Firebox

Common Criteria Deployment Guide

Version 1.0

Fireware v12.6.2
10 August 2020

About This Guide

The *Firebox Common Criteria Deployment Guide* describes how to configure and deploy a WatchGuard Firebox in compliance with the Common Criteria certification requirements. For complete product documentation, see the Firebox documentation set, available online at https://www.watchguard.com/wgrd-help/documentation/overview.

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Guide revised: 8/10/2020

Copyright, Trademark, and Patent Information

Complete copyright, trademark, patent, and licensing information can be found in the *Copyright and Licensing Guide*, available online at https://www.watchguard.com/wgrd-help/documentation/overview.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, providing best-in-class Unified Threat Management, Next Generation Firewall, secure Wi-Fi, and network intelligence products and services to more than 75,000 customers worldwide. The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for Distributed Enterprises and SMBs. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

Address

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

Support

www.watchguard.com/support
U.S. and Canada +877.232.3531
All Other Countries +1.206.521.3575

Sales

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.613.0895

Contents

Introduction 7

Product Overview 7

Product Architecture 7

Target of Evaluation 8

Firmware Version 8

Supported Hardware 8

Approved Administration Methods 8

Initial Configuration 9

Firebox Factory-Default Settings 9

Activate Your Firebox 10

Run the Web Setup Wizard 11

Upgrade Fireware OS 13

Upgrade the Firebox Recovery Image 14

Enable CSfC Mode 15

System Integrity Checks 16

Boot Time 16

Run Time 16

Upgrade 16

Authentication 17

Firebox Roles and Users 17

Add a New Device Management User Account 18

Passphrase Requirements and Recommendations 19

Change the Minimum Passphrase Length 19

Change a User Passphrase 20

Configure Account Lockout Settings 21

Unlock a Locked Device Management User Account 22

Configure Management Session Timeouts 22

Manually Terminate a Management Session 23

Configure the Logon Disclaimer 24

Web Server Certificate 25

Import and Install a Web Server Certificate 25

Create a CSR 26

Use the CSR to Request a Signed Certificate From a Trusted CA 29

Import the CA Certificates and Web Server Certificate 30

Configure the Firebox to Use the New Web Server Certificate 32

View and Delete Certificates 33

Audit Logging 34

Local Audit Log Storage 34

Audit Log Storage Capacity and Log Deletion 34

See Audit Log Messages Stored on the Firebox 35

Configure Logging Settings 35

Configure Logging in Firewall Policies 35

Configure Global Logging Settings 37

Configure Diagnostic Log Levels 38

Send Log Messages to a Syslog Server 38

Audit Log Format 40

Example Event Logs 40

Example Traffic Audit Log 41

Audit Log Records 43

System Time 70

Change the Time Zone 70

Configure NTP Servers 71

Manually Update the System Clock 72

Firewall Policies and Security Services 72

Default Firewall Policies and Services 72

Factory-Default Policies 72

Web Setup Wizard Default Policies and Services 73

Default Security Services Configuration 74

Default Threat Protection 75

Default Packet Handling 76

Packets Dropped by Default 78

Blocked Sites 78

Blocked Ports 81

Security Services Priority 82

Configure Firewall Policies 83

Firewall Policy Types 83

Add a Firewall Policy 83

Configure Policy Properties 86

Policy Precedence 89

Set Precedence Manually 89

Hidden Policies 90

Unhandled Packets 90

Stateful Sessions 90

Traffic From the Firebox 90

Built-In IPSec Policy 90

Deny All “Reserved for Future Use” Network Traffic 91

Deny Traffic from Invalid IPv4 and IPv6 Protocols 91

Add a Custom Policy to Deny Invalid IPv4 Protocols 92

Add a Custom Policy to Deny Invalid IPv6 Protocols 93

Configurable Firewall Policy Attributes 94

Policy Actions and Logging 95

Associate Policies with Network Interfaces 95

IPSec VPN 96

Configure a BOVPN Gateway 96

Add a Gateway 96

Configure the Gateway Endpoints 98

Configure IPSec VPN Phase 1 Settings 101

Add a Phase 1 Transform 105

Configure a BOVPN Tunnel 106

Add a Tunnel 106

Add a Tunnel Route 108

Configure Phase 2 Settings 109

Add a New Phase 2 Proposal 111

Use a Certificate for BOVPN Authentication 113

Import the Certificate 113

Configure the BOVPN to Use the Certificate 113

Control VPN Connections Based on Time of Day 114

Add Custom Firewall Policies for VPN Traffic 116

Troubleshoot Connections to External IT Entities 117

Verify Interface Connection Status 117

Look at Firebox Log Messages 118

Verify DNS Functionality 118

Run Network Diagnostic Tasks 119

Run a Basic Diagnostics Command 119

Use Command Arguments 120

Download a PCAP File 120

Run the VPN Diagnostic Report 122

VPN Diagnostic Report Details 123

Force a VPN Tunnel Rekey 124

Introduction

This document describes how to install and configure WatchGuard's Firebox Next Generation Firewall (NGFW) products running Fireware version 12.6.2 and certified under Common Criteria for conformance with these protection profiles:

Network Device

Network Device collaborative Protection Profile for Network Devices Version 2.1 (cpp_nd_v2.1)

Virtual Private Network

Protection Profile Module for Virtual Private Network (VPN) Gateways (mod_vpngw_v1.0)

Firewall

Firewall collaborative Protection Profile Module for Stateful Traffic Filter Firewalls v1.3 (mod_cpp_fw_v1.3)

To configure your Firebox in conformance to these Common Criteria standards, you must configure, deploy, and manage it as described in this document.

This document is a supplement to other available Firebox documentation available online on the WatchGuard Product Documentation page.

Product Overview

WatchGuard's Firebox Next Generation Firewall (NGFW) products are a family of standalone appliances that can be administered locally or remotely without any management software or devices. The Firebox provides controlled connectivity between two or more network environments. It mediates information flows between clients and servers located on internal and external networks governed by the firewalls.

Product Architecture

Firebox appliances run Fireware OS. The Firebox separates the organization’s internal networks from external network connections to decrease the risk of an external attack. It protects the internal, private networks from unauthorized users on the Internet. The Firebox examines traffic that enters and leaves the protected networks. The Firebox uses access policies to identify and filter different types of information and also controls protocols and ports protected computers can use on the Internet (outbound access).

Target of Evaluation

WatchGuard's Firebox Next Generation Firewall (NGFW) products running Fireware v12.6.2.

Firmware Version

The evaluated configuration requires Fireware v12.6.2 or higher.

Supported Hardware

The TOE includes these Firebox models and interface expansion modules:

- Firebox T Series: T20. T35, T40, T55, T70, T80
- Firebox M Series: M270, M370, M470, M570, M670, M4600, M5600
- Firebox M 8 Port 1Gb Copper Module
- Firebox M 8 Port 1Gb SFP Fiber Module
- Firebox M 4 Port 10 Gb SFP+ Fiber Module
- Firebox M 2 Port 40Gb QSFP+ Fiber Module

Approved Administration Methods

To configure and manage the Firebox in compliance with Common Criteria requirements, you must use only these management interfaces:

- Fireware Web UI
- Fireware Command Line Interface (CLI)

When configured in CSfC mode, the only approved method to connect to the CLI is to connect directly to the Firebox console port. SSH connections to the CLI are not an approved administration method.

This document describes how to use Fireware Web UI to configure required settings. You can also use the CLI to configure most required settings.

> ⓘ You cannot configure proxy action settings from the CLI.

Initial Configuration

Firebox Factory-Default Settings

Your Firebox ships with these factory-default settings:

Default network interface settings:

- Interface 0 is enabled as an external interface, as a DHCP client.
- Interface 1 is enabled as a trusted interface, with the IP address 10.0.1.1/24, and DHCP server is enabled.
- All other interfaces are enabled as optional interfaces, with the IP addresses 10.0.x.1/24 (where x is the interface number), DHCP server is disabled.
- Interface 32 is enabled as a trusted interface, with the IP address 10.0.32.1, and DHCP server is enabled (Firebox M5600 only).

Default Fireware Web UI management port:

- The default port for connections to Fireware Web UI is port 8080.
- To connect to Fireware Web UI on interface 1, browse to `https://10.0.1.1:8080`.
- To connect to Fireware Web UI on interface 32, browse to `https://10.0.32.1:8080`.

Console management port:

- The administrator can always log on to the Firebox CLI through the serial console port with the Device Management user account credentials.

Default Device Management user accounts and credentials:

- Device Administrator role with read-write access
  - User name: `admin`
  - Passphrase: `readwrite`
- Device Monitor role with read-only access
  - User name `status`
  - Passphrase: `readonly`

When you run the Web Setup Wizard, you can change the network settings and set new passphrases for the Device Management accounts.

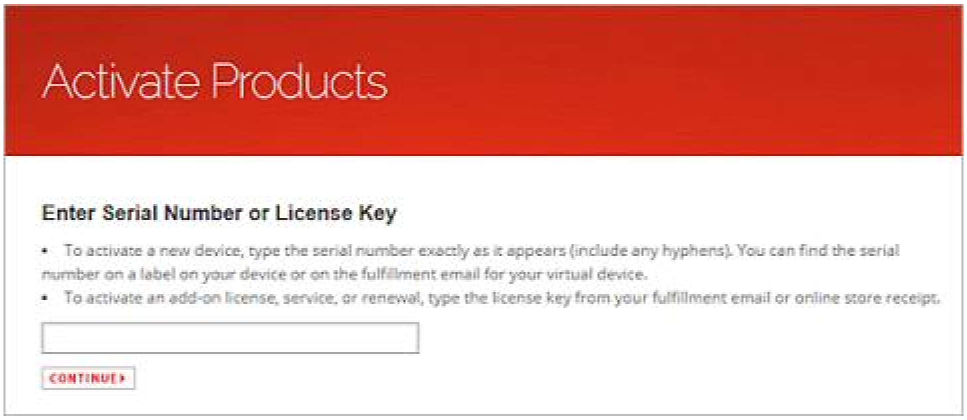
By default, the Firebox does not allow management connections to Fireware Web UI from the external network (interface 0).

Activate Your Firebox

You must activate your Firebox with WatchGuard to enable your hardware replacement warranty, receive technical support, and start your subscription to licensed security services.

To activate your Firebox:

1. Open a web browser and go to www.watchguard.com/activate.
2. Log in to your WatchGuard account or create a new account*.
   * If you create a new account, return to www.watchguard.com/activate after you finish the account creation process.
3. Type the Firebox serial number. Make sure to include any hyphens.



Activate Products

Enter Serial Number or License Key

- To activate a new device, type the serial number exactly as it appears (include any hyphens). You can find the serial number on a label on your device or on the fulfillment email for your virtual device.
- To activate an add-on license, service, or renewal, type the license key from your fulfillment email or online store receipt.

4. Click **Continue**.
5. Type a friendly name to identify the Firebox in your account.
6. (Optional) Select free trials for your Firebox, if available.

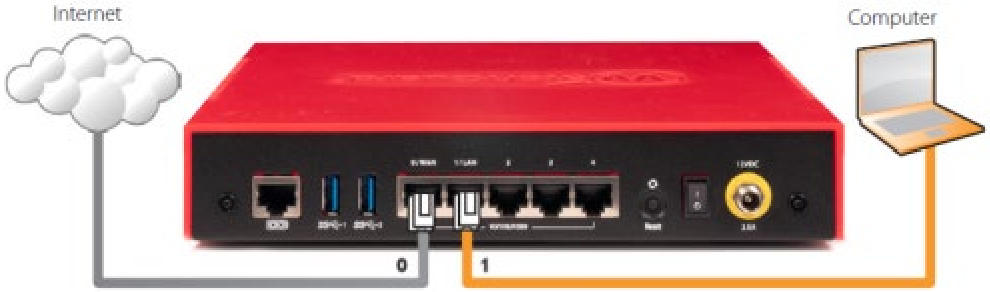
After activation is complete, the Firebox appears in the **Manage Products** list in your WatchGuard account. The activation process generates a Firebox feature key that enables you to configure licensed features and services on your Firebox. The Firebox connects to WatchGuard to download the feature key during setup.

> ⓘ If the network where you set up the Firebox does not connect to the Internet, save a copy of the Firebox feature key before you run the Web Setup Wizard. You can get the feature key from the **Product Details** page for your Firebox in your WatchGuard account.

Run the Web Setup Wizard

The Web Setup Wizard helps you configure network settings, device information, and administrative passphrases. It also automatically configures policies and services with recommended settings.

To run the Web Setup Wizard, connect your Firebox to your computer and to a network with Internet access.



To connect and power on the Firebox:

1. Connect Firebox interface 0 to a network with Internet access.
2. Power on the Firebox.
3. Connect Firebox interface 1 to your computer. For a Firebox M5600, connect your computer to interface 32.
   If your computer is configured to use DHCP. The Firebox assigns your computer an IP address on the 10.0.1.0/24 network. For an M5600, the Firebox assigns your computer an IP address on the 10.0.32.0/24 subnet.
4. If your computer is not configured to use DHCP, change the IP address of your computer to an IP address on the same subnet as the default Firebox interface IP address.

To run the Web Setup Wizard:

1. On the computer connected to the Firebox, open a web browser and go to **https://10.0.1.1:8080**. For a Firebox M5600, go to **https://10.0.32.1:8080**.
   You can safely ignore certificate warnings because the Firebox uses a self-signed certificate.
2. Log in with the default user name **admin** and the passphrase **readwrite**.
3. Select **New Configuration**.
4. Follow the steps in the Web Setup Wizard to configure your Firebox.

The Web Setup Wizard helps you to complete these configuration steps:

Configure the External interface

Configure the method you want your device to use to set an external IP address. The choices are:

- DHCP — Type the DHCP identification as supplied by your ISP.
- PPPoE — Type the PPPoE information as supplied by your ISP.
- Static — Type the static IP address and gateway IP address, as supplied by your ISP.

Configure DNS and WINS servers (Optional)

Configure the Domain DNS and WINS server addresses you want the Firebox to use.

Configure the Trusted interface

Type the IP address of the trusted interface. (Optional) If you want the Firebox to assign IP addresses to computers that connect to the trusted network, you can enable the DHCP server and assign a range of IP addresses on the same subnet as the interface IP address.

Create passphrases for your device

Set new passphrases for the status (read-only) and admin (read/write) built-in user accounts. Both passphrases must be at least 8 characters long, and they must be different from each other.

Enable remote management (Optional)

This option enables management connections to the Firebox through the external interface. Do not enable this option.

Add device information

You can type a device name, location, and contact information to save management information for this device. By default, the device name is set to the model number of your Firebox. The location and contact information are optional.

Set the time zone

Select the time zone where the Firebox is located.

Add the feature key

If the Firebox cannot connect to WatchGuard to download the Firebox feature key, you can paste it into the Web Setup Wizard. You can get the feature key on the Product Details page for your Firebox at www.watchguard.com.

> ⚠ If you do not add the feature key, the Web Setup Wizard cannot configure licensed subscription services. Without a feature key, the Firebox allows only one outbound connection from the trusted network to the Internet.

Configure subscription services

The setup wizard shows a list of licensed services from the feature key. The setup wizard automatically enables the listed services with recommended settings. For WebBlocker, the setup wizard recommends content categories to block, and you can change these settings in the setup wizard.

Review the configuration

After you review the configuration summary, the setup wizard saves the configuration to the Firebox.

After you finish the Web Setup Wizard, your Firebox:

- Allows outbound FTP, Ping, DNS, TCP, and UDP connections.
- Blocks all unrequested traffic from the external network.
- Inspects outgoing FTP, HTTP, and HTTPS traffic.
- Uses licensed security services to protect the internal network.

For details about the default policies and services, see *Web Setup Wizard Default Policies and Services*.

You can connect to Fireware Web UI to further customize your configuration.

> ⓘ If you change the IP address of the trusted interface, you must make sure your IP address matches the subnet of the trusted network before you connect to the device.

Upgrade Fireware OS

The installed Fireware version appears in the Front Panel when you log in to Fireware Web UI. If your Firebox runs a Fireware version lower than Fireware v12.6.2, you must upgrade the Firebox.

To download and apply an upgrade file, from Fireware Web UI:

1. Go to the Software Downloads page at software.watchguard.com.
2. On the Software Downloads page for your Firebox model, download and unzip the Fireware v12.6.2 Sysa-dl ZIP file for OS updates from the Web UI.

> ⓘ To request the Fireware v12.6.2 upgrade file for Firebox T35, T55, or T70, send a request to CSfC@watchguard.com.

3. Log in to Fireware Web UI with the user name **admin** and the admin (read/write) passphrase you specified in the Web Setup Wizard.
4. From Fireware Web UI, select **System > Upgrade OS**.
   The Upgrade OS page appears.
5. Select **I have an upgrade file**.
6. To select the upgrade file from the directory where you unzipped or installed it, click **Browse** or **Choose File**. The button name depends on your browser.
   The upgrade file extension is sysa-dl.
7. Click **Upgrade**.
   The Firebox uploads the selected file, and the upgrade proceeds automatically.

Upgrade the Firebox Recovery Image

If you start the Firebox in recovery mode, it uses a recovery software image. For your Firebox to operate in compliance with Common Criteria requirements, you must upgrade the recovery image to version 12.6.2. The recovery image file extension is **.sysb-dl**.

Download the recovery software image upgrade file for your Firebox model:

Firebox Model	Upgrade File
M4600, M5600	http://cdn.watchguard.com/SoftwareCenter/Files/XTM/12_6_2/M4600_M5600_12_6_2.sysb-dl
M270, M370, M470, M570, M670	http://cdn.watchguard.com/SoftwareCenter/Files/XTM/12_6_2/M270_M370_M470_M570_M670_12_6_2.sysb-dl
T80	http://cdn.watchguard.com/SoftwareCenter/Files/XTM/12_6_2/T80_12_6_2.sysb-dl
T40, T20	http://cdn.watchguard.com/SoftwareCenter/Files/XTM/12_6_2/T20_T40_12_6_2.sysb-dl
T35, T55, T70	Send a request to CSfC@watchguard.com

To install the recovery software image upgrade:

1. Log in to Fireware Web UI with the user name **admin** and the admin (read/write) passphrase you specified in the Web Setup Wizard.
2. From Fireware Web UI, select **System > Upgrade OS**.
   The Upgrade OS page appears.
3. Select **I have an upgrade file**.
4. To select the upgrade file from the directory where you downloaded it, click **Browse** or **Choose File**. The upgrade file extension is **.sysb-dl**.
5. Click **Upgrade**.
   A message appears when the upgrade is complete.

Enable CSfC Mode

To configure your Firebox in compliance with Common Criteria, you must enable CSfC mode. Some settings required for compliance with Common Criteria are available only when CSfC mode is enabled. Other settings are disabled for compliance with Common Criteria requirements. To enable CSfC mode, you must use Fireware CLI.

To manage a Firebox from the CLI, connect your computer to the console port on the Firebox. To do this you must have a serial console cable. Your computer must have an available serial port and an installed terminal client application, such as PuTTY.

To connect to the Firebox CLI through the console port:

1. Connect a serial cable from your computer to the console port on the Firebox.
2. In your terminal application, open a new connection window.
3. Set the terminal type to VT100.
   If you do not set the terminal type to VT100, some command and control key functions do not work. For example, Ctrl-C does not break, some special characters do not type, and ESC does not work.
4. Set your serial connection parameters to:
   - Port — The serial port on your computer, usually COM1
   - Baud Rate — 115200
   - Data Bits — 8
   - Stop Bits — 1
   - Parity — None
   - Flow Control — None

7. Open a terminal connection.
   The connection window displays a welcome message and the Firebox login prompt.

To enable CSfC Mode in Fireware CLI:

1. Open a terminal connection to the Firebox console.
2. Type the user name **admin**.
3. Type the passphrase for the admin user account. Press **Enter**.
4. Type the command `csfc enable`.
   CSfC mode is enabled and the Firebox reboots.

When CSfC mode is enabled, some Firebox functionality changes:

- To connect to the CLI you must connect a serial cable to the Firebox console port.
- TLS v1.3 is disabled by default.
- The CLI supports commands to see TLS v1.3 status and to enable and disable it:
  - `show tlsv13` — shows whether TLS v1.3 is enabled
  - `tlsv13 enable` — enables TLS v1.3
  - `tlsv13 disable` — disables TLS v1.3 (this is the default in CSfC mode)

- The Firebox performs integrity checks at system boot time and before any upgrade. For more information, see *System Integrity Checks*.
- The Firebox cannot auto-restore a backup image when it starts in recovery mode.

System Integrity Checks

In CSfC mode, the Firebox uses a cryptographic signature to check integrity of the appliance each time the Firebox boots, and before each software upgrade. These integrity checks ensure that system files are valid and have not been corrupted.

Boot Time

The public key is installed with the appliance image. When the Firebox boots, it uses the public key to check the integrity of most files, directories, and device nodes on the appliance, before it mounts the root file system. If the integrity check fails, the Firebox immediately shuts down. If the Firebox shuts down due to an integrity check failure, all interfaces are disabled, and you cannot connect to the Firebox to see status.

The cryptographic module undergoes known-answer self-tests during boot to ensure functionality. Upon failure, boot is halted and a log is displayed to the serial console

> ⓘ To verify that the shut down is caused by an integrity check failure, you can connect to the serial console while you reboot the Firebox. If the integrity check fails, the error `Error: integrity check failed` appears in the console before the system shuts down.

If the Firebox shuts down due to an integrity check failure, reboot the Firebox. If that does not resolve the issue, contact WatchGuard Support for assistance.

Run Time

Random noise source health tests are continually performed during run-time to verify the health of the Firebox’s noise source.

Upgrade

When you select a Fireware upgrade file to install, the Firebox checks the upgrade file for the presence of a cryptographic signature. If the cryptographic signature is present, the Firebox uses the public key from the previously installed image to check the relevant portion of the upgrade file. If the Firebox cannot verify the signature, or if the signature is not present, the Firebox refuses the upgrade.

Authentication

Firebox Roles and Users

With role-based administration on your Firebox, you can share the configuration and monitoring responsibilities for your Firebox between several individuals in your organization. This enables you to run audit reports to monitor which administrators make which changes in your device configuration file.

Each Firebox includes these roles that you can assign to the unique user accounts you add: *Device Administrator*, *Device Monitor*, and *Guest Administrator*.

Role	Description
Device Administrator	User accounts that are assigned the Device Administrator role can connect to the device with read-write permissions to make changes to the device configuration file and monitor the device.
Device Monitor	User accounts that are assigned the Device Monitor role can connect to the device with read-only permissions to monitor the device.
Guest Administrator	User accounts that are assigned the Guest Administrator role can only connect to the device to manage the list of guest user accounts for connections to the hotspot enabled on the device.

Each Firebox includes three default user accounts. You cannot delete these accounts.

Default User Account	Description	Default Passphrase
admin	The default Device Administrator user account with read-write permissions.	readwrite
status	The default Device Monitor user account with read-only permissions.	readonly
wg-support	The user account for WatchGuard Support access to your device. Disabled by default.	None

When you add new Device Management users to your Firebox, the account information for the users is stored in a separate file from the device configuration file. This means that if you must restore an earlier version of your configuration file to your Firebox, the user accounts you added are not affected. If you restore the factory-default settings for your Firebox, however, all the Device Management user accounts you added are removed; only the default user accounts are available, with the default passphrases restored.

