

# What's New in Fireware v12.1

# What's New in Fireware v12.1

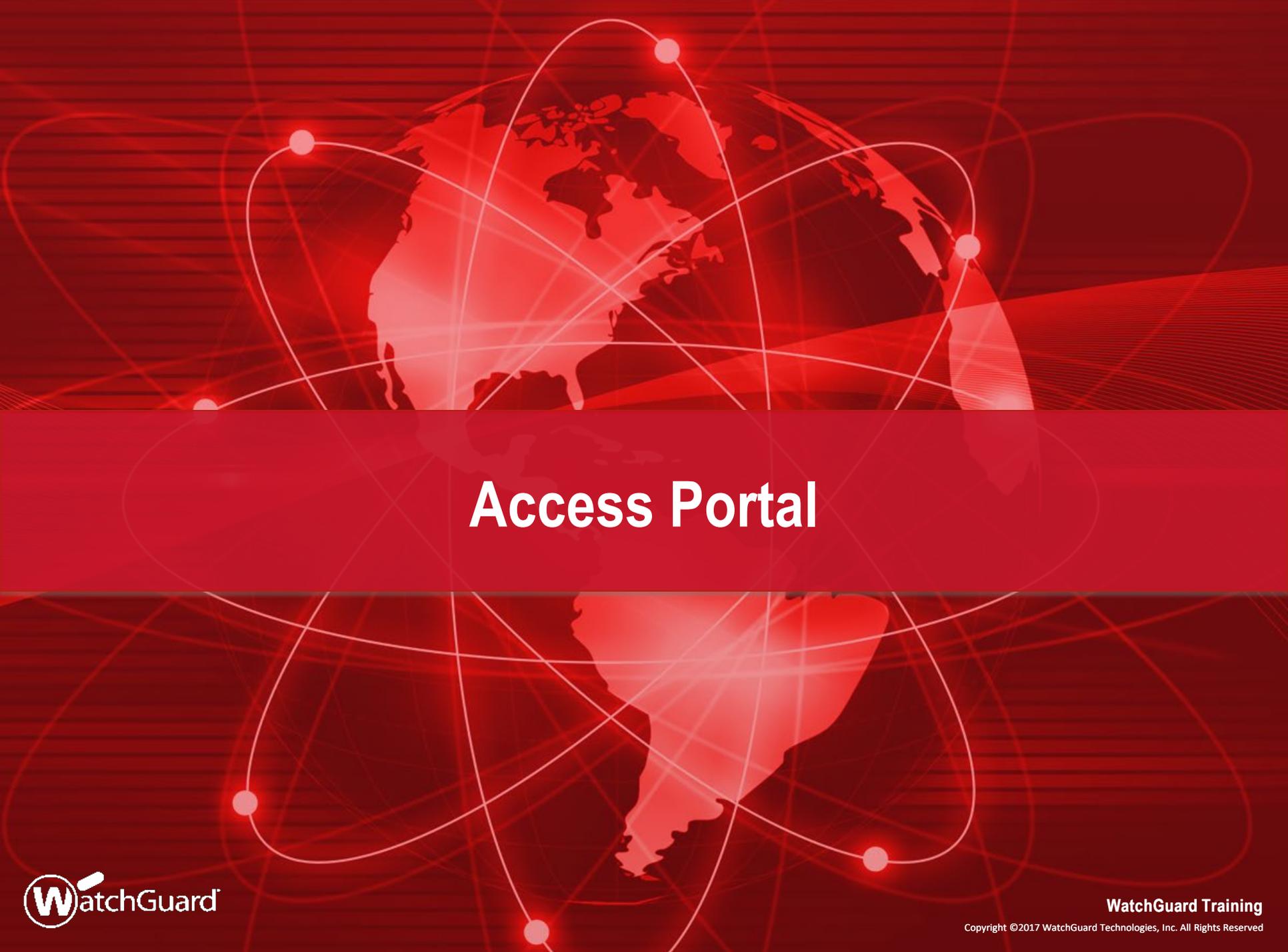
- Access Portal and SAML Single Sign-On
- HTTPS Content Inspection Enhancements
- Secure IMAP (IMAPS) Proxy
- WebBlocker UX/UI Enhancements
- Mobile VPN with SSL Portal Updates
- Mobile VPN with IKEv2
- BOVPN over TLS
- SSL/TLS Shared Settings
- Modem as an External Interface



# What's New in Fireware v12.1

- Multi-WAN Link Monitor Updates
- Wildcard Support for IPv4 Addresses
- Gateway Wireless Controller Enhancements

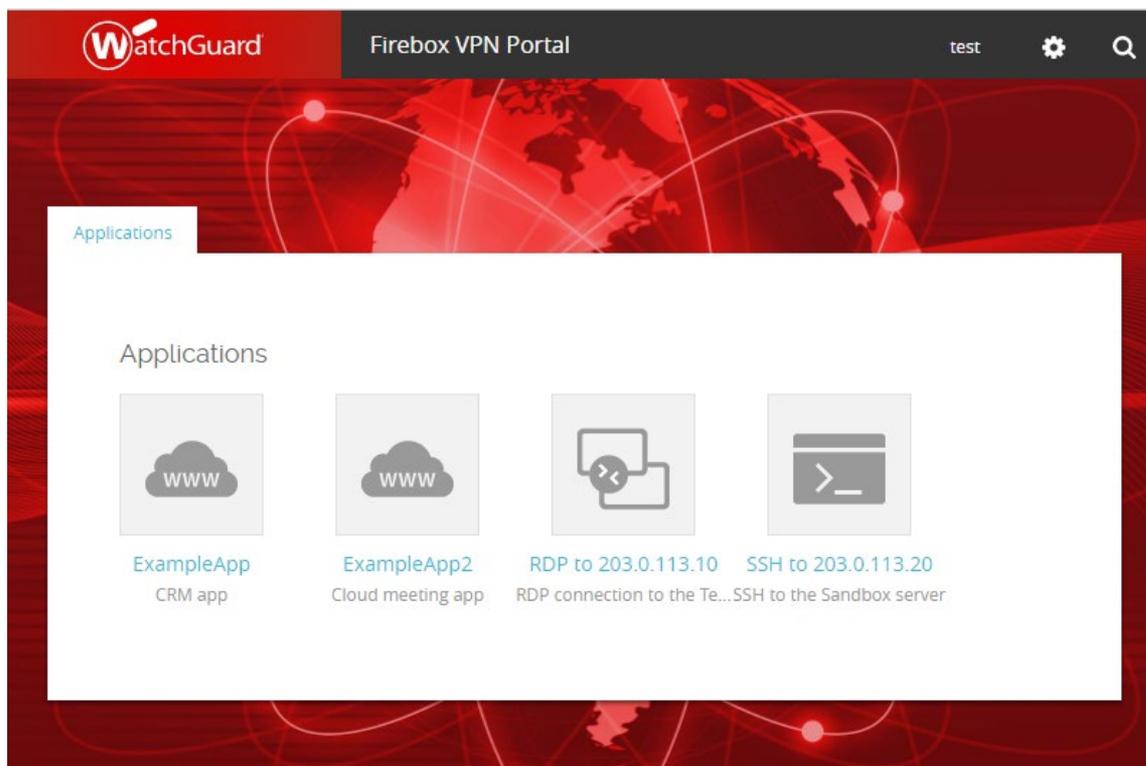




# Access Portal

# Access Portal

- The new Access Portal feature connects users to external third-party web apps, and in-browser RDP and SSH sessions to local resources, without a VPN client



# Access Portal

- Secure remote access to virtual machines through RDP gives privileged network administrators the flexibility to manage network operations remotely
- SSH sessions in HTML5-compliant and SSL-compliant web browsers enables privileged administrators to work in a secure shell to manage critical network assets
- TLS 1.2 adds security to RDP and SSH sessions

# Access Portal

- HTTPS connections to apps are proxied by the Firebox
- Users authenticate to the Access Portal and see links to web apps, RDP hosts, and SSH hosts
  - You can specify the apps/app groups that users and user groups can connect to
- Single Sign-On through a third-party identity provider (Okta, OneLogin, Shibboleth, etc.) is supported through the SAML authentication protocol
- Access Portal is not supported on XTM, XTMv, T, M200, or M300 devices. The Access Portal is supported on FireboxV, FireboxCloud, and all other Fireboxes.

# Access Portal

- Access Portal is a subscription service included in the Total Security Suite
  - Users with a Total Security Suite subscription must update the feature key on the Firebox to get the Access Portal license

# Access Portal — Shared Settings

- Access Portal and Mobile VPN with SSL share these VPN portal settings:
  - Interfaces on which the VPN portal is available
  - Authentication server
  - VPN Portal port
    - The VPN Portal port is the TCP configuration channel for Mobile VPN with SSL and the Access Portal
    - The data channel for Mobile VPN with SSL appears in the Mobile VPN with SSL settings

# Access Portal — Shared Settings

- Access Portal, Mobile VPN with SSL, and Management Tunnels over SSL share the *WatchGuard SSLVPN* firewall policy
- Any-External is the only available interface for the Access Portal if Mobile VPN with SSL has not been configured on the Firebox
- Any-External, Any-Trusted, and Any-Optional interfaces are available if the Access Portal is enabled, and Mobile VPN with SSL is enabled (or was enabled previously) with the default interface settings
- Shared SSL/TLS settings affect several Firebox features and are described in more detail in the *SSL/TLS Shared Settings* section

# Access Portal — Configure

- Add web apps, RDP hosts, and SSH hosts on the Firebox

Enable Access Portal

Applications | User Connections Settings

### Web Applications and Application Groups

Specify the applications that appear in the VPN Portal. Applications appear in the order specified in this list.

NAME	DESCRIPTION	TYPE	HOST LOCATION
▼ Applications		Application Group	
 ExampleApp	CRM app	Web Application	http://www.example.com
 ExampleApp2	Cloud meeting app	Web Application	http://www.example.com
 RDP to 203.0.113.10	RDP connection to the Test server	Host Desktop Access (RDP)	203.0.113.10:3389
 SSH to 203.0.113.20	SSH to the Sandbox server	Host Shell Access (SSH)	203.0.113.20:22
 test	test	Web Application	http://www.google.com

ADD ▼ EDIT REMOVE MOVE UP MOVE DOWN

# Access Portal — Configure

- Specify which apps users and groups can connect to

Configure the settings for this user or group.

Authentication Server

Type

Name

Select the resources that are available to this user or group.

NAME	TYPE
<input type="checkbox"/> Applications	Application Group
<input checked="" type="checkbox"/>  ExampleApp	Web Application
<input checked="" type="checkbox"/>  ExampleApp2	Web Application
<input checked="" type="checkbox"/>  RDP to 203.0.113.10	Host Desktop Access (RDP)
<input checked="" type="checkbox"/>  SSH to 203.0.113.20	Host Shell Access (SSH)

# Access Portal — Configure

- You can customize these elements of the login and portal pages:
  - Page title
  - Login logo
  - Header logo
  - Background image
- You can also upload a custom .CSS file to customize page elements, such as buttons

The screenshot displays the 'Customization' tab of the WatchGuard configuration interface. It features a navigation bar with 'General', 'Customization', and 'SAML' tabs. The 'Page Title' field is set to 'Example Company Access Portal'. The 'Custom login logo' section is checked and shows a blue logo with 'Example Company' text. Below it, there is a 'Choose File' button with 'logo.jpg' selected, and 'UPLOAD' and 'RESET IMAGE' buttons. The 'Custom header logo' section is unchecked and shows a 'NO IMAGE AVAILABLE' placeholder. Below it, there is a 'Choose File' button with 'No file chosen' selected, and 'UPLOAD' and 'RESET IMAGE' buttons. The 'Custom background image' section is also unchecked and shows a 'NO IMAGE AVAILABLE' placeholder. Below it, there is a 'Choose File' button with 'No file chosen' selected, and 'UPLOAD' and 'RESET IMAGE' buttons. The 'Custom CSS file' section is unchecked and shows a 'Choose File' button with 'No file chosen' selected, and 'UPLOAD' and 'RESET CSS' buttons. At the bottom, there are two buttons: 'PREVIEW LOGIN PAGE' and 'PREVIEW APPLICATION PAGE'.

# Access Portal — Configure

- Configure the interface, authentication server, and port settings
- These settings are shared with Mobile VPN with SSL
- The Access Portal appears at `https://<host name or IP address of the Firebox>` unless you change the port number

Access Portal / VPN Portal

Click the lock to prevent further changes

General Customization SAML

### Interfaces

Specify the interfaces for connections to the VPN Portal

INTERFACE ↕
Any-External
Any-Trusted
Any-Optional

Any-External ▾ ADD REMOVE

### Authentication Servers

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

AUTHENTICATION SERVER
Firebox-DB

Firebox-DB ▾ ADD REMOVE MOVE UP MOVE DOWN

### Timeouts

Session Timeout  hours

Idle Timeout  minutes

### VPN Portal Port

Port

# Access Portal — Configure

- You cannot change the VPN Portal Port if the Access Portal and Mobile VPN with SSL are both enabled
- If you change the TCP data channel for Mobile VPN with SSL, the VPN Portal port inherits that setting

Activate Mobile VPN with SSL

General	Authentication	Advanced
Authentication	SHA-256	
Encryption	AES (256-bit)	
Data channel	TCP	444

VPN Portal Port

Specify the VPN Portal Port. This is the configuration port shared by Mobile SSL VPN Clients and users of the Access Portal.

The TCP data channel port for Mobile VPN with SSL has precedence over the VPN Portal port. To set the Mobile VPN with SSL port, [click here](#).

VPN Portal Port 444

# Access Portal — Configure

- If you select UDP for the Mobile VPN with SSL data channel, you can specify a different VPN Portal port

Activate Mobile VPN with SSL

General	Authentication	Advanced
Authentication	SHA-256	
Encryption	AES (256-bit)	
Data channel	UDP	444

VPN Portal Port

Specify the VPN Portal Port. This is the configuration port shared by Mobile SSL VPN Clients and users of the Access Portal.

VPN Portal Port 445

# Access Portal — SAML Single Sign-On

- SAML 2.0 is the single sign-on (SSO) standard for easy access to web applications through SSO technologies
- Access Portal offers a centralized sign-in experience with the convenience of SAML 2.0 for IT administrators who require a convenient and authenticated solution
- SAML authentication occurs between a Service Provider (SP) and an Identity Provider (IdP)
  - The Firebox is the SP
  - A third-party identity provider that you specify, such as Okta or OneLogin, is the IdP

# Access Portal — SAML Single Sign-On

- To enable SAML for the Access Portal:
  - Configure the SAML settings on your Firebox
    - You can specify the optional IdP metadata URL if your IdP can send metadata to service providers
  - Give the Firebox SAML information to your IdP administrator
    - The Firebox automatically generates a webpage at `https://<SAML hostname or Firebox IP address>/auth/saml` that shows the Firebox SAML URLs and certificate
  - The IdP administrator must configure your IdP account with the Firebox SAML URLs and certificate

# Access Portal — SAML Single Sign-On

- SAML settings on the Firebox (Web UI)

General Customization **SAML**

To authenticate Clientless VPN users with SAML single sign-on, the Firebox exchanges authentication information with an Identity Provider (IDP) you specify.

Enable SAML

### Service Provider (SP) Settings

To configure your Firebox as the SAML Service Provider, specify the name of your IDP to appear as the authentication server name.

IDP Name

For the Host Name, specify a fully qualified domain name that resolves to the Firebox external interface.

Host Name

After you save the configuration to your Firebox, follow the IDP configuration instructions at <https://portal.example.com/auth/saml>

### Identity Provider (IDP) Settings

Specify the SAML connection settings for your third-party Identity Provider.

IDP Metadata URL

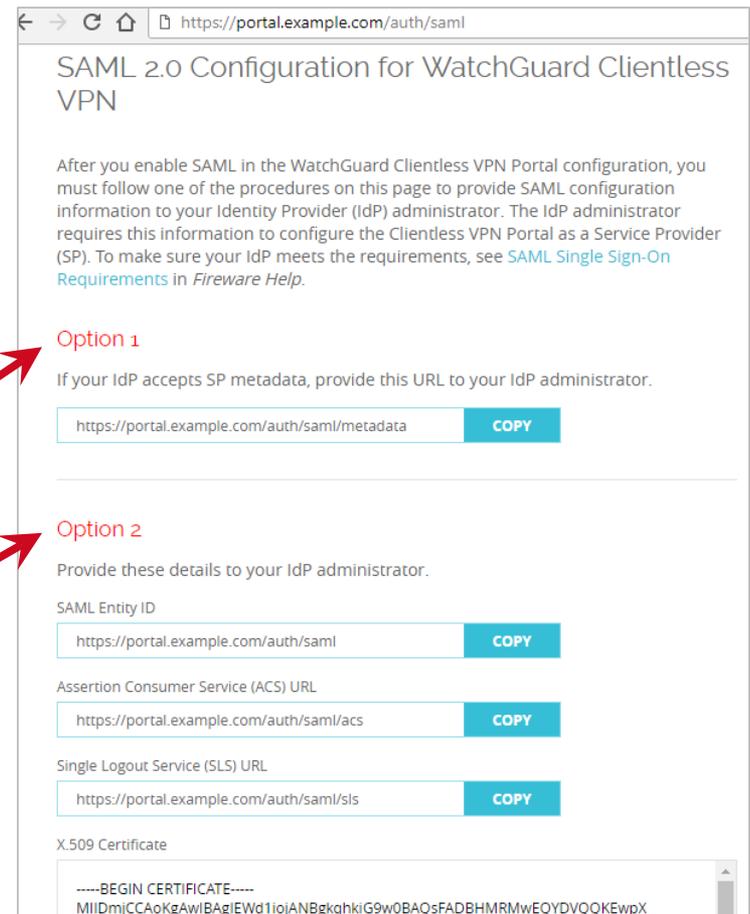
Group Attribute Name  [EDIT](#)

# Access Portal — SAML Single Sign-On

- SAML IdP instructions appear on a webpage generated from the SAML host name you specify

*Automatic IdP configuration*

*Manual IdP configuration*



https://portal.example.com/auth/saml

## SAML 2.0 Configuration for WatchGuard Clientless VPN

After you enable SAML in the WatchGuard Clientless VPN Portal configuration, you must follow one of the procedures on this page to provide SAML configuration information to your Identity Provider (IdP) administrator. The IdP administrator requires this information to configure the Clientless VPN Portal as a Service Provider (SP). To make sure your IdP meets the requirements, see [SAML Single Sign-On Requirements](#) in *Fireware Help*.

**Option 1**

If your IdP accepts SP metadata, provide this URL to your IdP administrator.

**COPY**

**Option 2**

Provide these details to your IdP administrator.

