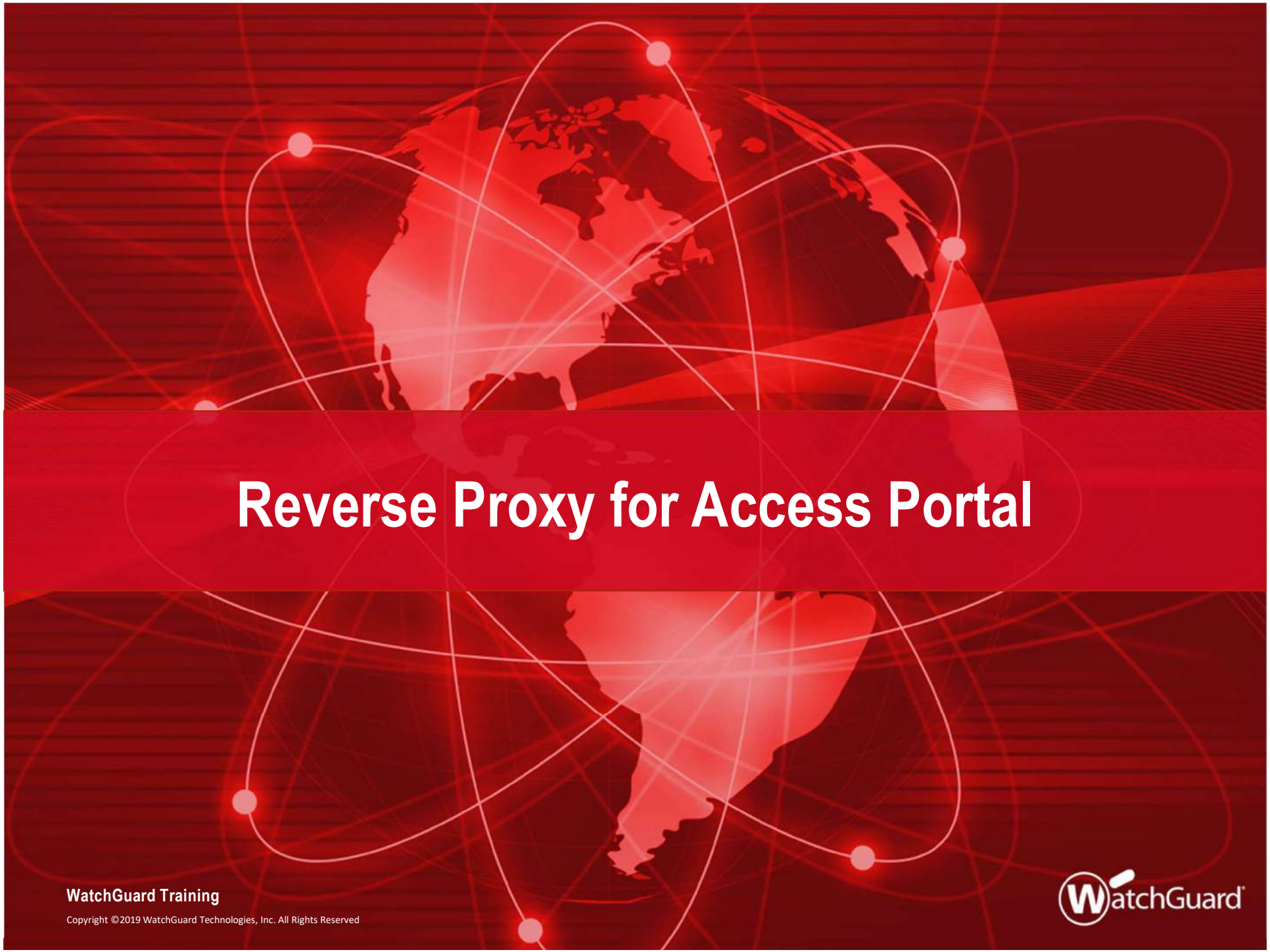
What's New in Fireware v12.5

WatchGuard Training

What's New in Fireware v12.5

- Reverse Proxy for Access Portal
- NetFlow Egress
- WebBlocker Override Enhancements
- Proxy Warn Message Customization
- ECDSA Certificates for BOVPN and BOVPN Virtual Interfaces
- Gateway Wireless Controller Enhancements
- Support for Multiple RADIUS Servers



Reverse Proxy for Access Portal

WatchGuard Training

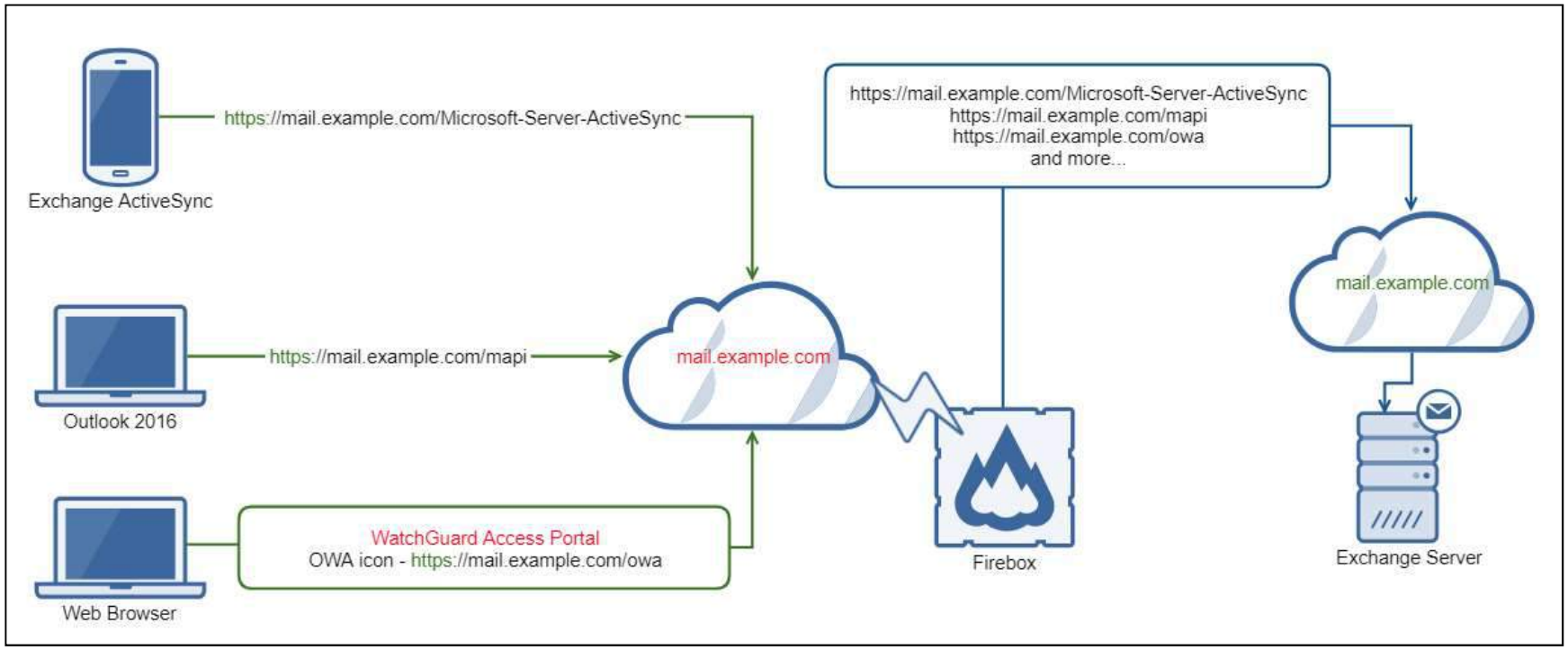
Reverse Proxy

- In the Access Portal configuration, you can now configure HTTP reverse proxy actions so remote users can connect to internal applications and Microsoft Exchange services with an external URL
- With reverse proxy actions, you can give remote teams access to internal resources without the need for a VPN
- Because multi-factor authentication is supported, you can deploy this solution in compliance environments

Reverse Proxy

- The reverse proxy on the Firebox forwards HTTP traffic from external networks to Exchange servers or other web servers on your internal networks
- You can configure reverse proxy actions so remote users can connect to an internal Exchange server with these clients:
  - Mobile devices with Microsoft mail clients (through ActiveSync)
  - Microsoft Outlook
  - Microsoft Outlook Web Access
  - Microsoft Outlook Web Access through the Access Portal (with automatic sign-in)
- You can also configure reverse proxy actions so users can connect to other internal web apps through the Access Portal

Configuration Example



Authentication and Access to Web Apps

- Users can be authenticated by Firebox to access internal applications
  - Users can be authenticated by Activesync through the Firebox for mobile email applications
  - Users can be authenticated by HTTP over SSL through the Firebox for select email applications
  - Users can be authenticated by MFA through the Firebox to access internal web applications
- We recommend that custom web apps use the Access Portal for security reasons. HTTP basic uses clear text which is not secure, so these apps require the security protections offered by the Access Portal

Authentication and Access to Web Apps

- There is an option to forward Access Portal credentials
  - Enable this option to automatically log users in to web apps with their Access Portal credentials
  - When this feature is enabled, the Access Portal caches user credentials. The cached credentials are sent to the web app with HTTP authorization header over TLS
- To sign in to web apps with Access Portal credentials:
  - The web app must accept HTTP basic authentication or SAML
  - The Access Portal and the web app must use the same authentication domain

Authentication and Access to Web Apps

- Do not enable the option to forward Access Portal credentials in these cases:
  - Users log in to the Access Portal with SAML
  - Users log in to the Access Portal with a different authentication domain than the web app (for example, with Firebox-DB)

Certificates

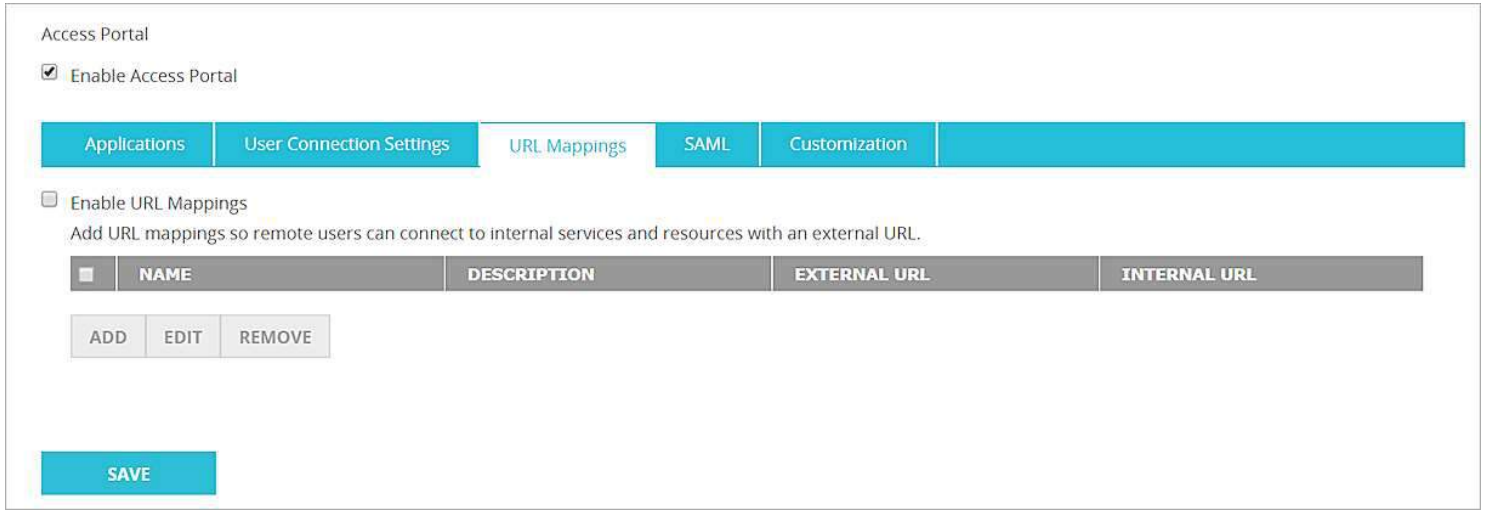
- To avoid certificate warnings on client side, Firebox web certificate should include host names of the web apps as subject alternative names or use a wildcard host name (*.example.com) as the common name
- To validate the server certificate of the web app, the self-signed certificate option for the reverse proxy action must be disabled and the CA certificates must be present on Firebox
- If the self-signed certificate option for an internal web app is disabled, the Firebox validates the server certificate of the web app and denies access if the certificate is not trusted

Minimum Requirements for Web Apps

- The Outlook Web Application is supported for the reverse proxy action
- Reverse proxy actions also support internal web applications
- HTML5, TLS 1.2 or higher, any port, HTTP and HTTPS
- Web app must be on the same domain as the Access Portal

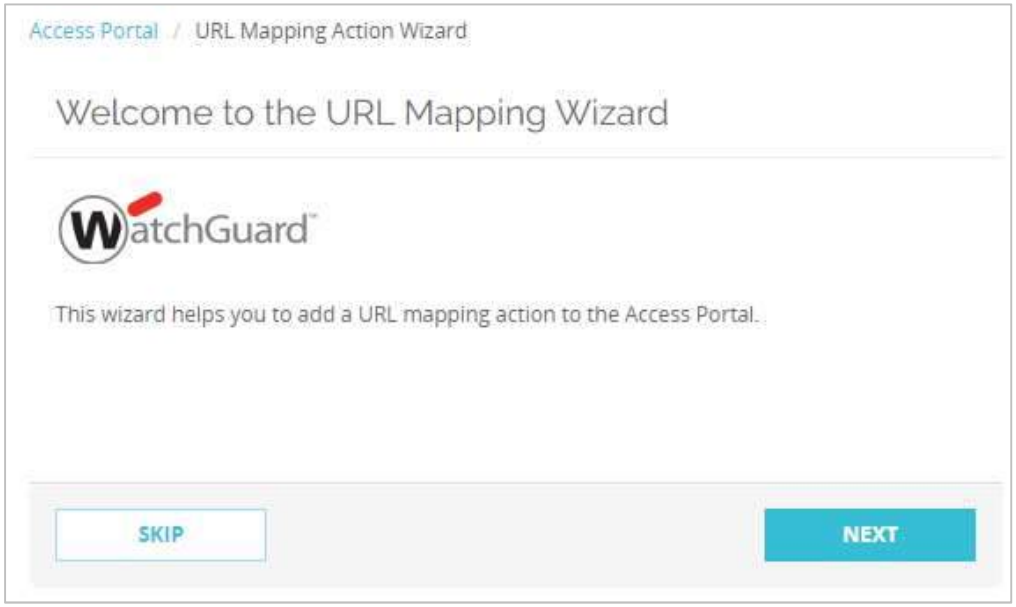
Add an Action

- You can add reverse proxy actions in the Access Portal configuration
  - Check box to enable URL mappings
  - Add, edit, and remove URL mappings
  - The URL mappings list shows the external URLs that are redirected to the URLs of the internal web resources



