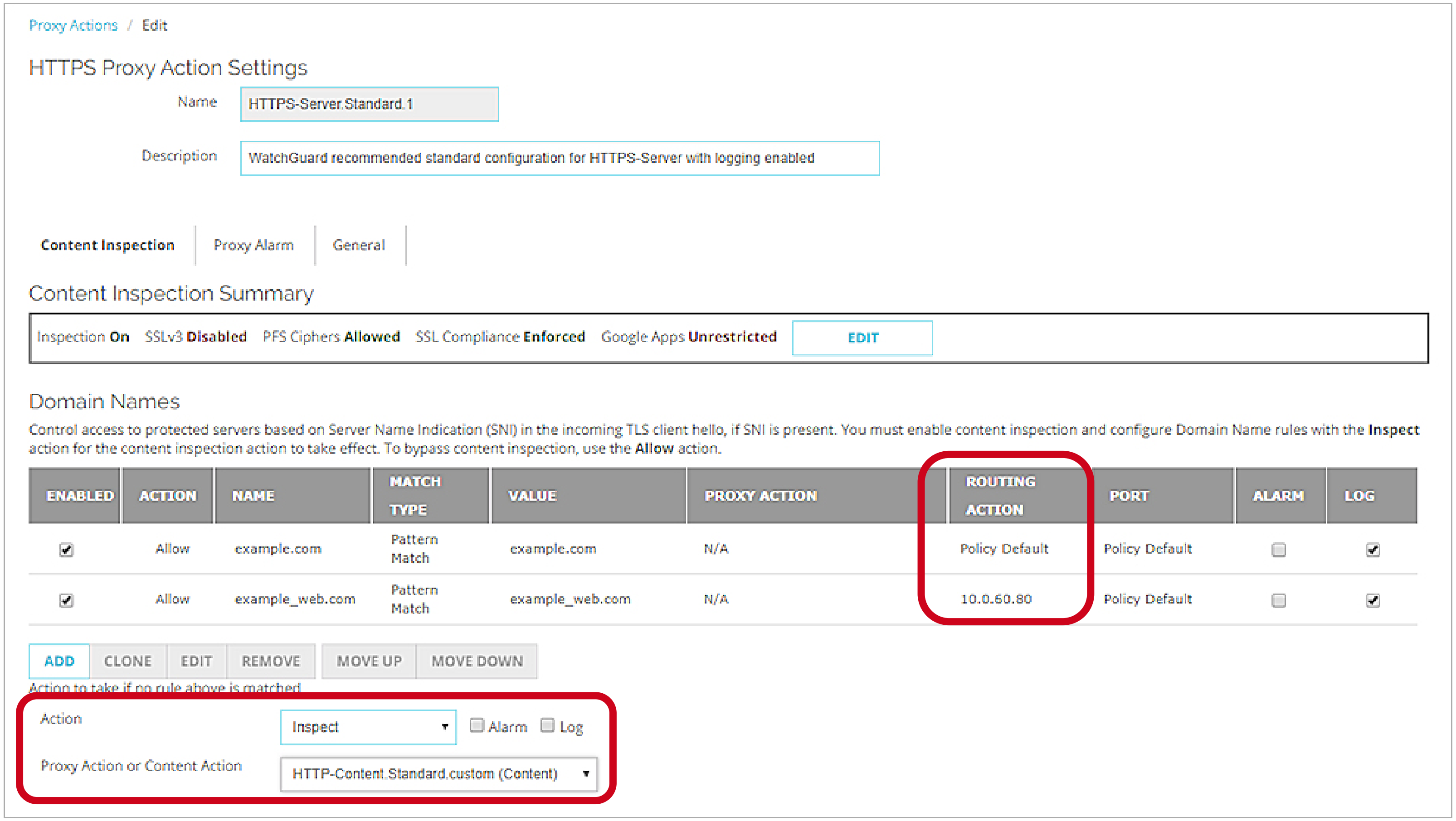
HTTP Port: ○ Use Policy Default ● Use 80

HTTPS Port: ○ Use Policy Default ● Use 443

□ TLS/SSL Offload ☑ Log

Content Actions in Fireware Web UI

- HTTPS proxy action with routing actions and a content action



Proxy Actions / Edit

HTTPS Proxy Action Settings

Name: HTTPS-Server.Standard.1

Description: WatchGuard recommended standard configuration for HTTPS-Server with logging enabled

Content Inspection Summary

Inspection **On** SSLv3 **Disabled** PFS Ciphers **Allowed** SSL Compliance **Enforced** Google Apps **Unrestricted**

Domain Names

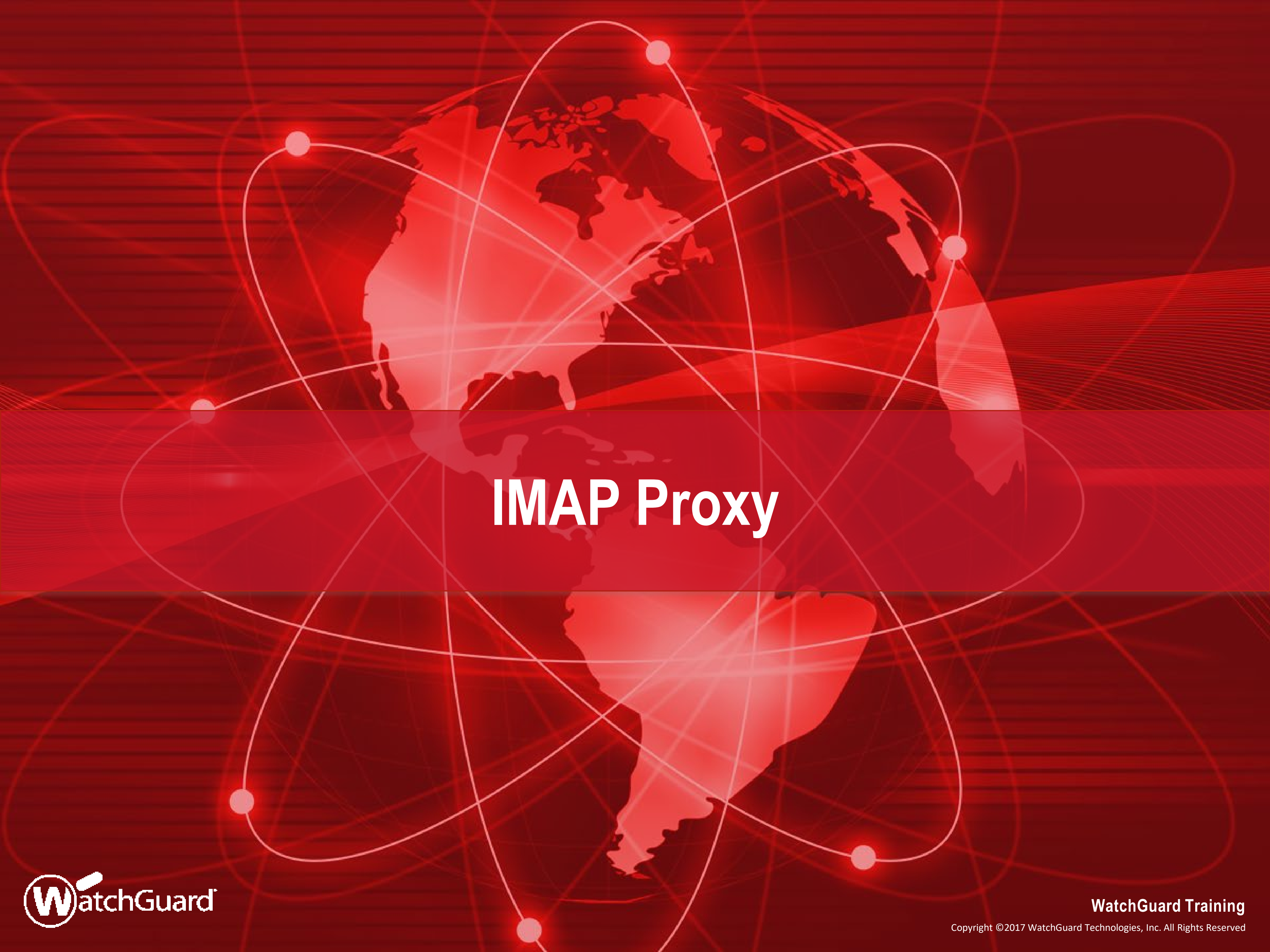
Control access to protected servers based on Server Name Indication (SNI) in the incoming TLS client hello, if SNI is present. You must enable content inspection and configure Domain Name rules with the **Inspect** action for the content inspection action to take effect. To bypass content inspection, use the **Allow** action.

ENABLED	ACTION	NAME	MATCH TYPE	VALUE	PROXY ACTION	ROUTING ACTION	PORT	ALARM	LOG
☑	Allow	example.com	Pattern Match	example.com	N/A	Policy Default	Policy Default	□	☑
☑	Allow	example_web.com	Pattern Match	example_web.com	N/A	10.0.60.80	Policy Default	□	☑

Action to take if no rule above is matched

Action: Inspect ▾ □ Alarm □ Log

Proxy Action or Content Action: HTTP-Content.Standard.custom (Content) ▾



IMAP Proxy

WatchGuard Training

IMAP Protocol

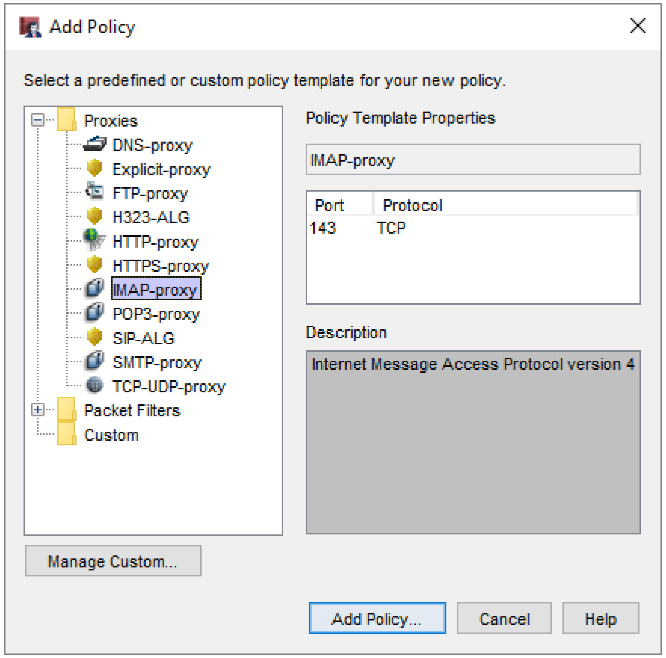
- Fireware now includes an IMAP proxy policy
- The IMAP proxy policy supports IMAP v4 on TCP port 143
- The IMAP proxy does **not** support IMAP over SSL/TLS

IMAP Proxy Policy

- The IMAP proxy settings are similar to the POP3 proxy
- IMAP supports more complex actions than POP3
  - IMAP clients synchronize changes to the IMAP server
  - IMAP clients can request many types of information: headers, envelope information, message text, and more
  - Multiple IMAP clients can connect to the same IMAP server
    - All clients must stay in sync with the server
- The IMAP proxy applies only to clients that connect to the IMAP server through the IMAP proxy

IMAP Proxy Policy

- To add an IMAP proxy policy, select the **IMAP-proxy** policy template



Add Policy

Select a predefined or custom policy template for your new policy.