SAML Entity ID  
 **COPY**

Assertion Consumer Service (ACS) URL  
 **COPY**

Single Logout Service (SLS) URL  
 **COPY**

X.509 Certificate

```
-----BEGIN CERTIFICATE-----
MIIDmjCCAoKgAwIBAgIEWd1iojANBgkqhkiG9w0BAQsFADBHMwEQYDVQQKEwpx
```

# Access Portal

- Users connect to the Access Portal at `https://<host name or IP address of the Firebox>` and authenticate to the authentication server you specified



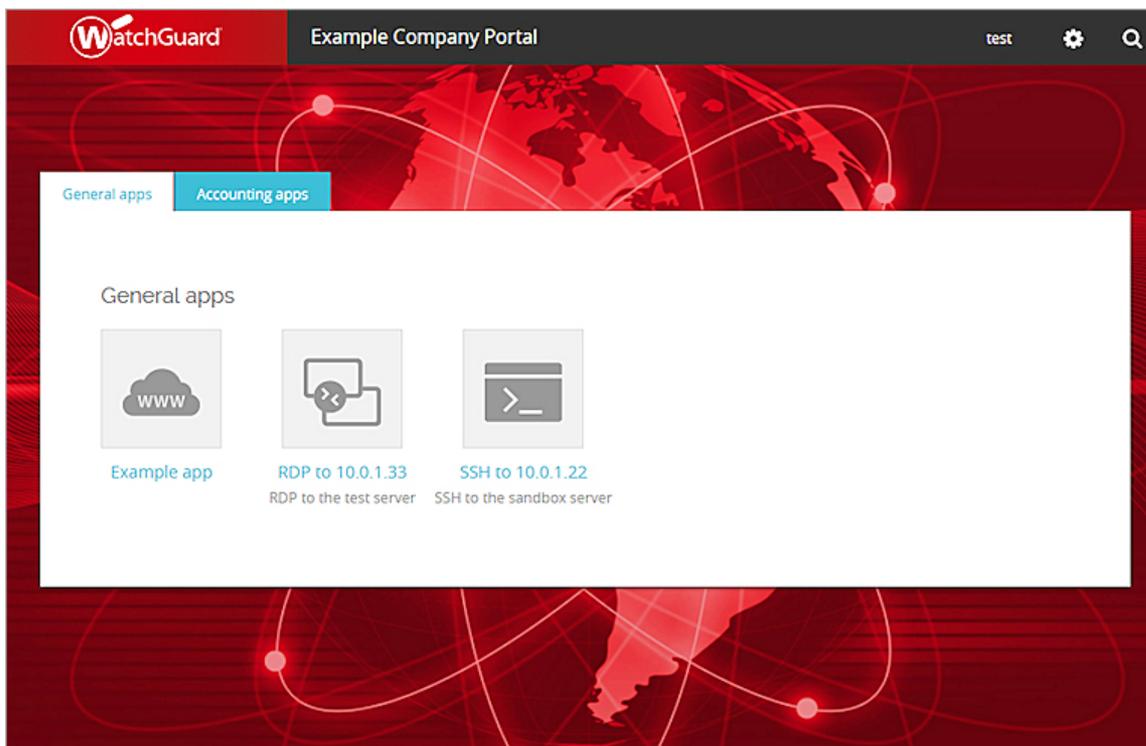
# Access Portal

- If you enabled SAML, the SAML identity provider you specified appears in the list of authentication servers



# Access Portal

- After the user authenticates, apps appear in the portal that the user has permission to connect to
- Click an app to connect



# Access Portal — Authenticated Users

- You can see the users that are connected to the Access Portal
- From Fireware Web UI, on the **System Status > Authentication List** page

Authentication List 30 SECONDS ▾ ||

## Authentication List

### Summary

Mobile VPN with L2TP: 0	Mobile VPN with SSL: 0	Mobile VPN with IPsec: 0
Mobile VPN with IKEv2: 0	<b>Access Portal: 0</b>	Firewall: 0
Total Users: 0		

Users Locked Out: 0 [UNLOCK USERS](#)

### Authenticated Users

[LOG OFF USERS](#)

USER	TYPE	DOMAIN	CLIENT	ELAPSED TIME	IP ADDRESS	LOGIN LIMIT
------	------	--------	--------	--------------	------------	-------------

# Access Portal — Authenticated Users

- From Firebox System Manager, on the **Authentication List** tab

The screenshot displays the Firebox System Manager interface for IP address 203.0.113.20. The 'Authentication List' tab is active, showing a summary of user statistics. The 'Access Portal' status is highlighted with a red box, indicating 0 users. Below the summary, there are tabs for 'Firewall Users', 'Mobile VPN Users', and 'Management Users'. A table with columns for 'User', 'Type', 'Auth Client', 'IP Address', 'Elapsed Time', and 'Login limit' is present but empty. At the bottom, there is a 'Refresh Interval' set to 5 seconds, a 'Pause' button, and a 'Hotspot Clients' button.

Blocked Sites	Subscription Services	Gateway Wireless Controller	Traffic Management	User Quotas
Front Panel	Traffic Monitor	Bandwidth Meter	Service Watch	Status Report

Summary

Mobile VPN with IPSec:	0	Firewall:	0
Mobile VPN with SSL:	0	Management Users:	7
Mobile VPN with LZTP:	0	Users Locked Out:	0
Mobile VPN with IKEv2:	0		
Access Portal:	0		
Total Users:	7		

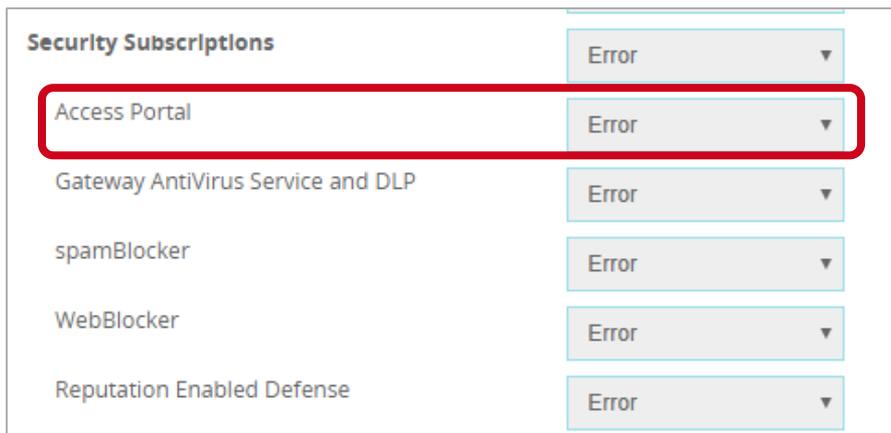
Firewall Users | Mobile VPN Users | Management Users

User	Type	Auth Client	IP Address	Elapsed Time	Login limit
------	------	-------------	------------	--------------	-------------

Refresh Interval: 5 seconds | Pause | Hotspot Clients

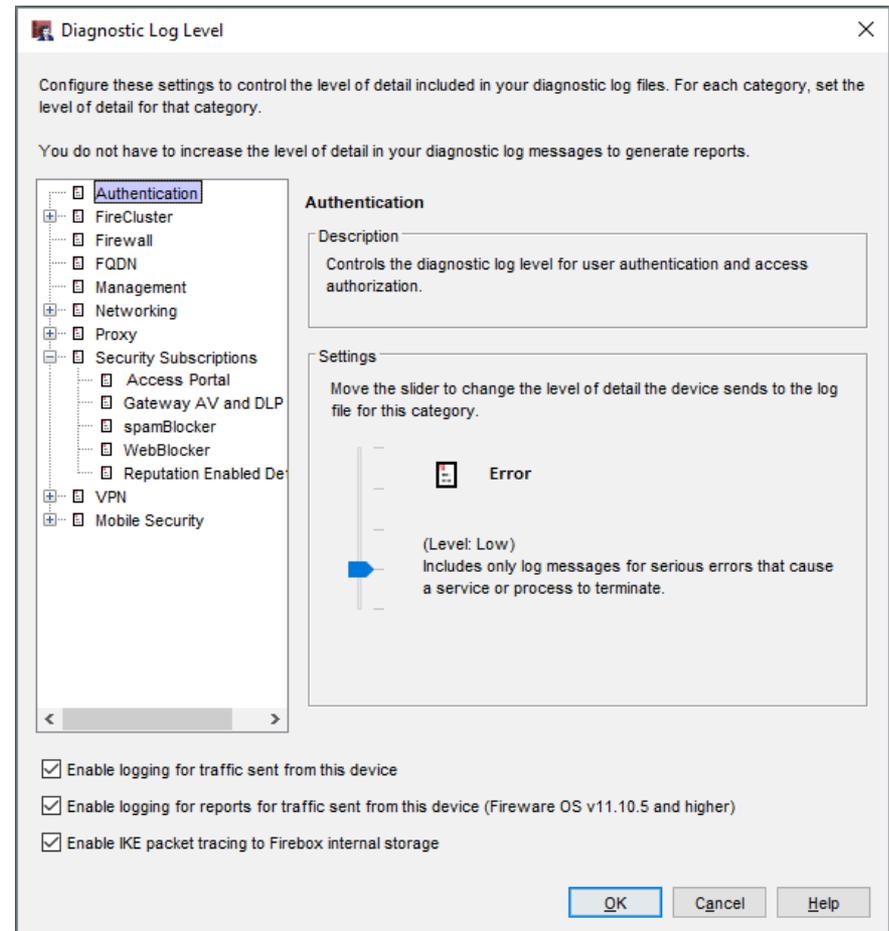
# Access Portal — Diagnostic Log Level

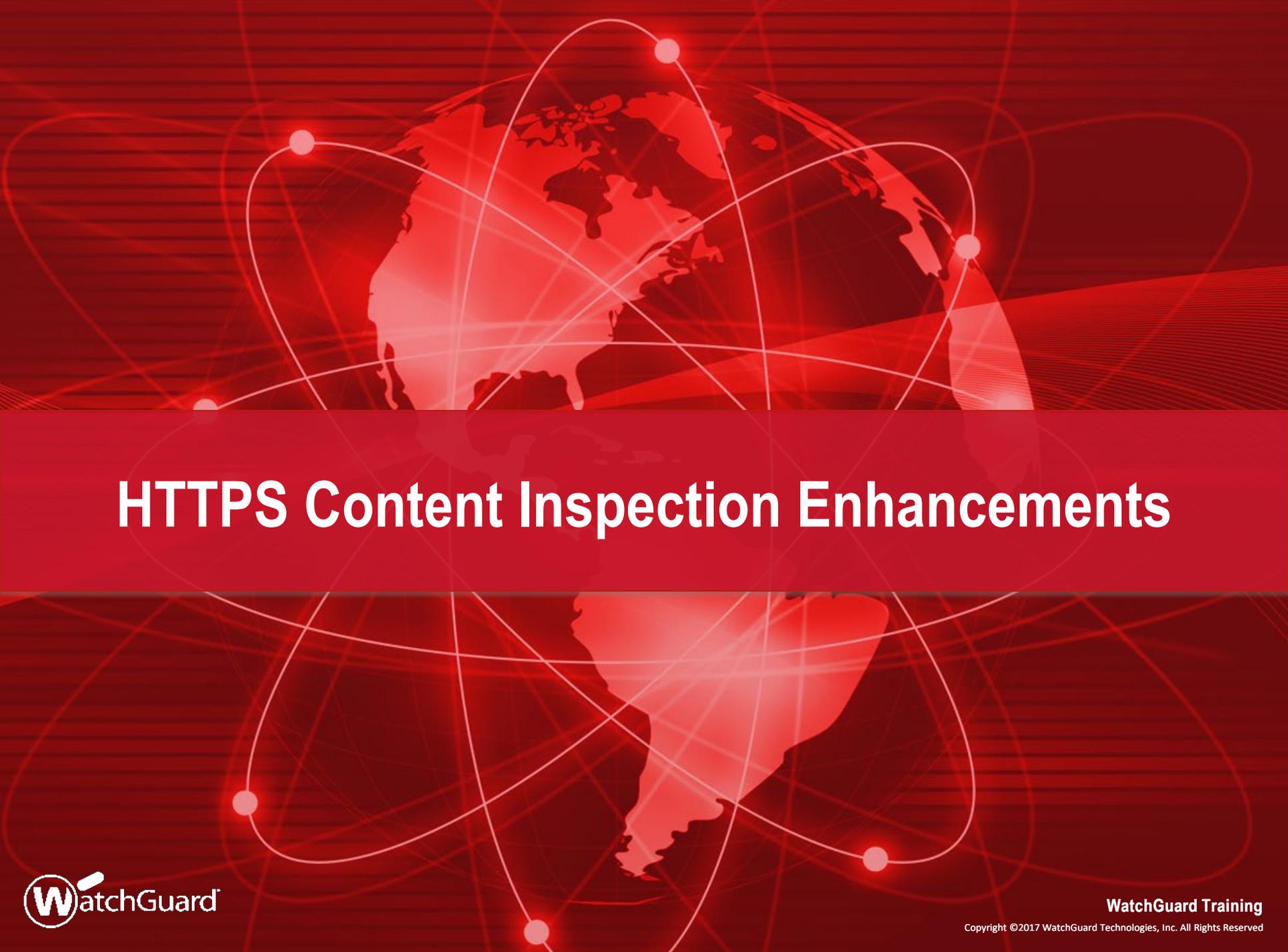
- You can also set the diagnostic log level for Access Portal connections
- Fireware Web UI:
  1. Select **System > Diagnostic Log**
  2. In the **Subscription Services** section, select the log level for the **Access Portal** option



# Access Portal — Diagnostic Log Level

- Policy Manager:
  1. Select **Setup > Logging > Diagnostic Log Level**
  2. Expand **Security Services** and select **Access Portal**
  3. This option is also available in Device Configuration Templates





# HTTPS Content Inspection Enhancements

# Content Inspection Exceptions List

- Messaging applications and proxying technologies have led the way in non-standard HTTPS traffic
- This can lead to problems for SSL inspection, which often burdens the IT administrator with error messages and cumbersome troubleshooting experiences
- The Content Inspection Exceptions List is a predefined list of noncompliant, SSL-based, web applications that makes it easy to enable the HTTPS proxy with minimal interference in the end-user browsing experience, or a burden on the IT administrator

# Content Inspection Exceptions List

- In the HTTPS-Client proxy action, the HTTPS Content Inspection settings now include a Predefined HTTPS Content Inspection Exceptions List
  - When Content Inspection is enabled, the HTTPS proxy does not inspect traffic for domains in the Predefined Exception List
  - The predefined list includes domain names associated with services that do not function correctly when content inspection is enabled
- This change improves usability of HTTPS Content Inspection
  - The Predefined Exception List enables many services to function correctly when content inspection is enabled, without manual configuration of Domain Name rules

# Content Inspection Exceptions List

- When you enable Content Inspection in a proxy action, the Predefined Content Inspection Exceptions List is enabled by default
- If you do not want to allow connections to the domains in the exception list you can disable the entire exception list, or disable specific exceptions
  - To disable the predefined exceptions, clear the **Enable Predefined Content Inspection Exceptions** check box
  - To disable specific predefined exceptions, click **Manage Exceptions**, and then disable specific exceptions

# Content Inspection Exceptions List

- The Predefined Content Inspection Exceptions List includes domain names used by services such as:
  - Microsoft services — Office Online, Skype, Teams, Exchange, Sharepoint, Onedrive, Product Activation
  - Apple services — iTunes, iCloud, App Store
  - Adobe services — Creative Cloud, Sign
  - Other services — Facebook, LinkedIn, Dropbox, Okta
- In the Content Inspection settings, you can see and manage the list of predefined exceptions

# Content Inspection Exceptions List

- The Predefined Content Inspection Exceptions list is available with Fireware v12.1 and WatchGuard System Manager v12.1
- The predefined exceptions list is created and maintained by WatchGuard
  - You can enable or disable the predefined exceptions
  - You cannot add or remove exceptions
  - You can use Domain Name rules to specify the action for other domains you do not want to inspect

# HTTPS Proxy Action UI Updates

- Content Inspection — Firewall Web UI

Fireware Web UI
User: admin ?

[Proxy Actions](#) / [Edit](#)

🔒 *Click the lock to prevent further changes*

### HTTPS Proxy Action Settings

Name:

Description:

Content Inspection
WebBlocker
Proxy Alarm
General

### Content Inspection Summary

Inspection On
SSLv3 Disabled
OCSP Lenient
PES Ciphers Allowed
SSL Compliance Enforced
Google Apps Unrestricted
EDIT

Enable Predefined Content Inspection Exceptions.
 MANAGE EXCEPTIONS

### Domain Names

Allow or deny access to a site if the server name matches a configured domain name on this list. 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	ALARM	LOG
<input checked="" type="checkbox"/>	Allow	WatchGuard Services	Pattern Match	*.watchguard.com	N/A	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Allow	*.mojonetworks.cor	Pattern Match	*.mojonetworks.com	N/A	<input type="checkbox"/>	<input type="checkbox"/>

# HTTPS Proxy Action UI Updates

- Manage Content Inspection Exceptions

### Manage Content Inspection Exceptions ✕

This list includes domains for services that are known to be incompatible with content inspection. The HTTPS proxy does not perform content inspection for a domain when the content inspection exception is enabled.

Content inspection exceptions are shared by all HTTPS proxy actions that have predefined content inspection exceptions enabled.

Show all domain names ▼

<input type="checkbox"/>	STATUS	DOMAIN NAMES	SERVICES
<input type="checkbox"/>	Enabled	*.dropbox.com	Dropbox
<input type="checkbox"/>	Enabled	*.okta.com	Okta
<input type="checkbox"/>	Enabled	*.oktacdn.com	Okta
<input type="checkbox"/>	Enabled	*.skype.net	Skype;Skype Mobile
<input type="checkbox"/>	Enabled	*.skype.com	Skype;Skype Mobile;Microsoft Teams
<input type="checkbox"/>	Enabled	*.dc.trouter.io	Skype;Skype Mobile;Microsoft Teams
<input type="checkbox"/>	Enabled	*.skype.cloudapp.net	Skype Mobile
<input type="checkbox"/>	Enabled	*.whatsapp.net	WhatsApp Mobile;WhatsApp Desktop
<input type="checkbox"/>	Enabled	*.web.whatsapp.com	WhatsApp Desktop
<input type="checkbox"/>	Enabled	*.update.microsoft.com	Microsoft Update
<input type="checkbox"/>	Enabled	*.settings-win.data.microsoft.com	Microsoft Update
<input type="checkbox"/>	Enabled	*.vortex-win.data.microsoft.com	Microsoft Update

SELECT ACTION ▼ SAVE CANCEL

# HTTPS Proxy Action UI Updates

- Content Inspection — Policy Manager

HTTPS Proxy Action Configuration (predefined)

Name:

Description:

Categories

- Content Inspection
- WebBlocker
- General Settings

**Content Inspection Summary**

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

Enable Predefined Content Inspection Exceptions. (Fireware OS v12.1 and higher)

**Domain Names**

Allow or deny access to a site if the server name matches a configured domain name on this list. 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.