Add an Action

- When you select to add a reverse proxy action, a wizard appears
  - You can use the wizard or skip it to manually configure an action
  - To configure Exchange services, we recommend the wizard because it includes pre-defined mappings



Add an Action

- When you add a reverse proxy action, you must specify these settings:
  - Type of URL mapping
  - External URL
  - Internal URL
  - Whether the service has a self-signed certificate
  - Authentication (Access Portal or HTTP Basic)
  - Whether to add the app to the Access Portal
  - Action name and description
  - Description
  - URL path mapping

Add an Action

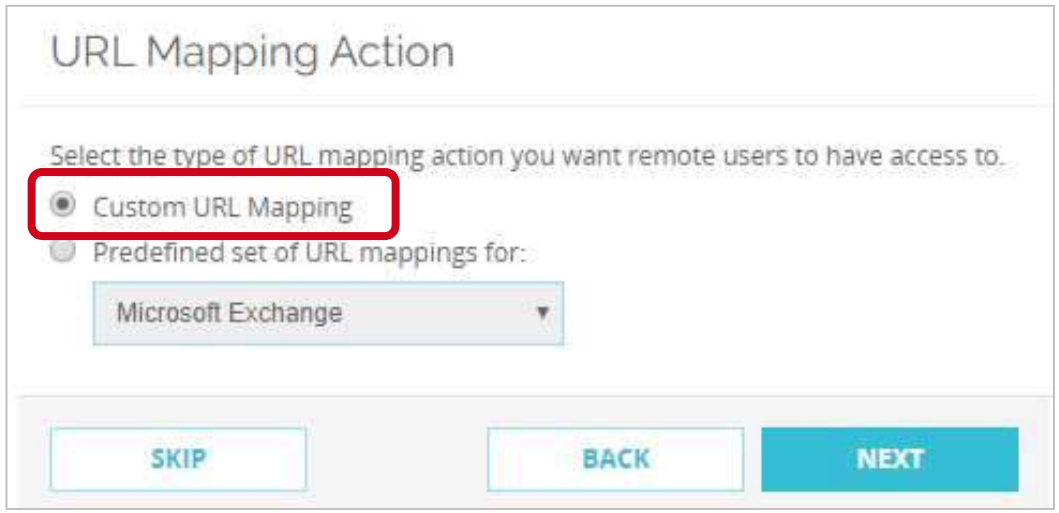
- When you add a reverse proxy action for Microsoft Exchange, you must also specify:
  - Email domain (for Exchange services only)
  - Autodiscover URL (for Exchange services only)
  - Whether to add OWA as a web app in the Access Portal
  - Whether to forward credentials from the Access Portal to OWA

Add an Action

- If you select to add the app to the Access Portal, you must also specify:
  - App name
  - App description (optional)
  - Custom icon (optional)
  - Whether to forward credentials from the Access Portal to the URL

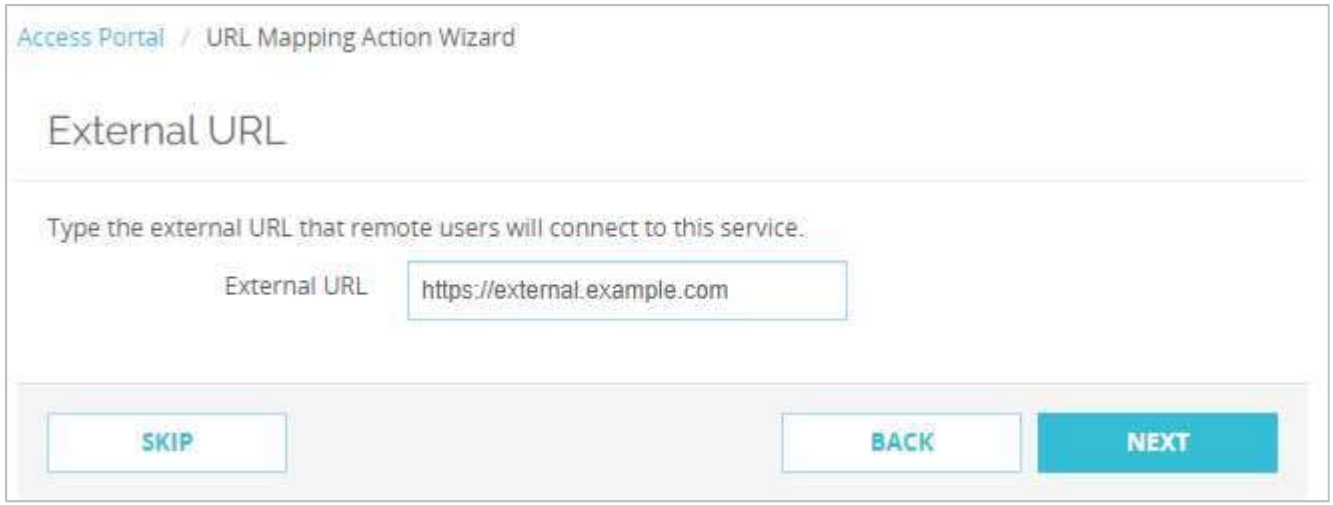
Add an Action (Wizard)

- In the wizard, to add an action other than a Microsoft Exchange action:
  - Select **Custom URL Mapping**



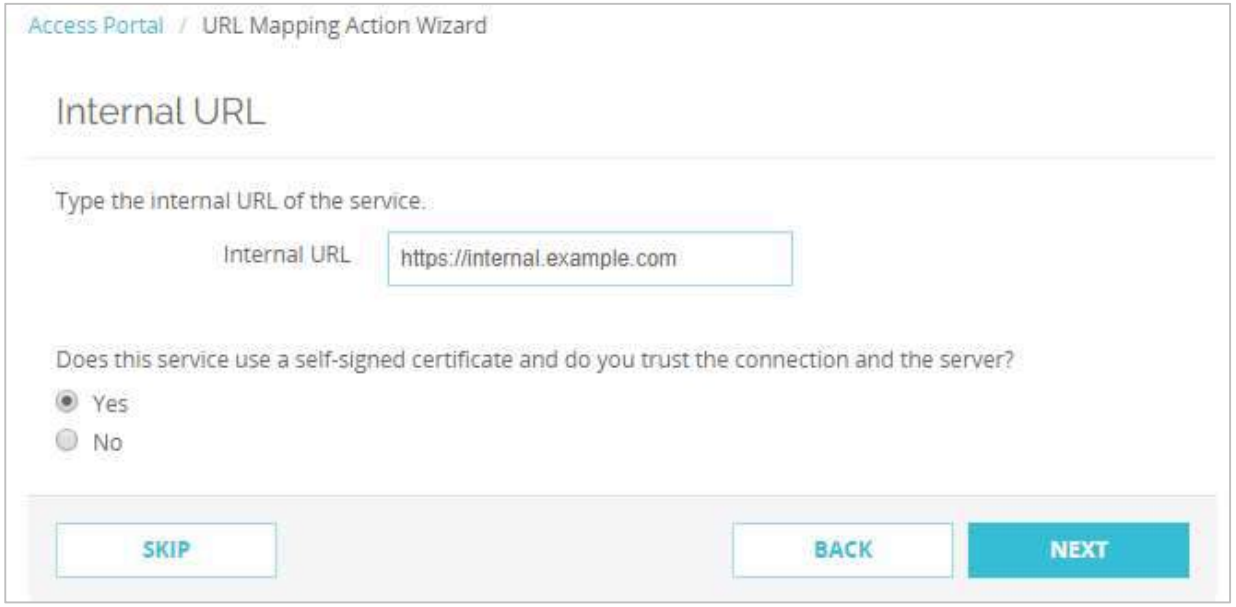
Add an Action (Wizard)

- Specify the external URL for user connections



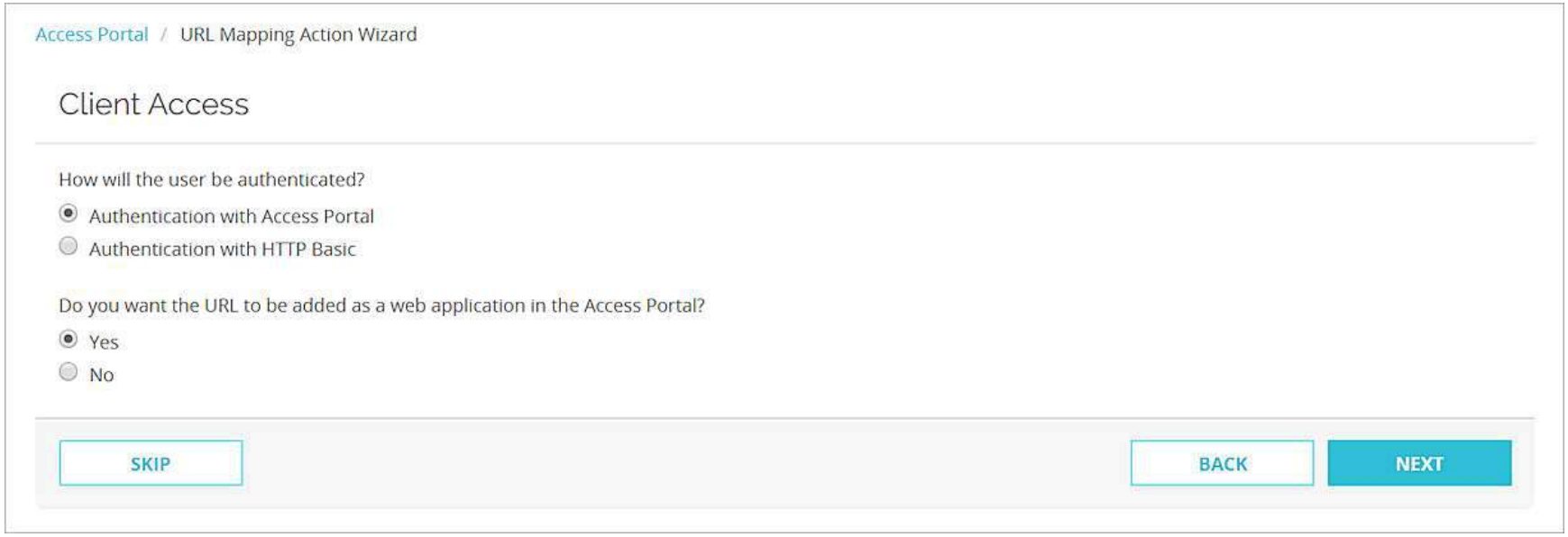
Add an Action (Wizard)

- Specify the internal URL of the server and whether the server has a self-signed certificate



Add an Action (Wizard)

- Select how to authenticate users
- Select whether to add this URL as a web app in the Access Portal

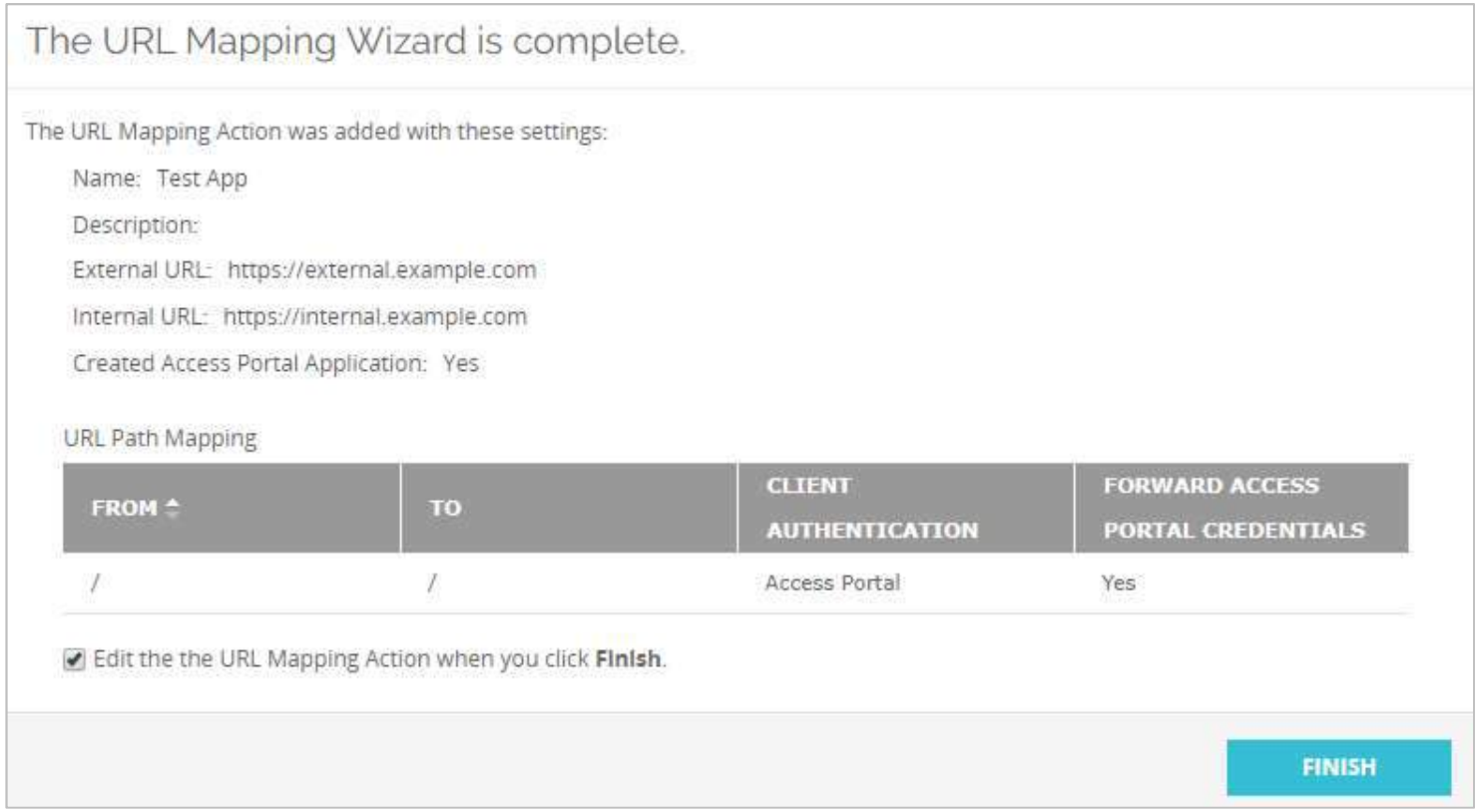


Add an Action (Wizard)

