



# What's New in Fireware v12.1.1

# 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

# DNSWatch Threat Intelligence

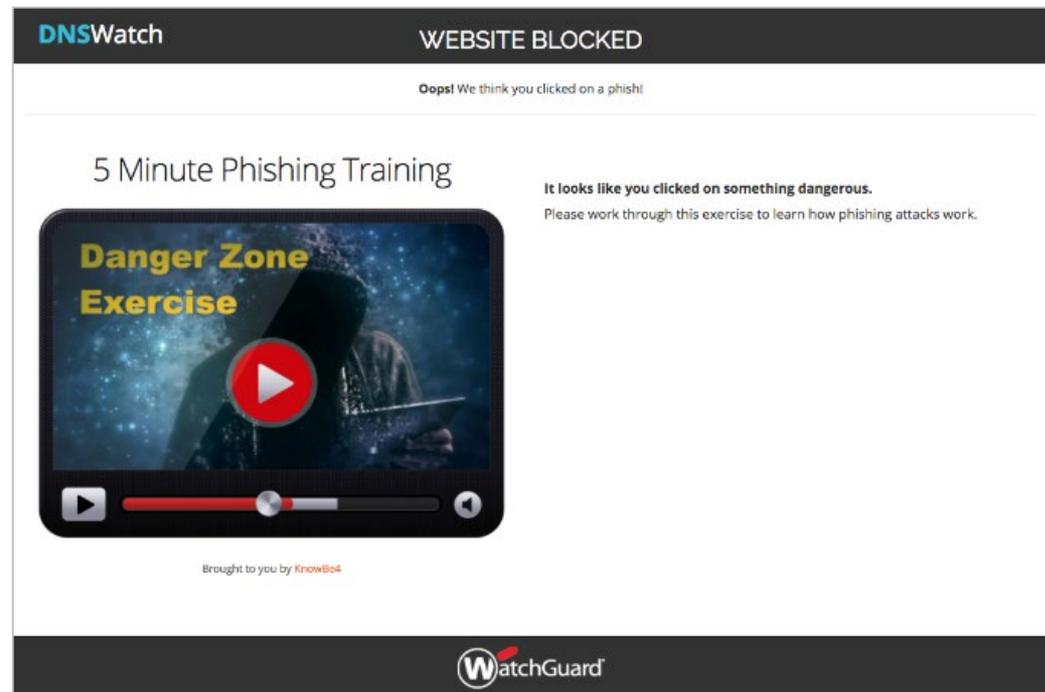
- WatchGuard uses a complex set of heuristics to identify malicious certificates and websites
- DNSWatch polls threat intelligence sources daily to identify new malicious domains and update the Domain Feeds
- DNSWatch users can also share domains they manually add to the DNSWatch Blacklist with WatchGuard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

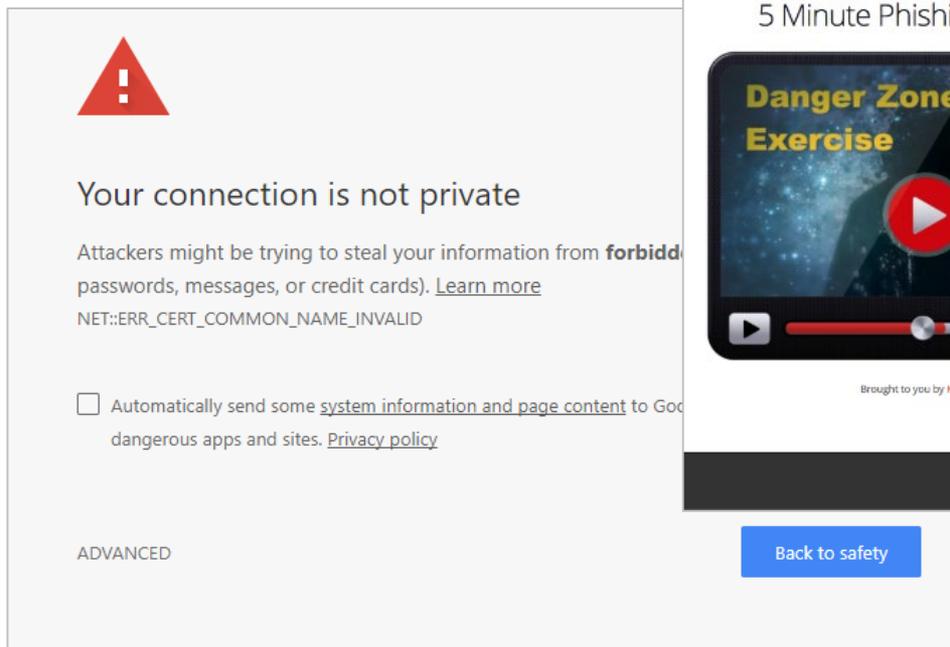
# DNSWatch Deny Page

- 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



A screenshot of a browser security warning. At the top left is a red triangle with a white exclamation mark. Below it, the text reads: "Your connection is not private". A paragraph follows: "Attackers might be trying to steal your information from **forbidden** (https://www.example.com/). This error can be caused by a misconfigured browser (e.g., missing certificates) or by a corrupted browser cache. (Learn more about this error.)" Below this is a checkbox: "Automatically send some system information and page content to Google Analytics to help improve our products. You can turn this off at any time. [Privacy policy](#)". At the bottom left, the word "ADVANCED" is displayed.