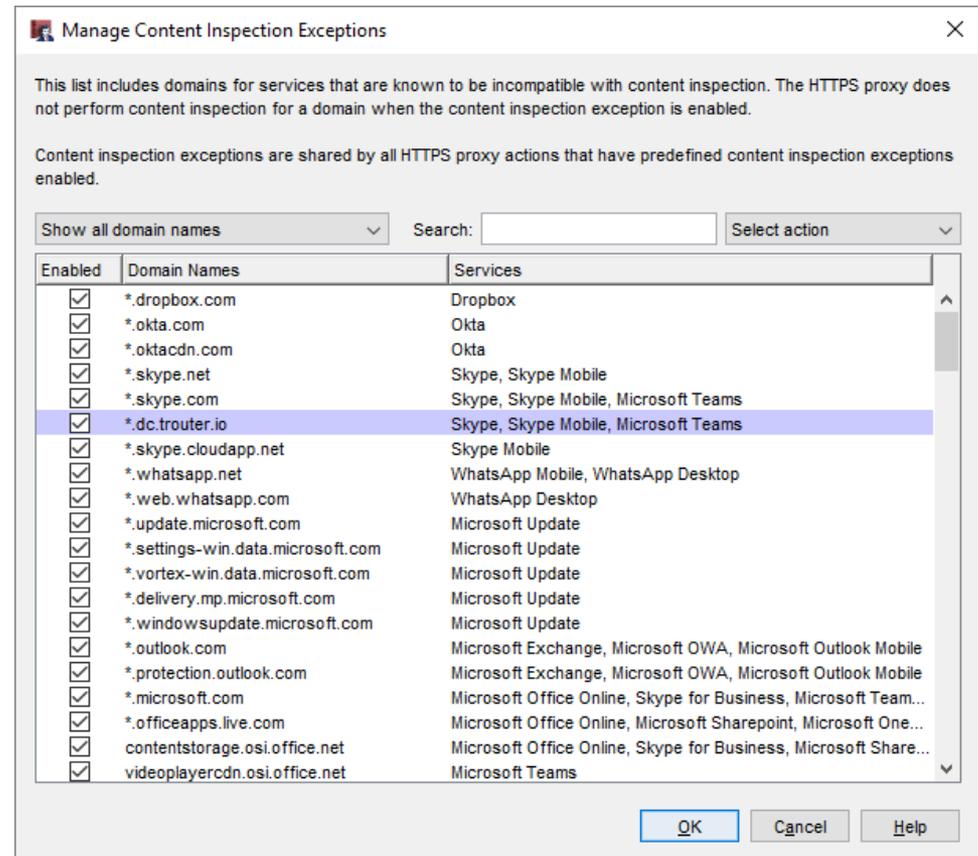
Enabled	Action	Name	Match Type	Value	Proxy Action	Routing Ac...	Port	Alarm	Log
<input checked="" type="checkbox"/>	Allow	WatchGuard Ser...	Pattern Match	*.watchguard.com	N/A	N/A	N/A	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Allow	*.mojonetworks.c...	Pattern Match	*.mojonetworks....	N/A	N/A	N/A	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Allow	*.cloudwifi.com	Pattern Match	*.cloudwifi.com	N/A	N/A	N/A	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Allow	redirector.online....	Pattern Match	redirector.online....	N/A	N/A	N/A	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Allow	*.airtightnetworks...	Pattern Match	*.airtightnetwork...	N/A	N/A	N/A	<input type="checkbox"/>	<input type="checkbox"/>

Action to take if no rule above is matched

Action:   Alarm  Log

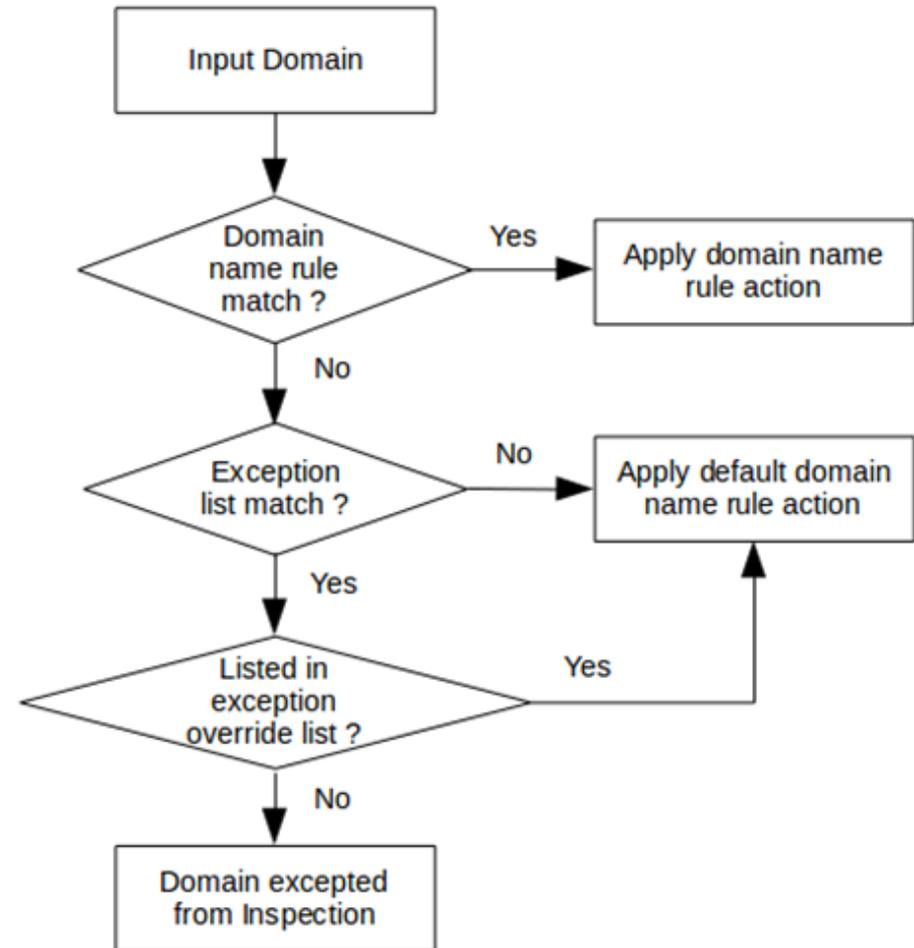
# HTTPS Proxy Action UI Updates

- To disable an exception, clear the **Enabled** check box
- To enable or disable multiple exceptions:
  - Select one or more domain names
  - Select the action **Enable** or **Disable**



# HTTPS Proxy Flow Changes

- Domain name rules take higher precedence than any match in the predefined exception list
- If a domain name rule is matched, the action from that rule will always be applied

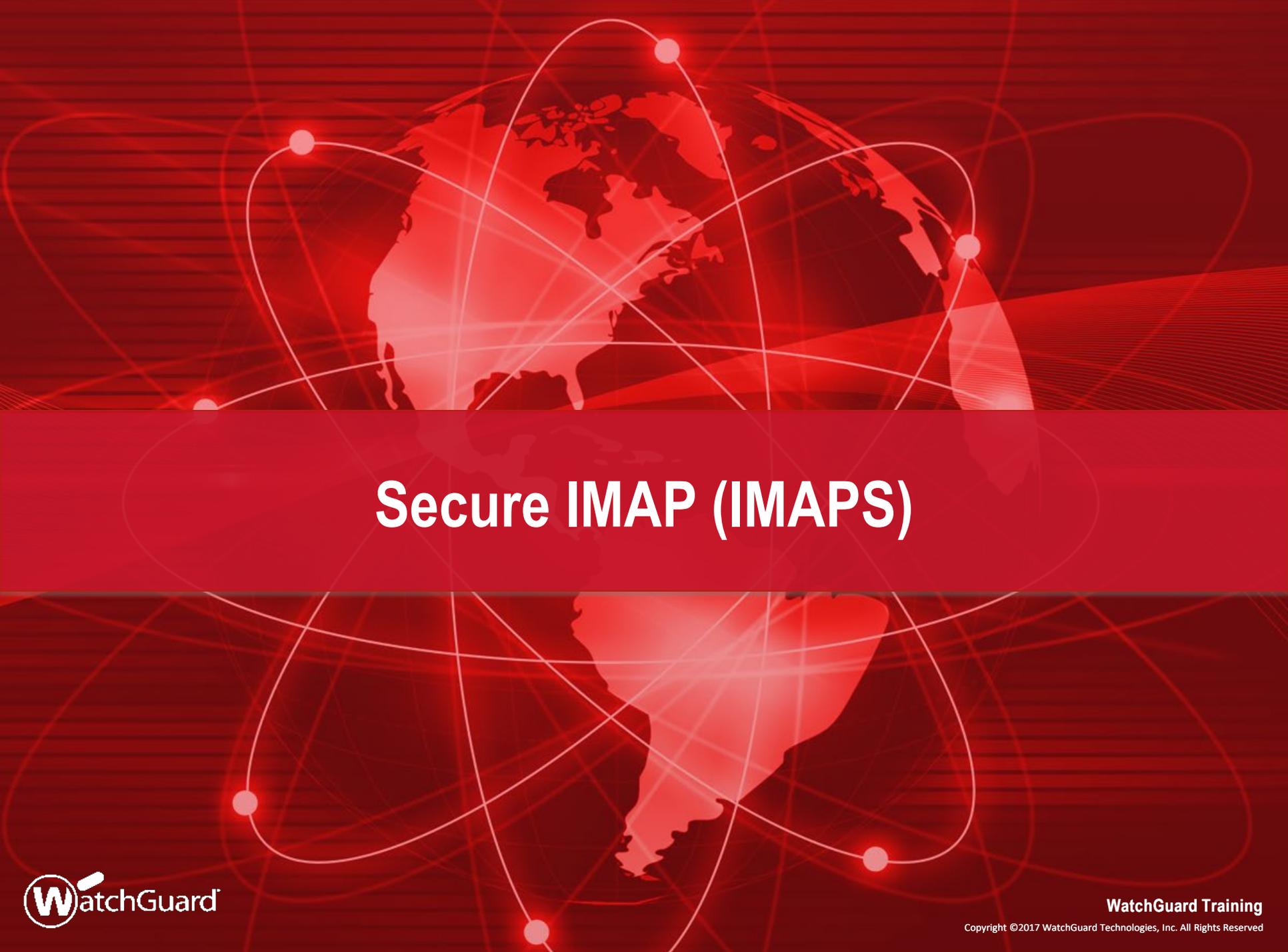


# Log Message Update

- A new traffic log message is generated when an exception list match occurs
- The log message text:

```
msg="ProxyAllow: HTTPS content inspection  
exception list match"
```

```
<ProxyMatch d="2017-09-18T18:37:38" orig="WatchGuard-XTM" cname="" proc_id="https-proxy" pri="6" rc="590" seq="34405" disp="Allow" msg_id="2CFF-0  
00A" src_intf="1-Trusted" dst_intf="0-External" policy="HTTPS-proxy-00" src_ip="10.0.1.2" dst_ip="162.125.1.1" src_port="36419" dst_port="443" pr  
="https/tcp" msg="ProxyAllow: HTTPS content inspection exception list match" proxy_act="HTTPS-Client.Standard.1" sni="www.dropbox.com" cn="" exce  
ption_rule="*.dropbox.com" action="allow" geo_dst="USA" log_type="tr"/>
```



# Secure IMAP (IMAPS)

# Secure IMAP (IMAPS)

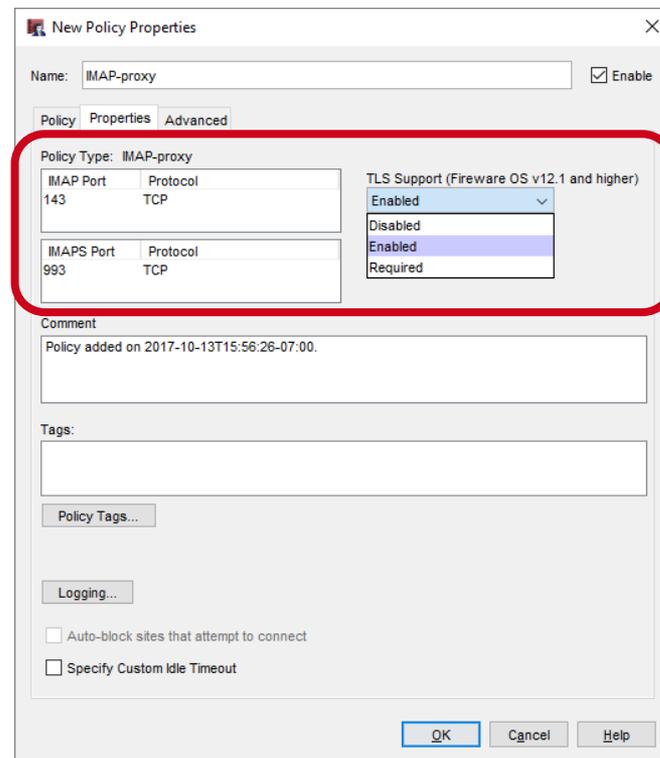
- IMAP is an alternative to SMTP for mail traffic among popular email vendors (Apple, Google, etc.)
- Secure IMAP (IMAPS) is an SSL-compliant proxy solution for the IMAP protocol
- The IMAP proxy and TCP-UDP proxy now support Secure IMAP (IMAPS)
  - The IMAP proxy supports:
    - IMAP on TCP port 143
    - IMAP over TLS on TCP port 993 (new)
- STARTTLS is not supported

# Secure IMAP (IMAPS)

- Options for enabling SSL inspection are:
  - IPS
  - URL filtering
  - App Control for IMAP — A protocol regularly used for Apple iOS, Gmail, and other mail service providers

# TLS Support in the IMAP Proxy

- New **TLS Support** option on the IMAP policy **Properties** tab:
  - **Disabled** — IMAP proxy listens on port 143 only
  - **Enabled** (default ) — IMAP proxy listens on ports 143 and 993
  - **Required** — IMAP proxy listens on port 993 only
- The **Port** list is updated based on the configured TLS Support option



# IMAP Proxy Action TLS Settings

- IMAP proxy actions now include a TLS category
  - TLS settings are configurable only when TLS Support is set to **Enabled** or **Required** in the IMAP policy **Properties** tab
- The TLS settings in the proxy action include:
  - **TLS Profile**
  - **Action**

The screenshot shows a configuration window titled "Clone IMAP Proxy Action Configuration". The "Name" field is "IMAP-Client.Standard.1" and the "Description" is "Guard recommended standard configuration for IMAP-Client with logging enabled".

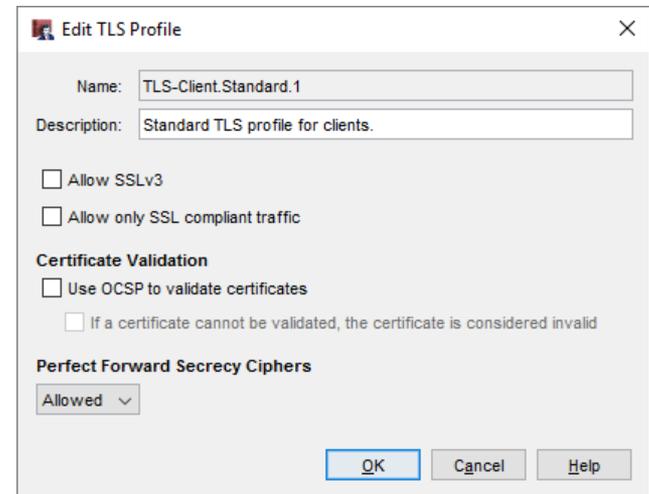
On the left, a "Categories" tree is shown with "TLS" selected. The main area is titled "TLS" and contains a "Content Inspection Summary (Fireware OS v12.1 and higher)" box. Inside this box, the "TLS Profile" is set to "TLS-Client.Standard". Below this, the status is shown as: "SSLv3 Disabled", "OCSP Disabled", "PFS Ciphers Allowed", and "SSL Compliance Not enforced".

Below the summary box, the "Action" is set to "Inspect" (with a dropdown menu showing "Allow" and "Inspect" options). There are checkboxes for "Alarm" (unchecked) and "Log" (checked).

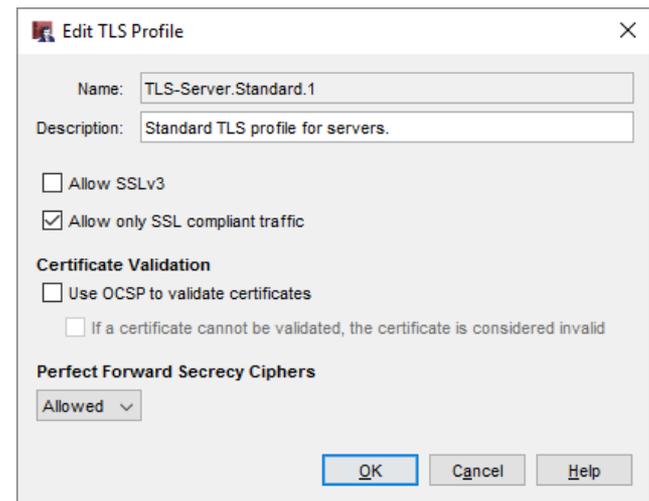
At the bottom right, there are "OK", "Cancel", and "Help" buttons.

# TLS Profiles

- A TLS Profile is a collection of TLS-related security settings:
  - Allow SSLv3
  - Allow only SSL compliant traffic
  - Certificate Validation (OCSP)
  - Perfect Forward Secrecy Ciphers
- TLS profiles and default settings are client and server specific
- You can select the same TLS profile in more than one IMAP proxy action



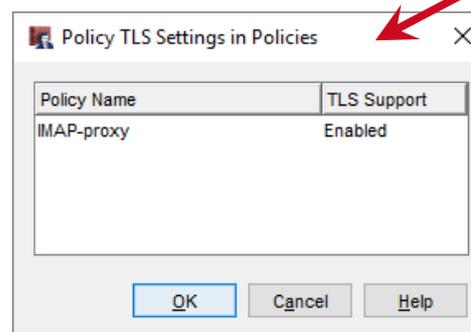
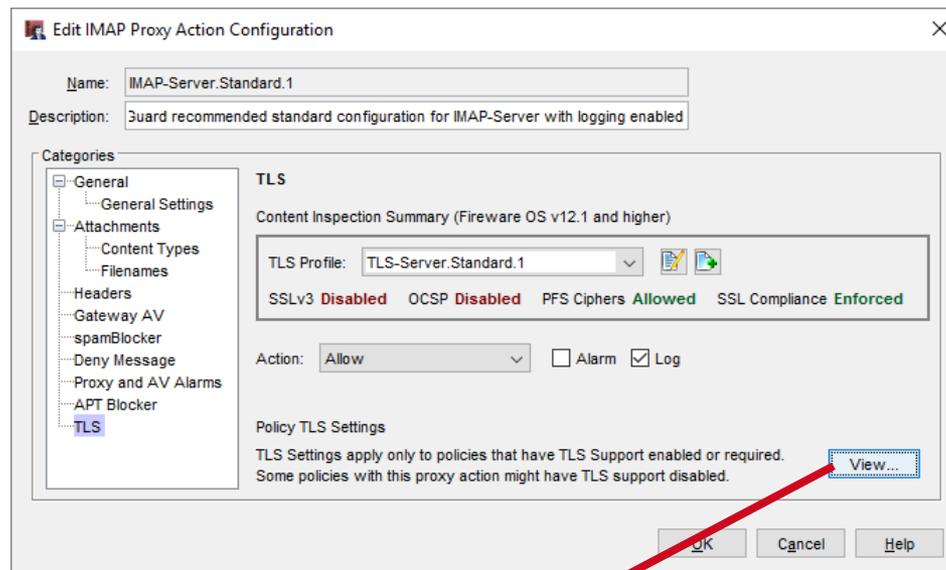
The screenshot shows the 'Edit TLS Profile' dialog box for a client profile. The 'Name' field is 'TLS-Client.Standard.1' and the 'Description' is 'Standard TLS profile for clients.' The 'Allow SSLv3' checkbox is unchecked. The 'Allow only SSL compliant traffic' checkbox is also unchecked. Under 'Certificate Validation', the 'Use OCSP to validate certificates' checkbox is unchecked, and the sub-option 'If a certificate cannot be validated, the certificate is considered invalid' is checked. Under 'Perfect Forward Secrecy Ciphers', the dropdown menu is set to 'Allowed'. The 'OK', 'Cancel', and 'Help' buttons are at the bottom right.