Add a New Device Management User Account

You can add a user account with the *Device Administrator* or *Device Monitor* role.

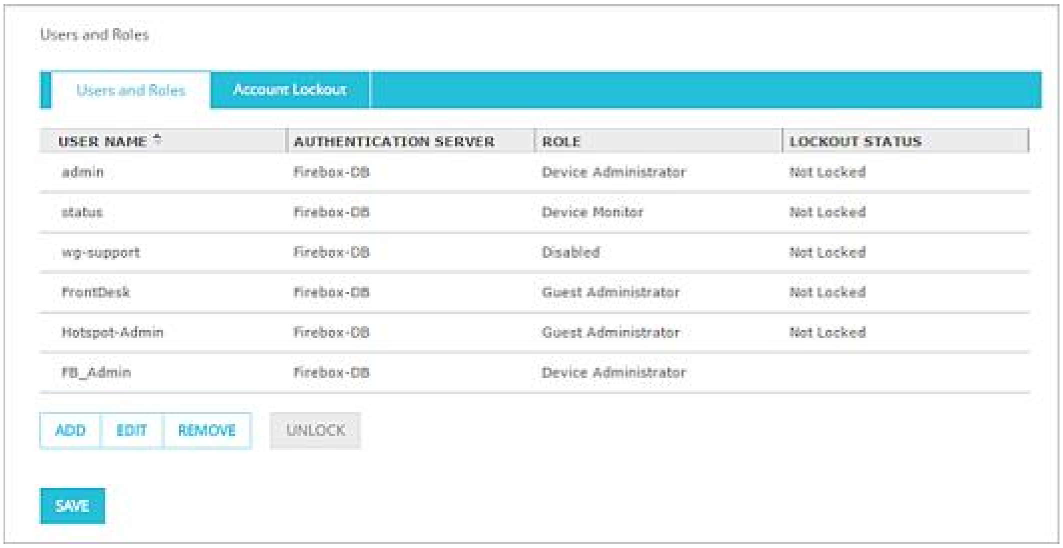
> ⓘ For a compliant configuration, all user accounts must use Firebox-DB as the authentication server.

When you add a device management user account that uses Firebox-DB as the authentication server, you must specify a passphrase.

To add a new device user account, from Fireware Web UI:

1. Select **System > Users and Roles**.

   The Users and Roles page appears.

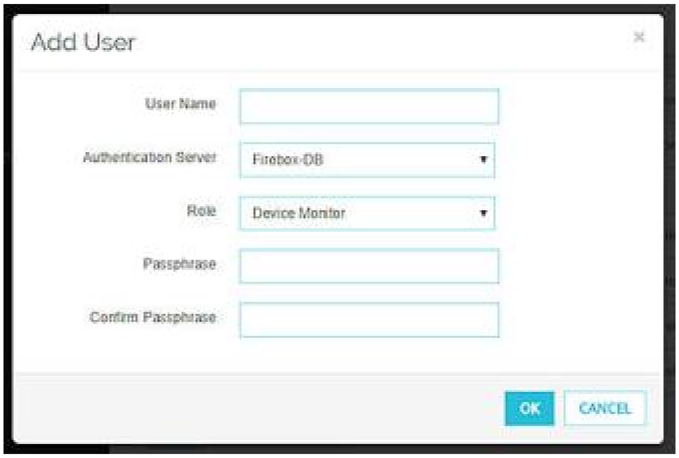


Users and Roles

USER NAME	AUTHENTICATION SERVER	ROLE	LOCKOUT STATUS
admin	Firebox-DB	Device Administrator	Not Locked
status	Firebox-DB	Device Monitor	Not Locked
wg-support	Firebox-DB	Disabled	Not Locked
FrontDesk	Firebox-DB	Guest Administrator	Not Locked
Hotspot-Admin	Firebox-DB	Guest Administrator	Not Locked
FB_Admin	Firebox-DB	Device Administrator	

2. Click **Add**.

   The Add User dialog box appears.



Add User

User Name	
Authentication Server	Firebox-DB ▾
Role	Device Monitor ▾
Passphrase	
Confirm Passphrase	

3. In the **User Name** text box, type the user name for the user account.

4. From the **Authentication Server** drop-down list, select the authentication server for this user account. For a compliant configuration, you must select **Firebox-DB**.
5. From the **Role** drop-down list, select the role for this user account.
6. In the **Passphrase** and **Confirm Passphrase** text boxes, type a secure passphrase for this user account.
7. Click **OK**.
   The user account appears in the Users and Roles list.
8. Click **Save**.

Passphrase Requirements and Recommendations

User account passphrases must meet these requirements:

- Minimum length: 8 characters (To change this, see *Change the Minimum Passphrase Length*)
- Maximum length: 32 characters
- Allowed characters:
  - Letters: A-Z, a-z
  - Numbers: 0-9
  - Special characters: !@#$%^&*()

To create secure passphrases, we recommend that you:

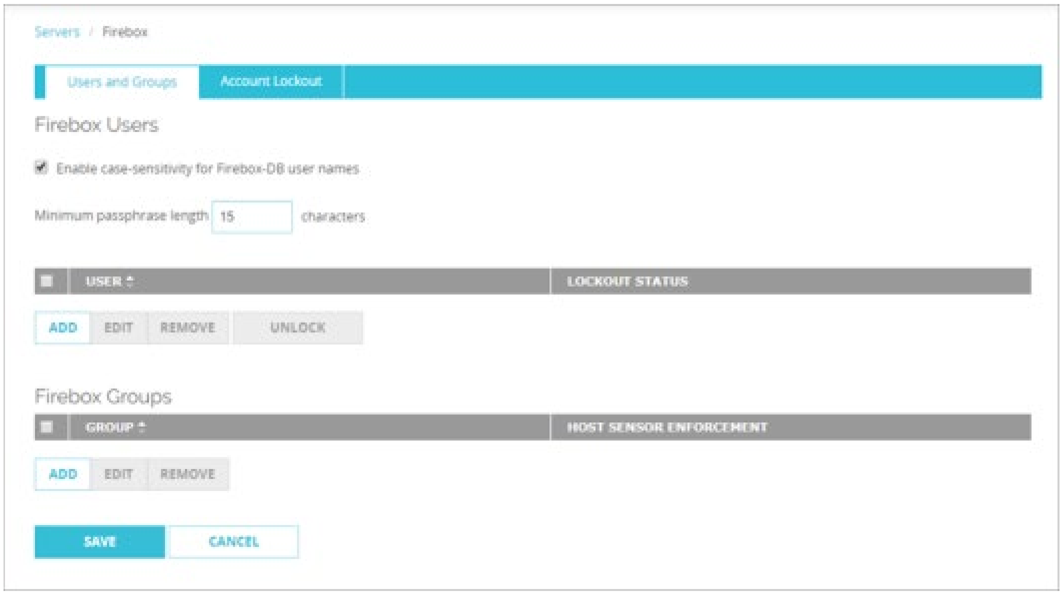
- Use a longer passphrase for stronger security.
- Use a combination of uppercase and lowercase letters, numbers, and special characters.
- Do not use a word from standard dictionaries, even if you use it in a different sequence or in a different language.
- Do not use a business name, familiar name, or the name of a person.

Change the Minimum Passphrase Length

By default, the Firebox accepts a passphrase with a minimum length of eight characters. You can change the minimum required passphrase length for Firebox user authentication. The minimum passphrase length applies to all users who authenticate to the Firebox (Firebox-DB). This includes both management user accounts, and any other user accounts you add.

To change the minimum passphrase length, from Fireware Web UI:

1. Select **Authentication > Servers**.
2. Select **Firebox-DB**.



Firebox Users

☑ Enable case-sensitivity for Firebox-DB user names

Minimum passphrase length 15 characters

Firebox Groups

3. In the **Minimum passphrase length** text box, type or select the minimum passphrase length.
   Configurable minimum passphrase length values range from 8 to 32 characters.
4. Click **Save**.

After you change the minimum passphrase length, the Firebox enforces the minimum length when you change a passphrase for an existing user account, or add a new user account.

Change a User Passphrase

After you change the passphrase length requirements, you can change user passphrases to meet the new requirements.

To change the passphrase of a Device Management user account:

1. Log in to Fireware Web UI.
2. Select **System > Users and Roles**.
3. Select the user name. Click **Edit**.
   The Edit User dialog box appears.
4. Type and confirm the new **Passphrase**.
5. Click **OK**.
6. Click **Save**.

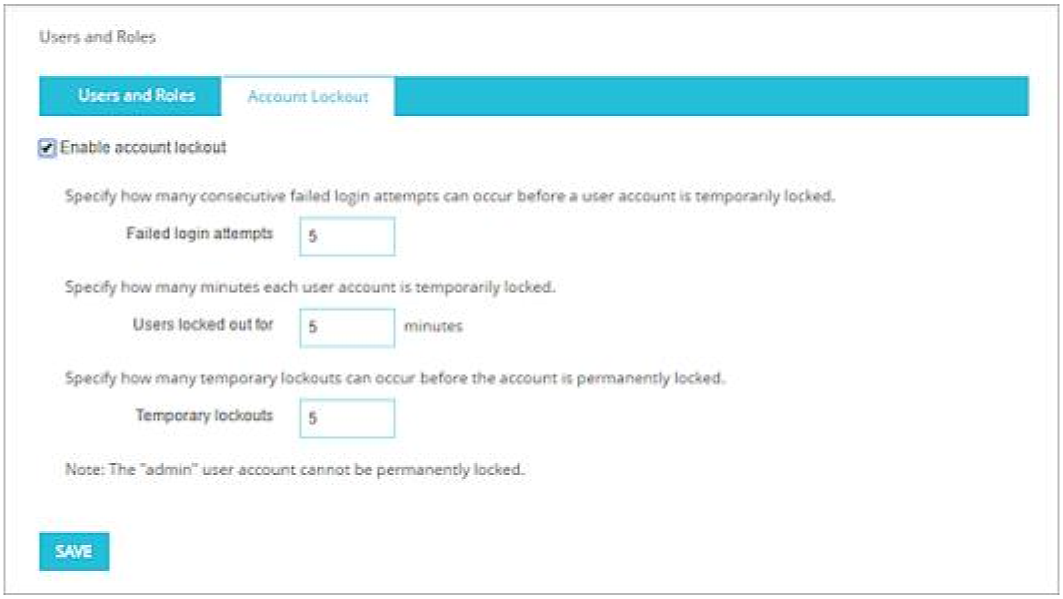
Configure Account Lockout Settings

You can enable Account Lockout to prevent brute force attempts to guess user account passphrases. When Account Lockout is enabled, the Firebox temporarily locks a user account after a specified number of consecutive, unsuccessful login attempts, and permanently locks a user account after a specified number of temporary account lockouts. A permanently locked user account can be unlocked only by a user with *Device Administrator* credentials.

> ⓘ The default *admin* user account can be temporarily locked for connections to the Web UI but cannot be permanently locked. When CSfC mode is enabled, the admin user account is never locked for connections to the CLI through the serial console port.

To configure Account Lockout settings for Device Management user accounts, from Fireware Web UI:

1. Select **System > Users and Roles**.
   The Users and Roles page appears.
2. Select the **Account Lockout** tab.
3. Select the **Enable account lockout** check box.



Users and Roles

☑ Enable account lockout

Specify how many consecutive failed login attempts can occur before a user account is temporarily locked.

Failed login attempts: 5

Specify how many minutes each user account is temporarily locked.

Users locked out for: 5 minutes

Specify how many temporary lockouts can occur before the account is permanently locked.

Temporary lockouts: 5

Note: The "admin" user account cannot be permanently locked.

4. In the **Failed login attempts** text box, type the number of consecutive failed login attempts that can occur before a user account is temporarily locked.
5. In the **Users locked out for** text box, type the number of minutes that a temporarily locked account remains locked.
6. In the **Temporary lockouts** text box, type the number of temporary lockouts that can occur before an account is permanently locked.
7. Click **Save**.

Unlock a Locked Device Management User Account

If Account Lockout is enabled for Device Management user accounts, a Device Management user account can be temporarily or permanently locked after a specified number of failed login attempts. A user with the Device Administrator credentials can unlock a locked account.

To unlock a locked Device Management user account, from Fireware Web UI:

1. Select **System > Users and Roles**.
   The Users and Roles page appears, with the Users and Roles tab selected. The Lockout Status column shows whether an account is locked.
2. Select a locked account.
3. Click **Unlock**.
   A confirmation message appears.
4. Click **Yes**.

Configure Management Session Timeouts

You can set the time period that a user who is logged in with read/write privileges remains authenticated before the Firebox terminates the session. Session timeouts apply to both local management sessions (CLI management sessions through the serial connection) and remote management sessions (through Fireware Web UI).

There are two management session timeouts:

Session Timeout

> The session timeout specifies the maximum length of time a management user can remain authenticated to the Firebox, regardless of user activity. The default session timeout is 10 hours.

Idle Timeout

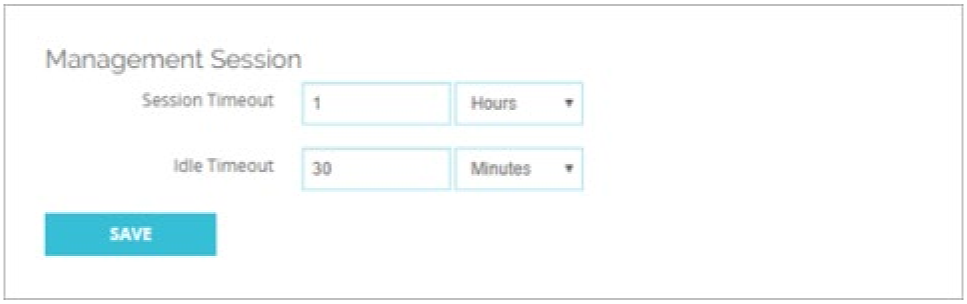
> The idle timeout specifies the maximum length of time a management user can remain authenticated to the Firebox when the user is idle (not sending any traffic to the Firebox). The default idle timeout is 15 minutes.

When either session timeout expires, the Firebox terminates the management session.

> ⓘ If you configure both session timeouts to zero (0) seconds, minutes, hours, or days, the session does not expire and the management user can stay authenticated for any length of time.

To configure the session timeout settings, from Fireware Web UI:

1. Select **Authentication > Settings**.
2. Scroll down to the **Management Session** settings.



Management Session

Session Timeout: 1 Hours

Idle Timeout: 30 Minutes

3. In the **Session Timeout** settings, specify the maximum length of time the user can remain authenticated to the Firebox.
4. In the **Idle Timeout** settings, specify the maximum length of time the user can remain authenticated to the Firebox when the user is idle.
5. Click **Save**.

Updated session timeouts apply to all new management sessions to Fireware Web UI and to connections to the CLI through a console connection. They do not affect users currently authenticated to the Firebox.

> ⓘ For updated session timeouts to apply to your management session, you must log out and log in again.

Manually Terminate a Management Session

To terminate your current management session:

- To terminate your current management session to Fireware Web UI, click **Logout**.
- To terminate your current management session to the CLI, in Main command mode, type **exit**.

An administrator can also manually terminate the session of another connected management user. To terminate the session of a management user, you must be logged in to the Firebox as a user with Device Administrator credentials.

To terminate an active management session, from Fireware Web UI:

1. Select **System Status > Users and Roles**.
   The Users and Roles page appears.
2. From the **Users and Roles** list, select the check box for one or more authenticated management users.
3. Click **Log off users**.
   The selected users are logged off from the device.

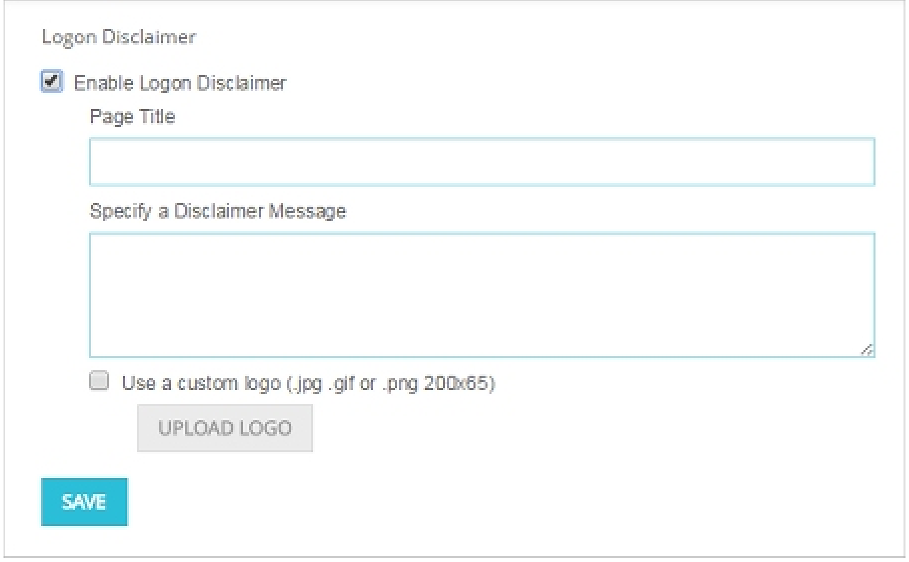
> ⓘ If you select your own management session, your session ends immediately.

Configure the Logon Disclaimer

To enable the Firebox to show a message before a user logs in, you can enable the Logon Disclaimer.

To enable and configure the Logon Disclaimer:

1. Select **System > Logon Disclaimer**.
   The Logon Disclaimer page appears.



Logon Disclaimer

☑ Enable Logon Disclaimer

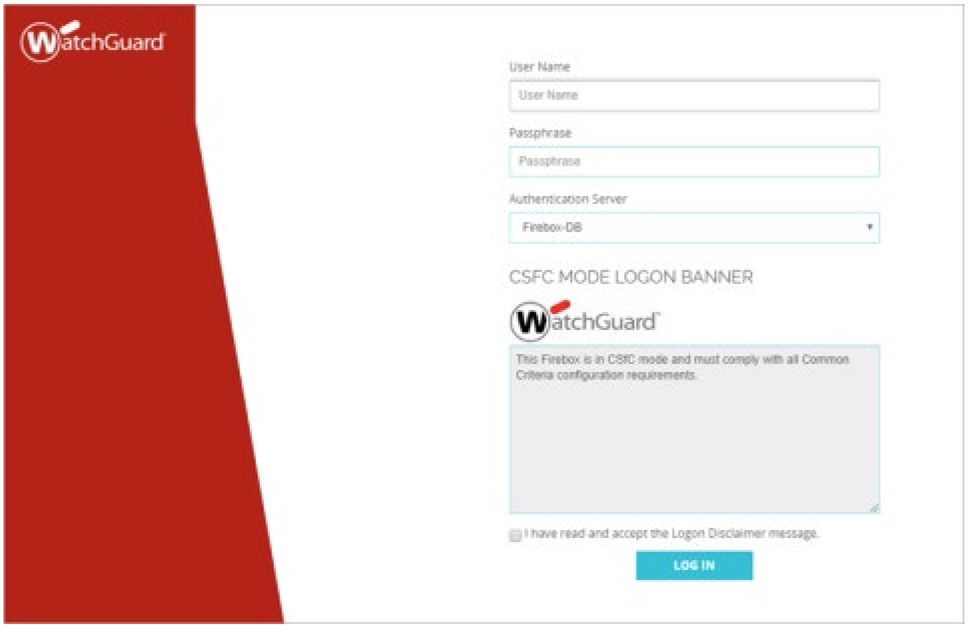
Page Title

Specify a Disclaimer Message

☐ Use a custom logo (.jpg .gif or .png 200x65)

2. Select the **Enable Logon Disclaimer** check box.
3. In the **Page Title** text box, type the text for the title of the **Logon Disclaimer** page.
4. In the **Specify a Disclaimer Message** text box, type or paste the text for the disclaimer message.
5. To add a custom logo to the disclaimer message:
   a. Select the **Use a custom logo** check box.
   b. Click **Upload Logo** and select the image file.
6. Click **Save**.

When the logon disclaimer is enabled, Device Management users must accept the Logon Disclaimer message to log in to Fireware Web UI.



User Name

User Name

Passphrase

Passphrase

Authentication Server

Firebox-DB

CSFC MODE LOGON BANNER

This Firebox is in CSfC mode and must comply with all Common Criteria configuration requirements.

□ I have read and accept the Logon Disclaimer message.

The text also appears in the CLI console before a user logs in.

Web Server Certificate

The default web server certificate on the Firebox is a self-signed certificate. To configure your Firebox to use an ECDSA certificate, you must import a new web server certificate, and configure the Firebox to use it as the web server certificate.

Import and Install a Web Server Certificate

You can replace the default self-signed web server certificate with a signed CA certificate that will be automatically trusted by web browsers. To use a signed CA certificate, you must import this certificate to your Firebox before you can select it as the current web server certificate. In most cases, this certificate signed by a Certificate Authority (CA) requires one or more root and intermediate certificates to complete the chain of trust for the current certificate. You must import these certificates to your Firebox in the correct order before you install the new web server certificate so that the chain of trust is established.

To import and install a new web server certificate, you must complete these procedures:

1. Create a Certificate Signing Request (CSR) for a new web server certificate.
2. Use the CSR to request a signed certificate from a trusted CA.
3. Import the CA certificates in the certificate chain of trust, and import the new web server certificate.
4. Configure the Firebox to use the new web server certificate.

The steps to complete each procedure are described below.

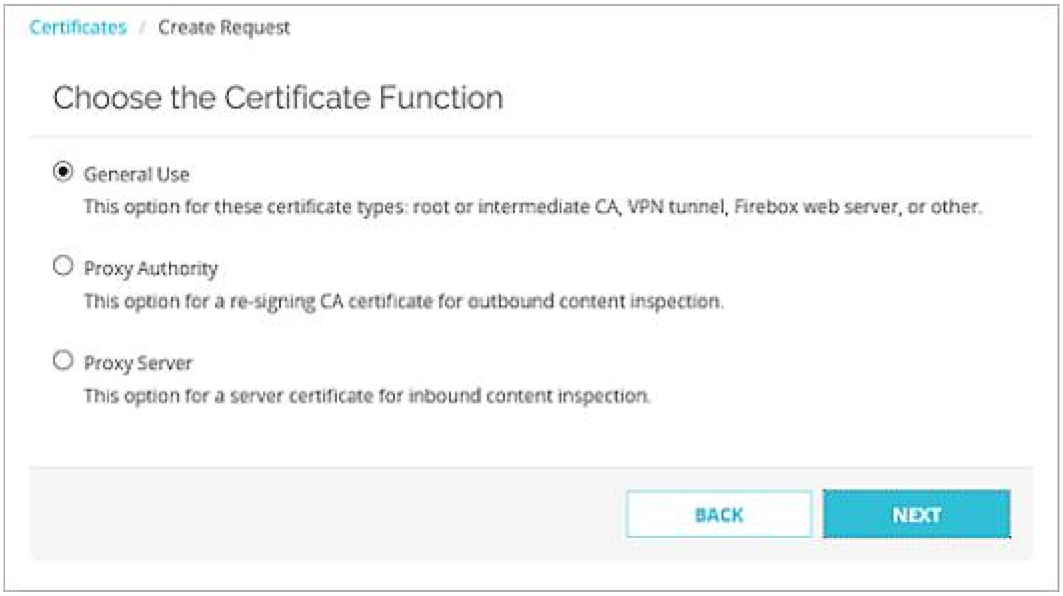
ⓘ If you create a certificate with third-party software such as OpenSSL, the EKU field in the certificate must be populated with the values for *TLS Web Server Authentication* and *TLS Web Client Authentication*. These values are required for any web server certificates imported on the Firebox.