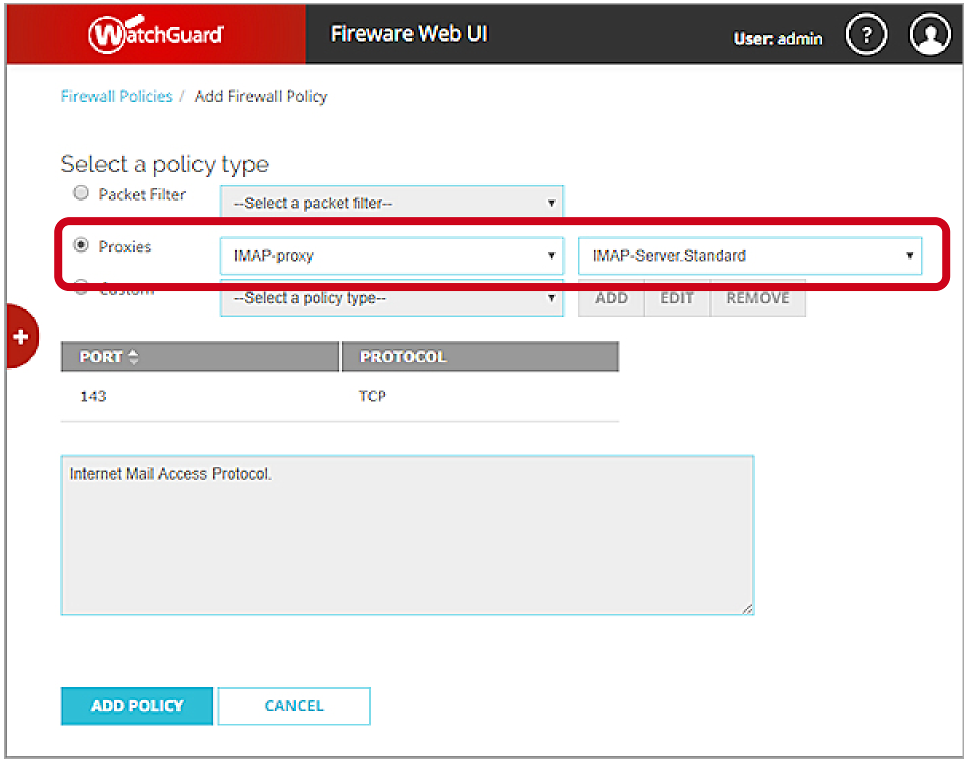
Policy Template Properties

IMAP-proxy

Port	Protocol
143	TCP

Description

Internet Message Access Protocol version 4



Select a policy type

○ Packet Filter --Select a packet filter--

● Proxies IMAP-proxy IMAP-Server.Standard

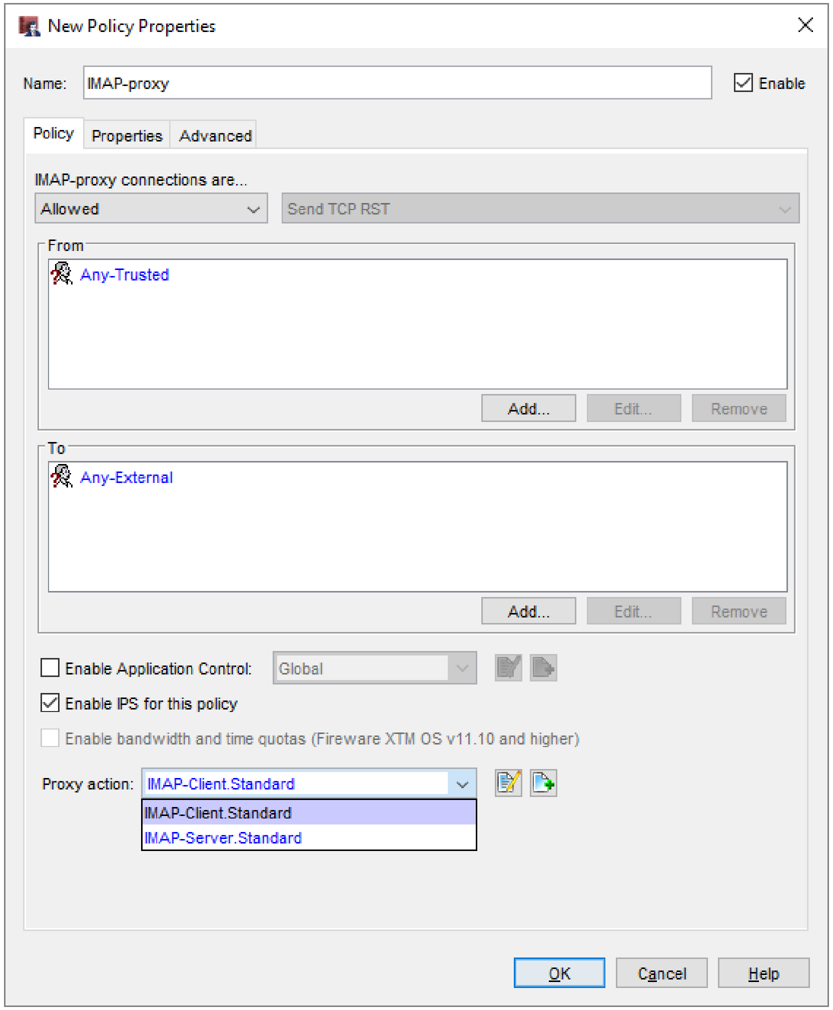
○ Custom --Select a policy type--

PORT	PROTOCOL
143	TCP

Internet Mail Access Protocol.

IMAP Proxy

- There are two new predefined proxy actions:
  - **IMAP-Client.Standard** for outbound IMAP client connections
  - **IMAP-Server.Standard** for inbound connections to an IMAP server



New Policy Properties

Name: IMAP-proxy ☑ Enable

Policy | Properties | Advanced

IMAP-proxy connections are... Allowed | Send TCP RST

From: Any-Trusted

To: Any-External

□ Enable Application Control: Global

☑ Enable IPS for this policy

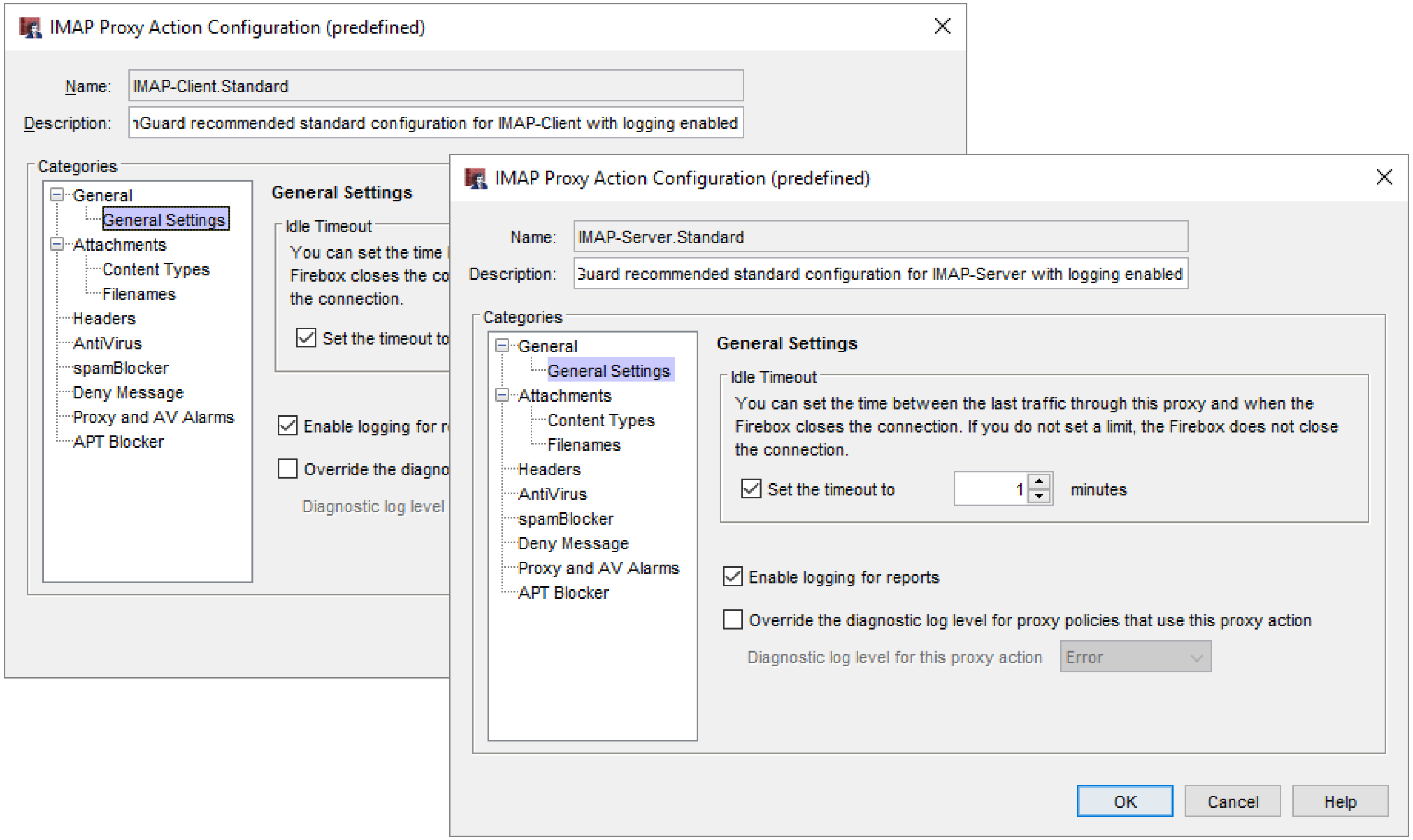
□ Enable bandwidth and time quotas (Fireware XTM OS v11.10 and higher)

Proxy action: IMAP-Client.Standard

- IMAP-Client.Standard
- IMAP-Server.Standard

IMAP Proxy Action Settings

- Settings in IMAP proxy actions are similar to the settings in POP3 proxy actions



IMAP Proxy Action Configuration (predefined)

Name: IMAP-Client.Standard

Description: ıGuard recommended standard configuration for IMAP-Client with logging enabled

Categories

General Settings

Idle Timeout

You can set the time l
Firebox closes the co
the connection.

☑ Set the timeout to

☑ Enable logging for r

☐ Override the diagno

Diagnostic log level

IMAP Proxy Action Configuration (predefined)

Name: IMAP-Server.Standard

Description: Guard recommended standard configuration for IMAP-Server with logging enabled

Categories

General Settings

Idle Timeout

You can set the time between the last traffic through this proxy and when the Firebox closes the connection. If you do not set a limit, the Firebox does not close the connection.

☑ Set the timeout to 1 minutes

☑ Enable logging for reports

☐ Override the diagnostic log level for proxy policies that use this proxy action

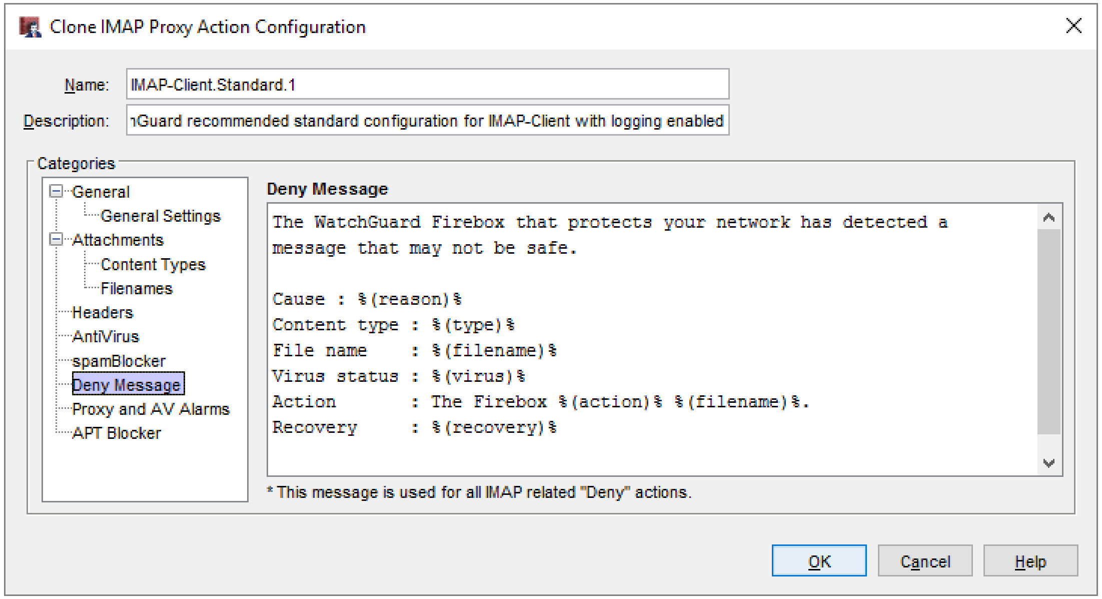
Diagnostic log level for this proxy action: Error

IMAP Proxy — Subscription Services

- The IMAP proxy supports these Subscription Services:
  - Application Control
  - Intrusion Prevention Service (IPS)
  - Gateway AntiVirus
  - spamBlocker
  - APT Blocker

IMAP Proxy — Deny Message

- If the IMAP proxy locks or removes an attachment, it adds a text file with the Deny Message as a message attachment
  - The text file attachment file name starts with: `wgrd_deny_msg`
  - The Deny Message text file includes the content you configure in the IMAP proxy action



Name: IMAP-Client.Standard.1

Description: ıGuard recommended standard configuration for IMAP-Client with logging enabled

Deny Message

```
The WatchGuard Firebox that protects your network has detected a
message that may not be safe.

Cause : %(reason)%
Content type : %(type)%
File name    : %(filename)%
Virus status : %(virus)%
Action       : The Firebox %(action)% %(filename)%.
Recovery     : %(recovery)%
```

* This message is used for all IMAP related "Deny" actions.