The screenshot shows the 'Edit TLS Profile' dialog box for a server profile. The 'Name' field is 'TLS-Server.Standard.1' and the 'Description' is 'Standard TLS profile for servers.' The 'Allow SSLv3' checkbox is unchecked. The 'Allow only SSL compliant traffic' checkbox is checked. Under 'Certificate Validation', the 'Use OCSP to validate certificates' checkbox is unchecked, and the sub-option 'If a certificate cannot be validated, the certificate is considered invalid' is checked. Under 'Perfect Forward Secrecy Ciphers', the dropdown menu is set to 'Allowed'. The 'OK', 'Cancel', and 'Help' buttons are at the bottom right.

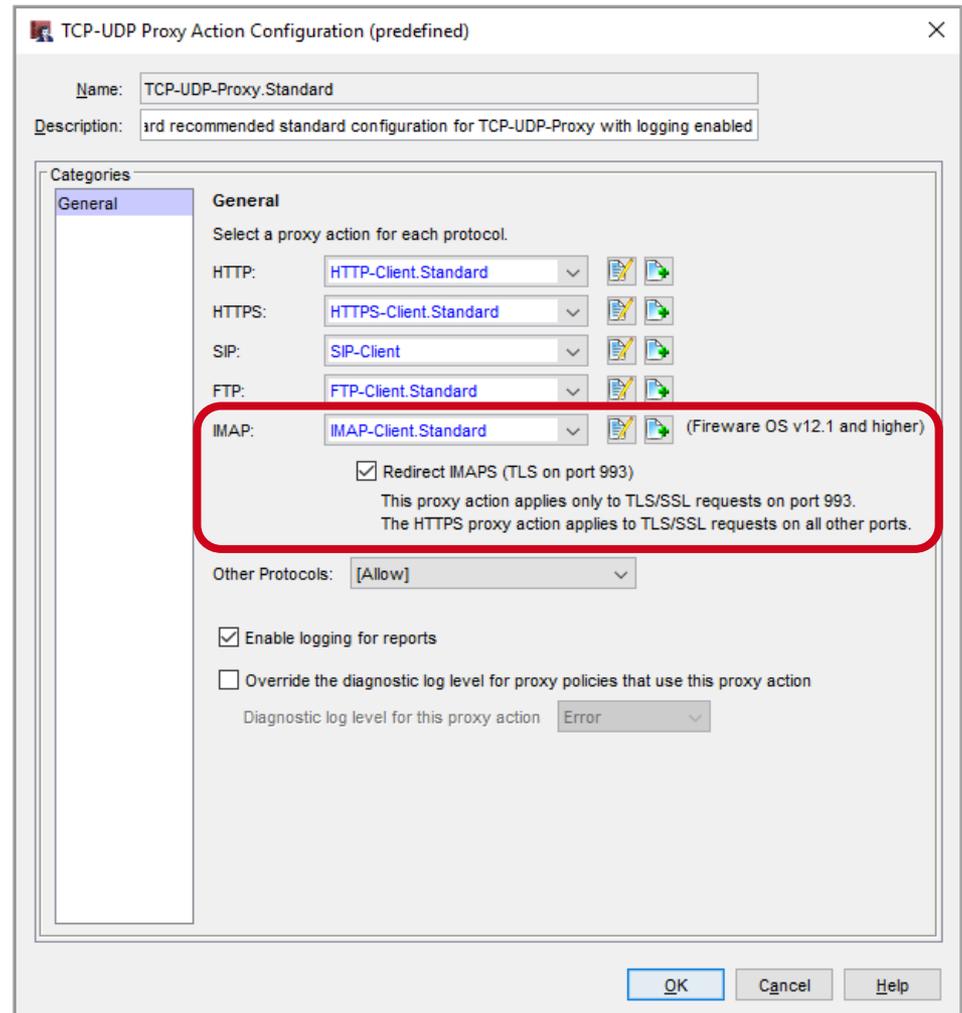
# IMAP Proxy Action TLS Settings

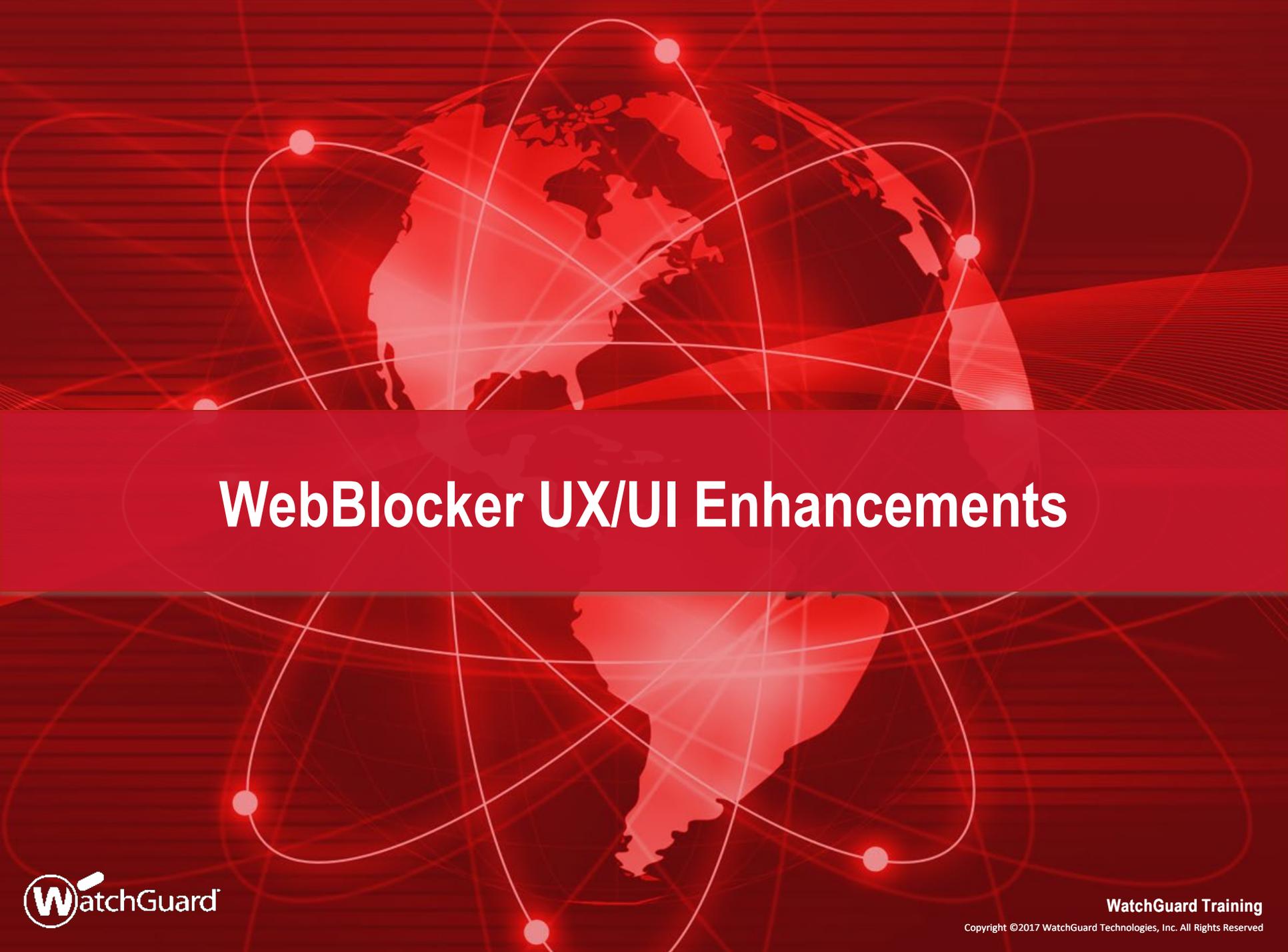
- An IMAP proxy action can apply to more than one policy
  - TLS settings apply only when TLS Support is enabled or required in a policy
  - If you edit the proxy action from the **Proxy Actions** list, click **View** to see the TLS settings for all policies that use the proxy action



# TCP/UDP Proxy

- TCP-UDP proxy action now supports IMAP
  - Select an **IMAP-Client** proxy action, or select **Allow** or **Deny**
  - The IMAP proxy action applies only to TLS/SSL requests on port 993
  - The HTTPS proxy action applies to TLS/SSL requests on all other ports





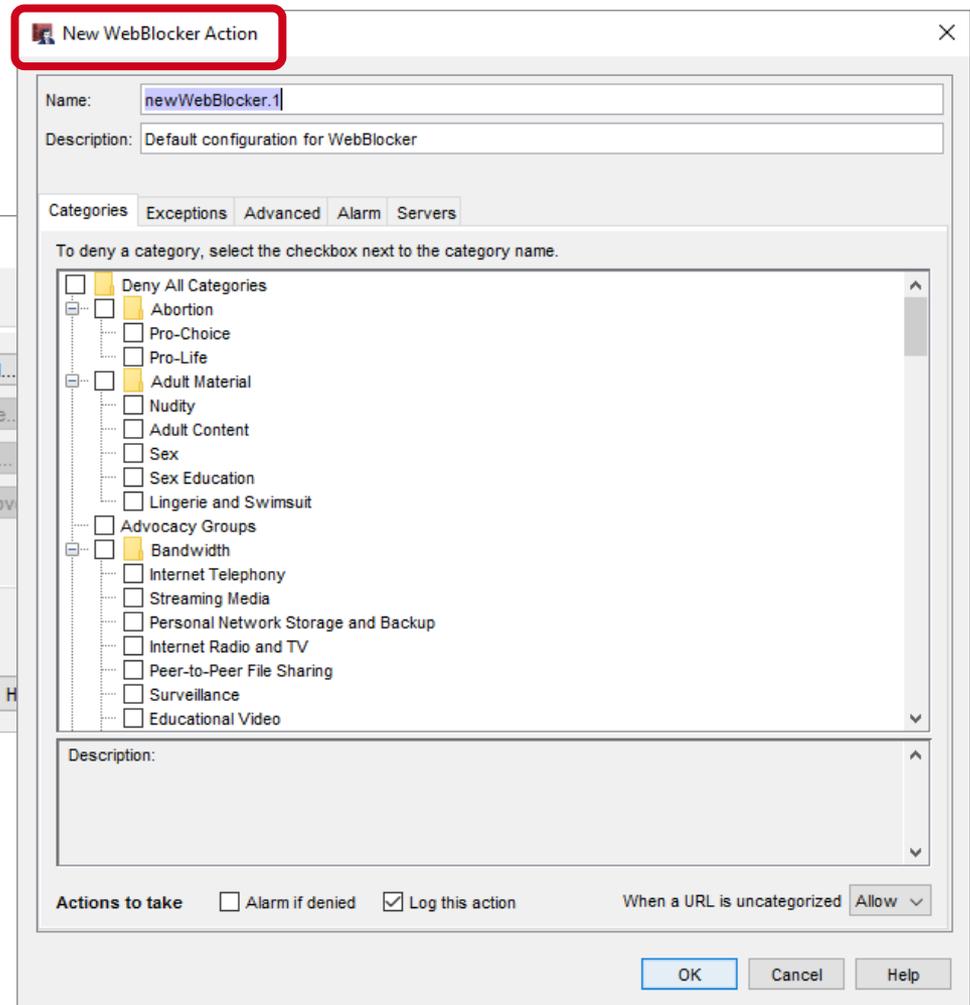
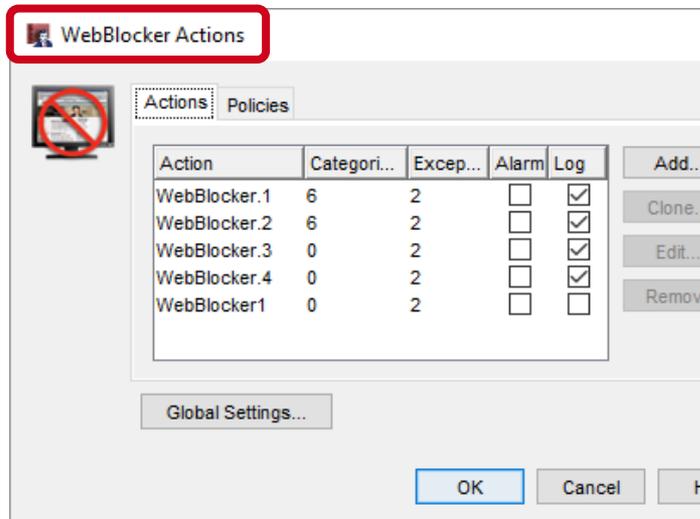
# WebBlocker UX/UI Enhancements

# WebBlocker UX/UI Enhancements

- WebBlocker has been updated to have more consistent terminology — WebBlocker Action
  - *WebBlocker Profile* changed to *WebBlocker Action*
  - *WebBlocker Configurations* changed to *WebBlocker Actions*
  - *New/Edit/Clone WebBlocker Configuration* changed to *New/Edit/Clone WebBlocker Action*

# WebBlocker UX/UI Enhancements

- Consistent terminology — *WebBlocker Action*



# WebBlocker UX/UI Enhancements

- Action changed from *Block* to *Deny*

The image displays two overlapping windows of the 'Activate WebBlocker Wizard' interface. The background window shows the 'Block' configuration screen, and the foreground window shows the 'Deny' configuration screen. A red arrow points from the 'Select categories to block' label in the background to the 'Select categories to deny' label in the foreground, illustrating the change in action.

**Background Window (Block Configuration):**

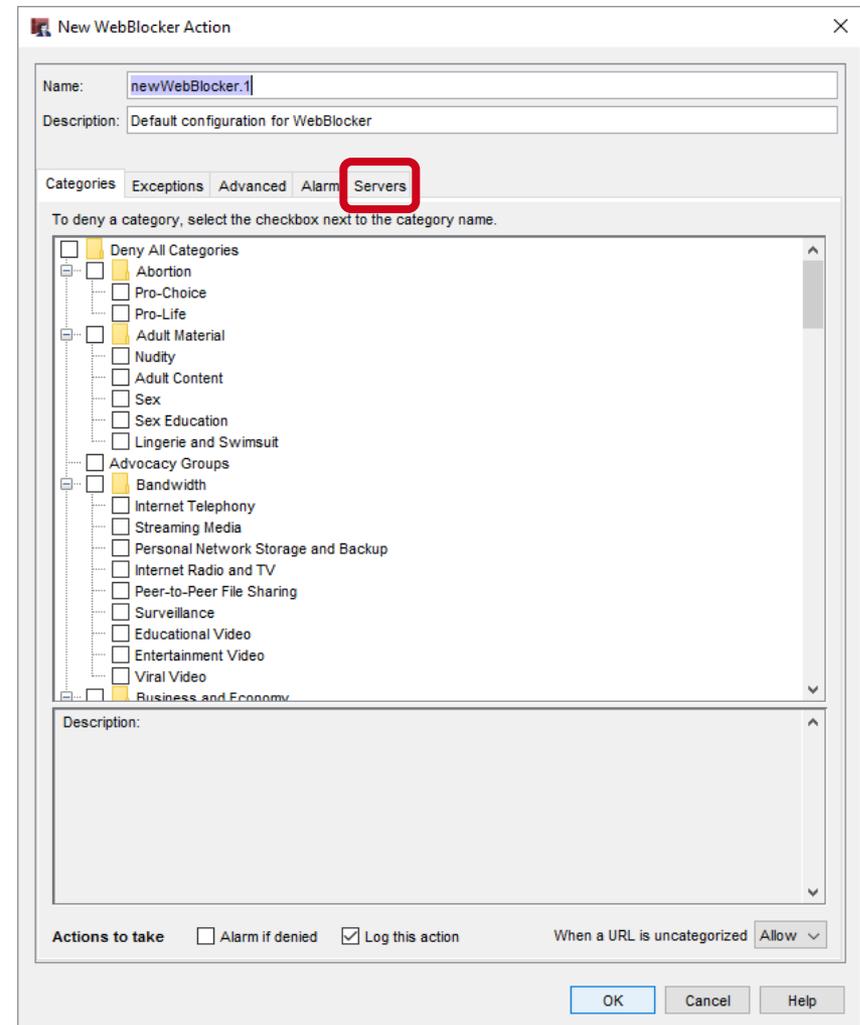
- Title: Activate WebBlocker Wizard
- Section: Select categories to block
- Instruction: To block a category, select the checkbox next to the category name.
- Categories (all unchecked):
  - Deny All Categories
  - Abortion
    - Pro-Choice
    - Pro-Life
  - Adult Material
    - Nudity
    - Adult Content
    - Sex
    - Sex Education
    - Lingerie and Swimsuit
  - Advocacy Groups
  - Bandwidth
  - Internet Telephony
- Description: [Empty text area]
- When a URL is uncategorized: Allow
- Buttons: Help, < Back, Next >, Cancel

**Foreground Window (Deny Configuration):**

- Title: Activate WebBlocker Wizard
- Section: Select categories to deny
- Instruction: To deny a category, select the checkbox next to the category name.
- Categories (all unchecked):
  - Deny All Categories
  - Abortion
    - Pro-Choice
    - Pro-Life
  - Adult Material
    - Nudity
    - Adult Content
    - Sex
    - Sex Education
    - Lingerie and Swimsuit
  - Advocacy Groups
  - Bandwidth
  - Internet Telephony
- Description: [Empty text area]
- When a URL is uncategorized: Allow
- Buttons: Help, < Back, Next >, Cancel

# WebBlocker UX/UI Enhancements

- The **Servers** tab has moved to the far right



# WebBlocker UX/UI Enhancements

- Improvements to the **New/Edit WebBlocker Exception** dialog box include additional descriptive information on pattern match and wildcards

**New WebBlocker Exception**

Name:   Enabled

Action:   Alarm  Log

Exception

Match Type:

Type:

Pattern:

Example: www.somesite.com/\* or www.\*.com:8080/\*

**Additional Information**

When you use a pattern match:

- Make sure the pattern you enter does not include http://.
- Use the wildcard symbol, \*, to match any character.
- You can use more than one wildcard in one pattern.

For example, the pattern, www.somesite.com/\* will match all URL paths on the www.somesite.com web site.

For more information and examples, click [Help](#).

# WebBlocker UX/UI Enhancements

- Improved WebBlocker wizard

Activate WebBlocker Wizard

Select a name for the WebBlocker action

The name is used to identify this WebBlocker action for later application to a proxy action.