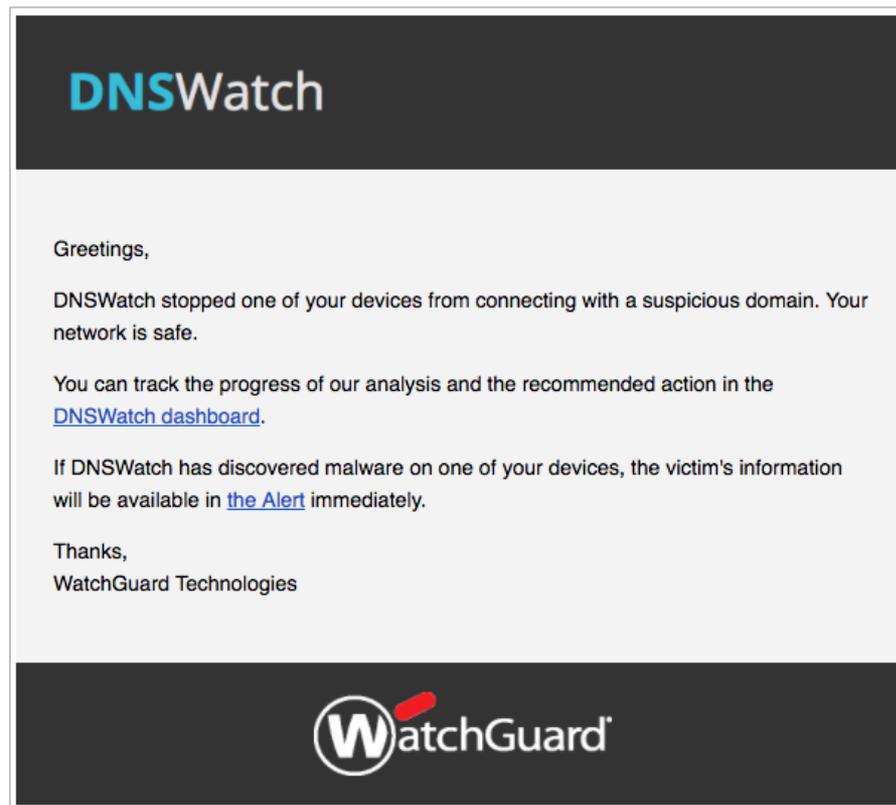


A screenshot of a "WEBSITE BLOCKED" page. The top left corner has the "DNSWatch" logo. The top right corner says "WEBSITE BLOCKED". Below that, it says "Oops! We think you clicked on a phisht". The main content area features a video player titled "5 Minute Phishing Training". The video thumbnail shows a person in a dark hoodie with the text "Danger Zone Exercise" overlaid. To the right of the video, it says "It looks like you clicked on something dangerous. Please work through this exercise to learn how phishing attacks work." Below the video player, it says "Brought to you by KnowBe4". At the bottom right, the WatchGuard logo is visible.