IMAP Proxy — Message Scan Cache

- There can be a brief delay while a message is scanned
- To avoid rescanning, the IMAP proxy stores a local cache of email message actions and scan results
- The cached information includes:
  - Message UID and Envelop hash value (to identify the message)
  - spamBlocker score result and action
  - Virus Outbreak Detection and action
  - Final action for the message and the reason:
    - Filename, Content Type, and Header filtering
    - Gateway AV and APT Blocker scans

IMAP Proxy — Local Message Scan Cache

- If a requested message is in the cache, the IMAP proxy uses the prior message handling/scanning result
- If a requested message is not in the cache, the IMAP proxy:
  - Gets the full email message for scanning
  - Stores the handling/scanning results to the cache
- The cache size varies by Firebox model and is not configurable

New OS Compatibility Setting

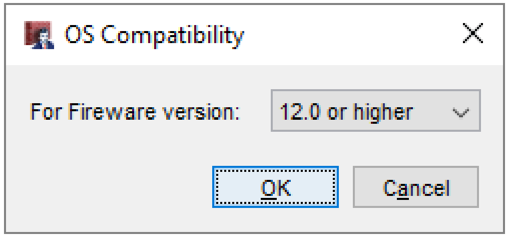
WatchGuard Training

Fireware OS Compatiblity Setting

- You can use Policy Manager to configure Fireboxes that use different versions of Fireware
  - Some Fireware features are supported only in specific Fireware versions or have different settings in different Fireware versions
  - If you use Policy Manager to create a new Firebox configuration, you must select the OS Compatibility setting to one of these options:
    - 11.4 - 11.8.x
    - 11.9 - 11.12.x
    - 12.0 or higher *(new)*
  - If you open a configuration from a Firebox, the OS Compatibility is automatically set, based on the installed version of Fireware

New OS Compatibility Setting

- To configure the OS Compatibility setting, in Policy Manager, select **Setup > OS Compatibility**
- To configure features that require Fireware v12.0, the OS Compatibility must be set to **12.0 or higher**
- The Fireware version is automatically set to v12.0 or higher when you open a configuration from a Firebox that runs Fireware v12.0


OS Compatibility

For Fireware version: 12.0 or higher

Gateway Wireless Controller Enhancements

WatchGuard Training

AP Firmware Updates

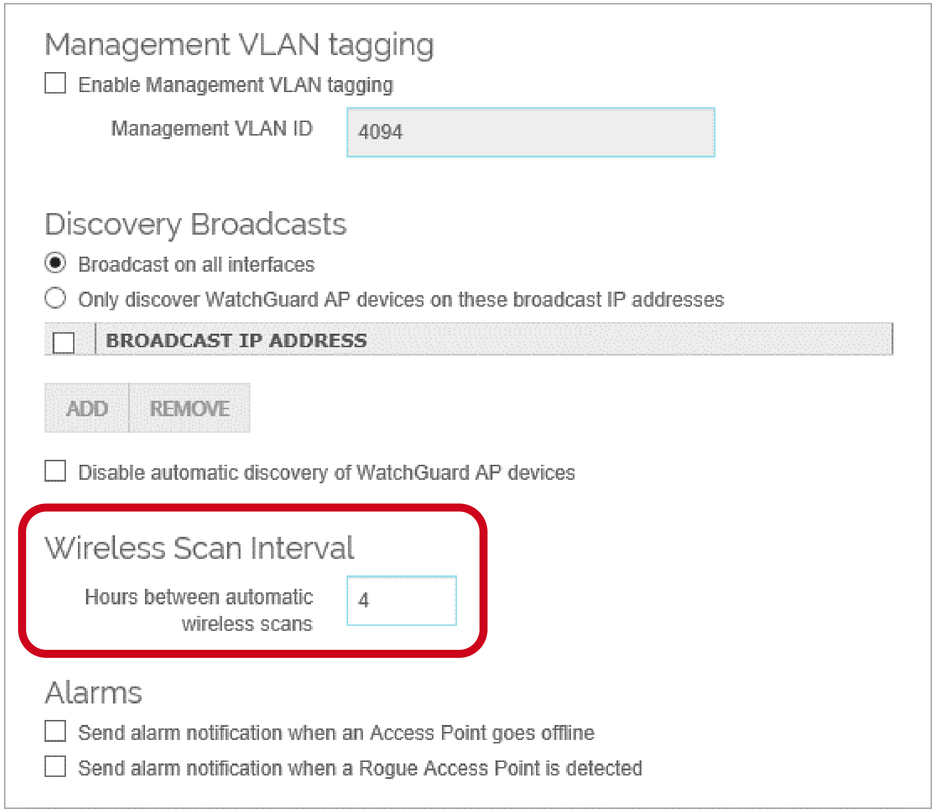
- Updated AP firmware includes stability and security enhancements
  - AP100, AP102, AP200 — 1.2.9.13
  - AP300 — 2.0.0.8
  - AP120, AP320, AP322, AP420 — 8.3.0
    - Version 8.3.0 firmware for AP120, AP320, AP322, and AP420 is only supported for Fireboxes that run Fireware v11.12.4 or higher

Improved Discovery and Pairing Times

- Much faster initial discovery and pairing times for AP120, AP320, AP322, and AP420 devices with v8.3.0 firmware
- It now only takes a few minutes for new AP devices to be discovered and paired to the Gateway Wireless Controller

Increased Wireless Maps Scan Interval

- The default **Wireless Scan Interval** in the Gateway Wireless Controller settings is now set to every 4 hours instead of 1 hour, which reduces resource usage
- The wireless scan interval is used for AP channel selection, wireless deployment maps, and rogue access point detection



Management VLAN tagging

□ Enable Management VLAN tagging

Management VLAN ID 4094

Discovery Broadcasts

● Broadcast on all interfaces

○ Only discover WatchGuard AP devices on these broadcast IP addresses

□	BROADCAST IP ADDRESS

□ Disable automatic discovery of WatchGuard AP devices

Wireless Scan Interval

Hours between automatic wireless scans 4

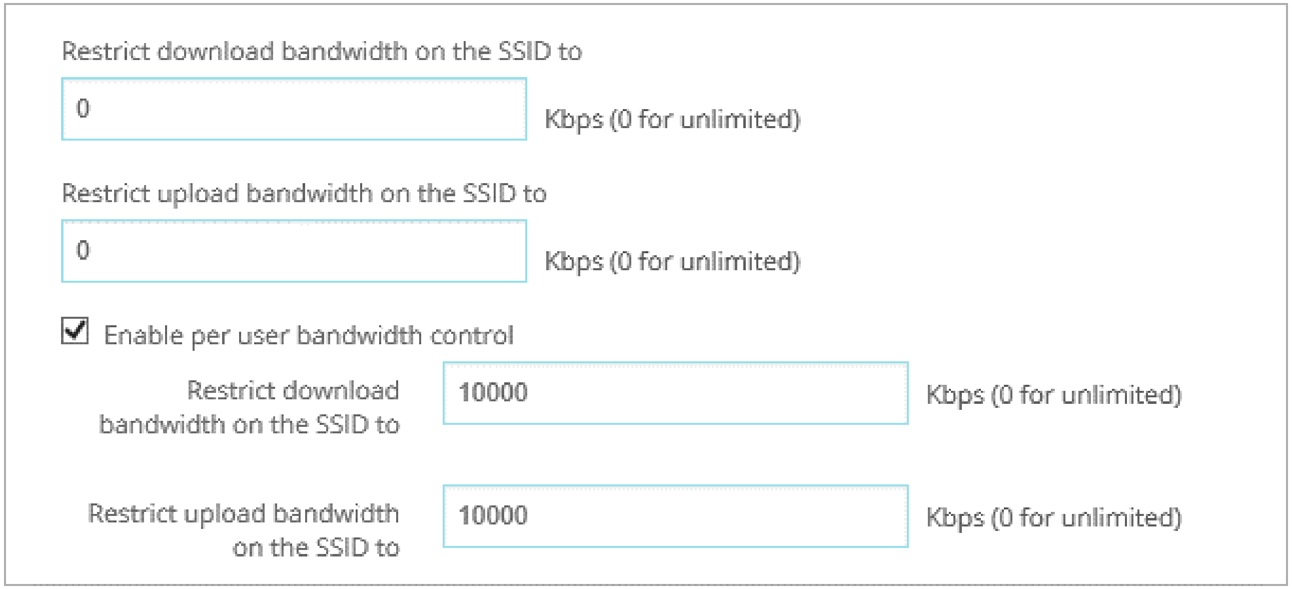
Alarms

□ Send alarm notification when an Access Point goes offline

□ Send alarm notification when a Rogue Access Point is detected

Rate Shaping Enhancements

- You can now configure separate upload and download rate limits for each SSID and for each user in an SSID configuration
  - AP100, AP102, AP200, and AP300 devices only support the download rate limits



Restrict download bandwidth on the SSID to

0 Kbps (0 for unlimited)

Restrict upload bandwidth on the SSID to

0 Kbps (0 for unlimited)

☑ Enable per user bandwidth control

Restrict download bandwidth on the SSID to 10000 Kbps (0 for unlimited)

Restrict upload bandwidth on the SSID to 10000 Kbps (0 for unlimited)

Deprecated Wireless Options

- **Restart Wireless**
  - You can now only complete a reboot action for an AP device
  - When you reboot an AP device manually or as a scheduled restart, the configuration is reloaded and auto-channel selection occurs
- **Outdoor only channels** — Outdoor models AP102 and AP322 will continue to enforce channel restrictions according to outdoor-only channel availability
- **Disable DFS channels** — You can no longer disable the use of DFS channels on any AP device model
- **Rate option** — The Rate control option for a radio is removed; the default setting is now **Auto**

Wireless Option Terminology Updates

- Improved parity between Wi-Fi Cloud and local Gateway Wireless Controller (GWC) feature terminology

	Previous Name	New Name
AP device and GWC Settings	Management VLAN	Communication VLAN
Radio Settings	Channel HT Mode	Channel Width
	TX Power	Transmit Power
	Country	Country of Operation
	Band	Frequency Band
SSID Settings	Broadcast SSID and respond to SSID queries	Broadcast SSID
	Station Isolation	Client Isolation
Monitoring	Foreign BSSIDs	External BSSIDs

Mobile VPN with PPTP Removed

WatchGuard Training

Mobile VPN with PPTP Removed

- In Fireware v12.0, Mobile VPN with PPTP is no longer available
  - PPTP is an older VPN protocol that is not considered secure
- If your configuration includes Mobile VPN with PPTP, we recommend that you use a different Mobile VPN solution before you upgrade
  - To compare mobile VPN solutions, see Select the Type of Mobile VPN to Use in *Fireware Help*
  - For minimal changes to your Firebox and mobile clients, we recommend that you select the Mobile VPN with L2TP solution
  - For more information, see How do I migrate from PPTP to L2TP? in the WatchGuard Knowledge Base

Mobile VPN with PPTP Removed

- After you upgrade to Fireware v12.0:
  - If the built-in *PPTP-Users* group includes users, or if an alias or policy includes the *PPTP-Users* group, this group is renamed to *PPTP-Users-Legacy*
  - You can view and delete the *PPTP-Users-Legacy* group
  - You cannot view the Mobile VPN with PPTP configuration in the WebUI, Policy Manager, or the CLI

Updated Default VPN Security Settings

Updated Default VPN Security Settings

- New VPN connections created in Fireware v12.0 have stronger default authentication and encryption settings
- The new default settings apply to all VPN products:
  - Manual BOVPN
  - BOVPN virtual interfaces
  - Mobile VPN with IPSec
  - Mobile VPN with SSL
  - Mobile VPN with L2TP

Updated Default VPN Security Settings

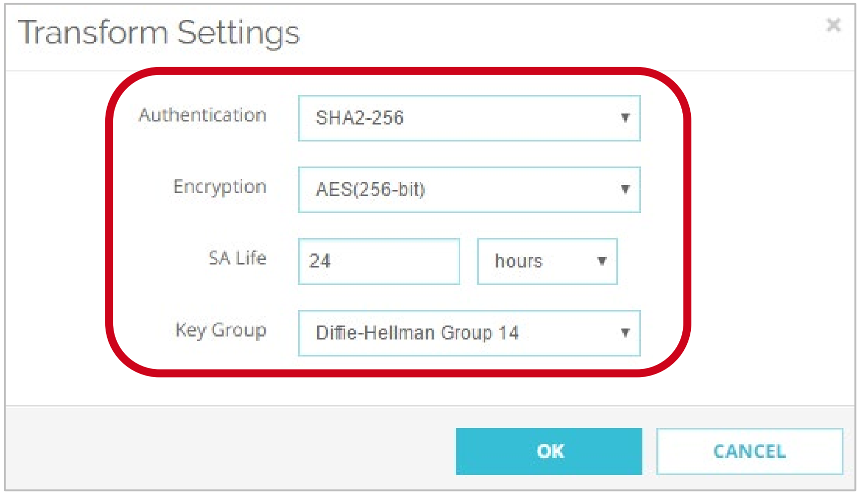
- If you use Policy Manager v12.0 to open an XML configuration file for Fireware v11.12.4 or lower, the new default settings for BOVPN, BOVPN virtual interfaces, Mobile VPN with IPSec, and Mobile VPN with L2TP do not appear for new VPN connections
  - To convert the configuration file to v12.0, select **Setup** > **OS Compatibility**
  - After the file is converted, the default settings appear for new VPN connections

Updated Default VPN Security Settings

- For BOVPN, BOVPN virtual interfaces, and Mobile VPN with IPSec, the new Phase 1 and 2 defaults are:
  - Authentication — **SHA-2 (256)**
  - Encryption — **AES (256)**
  - Diffie-Hellman Group — **14**
  - Perfect Forward Secrecy (PFS) — **Enabled**
- For BOVPN and BOVPN virtual interfaces, the new SA Life value is **24 hours**
- The Traffic option for Force Key Expiration is now disabled for Mobile VPN with IPSec

Updated Default VPN Security Settings

- Phase 1 settings for BOVPN and BOVPN virtual interfaces



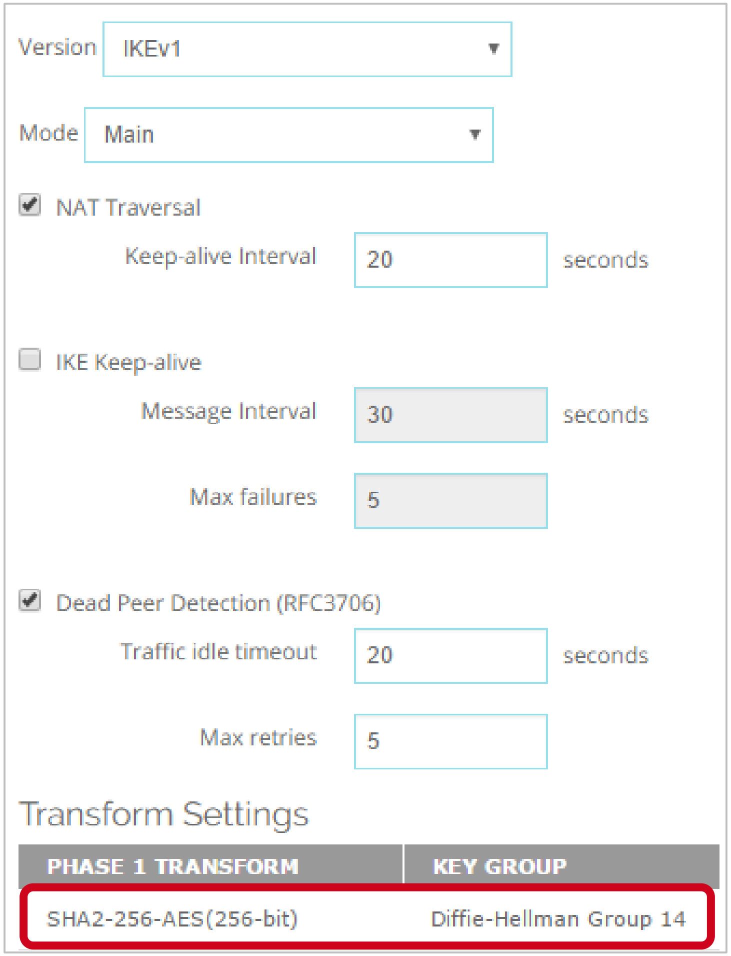
Transform Settings

Authentication: SHA2-256

Encryption: AES(256-bit)