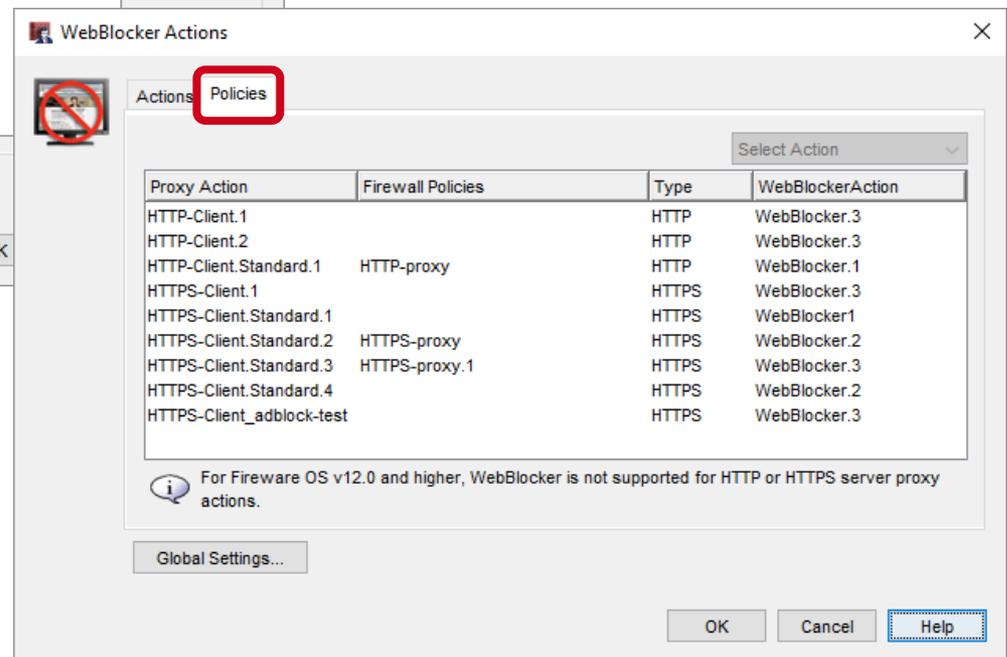
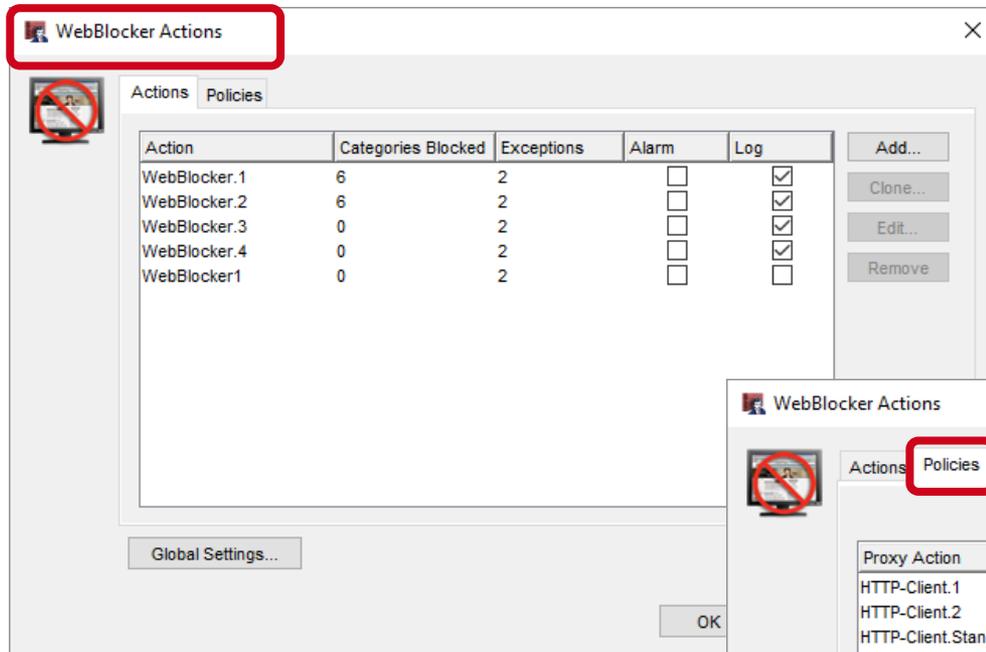
Name:

Help < Back Next > Cancel

# WebBlocker UX/UI Enhancements

- Completely revised WebBlocker dialog box
- Old **Configure WebBlocker** dialog box renamed to **WebBlocker Actions**
- From the **Policy** tab, multiple policies can be selected to apply the actions

# WebBlocker UX/UI Enhancements





# Mobile VPN with SSL

# Mobile VPN with SSL Portal Updates

- Mobile VPN with SSL and the Access Portal share the new VPN Portal settings
- To configure these settings for Mobile VPN with SSL, on the **Authentication** tab, click **Configure**

Mobile VPN with SSL

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

Activate Mobile VPN with SSL

General Authentication **Advanced**

### Authentication Server Settings

Auto reconnect after a connection is lost

Force users to authenticate after a connection is lost

Allow the Mobile VPN with SSL client to remember password

Define users and groups to authenticate with Mobile VPN with SSL. The users and groups you define are automatically included in the "SSLVPN-Users" group.

<input type="checkbox"/>	NAME	TYPE	AUTHENTICATION SERVER
<input type="checkbox"/>	SSLVPN-Users	Group	Any

[ADD](#) [REMOVE](#)

### VPN Portal

**Interface for connections:**  
Any-External

**Authentication Servers:**  
Firebox-DB

**CONFIGURE**

**SAVE**

# Mobile VPN with SSL Portal Updates

- The **Configuration Channel** setting for Mobile VPN with SSL moved to the VPN Portal settings and is now named **VPN Portal port**

Mobile VPN with SSL / VPN Portal

General

### Authentication Servers

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

AUTHENTICATION SERVER	
Firebox-DB	

Firebox-DB ▼ **ADD** REMOVE MOVE UP MOVE DOWN

### Interfaces

Specify the interfaces for connections to the VPN Portal. These interfaces will appear in the "WG-VPN-Portal" alias. The "WG-VPN-Portal" alias is used in the "WatchGuard SSLVPN" policy.

INTERFACE	
Any-External	

Any-External ▼ **ADD** REMOVE

### VPN Portal Port

Specify the VPN Portal Port. This is the configuration port shared by Mobile SSL VPN Clients and users of the Access Portal.

VPN Portal Port 443

**SAVE** **CANCEL**

# Mobile VPN with SSL Portal Updates

- The **Data Channel** setting for Mobile VPN with SSL remains in the Mobile VPN with SSL settings

Mobile VPN with SSL

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

Activate Mobile VPN with SSL

General Authentication Advanced

Authentication SHA-256

Encryption AES (256-bit)

Data channel TCP 443

Keep-Alive Interval 11 seconds

Keep-Alive Timeout 60 seconds

Renegotiate Data Channel 480 minutes

# Mobile VPN with SSL Portal Updates

- The TCP Data Channel for Mobile VPN with SSL takes precedence over the VPN Portal port
- If you change the TCP Data Channel for Mobile VPN with SSL, the VPN Portal Port changes to the same port

Activate Mobile VPN with SSL

General	Authentication	Advanced
Authentication	SHA-256	
Encryption	AES (256-bit)	
Data channel	TCP	444

VPN Portal Port

Specify the VPN Portal Port. This is the configuration port shared by Mobile SSL VPN Clients and users of the Access Portal.

The TCP data channel port for Mobile VPN with SSL has precedence over the VPN Portal port. To set the Mobile VPN with SSL port, [click here](#).

VPN Portal Port 444

# Mobile VPN with SSL Portal Updates

- If you change the UDP Data Channel for Mobile VPN with SSL, the VPN Portal Port is not affected

Activate Mobile VPN with SSL

General	Authentication	Advanced
Authentication	SHA-256	
Encryption	AES (256-bit)	
Data channel	UDP	444

VPN Portal Port

Specify the VPN Portal Port. This is the configuration port shared by Mobile SSL VPN Clients and users of the Access Portal.

VPN Portal Port 443

# Mobile VPN with SSL Portal Updates

- Interface and authentication server settings apply to both Mobile VPN with SSL and the Access Portal

Mobile VPN with SSL / VPN Portal

General

### Authentication Servers

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

<b>AUTHENTICATION SERVER</b>	
Firebox-DB	

Firebox-DB ▼ **ADD** REMOVE MOVE UP MOVE DOWN

### Interfaces

Specify the interfaces for connections to the VPN Portal. These interfaces will appear in the "WG-VPN-Portal" alias. The "WG-VPN-Portal" alias is used in the "WatchGuard SSLVPN" policy.

<b>INTERFACE</b> ↕	
Any-External	

Any-External ▼ **ADD** REMOVE

### VPN Portal Port

Specify the VPN Portal Port. This is the configuration port shared by Mobile SSL VPN Clients and users of the Access Portal.

VPN Portal Port

**SAVE** **CANCEL**

# Mobile VPN with SSL Portal Updates

- To download the client software for Mobile VPN with SSL, you must now go to:

`https://<host name or IP address>/sslvpn.html`

- The software downloads page for Mobile VPN with SSL is no longer available at:

`https://<host name or IP address>`

- The Access Portal now appears at:

`https://<host name or IP address>`



# Mobile VPN with IKEv2

# Mobile VPN with IKEv2

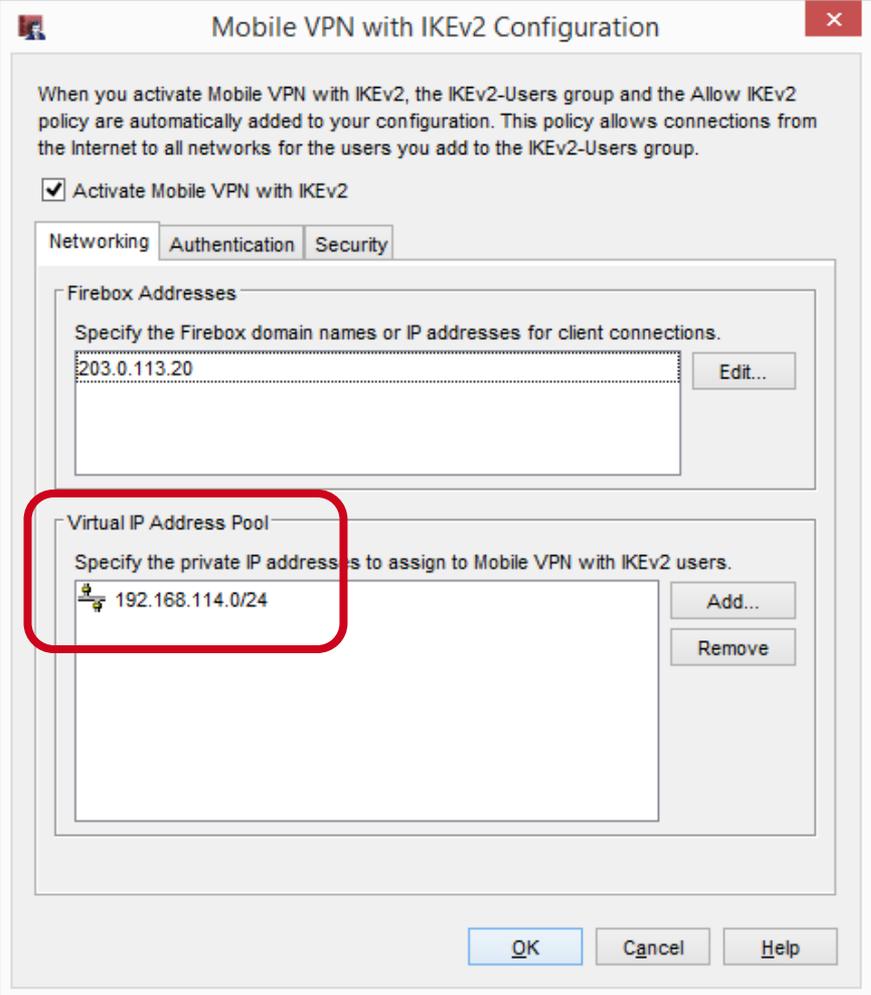
- IKEv2 is a tunneling protocol for IKEv2/IPSec VPNs
- You can now configure the native IKEv2 VPN clients on Windows, macOS, and iOS mobile devices rather than third-party clients
  - Mobile users can connect to corporate resources through an IKEv2/IPSec tunnel to the Firebox
- You can preconfigure corporate mobile devices for rollout or support BYOD scenarios
- Android users can connect with the free, third-party *strongSwan* app

# Mobile VPN with IKEv2

- You can configure Mobile VPN with IKEv2 on the Firebox manually or with a wizard
- Mobile VPN with IKEv2 sends all traffic over the VPN tunnel (full tunnel)
- Client devices control routing, not the Firebox
- The *IPSec VPN Users* value in the feature key is a combined limit for Mobile VPN with IKEv2 and Mobile VPN with IPSec
  - Example — If a feature key allows 250 IPSec VPN user connections, and 200 Mobile VPN with IPSec users are connected, 50 Mobile VPN with IKEv2 users can connect

# Mobile VPN with IKEv2

- When you enable Mobile VPN with IKEv2, the Firebox automatically assigns a default virtual IP address pool for IKEv2 users



**Mobile VPN with IKEv2 Configuration**

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

Activate Mobile VPN with IKEv2

Networking Authentication Security

**Firebox Addresses**

Specify the Firebox domain names or IP addresses for client connections.

203.0.113.20 Edit...

**Virtual IP Address Pool**

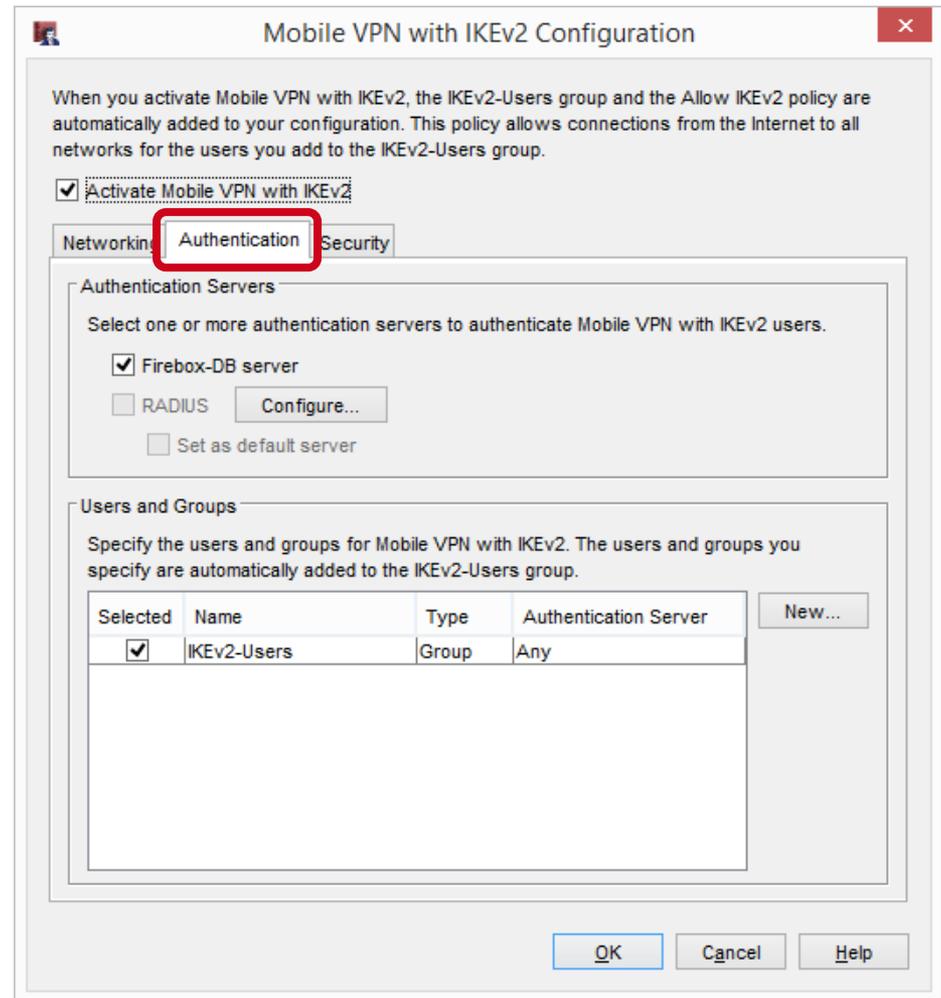
Specify the private IP addresses to assign to Mobile VPN with IKEv2 users.

192.168.114.0/24 Add... Remove

OK Cancel Help

# Mobile VPN with IKEv2

- The **Authentication** tab



Mobile VPN with IKEv2 Configuration

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

Activate Mobile VPN with IKEv2

Networking **Authentication** Security

**Authentication Servers**

Select one or more authentication servers to authenticate Mobile VPN with IKEv2 users.

Firebox-DB server  
 RADIUS   
 Set as default server

**Users and Groups**

Specify the users and groups for Mobile VPN with IKEv2. The users and groups you specify are automatically added to the IKEv2-Users group.

Selected	Name	Type	Authentication Server	New...
<input checked="" type="checkbox"/>	IKEv2-Users	Group	Any	

# Mobile VPN with IKEv2

- You can select a Firebox certificate or a third-party certificate

**Mobile VPN with IKEv2 Configuration**

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

**Activate Mobile VPN with IKEv2**

Networking | Authentication | Security

Phase 1 | Phase 2

**Certificate**

Select a certificate type for client authentication.

Type: Firebox Generated Certificate

Common Name: o=WatchGuard ou=Fireware cn=ike2muvpn Server

**IKEv2 Shared Settings**

Phase 1 Transforms

Phase 1 Transform	Key Group
SHA2-256-AES (256-bit)	Diffie-Hellman Group14
SHA1-AES (256-bit)	Diffie-Hellman Group5
SHA1-AES (256-bit)	Diffie-Hellman Group2
SHA1-3DES	Diffie-Hellman Group2

These IKEv2 settings are shared by all IKEv2 gateways on your Firebox that have at least one Remote Gateway with a dynamic IP address. This includes BOVPN Gateways and BOVPN virtual interfaces.

To change these settings, click Edit

**Firebox Address and Certificate Settings**

Select a certificate type for client authentication.

Type: Firebox-Generated Certificate

Specify Third-Party Certificate for client connections. This information will be included in the Firebox certificate.