Back to safety

# DNSWatch Email Alerts

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



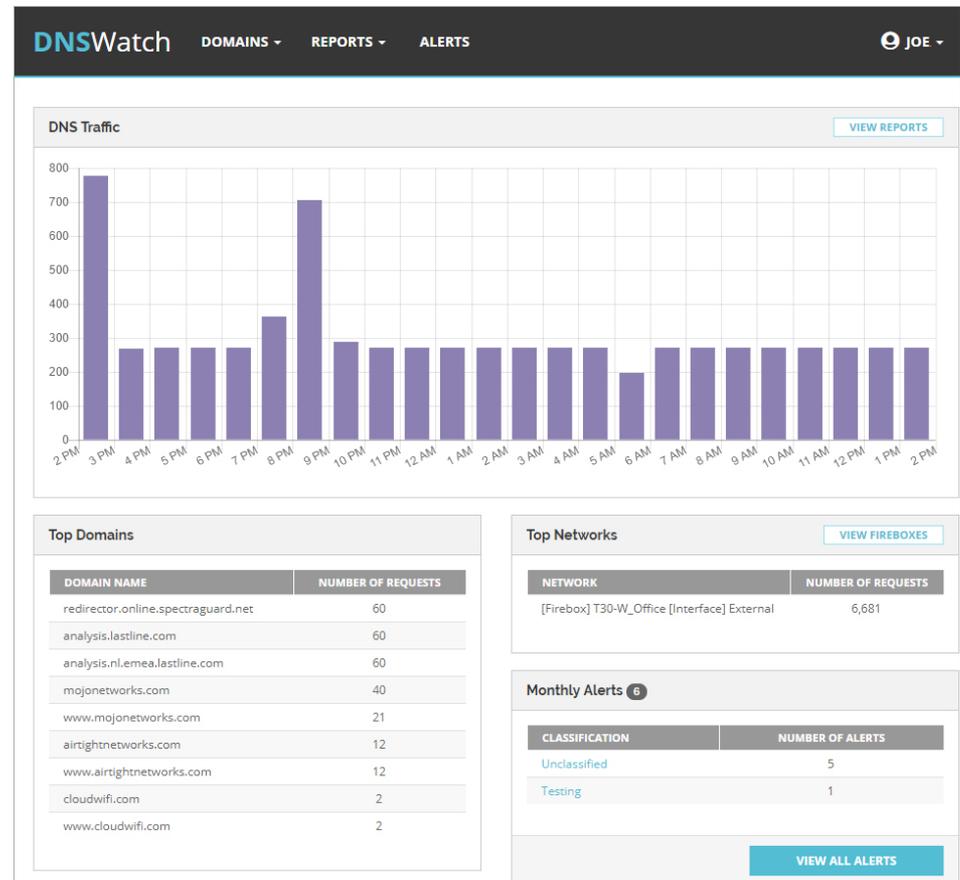
# Manage DNSWatch

- 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**

**User Account Settings**

Profile

Notifications

**DNSWatch Settings**

**Protected Fireboxes**

Block Page Content

Block Page Style

Domain Sharing

**Team Settings**

Team Members

**Protected Fireboxes**

These Fireboxes are protected by DNSWatch.



T30-W\_Office 70AD078BD92F1

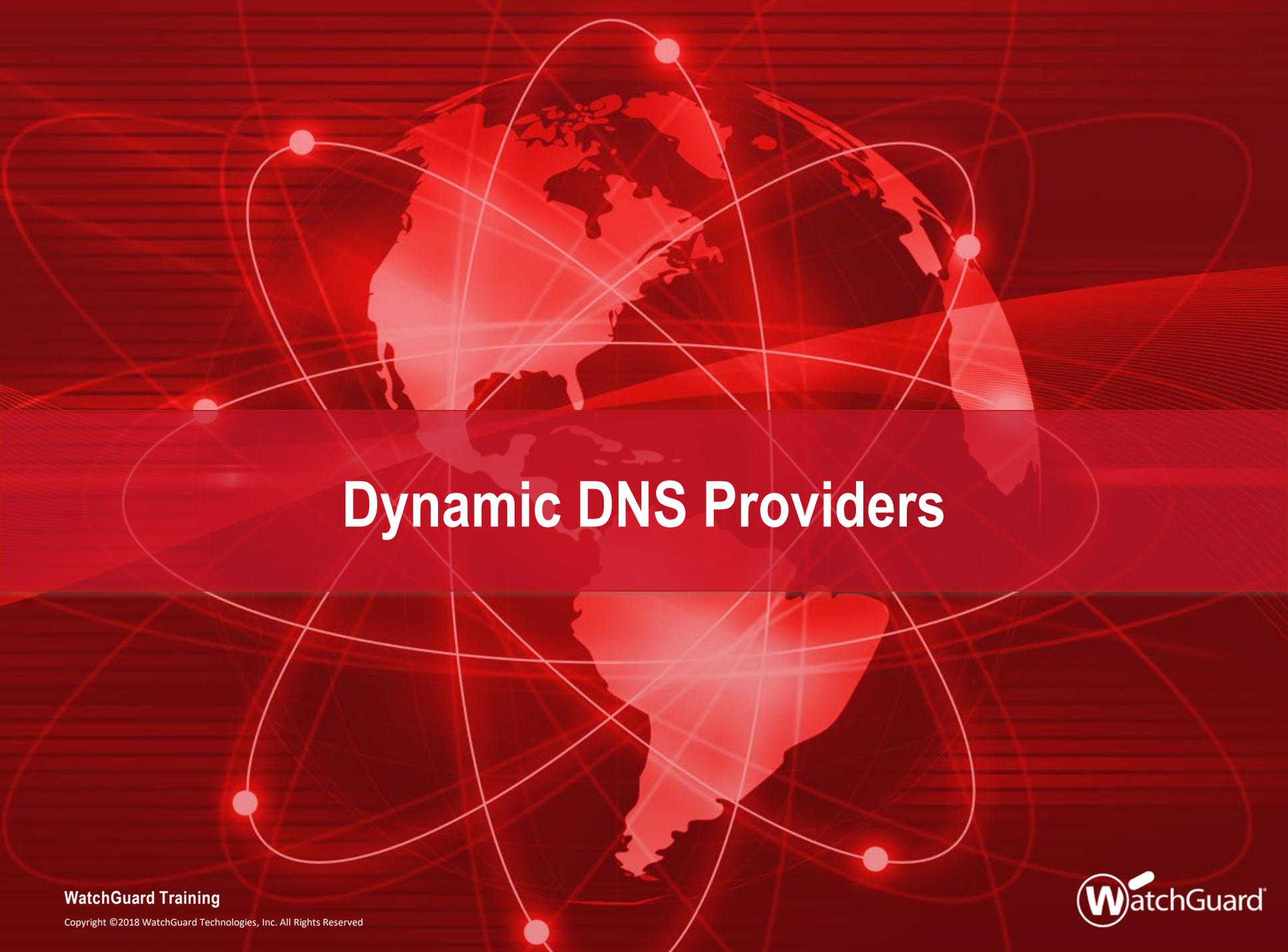
INTERFACE	NETWORK	REGISTERED	LAST DNS REQUEST
External	203.0.113.10/32	March 5, 2018, 12:31 a.m.	March 21, 2018, 3:42 p.m.