SA Life: 24 hours

Key Group: Diffie-Hellman Group 14



Version: IKEv1

Mode: Main

☑ NAT Traversal

Keep-alive Interval: 20 seconds

□ IKE Keep-alive

Message Interval: 30 seconds

Max failures: 5

☑ Dead Peer Detection (RFC3706)

Traffic idle timeout: 20 seconds

Max retries: 5

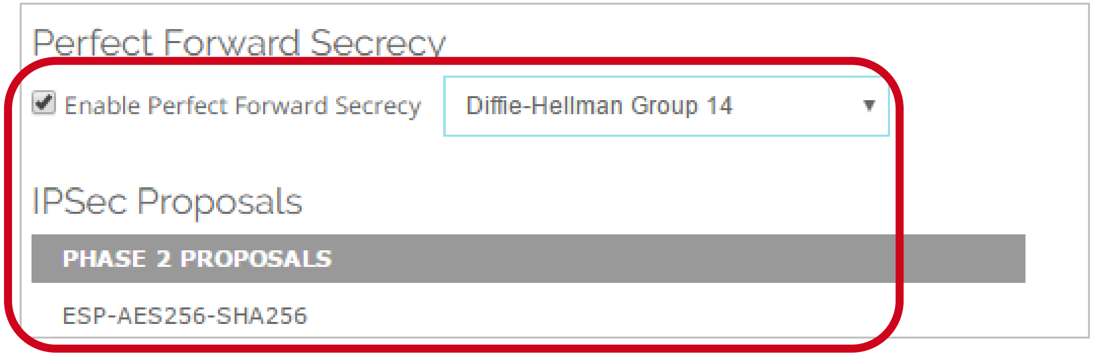
Transform Settings

PHASE 1 TRANSFORM	KEY GROUP
SHA2-256-AES(256-bit)	Diffie-Hellman Group 14

WatchGuard Training

Updated Default VPN Security Settings

- Phase 2 settings for BOVPN and BOVPN virtual interfaces



Perfect Forward Secrecy

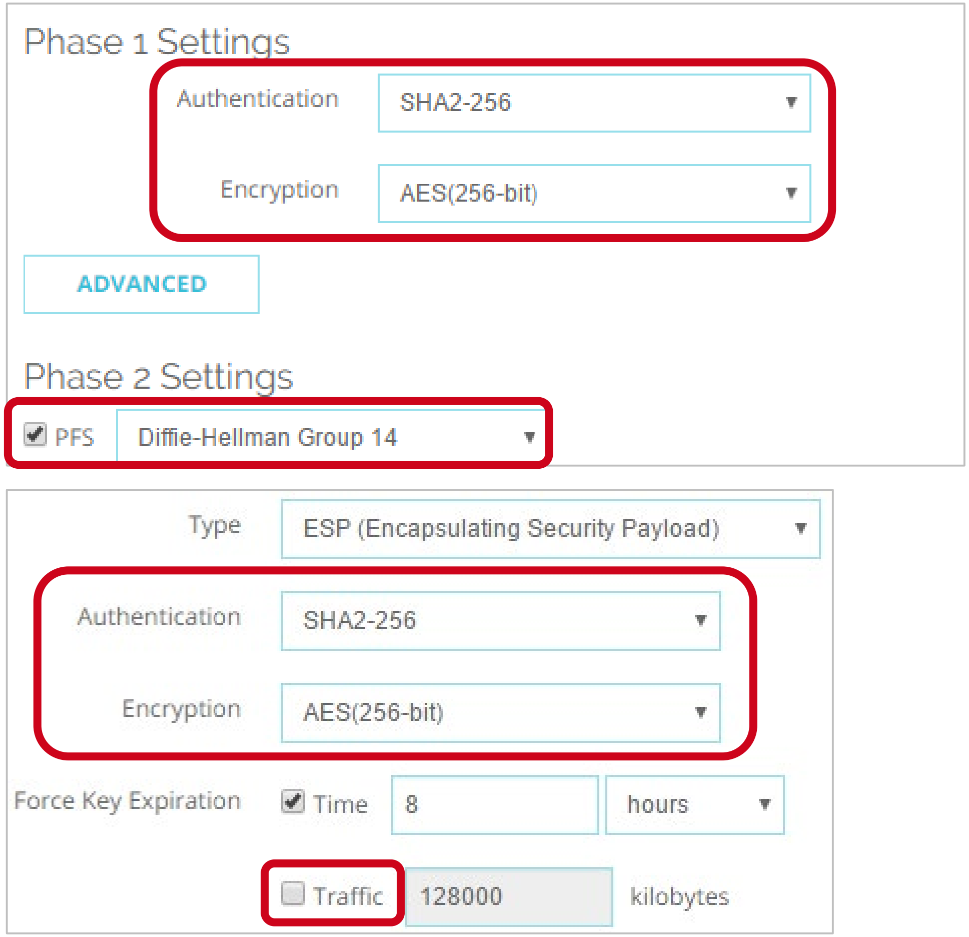
☑ Enable Perfect Forward Secrecy: Diffie-Hellman Group 14

IPSec Proposals

PHASE 2 PROPOSALS
ESP-AES256-SHA256

Updated Default VPN Security Settings

- Phase 1 and 2 settings for Mobile VPN with IPSec



Phase 1 Settings

Authentication: SHA2-256

Encryption: AES(256-bit)

Phase 2 Settings

☑ PFS: Diffie-Hellman Group 14

Type: ESP (Encapsulating Security Payload)

Authentication: SHA2-256

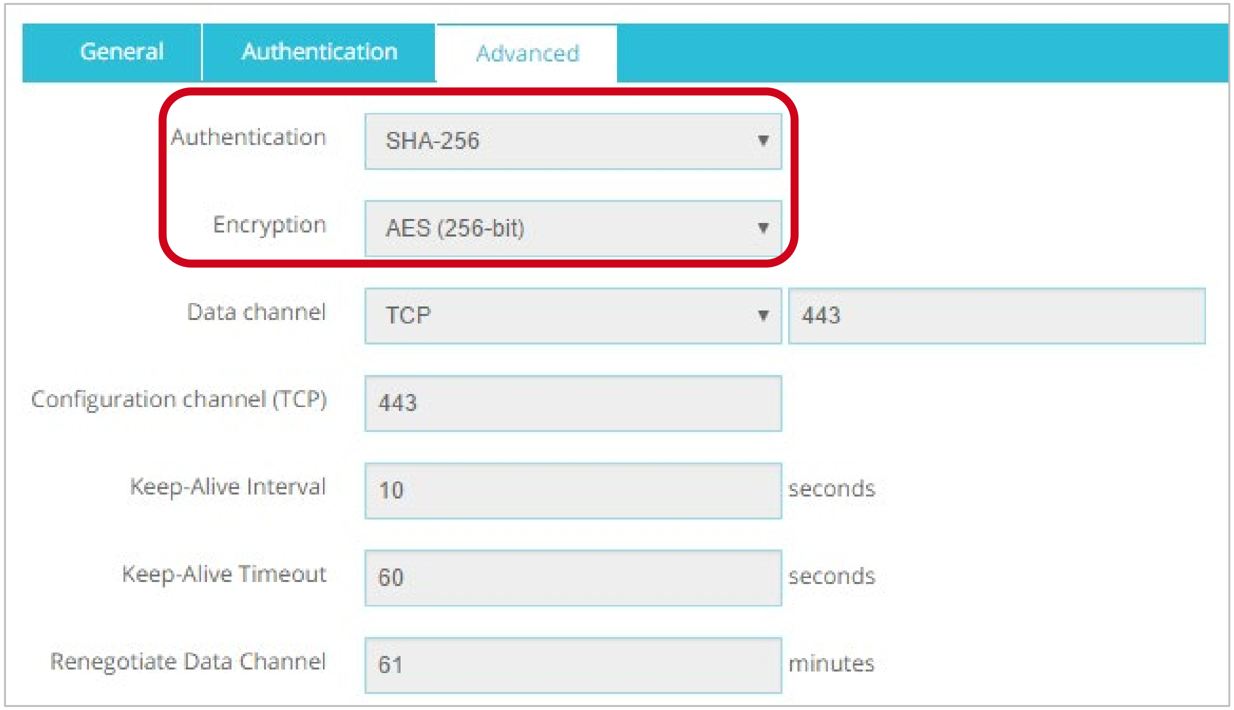
Encryption: AES(256-bit)

Force Key Expiration: ☑ Time 8 hours

□ Traffic 128000 kilobytes

Updated Default VPN Security Settings

- For Mobile VPN with SSL, the new defaults are:
  - Authentication — **SHA-2 (256)**
  - Encryption — **AES (256)**



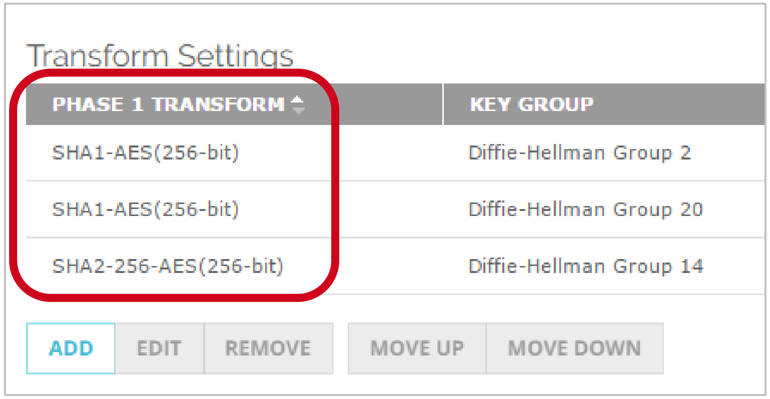
Authentication	SHA-256 ▾	
Encryption	AES (256-bit) ▾	
Data channel	TCP ▾	443
Configuration channel (TCP)	443	
Keep-Alive Interval	10	seconds
Keep-Alive Timeout	60	seconds
Renegotiate Data Channel	61	minutes

Updated Default VPN Security Settings

- For Mobile VPN with L2TP, the new Phase 1 defaults are:
  - SHA2(256)–AES(256) and Diffie-Hellman 14
  - SHA1–AES(256) and Diffie-Hellman 20
  - SHA1–AES(256) and Diffie-Hellman 2
- Phase 2 defaults:
  - ESP–AES(256)–SHA1
  - ESP–AES(128)–SHA1
  - ESP – AES(256)–SHA2(256)

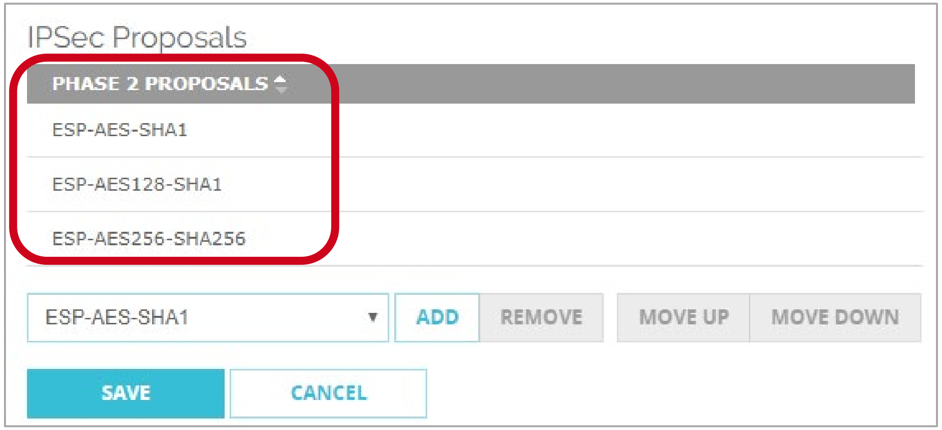
Updated Default VPN Security Settings

- Phase 1 and 2 settings for Mobile VPN with L2TP



Transform Settings

PHASE 1 TRANSFORM	KEY GROUP
SHA1-AES(256-bit)	Diffie-Hellman Group 2
SHA1-AES(256-bit)	Diffie-Hellman Group 20
SHA2-256-AES(256-bit)	Diffie-Hellman Group 14