# Mobile VPN with IKEv2

- Firebox and third-party certificates have these requirements:
  - Extended Key Usage (EKU) flags *serverAuth* and *IP Security IKE Intermediate* (OID 1.3.6.1.5.5.8.2.2)
  - IP address or DNS name as a Subject Alternative Name value

# Mobile VPN with IKEv2

- The policy for Mobile VPN with IKEv2 appears on the **Firewall** tab in the policy list

Firewall Mobile VPN with IPsec

Filter: N

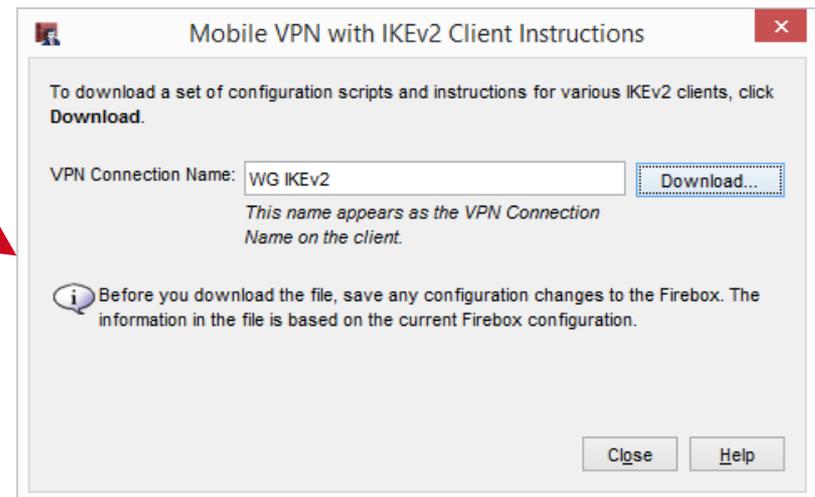
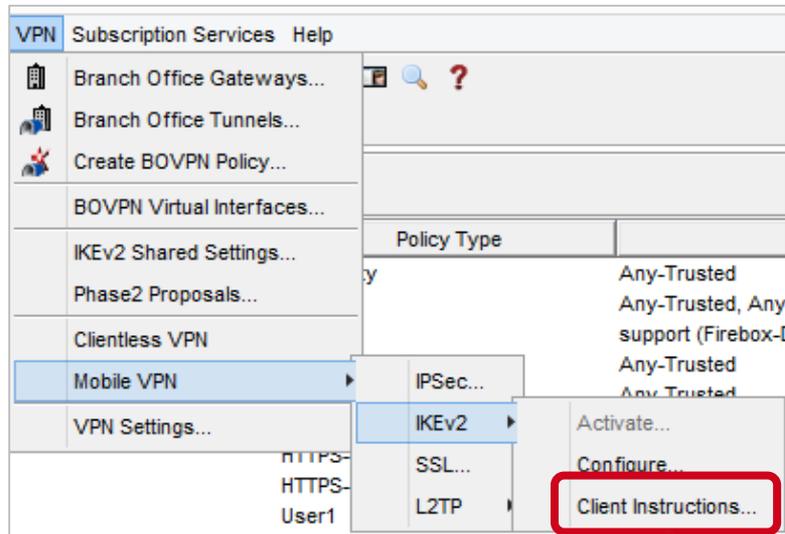
Order /	Action	Policy Name	Policy Type	From	To	Port
1	✓	FTP-proxy	FTP-proxy	Any-Trusted	Any-External	tcp:21
2	✓	FTP	FTP	Any-Trusted, Any-Optional	Any-External	tcp:21
3	✓	HTTP	HTTP	support (Firebox-DB)	Any-External	tcp:80
4	✓	HTTP-proxy	HTTP-proxy	Any-Trusted	Any-External	tcp:80
5	✓	POP3-proxy	POP3-proxy	Any-Trusted	Any-External	tcp:110
6	✓	WatchGuard SSLVPN	SSL-VPN	WG-VPN-Portal	Firebox	tcp:443
7	✓	HTTPS-proxy	HTTPS-proxy	Any-Trusted	Any-External	tcp:443
8	✓	HTTPS-proxy.1	HTTPS-proxy	Any-Trusted	Any-External	tcp:443
9	✓	User1	User1	User1	Any-External	tcp:666
10	✓	WatchGuard L2TP	L2TP	L2TP-IPsec	Firebox	udp:1701
11	✓	WatchGuard Gateway Wireless Controller	WG-Gateway-Wireless-Controller	Any-Trusted, Any-Optional	Firebox	udp:2529
12	✓	RDP-2-Mgmt-Svr_WkStn	RDP	Any-External	Any-External -->	192.168.tcp:3389
13	✓	WatchGuard Authentication	WG-Auth	Any-Trusted, Any-Optional	Firebox	tcp:4100
14	✓	WatchGuard Web UI	WG-Fireware-XTM-WebUI	Any-Trusted, Any-Optional, Any-External	Firebox	tcp:8080
15	✓	Ping	Ping	Any-Trusted, Any-Optional	Any	icmp (type: 8, code: 255)
16	✓	DNS-proxy	DNS-proxy	Any-Trusted	Any-External	tcp:53 udp:53
17	✓	DNS-proxy.1	DNS-proxy	Any-External	Any-Trusted	tcp:53 udp:53
18	✓	WG-Logging	WG-Logging	Any-External	Any-External -->	10.0.20.!:tcp:4107 tcp:4115
19	✓	WG-WebBlocker	WG-WebBlocker	Any-External	Any-External -->	10.0.20.!:tcp:5003 udp:5003
20	✓	WG-Mgmt-Server	WG-Mgmt-Server	Any-External	Any-External -->	192.168.tcp:4110 tcp:4112-4113
21	✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-Optional, Any-External	Firebox	tcp:4105 tcp:4117 tcp:4118
22	✓	WG-LogViewer-ReportMgr	WG-LogViewer-ReportMgr	Any-External	Any-External -->	10.0.20.!:tcp:4121 tcp:4122 tcp:4130
23	✓	Outgoing	TCP-UDP	Any-Trusted, Any-Optional	Any-External	tcp:0 (Any) udp:0 (Any)
24	✓	BOVPN-Allow.out	Any	Any	tunnel.seattle, Toronto.TL:!	any
25	✓	DVCP-BOVPN-Allow-out	Any	Any	XTM1050_10.Trusted Net:!	any
26	✓	Allow L2TP-Users	Any	L2TP-Users (Any)	Any	any
27	✓	Allow IKEv2-Users	Any	IKEv2-Users (Any)	Any	any

# Mobile VPN with IKEv2 — Client Instructions

- You can download a Client Instructions file from the Firebox that contains automatic configuration scripts and instructions for IKEv2 VPN clients in Windows, macOS, iOS, and Android
  - The client settings and the certificate are installed automatically by the script
  - You must save the Firebox configuration before the file is available to download

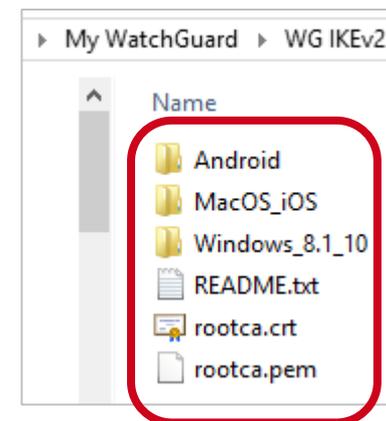
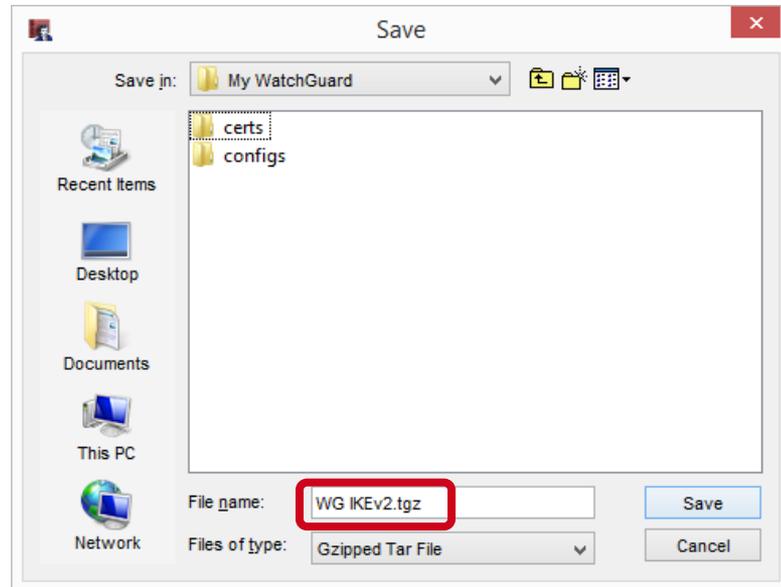
# Mobile VPN with IKEv2 — Client Instructions

- Download the **Client Instructions** from the Firebox



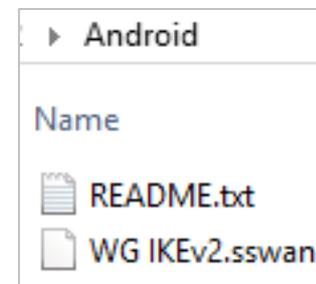
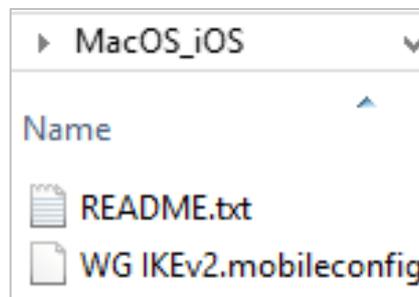
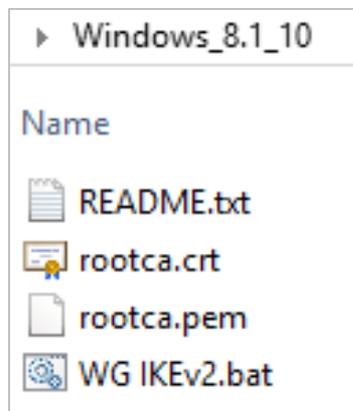
# Mobile VPN with IKEv2 — Client Instructions

- Save the .TGZ archive
- Extract the files from the .TGZ archive



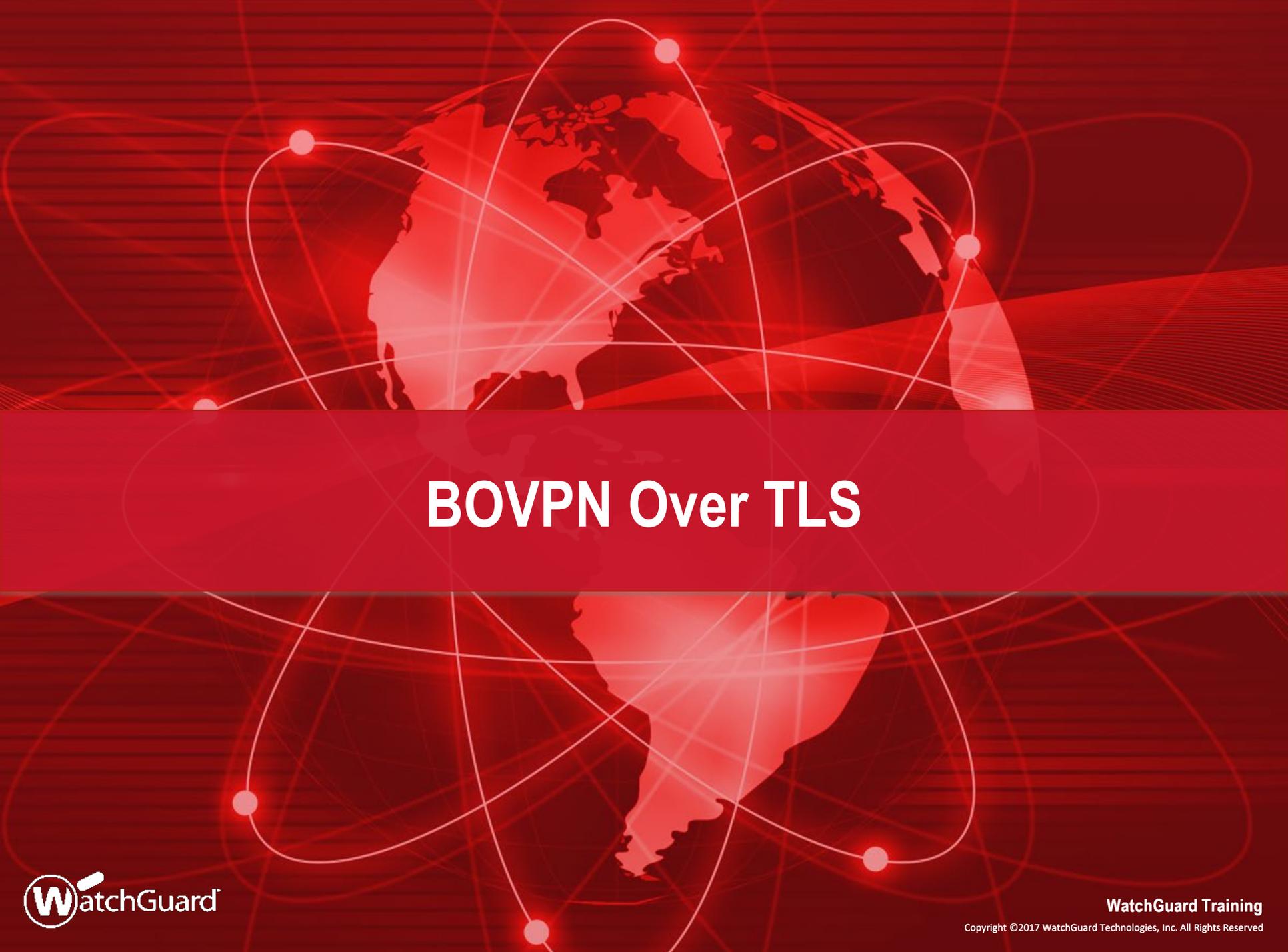
# Mobile VPN with IKEv2 — Client Instructions

- Each folder contains instructions and an automatic configuration script that are specific to your operating system



# Mobile VPN with IKEv2 — Client Instructions

- You can manually configure an IKEv2 VPN connection on your device rather than run the script
  - On your device, you must install the `rootca.pem` or `rootca.crt` files provided in the .TGZ download file to establish an IKEv2 VPN connection
  - Instructions for manual configuration are included in each folder in the .TGZ download file



# BOVPN Over TLS

# BOVPN Over TLS

- You can now enable a BOVPN over TLS tunnel between Fireboxes
- BOVPN over TLS uses port 443, which is typically open on networks
- This is recommended as an alternative BOVPN solution when:
  - Your business operates in a location where you do not have full network control, such as a shared office space or a shopping mall, and you cannot open ports required by our IPsec-based BOVPN
  - IPsec traffic is not correctly handled by your ISP, modem, or router, or is not allowed on your network

# BOVPN Over TLS

- BOVPN over TLS uses a client/server model
  - On a Firebox configured in Server mode, you can configure tunnels to one or more Fireboxes configured in Client mode
  - On a Firebox configured in Client mode, you can configure tunnels to one or more Fireboxes configured in Server mode
  - A Firebox cannot be configured as both a server and client
  - Supports only hub-and-spoke topologies
- BOVPN over TLS is supported only for Firebox endpoints
- In Fireware v12.1, BOVPN over TLS is available only in Fireware Web UI

# BOVPN Over TLS

- Enable Client Mode

Branch Office VPN over TLS

Enable Branch Office VPN over TLS to configure a hub-and-spoke VPN when IKE/IPSec traffic is not allowed.

Branch Office VPN over TLS is **Enabled In Client Mode**. Click to [Change Mode](#) or [Disable](#).

## Client Settings

BOVPN over TLS Servers

ENABLED	TUNNEL NAME	PRIMARY SERVER	DESCRIPTION
Yes	BovpnTLS.1	198.51.100.2	Tunnel to the Toronto TLS server

[ADD](#)

[EDIT](#)

[REMOVE](#)

# BOVPN Over TLS

- Configure Client mode

BOVPN over TLS (Client Mode) / Edit Server

Specify the connection settings for a BOVPN over TLS server that can create a tunnel with this BOVPN over TLS client.

Tunnel Name

Description  *Optional*

Enable

Specify the Firebox IP addresses or domain names for client connections.

Primary Server

Backup Server  *Optional*

For authentication, specify a Tunnel ID to identify this Firebox and a pre-shared key.

Tunnel ID

Pre-Shared Key

Advanced Options

Add this tunnel to the BOVPN-Allow policies

# BOVPN Over TLS

- The **Advanced Settings** dialog box contains the authentication and encryption settings
- The TCP data channel is permanently set to port 443
- To specify a port other than 443, you must select UDP
- The **Import configuration file** option is for testing purposes and will be removed in a future release

The image displays two screenshots of the 'Advanced Settings' dialog box. The top screenshot shows the 'Data channel' set to 'TCP' and port '443'. The bottom screenshot shows the 'Data channel' set to 'UDP' and port '443'. Both screenshots show other settings like 'Virtual IP Address Pool', 'Authentication', 'Encryption', 'Keep-Alive Interval', 'Keep-Alive Timeout', and 'Renegotiate Data Channel'.

Setting	Value
Virtual IP Address Pool	192.168.113.0 / 24
Authentication	SHA-256
Encryption	AES (256-bit)
Data channel	TCP / 443
Keep-Alive Interval	10 seconds
Keep-Alive Timeout	60 seconds
Renegotiate Data Channel	8 hours

Setting	Value
Virtual IP Address Pool	192.168.113.0 / 24
Authentication	SHA-256
Encryption	AES (256-bit)
Data channel	UDP / 443
Keep-Alive Interval	10 seconds
Keep-Alive Timeout	60 seconds
Renegotiate Data Channel	8 hours

# BOVPN Over TLS

- You can add tunnels to multiple TLS servers

Branch Office VPN over TLS

Enable Branch Office VPN over TLS to configure a hub-and-spoke VPN when IKE/IPSec traffic is not allowed.

Branch Office VPN over TLS is **Enabled in Client Mode**. Click to [Change Mode](#) or [Disable](#).

### Client Settings

BOVPN over TLS Servers

ENABLED 	TUNNEL NAME	PRIMARY SERVER	DESCRIPTION
Yes	BovpnTLS.1	198.51.100.2	Tunnel to the Toronto TLS server
Yes	BovpnTLS.2	192.0.2.2	Tunnel to the New York TLS server

[ADD](#) [EDIT](#) [REMOVE](#)

# BOVPN Over TLS

- You must also configure at least one Firebox in Server mode
- Enable Server mode

### BOVPN over TLS Mode ×

Specify the BOVPN over TLS mode. The Firebox can operate as a BOVPN over TLS client or a BOVPN over TLS server, but not both at the same time.

Firebox Mode

Specify the Firebox IP addresses or domain names for client connections.

Primary Server

Backup Server  *(Optional)*

# BOVPN Over TLS

## ■ Configure Server mode

BOVPN over TLS (Server Mode) / Add Client

Specify the connection settings for a BOVPN over TLS client that can create a tunnel with this Firebox.

Tunnel ID

Description  *Optional*

Pre-Shared Key

Enable

Client Routes

- Send all client traffic through the tunnel
- Specify the destination addresses that the client will route through the tunnel

Server Routes Specify the destination addresses that the server will route through the tunnel.

DESTINATION	METRIC
10.0.50.0/24	101

Add this tunnel to the BOVPN-Allow policies

# BOVPN Over TLS

- Configure Server mode

Branch Office VPN over TLS

Enable Branch Office VPN over TLS to configure a hub-and-spoke VPN when IKE/IPSec traffic is not allowed.

Branch Office VPN over TLS is **Enabled In Server Mode**. Click to [Change Mode](#) or [Disable](#).

### Server Settings

Specify the Firebox IP addresses or domain names for clients to connect to.

Primary Server  Backup Server

[EDIT](#)

Aliases for the BOVPN over TLS clients in this list are automatically created for use in firewall policies.

ENABLED 	TUNNEL ID	DESCRIPTION
Yes	TLSTunnel1	

[ADD](#) [EDIT](#) [REMOVE](#)

The BOVPN over TLS server is configured to use **TCP** port **443** and assign IP addresses to clients from **192.168.113.0/24**.