Create a CSR

To create a self-signed certificate, you add part of a cryptographic key pair in a certificate signing request (CSR) and send the request to a CA. The CA issues a certificate after the CA receives the CSR and verifies your identity.

To create a CSR with Fireware Web UI:

1. Select **System > Certificates**.
2. Click **Create CSR**.
   The CSR Wizard starts.
3. Click **Next**.
4. Select **General Use**.



Certificates / Create Request

Choose the Certificate Function

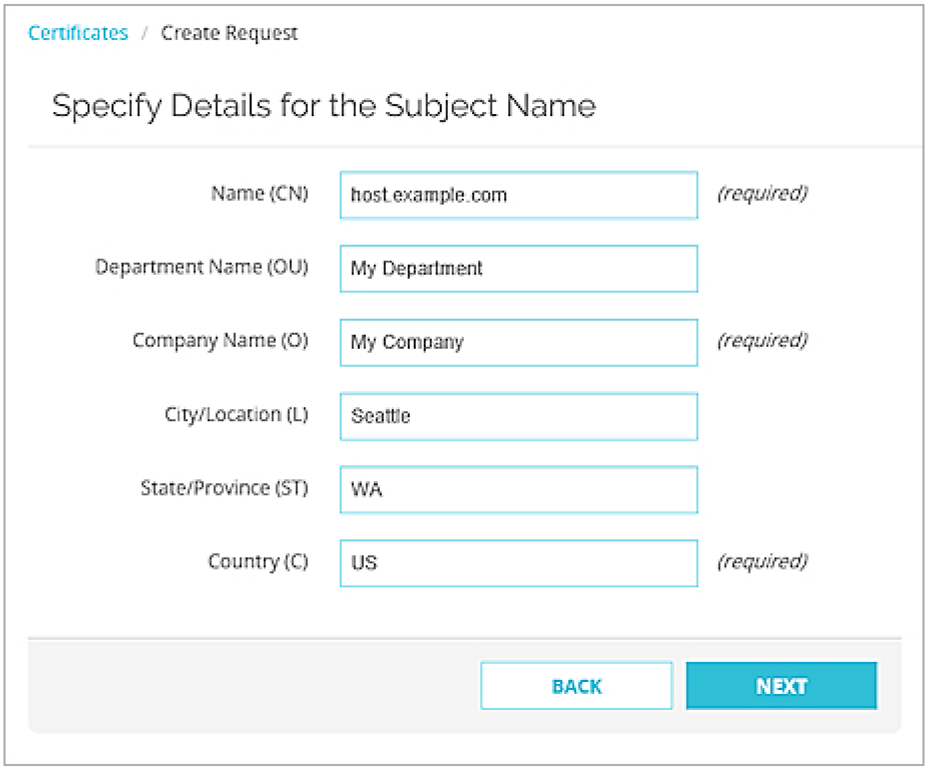
● General Use
This option for these certificate types: root or intermediate CA, VPN tunnel, Firebox web server, or other.

○ Proxy Authority
This option for a re-signing CA certificate for outbound content inspection.

○ Proxy Server
This option for a server certificate for inbound content inspection.

5. Click **Next**.
6. Type these certificate request details:
   - **Name (CN)** — The CN (Common Name) is the fully qualified domain name of the device you want to secure, such as *host.example.com*.
   - **Department Name (OU)** — Type the OU (Organizational Unit) that the device belongs to. For example, IT or Sales.
   - **Company Name (O)** — Type the name of the company that the device belongs to.
   - **City/Location (L)** — Type the city or location where the device is located.

- **State/Province (ST)** — Type the two-character state or province code where the device is located.
- **Country (C)** — Type the two-character country code where the device is located.



Specify Details for the Subject Name

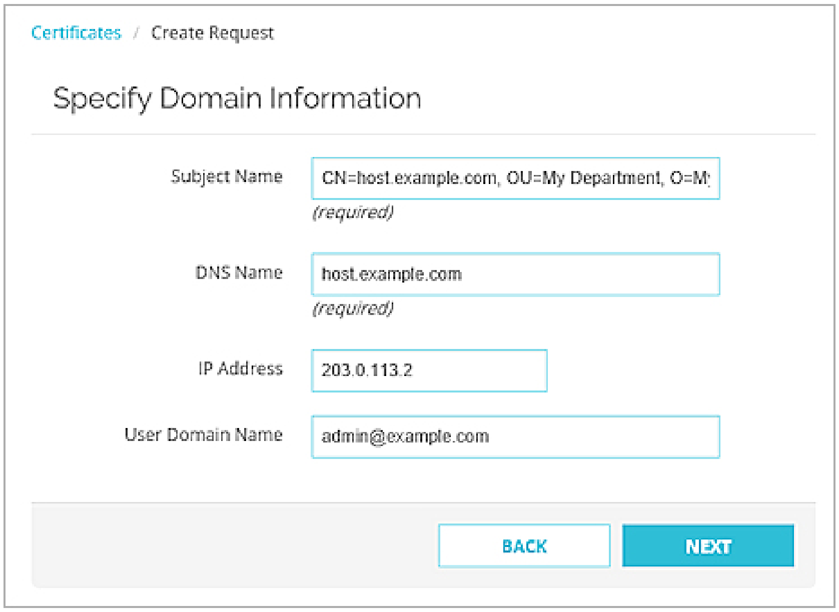
Name (CN)	host.example.com	(required)
Department Name (OU)	My Department	
Company Name (O)	My Company	(required)
City/Location (L)	Seattle	
State/Province (ST)	WA	
Country (C)	US	(required)

7. Click **Next**.

   The wizard creates a subject name based on the information you entered on the previous page.

8. Type the appropriate domain information:

   - **Subject Name** — The Subject Name is completed automatically with information you specified in a previous step.
   - **DNS Name** — The DNS name of the device you want to secure, such as *host.example.com*.
   - **IP Address** — The IP address of the device you want to secure.
   - **User Domain Name** — The administrator email address for the device domain.



Certificates / Create Request

Specify Domain Information

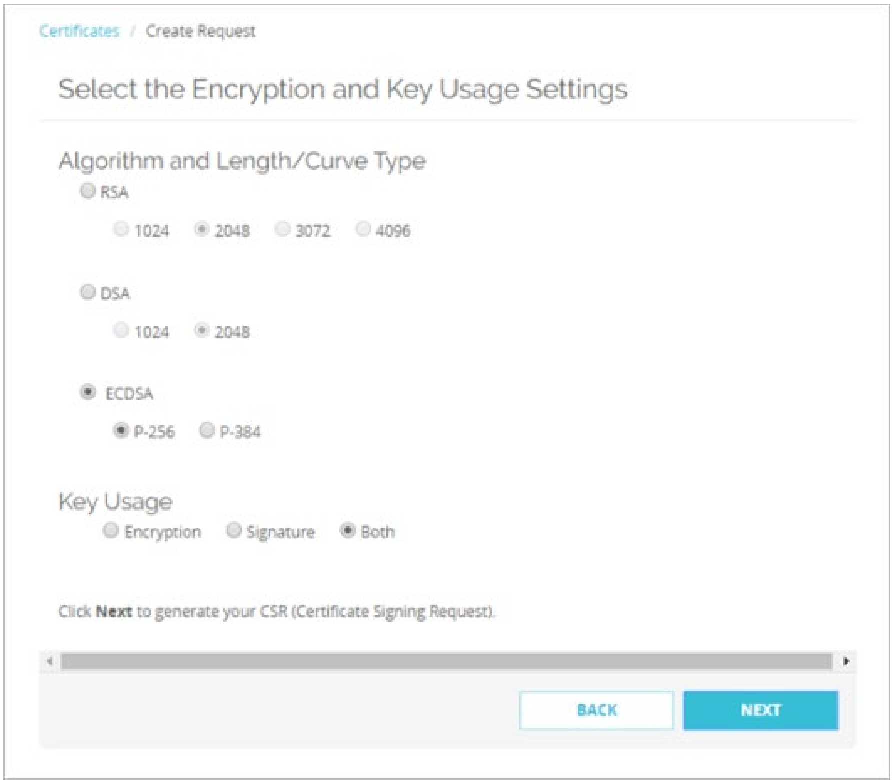
Subject Name: CN=host.example.com, OU=My Department, O=M; *(required)*

DNS Name: host.example.com *(required)*

IP Address: 203.0.113.2

User Domain Name: admin@example.com

9. Click **Next**.
10. Select the algorithm, key length, and key usage.
    - **Algorithm and Length/Curve Type** — Select **ECDSA** and either **P-256** or **P384**.
    - **Key Usage** — Select **Both**.



Certificates / Create Request

Select the Encryption and Key Usage Settings

Algorithm and Length/Curve Type

○ RSA

○ 1024 ● 2048 ○ 3072 ○ 4096

○ DSA

○ 1024 ● 2048

● ECDSA

● P-256 ○ P-384

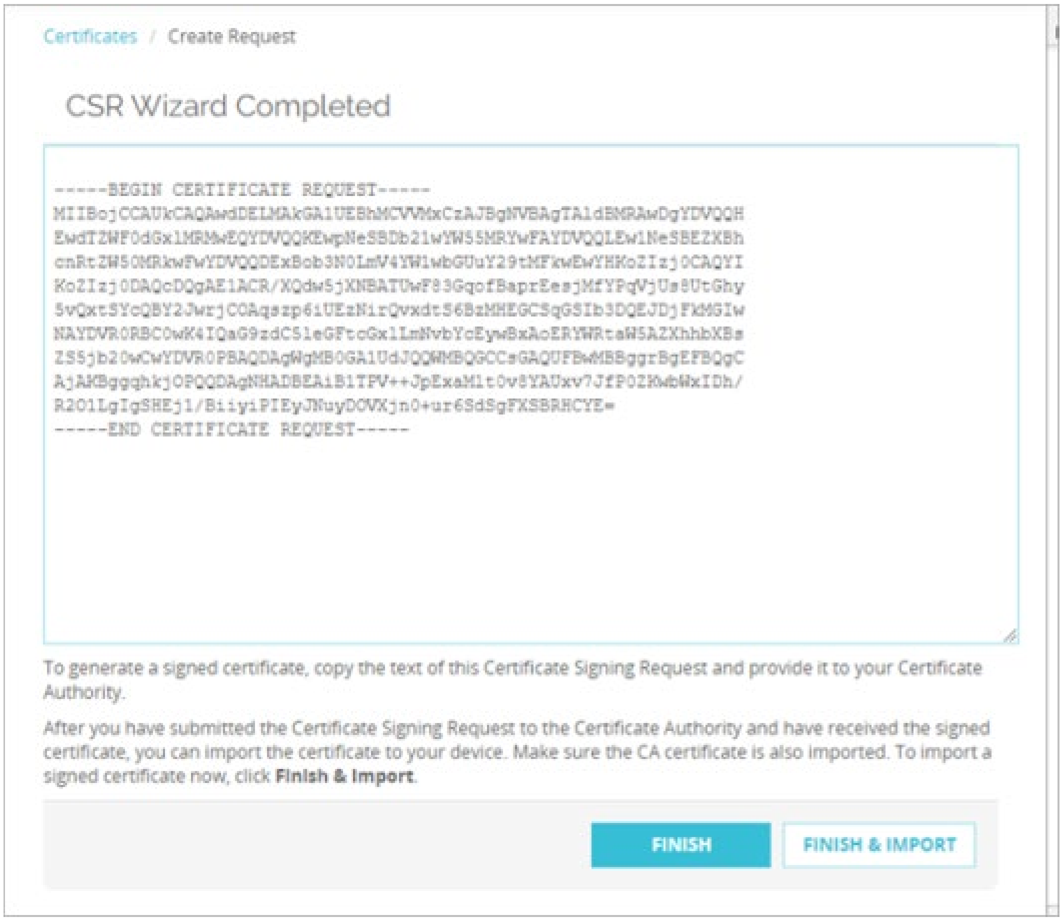
Key Usage

○ Encryption ○ Signature ● Both

Click **Next** to generate your CSR (Certificate Signing Request).

11. Click **Next**.

    The generated CSR is displayed.



CSR Wizard Completed

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBojCCAUkCAQAwdDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQH
EwdTZWF0dGxlMRMwEQYDVQQKEwpNeSBDb21wYW55MRYwFAYDVQQLEw1NeSBEZXBh
cnRtZW50MRkwFwYDVQQDExBob3N0LmV4YW1wbGUuY29tMFkwEwYHKoZIzj0CAQYI
KoZIzj0DAQcDQgAE1ACR/XQdw5jXNBATUwF83GqofBaprEesjMfYPqVjUs8UtGhy
5vQxtSYcQBY2JwrjCOAqszp6iUEzNirQvxdt56BzMHEGCSqGSIb3DQEJDjFkMGIw
NAYDVR0RBC0wK4IQaG9zdC5leGFtcGxlLmNvbYcEywBxAoERYWRtaW5AZXhhbXBs
ZS5jb20wCwYDVR0PBAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcD
AjAKBggqhkjOPQQDAgNHADBEAiB1TPV++JpExaMltOv8YAUxv7JfP0ZKwbWxIDh/
R2O1LgIgSHEj1/BiiyiPIEyJNuyDOVXjn0+ur6SdSgFXSBRHCYE=
-----END CERTIFICATE REQUEST-----
```

To generate a signed certificate, copy the text of this Certificate Signing Request and provide it to your Certificate Authority.

After you have submitted the Certificate Signing Request to the Certificate Authority and have received the signed certificate, you can import the certificate to your device. Make sure the CA certificate is also imported. To import a signed certificate now, click **Finish & Import**.

You must send this CSR to a certificate authority (CA) for signing before you can use it with your Firebox.

When you import the finished certificate, you must first import the CA certificate used to sign the new certificate with the **General Use** category.

- Click **Finish & Import** to import a certificate.

  The Import Certificate dialog box appears.

- Click **Finish** to close the wizard.

Use the CSR to Request a Signed Certificate From a Trusted CA

A certificate authority (CA) signs and issues certificates. These CA-signed certificates are automatically trusted by client web browsers because they originate from a trusted source.

After the CSR is created, you must send the CSR to a Trusted CA for signing. When you receive the signed web server certificate for your Firebox, you must first import the CA certificate chain to your Firebox to establish trust, then import your Firebox Web Server certificate.

Import the CA Certificates and Web Server Certificate

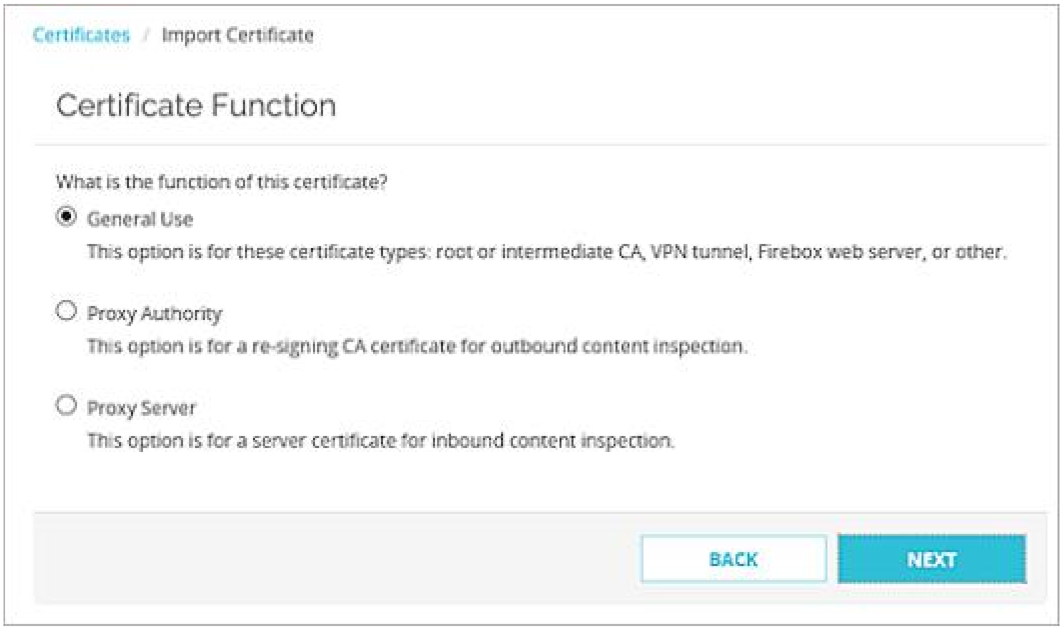
You must import the CA certificates required for the chain of trust for your new signed Web Server certificate to your Firebox.

First, you must download the CA certificate chain that was used to sign your new Web Server certificate. This usually includes a root certificate and one or more intermediate certificates. Your Certificate Authority might have multiple options to download their CA certificates, including individual Base-64 encoded PEM files and PFX certificate file bundles.

When you import these certificates to your Firebox, you must import them in the correct order to establish the certificate chain of trust. Import the root CA certificate first. Then import all other required certificates in the chain of trust. When you import the certificate, select the **General Use** certificate function.

To import CA certificates to the Firebox, from Fireware Web UI:

1. Select **System > Certificates**.
   The Certificates page appears.
2. Click **Import Certificate**.
   The Import Certificate Wizard appears.
3. Click **Next**.
4. On the **Certificate Function** page, select **General Use**.



Certificate Function

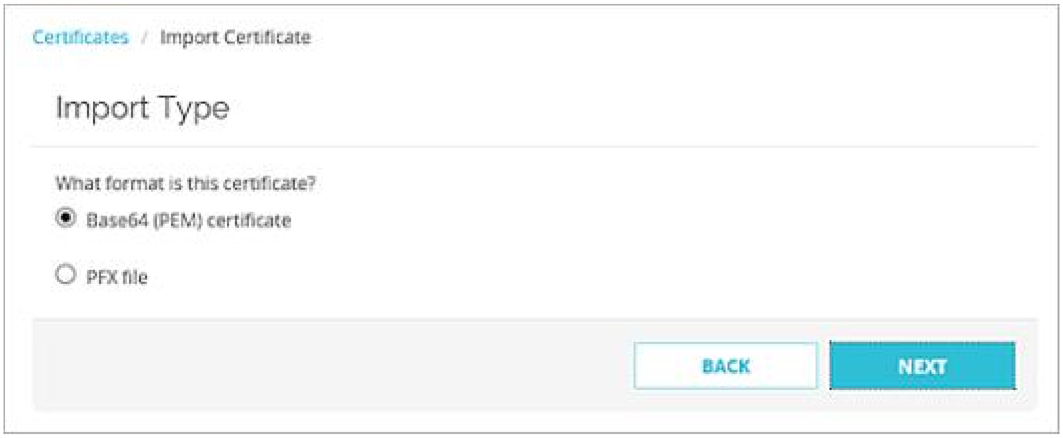
What is the function of this certificate?

● General Use
This option is for these certificate types: root or intermediate CA, VPN tunnel, Firebox web server, or other.

○ Proxy Authority
This option is for a re-signing CA certificate for outbound content inspection.

○ Proxy Server
This option is for a server certificate for inbound content inspection.

5. Click **Next**.
6. On the **Import Type** page, select the **Base64 (PEM) certificate** or **PFX file** certificate type.



Certificates / Import Certificate

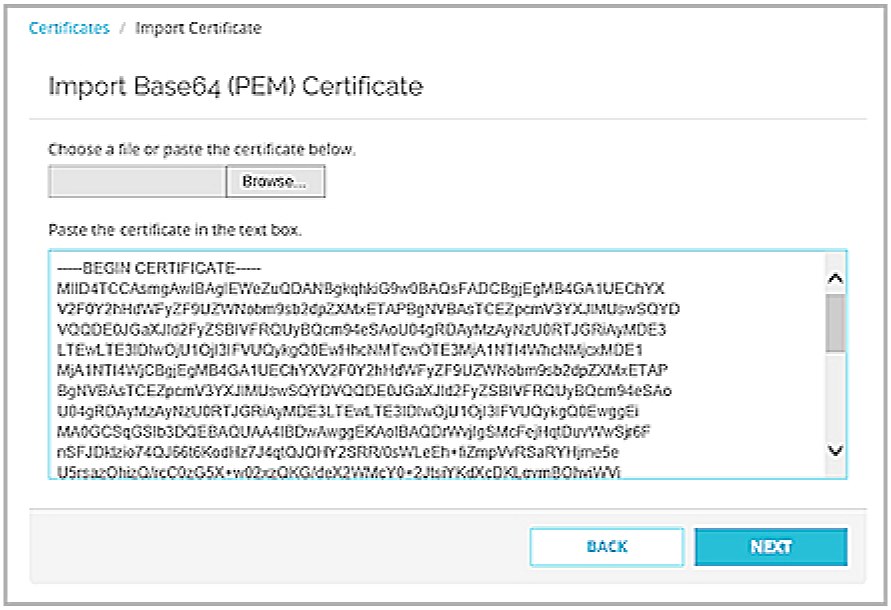
Import Type

What format is this certificate?

● Base64 (PEM) certificate

○ PFX file

7. If you selected **Base64 (PEM) certificate**, you can click **Browse** to select and load the certificate from a file, or copy and paste the PEM certificate contents in the text box. If the certificate includes a private key, type the password to decrypt the key.



Certificates / Import Certificate

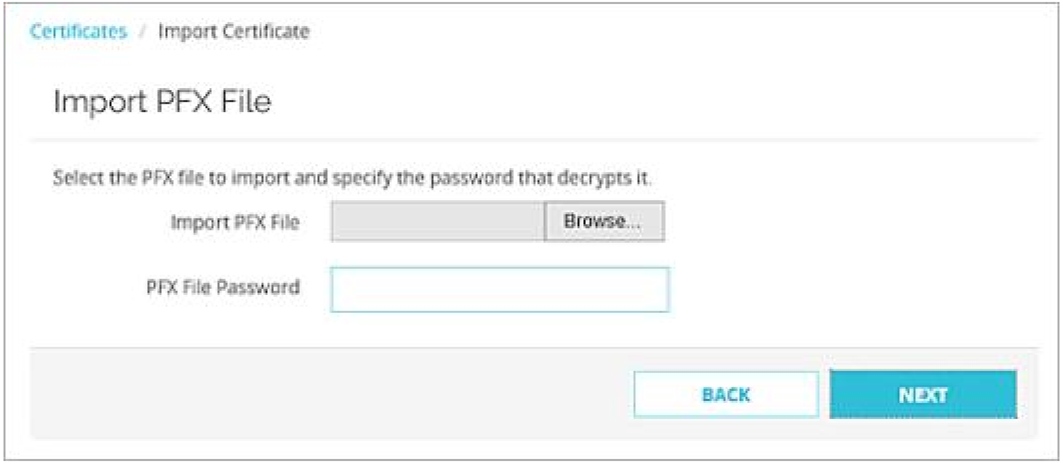
Import Base64 (PEM) Certificate

Choose a file or paste the certificate below.

Paste the certificate in the text box.