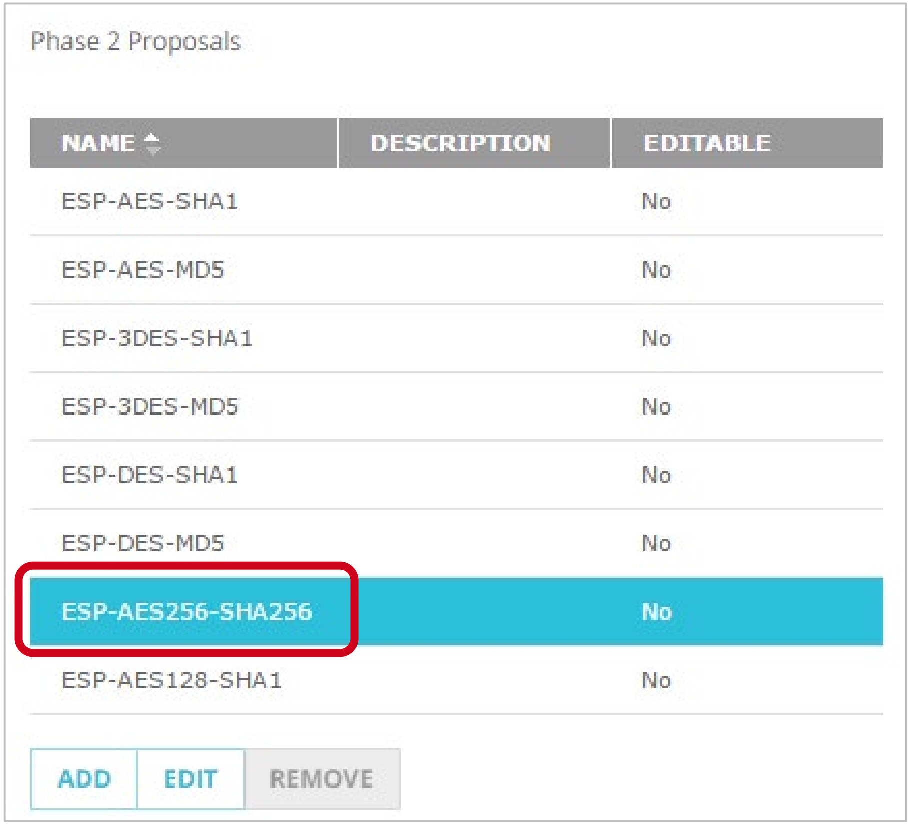
IPSec Proposals

PHASE 2 PROPOSALS
ESP-AES-SHA1
ESP-AES128-SHA1
ESP-AES256-SHA256

ESP-AES-SHA1

Updated Default VPN Security Settings

- The **Phase 2 Proposals** list now includes the ESP-AES256-SHA256 transform



Phase 2 Proposals

NAME	DESCRIPTION	EDITABLE
ESP-AES-SHA1		No
ESP-AES-MD5		No
ESP-3DES-SHA1		No
ESP-3DES-MD5		No
ESP-DES-SHA1		No
ESP-DES-MD5		No
ESP-AES256-SHA256		No
ESP-AES128-SHA1		No

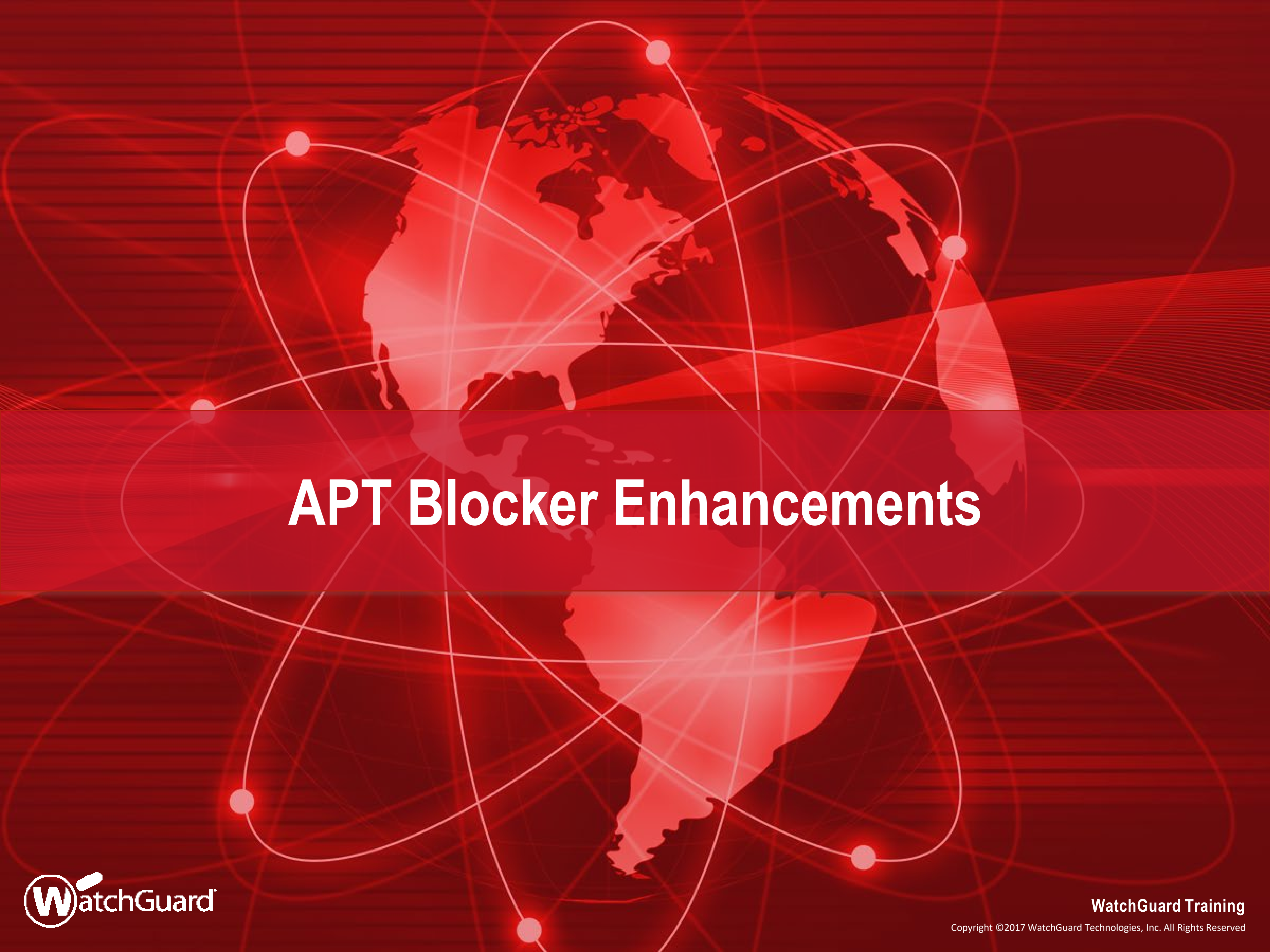
Updated Default VPN Security Settings

- SHA-2 is supported on these Firebox and XTM device models:
  - All Fireboxes
  - XTM devices with hardware cryptographic acceleration for SHA-2
- SHA-2 is not supported on XTM 505, 510, 520, 530, 515, 525, 535, 545, 810, 820, 830, 1050, and 2050 devices
- If your XTM device does not support SHA-2, the available proposals on your device do not include SHA-2

Removed Mobile VPN with SSL Settings

Removed Mobile VPN with SSL Settings

- These obsolete security settings were removed from Mobile VPN with SSL:
  - Encryption — Blowfish and DES
  - Authentication — MD5
- If your configuration includes MD5, this setting changes to SHA-256 after the upgrade
- If your configuration includes Blowfish or DES, this setting changes to AES-256 after the upgrade



APT Blocker Enhancements

APT Blocker JavaScript Scanning in Email

- APT Blocker now detects and scans JavaScript (.JS) files in email attachments
- This can help protect your network from a recent trend in ransomware delivered through JavaScript email attachments

APT Blocker JavaScript Scanning in Email

- APT Blocker now scans these file types:
  - Windows PE (Portable Executable) files, such as: .CPL, .EXE, .DLL, .OCX, .SYS, .SCR, .DRV, and .EFI
  - Adobe PDF documents
  - Microsoft Office documents
  - Rich Text Format (.RTF) documents
  - Android executable files (.APK)
  - Apple Mac application files (.APP)
  - JavaScript files (.JS) — New in v12.0 (email attachments only)

APT Blocker Zero-Day Protection for Email

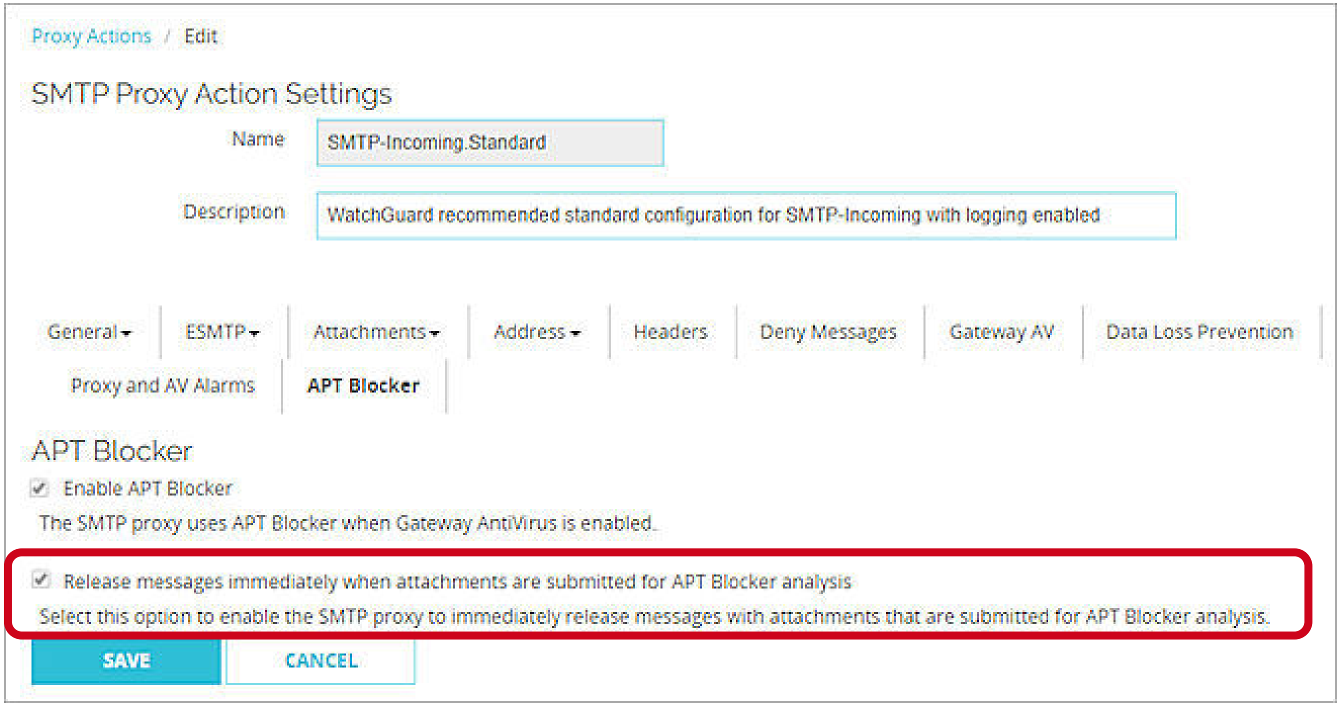
- A zero-day attack is a new attack that has not yet been analyzed and identified
- APT Blocker can help protect your network from zero-day attacks that are sent in email attachments
- When APT Blocker is enabled, the SMTP or IMAP proxy can delay delivery of the message while it submits the file attachment to the Lastline data center for analysis
  - APT Blocker analysis can take up to a few minutes for each file
  - If the Firebox cannot connect to the Lastline data center, APT Blocker releases the message
- Zero-day protection is always enabled in the IMAP proxy and is a configurable option in the SMTP proxy

APT Blocker Zero-Day Protection — SMTP

- The SMTP proxy has a new APT Blocker configuration option to enable zero-day protection
  - In previous Fireware versions, the SMTP proxy delivered a message while APT Blocker analysis of all attachments was in progress; this is still the default behavior
    - The default setting enables immediate message delivery, but does not provide protection against zero-day attacks in email attachments
  - You can now configure the SMTP proxy to delay delivery of a message until APT Blocker analysis of all attachments is complete
    - This protects against zero-day attacks, but can introduce a delay in message delivery while APT Blocker analysis is in progress

APT Blocker Zero-Day Protection — SMTP

- To enable APT Blocker zero-day protection, in the APT Blocker settings clear the **Release messages immediately when attachments are submitted for APT Blocker analysis** check box



Proxy Actions / Edit

SMTP Proxy Action Settings

Name: SMTP-Incoming.Standard

Description: WatchGuard recommended standard configuration for SMTP-Incoming with logging enabled