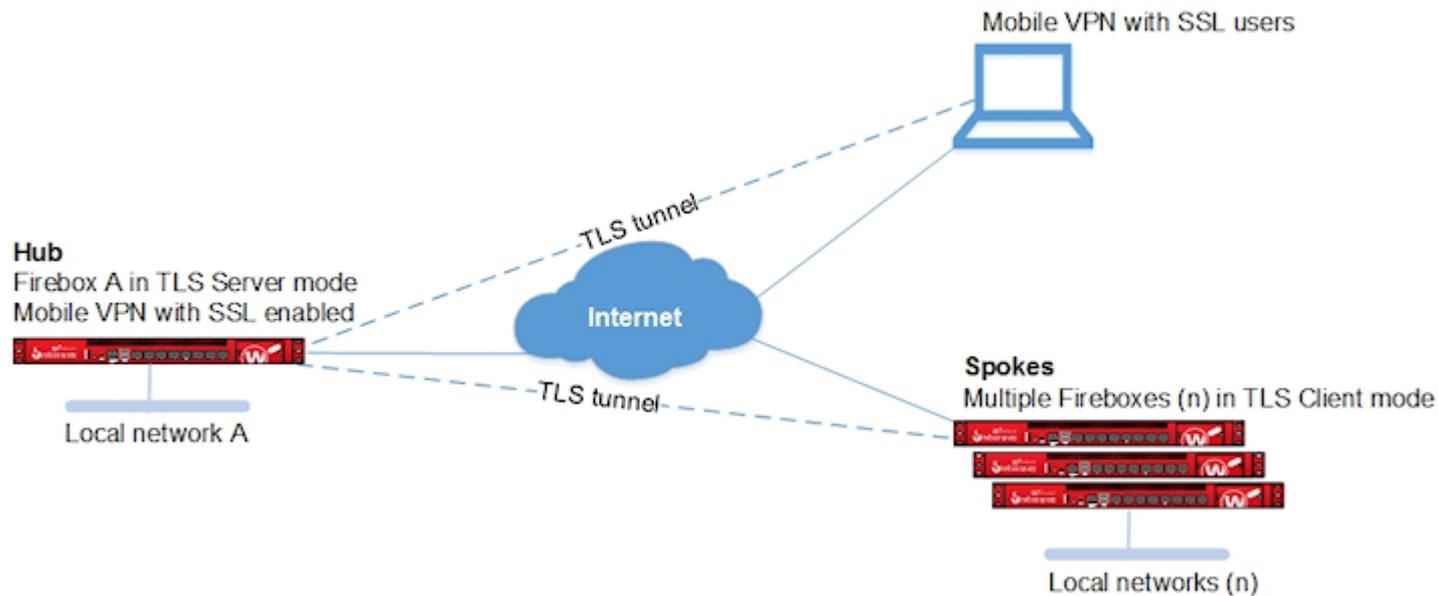
[ADVANCED](#)

# BOVPN Over TLS

- Two configuration options are supported:
  - Option 1 — TLS server connects to multiple TLS clients
  - Option 2 — TLS client connects to multiple TLS servers
    - This option consumes more resources on the Firebox than Option 1

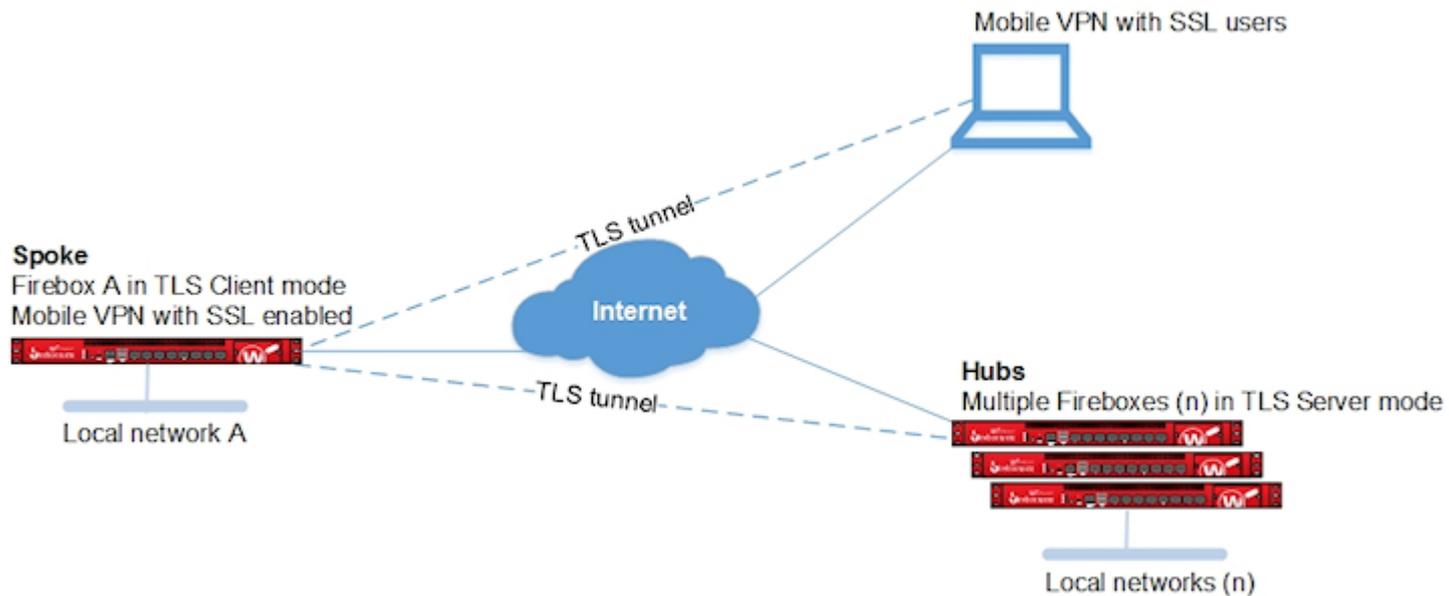
# BOVPN Over TLS

- Option 1:



# BOVPN Over TLS

- Option 2:



# BOVPN Over TLS

- The BOVPN-Allow.in and BOVPN-Allow.out policies are shared with BOVPN, BOVPN virtual interfaces, and TLS BOVPN

Name   Enable

Settings Application Control Traffic Management Scheduling Advanced

Connections are

Policy Type **Any**

PORT	PROTOCOL
	Any

**FROM**

- TLSTunnel
- TLSTunnel2
- BOVPN.VIF.Portland
- BOVPNTunnel.Seattle

**TO**

- Any

ADD REMOVE ADD REMOVE

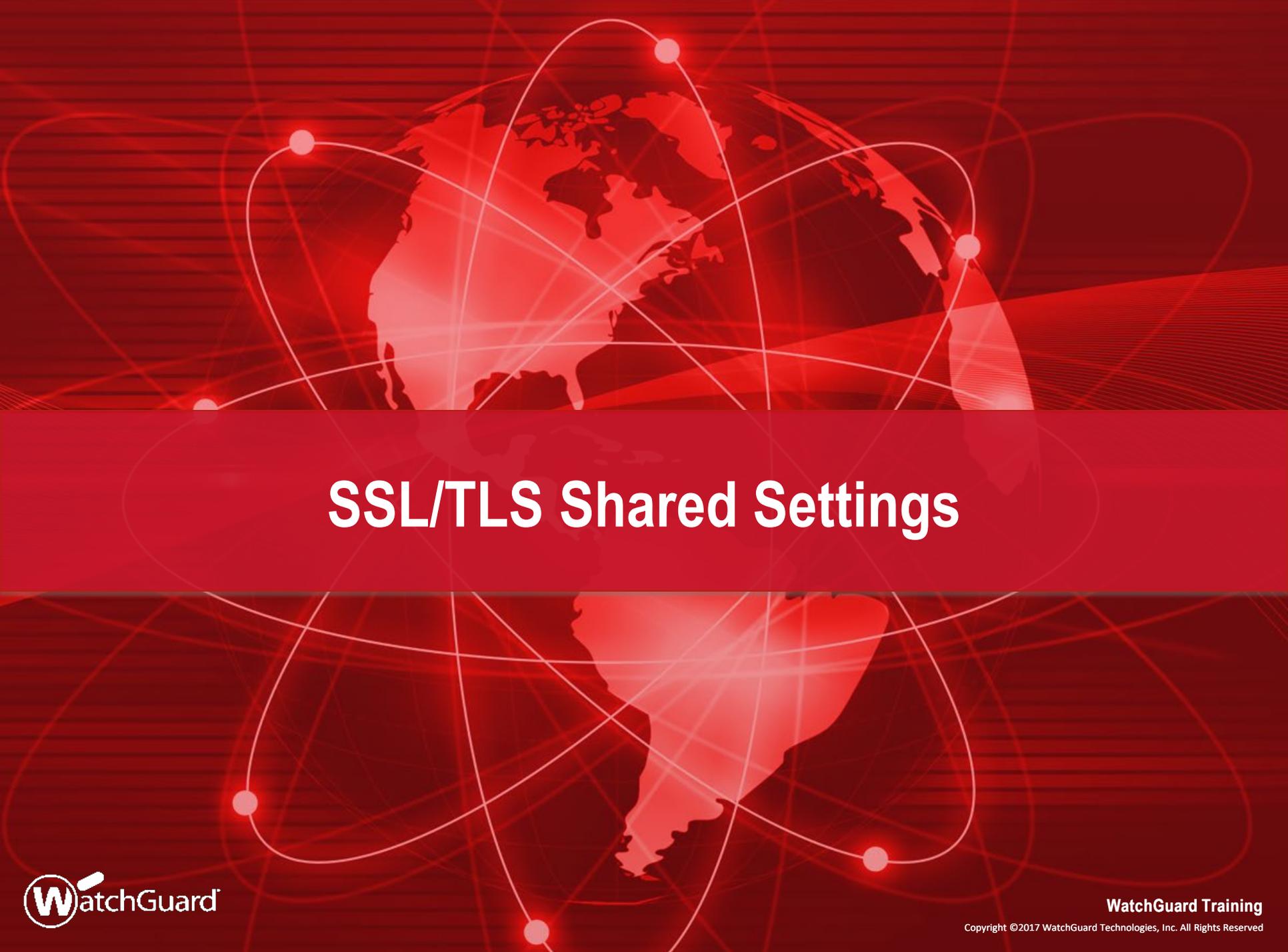
# BOVPN Over TLS

- From Fireware Web UI, on the **System Status > VPN Statistics > Branch Office VPN** tab, you can see BOVPN over TLS tunnels
- You can filter the page on **TLS Tunnels** and **Edit** the tunnel settings

The screenshot displays the WatchGuard Fireware Web UI interface for VPN Statistics. The main panel is titled "VPN Statistics" and has tabs for "Statistics", "Branch Office VPN", "Mobile VPN", and "Debug". The "Branch Office VPN" tab is selected. A dropdown menu labeled "Show All" is highlighted with a red box. An arrow points from this dropdown to a secondary dropdown menu that is also highlighted with a red box, showing the "TLS Tunnels" option selected. Below the dropdowns, there is a list of VPN tunnels. The first three entries are IKEv1 Gateways: "gateway.modem", "gateway.seattle", and "XTM1050\_10.1", each with an "Error" status and "EDIT", "DEBUG", and "REKEY TUNNELS" buttons. The last two entries are TLS Tunnels: "TLSTunnel" and "TLSTunnel2", each with an "EDIT" button. These two TLS Tunnel entries are highlighted with a red box.

# BOVPN Over TLS

- Unsupported features:
  - Active/active FireCluster
  - IP address ranges
  - BOVPN NAT
  - Dynamic routing over the VPN tunnel
  - Multicast traffic over the VPN tunnel
  - Policy-based routing
- Third-party certificates are not supported



# SSL/TLS Shared Settings

# SSL/TLS Shared Settings

- Several Firebox features use SSL/TLS for secure communication and share the same OpenVPN server
- The features that share the OpenVPN server, in order of precedence from highest to lowest, are:
  - Management Tunnel over SSL on hub devices
  - BOVPN over TLS in Server mode
  - Mobile VPN with SSL
  - Access Portal

# SSL/TLS Shared Settings

- Features with lower precedence inherit some SSL/TLS settings from enabled features with higher precedence
- The shared settings are not configurable for the features with lower precedence

# SSL/TLS Shared Settings

- When you enable more than one of these features, informational messages appear when settings are inherited from another feature
- Example messages:

Mobile VPN with SSL

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

Activate Mobile VPN with SSL

The Management Tunnel over SSL feature is enabled and overrides some settings. [CLIENT MEMBERS](#)

The BOVPN over TLS server feature is enabled and overrides some settings.

# SSL/TLS Shared Settings

- When you enable Management Tunnel over SSL, BOVPN over TLS, Mobile VPN with SSL, or the Access Portal, the *WatchGuard SSLVPN* policy is created automatically
- In Fireware v12.1 and higher:
  - The *WatchGuard SSLVPN* policy includes the alias WG-VPN-Portal
  - By default, the alias WG-VPN-Portal includes only the Any-External interface
- The *WatchGuard SSLVPN* policy is shared by Management Tunnel over SSL, BOVPN over TLS, Mobile VPN with SSL, and the Access Portal

# SSL/TLS Shared Settings

- If the WatchGuard SSLVPN policy is part of your configuration and you upgrade to Fireware v12.1, the *WatchGuard SSLVPN* policy does not immediately change
- However, if you save the settings for BOVPN over TLS or Mobile VPN with SSL, even if you make no changes, the *WatchGuard SSLVPN* policy changes:
  - The alias WG-VPN-Portal appears in the **From** field of the *WatchGuard SSLVPN* policy
  - Interfaces in the *WatchGuard SSLVPN* policy are moved to the WG-VPN-Portal alias
  - Aliases that are not interfaces, such as IP addresses or users, are not moved to the WG-VPN-Portal alias, but are included in the **From** field

# SSL/TLS Shared Settings

- To edit the interfaces in the WG-VPN-Portal alias, you must edit the **Interfaces** setting in the VPN Portal settings

# SSL/TLS Shared Settings

- **Example 1** — Management Tunnel over SSL on a hub device, BOVPN over TLS in Server mode, Mobile VPN with SSL, and Access Portal are enabled
- These settings are not configurable:
  - BOVPN over TLS in Server mode — Firebox IP addresses, virtual IP address pool, data channel protocol and port, and renegotiate data channel
  - Mobile VPN with SSL — Firebox IP addresses, networking method, virtual IP address pool, VPN resources, data channel, authentication, encryption, and timers
  - Access Portal — VPN Portal port

# SSL/TLS Shared Settings

- BOVPN over TLS in Server mode

Branch Office VPN over TLS

Enable Branch Office VPN over TLS to configure a hub-and-spoke VPN when IKE/IPSec traffic is not allowed.

The Management Tunnel over SSL feature is enabled and overrides some settings.

[CLIENT MEMBERS](#)

Branch Office VPN over TLS is **Enabled In Server Mode**. Click to [Change Mode](#) or [Disable](#).

# SSL/TLS Shared Settings

- Mobile VPN with SSL

Mobile VPN with SSL

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

Activate Mobile VPN with SSL

The Management Tunnel over SSL feature is enabled and overrides some settings. [CLIENT MEMBERS](#)

The BOVPN over TLS server feature is enabled and overrides some settings.

# SSL/TLS Shared Settings

- VPN Portal Port

## VPN Portal Port

Specify the VPN Portal Port. This is the configuration port shared by Mobile SSL VPN Clients and users of the Access Portal.

The data channel port for BOVPN over TLS has precedence over the VPN Portal port. To set the BOVPN over TLS port, [click here](#).

VPN Portal Port

# SSL/TLS Shared Settings

- **Example 2** — BOVPN over TLS in Server mode, Mobile VPN with SSL, and Access Portal are enabled
- These settings are not configurable:
  - Mobile VPN with SSL — Firebox IP addresses, networking method, virtual IP address pool, VPN resources, data channel, authentication, encryption, and timers
  - Access Portal — VPN Portal port
- In the BOVPN over TLS settings, you can configure the Data Channel for TCP or UDP
  - The Data Channel setting affects the Data Channel setting for Mobile VPN with SSL

# SSL/TLS Shared Settings

- If the BOVPN over TLS Data Channel is configured for TCP:
  - Data Channel port for BOVPN over TLS is 443 and cannot be configured
  - Data Channel for Mobile VPN with SSL is TCP 443 and cannot be configured
  - VPN Portal port is 443 and cannot be configured

# SSL/TLS Shared Settings

- BOVPN over TLS Data Channel

### Advanced Settings ×

Virtual IP Address Pool  /

Authentication  ▼

Encryption  ▼

Data channel  ▼ :

# SSL/TLS Shared Settings

- Mobile VPN with SSL Data Channel

Mobile VPN with SSL

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

Activate Mobile VPN with SSL

The BOVPN over TLS server feature is enabled and overrides some settings.

General Authentication **Advanced**

Authentication SHA-256

Encryption AES (256-bit)

Data channel TCP 443

# SSL/TLS Shared Settings

- VPN Portal Port

## VPN Portal Port

Specify the VPN Portal Port. This is the configuration port shared by Mobile SSL VPN Clients and users of the Access Portal.

The data channel port for BOVPN over TLS has precedence over the VPN Portal port. To set the BOVPN over TLS port, [click here](#).

VPN Portal Port

# SSL/TLS Shared Settings

- If the BOVPN over TLS Data Channel is UDP:
  - Data Channel for BOVPN over TLS can be a port other than 443
  - Data Channel for Mobile VPN with SSL changes to UDP, and the port changes to the port you specified for the BOVPN over TLS Data Channel
  - VPN Portal port is 443 and cannot be configured
  - The *WatchGuard SSLVPN* policy includes the UDP and TCP ports

# SSL/TLS Shared Settings

- BOVPN over TLS Data Channel

### Advanced Settings

Virtual IP Address Pool	<input type="text" value="192.168.113.0"/> / <input type="text" value="24"/>
Authentication	<input type="text" value="SHA-256"/> ▼
Encryption	<input type="text" value="AES (256-bit)"/> ▼
Data channel	<input type="text" value="UDP"/> ▼ : <input type="text" value="444"/>

# SSL/TLS Shared Settings

- Mobile VPN with SSL Data Channel

Mobile VPN with SSL

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

Activate Mobile VPN with SSL

The BOVPN over TLS server feature is enabled and overrides some settings.

General Authentication **Advanced**

Authentication SHA-256 ▼

Encryption AES (256-bit) ▼

Data channel UDP ▼ 444

# SSL/TLS Shared Settings

- VPN Portal Port

## VPN Portal Port

Specify the VPN Portal Port. This is the configuration port shared by Mobile SSL VPN Clients and users of the Access Portal.

The data channel port for BOVPN over TLS has precedence over the VPN Portal port. To set the BOVPN over TLS port, [click here](#).

