What's New in Fireware v12.1.1

WatchGuard Training

What's New in Fireware v12.1.1

- DNSWatch
- New Dynamic DNS Providers
- Firebox Wireless Enhancements
- Networking Enhancements
  - USB Modem Support
  - Hot Plug Modem Support
  - DHCP Server Gateway Enhancements
  - VLAN Traffic Setting Enhancements

What's New in Fireware v12.1.1

- BOVPN over TLS Support for WatchGuard System Manager and Policy Manager
- Content inspection settings moved from HTTPS proxy actions to TLS profiles

New DNSWatch Service

WatchGuard Training

DNSWatch Threat Intelligence

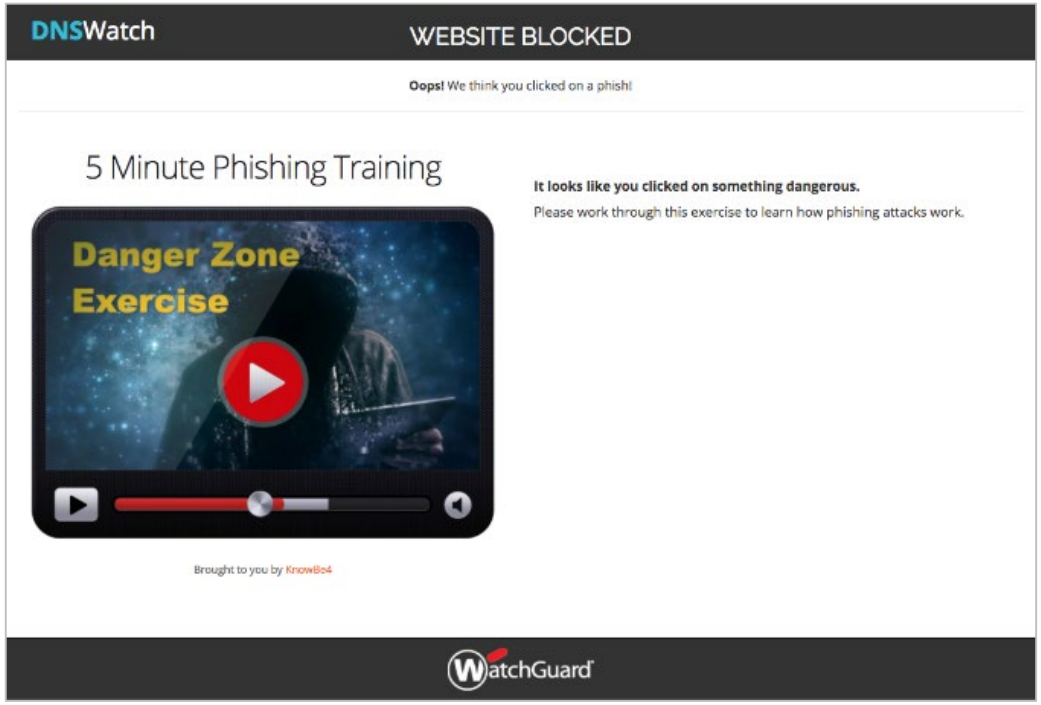
- WatchGuard uses a complex set of heuristics to identify malicious certificates and websites
- DNSWatch polls threat intelligence sources daily to identify new malicious domains and update the Domain Feeds
- DNSWatch users can also share domains they manually add to the DNSWatch Blacklist with WatchGuard to help improve DNSWatch for all users

DNSWatch and the Firebox

- When the Firebox receives a DNS query from a host on a protected network, it forwards the request to DNSWatch
- DNSWatch evaluates whether the domain is a known threat
  - If the domain is not a known threat:
    - DNSWatch resolves the DNS query to the destination
  - If the domain is a known threat:
    - DNSWatch resolves the domain to the IP address of the DNSWatch Blackhole Server
    - The DNSWatch Blackhole Server attempts to gather more information about the threat from the host endpoint
    - For HTTP and HTTPS requests, the DNSWatch Blackhole Server displays a customizable deny page to the user

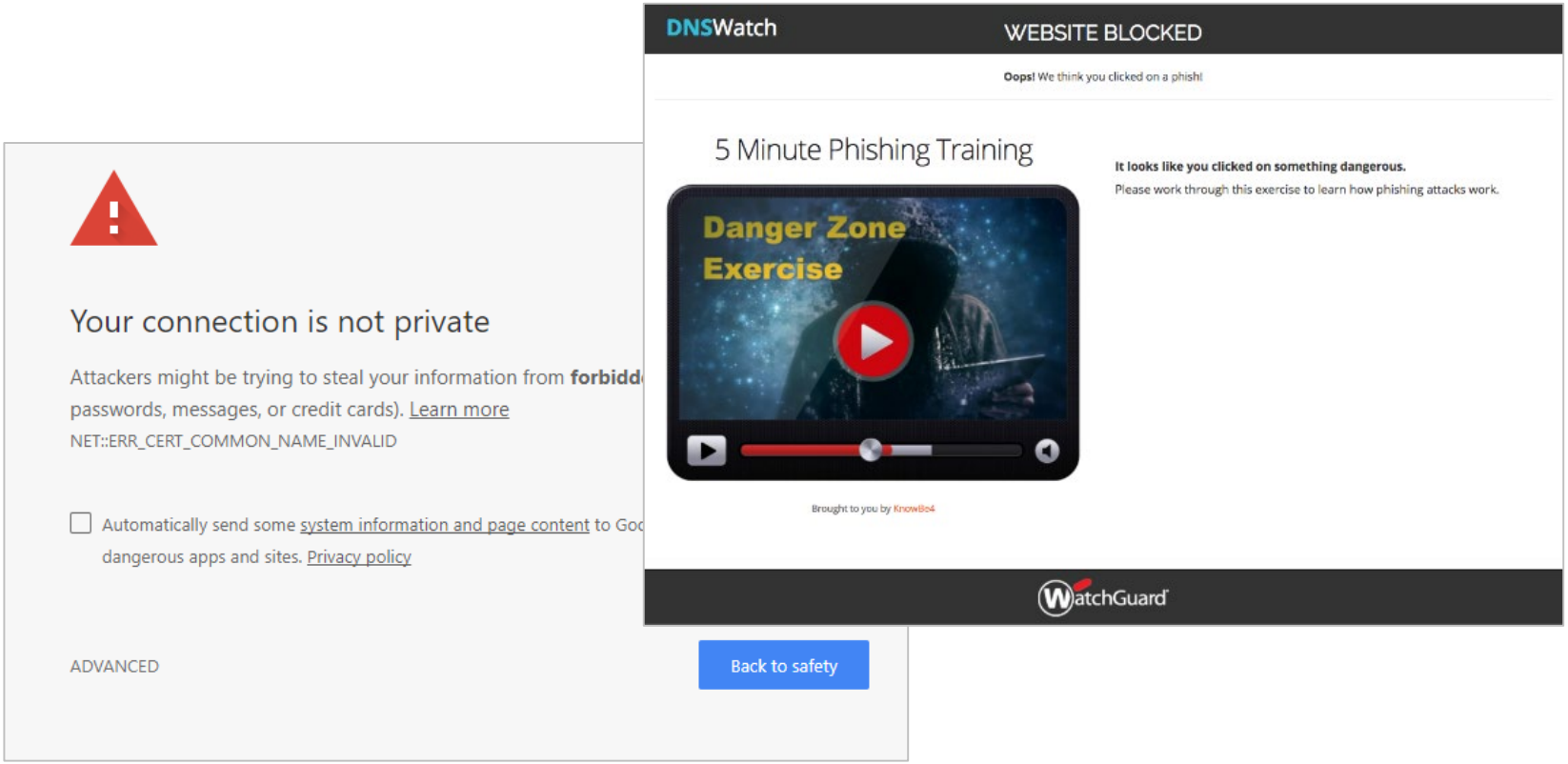
DNSWatch Deny Page

- When an HTTP connection is blocked, a customizable deny page appears to the user
- The Deny Page includes a short training exercise about how to recognize phishing attacks