APT Blocker

☑ Enable APT Blocker

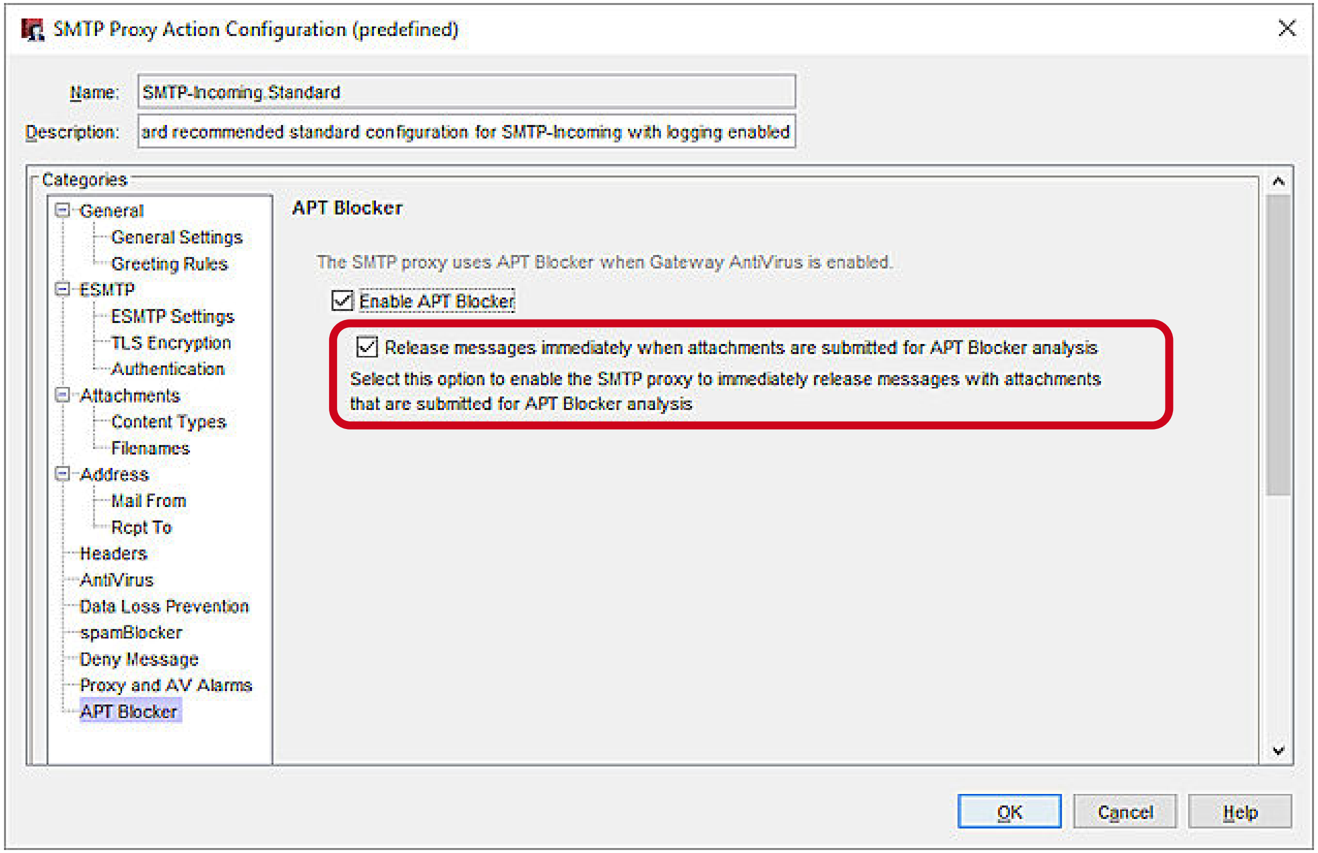
The SMTP proxy uses APT Blocker when Gateway AntiVirus is enabled.

☑ Release messages immediately when attachments are submitted for APT Blocker analysis

Select this option to enable the SMTP proxy to immediately release messages with attachments that are submitted for APT Blocker analysis.

APT Blocker Zero-Day Protection — SMTP

- The new APT Blocker zero-day protection option in Policy Manager



SMTP Proxy Action Configuration (predefined)

Name: SMTP-Incoming.Standard

Description: ard recommended standard configuration for SMTP-Incoming with logging enabled

Categories

- General
  - General Settings
  - Greeting Rules
- ESMTP
  - ESMTP Settings
  - TLS Encryption
  - Authentication
- Attachments
  - Content Types
  - Filenames
- Address
  - Mail From
  - Rcpt To
- Headers
- AntiVirus
- Data Loss Prevention
- spamBlocker
- Deny Message
- Proxy and AV Alarms
- APT Blocker

APT Blocker

The SMTP proxy uses APT Blocker when Gateway AntiVirus is enabled.

☑ Enable APT Blocker

☑ Release messages immediately when attachments are submitted for APT Blocker analysis

Select this option to enable the SMTP proxy to immediately release messages with attachments that are submitted for APT Blocker analysis

APT Blocker Zero-Day Protection — SMTP

- When you enable zero-day protection in the SMTP proxy, if the MD5 value of an SMTP file attachment does not match the MD5 value of a previously analyzed file, the SMTP proxy delays delivery of the message while it submits the file attachment to the Lastline data center for analysis
  - If the SMTP proxy receives the result from Lastline before the sending MTA times out, the proxy takes the configured APT Blocker action based on the result
  - If the sending MTA times out before the transaction is completed, the message is not delivered
  - If the sending MTA resends the message, the SMTP proxy takes the configured APT Blocker action based on the APT Blocker analysis result

APT Blocker Zero-Day Protection — IMAP

- Zero-day protection is always enabled in the IMAP proxy
- If the MD5 value of an IMAP file attachment does not match the MD5 value of a previously analyzed file, the IMAP proxy delays delivery of the message while it submits the file attachment to the Lastline data center for analysis
  - If the IMAP proxy receives the result from Lastline before the IMAP server times out, the proxy takes the configured APT Blocker action based on the result
  - If the IMAP server times out before the transaction is completed, the IMAP client cannot retrieve the message
  - When the IMAP client requests the message again, the IMAP proxy takes the configured APT Blocker action based on the APT Blocker analysis result

APT Blocker Zero-Day Protection in Email

- Zero-day protection can cause a delay in message delivery, especially for messages that contain multiple attachments
- The IMAP proxy submits all file attachments for APT Blocker analysis at the same time
- The SMTP proxy submits file attachments for APT Blocker analysis one at a time
  - To reduce delivery delays, senders can attach multiple files as a single archive file
  - The SMTP proxy submits the archive for APT Blocker analysis, all files are analyzed at the same time

WebBlocker Enhancements

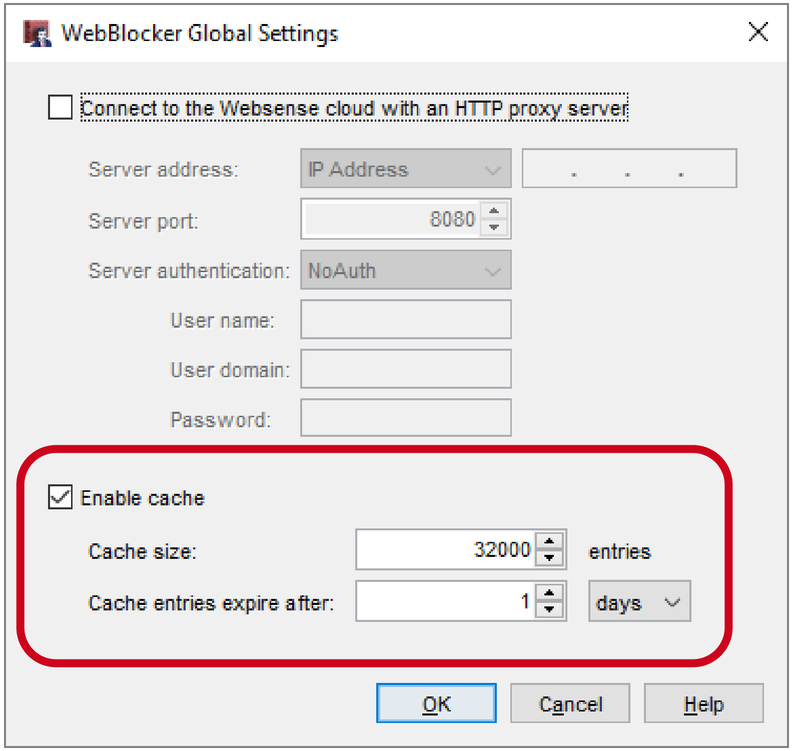
WatchGuard Training

WebBlocker Encrypted Lookups

- Lookup requests from the Firebox to the Websense cloud are now encrypted with HTTPS
  - Websense is now Forcepoint
- If your Firebox uses a web proxy server for connections to Websense cloud, make sure the proxy server can handle HTTPS connections

WebBlocker Configurable Cache Settings

- To improve performance, WebBlocker stores recent URL lookups in a local cache on the Firebox
- You can now set the WebBlocker cache settings in **WebBlocker Global Settings**
- We recommend that you start with the default cache size and expiration settings


WebBlocker Global Settings

☐ Connect to the Websense cloud with an HTTP proxy server

Server address: IP Address

Server port: 8080

Server authentication: NoAuth

User name:

User domain:

Password:

☑ Enable cache

Cache size: 32000 entries

Cache entries expire after: 1 days

WebBlocker Configurable Cache Settings

- Two new WebBlocker Global settings:
  - **Cache Size**
    - Controls how many recent URL lookups are stored in the cache
    - You can change the cache size to balance WebBlocker lookup performance with memory use on the Firebox
    - The maximum cache size varies by Firebox model
  - **Expiration**
    - Controls how long URL lookups remain in the cache
    - The default expiration setting is 1 day
    - Previously, the cache expiration was not configurable

Larger IPS Signature Set

Larger IPS Signature Set

- Intrusion Prevention Service (IPS) now includes a larger signature set for some Firebox models
- Signature sets include both IPS and Application Control rules; only the quantity of IPS rules changed
  - Standard signature set with approximately 1800 signatures:
    - Firebox T10, XTM 2 Series, FireboxV, XTMv, Firebox Cloud with less than 4 GB memory
  - Enhanced signature set with approximately 6000 signatures:
    - Firebox T30, T50, T70, M200, M300, XTM 33, 330, 5 Series, 810, 820, 830, 1050, and 2050

Larger IPS Signature Set

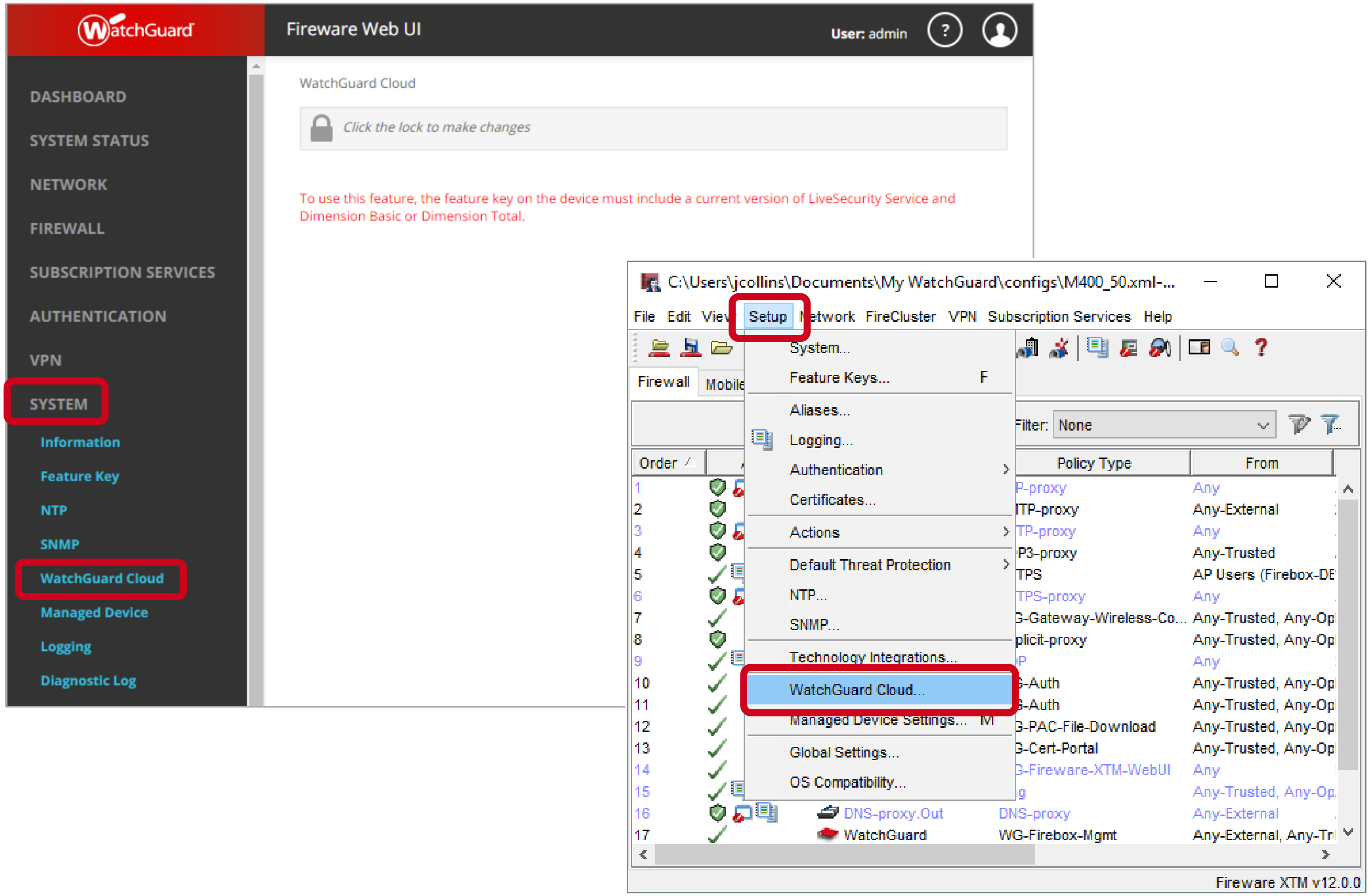
- Full signature set with approximately 8000 signatures (new in v12.0):
  - M370, M400, M440, M470, M500, M570, M670 M4600, M5600, XTM 870, 1500, 2520, FireboxV, XTMv, Firebox Cloud with 4 GB or more of memory