VPN Portal Port

443

# SSL/TLS Shared Settings

- *WatchGuard SSLVPN* policy

Firewall Policies / Edit

Name   Enable

Settings Application Control Traffic Management Scheduling Adv

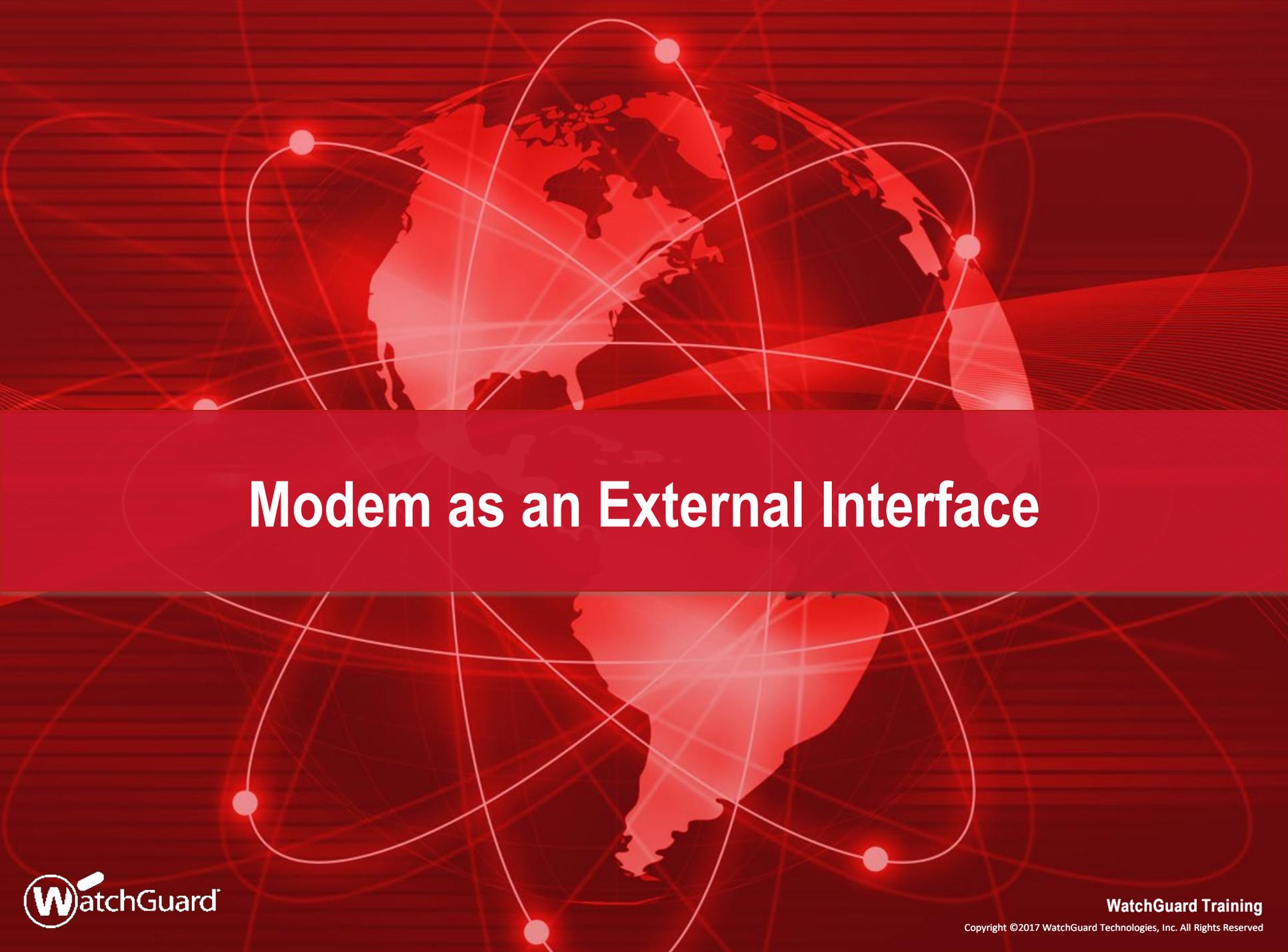
Connections are

Policy Type **SSL-VPN**

PORT	PROTOCOL
444	UDP
443	TCP

FROM

TO



# Modem as an External Interface

# Modem as an External Interface

- You can now enable a modem as an external interface
- If your business operates in areas with weak ISP coverage, or you have non-traditional methods for internet access, a dedicated modem interface can increase your network flexibility
- The modem interface can perform as a dedicated interface and support multi-WAN scenarios
- 3G/4G cellular modems currently supported for failover are supported as external interfaces

# Modem as an External Interface

- When you enable a modem, it appears in the list of interfaces as modem0

Interfaces		DNS/WINS				
INTERFAC	MODULE	NAME (ALIAS)	TYPE	IPV4 ADDRESS	IPV6 ADDRESS	NIC CONFIG
0	0	External	External	203.0.113.20/24	2001::56/64	Auto Negotiate
1	1	Trusted	Trusted	10.0.20.1/24		Auto Negotiate
2	2	Optional-1	External	192.0.2.2/24		Auto Negotiate
3	3	Optional-2	Disabled			Auto Negotiate
4	4	Optional-3	Disabled			Auto Negotiate
5	5	Optional-4	Disabled			Auto Negotiate
6	6	Optional-5	Disabled			Auto Negotiate
7	7	Optional-6	Disabled			Auto Negotiate
modem0		Modem	External	DHCP/PPP		

# Modem as an External Interface

- When you select to edit the modem interface, the **Modem** configuration page appears

INTERFACE	MODULE	NAME (ALIAS)	TYPE
0	0	External	External
1	1	Trusted	Trusted
2	2	Optional-1	External
3	3	Optional-2	Disabled
4	4	Optional-3	Disabled
5	5	Optional-4	Disabled
6	6	Optional-5	Disabled
7	7	Optional-6	Disabled
modem0	Modem	External	External

**EDIT**

Modem

 Click the lock to prevent further changes

Enable Modem

Account DNS Dial-up Advanced

Enable 3G/4G modem support

Dial-up Account Settings

Telephone number

Alternate telephone number

Access point name

Account name

Account domain

Account password

Enable modem and PPP debug trace

# Modem as an External Interface

- When you enable a modem, it appears in the list of aliases
  - You can add the modem to a policy
- The modem appears as an interface option in these configurations:
  - BOVPN and BOVPN virtual interfaces
  - Dynamic DNS
  - 1-to-1 NAT
  - SNAT
  - Dynamic NAT
  - Traffic management
    - Applies to modem interfaces for outgoing traffic only

# Modem as an External Interface

- Modem failover is supported for BOVPN and BOVPN virtual interfaces
- If you configure a modem interface as a BOVPN gateway, the **Use Modem for failover** option is not available

Branch Office VPN / Add

 Click the lock to prevent further changes

Gateway Name

General Settings | **Phase 1 Settings**

Credential Method

Use Pre-Shared Key

Use IPsec Firebox Certificate

Show All Certificates

ID	CERTIFICATE NAME	ALGORITHM	TYPE
----	------------------	-----------	------

Gateway Endpoint

	LOCAL INTERFACE	LOCAL TYPE	LOCAL ID	REMOTE IP	REMOTE TYPE	REMOTE ID
1	Modem	IP Address	203.0.113.2	198.51.100.2	IP Address	198.51.100.2

ADD EDIT REMOVE MOVE UP MOVE DOWN

Use Modem for failover **(Note: Unavailable when the BOVPN endpoint includes a local gateway that is a modem interface)**

Start Phase 1 tunnel when Firebox starts

# Modem as an External Interface

- If you select **Use Modem for failover** for a BOVPN gateway, the modem does not appear in the **External Interface** list in the local gateway settings

Gateway Endpoint

LOCAL INTERFACE	LOCAL TYPE

ADD EDIT REMOVE MOVE UP MOVE DOWN

Use Modem for failover

Start Phase 1 tunnel when Firebox starts

Gateway Endpoint Settings

A tunnel needs authentication on each side of the tunnel. Provide the configuration details for the gateway endpoints below.

Local Gateway Remote Gateway Advanced

External Interface

External  
External  
Optional-1

Specify the gateway ID for tunnel authentication.

By IP Address

By Domain Name

By User ID on Domain

By x500 Name

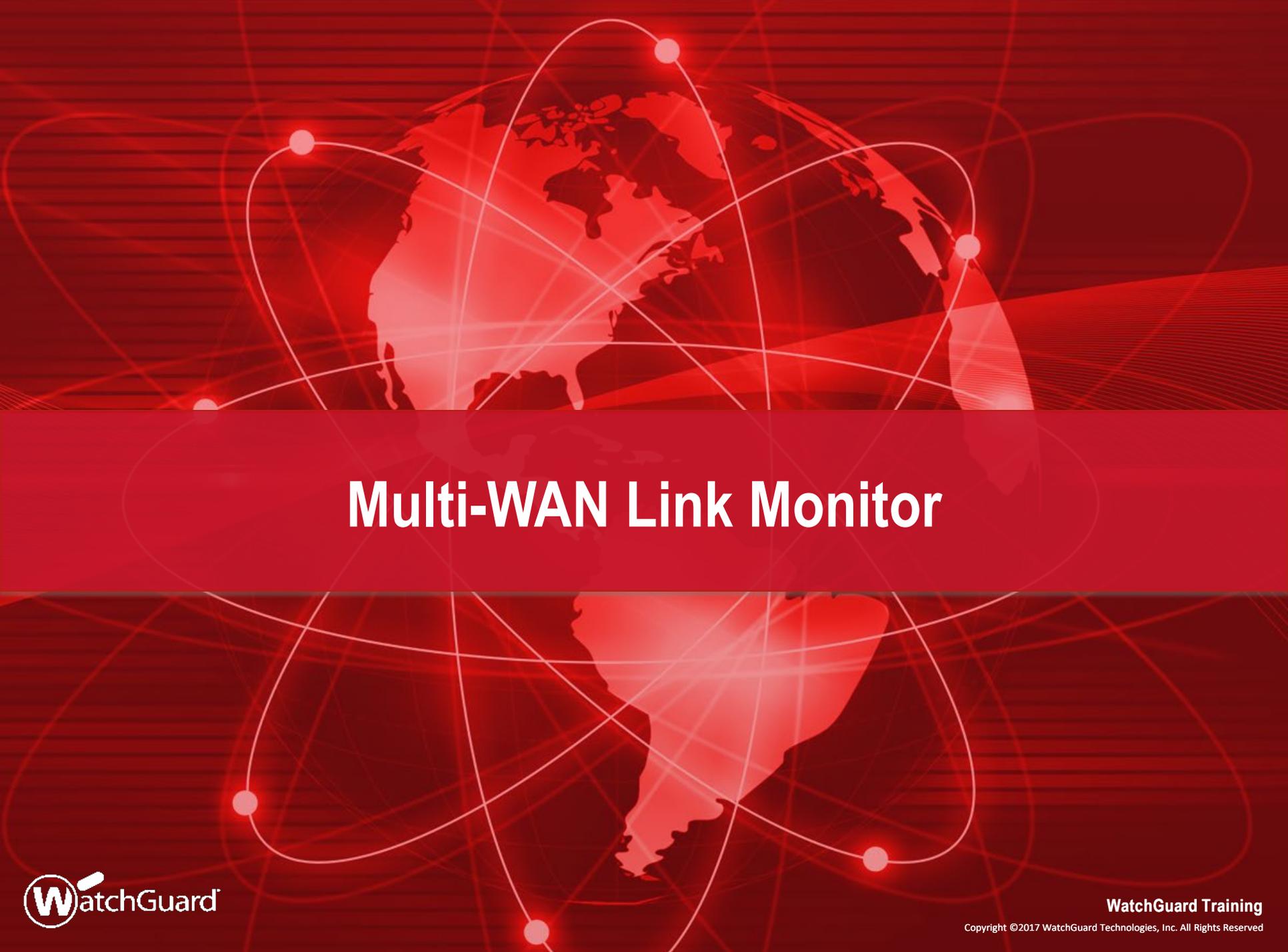
OK CANCEL

# Modem as an External Interface

- Multi-WAN and Link Monitor features are updated
  - You can now add a modem interface to Multi-WAN
  - By default, modems do not participate in Multi-WAN
  - You can enable Link Monitor for a modem that participates in Multi-WAN
  - By default, Link Monitor is disabled for modem interfaces to prevent bandwidth consumption
  - The **Link Monitor** tab was removed from the **Network > Modem** configuration page
- Link Monitor updates affect all interface types and are described in more detail in the next section

# Modem as an External Interface

- Unsupported features:
  - FireCluster
  - RapidDeploy
  - VLANs
  - Bridge mode
  - Multiple modem interfaces



# Multi-WAN Link Monitor

# Multi-WAN Link Monitor Updates

- You can now disable Link Monitor for any interface
- Fireware Web UI:

### Configure Link Monitor

Select whether this interface participates in Multi-WAN and how link monitor verifies the interface status.

**External**

Participate in Multi-WAN

Enable link monitor

To monitor the default gateway, link monitor must be enabled.

To monitor the connection to another source, select an option and specify an IP address or domain name.

Ping

TCP  Port

Both Ping and TCP must be successful to define the interface as active

Probe interval  seconds

Deactivate after  consecutive failures

Reactivate after  consecutive successes

# Multi-WAN Link Monitor Updates

- Policy Manager:

The screenshot shows the 'Network Configuration' window with the 'Multi-WAN' tab selected. The 'Link Monitor' sub-tab is active, and the 'Advanced' view is shown. The 'External Interfaces' list includes 'External', 'Optional-1', 'Optional-2', and 'Modem'. The 'Settings' section for the 'External' interface has the 'Enable Link Monitor' checkbox checked and highlighted with a red box. Below this, there are options to monitor the external interface by Ping, TCP, or Both, with fields for IP Address and Port. At the bottom, there are settings for Probe Interval (15 seconds), Deactivate After (3 consecutive failures), and Reactivate After (3 consecutive successes). The window has 'OK', 'Cancel', and 'Help' buttons at the bottom right.

Network Configuration

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

Multi-WAN Configuration  
Select the method to route non-IPSec traffic among more than one external interface. Click **Configure** to set more properties.  
Routing Table [v] [Configure...]

Link Monitor | Advanced

Select whether this interface participates in multi-WAN and how link monitor verifies the interface status.

External Interfac... Settings:

Enable Link Monitor  
To monitor the default gateway, link monitor must be enabled.

Monitor External by:

Ping IP Address [v] . . .

TCP IP Address [v] . . . Port: 80 [v]

Both Ping and TCP must be successful to define the interface as active

Use these settings for External:

Probe Interval: 15 [v] Seconds

Deactivate After: 3 [v] Consecutive Failures

Reactivate After: 3 [v] Consecutive Successes

OK Cancel Help

# Multi-WAN Link Monitor Updates

- When you add a new interface, Link Monitor is enabled by default for all interfaces except modems

Configure Link Monitor

Select whether this interface participates in Multi-WAN and how link monitor verifies the interface status.

**External**

Participate in Multi-WAN

Enable link monitor

To monitor the default gateway, link monitor must be enabled.

To monitor the connection to another source, select an option and specify an IP address or domain name.

Ping

TCP  Port

Both Ping and TCP must be successful to define the interface as active

Probe interval  seconds

Deactivate after  consecutive failures

Reactivate after  consecutive successes

OK CANCEL

Configure Link Monitor

Select whether this interface participates in Multi-WAN and how link monitor verifies the interface status.

**Modem**

Participate in Multi-WAN

Enable link monitor

To monitor the default gateway, link monitor must be enabled.

To monitor the connection to another source, select an option and specify an IP address or domain name.

Ping

TCP  Port

Both Ping and TCP must be successful to define the interface as active

Probe interval  seconds

Deactivate after  consecutive failures

Reactivate after  consecutive successes

OK CANCEL



# Wildcard IPv4 Addresses

# Wildcard IPv4 Addresses

- You can now specify wildcard IPv4 address in aliases and in policies
- If you create templates for repetitive IPv4 address patterns in your distributed enterprise, wildcard IPv4 addresses add convenience
  - On the Firebox, you can specify the wildcard IPv4 address in a policy rather than type each individual IPv4 address
- A built-in IP address calculator helps you determine IPv4 address ranges
- Wildcard IPv4 addresses in aliases and policies are also supported in Device Configuration Templates

# Wildcard IPv4 Addresses

- Example — The 10.0.0.5/255.255.0.255 wildcard IPv4 address generates a list of 256 IPv4 addresses in this sequence:
  - 10.0.1.5
  - 10.0.2.5
  - 10.0.3.5
  - 10.0.4.5
- In a distributed enterprise, you can assign these addresses to hosts at remote sites
  - In our example, you can use the third octet to identify each site
  - To create a Firebox policy with these IP addresses, you type the wildcard IPv4 address in the policy

# Wildcard IPv4 Addresses

- Example — HTTPS policy with a wildcard IPv4 address

The image shows two overlapping screenshots from the WatchGuard configuration interface. The left screenshot is the 'Add Member' dialog, and the right screenshot is the 'Firewall Policies / Add' configuration page.

**Add Member Dialog:**

- Member type: Wildcard IPv4 (highlighted with a red box)
- Address: 10.0.0.5
- Netmask: 255.255.0.255
- CALCULATE button
- IP Address Matches (256)
- IP ADDRESS list:
  - 10.0.0.5
  - 10.0.1.5
  - 10.0.2.5
- Search for an address in the IP Address Match list: [input] SEARCH
- OK and CANCEL buttons

**Firewall Policies / Add:**

- Name: HTTPS
- Enable:
- Settings | Application Control | Traffic Management | Scheduling | Advanced
- Connections are: Allowed
- Policy Type: HTTPS
- PORT: 443, PROTOCOL: TCP
- FROM: Any-Trust
- TO: 10.0.0.5/255.255.0.255 (highlighted with a red box)
- ADD and REMOVE buttons for both FROM and TO lists

# Gateway Wireless Controller Enhancements

# Min. Association RSSI and Smart Steering

- AP120, AP300, AP320, AP322, and AP420 now support minimum association RSSI and smart steering on the Gateway Wireless Controller
- Formerly known as *Fast Handover*, these options are now configured for each SSID

Network Name (SSID) WatchGuard

Settings Security Access Points

Broadcast SSID  
 Enable client isolation  
 Use the MAC Access Control list defined in the Gateway Wireless Controller Settings

Denied MAC Addresses

Enable VLAN tagging

VLAN ID

Automatically deploy this SSID to all unpaired WatchGuard Access Points  
 Mitigate WPA/WPA2 key reinstallation vulnerability in clients  
This function only available for supported devices.

Min Association RSSI  
 Smart Steering  
 Band Steering

# Min. Association RSSI and Smart Steering

- Min. Association RSSI
  - Minimum signal strength required to associate with an AP
  - Will not actively disconnect a client if signal strength falls below the minimum association RSSI
    - For the AP300, this is a global option. If one or more SSIDs with Min. Association RSSI enabled are assigned to an AP300, the option becomes global on all SSIDs for that AP, including those that do not have Min. Association RSSI enabled.
- Smart Steering
  - Can enable only if Min. Association RSSI is enabled
  - Prevents clients from staying connected to the current AP even though there is an AP with better signal strength in the vicinity
  - Proactively steers the client to a better AP for a better connection

# Min. Association RSSI and Smart Steering

- Parameters and thresholds for Min. Association RSSI and Smart Steering options are configured in the AP settings

The screenshot displays the WatchGuard configuration interface for an AP. The 'Radio Settings' tab is active. A red box highlights the following parameters:

Parameter	Value
Steering RSSI Threshold	-70
Steering Attempts Threshold	2
Steering Blackout Period	15
Roam Initiation Threshold Interval	10
Roam Initiation Threshold Packets	5

Other visible settings include:

- Network Settings:  DHCP  Static
- Log to a syslog server:
- Syslog server IP address: [Empty field]
- Enable Communication VLAN tagging:
- Communication VLAN: 4094
- Disable LEDs:

# Band Steering

- When an SSID is configured in both the 2.4 GHz and 5 GHz bands, clients can be steered towards the less congested 5 GHz band
- Helps to evenly distribute the wireless clients between the two bands on an AP
- Band Steering has been moved from the AP settings to the SSID settings with the new Min. Association RSSI and Smart Steering options

# Improved AP Passphrase Security

- Improved Gateway Wireless Controller and AP passphrase security
- Must always enter a passphrase when you enable the Gateway Wireless Controller for AP management
- The Gateway Wireless Controller automatically generates a unique passphrase for each AP

# Deprecated Wireless Options

- These wireless options are deprecated in Fireware v12.1:
  - Telecommuter mode for remote VPN deployment
  - Band Steering for the AP300
  - Deployment over wireless (AP300 only feature)

# AP325 Support

- Support added for the upcoming AP325
- 802.11ac 2x2 MU-MIMO Wave 2 access point
- Ideal for low to medium density deployments





# Thank You!

***NOTHING GETS  
PAST **RED.*****



**WatchGuard Training**

Copyright ©2017 WatchGuard Technologies, Inc. All Rights Reserved