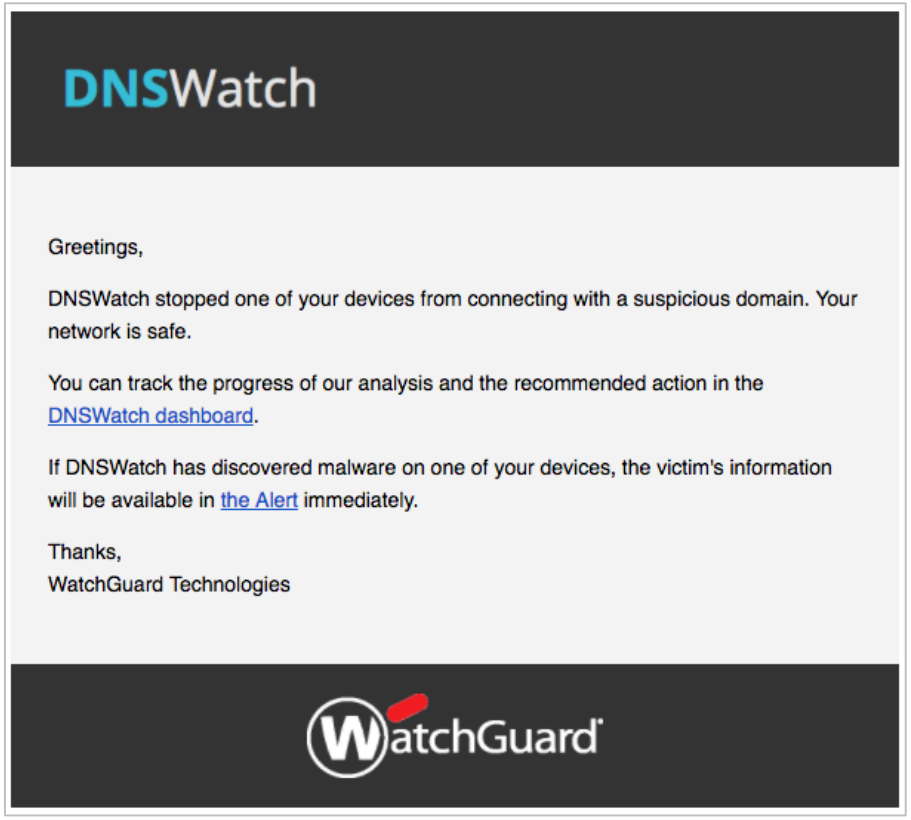
DNSWatch Deny Page

- For a denied HTTPS connection, an invalid certificate notice appears first
- The Deny Page appears only if the user continues to the site



DNSWatch Email Alerts

- When DNSWatch denies a connection, DNSWatch sends an email alert to account administrators, with a link to alert details

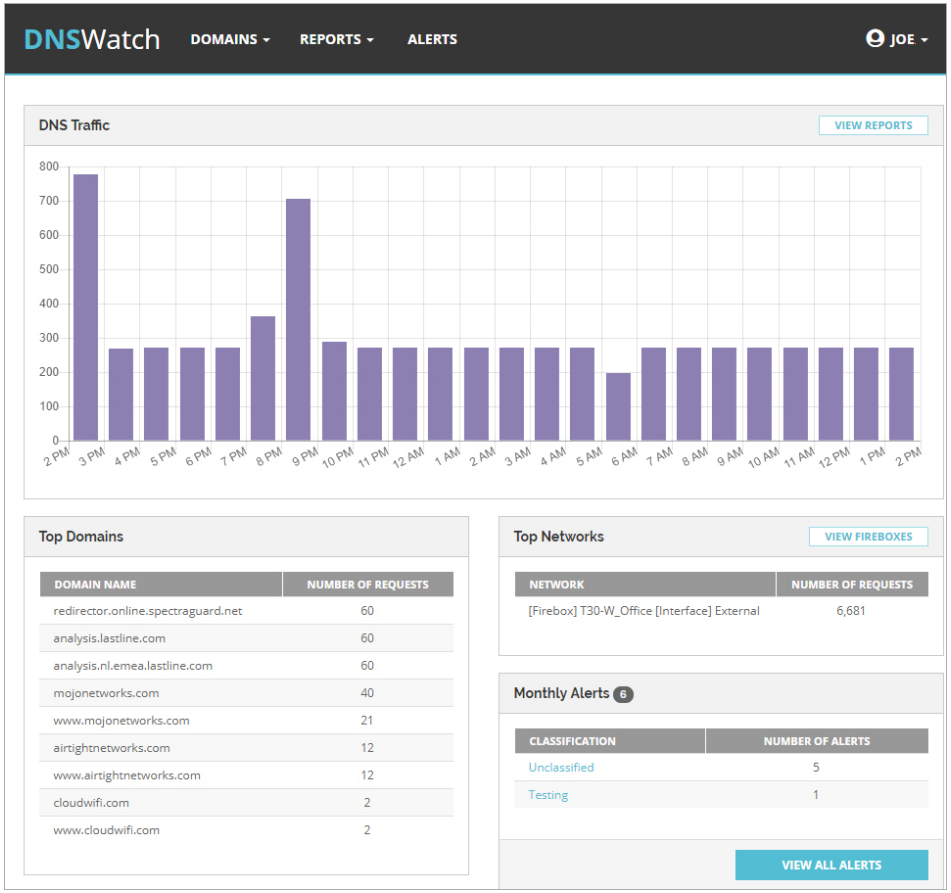


Manage DNSWatch

- After you activate DNSWatch for a Firebox in your account, you can connect to DNSWatch in the WatchGuard Portal
- In the WatchGuard Support Center, select **My WatchGuard > Manage DNSWatch**

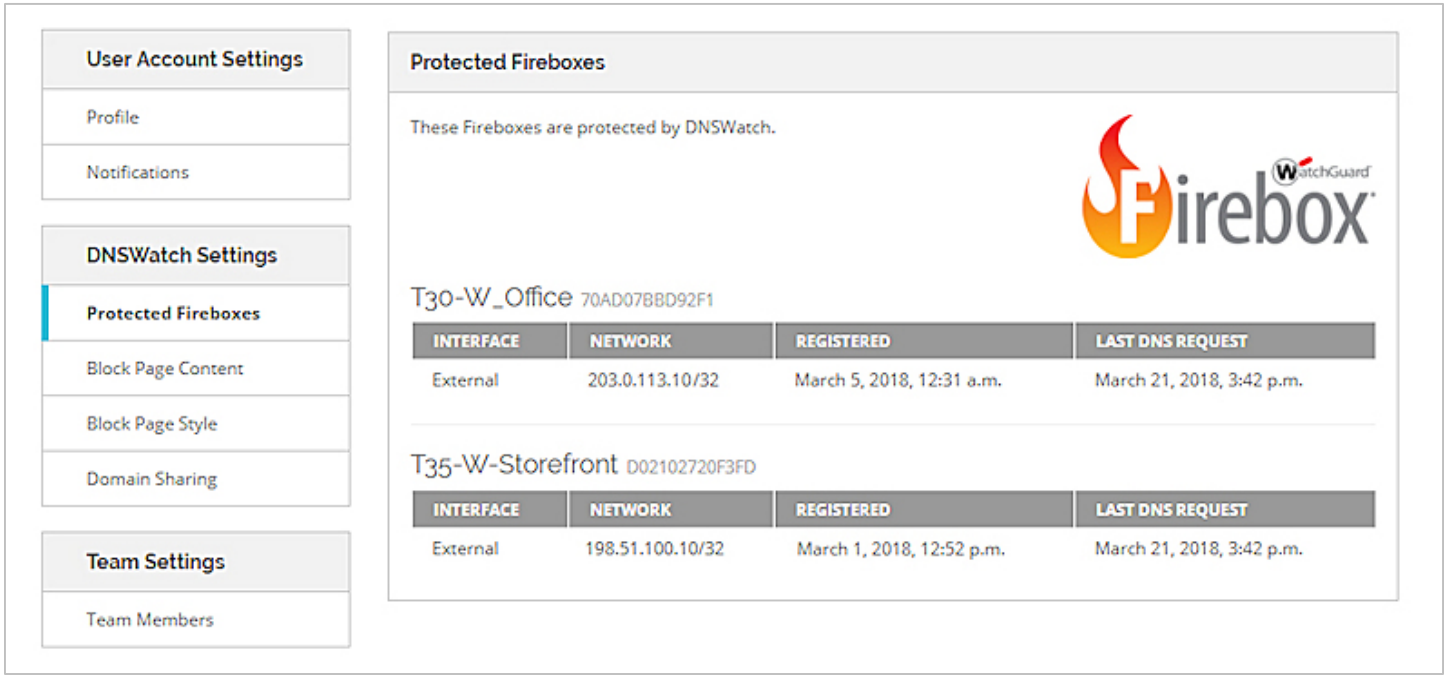
DNSWatch Dashboard

- The DNSWatch Dashboard provides:
  - DNS traffic data
  - Top domain requests
  - Top network requests
  - Monthly alert summary