WatchGuard Cloud

WatchGuard Cloud

- WatchGuard Cloud is WatchGuard's forthcoming Cloud platform, where you can connect to Dimension Cloud for visibility and management of Fireboxes that run Fireware v12.0 or higher
- Fireboxes that run v12.0 or higher now include a menu option for WatchGuard Cloud
  - Fireware Web UI — **Setup > WatchGuard Cloud**
  - Policy Manager — **System > WatchGuard Cloud**
- For the Fireware v12.0 release, you cannot enable WatchGuard Cloud on your Firebox

WatchGuard Cloud



WatchGuard Cloud

Click the lock to make changes

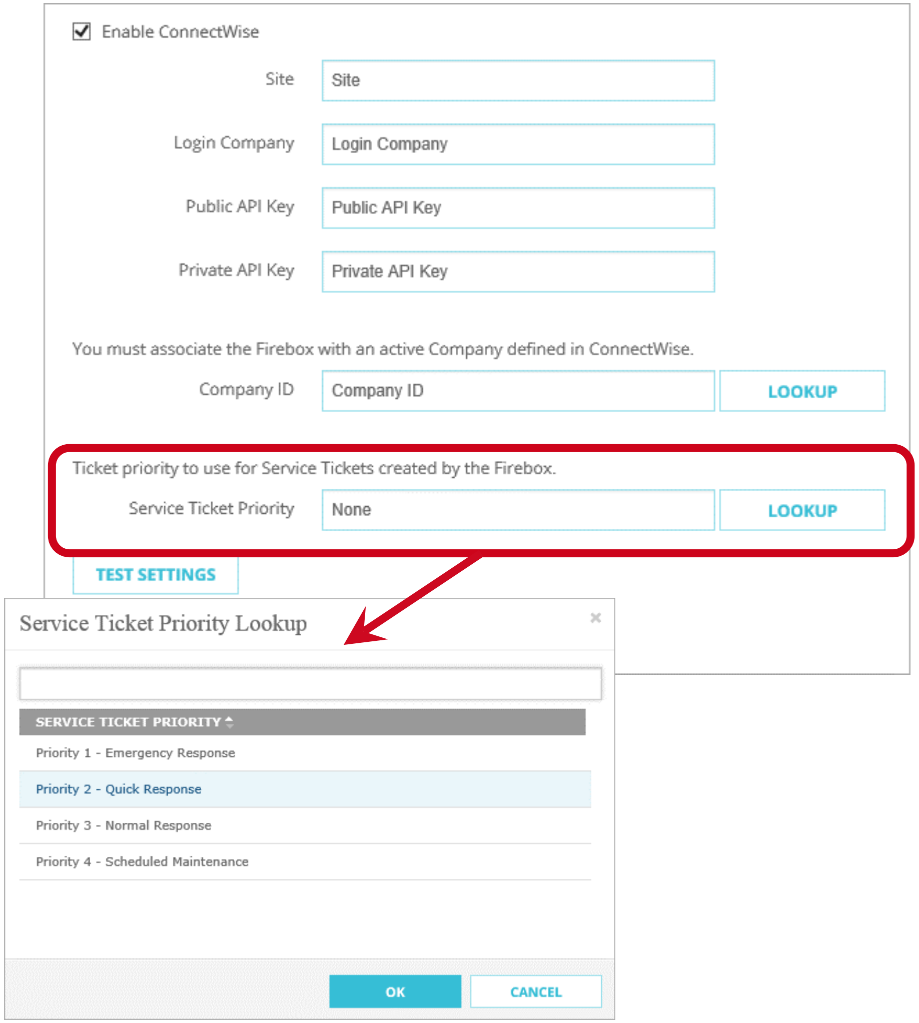
To use this feature, the feature key on the device must include a current version of LiveSecurity Service and Dimension Basic or Dimension Total.

ConnectWise Integration Enhancements

WatchGuard Training

Service Ticket Priority

- You can now configure the default ticket priority for service tickets generated by a Firebox
- To choose the priority from your ConnectWise configuration, click **Lookup**
- You can customize these priority levels in ConnectWise



☑ Enable ConnectWise

Site: Site

Login Company: Login Company

Public API Key: Public API Key

Private API Key: Private API Key

You must associate the Firebox with an active Company defined in ConnectWise.

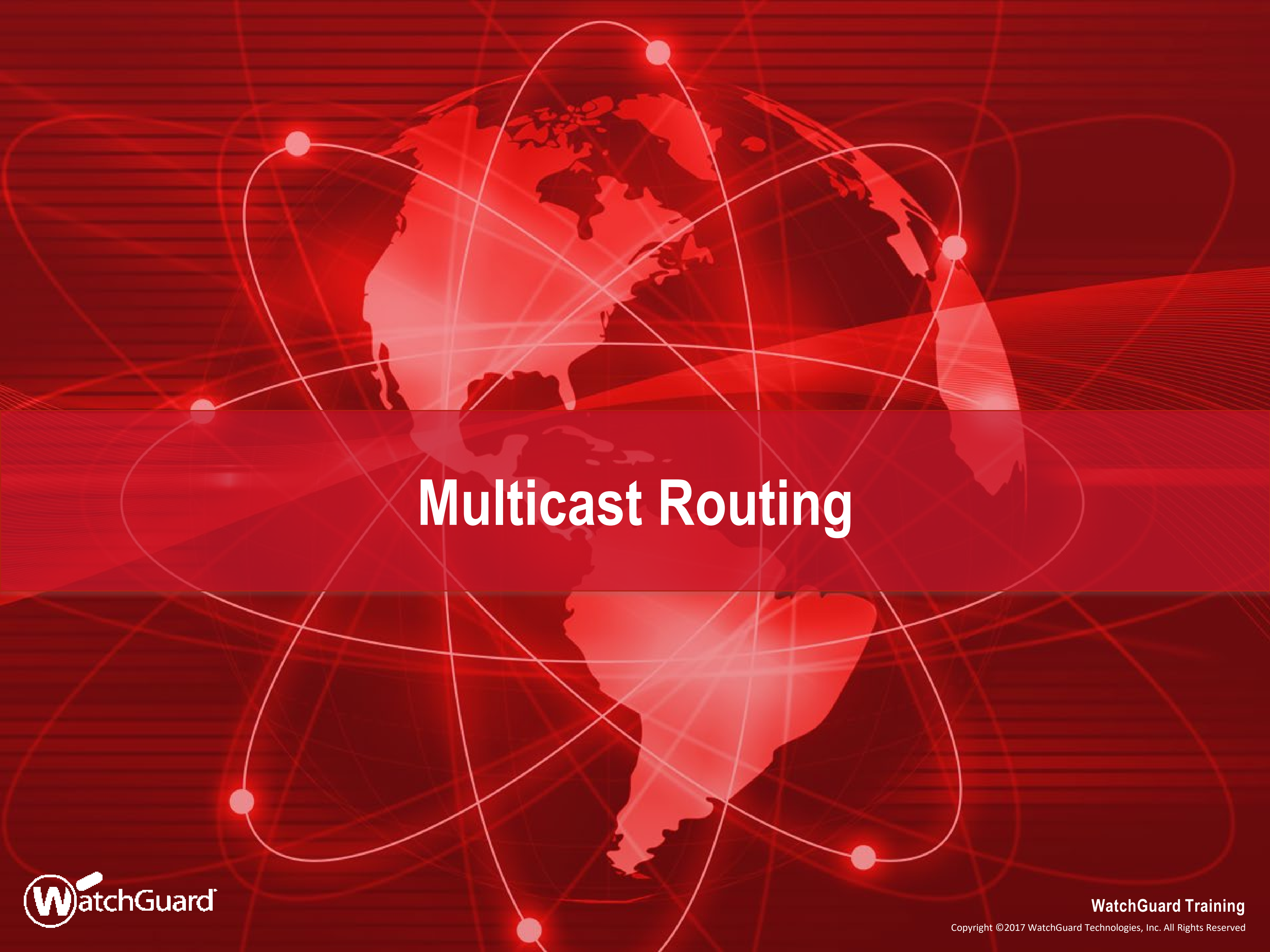
Company ID: Company ID

Ticket priority to use for Service Tickets created by the Firebox.

Service Ticket Priority: None

Service Ticket Priority Lookup

SERVICE TICKET PRIORITY
Priority 1 - Emergency Response
Priority 2 - Quick Response
Priority 3 - Normal Response
Priority 4 - Scheduled Maintenance



Multicast Routing

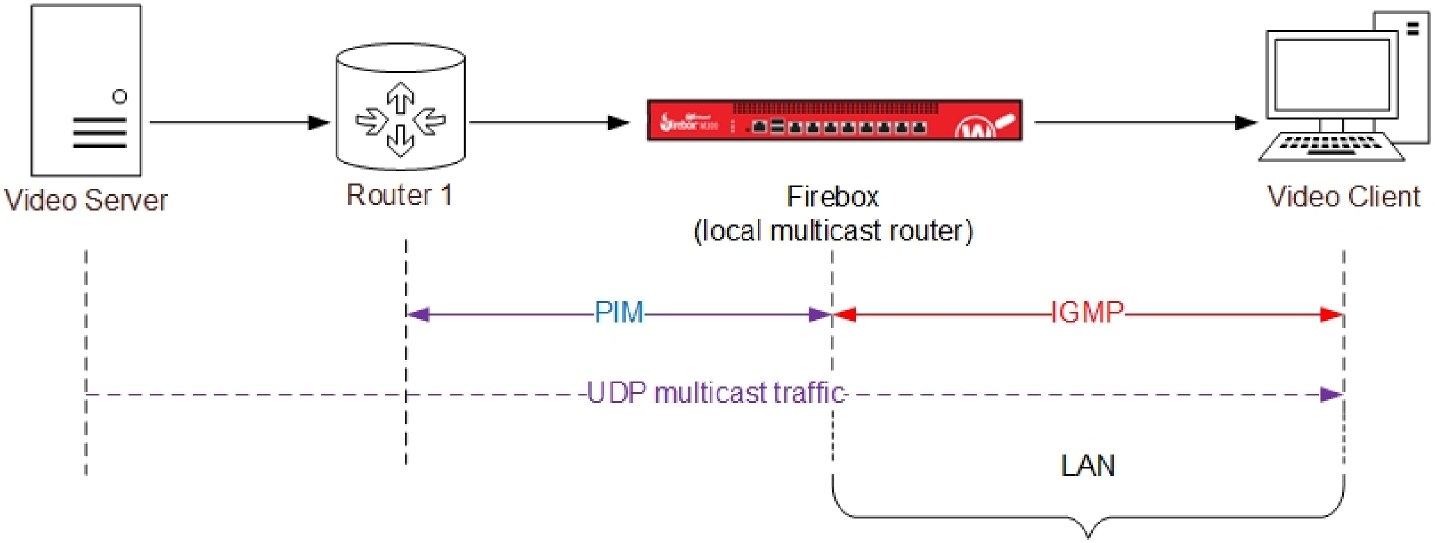
WatchGuard Training

Multicast Routing

- Fireware now includes support for multicast routing, a networking method for efficient distribution of one-to-many traffic
- Common uses include VOIP, video on demand (VOD), video conferencing, and IP television (IPTV)
- The Firebox acts as a local multicast router to forward multicast traffic from the source to receivers on your network
  - Receivers are nodes, such as workstations, that join the multicast group

Multicast Routing — Topology

- The Firebox is the local multicast router in this diagram



Multicast Routing

- Multicast routing on the Firebox has these configurable options:
  - Enable multicast globally
  - Select up to 31 interfaces for multicast
  - Select one or more Rendezvous Points (RPs)
- The most common multicast protocols are supported

Multicast Routing — Support Details

Supported Protocols	Unsupported Protocols
PIM Sparse Mode (PIM-SM)	Static multicast routes
Basic IGMP	PIM-DM
IGMPv2 and v3	IGMP snooping
IPv4	IGMP proxy
	IPv6

Supported Firebox Features	Unsupported Firebox Features
Mixed Routing mode	Bridge mode
BOVPN virtual interfaces	Drop-in mode
FireCluster Active/Passive	FireCluster Active/Active
	Manual BOVPN

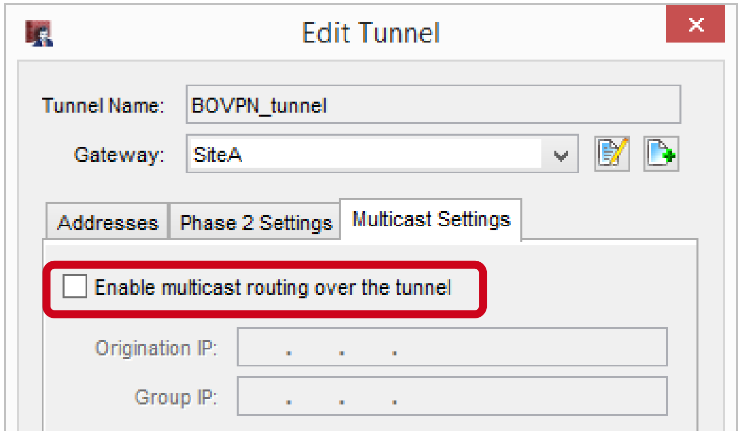
Multicast Routing — Support Details

Supported Interfaces	Unsupported Interfaces
Physical	Modem
VLAN	Mobile VPN
Bridge	Loopback
Link aggregation	
Wireless	
BOVPN virtual interfaces	

Supported Zones
External
Trusted
Optional
Custom

Multicast Routing — BOVPN Support Details

- The Firebox includes a legacy multicast setting for BOVPN that is supported in Fireware v12.0
- Before you can use the new multicast feature, you must disable the legacy BOVPN multicast setting



Edit Tunnel

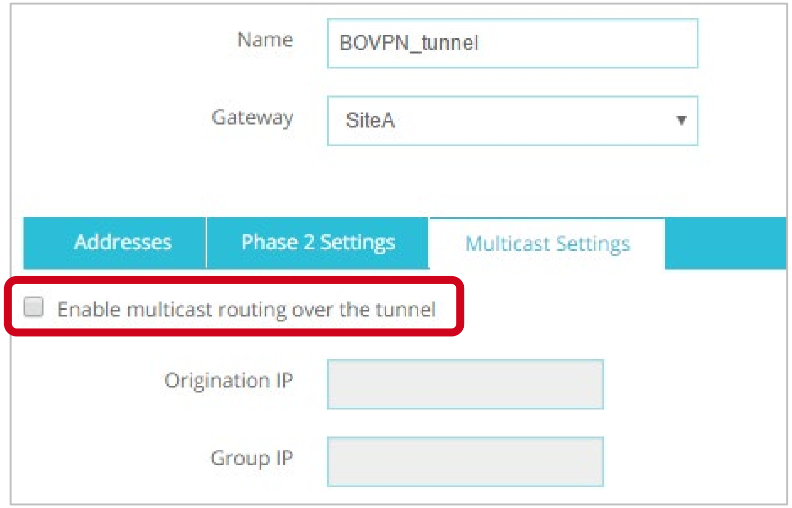
Tunnel Name: BOVPN_tunnel

Gateway: SiteA

□ Enable multicast routing over the tunnel

Origination IP: . . .