T35-W-Storefront D02102720F3FD

INTERFACE	NETWORK	REGISTERED	LAST DNS REQUEST
External	198.51.100.10/32	March 1, 2018, 12:52 p.m.	March 21, 2018, 3:42 p.m.

# 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

# Dynamic DNS Providers

- Firewall 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

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

# Dynamic DNS Providers

- Fireware Web UI

Dynamic DNS / External

Enable Dynamic DNS for interface

Interface Name

Provider  ▼

User Name

Password

Confirm Password

Domain

Options

Forced Update  days

Allow the dynamic DNS provider to determine the IP address

# Dynamic DNS Providers

- Policy Manager

Per Interface Dynamic DNS - Extern...

Enable Dynamic DNS

Provider: DynDNS.org

User Name: DynDNS.org

Password: no-ip.com

Confirm: dynu.com

Domain: dnsdynamic.org

Options:

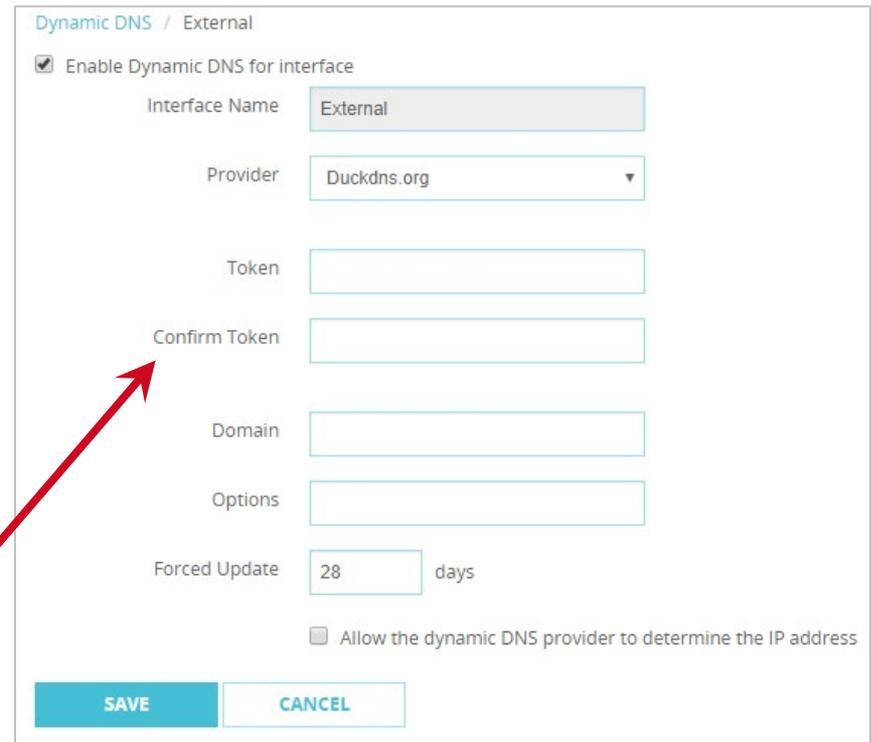
Forced Update: 28 day(s)

Allow DynDNS to determine the IP Address

OK Cancel Help

# 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



The screenshot shows the 'Dynamic DNS / External' configuration page. It includes a checkbox for 'Enable Dynamic DNS for interface', a dropdown for 'Interface Name' (set to 'External'), a dropdown for 'Provider' (set to 'Duckdns.org'), and input fields for 'Token', 'Confirm Token', 'Domain', and 'Options'. There is also a 'Forced Update' field set to '28' days and a checkbox for 'Allow the dynamic DNS provider to determine the IP address'. At the bottom are 'SAVE' and 'CANCEL' buttons. A red arrow points from the text in the list to the 'Token' field.

Dynamic DNS / External

Enable Dynamic DNS for interface

Interface Name: External

Provider: Duckdns.org

Token:

Confirm Token:

Domain:

Options:

Forced Update: 28 days

Allow the dynamic DNS provider to determine the IP address

SAVE CANCEL



# Firebox Wireless Enhancements

# 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

# 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

VLAN / Add VLAN Settings

VLAN Settings Secondary Network IPv6 Bridge Protocols

VLAN Configuration

Name

Description

VLAN ID

Security Zone

Select tagged traffic for interfaces

<input type="checkbox"/>	INTERFACE	TAGGED
<input type="checkbox"/>	VLAN1	No Traffic

SELECT TRAFFIC ▾

Apply firewall policies to intra-VLAN traffic

SAVE CANCEL

# DHCP Relay Server

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

The screenshot shows the 'Interfaces / Edit' configuration page. The 'Interface Name (Alias)' is 'Trusted', and the 'Interface Type' is 'Trusted'. The 'IPv4' tab is selected, showing an IP address of 10.0.90.1 with a /24 subnet. A red box highlights the 'DHCP Relay' dropdown menu, which is currently set to 'DHCP Relay'. Below this, there is a section for 'DHCP SERVERS' with a 'DHCP Server' input field, 'ADD', and 'REMOVE' buttons. At the bottom, there are 'SAVE' and 'CANCEL' buttons.