DNSWatch Protected Fireboxes

- To see a list of your protected Fireboxes:
  1. Click your user name and select **Settings**
  2. Select **Protected Fireboxes**



Learn More

- For information about how to get started with DNSWatch and to get more information about the service, see:
  - **Get Started with DNSWatch (download from Centercode)**
  - **Introduction to DNSWatch**

Dynamic DNS Providers

WatchGuard Training

Dynamic DNS Providers

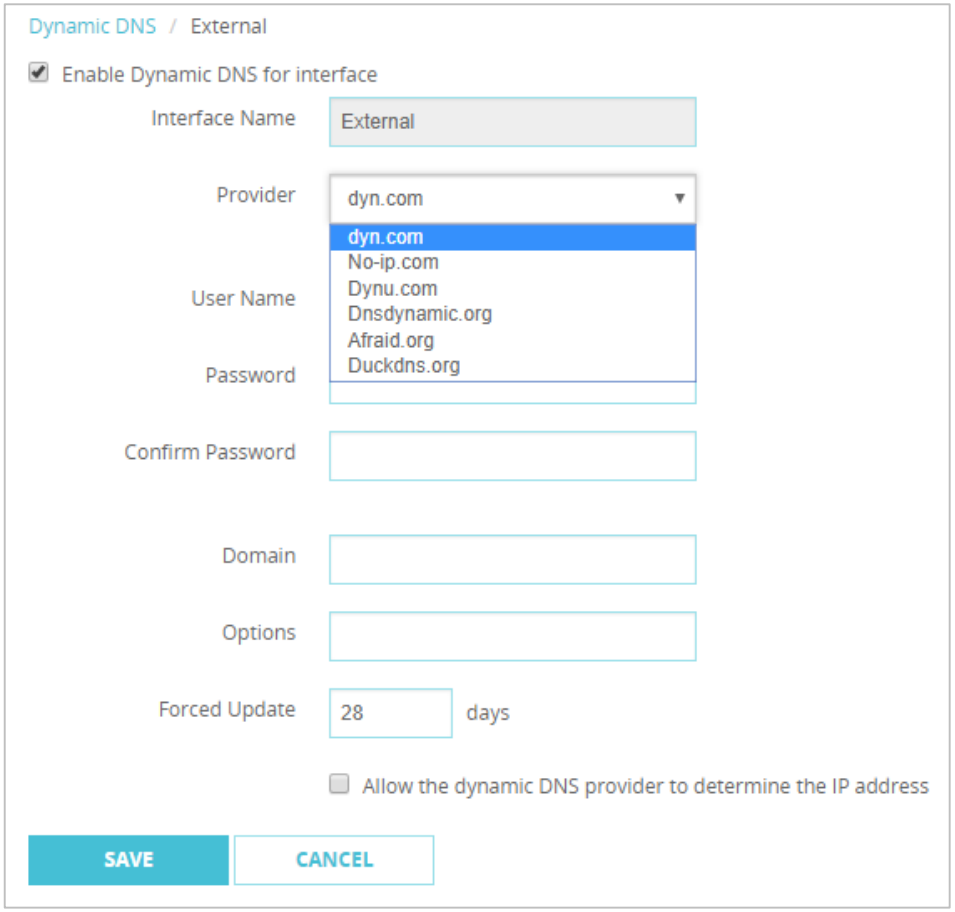
- Fireware now supports multiple dynamic DNS vendors
- With more dynamic DNS vendors in the market, WatchGuard can now provide several dynamic DNS options as part of our commitment to consumer choice

Dynamic DNS Providers

- Fireware supports these free dynamic DNS providers:
  - No-IP
  - Dynu
  - DNSdynamic
  - Afraid.org
  - Duck DNS
- Fireware continues to support Dyn, a dynamic DNS provider with tiered pricing

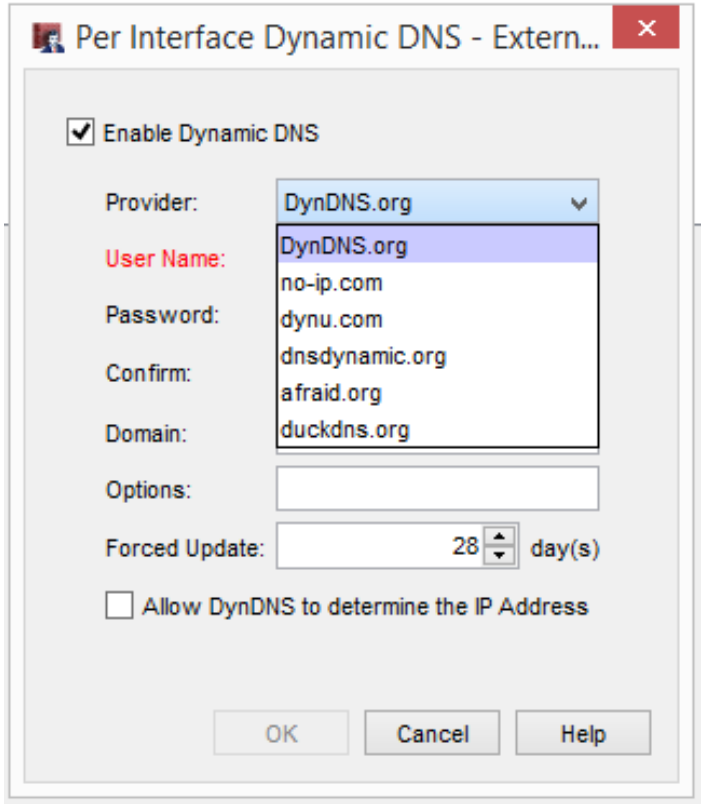
Dynamic DNS Providers

- Fireware Web UI



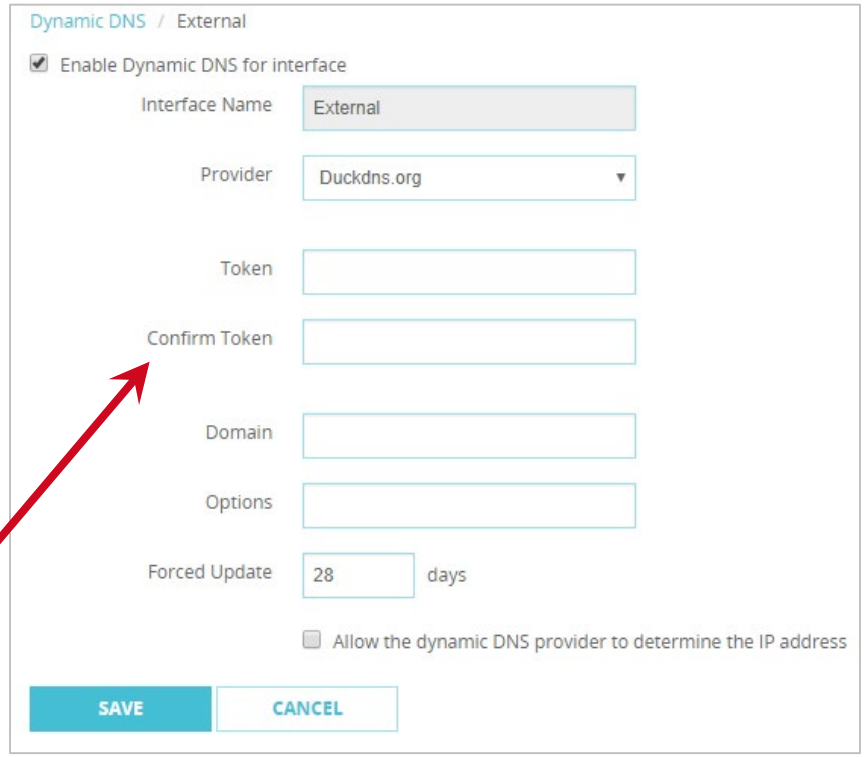
Dynamic DNS Providers

- Policy Manager



Dynamic DNS Providers

- The configuration process for Duck DNS is different from other providers
- You must log in to the Duck DNS website with a social network account or Google account
- To configure Duck DNS as a provider, you must specify a token for authentication instead of a user name and password