- If you select to add the app to the Access Portal, you must also specify:
  - App name
  - App description (optional)
  - Custom icon (optional)
  - Whether to forward credentials from the Access Portal to the URL
- If you chose not to add this URL as a web app in the Access Portal, you must type a name and description for the URL mapping action

Add an Action (Wizard)

- You can select to edit the action after the wizard closes
  - You might do this if you want to specify a path mapping



Add an Action (Manually)

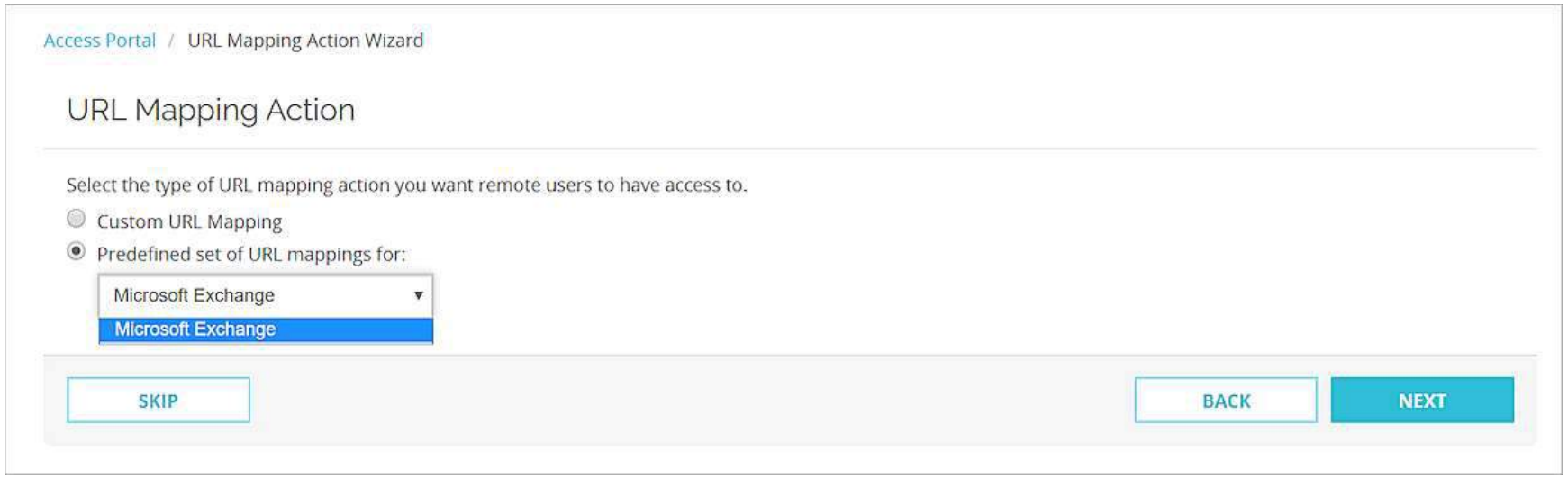
- Skip the wizard to manually add a reverse proxy action
- To manually add an action, you must:
  - Specify a name and description (optional)
  - Specify the URL that remote users will use to access this web service
  - Specify the internal URL of the web service
  - Specify whether the web service uses a self signed certificate
  - Add URL path mappings

Add an Exchange Action

- To configure a reverse proxy action for Exchange:
  - The Exchange server must accept HTTP basic authentication
  - The admin must configure the internal and external URLs in the Exchange settings

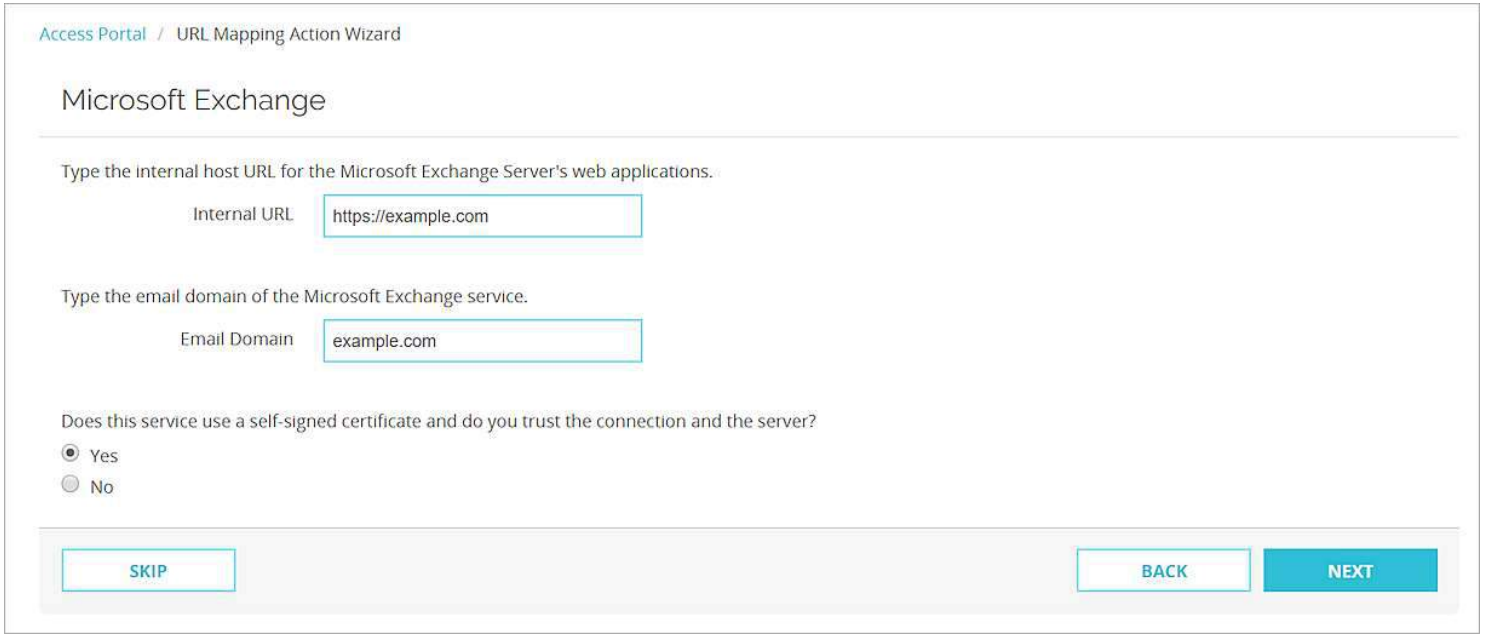
Add an Exchange Action (Wizard)

- In the wizard, to add a Microsoft Exchange action:
  - Select **Predefined set of URL mappings for**
  - From the drop-down list, select Microsoft Exchange



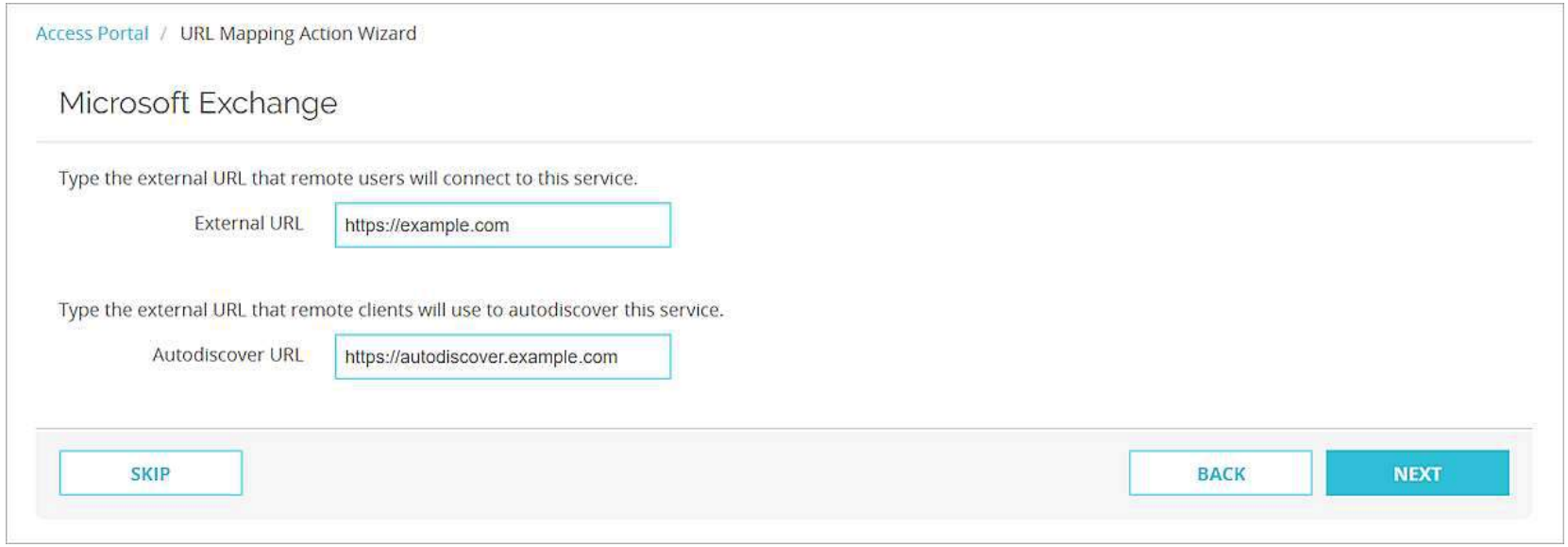
Add an Exchange Action (Wizard)

- Specify the internal host URL for the Microsoft Exchange Server's web applications
- Specify your Microsoft Exchange email domain
- Select whether the web service uses a self signed certificate



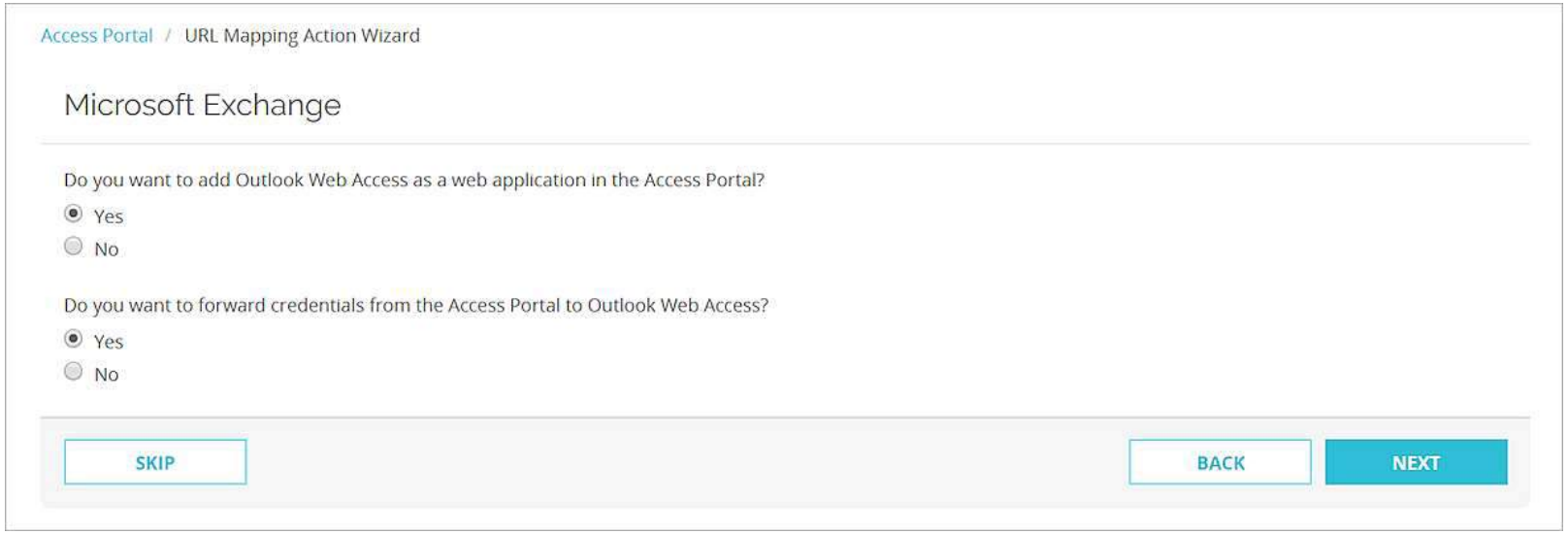
Add an Exchange Action (Wizard)

- Specify the URL that remote users will use to access this service
- Specify the URL that remote clients will use to autodiscover this service