Interfaces / Edit

Interface Name (Alias)

Interface Description

Interface Type

IPv4 IPv6 Secondary MAC Access Control Advanced

IP Address  /

**DHCP Relay** ▼

DHCP server IP addresses for all DHCP requests received on this interface

**DHCP SERVERS** ↕

DHCP Server

**ADD** **REMOVE**

**SAVE** **CANCEL**

# 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

Use DHCP Server

You can configure a maximum of six address ranges.

**Address Pool:**

Starting IP	Ending IP	
10.0.1.2	10.0.1.254	<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

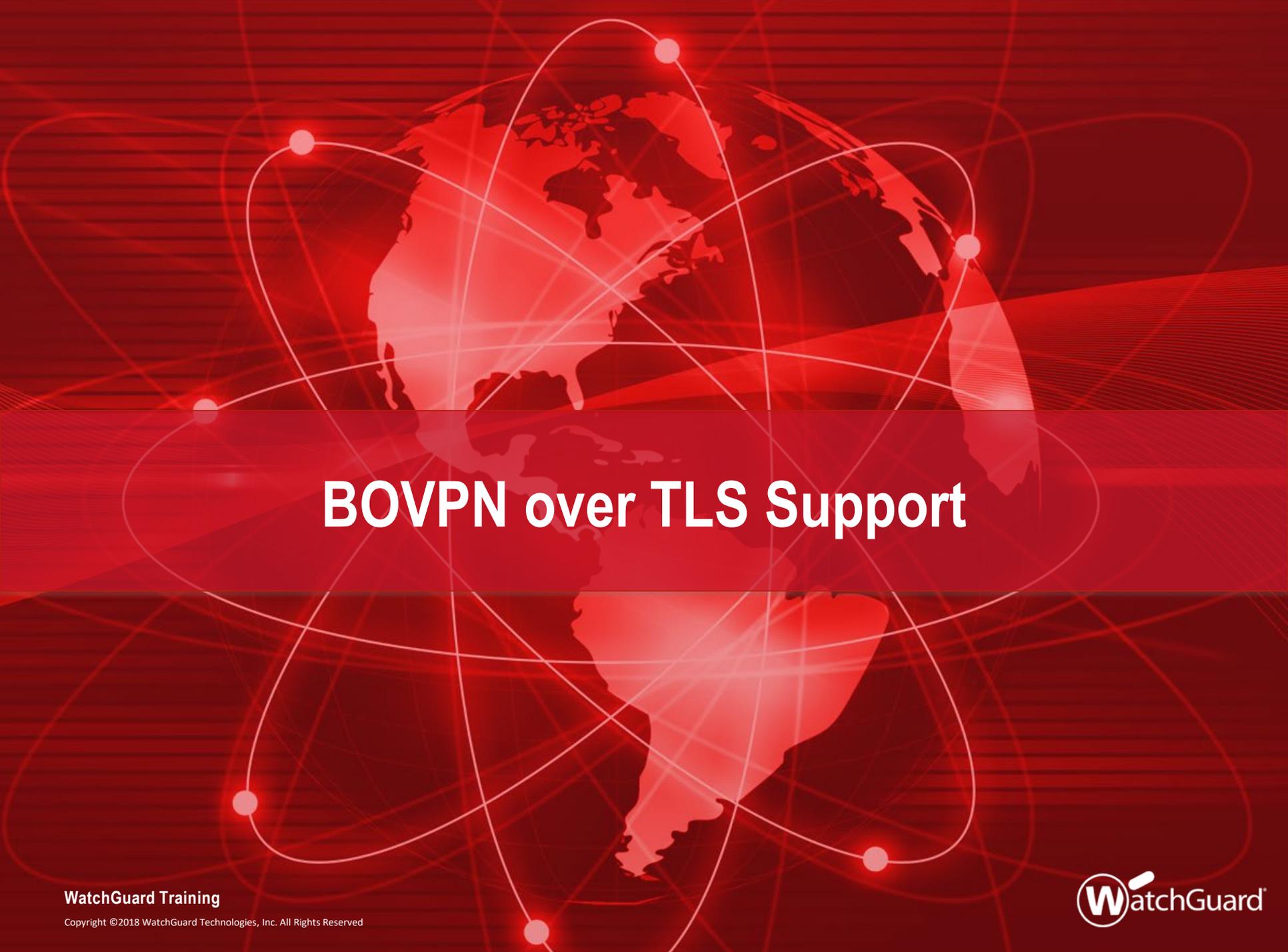
**Reserved Addresses:**

Reserved Name	Reservation IP	MAC Address	
			<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Leasing Time: 8 hours

**Default Gateway:**

Use Interface IP  Specify



# BOVPN over TLS Support

# 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**

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

Activate 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: **Server**

In server mode, the Firebox can accept connections from one or more BOVPN over TLS clients.

**Server Settings**

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

Primary Server:  Backup Server:

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

Enabled	Tunnel ID	Description
---------	-----------	-------------

Add... Edit... Remove Enable Disable

The BOVPN over TLS server is configured to use TCP port 443 and assign IP addresses to clients from 192.168.11.0/24.