Firebox Wireless Enhancements

WatchGuard Training

Firebox Wireless Enhancements

- You can now disconnect wireless clients from a Firebox from the **System Status > Wireless Statistics** page
- When you disable the wireless interfaces on a Firebox, the configuration of your interfaces is now preserved if you enable the wireless interfaces again
- You can no longer save a Firebox configuration if the insecure WEP shared key encryption mode is selected for wireless security on an SSID

Networking Enhancements

WatchGuard Training

USB Modem Support

- Fireware now supports the Verizon Global Modem USB730L (Vendor ID 0x1410, Product ID 0x9032)

Hot Plug Modem Support

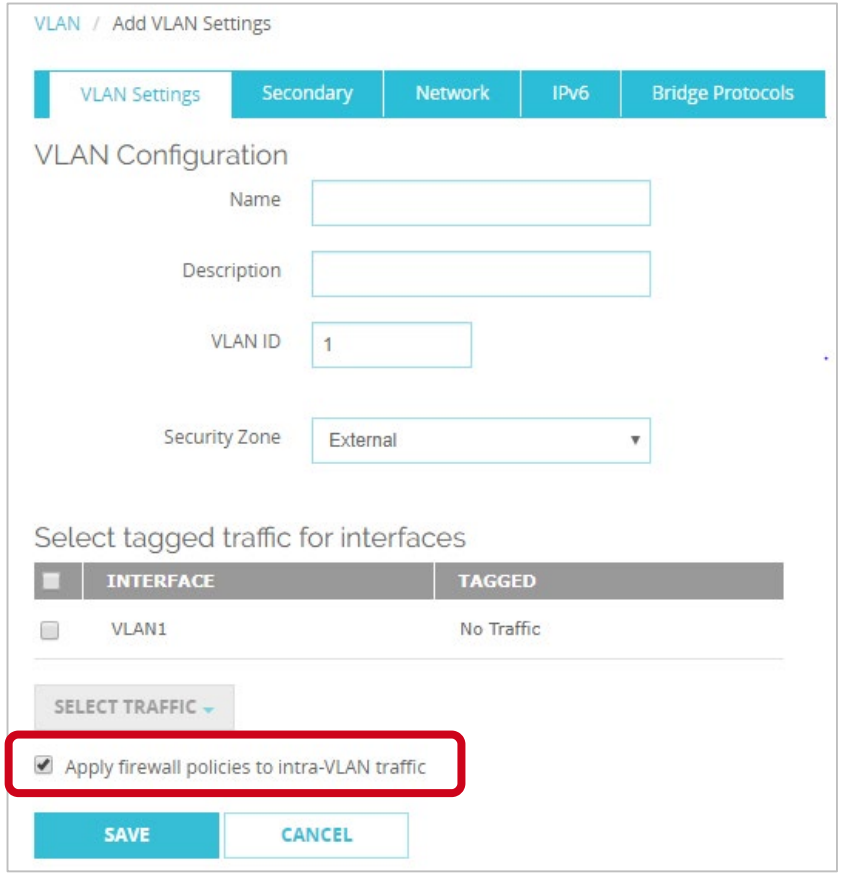
- You can now hot plug USB modems into the Firebox
- The modem operates and does not require you to reboot the Firebox when:
  - You plug in a new modem
  - You unplug a modem and plug it in again
  - The modem unexpectedly disconnects and reconnects to the Firebox
- If you unplug a modem and plug in a new modem that is a different model, you must update the modem configuration settings on the Firebox; you do not have to reboot the Firebox

Hot Plug Modem Support

- You can hot plug modems into the Firebox up to 10 times before you must reboot the Firebox
  - For example, when you hot plug a modem into the Firebox for the eleventh time, you must reboot the Firebox before the modem will operate

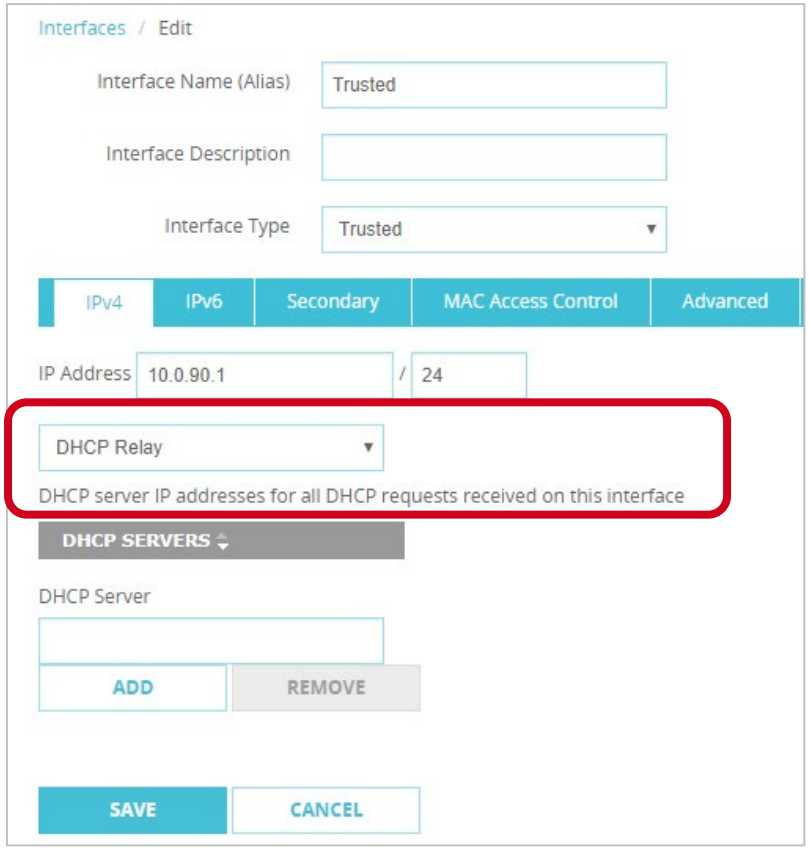
VLAN Traffic Settings

- When you create an external VLAN interface, the **Apply firewall policies to intra-VLAN traffic** option is now enabled by default



