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
Access Portal — Configure

- Specify which apps users and groups can connect to

![Configure the settings for this user or group.](image)

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>Application Group</td>
</tr>
<tr>
<td>ExampleApp</td>
<td>Web Application</td>
</tr>
<tr>
<td>ExampleApp2</td>
<td>Web Application</td>
</tr>
<tr>
<td>RDP to 203.0.113.10</td>
<td>Host Desktop Access (RDP)</td>
</tr>
<tr>
<td>SSH to 203.0.113.20</td>
<td>Host Shell Access (SSH)</td>
</tr>
</tbody>
</table>
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
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 — 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

<table>
<thead>
<tr>
<th>General</th>
<th>Authentication</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Authentication</td>
<td>SHA-256</td>
</tr>
<tr>
<td></td>
<td>Encryption</td>
<td>AES (256-bit)</td>
</tr>
<tr>
<td></td>
<td>Data channel</td>
<td>TCP</td>
</tr>
</tbody>
</table>

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.

![VPN Portal Configuration]

- For Mobile VPN with SSL, you can specify a different 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.

- 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)

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

**Select 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**: Okta

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

- **Host Name**: portal.example.com

After you save the configuration to your Firebox, follow the IDP configuration instructions at [https://portal.example.com/auth/saml](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**: memberOf [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
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](image)
Access Portal — Authenticated Users

- From Firebox System Manager, on the Authentication List tab
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

![Security Subscriptions](image)
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 — Fireware Web UI
HTTPS Proxy Action UI Updates

- Manage Content Inspection Exceptions
HTTPS Proxy Action UI Updates

- Content Inspection — Policy Manager
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"
  ```
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

![TLS Settings Configuration](image)
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
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*
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.

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

![Image of WebBlocker wizard interface]

Select a name for the WebBlocker action

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

Name: WebBlocker.3
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 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 Portal Updates

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

![SSL Portal Updates Diagram](image-url)
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.
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.
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 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

- The **Authentication** tab

![Mobile VPN with IKEv2 Configuration](image)

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**

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

- **Firebox-DD server**
- **RADIUS**

**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.

<table>
<thead>
<tr>
<th>Selected</th>
<th>Name</th>
<th>Type</th>
<th>Authentication Server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IKEv2-Users</td>
<td>Group</td>
<td>Any</td>
</tr>
</tbody>
</table>

[OK] [Cancel] [Help]
Mobile VPN with IKEv2

- You can select a Firebox certificate or a third-party certificate.
Mobile VPN with IKEv2

- Firebox and third-party certificates have these requirements:
  - Extended Key Usage (EPU) 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.
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**

<table>
<thead>
<tr>
<th>ENABLED</th>
<th>TUNNEL NAME</th>
<th>PRIMARY SERVER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>BovpnTLS.1</td>
<td>198.51.100.2</td>
<td>Tunnel to the Toronto TLS server</td>
</tr>
</tbody>
</table>

**Buttons:**

ADD  EDIT  REMOVE
BOVPN Over TLS

- Configure Client mode
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.
BOVPN Over TLS

- You can add tunnels to multiple TLS servers

<table>
<thead>
<tr>
<th>ENABLED</th>
<th>TUNNEL NAME</th>
<th>PRIMARY SERVER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>BovpnTLS.1</td>
<td>198.51.100.2</td>
<td>Tunnel to the Toronto TLS server</td>
</tr>
<tr>
<td>Yes</td>
<td>BovpnTLS.2</td>
<td>192.0.2.2</td>
<td>Tunnel to the New York TLS server</td>
</tr>
</tbody>
</table>
BOVPN Over TLS

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

![BOVPN over TLS Mode](image)
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**: TLSTunnel1
  - **Description**: Optional (text)
  - **Pre-Shared Key**: ********
  - **Enable**: Marked
  - **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** | **Edit** | **Remove**
  - **Add this tunnel to the BOVPN-Allow policies**

[SAVE] [CANCEL]
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.

<table>
<thead>
<tr>
<th>Primary Server</th>
<th>Backup Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>198.51.100.2</td>
<td>192.0.2.2</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>ENABLED</th>
<th>TUNNEL ID</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>TLSTunnel1</td>
<td></td>
</tr>
</tbody>
</table>

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
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.
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:

```plaintext
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.

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
SSL/TLS Shared 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

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

The BOVPN over TLS server feature is enabled and overrides some settings.
SSL/TLS Shared Settings

- VPN Portal Port

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

<table>
<thead>
<tr>
<th>General</th>
<th>Authentication</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication: SHA-256</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption: AES (256-bit)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data channel: TCP, 443</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SSL/TLS Shared Settings

- VPN Portal Port

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

- 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

```
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual IP Address Pool</td>
<td>192.168.113.0 / 24</td>
</tr>
<tr>
<td>Authentication</td>
<td>SHA-256</td>
</tr>
<tr>
<td>Encryption</td>
<td>AES (256-bit)</td>
</tr>
<tr>
<td>Data channel</td>
<td>UDP : 444</td>
</tr>
</tbody>
</table>
```
SSL/TLS Shared Settings

- Mobile VPN with SSL Data Channel

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**: SHA-256

## Advanced

- **Encryption**: AES (256-bit)

- **Data channel**: UDP 444
SSL/TLS Shared Settings

- VPN Portal Port

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**

![SSLVPN Policy Configuration](image-url)
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`
Modem as an External Interface

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

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

- **Policy Manager:**

  ![Multi-WAN Link Monitor Monitor Updates](image)
Multi-WAN Link Monitor Updates

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

<table>
<thead>
<tr>
<th>SSIDs</th>
<th>Settings</th>
<th>Radio Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Settings</td>
<td>DHCP</td>
<td>Static</td>
</tr>
<tr>
<td>Log to a syslog server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Syslog server IP address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Communication VLAN tagging</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication VLAN</td>
<td>4094</td>
<td></td>
</tr>
</tbody>
</table>

![Configured parameters for Min. Association RSSI and Smart Steering](image-url)

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

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
NOTHING GETS PAST RED.