```
-----BEGIN CERTIFICATE-----
MIID4TCCAsmgAwIBAgIEWeZuQDANBgkqhkiG9w0BAQsFADCBgjEgMB4GA1UEChYX
V2F0Y2hHdWFyZF9UZWNobm9sb2dpZXMxETAPBgNVBAsTCEZpcmV3YXJlMUswSQYD
VQQDE0JGaXJld2FyZSBIVFRQUyBQcm94eSAoU04gRDAyMzAyNzU0RTJGRiAyMDE3
LTEwLTE3IDIwOjU1OjI3IFVUQykgQ0EwHhcNMTcwOTE3MjA1NTI4WhcNMjcxMDE1
MjA1NTI4WjCBgjEgMB4GA1UEChYXV2F0Y2hHdWFyZF9UZWNobm9sb2dpZXMxETAP
BgNVBAsTCEZpcmV3YXJlMUswSQYDVQQDE0JGaXJld2FyZSBIVFRQUyBQcm94eSAo
U04gRDAyMzAyNzU0RTJGRiAyMDE3LTEwLTE3IDIwOjU1OjI3IFVUQykgQ0EwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDrWyjIgSMcFcjHqtDuvWwSjr6F
nSFJDkIzio74QJ66t6KodHz7J4qtQJOHY2SRR/0sWLeEh+fiZmpVvRSaRYHjme5e
U5rsazOhizQ/icC0zG5X+w02xzQKG/deX2WMcY0+2JtsiYKdXcDKLevm8OhwWVi
```

If you selected **PFX file**, type the **PFX File Password**, and click **Browse** to select the PFX file to upload.



Certificates / Import Certificate

Import PFX File

Select the PFX file to import and specify the password that decrypts it.

Import PFX File

PFX File Password

8. Click **Next**.

   The certificate is added to the Firebox.

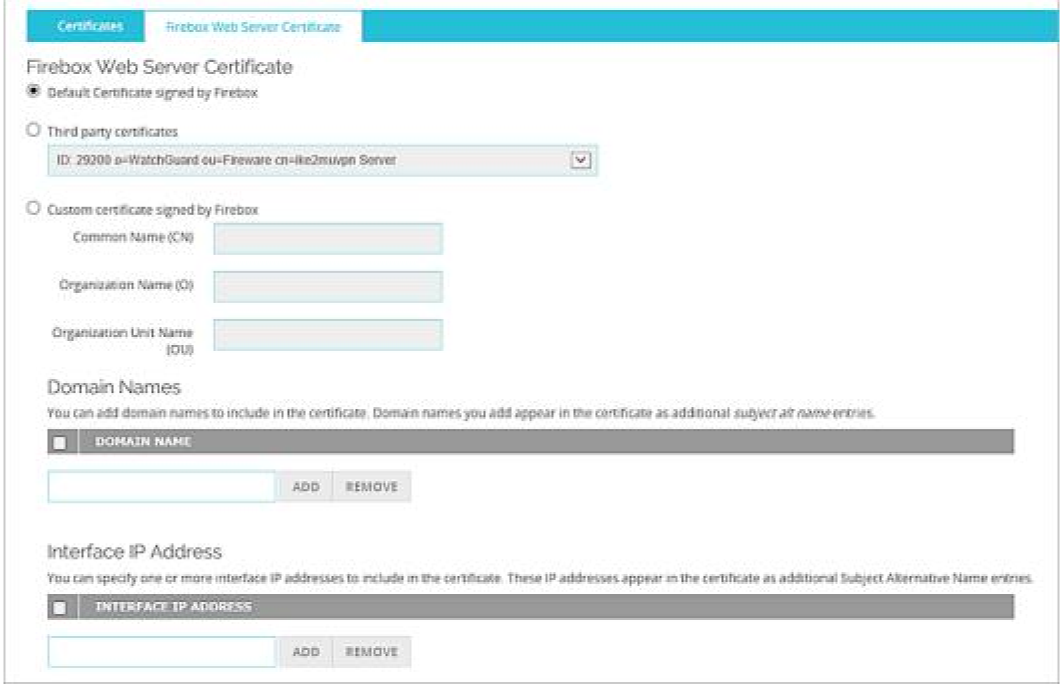
9. Click **Finish**.

Repeat these steps to import each certificate in the certificate chain of trust, and to import the new signed Web Server certificate to your Firebox.

Configure the Firebox to Use the New Web Server Certificate

To select the web server certificate for Firebox authentication, from Fireware Web UI:

1. Select **System > Certificates**.
2. Select the **Firebox Web Server Certificate** tab.



Firebox Web Server Certificate

● Default Certificate signed by Firebox

○ Third party certificates

ID: 29200 o=WatchGuard ou=Fireware cn=ike2muvpn Server

○ Custom certificate signed by Firebox

Common Name (CN)

Organization Name (O)

Organization Unit Name (OU)

Domain Names

You can add domain names to include in the certificate. Domain names you add appear in the certificate as additional *subject alt name* entries.

Interface IP Address

You can specify one or more interface IP addresses to include in the certificate. These IP addresses appear in the certificate as additional Subject Alternative Name entries.

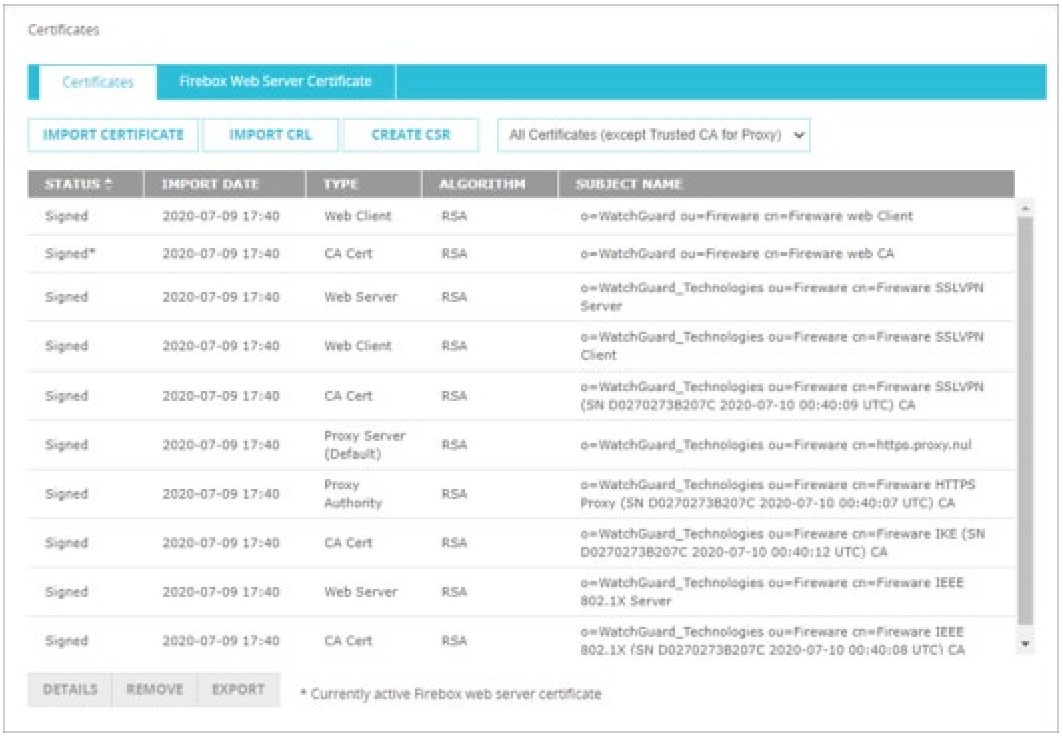
3. Select **Third party certificates**.
4. From the **Third party certificates** drop-down list, select the certificate you imported.
5. Click **Save**.

After you change the Firebox web server certificate, you are automatically logged out of Fireware Web UI. You must log in again to make any other configuration changes.

View and Delete Certificates

To see the certificates on the Firebox, from Fireware Web UI:

1. Select **System > Certificates**.


Certificates
Certificates
Firebox Web Server Certificate
IMPORT CERTIFICATE
IMPORT CRL
CREATE CSR
All Certificates (except Trusted CA for Proxy)

STATUS	IMPORT DATE	TYPE	ALGORITHM	SUBJECT NAME
Signed	2020-07-09 17:40	Web Client	RSA	o=WatchGuard ou=Fireware cn=Fireware web Client
Signed*	2020-07-09 17:40	CA Cert	RSA	o=WatchGuard ou=Fireware cn=Fireware web CA
Signed	2020-07-09 17:40	Web Server	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fireware SSLVPN Server
Signed	2020-07-09 17:40	Web Client	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fireware SSLVPN Client
Signed	2020-07-09 17:40	CA Cert	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fireware SSLVPN (SN D0270273B207C 2020-07-10 00:40:09 UTC) CA
Signed	2020-07-09 17:40	Proxy Server (Default)	RSA	o=WatchGuard_Technologies ou=Fireware cn=https.proxy.nul
Signed	2020-07-09 17:40	Proxy Authority	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fireware HTTPS Proxy (SN D0270273B207C 2020-07-10 00:40:07 UTC) CA
Signed	2020-07-09 17:40	CA Cert	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fireware IKE (SN D0270273B207C 2020-07-10 00:40:12 UTC) CA
Signed	2020-07-09 17:40	Web Server	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fireware IEEE 802.1X Server
Signed	2020-07-09 17:40	CA Cert	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fireware IEEE 802.1X (SN D0270273B207C 2020-07-10 00:40:08 UTC) CA

* Currently active Firebox web server certificate

2. To filter the certificate list, from the drop-down list at the top of the list, select the certificate type to filter on.

To remove a certificate:

1. On the **Certificates** tab, select the certificate.
2. Click **Remove**.
3. In the confirmation dialog box, click **OK**.
   The certificate is deleted from the Firebox. You do not need to click Save to complete this action.

> ⓘ You cannot delete the currently active Firebox web server certificate.

Audit Logging

The Firebox generates audit log messages about firewall traffic, events, and configuration changes.

Local Audit Log Storage

By default, the Firebox saves log messages in internal storage. When an event triggers a log message, the Firebox generates a log message and stores it on the Firebox. If the Firebox is configured to send log messages to a syslog server, the Firebox also attempts to send the log message to the syslog server.

Log messages remain in Firebox local storage until the next time the Firebox reboots. You cannot edit or delete log messages stored on the Firebox.

Audit Log Storage Capacity and Log Deletion

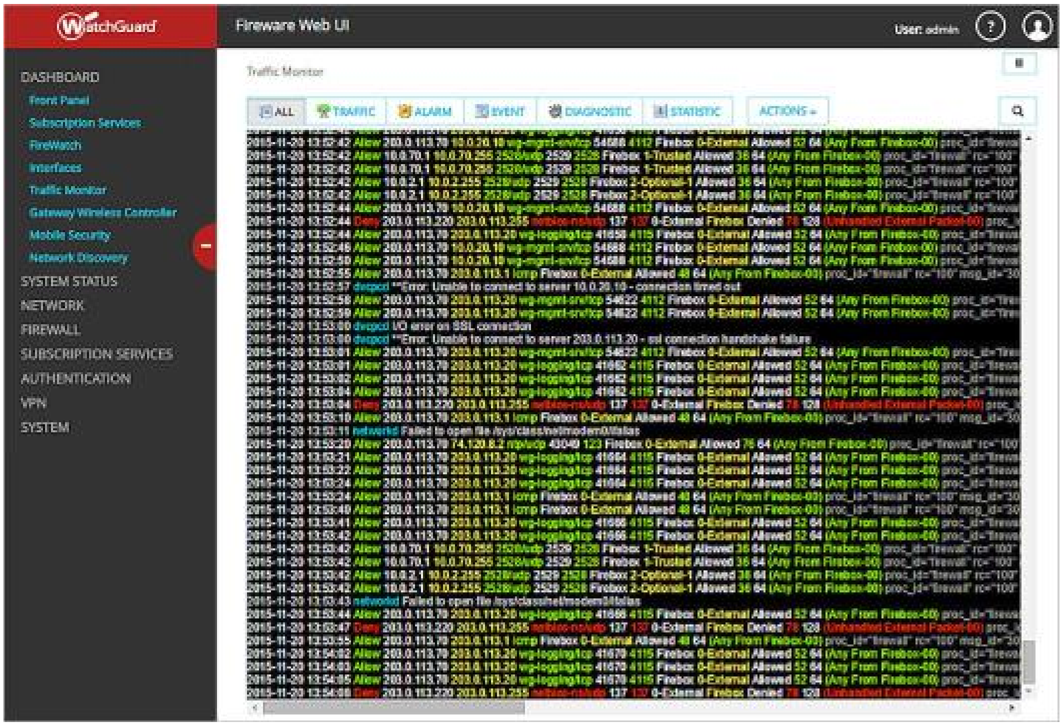
Firebox local storage always contains the most recent log messages. If the local storage on the Firebox becomes full, the Firebox deletes the oldest log messages so that it can store new log messages. If the Firebox removes old log messages, it generates a new log message about that event.

Audit log deletion behavior and audit log storage capacity are not configurable.

See Audit Log Messages Stored on the Firebox

To see log messages stored on the Firebox, from Fireware Web UI:

1. Select **Dashboard > Traffic Monitor**.