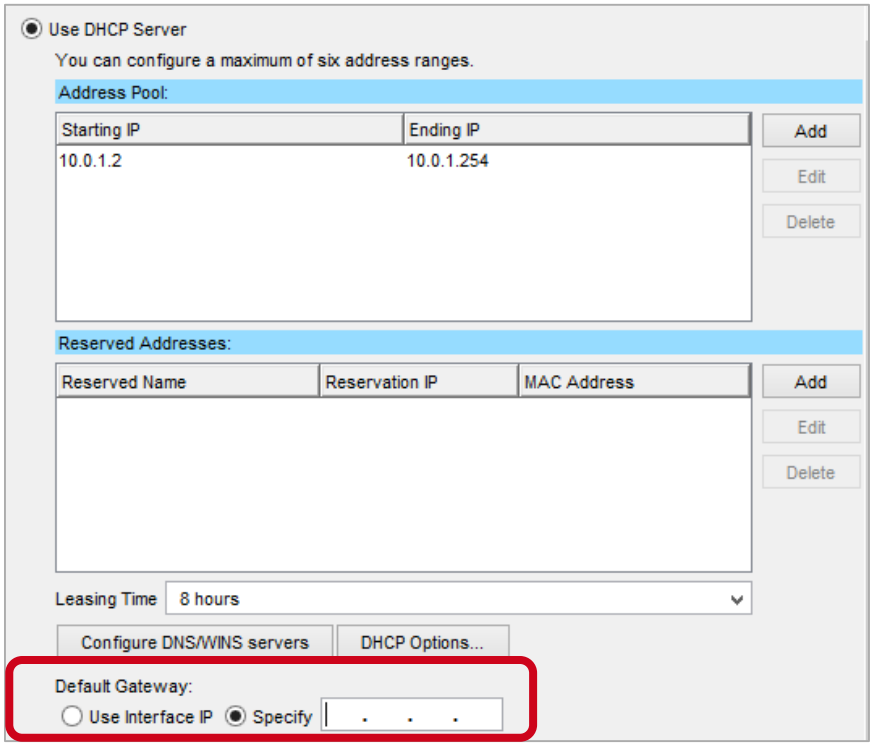
DHCP Relay Server

- When you enable DHCP Relay on an interface, the DHCP relay servers you specify now apply only to that interface



DHCP Server Gateway

- For a Firebox interface configured as a DHCP server, you can now specify a default gateway IP address that is not the Firebox interface IP address
- This is useful in complex environments with multiple gateways
  - Typical example — Voice over IP (VoIP) where phones use their own gateway on the network for VoIP service



BOVPN over TLS Support

WatchGuard Training

BOVPN over TLS Benefits

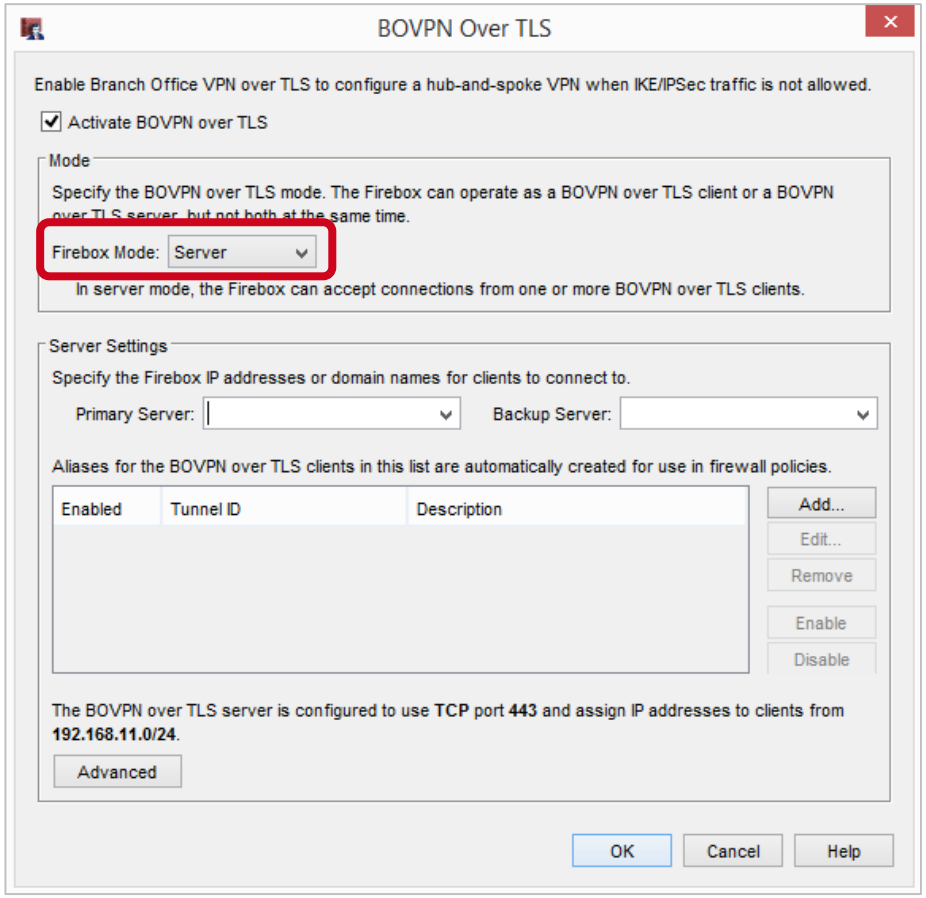
- BOVPN over TLS is a recent addition and offers an alternative to IPsec BOVPNs
- This feature was first supported in Fireware Web UI in Fireware v12.1
- Fireware v12.1.1 adds BOVPN over TLS support to WatchGuard System Manager (WSM) and Policy Manager; this feature is now supported across all WatchGuard user interfaces

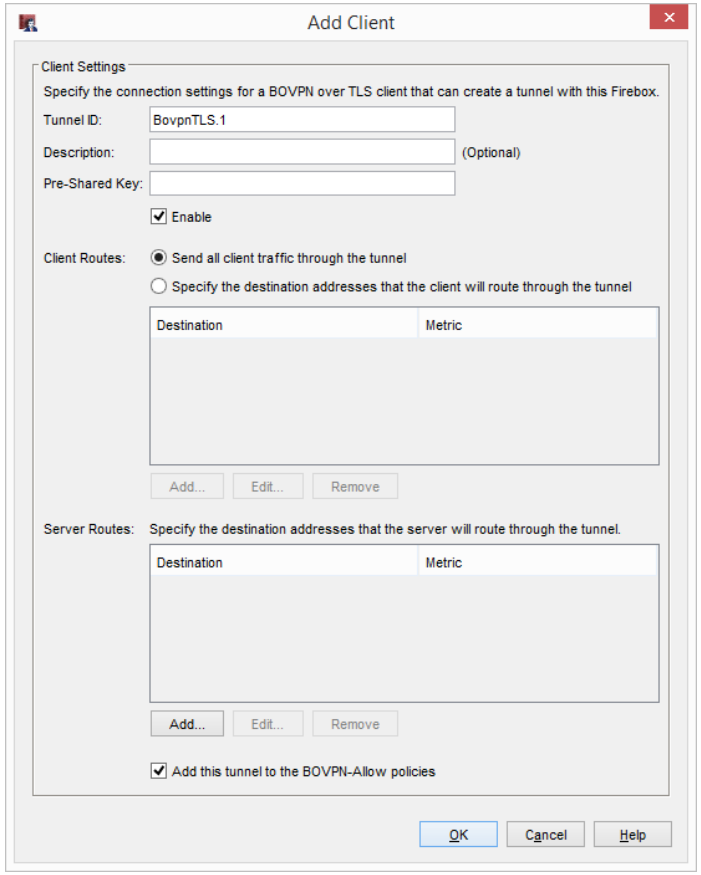
BOVPN over TLS Support for WSM and PM

- BOVPN over TLS allows you to enable a TLS tunnel between Fireboxes, and is an alternative BOVPN solution when your network does not support IPSec traffic
- Server mode and Client mode are supported