Group IP: . . .



Name BOVPN_tunnel

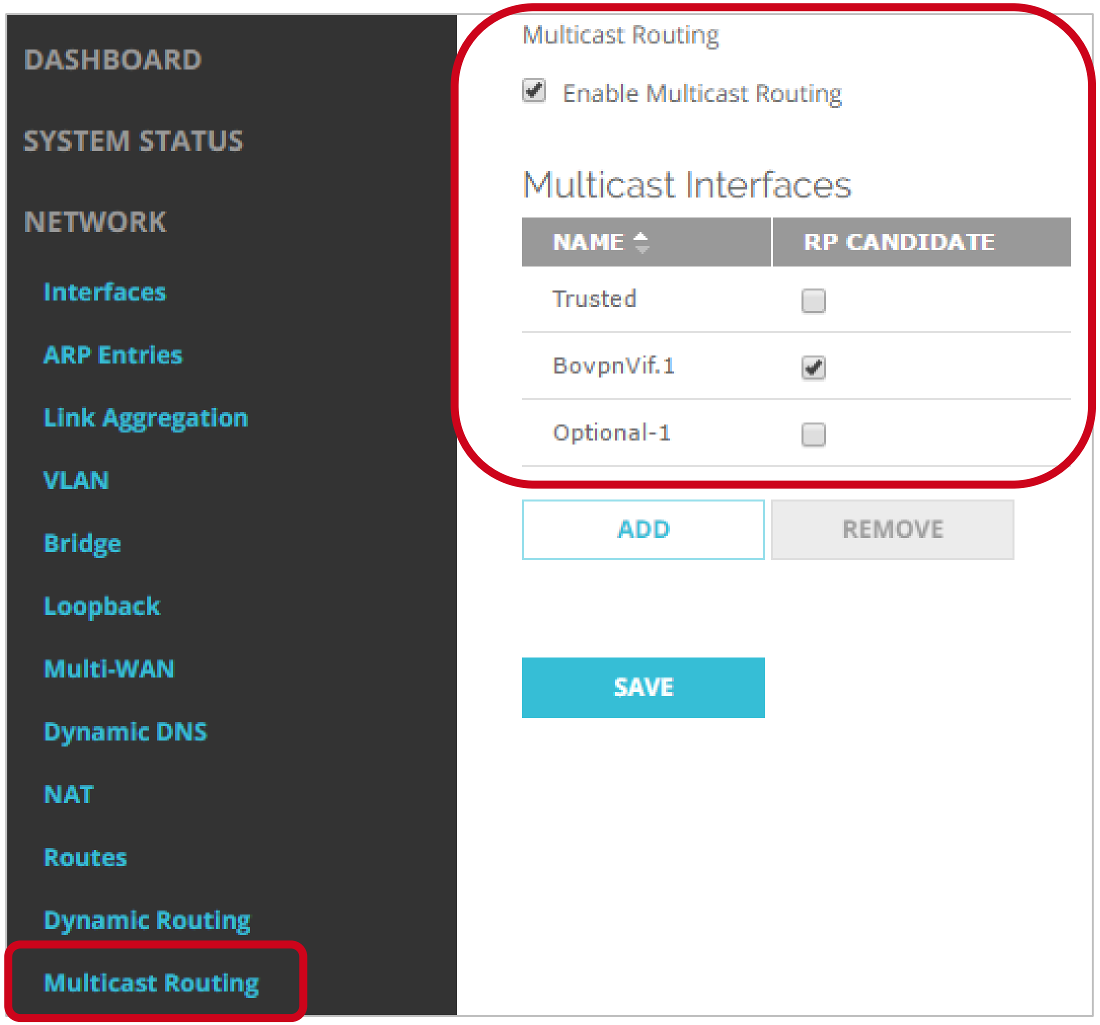
Gateway SiteA

□ Enable multicast routing over the tunnel

Origination IP

Group IP

Multicast Routing — Configuration (Web UI)



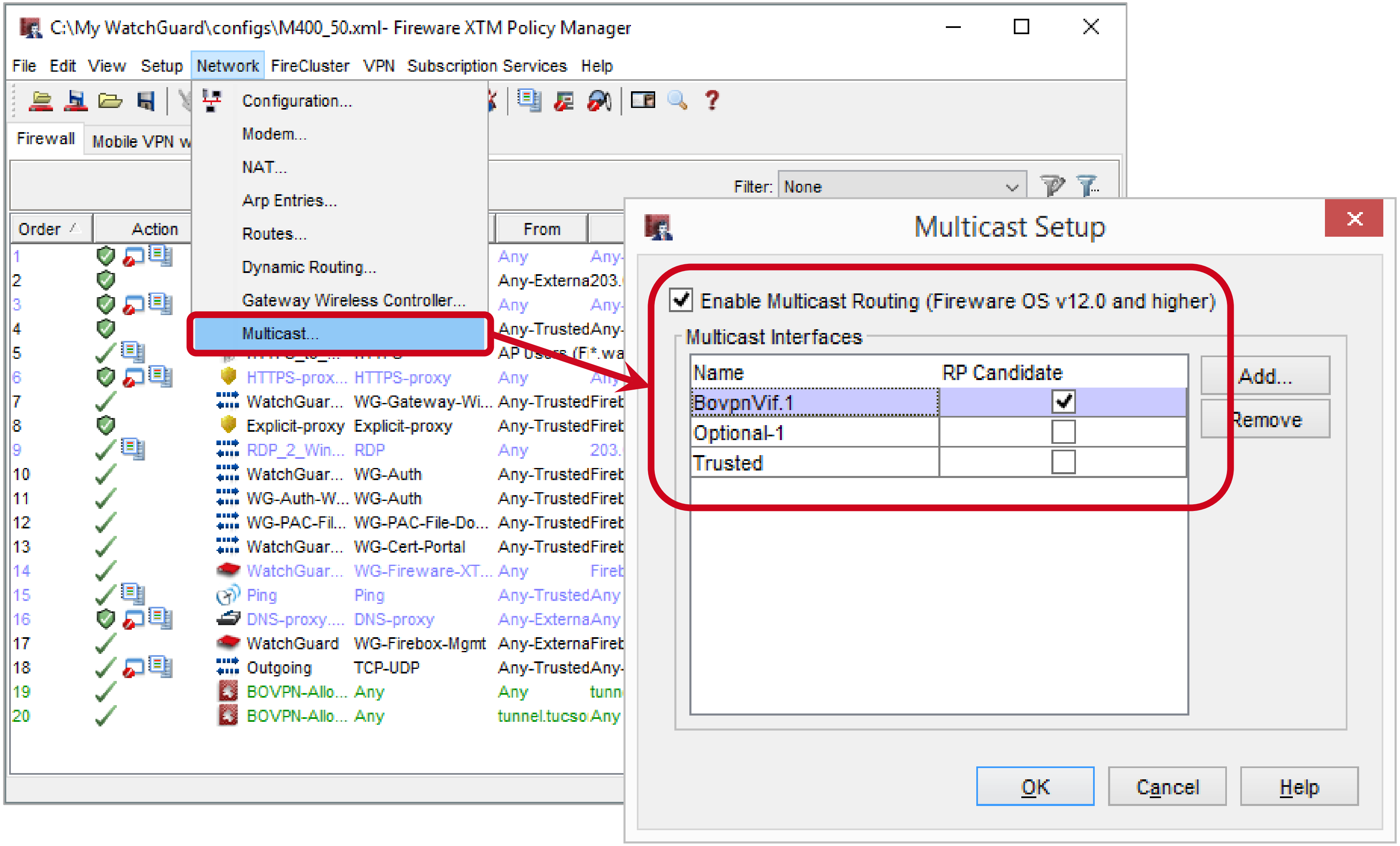
Multicast Routing

☑ Enable Multicast Routing

Multicast Interfaces

NAME	RP CANDIDATE
Trusted	□
BovpnVif.1	☑
Optional-1	□

Multicast Routing — Configuration (PM)



Order	Action			From	
1	✓			Any	Any-
2	✓			Any-Externa	203.
3	✓			Any	Any-
4	✓			Any-Trusted	Any-
5	✓			AP users (F	*.wa
6	✓	HTTPS-prox...	HTTPS-proxy	Any	Any-
7	✓	WatchGuar...	WG-Gateway-Wi...	Any-Trusted	Fireb
8	✓	Explicit-proxy	Explicit-proxy	Any-Trusted	Fireb
9	✓	RDP_2_Win...	RDP	Any	203.
10	✓	WatchGuar...	WG-Auth	Any-Trusted	Fireb
11	✓	WG-Auth-W...	WG-Auth	Any-Trusted	Fireb
12	✓	WG-PAC-Fil...	WG-PAC-File-Do...	Any-Trusted	Fireb
13	✓	WatchGuar...	WG-Cert-Portal	Any-Trusted	Fireb
14	✓	WatchGuar...	WG-Fireware-XT...	Any	Fireb
15	✓	Ping	Ping	Any-Trusted	Any
16	✓	DNS-proxy....	DNS-proxy	Any-Externa	Any
17	✓	WatchGuard	WG-Firebox-Mgmt	Any-Externa	Fireb
18	✓	Outgoing	TCP-UDP	Any-Trusted	Any-
19	✓	BOVPN-Allo...	Any	Any	tunn
20	✓	BOVPN-Allo...	Any	tunnel.tucso	Any

☑ Enable Multicast Routing (Fireware OS v12.0 and higher)

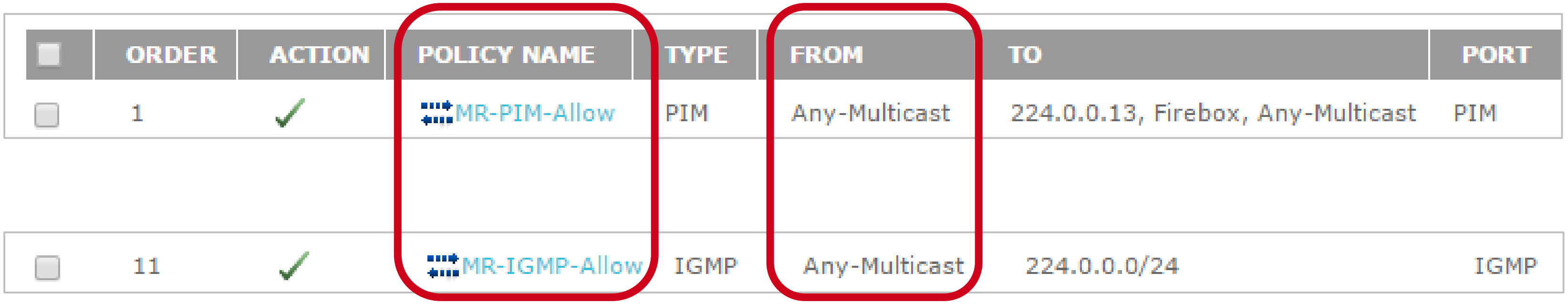
Multicast Interfaces

Name	RP Candidate
BovpnVif.1	☑
Optional-1	□
Trusted	□

WatchGuard Training

Multicast Routing — Policies and Aliases

- When you enable multicast routing, new policies for the PIM and IGMP protocols are added to your configuration
- The alias *Any-Multicast* is added to your configuration



□	ORDER	ACTION	POLICY NAME	TYPE	FROM	TO	PORT
□	1	✓	MR-PIM-Allow	PIM	Any-Multicast	224.0.0.13, Firebox, Any-Multicast	PIM
□	11	✓	MR-IGMP-Allow	IGMP	Any-Multicast	224.0.0.0/24	IGMP

Multicast Routing — Policies and Aliases

- You can specify only these options in a multicast policy:
  - Incoming interfaces
  - Source IP addresses
  - Destination IP addresses
  - Protocols and ports

What Else is New

WatchGuard Training

What Else is New

- The WatchGuard Mobile VPN app for iOS has been removed from the Apple Store (not related to Fireware v12.0)
  - If you have this app on your mobile device, we recommend that you use the native iOS VPN client instead

Thank You!

WatchGuard Training

NOTHING GETS PAST RED.

WatchGuard

WatchGuard Training