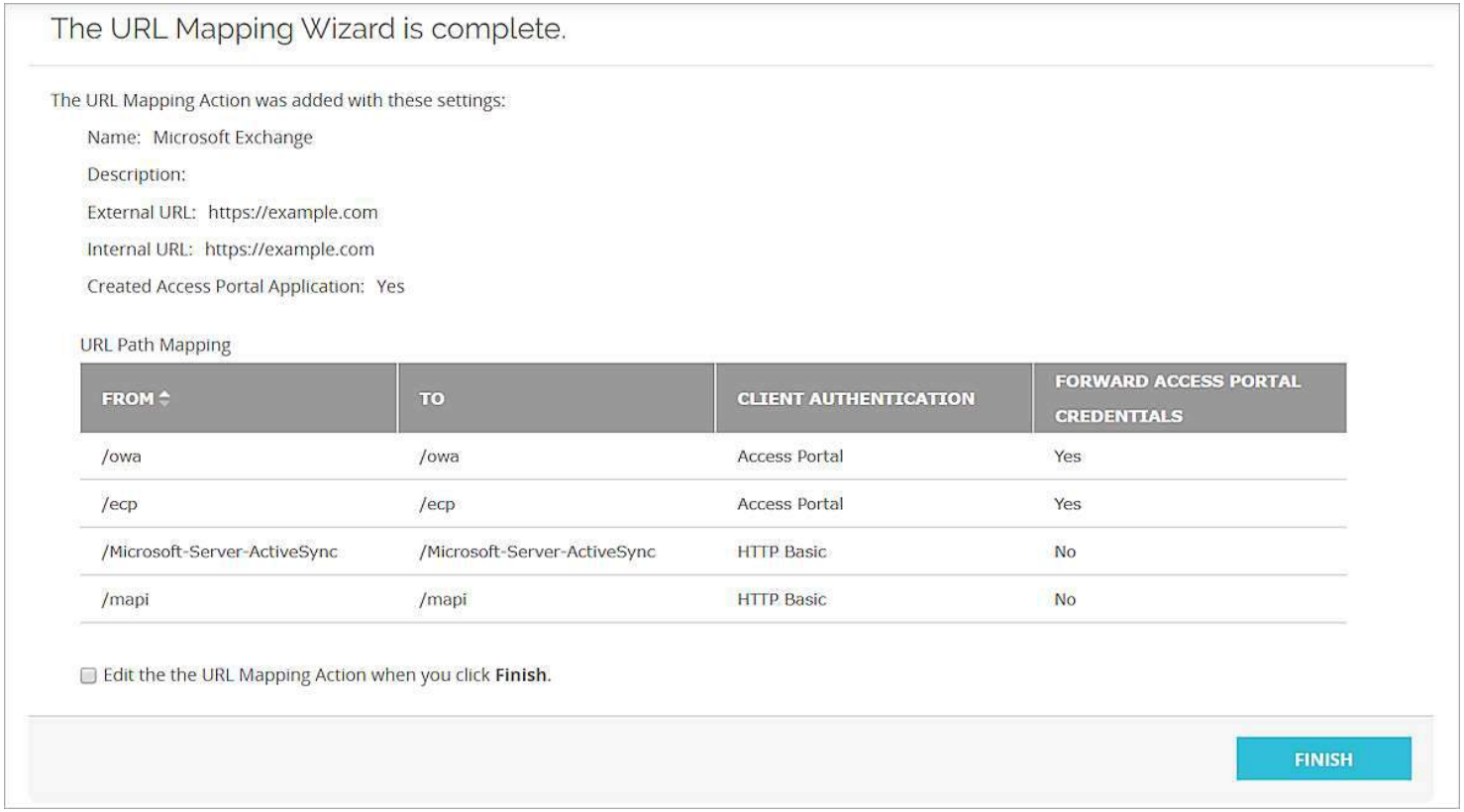
Add an Exchange Action (Wizard)

- Select whether to add Exchange as a web app in the Access Portal
- Select whether to forward credentials from the Access Portal to Exchange
  - This option automatically logs users in to web apps with their Access Portal credentials



Add an Exchange Action (Wizard)

- You can select to edit the action after the wizard closes
  - You might do this if you want to specify a path mapping


The URL Mapping Wizard is complete.

The URL Mapping Action was added with these settings:

Name: Microsoft Exchange

Description:

External URL: https://example.com

Internal URL: https://example.com

Created Access Portal Application: Yes

URL Path Mapping

FROM	TO	CLIENT AUTHENTICATION	FORWARD ACCESS PORTAL CREDENTIALS
/owa	/owa	Access Portal	Yes
/ecp	/ecp	Access Portal	Yes
/Microsoft-Server-ActiveSync	/Microsoft-Server-ActiveSync	HTTP Basic	No
/mapi	/mapi	HTTP Basic	No

☐ Edit the the URL Mapping Action when you click **Finish**.

FINISH

NetFlow Egress

WatchGuard Training

NetFlow Egress

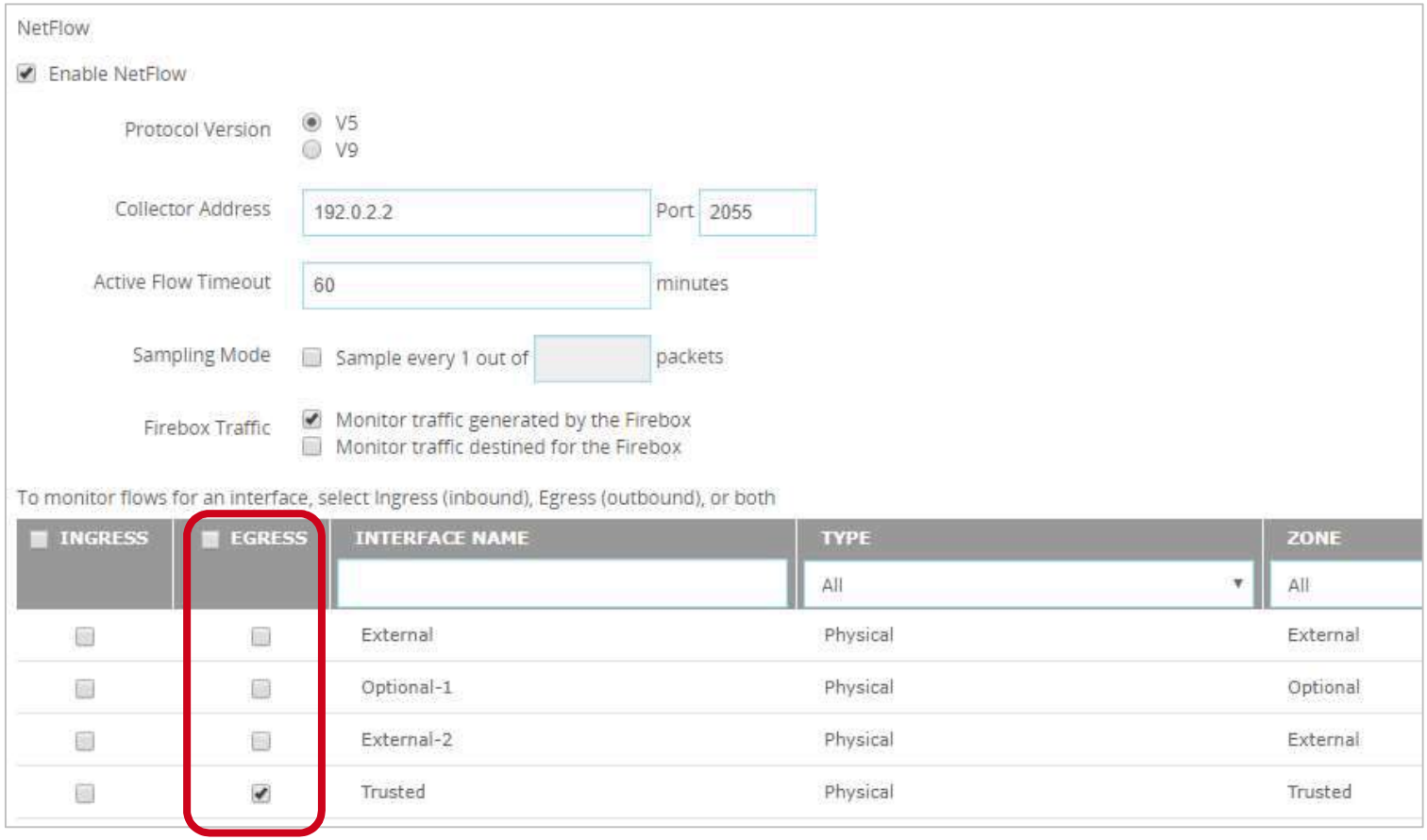
- The Firebox now supports NetFlow in both directions (ingress and egress) so you can gain more insight into your network traffic

NetFlow Egress

- In the NetFlow configuration, you can now select to monitor egress traffic for Firebox interfaces
  - Egress traffic is traffic that exits an interface
  - You can select to monitor ingress traffic, egress traffic, or both

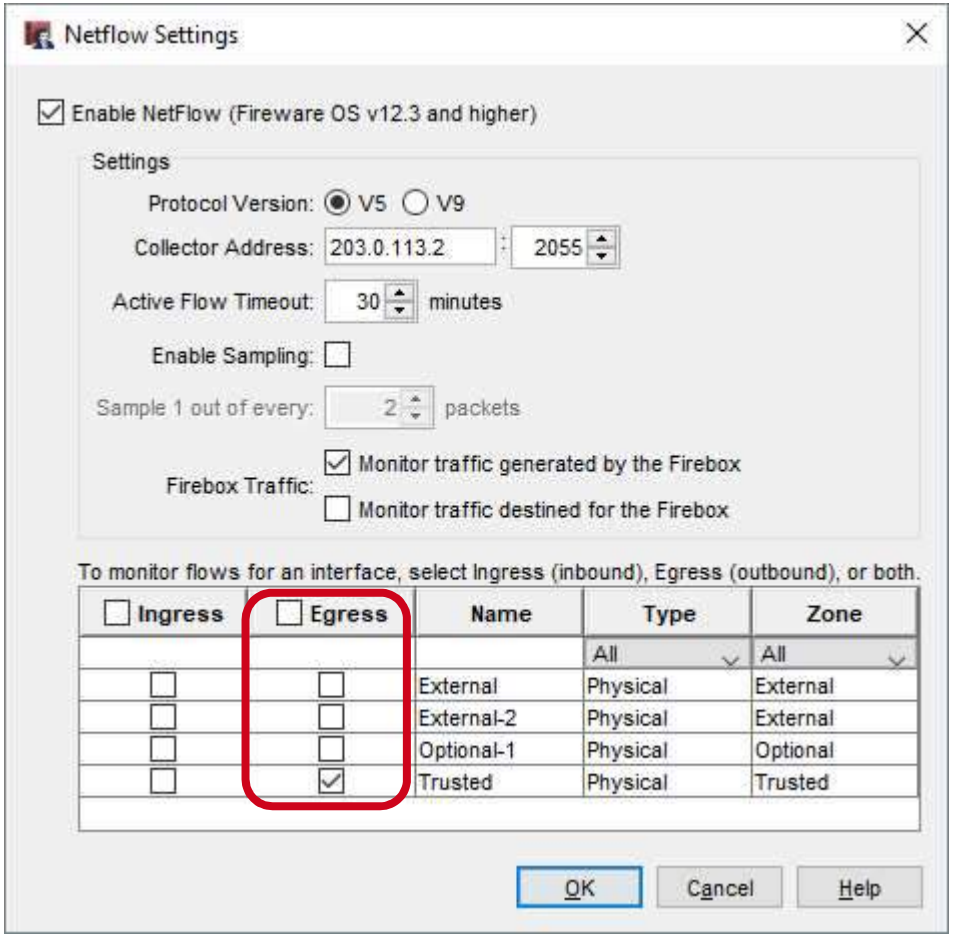
NetFlow Egress

- Web UI



NetFlow Egress

- Policy Manager

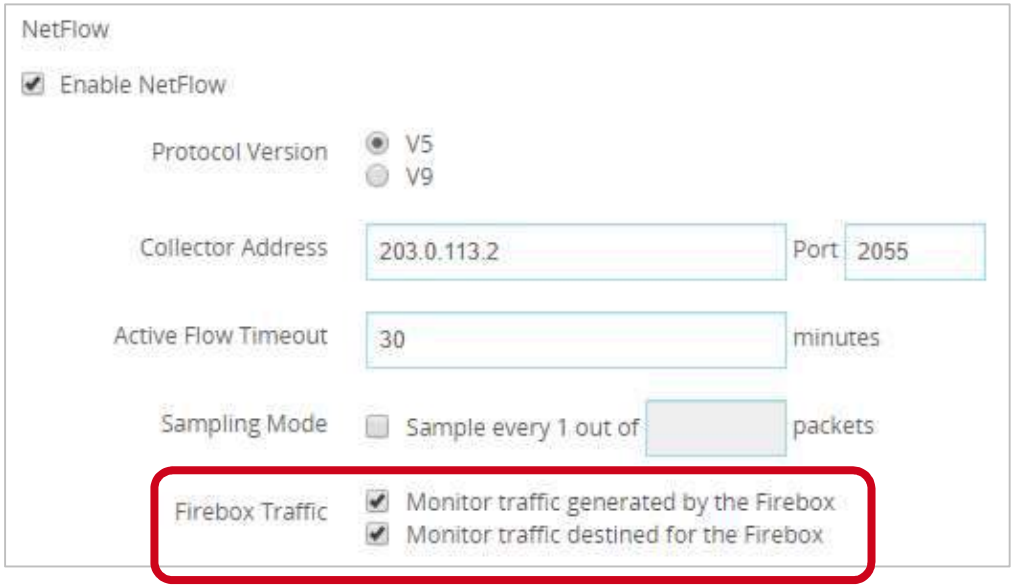


NetFlow Egress

- To monitor traffic generated by the Firebox itself (self-generated traffic), select one or both of these options:
  - Monitor traffic generated by the Firebox
  - Monitor traffic destined for the Firebox

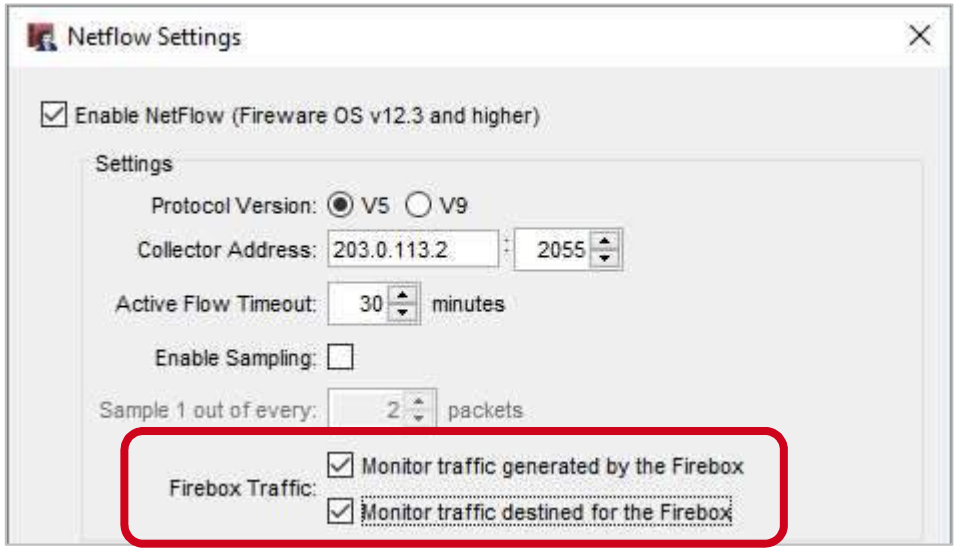
NetFlow Egress

- Web UI



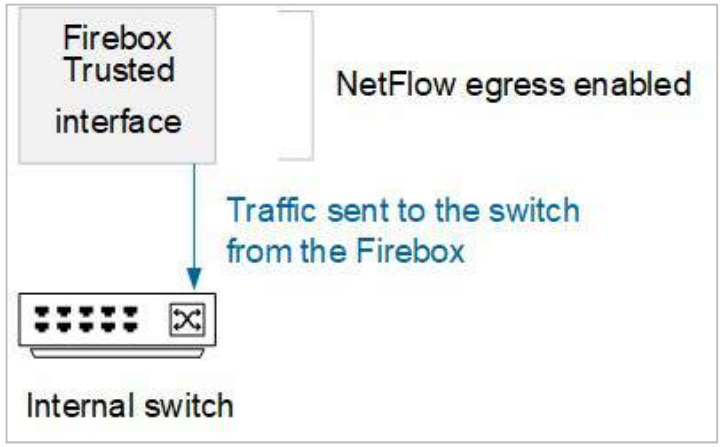
NetFlow Egress

- Policy Manager



NetFlow Egress

- **Example —**
  - If you have an internal switch without NetFlow, enable NetFlow egress on the internal Firebox interface the switch connects to
  - This captures traffic that exits the internal Firebox interface, which includes traffic sent to the switch