BOVPN over TLS Support for WSM and PM

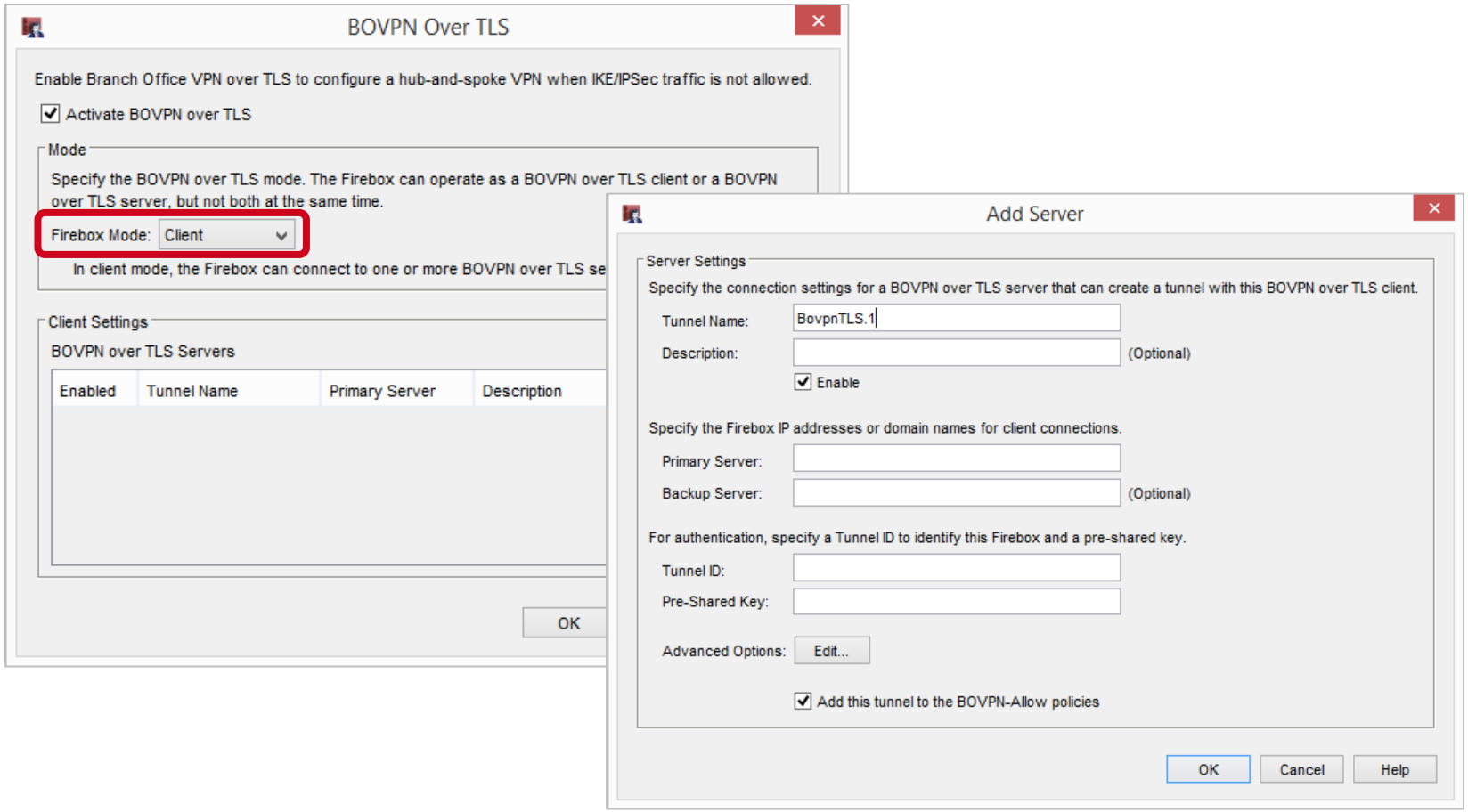
- Server mode in Policy Manager





BOVPN over TLS Support for WSM and PM

- Client mode in Policy Manager



HTTPS & TLS Profiles

WatchGuard Training

HTTPS & TLS Profiles

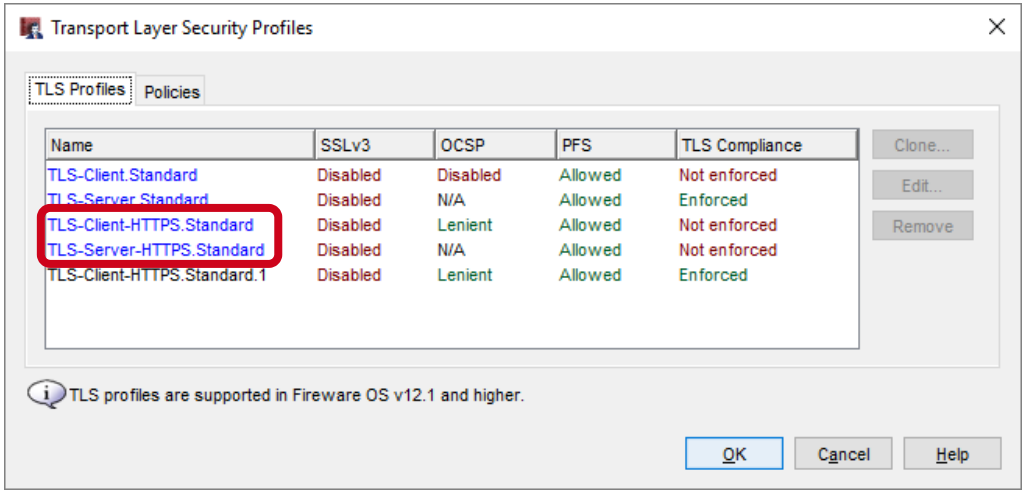
- WatchGuard continues to innovate our content inspection features to assist users in secure policy configuration
- TLS profiles contain the settings used for content inspection by proxy actions
  - You can use the same TLS profile for multiple policies
  - TLS profiles make it easier to configure and apply consistent settings for content inspection across multiple proxies

HTTPS & TLS Profiles

- Fireware v12.1 supported TLS profiles in the IMAP proxy
- Fireware v12.1.1 adds TLS profiles in the HTTPS proxy
- The content inspection settings have been moved from the HTTPS proxy actions to two new TLS profiles
  - TLS-Client-HTTPS.Standard — Settings used by an HTTPS client proxy action
  - TLS-Server-HTTPS.Standard — Settings used by the HTTPS server proxy action

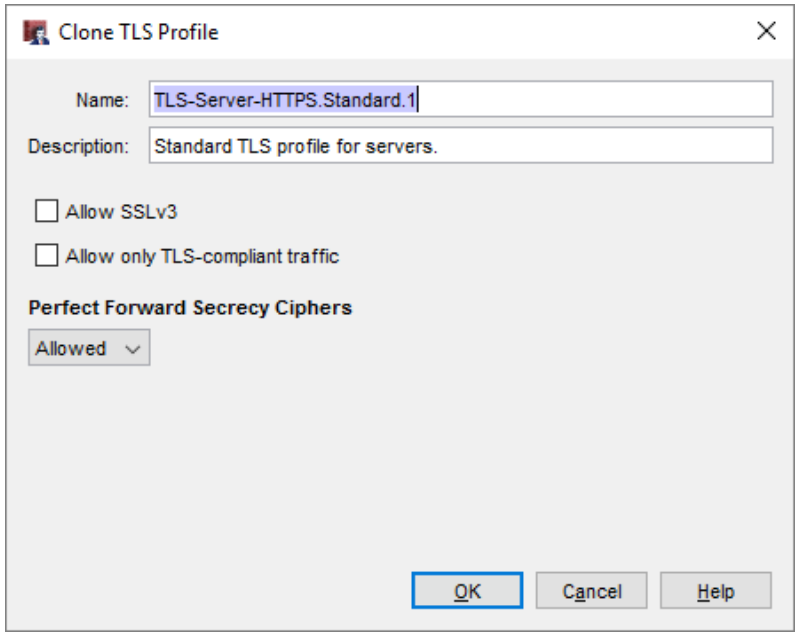
HTTPS & TLS Profiles

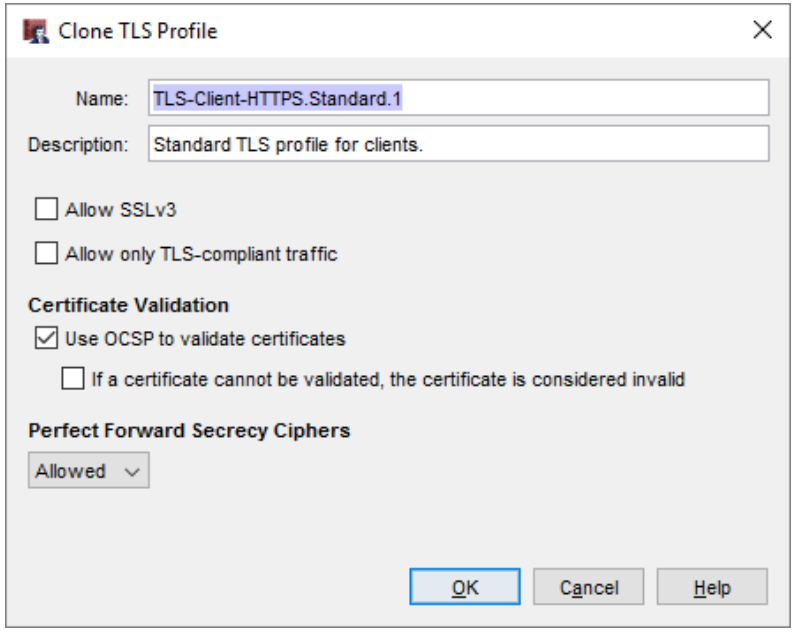
- You now configure content inspection settings in a TLS profile
- In Policy Manager, select **Setup > Actions > TLS Profiles**
- The **TLS Profiles** tab now has two predefined profiles for HTTPS proxies:
  - TLS-Client-HTTPS.Standard
  - TLS-Server-HTTPS.Standard