Advanced

OK Cancel Help

**Add Client**

**Client Settings**

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

Destination	Metric
-------------	--------

Add... Edit... Remove

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

Destination	Metric
-------------	--------

Add... Edit... Remove

Add this tunnel to the BOVPN-Allow policies

OK Cancel Help

# BOVPN over TLS Support for WSM and PM

- Client mode in Policy Manager

**BOVPN Over TLS**

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

Activate 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: **Client**

In client mode, the Firebox can connect to one or more BOVPN over TLS servers.

Client Settings

BOVPN over TLS Servers

Enabled	Tunnel Name	Primary Server	Description
---------	-------------	----------------	-------------

OK

**Add Server**

Server Settings

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.

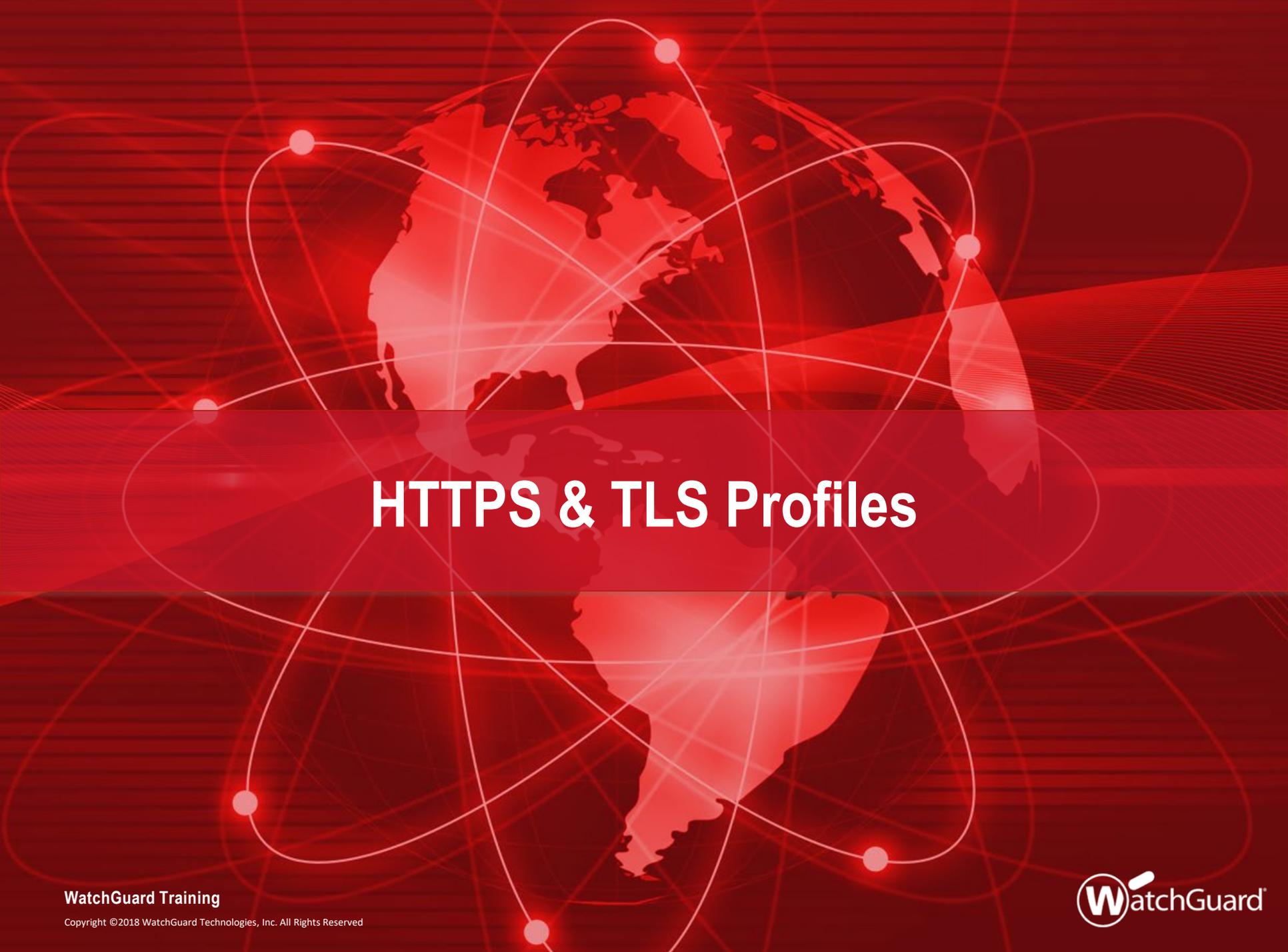
Tunnel ID:

Pre-Shared Key:

Advanced Options:

Add this tunnel to the BOVPN-Allow policies

OK Cancel Help



# HTTPS & TLS Profiles

# HTTPS & TLS Profiles

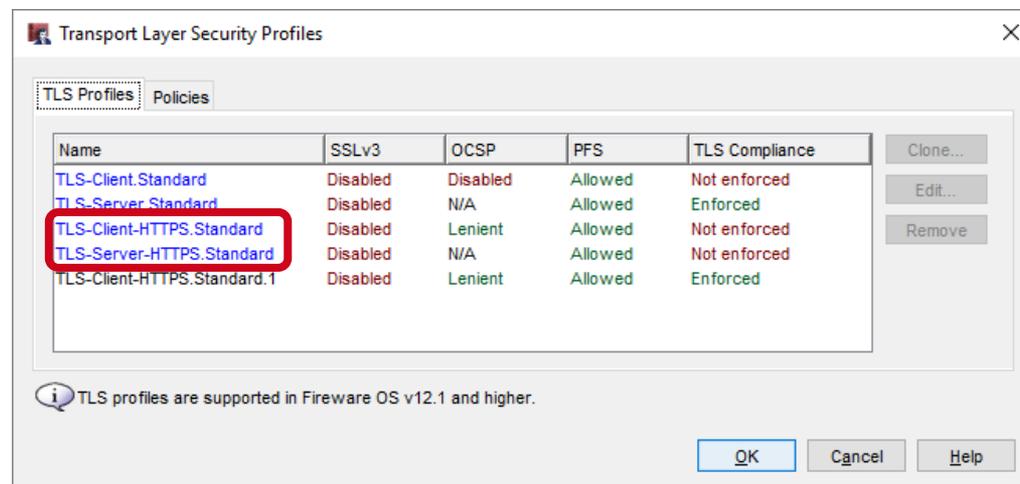
- WatchGuard continues to innovate our content inspection features to assist users in secure policy configuration
- TLS profiles contain the settings used for content inspection by proxy actions
  - You can use the same TLS profile for multiple policies
  - TLS profiles make it easier to configure and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

# HTTPS & TLS Profiles

- Firewall v12.1 supported TLS profiles in the IMAP proxy
- Firewall 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

The screenshot shows a 'Clone TLS Profile' dialog box with the following settings:

- Name: TLS-Server-HTTPS.Standard.1
- Description: Standard TLS profile for servers.
- Allow SSLv3
- Allow only TLS-compliant traffic
- Perfect Forward Secrecy Ciphers: Allowed (dropdown)

Buttons: OK, Cancel, Help

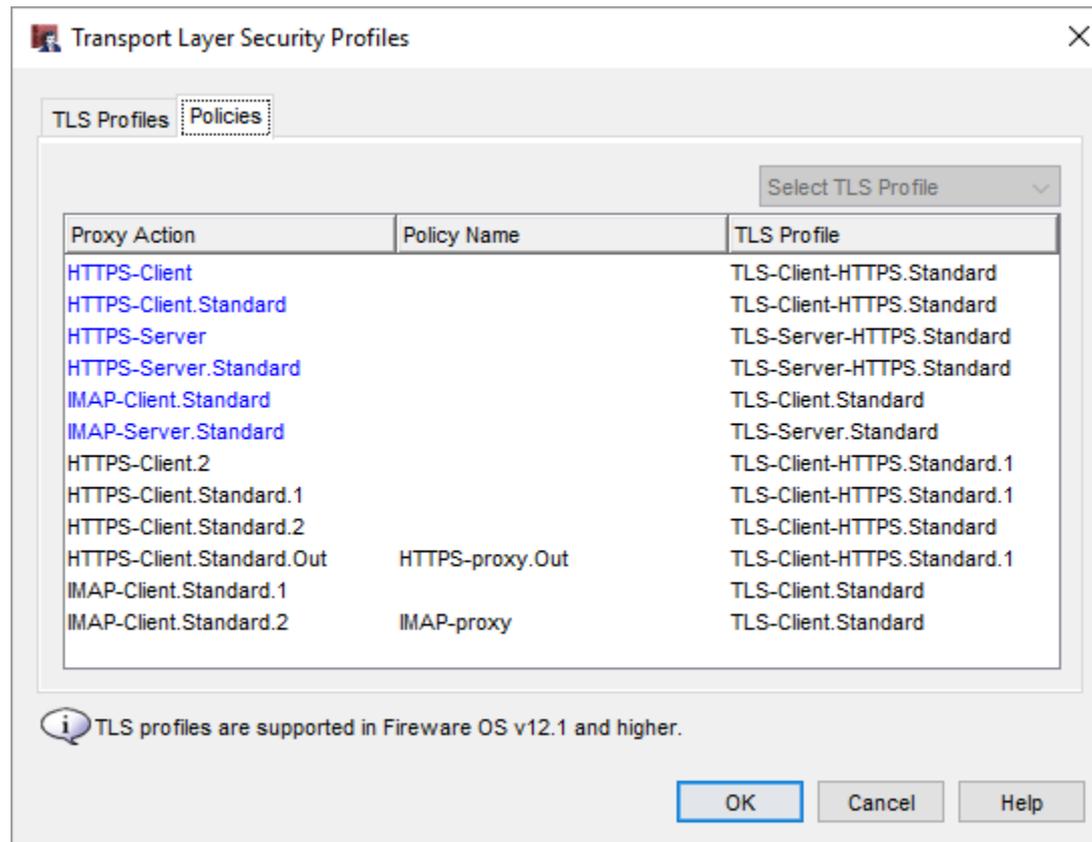
The screenshot shows a 'Clone TLS Profile' dialog box with the following settings:

- Name: TLS-Client-HTTPS.Standard.1
- Description: Standard TLS profile for clients.
- Allow SSLv3
- Allow only TLS-compliant traffic
- Certificate Validation:
  - Use OCSP to validate certificates
  - If a certificate cannot be validated, the certificate is considered invalid
- Perfect Forward Secrecy Ciphers: Allowed (dropdown)

Buttons: OK, Cancel, Help

# 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

**Edit HTTPS Proxy Action Configuration**

Name:

Description:

Categories

- Content Inspection
- WebBlocker
- General Settings

**Content Inspection Summary (Inspection Status - Domain Name Rules: On WebBlocker: Off)**

TLS Profile:

SSLv3 **Disabled** OCSP **Lenient** PFS Ciphers **Allowed** TLS Compliance **Enforced**

Enable Predefined Content Inspection Exceptions. (Fireware OS v12.1 and higher)  Google Apps **Unrestricted**

You can download the Proxy Authority certificate used for Content Inspection from the Certificate Portal at <http://<Firebox IP address>:4126/certportal>

**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 type="button" value="Add"/>
<input checked="" type="checkbox"/>	Allow	*.mojonetworks.com	Pattern Match	*.mojonetworks.com	N/A	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Clone..."/>
<input checked="" type="checkbox"/>	Allow	*.cloudwifi.com	Pattern Match	*.cloudwifi.com	N/A	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Edit..."/>
<input checked="" type="checkbox"/>	Allow	redirector.online.spect...	Pattern Match	redirector.online.spec...	N/A	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Remove"/>
<input checked="" type="checkbox"/>	Allow	*.airtightnetworks.com	Pattern Match	*.airtightnetworks.com	N/A	<input type="checkbox"/>	<input type="checkbox"/>	

# 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

Content Inspection Summary (Inspection Status - Domain Name Rules: On WebBlocker: Off)

TLS Profile: TLS-Client-HTTPS.Standard.1

SSLv3 **Disabled** OCSP **Lenient** PFS Ciphers **Allowed** TLS Compliance **Enforced**

Enable Predefined Content Inspection Exceptions. (Fireware OS v12.1 and higher) [Manage Exceptions...](#) Google Apps **Unrestricted** [Edit...](#)

You can download the Proxy Authority certificate used for Content Inspection from the Certificate Portal at <http://<Firebox IP address>:4126/certportal>

# 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

Content Inspection Summary (Inspection Status - Domain Name Rules: On WebBlocker: Off)

TLS Profile: TLS-Client-HTTPS.Standard.1

SSLv3 Disabled OCSP Lenient PFS Ciphers Allowed TLS Compliance Not enforced

Enable Predefined Content Inspection Exceptions. (Fireware OS v12.1 and higher) Manage Exceptions... Google Apps Unrestricted Edit...

You can download the Proxy Authority certificate used for Content Inspection from the Certificate Portal at <http://<Firebox IP address>:4126/certportal>

# HTTPS & TLS Profiles

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

TLS Profiles

Transport Layer Security Profiles

NAME ↕	SSLV3	OCSP	PFS	TLS COMPLIANCE
<a href="#">TLS-Client.Standard</a>	Disabled	Disabled	Allowed	Not enforced
<a href="#">TLS-Server.Standard</a>	Disabled	N/A	Allowed	Enforced
<a href="#">TLS-Client-HTTPS.Standard</a>	Disabled	Lenient	Allowed	Not enforced
<a href="#">TLS-Server-HTTPS.Standard</a>	Disabled	N/A	Allowed	Not enforced
<a href="#">TLS-Client-HTTPS.Standard.1</a>	Disabled	Lenient	Required	Not enforced

CLONE EDIT REMOVE

Policies that Support TLS Profiles

<input type="checkbox"/>	PROXY ACTION	FIREWALL POLICIES	TLS PROFILE
<input type="checkbox"/>	<a href="#">IMAP-Client.Standard</a>		TLS-Client.Standard
<input type="checkbox"/>	<a href="#">IMAP-Server.Standard</a>		TLS-Server.Standard
<input type="checkbox"/>	<a href="#">HTTPS-Client</a>		TLS-Client-HTTPS.Standard
<input type="checkbox"/>	<a href="#">HTTPS-Client.Standard</a>		TLS-Client-HTTPS.Standard
<input type="checkbox"/>	<a href="#">HTTPS-Server</a>		TLS-Server-HTTPS.Standard
<input type="checkbox"/>	<a href="#">HTTPS-Server.Standard</a>		TLS-Server-HTTPS.Standard
<input type="checkbox"/>	<a href="#">HTTPS-Client.Standard.1</a>	HTTPS-proxy	TLS-Client-HTTPS.Standard.1
<input type="checkbox"/>	<a href="#">HTTPS-Server.Standard.1</a>		TLS-Server-HTTPS.Standard
<input type="checkbox"/>	<a href="#">IMAP-Client.Standard.1</a>		TLS-Client.Standard
<input type="checkbox"/>	<a href="#">IMAP-Server.Standard.1</a>		TLS-Server.Standard

SELECT ACTION ▾ SAVE

# 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!**