NetFlow Egress

- If you enable both ingress and egress in the Firebox NetFlow configuration on multiple interfaces, be aware that your NetFlow data might include duplicate data
  - To avoid duplicate data, enable either ingress or egress rather than both

WebBlocker Override Enhancements

WatchGuard Training

WebBlocker Override

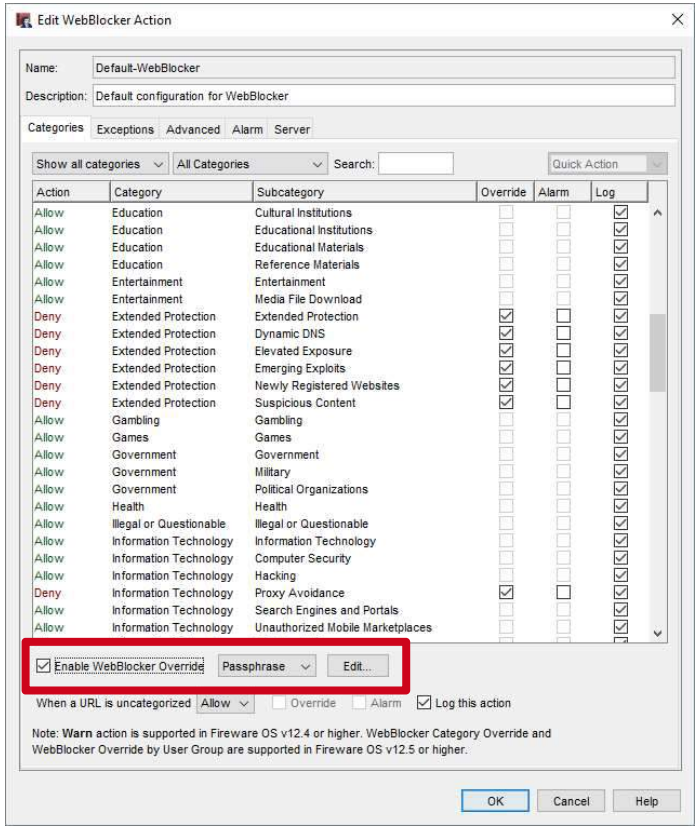
- Administrators now have more control over when users can override WebBlocker settings:
  - Enable or disable WebBlocker Override for websites in specific denied WebBlocker categories

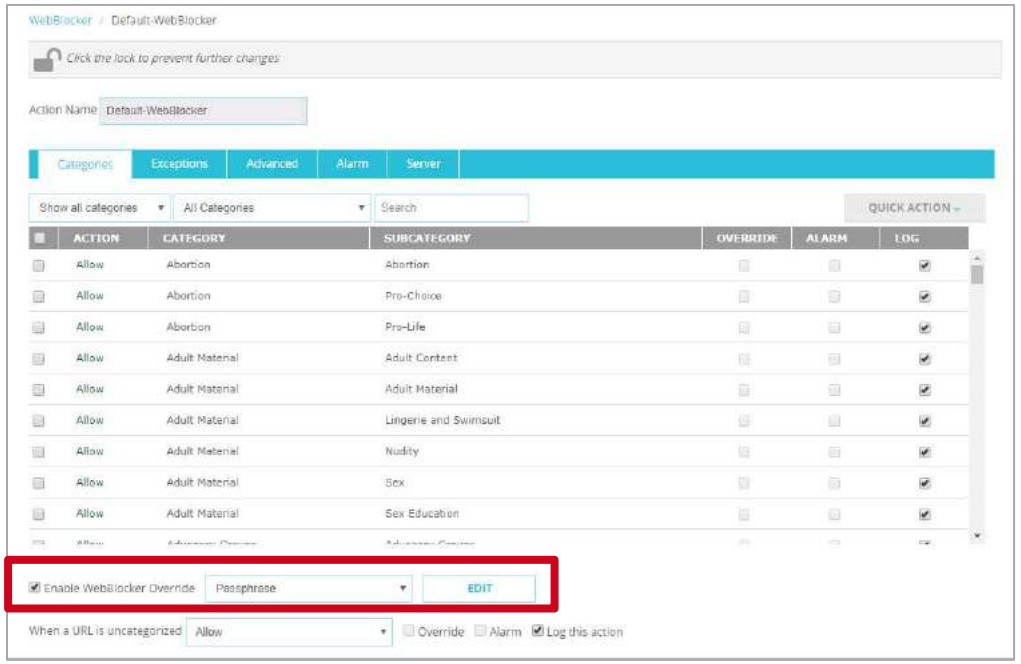
    Example: Enable override for all websites in the Health category but not the Shopping category
  - Allow users who are members of a specific user group to type their own credentials to override denied websites

    Example: Allow only users in the Teachers group to override WebBlocker settings

WebBlocker Override Settings

- In a WebBlocker action, WebBlocker Override settings have moved from the **Advanced** tab to the **Categories** tab





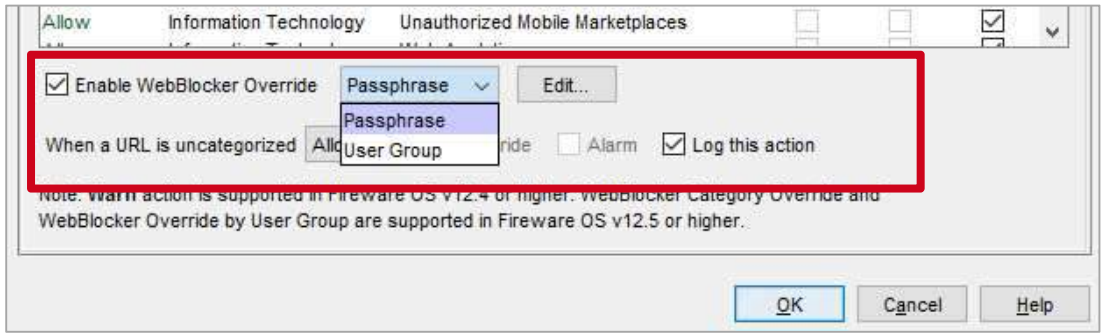
WebBlocker Override Methods

- You can now configure a WebBlocker action to use one of two override methods:
  - **Passphrase** – Specify a passphrase that users type to override the WebBlocker settings and get access to denied content. This method was also available in previous Fireware versions
  - **User Group** – Select an existing Firebox-DB or Active Directory user group. Other authentication servers are not supported for User Group override. Users who are members of the selected group can type their credentials to override the WebBlocker settings and get access to denied content
- For each WebBlocker action, you can configure only one method

Enable WebBlocker Override

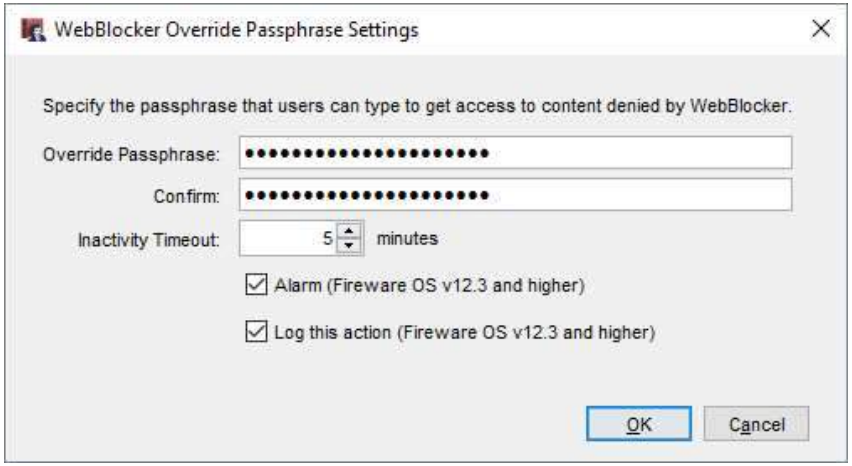
To enable WebBlocker Override:

1. Edit a WebBlocker action
2. In the **Categories** tab, select the **Enable WebBlocker Override** check box
3. From the drop-down list, select the override method:
   - **Passphrase** – Users type an override passphrase
   - **User Group** – Users in the selected group type their credentials
4. To configure Passphrase or User Group settings, click **Edit**



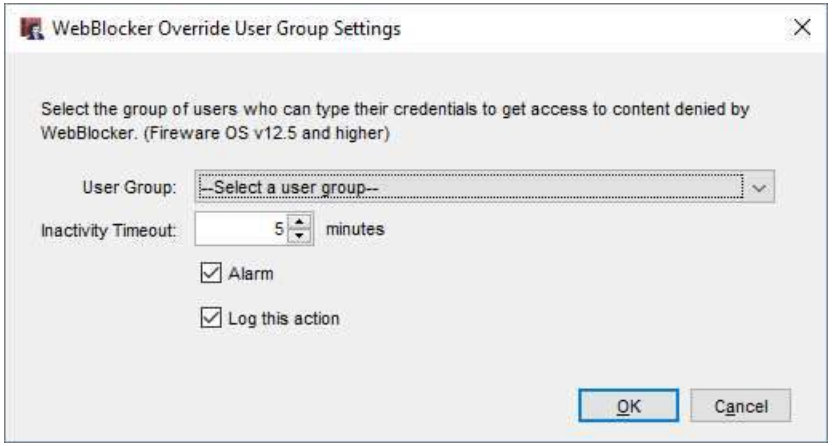
WebBlocker Override Passphrase Settings

- **Override Passphrase/Confirm** – Type an override passphrase between 8 and 32 characters
- **Inactivity Timeout** – Type the number of minutes after which inactive users can no longer access the content
- **Alarm/Log this action** – Specify whether to send an alarm and log message when someone uses the override passphrase



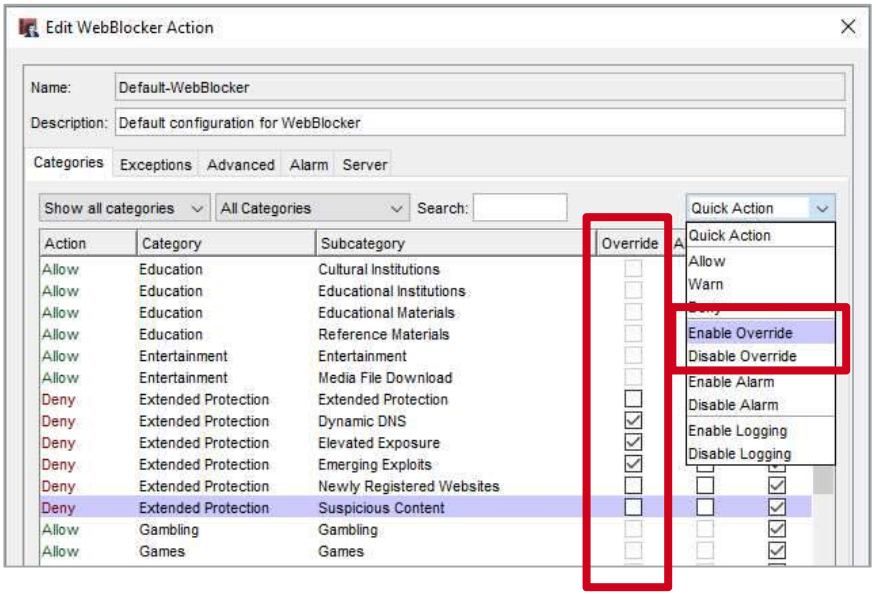
WebBlocker Override User Group Settings

- **User Group** – Select a Firebox-DB or Active Directory user group. Other authentication servers are not supported for User Group override
- **Inactivity Timeout** – Type the number of minutes after which inactive users can no longer access the content
- **Alarm/Log this action** – Specify whether to send an alarm and log message when someone overrides with user group credentials



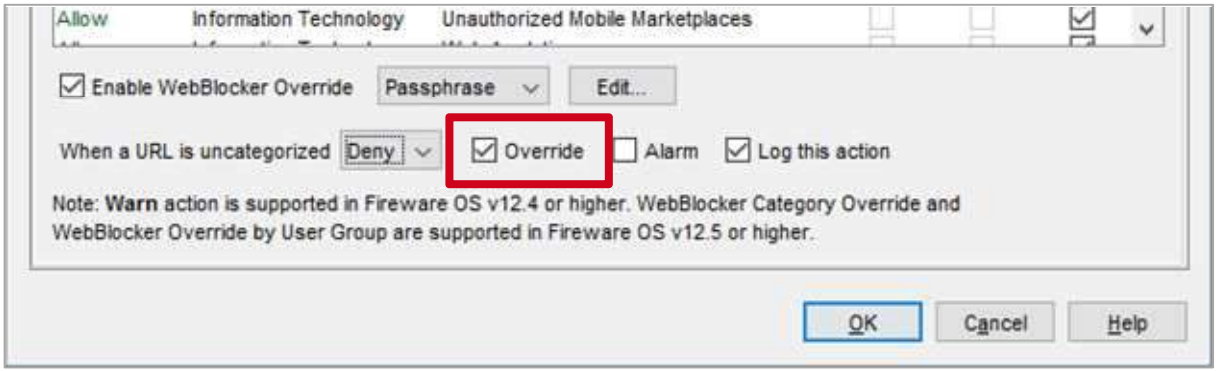
Select WebBlocker Override Categories

- When you enable WebBlocker Override in a WebBlocker action, it is enabled for all denied categories automatically
- To change which denied categories users can override:
  - In the **Override** column, select or clear the check boxes
  - Select a category, then from the **Quick Action** drop-down list, select **Enable Override** or **Disable Override**