HTTPS & TLS Profiles

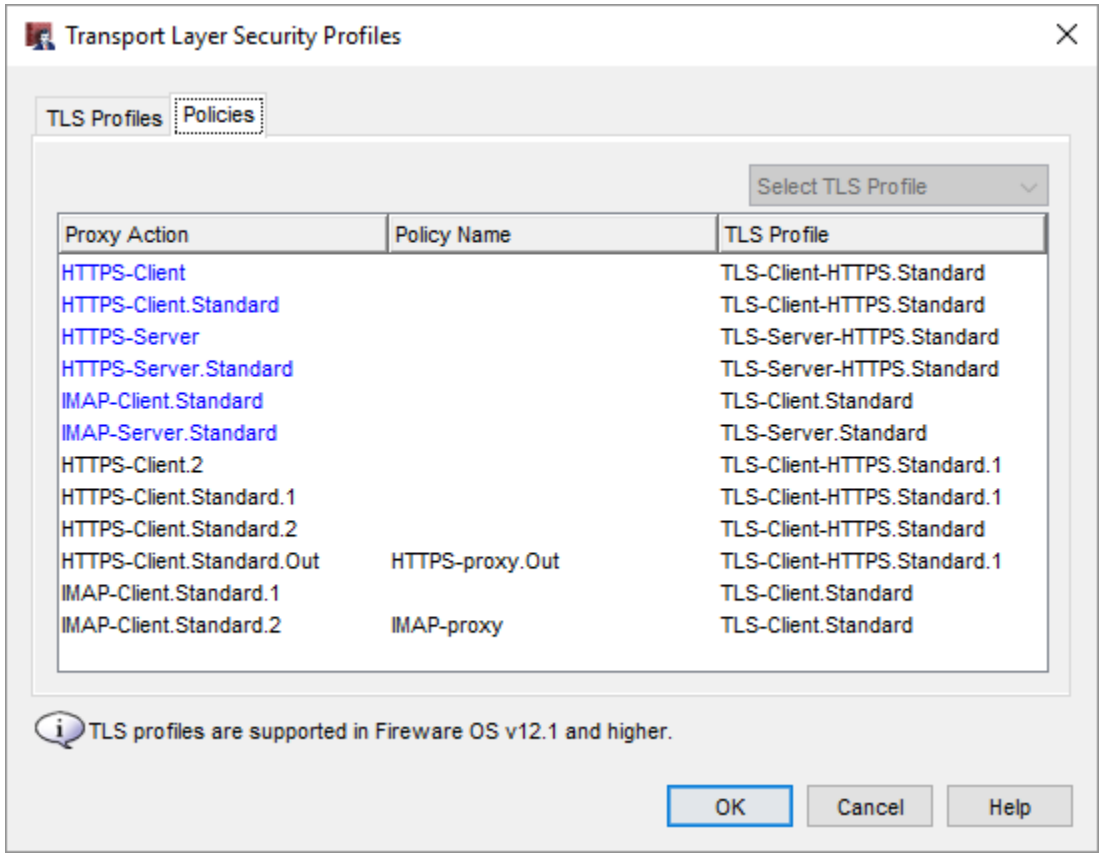
- The predefined HTTPS TLS profiles have different settings
  - Only the TLS-Client-HTTPS profile has OCSP settings for certificate validation
- To create a custom TLS profile, clone a predefined TLS profile