```
2015-11-20 13:52:42 Allow 203.0.113.70 10.0.20.10 wg-mgmt-srv/tcp 54688 4112 Firebox 0-External Allowed 52 64 (Any From Firebox-00) proc_id="firewa
2015-11-20 13:52:42 Allow 10.0.70.1 10.0.70.255 2528/udp 2529 2528 Firebox 1-Trusted Allowed 36 64 (Any From Firebox-00) proc_id="firewall" rc="100"
2015-11-20 13:52:42 Allow 10.0.70.1 10.0.70.255 2528/udp 2529 2528 Firebox 1-Trusted Allowed 36 64 (Any From Firebox-00) proc_id="firewall" rc="100"
2015-11-20 13:52:42 Allow 10.0.2.1 10.0.2.255 2528/udp 2529 2528 Firebox 2-Optional-1 Allowed 36 64 (Any From Firebox-00) proc_id="firewall" rc="100"
2015-11-20 13:52:42 Allow 10.0.2.1 10.0.2.255 2528/udp 2529 2528 Firebox 2-Optional-1 Allowed 36 64 (Any From Firebox-00) proc_id="firewall" rc="100"
2015-11-20 13:52:44 Allow 203.0.113.70 10.0.20.10 wg-mgmt-srv/tcp 54688 4112 Firebox 0-External Allowed 52 64 (Any From Firebox-00) proc_id="firewa
2015-11-20 13:52:44 Deny 203.0.113.220 203.0.113.255 netbios-ns/udp 137 137 0-External Firebox Denied 78 128 (Unhandled External Packet-00) proc_
2015-11-20 13:52:44 Allow 203.0.113.70 203.0.113.20 wg-logging/tcp 41658 4115 Firebox 0-External Allowed 52 64 (Any From Firebox-00) proc_id="firewa
2015-11-20 13:52:46 Allow 203.0.113.70 10.0.20.10 wg-mgmt-srv/tcp 54688 4112 Firebox 0-External Allowed 52 64 (Any From Firebox-00) proc_id="firewa
2015-11-20 13:52:50 Allow 203.0.113.70 10.0.20.10 wg-mgmt-srv/tcp 54688 4112 Firebox 0-External Allowed 52 64 (Any From Firebox-00) proc_id="firewa
2015-11-20 13:52:55 Allow 203.0.113.70 203.0.113.1 icmp Firebox 0-External Allowed 48 64 (Any From Firebox-00) proc_id="firewall" rc="100" msg_id="30
2015-11-20 13:52:57 dvcpcd **Error: Unable to connect to server 10.0.20.10 - connection timed out
2015-11-20 13:52:58 Allow 203.0.113.70 203.0.113.20 wg-mgmt-srv/tcp 54622 4112 Firebox 0-External Allowed 52 64 (Any From Firebox-00) proc_id="fire
2015-11-20 13:52:59 Allow 203.0.113.70 203.0.113.20 wg-mgmt-srv/tcp 54622 4112 Firebox 0-External Allowed 52 64 (Any From Firebox-00) proc_id="fire
2015-11-20 13:53:00 dvcpcd I/O error on SSL connection
2015-11-20 13:53:00 dvcpcd **Error: Unable to connect to server 203.0.113.20 - ssl connection handshake failure
2015-11-20 13:53:01 Allow 203.0.113.70 203.0.113.20 wg-mgmt-srv/tcp 54622 4112 Firebox 0-External Allowed 52 64 (Any From Firebox-00) proc_id="fire
2015-11-20 13:53:01 Allow 203.0.113.70 203.0.113.20 wg-logging/tcp 41662 4115 Firebox 0-External Allowed 52 64 (Any From Firebox-00) proc_id="firewa
2015-11-20 13:53:02 Allow 203.0.113.70 203.0.113.20 wg-logging/tcp 41662 4115 Firebox 0-External Allowed 52 64 (Any From Firebox-00) proc_id="firewa
2015-11-20 13:53:04 Allow 203.0.113.70 203.0.113.20 wg-logging/tcp 41662 4115 Firebox 0-External Allowed 52 64 (Any From Firebox-00) proc_id="firewa
2015-11-20 13:53:04 Deny 203.0.113.220 203.0.113.255 netbios-ns/udp 137 137 0-External Firebox Denied 78 128 (Unhandled External Packet-00) proc_
2015-11-20 13:53:10 Allow 203.0.113.70 203.0.113.1 icmp Firebox 0-External Allowed 48 64 (Any From Firebox-00) proc_id="firewall" rc="100" msg_id="30
2015-11-20 13:53:11 networkd Failed to open file /sys/class/net/modem0/ifalias
2015-11-20 13:53:20 Allow 203.0.113.70 74.120.8.2 ntp/udp 43049 123 Firebox 0-External Allowed 76 64 (Any From Firebox-00) proc_id="firewall" rc="100
2015-11-20 13:53:21 Allow 203.0.113.70 203.0.113.20 wg-logging/tcp 41664 4115 Firebox 0-External Allowed 52 64 (Any From Firebox-00) proc_id="firewa
2015-11-20 13:53:22 Allow 203.0.113.70 203.0.113.20 wg-logging/tcp 41664 4115 Firebox 0-External Allowed 52 64 (Any From Firebox-00) proc_id="firewa
2015-11-20 13:53:24 Allow 203.0.113.70 203.0.113.20 wg-logging/tcp 41664 4115 Firebox 0-External Allowed 52 64 (Any From Firebox-00) proc_id="firewa
2015-11-20 13:53:24 Allow 203.0.113.70 203.0.113.1 icmp Firebox 0-External Allowed 48 64 (Any From Firebox-00) proc_id="firewall" rc="100" msg_id="30
2015-11-20 13:53:40 Allow 203.0.113.70 203.0.113.1 icmp Firebox 0-External Allowed 48 64 (Any From Firebox-00) proc_id="firewall" rc="100" msg_id="30
2015-11-20 13:53:41 Allow 203.0.113.70 203.0.113.20 wg-logging/tcp 41666 4115 Firebox 0-External Allowed 52 64 (Any From Firebox-00) proc_id="firewa
2015-11-20 13:53:42 Allow 203.0.113.70 203.0.113.20 wg-logging/tcp 41666 4115 Firebox 0-External Allowed 52 64 (Any From Firebox-00) proc_id="firewa
2015-11-20 13:53:42 Allow 10.0.70.1 10.0.70.255 2528/udp 2529 2528 Firebox 1-Trusted Allowed 36 64 (Any From Firebox-00) proc_id="firewall" rc="100"
2015-11-20 13:53:42 Allow 10.0.70.1 10.0.70.255 2528/udp 2529 2528 Firebox 1-Trusted Allowed 36 64 (Any From Firebox-00) proc_id="firewall" rc="100"
2015-11-20 13:53:42 Allow 10.0.2.1 10.0.2.255 2528/udp 2529 2528 Firebox 2-Optional-1 Allowed 36 64 (Any From Firebox-00) proc_id="firewall" rc="100"
2015-11-20 13:53:42 Allow 10.0.2.1 10.0.2.255 2528/udp 2529 2528 Firebox 2-Optional-1 Allowed 36 64 (Any From Firebox-00) proc_id="firewall" rc="100"
2015-11-20 13:53:43 networkd Failed to open file /sys/class/net/modem0/ifalias
2015-11-20 13:53:44 Allow 203.0.113.70 203.0.113.20 wg-logging/tcp 41666 4115 Firebox 0-External Allowed 52 64 (Any From Firebox-00) proc_id="firewa
2015-11-20 13:53:47 Deny 203.0.113.220 203.0.113.255 netbios-ns/udp 137 137 0-External Firebox Denied 78 128 (Unhandled External Packet-00) proc_
2015-11-20 13:53:55 Allow 203.0.113.70 203.0.113.1 icmp Firebox 0-External Allowed 48 64 (Any From Firebox-00) proc_id="firewall" rc="100" msg_id="30
2015-11-20 13:54:02 Allow 203.0.113.70 203.0.113.20 wg-logging/tcp 41670 4115 Firebox 0-External Allowed 52 64 (Any From Firebox-00) proc_id="firewa
2015-11-20 13:54:03 Allow 203.0.113.70 203.0.113.20 wg-logging/tcp 41670 4115 Firebox 0-External Allowed 52 64 (Any From Firebox-00) proc_id="firewa
2015-11-20 13:54:05 Allow 203.0.113.70 203.0.113.20 wg-logging/tcp 41670 4115 Firebox 0-External Allowed 52 64 (Any From Firebox-00) proc_id="firewa
2015-11-20 13:54:08 Deny 203.0.113.220 203.0.113.255 netbios-ns/udp 137 137 0-External Firebox Denied 78 128 (Unhandled External Packet-00) proc_
```

2. To filter the log messages based on log message type, click a button at the top.
3. To clear all the log messages in the display, from the **Actions** drop-down list, select **Clear Traffic Monitor**.

   This clears the currently displayed log messages, but does not delete the log messages stored on the Firebox.

Configure Logging Settings

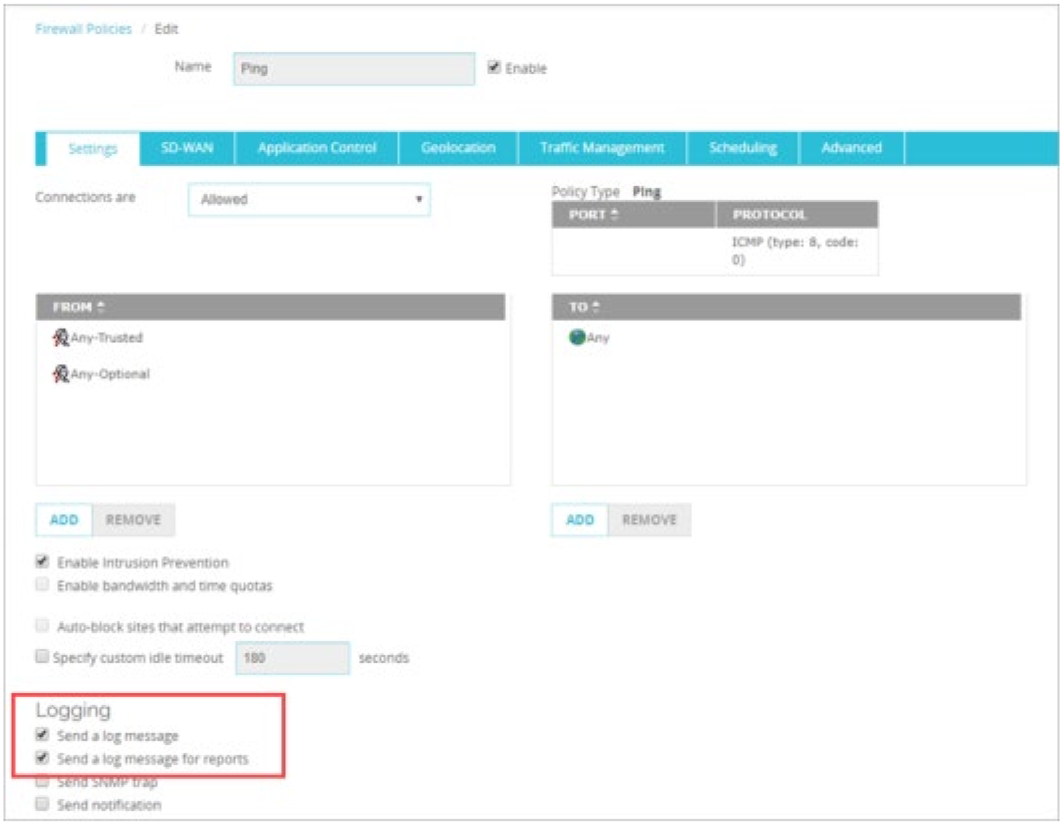
For the Firebox to generate log messages, you must enable logging in policies and in global settings. With the default configuration, most required logging settings are automatically enabled.

Configure Logging in Firewall Policies

The default firewall policies have logging enabled to generate traffic log messages. In any new policies you create, enable these logging settings.

To enable traffic logging in a packet filter policy:

1. Select **Firewall > Firewall Policies**.
2. Edit the policy.
3. In the **Logging** settings, select the **Send a log message** and **Send a log message for reports** check boxes.



Firewall Policies / Edit

Name: Ping ☑ Enable

Connections are: Allowed

Policy Type: Ping

PORT	PROTOCOL
	ICMP (type: 8, code: 0)

FROM: Any-Trusted, Any-Optional

TO: Any

☑ Enable Intrusion Prevention

□ Enable bandwidth and time quotas

□ Auto-block sites that attempt to connect

□ Specify custom idle timeout 180 seconds

Logging

☑ Send a log message

☑ Send a log message for reports

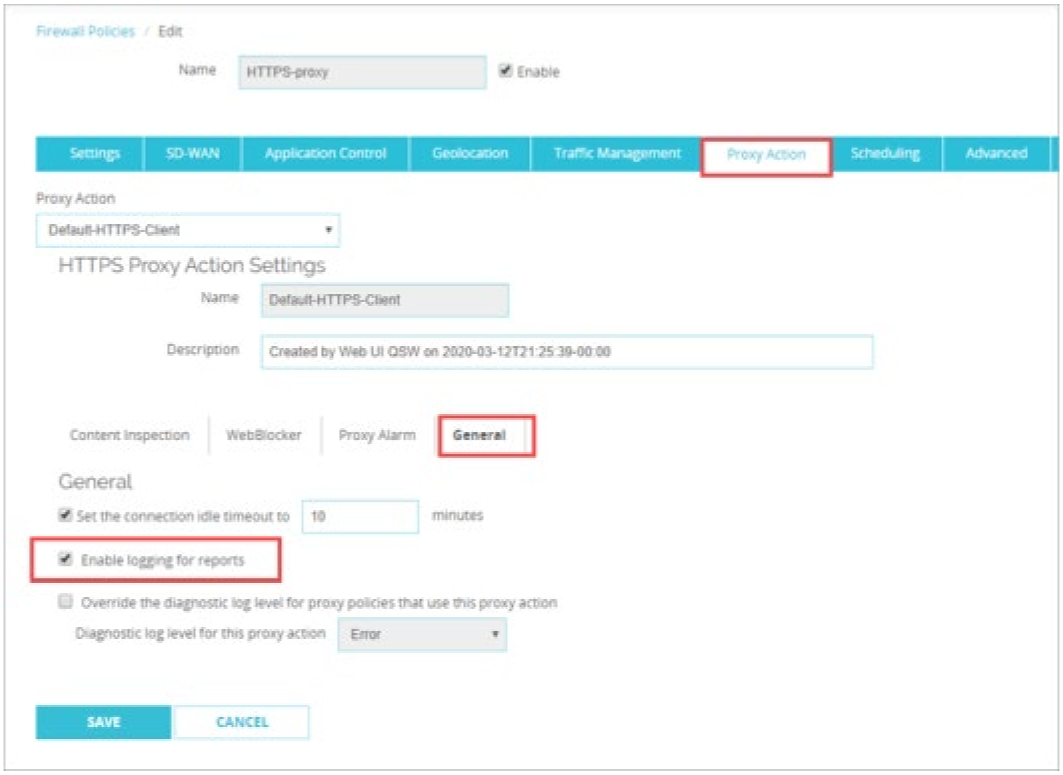
□ Send SNMP trap

□ Send notification

4. Click **Save**.

To enable traffic logging in a proxy policy:

1. Select **Firewall > Firewall Policies**.
2. Edit the policy.
3. Select the **Proxy Action** tab.
4. In the Proxy Action **General** settings, select the **Enable logging for reports** check box.



Firewall Policies / Edit

Name: HTTPS-proxy ☑ Enable

Proxy Action: Default-HTTPS-Client

HTTPS Proxy Action Settings

Name: Default-HTTPS-Client

Description: Created by Web UI QSW on 2020-03-12T21:25:39-00:00

General

☑ Set the connection idle timeout to 10 minutes

☑ Enable logging for reports

☐ Override the diagnostic log level for proxy policies that use this proxy action

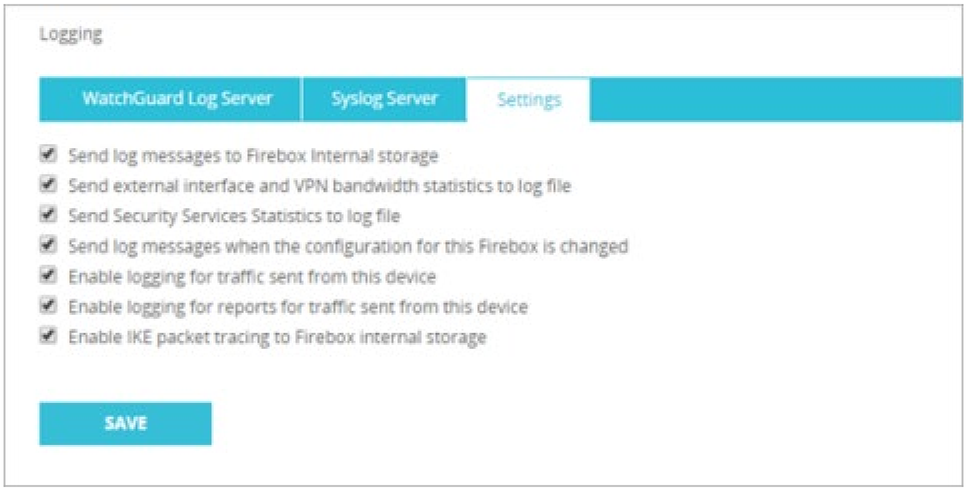
Diagnostic log level for this proxy action: Error

5. Click **Save**.

Configure Global Logging Settings

To configure the global logging settings, from Fireware Web UI:

1. Select **System > Logging**.
2. Select the **Settings** tab.
3. Enable all of the available logging options.



Logging

☑ Send log messages to Firebox internal storage
☑ Send external interface and VPN bandwidth statistics to log file
☑ Send Security Services Statistics to log file
☑ Send log messages when the configuration for this Firebox is changed
☑ Enable logging for traffic sent from this device
☑ Enable logging for reports for traffic sent from this device
☑ Enable IKE packet tracing to Firebox internal storage

4. Click **Save**.

Configure Diagnostic Log Levels

Diagnostic log level settings control the level of detail included in diagnostic log files. For the Firebox to generate all required log messages, you must set the Diagnostic Log Level to Debug for Authentication, Management, and VPN > IKE logging.

To configure diagnostic log levels, from Fireware Web UI:

1. Select **System > Diagnostic Log**.
2. Set the **Authentication** diagnostic log level to **Debug**.
3. Set the **Management** diagnostic level to **Debug**.
4. Set the **VPN > IKE** diagnostic log level to **Debug**.
5. Click **Save**.

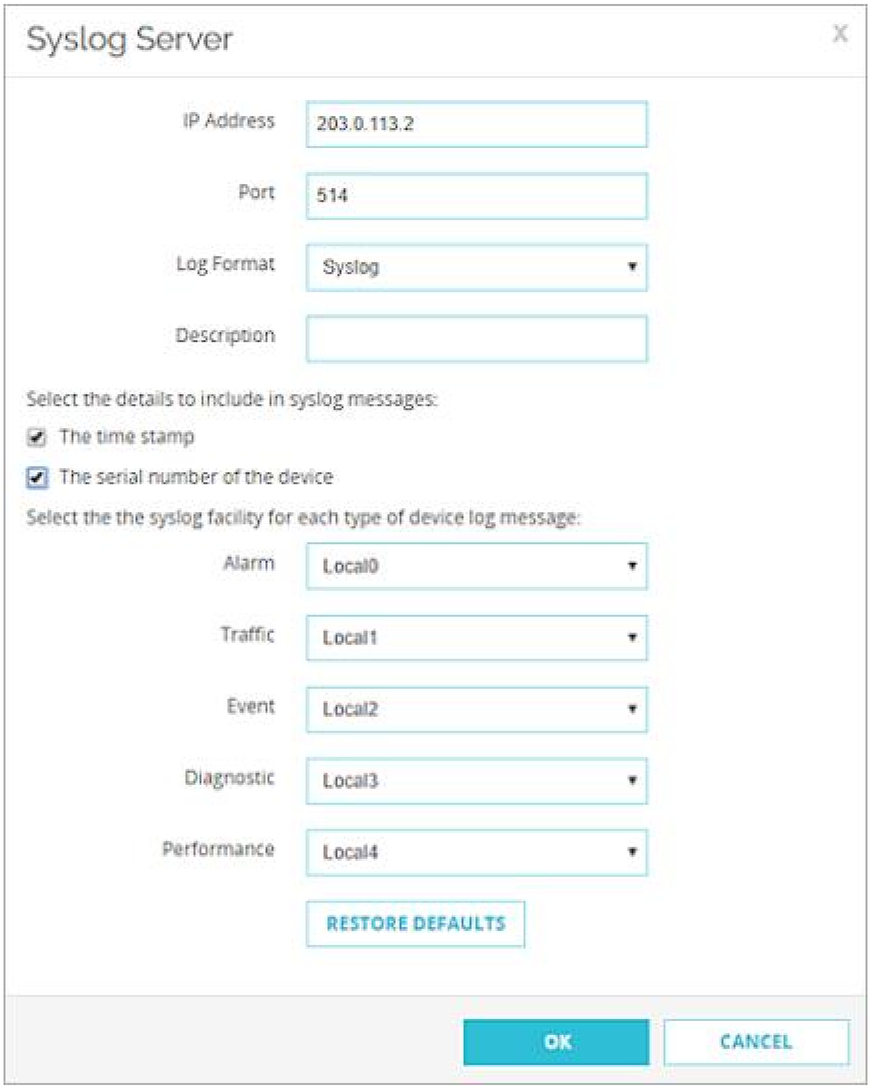
Send Log Messages to a Syslog Server

You can configure the Firebox to send syslog log messages to a syslog server. When you configure a syslog server, the Firebox sends all log messages to the specified syslog server immediately after they are generated.

> ⓘ Syslog log messages sent by the Firebox are not encrypted. To protect the connection, use an IPSec VPN tunnel to connect the Firebox to your syslog server. For more information, see *IPSec VPN*.
>
> ⓘ Firebox shutdown audit record and end audit capture log messages will not appear on syslog server due to shutdown timing. These log messages are available in Fireware Web UI.

To send log messages to a syslog server, from Fireware Web UI:

1. Select **System > Logging**.
   The Logging page appears.
2. Click the **Syslog Server** tab.
3. Select the **Send log messages to these syslog servers** check box.
4. Click **Add**.
   The Syslog Server dialog box appears.
5. In the **IP Address** text box, type the server IP address.
6. In the **Port** text box, the default syslog server port (514) appears. To change the server port, type or select a different port for your server.
7. From the **Log Format** drop-down list, select **Syslog**.


Syslog Server

IP Address: 203.0.113.2

Port: 514

Log Format: Syslog

Description:

Select the details to include in syslog messages:

☑ The time stamp

☑ The serial number of the device

Select the the syslog facility for each type of device log message:

Alarm: Local0

Traffic: Local1

Event: Local2

Diagnostic: Local3

Performance: Local4

8. (Optional) In the **Description** text box, type a description for the server.
9. To include the date and time that the event occurs on your Firebox in the log message details, select the **The time stamp** check box.
10. To include the serial number of the Firebox in the log message details, select the **The serial number of the device** check box.
11. In the **Syslog Settings** section, for each type of log message, select a syslog facility from the drop-down list.
12. Click **Save**.

Audit Log Format

Your Firebox sends several types of log messages for events that occur on the device. Each message includes the message type in the text of the message. The log messages types are:

- **Traffic** — Information about policy actions on firewall traffic.
- **Alarm** — Notification of an event that has an associated alarm.
- **Event** — Many types of events on the Firebox, including administrative actions, and updates to system components and services.
- **Diagnostic** — Detailed information for product components, based on the configured diagnostic log level.
- **Statistic** — Information about system performance.

Each log message includes a string of data about events or the traffic on the Firebox. The log message format varies depending on the type of log message. All log messages contain a time and date stamp to indicate when the event occurred.

The standard format for all audit logs is as follows:

<device ID>-<date>-<time><audit_record><message_id>

- **device ID** — Device name and serial number.
- **date** — Date on which the event occurred (yyyy-mm-dd).
- **time** — Time at which the event occurred (24-hour clock).
- **audit_record** — A variable string potentially containing the event information identified in column 3 of the table in *Audit Log Records*, the user identity which caused the event, an indication of success or failure (when applicable), and any other specific information related to the event.
- **message_id** — A unique message identification number to identify the log message. Not all log messages have a message ID.

Example Event Logs

For event logs, the audit record starts with the name of the component, followed by information about the event. Two examples:

Management user logged in to Fireware Web UI:

```
2020-03-19 16:28:39 sessiond Management user admin@Firebox-DB from 10.0.1.2 logged in
msg_id="3E00-0002"
```

DHCP server on the Firebox assigned an IP address to a network client:

```
2020-03-19 16:32:27 dhcpd DHCPREQUEST for 10.0.1.2 (10.0.1.1) from 00:24:9b:0c:c0:b6
(LAP-client) via eth1 msg_id="1600-0066"
```

Example Traffic Audit Log

Traffic log messages indicate traffic allowed or denied by the firewall policies. Each traffic log message includes a string of data about the traffic event. If you review the log messages in Traffic Monitor, the details in the log message have different colors to help visually distinguish each detail. Traffic log messages show information about security services. If a user is authenticated, the log messages includes the user name.

Here is an example of a traffic log message as it appears in Traffic Monitor:

```
2020-03-19 15:22:53 Allow 10.0.1.2 40.97.85.66 https/tcp 50929 443 1-Trusted 0-External
Proxy Allow: HTTPS Request categories (HTTPS-proxy.test-00) proc_id="https-proxy"
rc="590" msg_id="2CFF-0001" proxy_act="Default-HTTPS-Client" cats="Collaboration -
Office" service="Default-WebBlocker" geo_dst="USA" src_user="testuser@Firebox-DB"
dstname="outlook.office365.com"
```

Each log message indicates when the connection for the traffic occurred, the source and destination of the traffic, as well as the disposition of the connection, and other details. Examples are from the traffic log message shown above.

Time Stamp

The log message line begins with a time stamp that includes the time and date that the log message was created. The time stamp uses the time zone and current time from the Firebox.

Example: `2020-03-19 15:22:53`

Disposition

Each log message indicates the disposition of the traffic: Allow or Deny. If the log message is for traffic that was managed by a proxy policy, the traffic may be marked Allow even though the packet body was stripped or altered by the proxy action.

Example: `Allow`

Source and Destination Addresses

The log message shows the source and destination IP addresses of the traffic. If NAT was applied to the traffic, the NAT addresses appear later in the log message.

Example: `10.0.1.2` and `40.97.85.66`

Service and Protocol

The next entries in the log message are the service and protocol that managed the traffic. If the service cannot be determined, the port number appears instead.

Example: `https/tcp`

Source and Destination Ports

The next details in the log message are the source and destination ports. The source port identifies the return traffic. The destination port determines the service used for the traffic.

Example: `50929` and `443`

Source and Destination Interfaces

The source and destination interfaces are the physical or virtual interfaces that handle the connection for this traffic.

Example: `1-Trusted` and `0-External`

Connection Action

This is the action applied to the traffic connection. For proxy actions, this indicates whether the contents of the packet are allowed, dropped, or stripped.

Example: `Proxy Allow: HTTPS Request categories`

Policy Name

This is the name of the firewall policy that handles the traffic. The number (-00) is automatically appended to policy names.

Example: `(HTTPS-proxy.test-00)`

Process

This section of the log message shows the process that handles the traffic.

Example: `proc_id="https-proxy"`

Return Code

This is the return code for the packet, which is used in reports.

Example: `rc="590"`

Message Identification Number

Each traffic log message includes a unique message identification number.

Example: `msg_id="2CFF-0001"`

Proxy Action Details

The name of the proxy action and information related to categorization by security services.

Example: `proxy_act="Default-HTTPS-Client" cats="Collaboration - Office" service="Default-WebBlocker" geo_dst="USA" src_`

User Name

For traffic from an authenticated user, the log message shows the user name.

Example: `src_user="testuser@Firebox-DB"`

Destination Domain

If the destination is a domain name, the log message shows the domain name.

Example: `dstname="outlook.office365.com"`

Audit Log Records

This table contains examples of audit log messages for required auditable events.

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
NDcPP21/FWM13/VPNGWM10: FAU_GEN.1.1	Identification of Management User Changing Settings	Identification of management user modifying management settings	SyslogTimeReceived:Jul 31 17:06:10 SyslogMessage:80D60307ECBA9<46 >Jul 31 21:12:11 WG-m4600 80D60307ECBA9 (2020-07-31T21:12:11) configd[3301]: msg_id="0101-0001" Management user admin@Firebox-DB from 172.16.16.253 modified Authentication Settings
	Start up and shutdown of audit functions	None	Start Up
			SyslogTimeReceived:May 14 14:31:54 SyslogMessage:D0200CFFD2290<46 >May 14 18:24:55 WG-t35 D0200CFFD2290 (2020-05-14T18:24:55) loggerd: Watchguard loggerd v12.6.2.B620731 (C) 1996-2020 WatchGuard Technologies Inc.
			Shutdown
			SyslogTimeReceived:May 14 17:51:24 SyslogMessage:D0200CFFD2290<46 >May 14 21:44:23 WG-t35 D0200CFFD2290 (2020-05-14T21:44:23) loggerd[2118]: msg_id="3D00-0002" Watchguard loggerd v12.6.2.B620731 stopping capturing logs

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
	Administrative login and logout	Name of user account shall be logged if individual user accounts are required for administrators	See results for FIA_UIA_EXT.1 and FTA_SSL.4
	Changes to TSF data related to configuration changes	In addition to the information that a change occurred it shall be logged what has been changed	See results for FMT_SMF.1
	Generating/import of, changing, or deleting of cryptographic keys	In addition to the action itself a unique key name or key reference shall be logged	External Certificate import
			SyslogTimeReceived:Apr 15 12:03:18 SyslogMessage:D0200CFFD2290<47>Apr 15 12:03:18 WG-t35 D0200CFFD2290 (2020-04-15T16:03:18) certd[2123]: Imported ca certificate 9F053055FD81D69FE4BA814C56DF3D4BD2_ca
			CSR Generation
			SyslogTimeReceived:May 17 23:15:47 SyslogMessage:D0200CFFD2290<46>May 17 23:15:46 WG-t35 D0200CFFD2290 (2020-05-18T03:15:46) certd[2120]: msg_id="4001-0006" Generated

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
			certificate signing request CN=WG-t35.example.com, O=Gossamer, C=US.
			CSR Import
			SyslogTimeReceived:May 17 23:18:05 SyslogMessage:D0200CFFD2290<46>May 17 23:18:04 WG-t35 D0200CFFD2290 (2020-05-18T03:18:04) certd[2120]: msg_id="4001-0006" Imported certificate signed with CSR /C=US/O=Gossamer/CN=WG-t35.example.com.
			External Certificate Deleting
			SyslogTimeReceived:Apr 15 12:00:29 SyslogMessage:D0200CFFD2290<47>Apr 15 12:00:28 WG-t35 D0200CFFD2290 (2020-04-15T16:00:28) certd[2123]: Removed ca certificate 9F053055FD81D69FE4BA814C56DF3D4BD2_ca
			Internal CA Deleting
			SyslogTimeReceived:Apr 23 12:12:03 SyslogMessage:D0200CFFD2290<47>Apr 23 16:12:03 WG-t35 D0200CFFD2290 (2020-04-23T16:12:03) certd[2119]: Removed ssl certificate selfsignedCA

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
	Resetting passwords	Name of related user account shall be logged	WebUI
			SyslogTimeReceived:Jan 21 14:23:54 SyslogMessage:80D602F9C8FCD<46>Jan 21 19:24:03 WG-m4600 80D602F9C8FCD (2020-01-21T19:24:03) configd[2444]: msg_id="0101-0001" Management user admin@Firebox-DB from 172.16.16.253 modified management user status at Firebox-DB
			Console
			SyslogTimeReceived:Jan 21 14:28:14 SyslogMessage:80D602F9C8FCD<46>Jan 21 19:28:23 WG-m4600 80D602F9C8FCD (2020-01-21T19:28:23) configd[2444]: msg_id="0101-0001" Management user admin@Firebox-DB from console modified management user status at Firebox-DB
	Too much network traffic on an interface	Indication that packets were dropped	SyslogTimeReceived:Jul 16 00:08:15 SyslogMessage:D02800066D1CF<44>Jul 16 23:21:12 WG-t40 D02800066D1CF (2020-07-16T23:21:12) kernel: [1193247.882592] net_ratelimit: 20 callbacks suppressed
NDcPP21:FAU_STG.3/LocSpace	Low storage space for audit events	None	SyslogTimeReceived:Apr 23 03:24:14 SyslogMessage:D0200CFFD2290<46>Apr 23 07:19:28 WG-t35 D0200CFFD2290 (2020-04-23T07:19:28) loggerd[2115]:

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
			msg_id="3D01-0003" Archived log file /var/log/event.log which reached max size
NDcPP21:FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session	Reason for failure	SyslogTimeReceived:Jan 21 15:17:32 SyslogMessage:80D602F9C8FCD<43>Jan 21 20:17:41 WG-m4600 80D602F9C8FCD (2020-01-21T20:17:41) wrapper[3004]: nginx: 2020/01/21 20:17:41 [crit] 3067#0: *1652 SSL_do_handshake() failed (SSL: error:1420918C:SSL routines:tls_early_post_process_client_hello:version too low) while SSL handshaking, client: 172.16.8.254, server: 0.0.0.0:443
NDcPP21:FCS_IPSEC_EXT.1	Failure to establish an IPsec SA	Reason for failure	SyslogTimeReceived:Jan 29 13:05:35 SyslogMessage:80D602F9C8FCD<43>Jan 29 13:01:02 WG-m4600 80D602F9C8FCD (2020-01-29T18:01:02) iked[2999]: (172.16.8.254<->172.16.8.14)ikeDoXfrmSAHardExpire: REKEY: failed to find ipsecPcy by name()
VPNGWM10:FCS_IPSEC_EXT.1	Session Establishment with peer	Entire packet contents of packets transmitted/received during session establishment	Refer to STFFW13:FAU_GEN.1 section of DTR for entire packet contents
NDcPP21:FCS_NTP_EXT.1			Configure

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
	Configuration of a new time server Removal of configured time server	Identity of new/removed time server	SyslogTimeReceived:Apr 23 12:07:51 SyslogMessage:D0200CFFD2290<46>Apr 23 16:02:50 WG-t35 D0200CFFD2290 (2020-04-23T16:02:50) wrapper[2255]: (ntpd) Adding ntp server 172.16.8.254.
			Remove
			SyslogTimeReceived:Apr 23 12:07:51 SyslogMessage:D0200CFFD2290<46>Apr 23 16:02:50 WG-t35 D0200CFFD2290 (2020-04-23T16:02:50) wrapper[2255]: (ntpd) Removing ntp server 0.pool.ntp.org. SyslogTimeReceived:Apr 23 12:07:51 SyslogMessage:D0200CFFD2290<46>Apr 23 16:02:50 WG-t35 D0200CFFD2290 (2020-04-23T16:02:50) wrapper[2255]: (ntpd) Removing ntp server 1.pool.ntp.org. SyslogTimeReceived:Apr 23 12:07:51 SyslogMessage:D0200CFFD2290<46>Apr 23 16:02:50 WG-t35 D0200CFFD2290 (2020-04-23T16:02:50) wrapper[2255]: (ntpd) Removing ntp server 2.pool.ntp.org.
NDcPP21:FCS_TLSS_EXT.1	Failure to establish a TLS Session	Reason for failure	SyslogTimeReceived:May 17 23:12:15 SyslogMessage:D0200CFFD2290<46>May 17 23:12:14 WG-t35 D0200CFFD2290 (2020-05-18T03:12:14) wrapper[2252]: nginx:2020/05/17 23:12:14 [info] 2328#0: *593 SSL_do_handshake() failed (SSL: error:14094416:SSL routines:ssl3_read_bytes:sslv3 alert certificate unknown:SSL alert

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
			number 46) while SSL handshaking, client: 172.16.16.253, server: 0.0.0.0:443
FWM13:FFW_RUL_EXT.1	Application of rules configured with the 'log' operation	Source and destination addresses. Source and destination ports. Transport Layer Protocol. TOE Interface. TOE interface that is unable to process packets. Identifier of rule causing packet drop.	SyslogTimeReceived:Jan 9 17:59:35 SyslogMessage:D0200CFFD2290<44 >Jan 9 22:50:28 WG-t35 D0200CFFD2290 (2020-01-09T22:50:28) firewall: msg_id="3000-0148" Deny 0-External 1-Trusted 40 tcp 20 63 172.16.8.254 10.9.1.2 32000 21 offset 5 S 0 win 8192 (FFW.1.8-10.9.1.2-Deny-00)
FWM13:FFW_RUL_EXT.2	Dynamical definition of rule and Establishment of a session	None	SyslogTimeReceived:Mar 24 16:15:56 SyslogMessage:D0200CFFD2290<44 >Mar 24 20:12:50 WG-t35 D0200CFFD2290 (2020-03-24T20:12:50) firewall: msg_id="3000-0148" Deny 0-External 0-External 76 udp 20 63 172.16.8.254 38.145.155.206 123 123 geo_dst="USA" (Default-Drop-00) SyslogTimeReceived:Mar 24 16:15:57 SyslogMessage:D0200CFFD2290<44 >Mar 24 20:12:51 WG-t35 D0200CFFD2290 (2020-03-24T20:12:51) firewall: msg_id="3000-0148" Allow 0-External 1-Trusted 60 tcp 20 64

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
			172.16.8.254 172.16.16.253 55738 56947 offset 10 S 913276677 win 29200 msg="related" (FFW.2-p1-00) SyslogTimeReceived:Mar 24 16:15:58 SyslogMessage:D0200CFFD2290<44 >Mar 24 20:12:52 WG-t35 D0200CFFD2290 (2020-03-24T20:12:52) firewall: msg_id="3000-0148" Allow 0-External 1-Trusted 60 tcp 20 64 172.16.8.254 172.16.16.253 42898 56948 offset 10 S 1735116201 win 29200 msg="related" (FFW.2-p1-00)
	Result (i.e., drop, allow) of applying a rule in the ruleset to a network packet	None	Refer to FWM13:FFW_RUL_EXT.1 audit records in this document
	Configuration of the ruleset	None	Refer to FWM13:FMT_SMF.1/FFW audit records in this document
NDcPP21:FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded	Origin of the attempt (e.g., IP address)	2T16:14:27) admd[2973]: msg_id="1100-0005" Authentication of Admin user [status@Firebox-DB] from 172.16.16.253 was rejected, password is incorrect SyslogTimeReceived:Jan 22 11:14:27 SyslogMessage:80D602F9C8FCD<44 >Jan 22 16:14:27 WG-m4600 80D602F9C8FCD (2020-01-22T16:14:27) admd[2973]: msg_id="1100-0007" User status is

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
			locked out briefly after 5 login failures
NDcPP21:FIA_UAU_EXT.2	All use of the identification and authentication mechanism	Origin of the attempt (e.g., IP address)	See results for FIA_UIA_EXT.1
NDcPP21:FIA_UIA_EXT.1	All use of the identification and authentication mechanism	Provided user identity, origin of the attempt (e.g., IP address)	WebUI successful log in
			SyslogTimeReceived:Jan 17 16:10:55 SyslogMessage:80D602F9C8FCD<46>Jan 17 21:11:02 WG-m4600 80D602F9C8FCD (2020-01-17T21:11:02) sessiond[3014]: msg_id="3E00-0002" Management user admin@Firebox-DB from 172.16.16.253 logged in
			WebUI failed log in
			gagent[3025]: msg_id="5000-0001" WebUI User admin2@Firebox-DB from 172.16.16.253 log in attempt was rejected - invalid credentials.
			Console successful log in
			SyslogTimeReceived:Apr 14 12:11:57 SyslogMessage:D0200CFFD2290<46>Apr 14 12:11:56 WG-t35 D0200CFFD2290 (2020-04-14T16:11:56) admd[2223]: msg_id="1100-0004" Authentication

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
			of Admin user [admin@Firebox-DB] from console was accepted
			Console failed log in
			SyslogTimeReceived:Apr 14 12:13:14 SyslogMessage:D0200CFFD2290<44>Apr 14 12:13:13 WG-t35 D0200CFFD2290 (2020-04-14T16:13:13) admd[2223]: msg_id="1100-0005" Authentication of Admin user [admin@Firebox-DB] from console was rejected, password is incorrect
NDcPP21:FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	Reason for failure of certificate validation	Multiple Different Failure Examples
			Non-matching RID: SyslogTimeReceived:Apr 6 12:41:46 SyslogMessage:D0200CFFD2290<43>Apr 6 12:42:01 WG-t35 D0200CFFD2290 (2020-04-06T16:42:01) iked[2247]: msg_id="021A-000B" (172.16.8.11<->172.16.8.254)IKEv2 IKE_AUTH exchange from 172.16.8.11:500 to 172.16.8.254:500 failed. Gateway-Endpoint='Syslog-IPsec'. Reason=Received ID did not match the configured remote gateway endpoint ID. Expired Cert: SyslogTimeReceived:Aug 5 23:31:59 SyslogMessage:80D60307ECBA9<43>Aug 6 03:34:20 WG-m4600 80D60307ECBA9 (2020-08-06T03:34:20) iked[3664]: (172.16.8.14<-

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
			>172.16.8.254)CMgrValidateCert_GetPubKey: Cannot validate the peer certificate(err=-981, reason=<6_981>:certificate expired). Check CA certificate Corrupt Cert: SyslogTimeReceived:Aug 5 23:57:47 SyslogMessage:80D60307ECBA9<43>Aug 6 04:00:08 WG-m4600 80D60307ECBA9 (2020-08-06T04:00:08) iked[3664]: (172.16.8.14<->172.16.8.254)CMgrValidateCert_GetPubKey: Cannot validate the peer certificate(err=-982, reason=<6_982>:certificate validation fail). Check CA certificate Revoked Cert: SyslogTimeReceived:Aug 6 11:50:19 SyslogMessage:80D60307ECBA9<46>Aug 6 11:50:19 WG-m4600 80D60307ECBA9 (2020-08-06T15:50:19) iked[3664]: Check CERT: Subject: [c=US,st=MD,l=Catonsville,o=GSS,cn=tl1-16x.example.com,email=server-revoked-ecdsa@gossamersec.com] SyslogTimeReceived:Aug 6 11:50:19 SyslogMessage:80D60307ECBA9<47>Aug 6 11:50:19 WG-m4600 80D60307ECBA9 (2020-08-06T15:50:19) iked[3664]: Ocsp result is 1 SyslogTimeReceived:Aug 6 11:50:19 SyslogMessage:80D60307ECBA9<47>Aug 6 11:50:19 WG-m4600 80D60307ECBA9 (2020-08-06T15:50:19) iked[3664]: rs_crypto_validate_cert_ocsp: OCSP check failed!

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
			Missing OCSP Signing EKU: SyslogTimeReceived:Aug 6 11:55:54 SyslogMessage:80D60307ECBA9<46>Aug 6 11:55:54 WG-m4600 80D60307ECBA9 (2020-08-06T15:55:54) iked[3664]: Check CERT: Subject: [c=US,st=MD,l=Catonsville,o=GSS,cn=subsubca-ecdsa,email=subsubca-ecdsa@gossamersec.com] SyslogTimeReceived:Aug 6 11:55:54 SyslogMessage:80D60307ECBA9<47>Aug 6 11:55:54 WG-m4600 80D60307ECBA9 (2020-08-06T15:55:54) iked[3664]: Ocsp result is -1 SyslogTimeReceived:Aug 6 11:55:54 SyslogMessage:80D60307ECBA9<47>Aug 6 11:55:54 WG-m4600 80D60307ECBA9 (2020-08-06T15:55:54) iked[3664]: rs_crypto_validate_cert_ocsp: OCSP is not cached or expired
	Any addition, replacement or removal of trust anchors in the TOE's trust store	Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store	Addition: SyslogTimeReceived:Apr 15 12:03:18 SyslogMessage:D0200CFFD2290<47>Apr 15 12:03:18 WG-t35 D0200CFFD2290 (2020-04-15T16:03:18) certd[2123]: Imported ca certificate 9F053055FD81D69FE4BA814C56DF3D4BD2_ca Removal: SyslogTimeReceived:Apr 15 12:00:29 SyslogMessage:D0200CFFD2290<47>Apr 15 12:00:28 WG-t35 D0200CFFD2290 (2020-04-15T16:00:28) certd[2123]: Removed ca certificate

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
			9F053055FD81D69FE4BA814C56DF3D4BD2_ca
NDcPP21:FMT_MOF.1/Functions	Modification of the behavior of the transmission of audit data to an external IT entity	None	SyslogTimeReceived:Apr 15 13:40:34 SyslogMessage:D0200CFFD2290<46>Apr 15 13:40:34 WG-t35 D0200CFFD2290 (2020-04-15T17:40:34) loggerd: Watchguard loggerd v12.6.2.B617755 (C) 1996-2020 WatchGuard Technologies Inc. SyslogTimeReceived:Apr 15 13:40:34 SyslogMessage:D0200CFFD2290<46>Apr 15 13:40:34 WG-t35 D0200CFFD2290 (2020-04-15T17:40:34) configd[2117]: msg_id="0101-0001" Management user admin@Firebox-DB from 172.16.16.253 modified Logging SyslogTimeReceived:Apr 15 13:36:25 SyslogMessage:D0200CFFD2290<46>Apr 15 13:36:24 WG-t35 D0200CFFD2290 (2020-04-15T17:36:24) loggerd[2119]: msg_id="3D01-0003" Configured syslog server: 172.16.8.244
	Modification of the behavior of the handling of audit data	None	SyslogTimeReceived:Apr 15 13:46:21 SyslogMessage:D0200CFFD2290<46>Apr 15 13:46:21 WG-t35 D0200CFFD2290 (2020-04-15T17:46:21) configd[2117]: msg_id="0101-0001" Management user admin@Firebox-DB from 172.16.16.253 modified Diagnostic Log Level
	Modification of the behavior of the audit	None	N/A - can't be configured

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
	functionality when Local Audit Storage Space is full		
NDcPP21:FMT_MOF.1/Manual Update	Any attempt to initiate a manual update	None	See results for FPT_TUD_EXT.1
NDcPP21:FMT_MOF.1/Services	Starting and stopping of services	None	SyslogTimeReceived:Apr 15 13:56:54 SyslogMessage:D0200CFFD2290<43 >Apr 15 13:56:53 WG-t35 D0200CFFD2290 (2020-04-15T17:56:53) iked[2735]: Got System Shutdown Message: setting iked_restarted flag as true …
NDcPP21:FMT_MTD.1/CryptoKeys	Management of cryptographic keys	None	See results for FMT_SMF.1
NDcPP21:FMT_SMF.1	Ability to administer the TOE locally and remotely	In addition to the information that a change occurred it shall be logged what has been changed	See results for FIA_UIA_EXT.1
	Ability to configure the access banner		WebUI
			SyslogTimeReceived:May 17 22:48:23 SyslogMessage:D0200CFFD2290<46 >May 17 22:48:21 WG-t35 D0200CFFD2290 (2020-05-18T02:48:21) admd[2220]:

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
			msg_id="1100-0015" Logon Disclaimer was updated, the disclaimer message was changed from "GSS Test Banner 1" to "GSS Test Banner 2"
			Console
			SyslogTimeReceived:May 17 22:52:49 SyslogMessage:D0200CFFD2290<46>May 17 22:52:47 WG-t35 D0200CFFD2290 (2020-05-18T02:52:47) admd[2220]: msg_id="1100-0015" Logon Disclaimer was updated, the disclaimer message was changed from "GSS Test Banner 2" to "GSS Test Banner CLI"