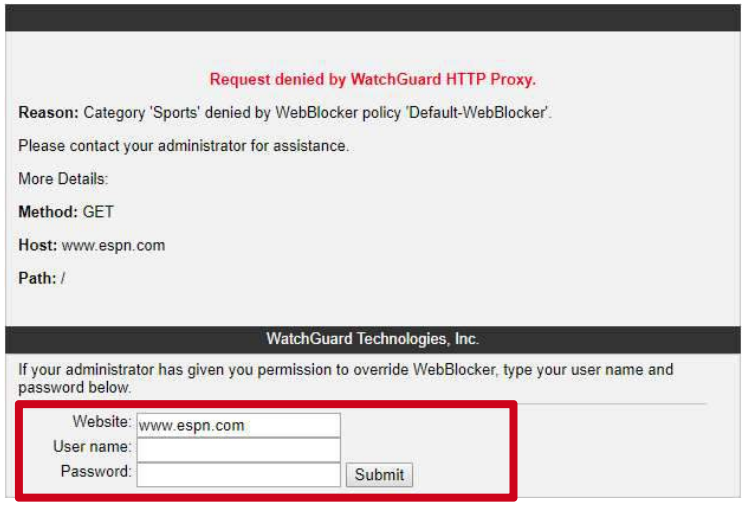
Override Denied Uncategorized URLs

- If the WebBlocker action denies uncategorized URLs, you can allow users to override the denied URLs
- Next to the **When a URL is uncategorized** drop-down list, select the **Override** check box



Override with User Group Credentials

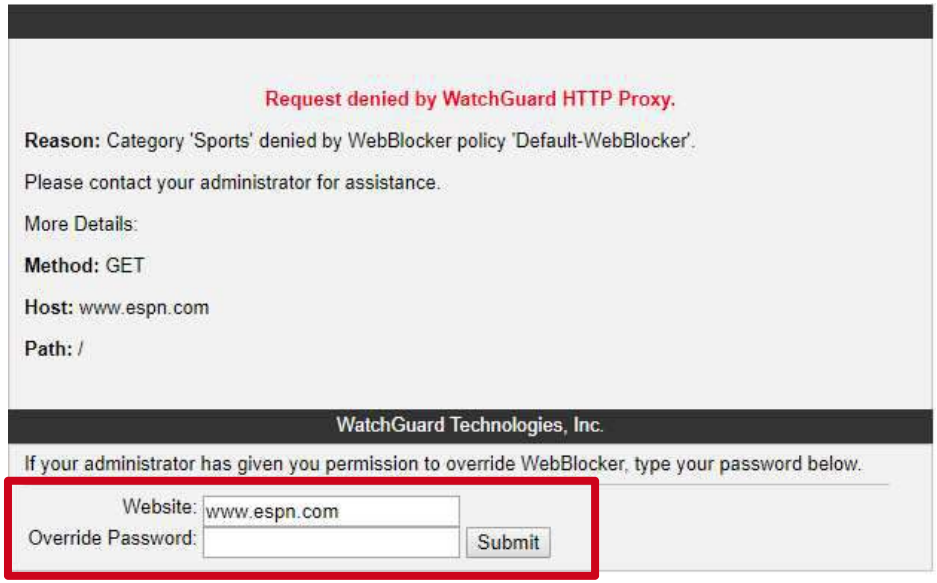
- If you configure WebBlocker Override for User Groups, all users see this page when they go to a site in a WebBlocker category that has override enabled:



- Users in the specified Firebox-DB or Active Directory user group can type their credentials to get access to the website
- This does not affect login limits configured in group settings

Override with the Override Passphrase

- If you configure the WebBlocker Override Passphrase, all users see this page when they go to a site in a WebBlocker category that has override enabled:



- Users can type the override passphrase specified in the WebBlocker action to get access to the website

WebBlocker Override Log Messages

- If you enable logging, the Firebox sends a log message when a user overrides WebBlocker:
  - Log message for a Passphrase override:

    Apr 3 16:57:00 2019 WatchGuard-XTM local1.info http-proxy[2642]: msg_id="1AFF-0021" Allow 1-Trusted 0-External tcp 10.0.1.70 157.140.2.32 49372 80 msg="ProxyAllow: HTTP Request categories" proxy_act="HTTP-Client.Standard.2" cats="" details="Allowed by passphrase overriding category action" op="GET" dstname="iczn.org" arg="/" geo_dst="GBR" (HTTP-proxy-00)

  - Log message for a User Group override:

    Apr 4 01:41:59 2019 WatchGuard-XTM local1.info http-proxy[2641]: msg_id="1AFF-0021" Allow 1-Trusted 0-External tcp 10.0.1.70 157.140.2.32 50369 80 msg="ProxyAllow: HTTP Request categories" proxy_act="HTTP-Client.Standard.2" cats="" details="Allowed by user group overriding category action. user=user1@ECObios, group=group1" op="GET" dstname="iczn.org" arg="/" geo_dst="GBR" src_user="test@jacky_radius" (HTTP-proxy-00)

WebBlocker Override – Upgrades

- When you upgrade to Fireware v12.5:
  - Users can no longer override WebBlocker for websites denied by WebBlocker exceptions and WebBlocker Server timeouts
  - WebBlocker actions that were not previously configured with an override passphrase do not have WebBlocker Override enabled
  - WebBlocker actions that were previously configured with an override passphrase have WebBlocker Override enabled:
    - WebBlocker Override uses the Passphrase override method with the same passphrase
    - All denied categories in the WebBlocker action have the **Override** check box selected automatically
    - If the WebBlocker action denied uncategorized URLs, the **Override** check box next to the **When a URL is uncategorized** drop-down list is selected automatically

Proxy Warn Message Customization

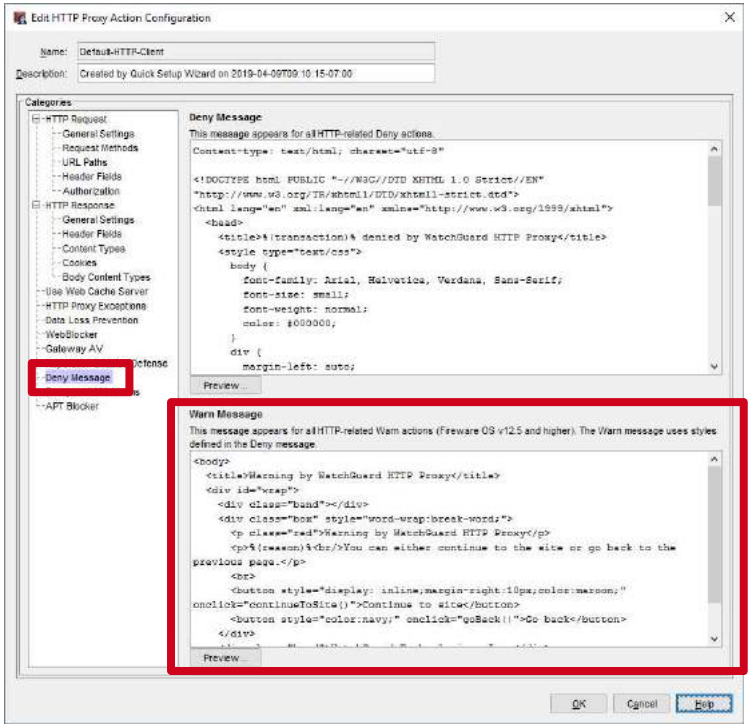
WatchGuard Training

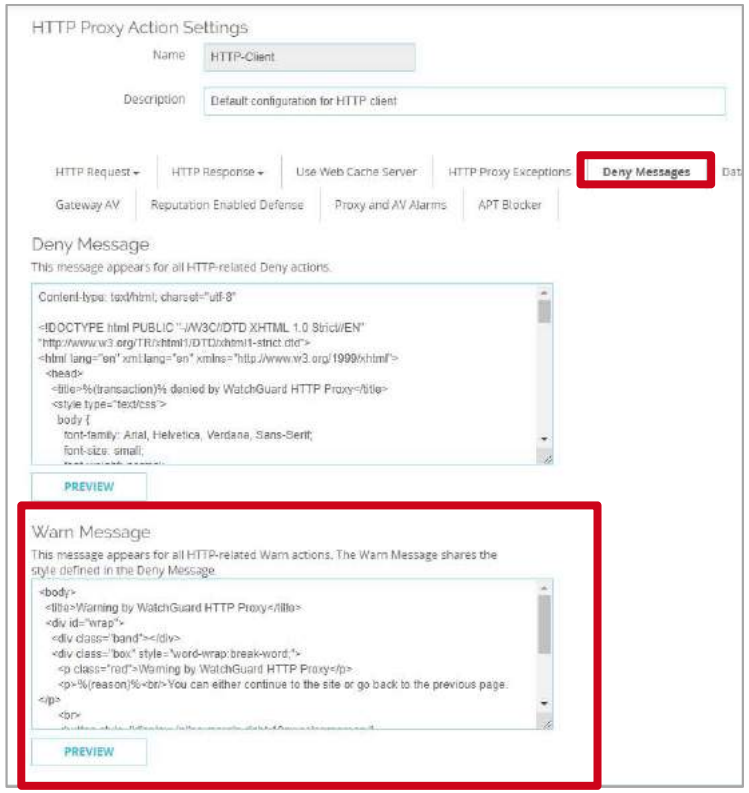
Proxy Warn Message

- You can now customize the Warn message used for HTTP and Explicit proxy Warn actions
- Administrators can use this feature to:
  - Customize the Warn message text and add content to educate and inform their users about acceptable usage policies
  - Match the Warn message appearance to the custom styles and branding used in the Deny message
- Preview buttons in the proxy action now show you a preview of both the Warn and Deny messages

Proxy Warn Message

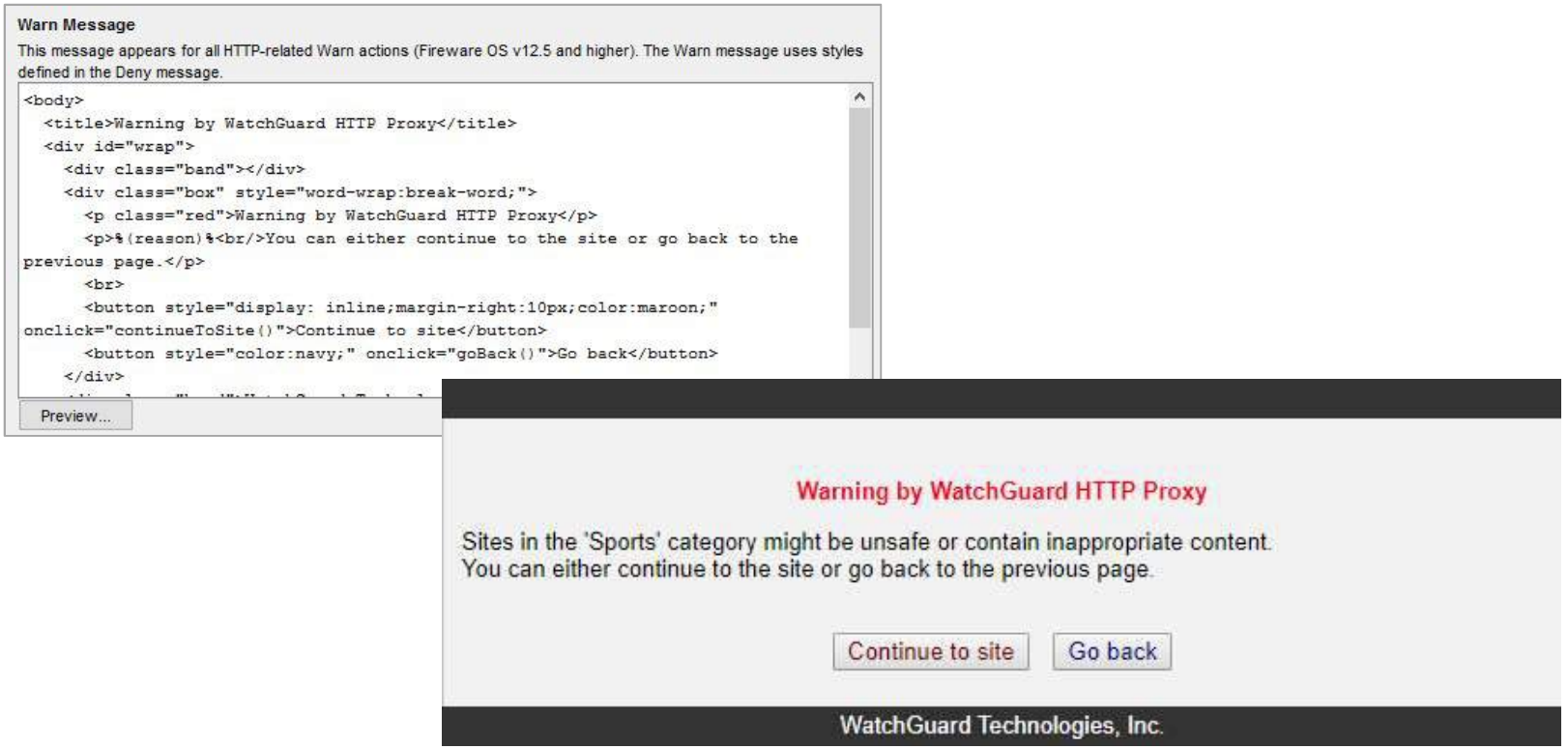
- In HTTP and Explicit proxy actions, the **Deny Message** category now includes a new **Warn Message** section
  - Currently, the Firebox uses the Warn Message text for WebBlocker Warn actions only





Proxy Warn Message – Upgrade

- After you upgrade to Fireware v12.5, all HTTP and Explicit proxy actions in your configuration include default Warn message text



Customize Proxy Warn Message Text

- To customize the proxy Warn message, in the **Warn Message** text box, edit the Warn message text and HTML code

- If the Warn message text does not include the <body> and </body> tags, your users see the default Warn message text instead of your custom Warn message