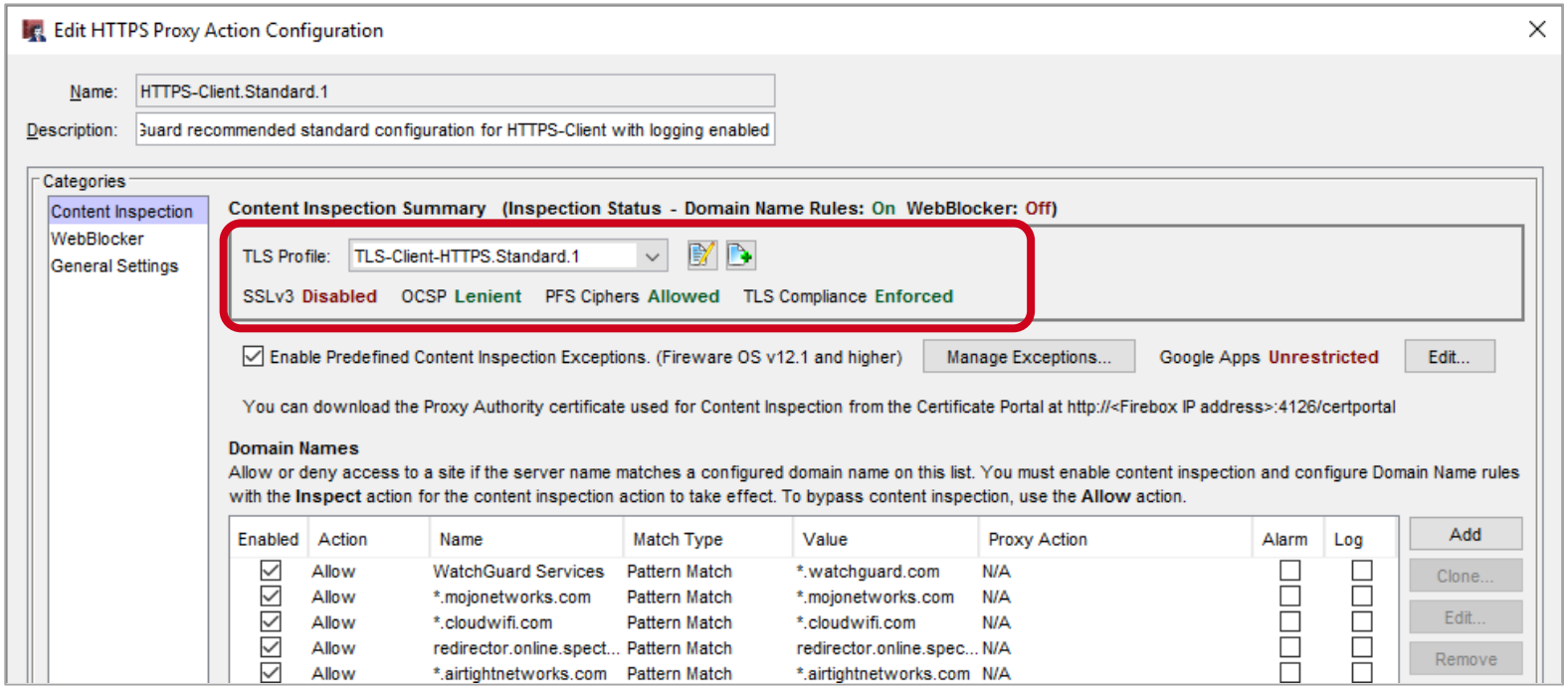
HTTPS & TLS Profiles

- On the **Policies** tab, you can assign a TLS profile to a proxy action



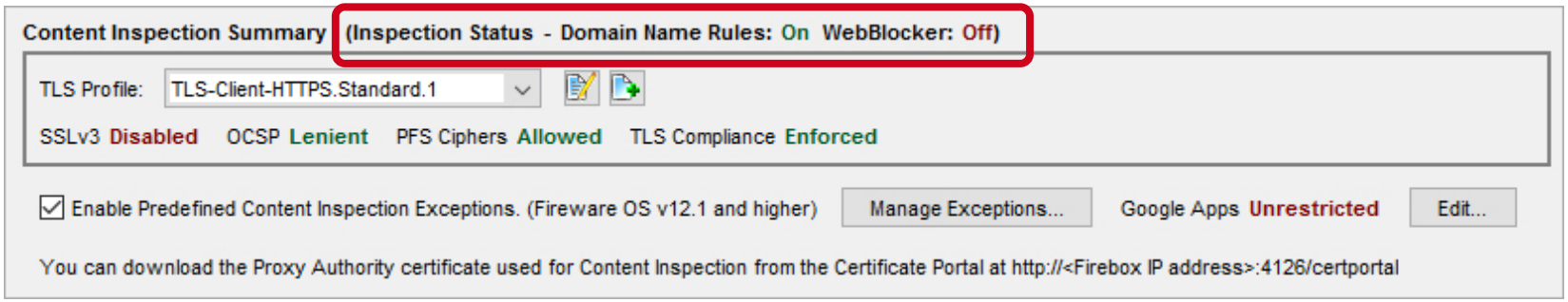
HTTPS & TLS Profiles

- In the **Content Inspection** settings in the HTTPS proxy action, you select the TLS profile
- The settings for the selected TLS profile appear below the **TLS Profile** drop-down list



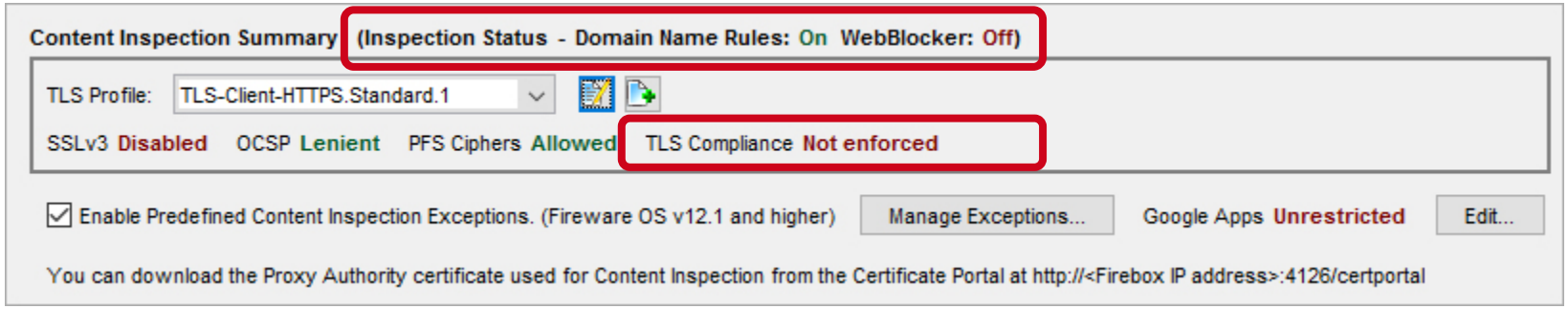
HTTPS & TLS Profiles

- The HTTPS proxy action no longer includes the **Enable content inspection** check box
- To enable content inspection, select the **Inspect** action in the Domain Names or the WebBlocker settings in the proxy action
- The **Inspection Status** shows whether the Inspect action is configured in the Domain Names or WebBlocker proxy action settings



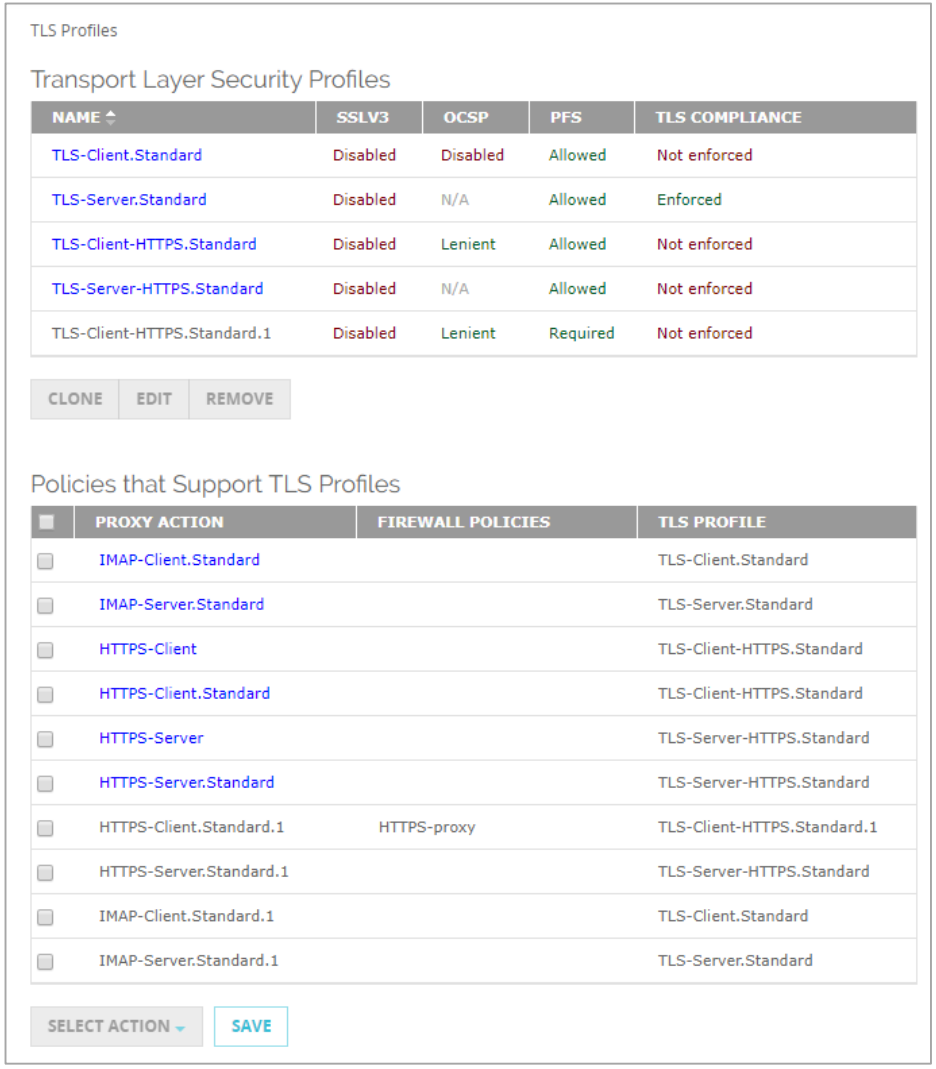
HTTPS & TLS Profiles

- With Fireware v12.1.1, you can enable content inspection and not enforce TLS compliance
  - This can enable some applications (such as Skype) to function when content inspection is enabled
- **SSL Compliance** is now called **TLS Compliance**
  - There is no change in functionality, just a more accurate name



HTTPS & TLS Profiles

- To configure TLS profiles from Fireware Web UI, select **Firewall > TLS Profiles**



HTTPS & TLS Profiles

- When you upgrade a Firebox to Fireware v12.1.1, HTTPS proxy actions are automatically updated
  - For any HTTPS proxy actions with content inspection enabled, the content inspection settings are moved to a new TLS profile
  - The HTTPS proxy action uses the new TLS profile

HTTPS & TLS Profiles

- If you use Policy Manager v12.1.1 to manage a Firebox that runs a lower version of Fireware:
  - You configure the content inspection settings in a TLS profile
  - When you save the configuration to the Firebox, the configuration is automatically changed to be compatible with the lower Fireware version
  - If you open the older configuration in Fireware Web UI, the content inspection settings are still configured in the proxy action
- For a v12.1.1 Device Configuration Template, if you apply the template to a Firebox that runs a lower version of Fireware, the default TLS Profile setting for that version of Fireware is applied to the Firebox

Thank You!