	Ability to configure the session inactivity time before session termination or locking		WebUI
			SyslogTimeReceived:Apr 23 12:48:52 SyslogMessage:D0200CFFD2290<46>Apr 23 16:48:51 WG-t35 D0200CFFD2290 (2020-04-23T16:48:51) sessiond[2265]: msg_id="3E00-0005" Updated the value of the management session idle timeout from 900 seconds to 1200 seconds.
			Console
			SyslogTimeReceived:Apr 23 12:51:05 SyslogMessage:D0200CFFD2290<46>Apr 23 16:51:05 WG-t35 D0200CFFD2290 (2020-04-

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
			23T16:51:05) sessiond[2265]: msg_id="3E00-0005" Updated the value of the management session idle timeout from 1200 seconds to 1500 seconds.
	Ability to update the TOE		See results for FPT_TUD_EXT.1
	Ability to configure the authentication failure parameters for FIA_AFL.1		SyslogTimeReceived:Apr 23 12:57:24 SyslogMessage:D0200CFFD2290<47>Apr 23 16:57:24 WG-t35 D0200CFFD2290 (2020-04-23T16:57:24) admd[2221]: read lockout option: enabled=1, failures=5, lockouts=5, duration=5 SyslogTimeReceived:Apr 23 12:57:24 SyslogMessage:D0200CFFD2290<47>Apr 23 16:57:24 WG-t35 D0200CFFD2290 (2020-04-23T16:57:24) admd[2221]: wgadmHandleCfgapi(): lockout configuration for mgmt users is changed
	Ability to configure firewall rules		See results for FWM13:FMT_SMF.1/FFW
	Ability to configure the cryptographic functionality		SyslogTimeReceived:May 15 11:53:12 SyslogMessage:D0200CFFD2290<47>May 15 11:53:12 WG-t35 D0200CFFD2290 (2020-05-15T15:53:12) iked[2242]: ike transform[#0]: dhgroup=19, encrypt=AES_CBC(256 bit),

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
			hash=SHA2_256, lifetime=86400 seconds
	Ability to configure the lifetime for IPsec SAs		SyslogTimeReceived:May 15 11:53:12 SyslogMessage:D0200CFFD2290<47 >May 15 11:53:12 WG-t35 D0200CFFD2290 (2020-05-15T15:53:12) iked[2242]: ike transform[#0]: dhgroup=19, encrypt=AES_CBC(256 bit), hash=SHA2_256, lifetime=86400 seconds
	Ability to import X.509v3 certificates		SyslogTimeReceived:Apr 15 12:03:18 SyslogMessage:D0200CFFD2290<47 >Apr 15 12:03:18 WG-t35 D0200CFFD2290 (2020-04-15T16:03:18) certd[2123]: Imported ca certificate 9F053055FD81D69FE4BA814C56DF 3D4BD2_ca
	Ability to configure audit behavior		WebUI
			SyslogTimeReceived:Apr 23 12:59:56 SyslogMessage:D0200CFFD2290<46 >Apr 23 16:59:56 WG-t35 D0200CFFD2290 (2020-04-23T16:59:56) configd[2113]: msg_id="0101-0001" Management user admin@Firebox-DB from 172.16.16.253 modified Diagnostic Log Level
			Console

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
			SyslogTimeReceived:Apr 23 13:04:17 SyslogMessage:D0200CFFD2290<46 >Apr 23 17:04:17 WG-t35 D0200CFFD2290 (2020-04-23T17:04:17) configd[2113]: msg_id="0101-0001" Management user admin@Firebox-DB from console modified Diagnostic Log Level
	Ability to set the time which is used for time-stamps		See results for FPT_STM_EXT.1
	Ability to configure the reference identifier for the peer		SyslogTimeReceived:May 15 11:57:48 SyslogMessage:D0200CFFD2290<47 >May 15 11:57:48 WG-t35 D0200CFFD2290 (2020-05-15T15:57:48) iked[2242]: remote gateway ip: 172.16.8.254, remote gateway id: type=IP_ADDR,value=172.16.8.254
	Configure Minimum Password length		SyslogTimeReceived:Apr 30 16:11:38 SyslogMessage:D0200CFFD2290<47 >Apr 30 16:11:38 WG-t35 D0200CFFD2290 (2020-04-30T20:11:38) admd[2223]: firebox-db minimum passphrase length updated from 10 to 8
	Enable 'CSfC Mode'		Enable: SyslogTimeReceived:Apr 23 18:00:45 SyslogMessage:D0200CFFD2290<46 >Apr 23 18:00:45 WG-t35 D0200CFFD2290 (2020-04-

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
			23T22:00:45) systemd: Enable CSfC mode successful Disable: SyslogTimeReceived:Apr 23 17:58:35 SyslogMessage:D0200CFFD2290<46 >Apr 23 17:58:34 WG-t35 D0200CFFD2290 (2020-04-23T21:58:34) systemd: Disable CSfC mode successful
FWM13:FMT_SMF.1/FFW	Creation of Firewall Rules	None	SyslogTimeReceived:Jan 14 10:59:35 SyslogMessage:80D602F9C8FCD<46 >Jan 14 15:47:12 WG-m4600 80D602F9C8FCD (2020-01-14T15:47:12) configd[2445]: msg_id="0101-0001" Management user admin@Firebox-DB from 172.16.16.253 added Policy Allow-All-00
	Deletion of Firewall Rules	None	SyslogTimeReceived:Jan 22 14:19:53 SyslogMessage:80D602F9C8FCD<46 >Jan 22 19:19:53 WG-m4600 80D602F9C8FCD (2020-01-22T19:19:53) configd[2444]: msg_id="0101-0001" Management user admin@Firebox-DB from 172.16.16.253 deleted Policy Allow-All-00
	Modification of Firewall Rules	None	SyslogTimeReceived:Jan 22 14:14:42 SyslogMessage:80D602F9C8FCD<46 >Jan 22 19:14:42 WG-m4600 80D602F9C8FCD (2020-01-22T19:14:42) configd[2444]: msg_id="0101-0001" Management user admin@Firebox-DB from

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
			172.16.16.253 modified Alias Allow-All.1.to
	Modification of Firewall Rule order	None	SyslogTimeReceived:Apr 29 11:26:21 SyslogMessage:D0200CFFD2290<46>Apr 29 11:26:20 WG-t35 D0200CFFD2290 (2020-04-29T15:26:20) configd[2114]: msg_id="0105-0001" Moved Allow-Management-Traffic policy from position 1 to 70
VPNGW10:FPF_RUL_EXT.1	Application of rules configured with the 'log' operation	Source and destination addresses Source and destination ports Transport Layer Protocol	See results for STFFW13:FFW_RUL_EXT.1
NDcPP21:FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).	Manual change
			SyslogTimeReceived:Jul 21 12:20:58 SyslogMessage:D02800066D1CF<46>Jul 21 16:20:00 WG-t40 D02800066D1CF (2020-07-21T16:20:00) systemd[2878]: msg_id="5501-0008" System time changed from 2020-07-21 12:20:58 to 2020-07-21 12:20:00
			Automated change
			08:06:26) ntpd[3841]: System time changed to Fri May 15 04:06:26 EDT

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
	FPT_STM_EXT.1)		2020 (offset -44570.239208s) from Fri May 15 16:29:16 EDT 2020
NDcPP21:FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None	Load/Initialize Update
			SyslogTimeReceived:Apr 14 12:53:33 SyslogMessage:D0200CFFD2290<47>Apr 14 12:53:33 WG-t35 D0200CFFD2290 (2020-04-14T16:53:33) systemd: current Platform[baring] Model[T35] Serial[D0200CFFD2290] Version[12.6.2] Build[617755]
			Update Success
			SyslogTimeReceived:Jan 22 14:39:03 SyslogMessage:80D602F9C8FCD<46>Jan 22 14:39:03 WG-m4600 80D602F9C8FCD (2020-01-22T19:39:03) systemd[4334]: msg_id="5501-0006" System upgrade to 12.6 successful, system needs to reboot
			Failure
			SyslogTimeReceived:Apr 23 18:07:12 SyslogMessage:D0200CFFD2290<44>Apr 23 18:07:11 WG-t35 D0200CFFD2290 (2020-04-23T22:07:11) systemd[2616]: msg_id="5501-001A" System upgrade failed: internal reason
NDcPP21:FTA_SSL.3	The termination	None	SyslogTimeReceived:Apr 23 13:18:35 SyslogMessage:D0200CFFD2290<46

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
	of a remote session by the session locking mechanism		>Apr 23 17:18:35 WG-t35 D0200CFFD2290 (2020-04-23T17:18:35) sessiond[2265]: Session idle Timeout has occured 14 SyslogTimeReceived:Apr 23 13:18:35 SyslogMessage:D0200CFFD2290<46 >Apr 23 17:18:35 WG-t35 D0200CFFD2290 (2020-04-23T17:18:35) sessiond[2265]: msg_id="3E00-0004" Management user admin@Firebox-DB from 172.16.16.253 logged out
NDcPP21:FTA_SSL.4	The termination of an interactive session	None	WebUI
			SyslogTimeReceived:Jan 22 14:31:22 SyslogMessage:80D602F9C8FCD<46 >Jan 22 14:31:22 WG-m4600 80D602F9C8FCD (2020-01-22T19:31:22) sessiond[3015]: msg_id="3E00-0004" Management user admin@Firebox-DB from 172.16.16.253 logged out
			Console
			SyslogTimeReceived:Jan 22 14:38:01 SyslogMessage:80D602F9C8FCD<46 >Jan 22 14:38:01 WG-m4600 80D602F9C8FCD (2020-01-22T19:38:01) sessiond[3015]: msg_id="3E00-0004" Management user admin from console logged out
NDcPP21:FTA_SSL_EXT.1	The termination of a local session by	None	Session Timeout: SyslogTimeReceived:May 15 13:34:24 SyslogMessage:D0200CFFD2290<46

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
	the session locking mechanism		>May 15 13:34:24 WG-t35 D0200CFFD2290 (2020-05-15T17:34:24) sessiond[2260]: msg_id="3E00-0004" Management user admin@Firebox-DB from 172.16.16.253 logged out - session timeout Idle Timeout: SyslogTimeReceived:May 15 13:49:24 SyslogMessage:D0200CFFD2290<46 >May 15 13:49:24 WG-t35 D0200CFFD2290 (2020-05-15T17:49:24) sessiond[2260]: msg_id="3E00-0004" Management user admin@Firebox-DB from 172.16.16.253 logged out - idle timeout
NDcPP21:FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions	Identification of the initiator and target of failed trusted channels establishment attempt	Initiation
			SyslogTimeReceived:Jan 27 15:10:43 SyslogMessage:80D602F9C8FCD<46 >Jan 27 15:07:29 WG-m4600 80D602F9C8FCD (2020-01-27T20:07:29) iked[2999]: msg_id="0207-0001" (172.16.8.14<->172.16.8.254)'Syslog-IPsec-Tunnel' BOVPN IPSec tunnel is established. local:172.16.8.14 remote:172.16.8.254 in-SA:0xd2a60685 out-SA:0xc2fe94ed role:initiator
			Termination
			SyslogTimeReceived:Apr 23 13:35:38 SyslogMessage:D0200CFFD2290<46

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
			>Apr 23 13:35:37 WG-t35 D0200CFFD2290 (2020-04-23T17:35:37) iked[2247]: (172.16.8.11<->172.16.8.254)Process DELETE payload: found IsakmpSA to delete (peer 172.16.8.254:500) SyslogTimeReceived:Apr 23 13:35:38 SyslogMessage:D0200CFFD2290<47>Apr 23 13:35:37 WG-t35 D0200CFFD2290 (2020-04-23T17:35:37) iked[2247]: (172.16.8.11<->172.16.8.254)IkeInDeleteProcess: delete Isakmp SA, reason=IKE_P1SA_REMOTE_DELETE
			Failure
			SyslogTimeReceived:Jan 27 15:04:56 SyslogMessage:80D602F9C8FCD<43>Jan 27 15:01:43 WG-m4600 80D602F9C8FCD (2020-01-27T20:01:43) iked[2999]: msg_id="021A-0015" (172.16.8.14<->172.16.8.254)IKEv2 IKE_SA_INIT exchange from 172.16.8.14:500 to 172.16.8.254:500 failed. Gateway-Endpoint='Syslog-IPsec'. Reason=Received N(NO_PROPOSAL_CHOSEN) message.
NDcPP21:FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path.	None	Initiation-TLS
			SyslogTimeReceived:May 17 23:12:15 SyslogMessage:D0200CFFD2290<46>May 17 23:12:14 WG-t35

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
	Failures of the trusted path functions		D0200CFFD2290 (2020-05-18T03:12:14) wrapper[2252]: nginx:2020/05/17 23:12:14 [info] 2328#0: *594 SSL connection established while SSL handshaking, client: 172.16.16.253, server: 0.0.0.0:443
			Termination-TLS
			SyslogTimeReceived:May 17 23:45:42 SyslogMessage:D0200CFFD2290<46>May 17 23:45:41 WG-t35 D0200CFFD2290 (2020-05-18T03:45:41) wrapper[2252]: nginx:2020/05/17 23:45:41 [info] 2328#0: *1204 client closed connection while waiting for request, client: 172.16.8.254, server: 0.0.0.0:443
			Failure-TLS
			SyslogTimeReceived:May 17 23:12:15 SyslogMessage:D0200CFFD2290<46>May 17 23:12:14 WG-t35 D0200CFFD2290 (2020-05-18T03:12:14) wrapper[2252]: nginx:2020/05/17 23:12:14 [info] 2328#0: *593 SSL_do_handshake() failed (SSL: error:14094416:SSL routines:ssl3_read_bytes:sslv3 alert certificate unknown:SSL alert number 46) while SSL handshaking, client: 172.16.16.253, server: 0.0.0.0:443

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
			Initiation-IPsec
			SyslogTimeReceived:Jan 27 15:10:43 SyslogMessage:80D602F9C8FCD<46>Jan 27 15:07:29 WG-m4600 80D602F9C8FCD (2020-01-27T20:07:29) iked[2999]: msg_id="0207-0001" (172.16.8.14<->172.16.8.254)'Syslog-IPsec-Tunnel' BOVPN IPSec tunnel is established. local:172.16.8.14 remote:172.16.8.254 in-SA:0xd2a60685 out-SA:0xc2fe94ed role:initiator
			Termination-IPsec
			SyslogTimeReceived:Apr 23 13:35:38 SyslogMessage:D0200CFFD2290<46>Apr 23 13:35:37 WG-t35 D0200CFFD2290 (2020-04-23T17:35:37) iked[2247]: (172.16.8.11<->172.16.8.254)Process DELETE payload: found IsakmpSA to delete (peer 172.16.8.254:500) SyslogTimeReceived:Apr 23 13:35:38 SyslogMessage:D0200CFFD2290<47>Apr 23 13:35:37 WG-t35 D0200CFFD2290 (2020-04-23T17:35:37) iked[2247]: (172.16.8.11<->172.16.8.254)IkeInDeleteProcess: delete Isakmp SA, reason=IKE_P1SA_REMOTE_DELETE
			Failure-IPsec

PP/Module:SFR	Auditable Event	Additional Audit Record Contents	Audit Record
			SyslogTimeReceived:Jan 27 15:04:56 SyslogMessage:80D602F9C8FCD<43 >Jan 27 15:01:43 WG-m4600 80D602F9C8FCD (2020-01-27T20:01:43) iked[2999]: msg_id="021A-0015" (172.16.8.14<->172.16.8.254)IKEv2 IKE_SA_INIT exchange from 172.16.8.14:500 to 172.16.8.254:500 failed. Gateway-Endpoint='Syslog-IPsec'. Reason=Received N(NO_PROPOSAL_CHOSEN) message.

System Time

Network Time Protocol (NTP) synchronizes computer clock times across a network. Your Firebox can use NTP to automatically get the correct time from NTP servers on the Internet to set the system clock.

> ⓘ It is important that the time on your device is set correctly. The Firebox uses the time from its system clock for time stamps in log messages.

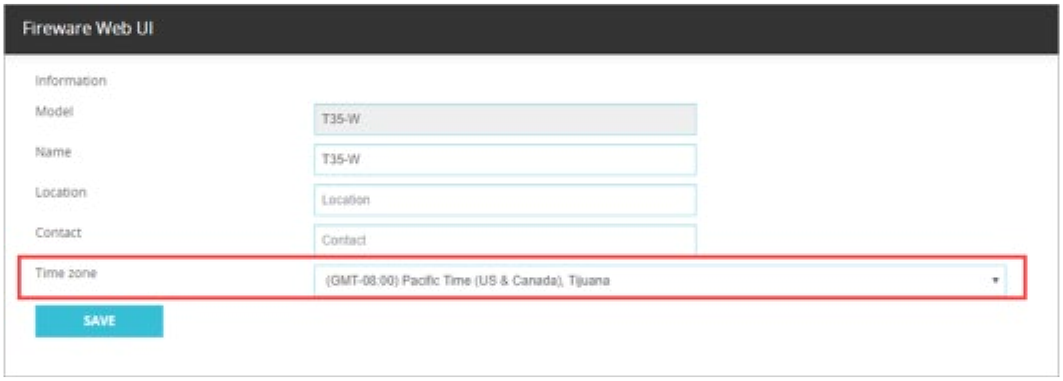
When you run the Web Setup Wizard for initial device configuration, you select a time zone. The Firebox uses NTP and the selected time zone to synchronize the system time. You can update the time zone and default NTP servers.

> ⓘ By default, the Firebox does not accept broadcast or multicast NTP packets. There is no way to enable this behavior on the Firebox.

Change the Time Zone

To change the time zone, from Fireware Web UI:

1. Select **System > Information**.
   The Information page appears.



Information

Model	T35-W
Name	T35-W
Location	Location
Contact	Contact
Time zone	(GMT-08:00) Pacific Time (US & Canada), Tijuana

2. From the **Time zone** drop-down list, select the time zone for the physical location of the Firebox. The time zone setting controls the date and time that appear in audit log messages.

Configure NTP Servers

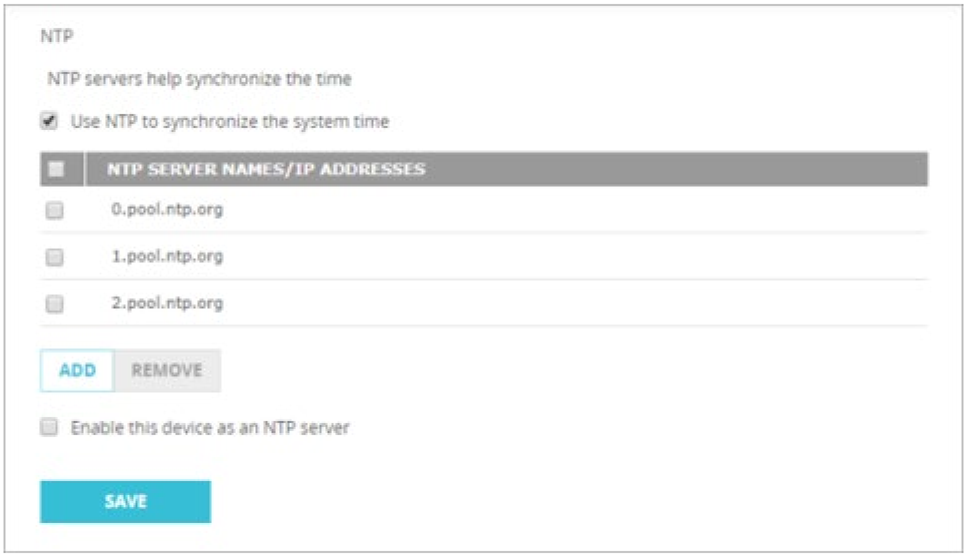
The Firebox can connect to up to three NTP servers to synchronize system time. By default, the Firebox connects to these NTP servers:

0.pool.ntp.org
1.pool.ntp.org
2.pool.ntp.org

> ⓘ Connections to the NTP servers are not encrypted. To protect the connection, route the connection to the NTP server through an IPSec VPN tunnel. For information about how to set up a VPN tunnel, see *IPSec VPN*.

To change NTP settings, from Fireware Web UI:

1. Select **System > NTP**.
   The NTP Setting page appears



NTP

NTP servers help synchronize the time

☑ Use NTP to synchronize the system time

□	NTP SERVER NAMES/IP ADDRESSES
□	0.pool.ntp.org
□	1.pool.ntp.org
□	2.pool.ntp.org

□ Enable this device as an NTP server

2. To remove an NTP server, select the server entry and click **Remove**.
3. To add an NTP server, click **Add**.
4. From the **Choose Type** drop-down list, select **Host IP** or **Host Name**.
5. Type the IP address or host name of the NTP server. Click **OK**.
6. Click **Save**.

If the system time differs by more than 1000 seconds from the time received from the NTP server, the Firebox does not update the system time. If needed, you can manually update the system clock, as described in the next section.

Manually Update the System Clock

For information about how to connect to the Firebox console port, see *Initial Configuration*.

To manually update the system clock:

1. Open a terminal connection to the Firebox console.
2. Type the user name **admin**, or the user name of another administrative user.
3. Type the passphrase for the user account. Press **Enter**.
4. To see the current time, type the command: `show clock`.
5. To set the system time, type the command `clock time hh:mm:ss`.
6. To set the system date, type the command `clock date mm/dd/yyyy`.
7. To log out, type **exit**.

Firewall Policies and Security Services

Firewall policies define the rules for what connections and content the Firebox allows and denies. When you add a policy to your Firebox configuration file, you add a set of rules that tell the Firebox to allow or deny traffic based upon factors such as source and destination of the packet or the TCP/IP port or protocol used for the packet.

In each firewall policy, you define rules to:

- Set allowed traffic sources and destinations.
- Enable security services.
- Configure filter rules in proxy actions (for proxy policies).
- Configure properties such as Traffic Management, NAT, and log settings.

Default Firewall Policies and Services

Factory-Default Policies

Before you run the Web Setup Wizard, the Firebox has a small set of default policies that allow:

- Management connections to the Firebox from trusted and optional networks.
- TCP and UDP traffic from trusted and optional networks to the external network.
- Ping traffic from trusted and optional networks to any destination.

After you start a Firebox with factory-default settings, you must connect to the Firebox on interface 1 or interface 32 and run the Web Setup Wizard to create a basic configuration.

Web Setup Wizard Default Policies and Services

The Web Setup Wizard configures these default policies:

- FTP-proxy, with the *Default-FTP-Client* proxy action
- HTTP-proxy, with the *Default-HTTP-Client* proxy action
- HTTPS-proxy, with the *Default-HTTPS-Client* proxy action
- WatchGuard Certificate Portal
- WatchGuard Web UI
- Ping
- DNS
- WatchGuard
- Outgoing

With these default policies, the Firebox:

- Does not allow inbound connections from the external network to the trusted or optional networks, or to the Firebox.
- Allows management connections to the Firebox from the trusted and optional networks only.
- Inspects outgoing FTP, HTTP, and HTTPS traffic, with recommended proxy action settings.
- Uses Application Control, WebBlocker, Gateway AntiVirus, Intrusion Prevention, Application Control, Reputation Enabled Defense, Botnet Detection, Geolocation, and APT Blocker security services to protect the trusted and optional networks.
- Allows outgoing FTP, Ping, DNS, TCP, and UDP connections from the trusted and optional networks.

The Web Setup Wizard creates three proxy actions that are used by the default proxy policies.

Default-FTP-Client

- Used by the FTP-proxy
- Based on FTP-Client.Standard
- Gateway AntiVirus is enabled
- Logging for reports is enabled

Default-HTTP-Client

- Used by the HTTP-proxy
- Based on the HTTP-Client.Standard proxy action
- WebBlocker, Gateway AntiVirus, Reputation Enabled Defense, and APT Blocker are enabled
- Logging for reports is enabled

Default-HTTPS-Client

- Used by the HTTPS-proxy
- Based on the HTTPS-Client.Standard proxy action
- WebBlocker is enabled

- Content inspection uses the Default-HTTP-Client proxy action, but content inspection is not enabled
- Logging for reports is enabled

You can edit these proxy actions to suit the needs of your network, and you can use these proxy actions for other proxy policies you add.

Default Security Services Configuration

The setup wizards enable most licensed security services by default with recommended settings if the feature key includes those features. The Botnet Detection and Geolocation features are enabled if the Firebox has a feature key for Reputation Enabled Defense.

> ⚠ The setup wizards configure subscription services only if the Firebox has a feature key that includes those services. If there is no feature key, or if there are no licensed subscription services in the feature key, the wizard configures the policies without subscription services enabled.