Proxy Warn Message Variables

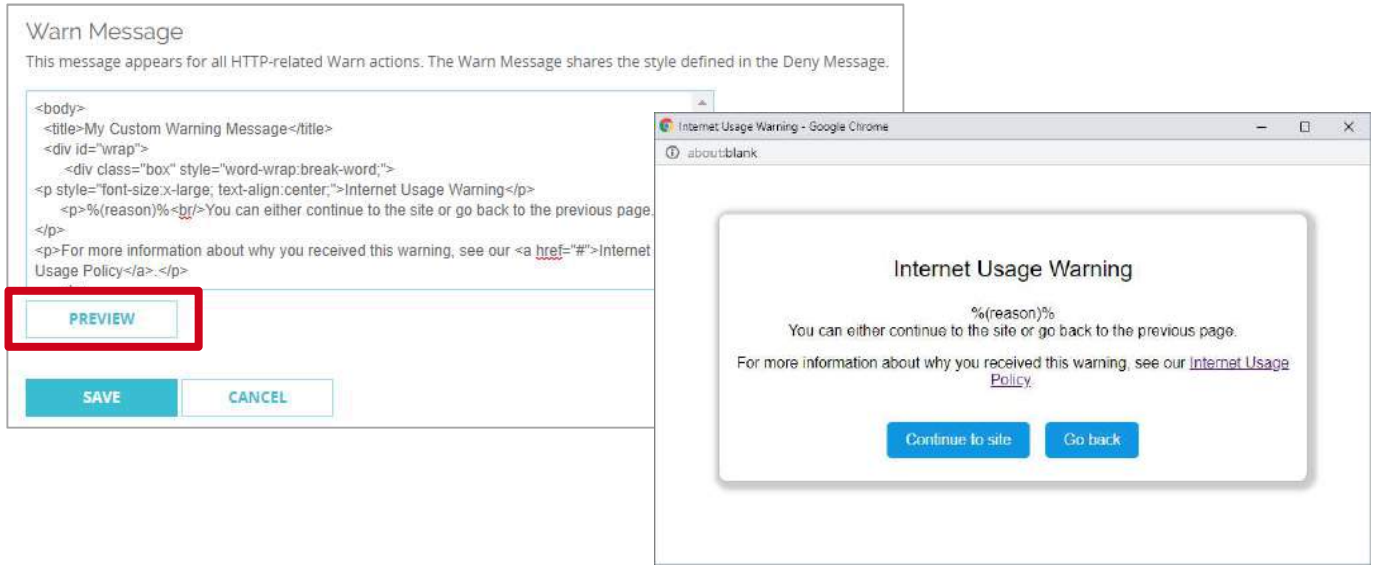
- You can include these variables in the Warn message text:
  - %(transaction)% – Transaction that caused the warning
  - %(reason)% – Reason the Firebox showed the warning
  - %(method)% – Request method from the request
  - %(url-host)% – Server host name (or IP address) from the URL
  - %(url-path)% – Path from the URL
  - %(user-name)% – Authenticated user name
  - %(serial)% – Serial number of the Firebox
  - %(firewall)% – Name of the Firebox
- When the Warn message appears in the browser, users see the relevant text instead of the variable name

Customize Proxy Warn Message Styles

- The Warn message uses the styles defined in the <HEAD> section of the proxy action Deny message
- To customize the styles, make updates in the Deny message text box
- Style changes apply to both the Deny and Warn messages

Preview the Proxy Warn Message

- To see a preview of the Warn message or Deny message in a pop-up dialog box, click **Preview**



  - Previews show variable names, not the text that replaces them
  - In Policy Manager, the Preview displays the **Continue to Site** and **Go Back** buttons as text, but they appear as buttons in the Warn message your users see

ECDSA Certificates

WatchGuard Training

ECDSA Certificates

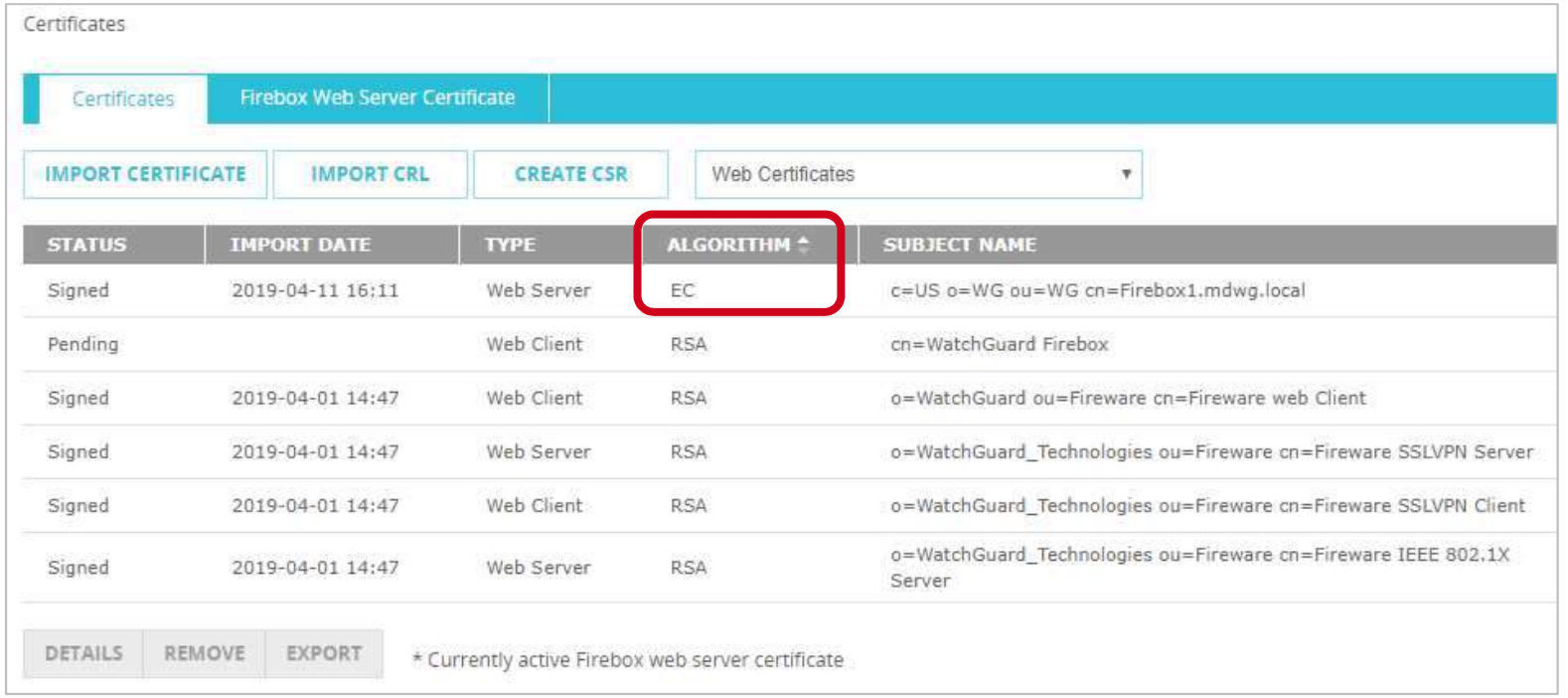
- The Firebox now supports Elliptic Curve Digital Signature Algorithm (ECDSA) certificates for BOVPN, BOVPN virtual interfaces, and Mobile VPN with IKEv2
- Compared to RSA, ECDSA certificates have equivalent security, smaller keys, and increased efficiency
- Governments in some countries require ECDSA certificates for regulation compliance

ECDSA Certificates

- ECDSA certificates are also known as EC certificates
- You must import EC certificates
  - The Firebox does not generate certificate signing requests for EC certificates
- The Firebox supports these elliptic curves:
  - Prime256v1
  - Secp384r1
  - Secp521r1

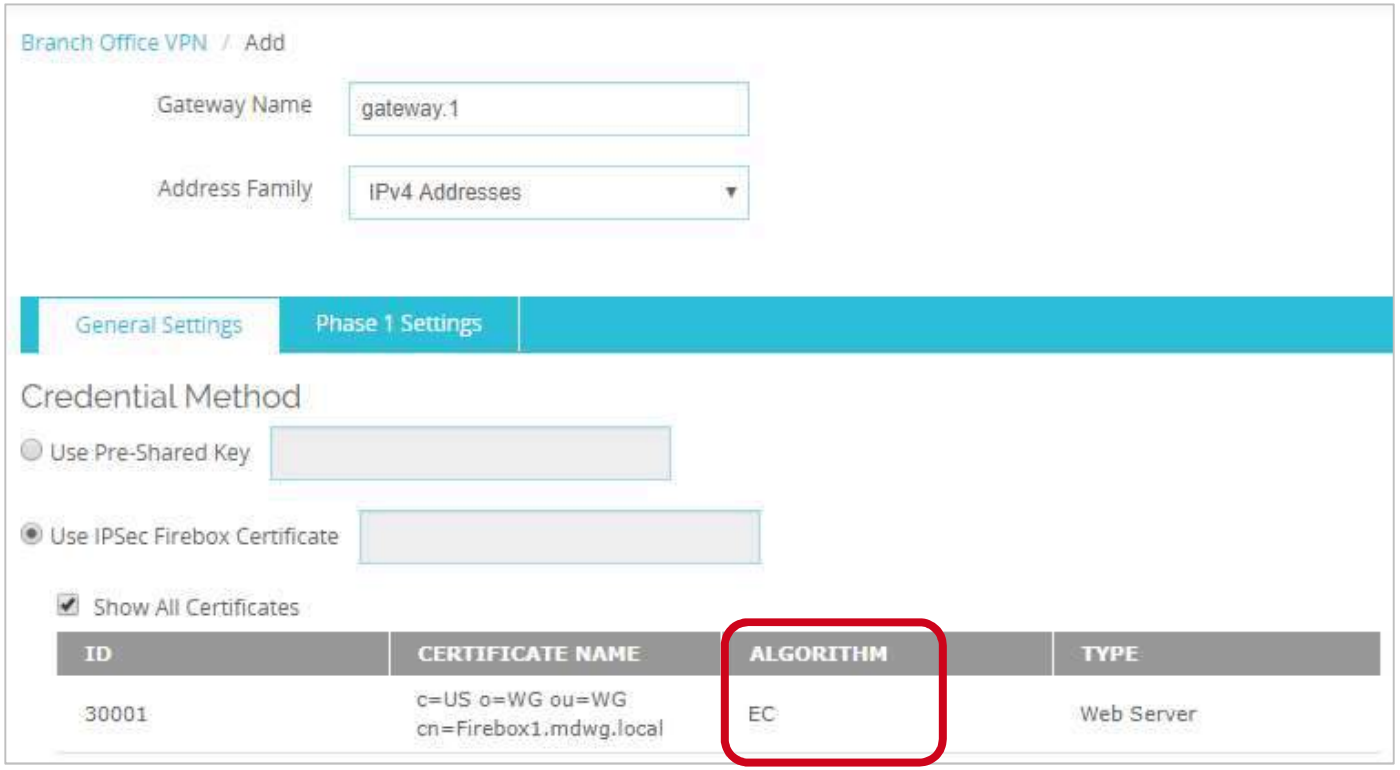
ECDSA Certificates for BOVPN and BOVPN VIF

- When you import an EC certificate on your Firebox, the algorithm appears as *EC*



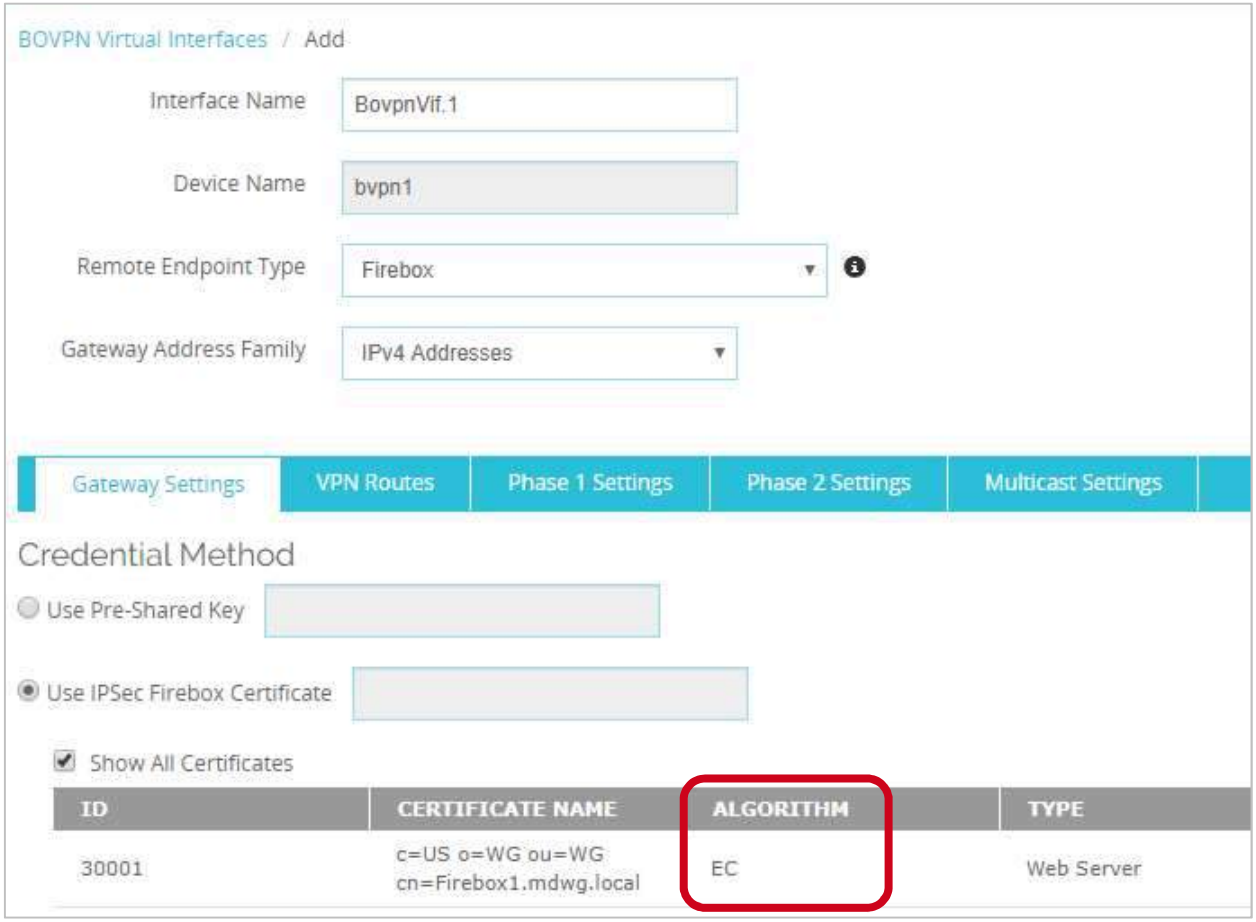
EC Certificates for BOVPN and BOVPN VIF

- In the BOVPN gateway and BOVPN virtual interface configurations, you can select an EC certificate
- BOVPN gateway



ECDSA Certificates for BOVPN and BOVPN VIF

- BOVPN virtual interface



ECDSA Certificates for BOVPN and BOVPN VIF

- BOVPNs and BOVPN virtual interfaces support EC certificates for IKEv1 and IKEv2
- BOVPN tunnels with IKEv1 —
  - If one VPN peer uses an EC certificate, the other peer must use an EC certificate
  - VPN peers can use EC certificates with different elliptic curves
    - The peer that initiates the VPN connection determines the authentication method
  - The EC certificate determines the Hash algorithm
    - For example, if you select SHA256-AES256-DH14 as the Phase 1 transform and specify an ECDSA-384 certificate, the Hash algorithm is SHA384 instead of SHA256

ECDSA Certificates for BOVPN and BOVPN VIF

- BOVPN tunnels with IKEv2 —
  - If one VPN peer uses an EC certificate, the other peer must use an EC certificate
  - VPN peers can have EC certificates with different elliptic curves
    - Each peer determines its own authentication method based on the EC certificate, which means peers can use different authentication methods

ECDSA Certificates for Mobile VPN with IKEv2

- The Firebox supports EC certificates for Mobile VPN with IKEv2
- IKEv2 clients must also support EC certificates, but support varies by operating system
  - **Windows 10** — Partial support (ECDSA-256 and ECDSA-384 only)
  - **Android** — Support with strongSwan, an open-source client
  - **macOS and iOS** — No support

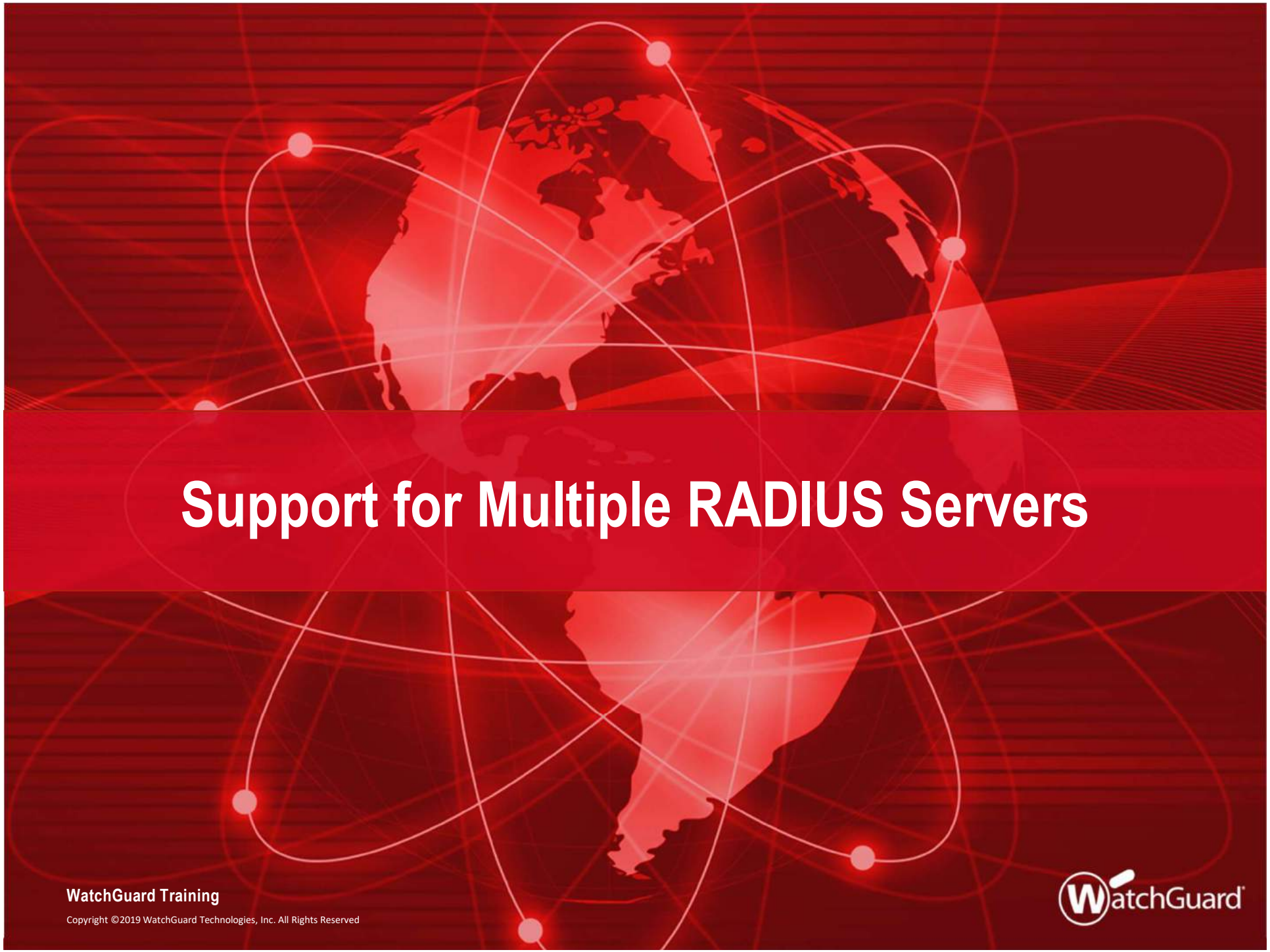
Gateway Wireless Controller Enhancements

WatchGuard Training

Gateway Wireless Controller Enhancements

- Added support for the upcoming AP327X platform
  - IP67-rated Outdoor AP
  - Dual Radio 802.11ac Wave 2
  - External antenna support

- Additional suffix support for AP firmware versions
  - x.x.x-xxx.x
  - Currently only the AP125 has an additional suffix in the firmware version: 8.6.0-644.3
  - Suffix does not appear in the UI when the AP is unpaired



Support for Multiple RADIUS Servers

WatchGuard Training

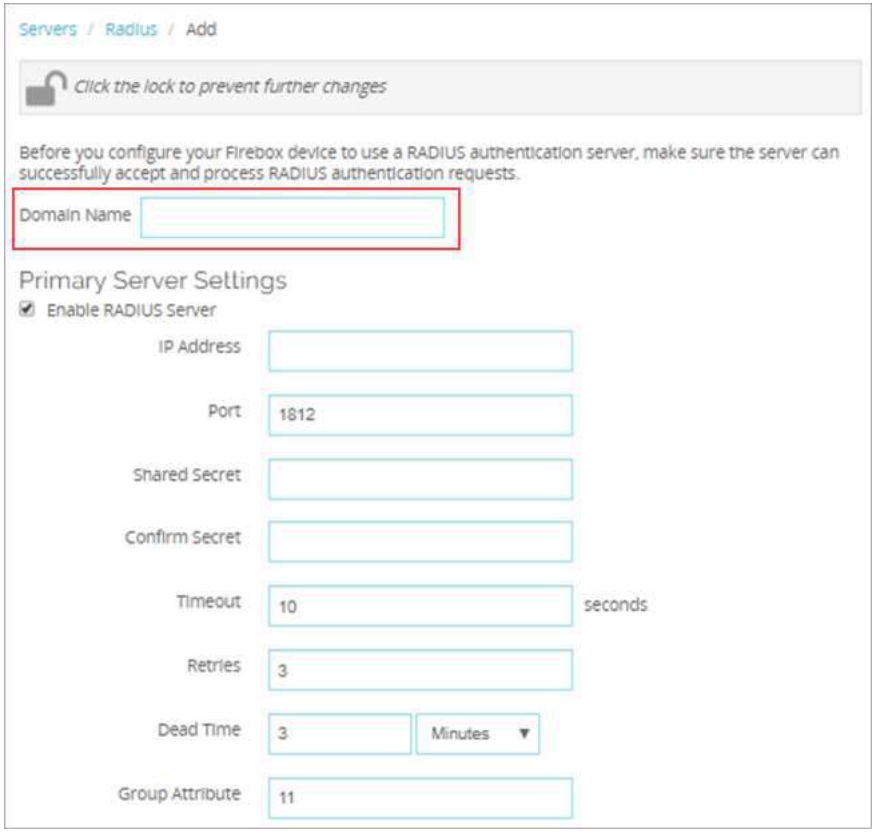
Multiple RADIUS Servers

Support for more than one RADIUS server in Web UI and WSM

- All features that supported RADIUS authentication servers now support multiple RADIUS authentication servers
- Improved workflow for adding a RADIUS server
- SecurID servers are now RADIUS servers with SecurID enabled

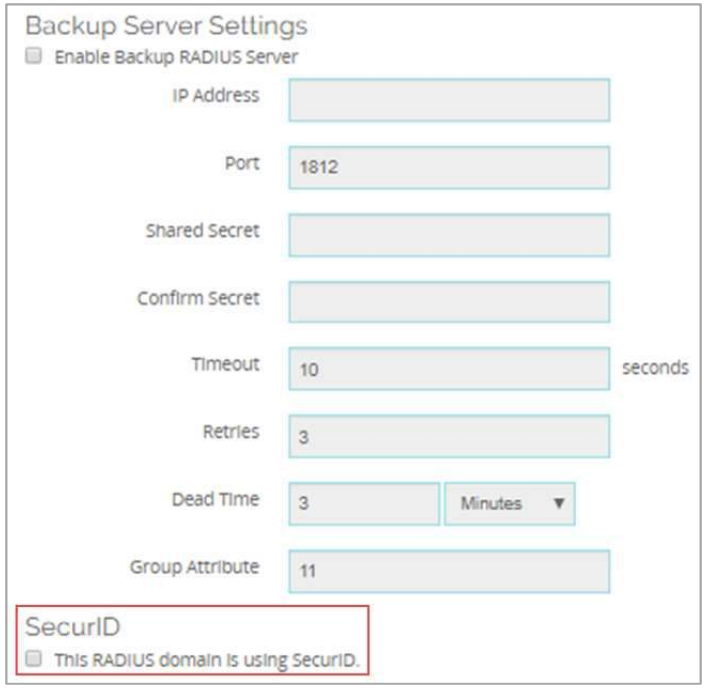
Unique Domain Names

- You must specify a unique Domain Name for each RADIUS Server
  - Important: You cannot edit the Domain Name after you add a server



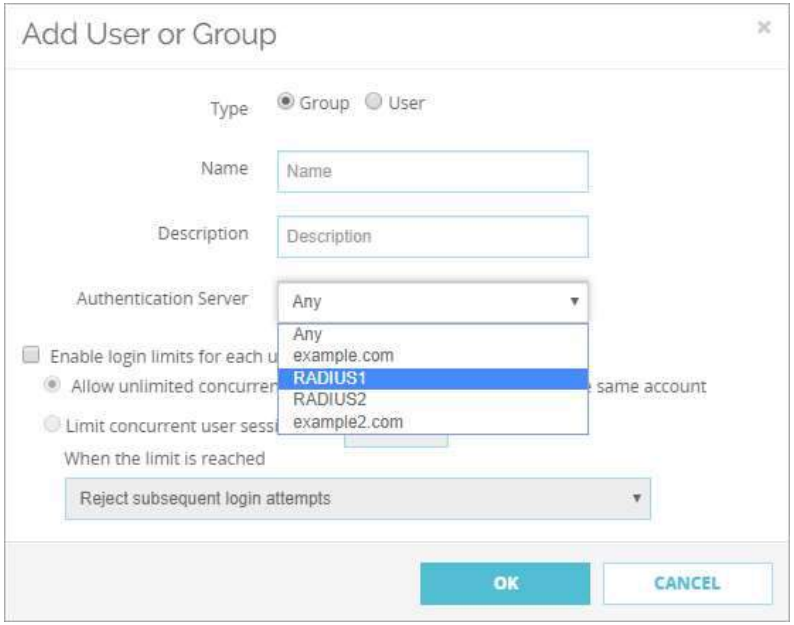
New SecurID option

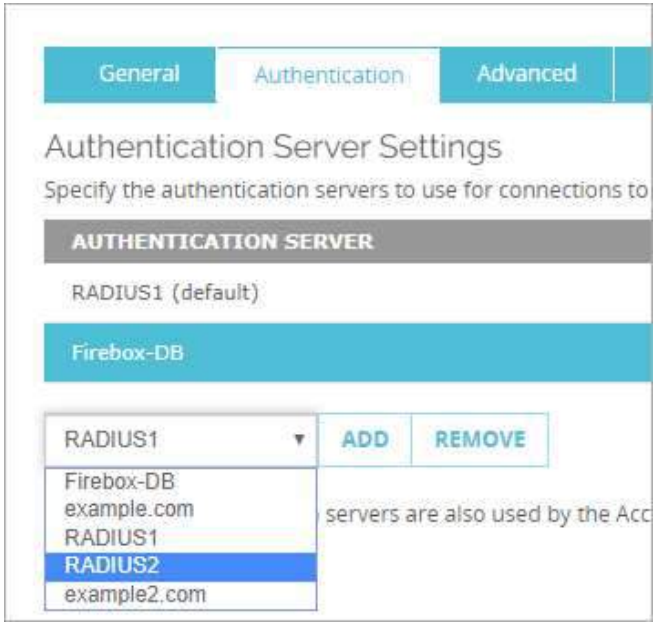
- SecurID cannot be configured as a standalone authentication server in v12.5
- We now have RADIUS servers with SecurID enabled
- New check box instead of a tab if RADIUS uses SecurID



RADIUS Servers Available in All Features

- In features that require authentication server configuration, all configured RADIUS servers appear in the drop-down lists
- If a server is RADIUS with SecurID enabled, it will not appear in lists for features not supported by SecurID





RADIUS Server Drop-Down Lists

- Users and Groups
- Mobile VPN with IKEv2
- Mobile VPN with L2TP
- Mobile VPNS with SSL
- Mobile VPN with IPSec
- Default Authentication Servers
- **System > Users and Roles**
- **Hotspot > Guest Administrators**
- Wireless Access Point – only with *WPA, WPA2 or WPA/WPA2*
- **Access Portal > User Connection Settings**
- 4100 authentication page – *Default server appears first*
- Web UI Login page – *Must select RADIUS first, then the appropriate RADIUS server*

RADIUS + SecurID Servers Not Available

- If SecurID is enabled for the RADIUS server, the server does not appear in the Authentication Server drop-down list for features that do not support SecurID
  - Mobile VPN with IKEv2
  - Mobile VPN with L2TP
  - **Hotspot > Guest Administrators**
  - Wireless Access Point

Upgrade Considerations

- After you upgrade to Fireware v12.5, any previously configured SecurID servers become RADIUS servers with SecurID enabled

No changes to:

- RADIUS SSO
- Gateway Wireless Controller

WatchGuard Training