Intrusion Prevention Service

Enabled for all policies except *WatchGuard*, *WatchGuard Certificate Portal*, and *WatchGuard Web UI*.

Scan mode — Full Scan

Actions by threat level:

- Critical — Drop, Alarm, Log
- High — Drop, Alarm, Log
- Medium — Drop, Log
- Low — Drop, Log
- Information — Allow

Application Control

Enabled for all policies except *WatchGuard*, *WatchGuard Certificate Portal*, and *WatchGuard Web UI*.

Global Application Control actions:

- Drop — Application — Crypto Admin
- Drop — Application Category — Bypass Proxies and Tunnels

Reputation Enabled Defense

Enabled for the *HTTP-proxy* policy.

Action — Immediately block URLs that have a bad reputation, Log this action.

Botnet Detection

Enabled to block traffic from suspected botnet sites.

Geolocation

Enabled to identify the geographic location of connections through the Firebox.

WebBlocker

Enabled for the *HTTP-proxy* and *HTTPS-proxy* policies.

Settings for the *Default-WebBlocker* action:

- Categories — The Default WebBlocker action blocks content categories you select in the setup wizard.
- Server Timeout — By default, the server timeout setting is configured to deny access if the Firebox cannot connect to the WebBlocker Server.
- License Bypass — By default, the license bypass setting is configured to deny access when the WebBlocker license expires.

Gateway AntiVirus

Enabled for the *HTTP-proxy* and *FTP-proxy* policies.

- FTP — AV Scan all content (uploads and downloads).
- HTTP — AV Scan all content (content types and body content types).
- Default-HTTP-Client proxy action, the action for the **Windows EXE/DLL** Body Content Rule is also set to **AV Scan**.

Action — Drop and Alarm when a virus is found or a scan error occurs.

APT Blocker

Enabled for the *FTP-proxy* and *HTTP-proxy* policies.

Actions by threat level:

- High — Drop, Alarm, Log
- Medium — Drop, Alarm, Log
- Low — Drop, Alarm, Log
- Clean — Allow

Default Threat Protection

Default threat protection options for the Firebox can stop threats such as SYN flood attacks, spoofing attacks, and port or address space probes. With default threat protection, a firewall examines the source and destination of each packet it receives. It looks at the IP address and port number and monitors the packets to look for patterns that show your network is at risk. If a risk exists, you can configure the Firebox to automatically block a possible attack.

Default Threat Protection includes these settings:

- Default Packet Handling — Blocks dangerous activities, spoofing, and denial of service attacks
- Blocked Sites — Denies traffic to or from blocked sites
- Blocked Ports — Denies inbound traffic from external network to blocked ports

Default Packet Handling

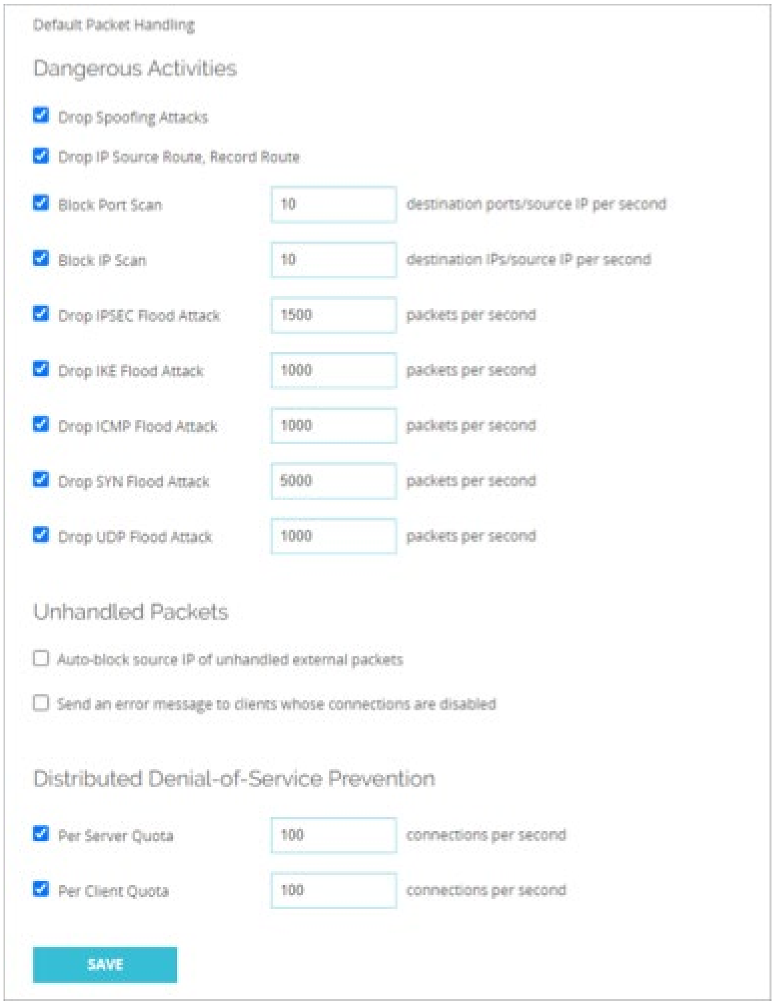
When the Firebox receives a packet, it examines the source and destination for the packet. It looks at the IP address and the port number. The device also monitors the packets to look for patterns that can show your network is at risk. This process is called *default packet handling*.

By default, the Firebox is configured to block all dangerous activities and denial of service attacks.

Configure Default Packet Handling Settings

To configure Default Packet Handling options, from Fireware Web UI:

1. Select **Firewall > Default Packet Handling**.



Default Packet Handling

Dangerous Activities

☑ Drop Spoofing Attacks

☑ Drop IP Source Route, Record Route

☑ Block Port Scan 10 destination ports/source IP per second

☑ Block IP Scan 10 destination IPs/source IP per second

☑ Drop IPSEC Flood Attack 1500 packets per second

☑ Drop IKE Flood Attack 1000 packets per second

☑ Drop ICMP Flood Attack 1000 packets per second

☑ Drop SYN Flood Attack 5000 packets per second

☑ Drop UDP Flood Attack 1000 packets per second

Unhandled Packets

☐ Auto-block source IP of unhandled external packets

☐ Send an error message to clients whose connections are disabled

Distributed Denial-of-Service Prevention

☑ Per Server Quota 100 connections per second

☑ Per Client Quota 100 connections per second

Firebox Default Packet Handling settings

2. Select the check boxes for the traffic patterns you want the Firebox to drop.
3. To change the traffic threshold for a packet type, edit the value in the adjacent text box.
4. Click **Save**.

ⓘ When **Drop Spoofing Attacks** is enabled, the Firebox verifies the source IP address of a packet is from a network on the specified interface. This option is enabled by default. In CSfC mode, this option must be enabled for a compliant configuration.

About Flood Attack Thresholds

To prevent flood attacks, in the **Default Packet Handling** page, you can specify thresholds for the allowed number of packets per second for different types of traffic. When the number of packets received on an interface exceeds the specified threshold, the device starts to drop traffic of that type on the interface.

For example, with the **Drop SYN Flood Attack** threshold at the default value of 5000, the device starts to drop SYN packets from an interface that receives more than 5000 SYN packets per second. The device does not drop other types of traffic or traffic received on other interfaces.

ⓘ The Firebox generates up to three log messages a minute when the rate of packets received on an interface is above a specified threshold.

The Firebox does not drop every packet received over the specified threshold immediately. This table shows whether the device drops a packet, based on the rate of packets of that type received on an interface:

Rate of packets received	Packets dropped
Below the threshold	No packets
Between the threshold and twice the threshold	25% of packets of that type
More than twice the threshold	All packets of that type

When the rate of packets received on the interface falls back below the threshold, the device no longer drops packets of that type.

Packets Dropped by Default

By default, the Firebox drops these packets:

1. Packets which are invalid fragments.
2. Fragments that cannot be completely re-assembled.
3. Packets where the source address is equal to the address of the network interface where the network packet was received.
4. Packets where the source address does not belong to the networks associated with the network interface where the network packet was received.
5. Packets where the source address is defined as being on a broadcast network.
6. Packets where the source address is defined as being on a multicast network.
7. Packets where the source address is defined as being a loopback address.
8. Packets where the source or destination address of the network packet is a link-local address.
9. Packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified.

In addition, you must add entries to the Blocked Sites list so the Firebox drops these packets:

1. Packets where the source or destination address of the network packet is defined as being an address 'reserved for future use' as specified in RFC 5735 for IPv4.
2. Packets where the source or destination address of the network packet is defined as an 'unspecified address' or an address 'reserved for future definition and use' as specified in RFC 3513 for IPv6.

For the steps to add the required blocked sites, see Add Blocked Sites.

Blocked Sites

A blocked site is an IP address that cannot make a connection through the Firebox. You configure Firebox policies and services with the Block action when you want the Firebox to automatically block the source of suspicious traffic. You can also permanently block all connections to or from a site. By default, the Firebox sends a log message each time a blocked site tries to connect to your network. From the log file, you can see the services that the sources use to launch attacks.

You can define two different types of blocked IP addresses: permanent and auto-blocked. You can also configure blocked site exceptions.

Auto-Blocked Sites

> If traffic matches a firewall policy or service configured with the Block action, the Firebox automatically adds the source of the traffic to the temporary blocked sites list. You can also manually add and remove sites from this list.
>
> In Fireware Web UI, the **System Status > Blocked Sites** page shows a list of IP addresses currently on the Blocked Sites list, the reason each site was added to the list, and the expiration time (when the site is removed from the Blocked Sites list).

Permanently Blocked Sites

You can manually add a site that you want to block permanently. You can also add blocked site exceptions for sites you never want the Firebox to block.

In Fireware Web UI, the **Firewall > Blocked Sites** page is where you can configure IP addresses for permanently blocked sites.

Blocked Site Exceptions

From the **Firewall > Blocked Sites** page you can also define blocked site exceptions. By default, this list includes exceptions for servers that WatchGuard products and subscription services connect to.

Add Blocked Sites

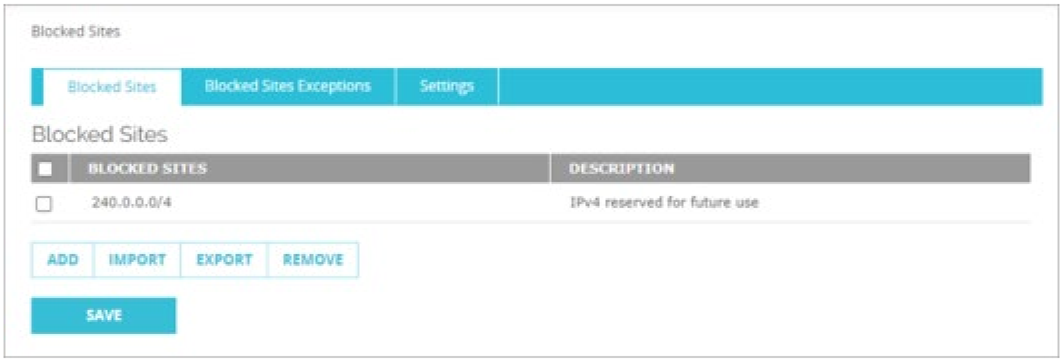
To comply with requirements to drop invalid tra, you must add entries to the blocked sites list for:

- IPv4 address block defined as 'reserved for future use' in RFC 5735.
- IPv6 addresses defined as 'unspecified address' or 'reserved for future definition and use' in RFC 3513.

To edit the Blocked Sites list, select **Firewall > Blocked Sites**.

To add the required IPv4 address block to the Blocked Sites list:

1. On the Blocked Sites page, click **Add**.
   The Add Sites dialog box appears.
2. From the **Choose Type** drop-down list, select **Network IPv4**.
3. Type the network IP address `240.0.0.0/4`.
   RFC 5735 defines this address block as 'reserved for future use' .
4. In the **Description** text box, type a description, such as **IPv4 reserved for future use**.
5. Click **OK**.
   The IP address is added to the Blocked Sites list.



Blocked Sites

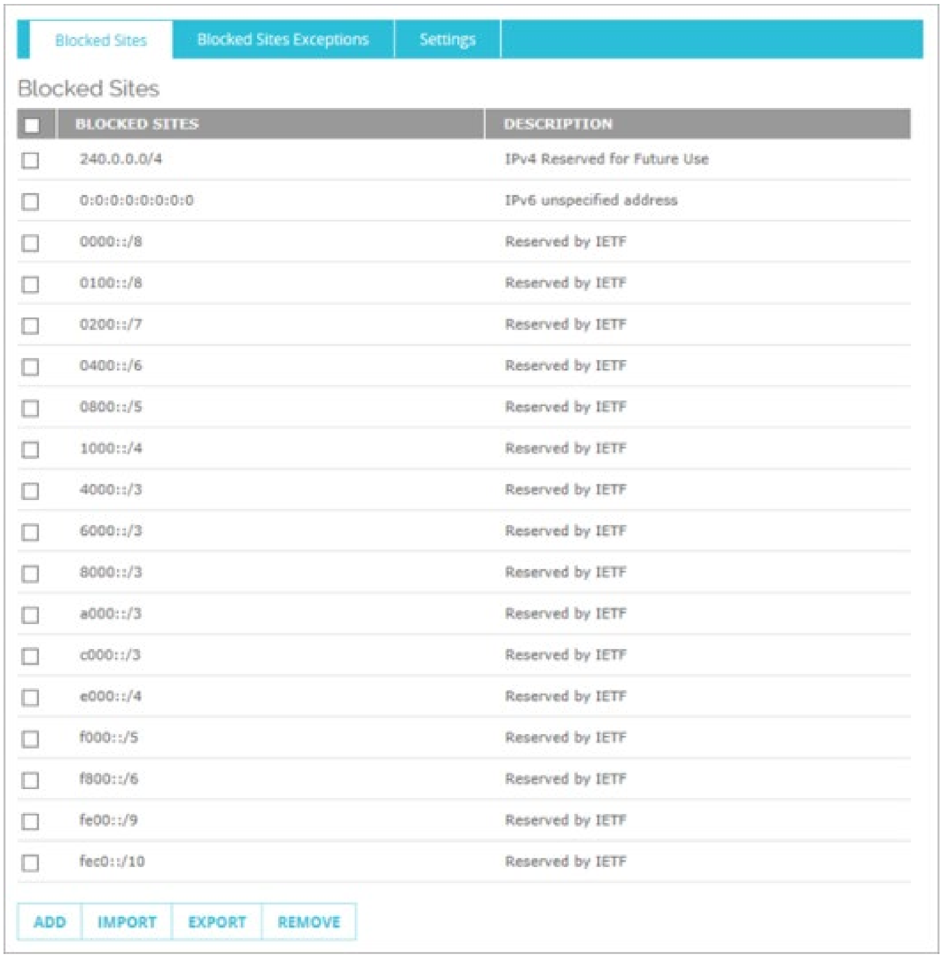
☐	BLOCKED SITES	DESCRIPTION
☐	240.0.0.0/4	IPv4 reserved for future use

6. Click **Save**.

To add required IPv6 addresses to the Blocked Sites list:

1. On the Blocked Sites page, click **Add**.
   The Add Sites dialog box appears.
2. From the **Choose Type** drop-down list, select **Host IPv6**.
3. Type the host IP address `0:0:0:0:0:0:0:0`.
   RFC 3513 defines this as the "unspecified address' .
4. In the **Description** text box, type a description, such as **IPv6 unspecified address**.
5. Click **OK**.
   The IP address is added to the Blocked Sites list.
6. Add **Network IPv6** addresses for these reserved IPv6 network addresses:

   0000::/8
   0100::/8
   0200::/7
   0400::/6
   0800::/5
   1000::/4
   4000::/3
   6000::/3
   8000::/3
   a000::/3
   c000::/3
   e000::/4
   f000::/5
   f800::/6
   fe00::/9
   fec0::/10



Blocked Sites

□	BLOCKED SITES	DESCRIPTION
□	240.0.0.0/4	IPv4 Reserved for Future Use
□	0:0:0:0:0:0:0:0	IPv6 unspecified address
□	0000::/8	Reserved by IETF
□	0100::/8	Reserved by IETF
□	0200::/7	Reserved by IETF
□	0400::/6	Reserved by IETF
□	0800::/5	Reserved by IETF
□	1000::/4	Reserved by IETF
□	4000::/3	Reserved by IETF
□	6000::/3	Reserved by IETF
□	8000::/3	Reserved by IETF
□	a000::/3	Reserved by IETF
□	c000::/3	Reserved by IETF
□	e000::/4	Reserved by IETF
□	f000::/5	Reserved by IETF
□	f800::/6	Reserved by IETF
□	fe00::/9	Reserved by IETF
□	fec0::/10	Reserved by IETF

Configured blocked sites list with all required sites added

Blocked Ports

You can use the Blocked Ports page to add a port number to the Blocked Ports list. The Firebox denies all traffic to blocked ports on all external interfaces.

By default, the Firebox blocks traffic on these ports:

1
111
513
514
2049
6000
6001
6002
6003
6004
6005
7100
8000

To configure blocked ports, from Fireware Web UI:

1. Select **Firewall > Blocked Ports**.
2. To add a port, type the port number and click **Add**.
3. To automatically block sites that use a blocked port, select the **Automatically block sites that try to use blocked ports** check box.
4. To save the configuration change, click **Save**.

If you enable the option to automatically block sites that try to use blocked ports, the address of the computer that tries to use a blocked port is added to the Auto-Blocked Sites List.

Security Services Priority

With a Total Security Suite subscription, the Firebox and WatchGuard security services provide comprehensive protection against attacks. When a Firebox with all services enabled receives a packet, these global services inspect the packet before any configured policies and security services:

- Default Threat Protection
- Botnet Detection
- DNSWatch (when the packet arrives internally on UDP port 53)

If the packet is allowed, then it moves to policy-based inspection and the security services that are enabled in those policies. This list shows the order that security services scan the packet and, when enabled in a proxy policy, inspect the content:

1. Geolocation
2. Application Control and Intrusion Prevention Service
3. WebBlocker or spamBlocker
4. Reputation Enabled Defense
5. Gateway AntiVirus
6. IntelligentAV
7. APT Blocker
8. Data Loss Prevention

> ⓘ The order can change based on the packet type. In general, the services race to inspect the content and the first service to deny the content drops the connection. After the connection drops, the other services do not scan the packet.

Configure Firewall Policies

Firewall Policy Types

Your Firebox uses two categories of policies to filter network traffic: *packet filters* and *proxies*.

Packet Filter Policy

A packet filter policy examines the IP header of each packet at the network and transport protocol packet layers. If the packet header information is legitimate and the content of the packet header matches a packet filter policy that allows traffic, the Firebox allows the packet. Otherwise, the Firebox drops the packet.

Proxy Policy or ALG (Application Layer Gateway)

A proxy policy examines both the IP header information and the content of each packet at the application layer to make sure that connections are compliant with protocols. If the packet header information is legitimate, and the content of the packet matches the criteria set in the proxy policy, then the Firebox allows the packet. If the content does not match the criteria set in the proxy policy, the proxy drops the packet or, in some cases, allows the packet and removes disallowed content. An ALG completes the same functions as a proxy, but also provides transparent connection management.

For each policy type, the policy template defines the ports and protocols the policy applies to.

> ⓘ The FTP packet filter and proxy policies do transparent connection management for the FTP data channel. The FTP policy is configured for TCP port 21, which is used for the FTP handshake. The FTP policy dynamically opens another negotiated port for data transfer.

Add a Firewall Policy

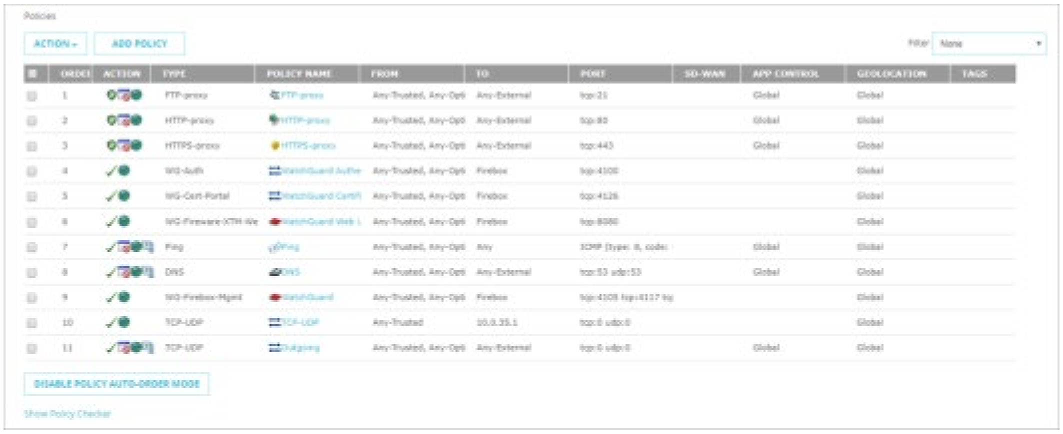
Your Firebox configuration includes a default set of policies and predefined policy templates. When you add a policy, you select a policy template. The template specifies whether the policy is a packet filter or proxy policy, and defines the ports and protocols the policy applies to. After you use a policy template to add a new policy, you can configure other policy properties, such as subscription services, QoS actions, and operating schedules.

After you add a policy to your configuration, you define rules to:

- Set allowed traffic sources and destinations.
- Enable security services.
- Configure filter rules in proxy actions (for proxy policies).
- Configure properties such as Traffic Management, NAT, and log settings.

To add a firewall policy, from Fireware Web UI:

1. Select **Firewall > Firewall Policies**.
   The Policies list appears.



Policies

ACTION ▾ | ADD POLICY

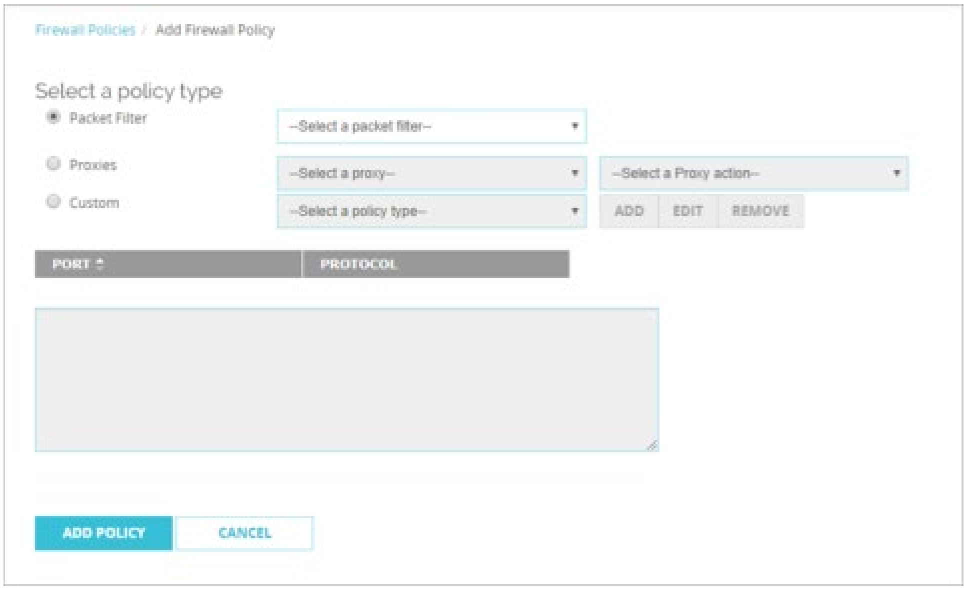
Filter: None ▾

☐	ORDER	ACTION	TYPE	POLICY NAME	FROM	TO	PORT	SD-WAN	APP CONTROL	GEOLOCATION	TAGS
☐	1		FTP-proxy	FTP-proxy	Any-Trusted, Any-Opti	Any-External	tcp:21		Global	Global	
☐	2		HTTP-proxy	HTTP-proxy	Any-Trusted, Any-Opti	Any-External	tcp:80		Global	Global	
☐	3		HTTPS-proxy	HTTPS-proxy	Any-Trusted, Any-Opti	Any-External	tcp:443		Global	Global	
☐	4	✓	WG-Auth	WatchGuard Authe	Any-Trusted, Any-Opti	Firebox	tcp:4100			Global	
☐	5	✓	WG-Cert-Portal	WatchGuard Certifi	Any-Trusted, Any-Opti	Firebox	tcp:4126			Global	
☐	6	✓	WG-Fireware-XTM-We	WatchGuard Web I	Any-Trusted, Any-Opti	Firebox	tcp:8080			Global	
☐	7	✓	Ping	Ping	Any-Trusted, Any-Opti	Any	ICMP (type: 8, code:		Global	Global	
☐	8	✓	DNS	DNS	Any-Trusted, Any-Opti	Any-External	tcp:53 udp:53		Global	Global	
☐	9	✓	WG-Firebox-Mgmt	WatchGuard	Any-Trusted, Any-Opti	Firebox	tcp:4105 tcp:4117 tcp			Global	
☐	10	✓	TCP-UDP	TCP-UDP	Any-Trusted	10.0.35.1	tcp:0 udp:0			Global	
☐	11	✓	TCP-UDP	Outgoing	Any-Trusted, Any-Opti	Any-External	tcp:0 udp:0		Global	Global	

DISABLE POLICY AUTO-ORDER MODE

Show Policy Checker

2. Click **Add Policy**.



Firewall Policies / Add Firewall Policy

Select a policy type

● Packet Filter — --Select a packet filter-- ▾

○ Proxies — --Select a proxy-- ▾ — --Select a Proxy action-- ▾

○ Custom — --Select a policy type-- ▾ — ADD | EDIT | REMOVE

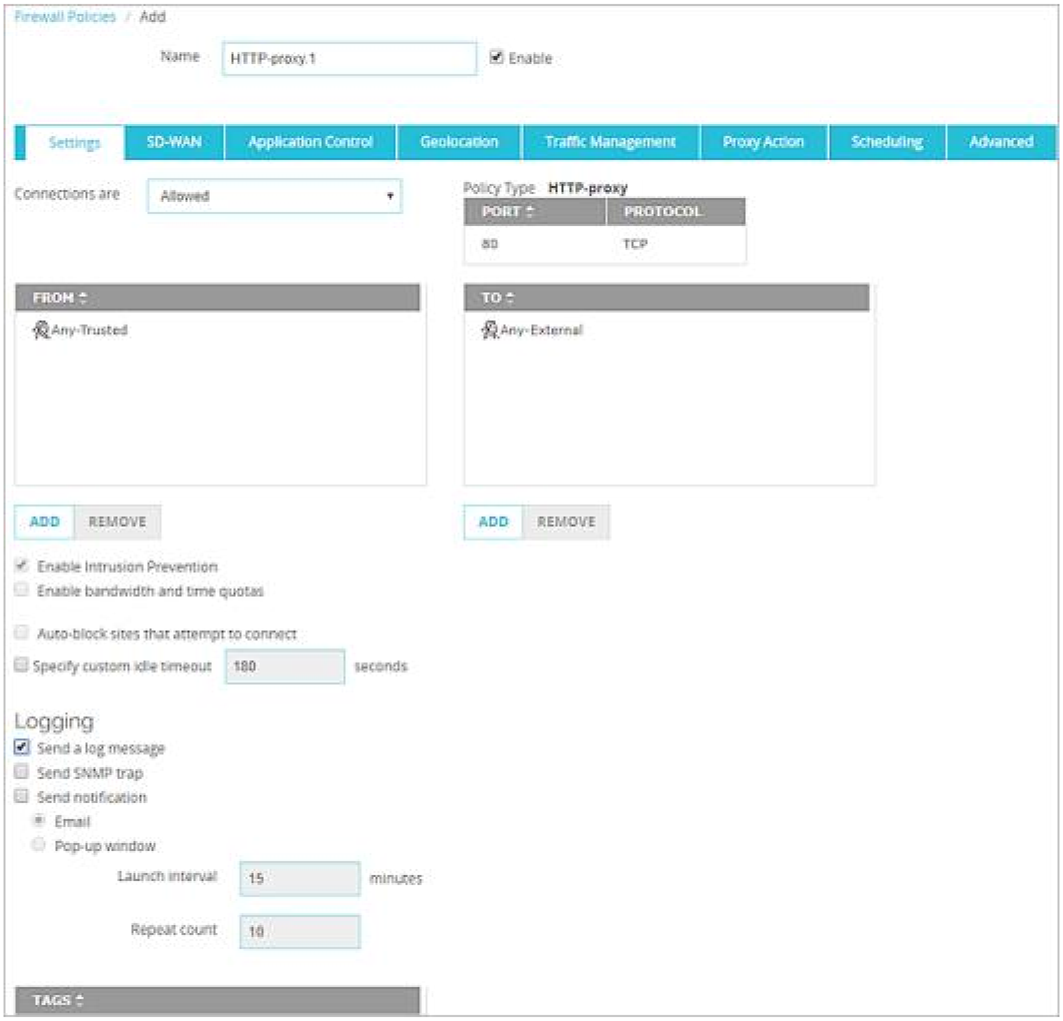
PORT ⇕	PROTOCOL

ADD POLICY | CANCEL

3. Select a policy type:
   - **Packet Filter**
   - **Proxies**
   - **Custom**
4. For a packet filter, from the adjacent drop-down list, select a policy template.
   For a proxy, from the adjacent drop-down list, select a proxy policy template, and from the second drop-down list, select a proxy action.
   For a custom policy, from the adjacent drop-down list, select a custom policy template or click **Add** to create a new custom policy template.

ⓘ To create a policy to handle traffic for specific protocols and ports that are not included in the predefined policy templates, add a custom policy template, and use that template to create a custom policy.

5. Click **Add Policy**.
The properties appear. The Port and Protocol depend on the policy template you selected.



Name HTTP-proxy.1 ☑ Enable

Connections are Allowed

Policy Type HTTP-proxy

PORT ≑	PROTOCOL
80	TCP

FROM ≑
Any-Trusted

TO ≑
Any-External

☑ Enable Intrusion Prevention
□ Enable bandwidth and time quotas

□ Auto-block sites that attempt to connect
□ Specify custom idle timeout 180 seconds

Logging
☑ Send a log message
□ Send SNMP trap
□ Send notification
● Email
○ Pop-up window
Launch interval 15 minutes
Repeat count 10

6. Configure the source, destination, and other policy properties, as described in the next section.
7. Click **Save**.

Configure Policy Properties

Each policy type has a default definition, which consists of settings that are appropriate for most organizations. You can modify policy settings, or add other settings such as traffic management and operating schedules.

On the **Settings** tab, you can set basic information about a policy, such as whether it allows or denies traffic, and set access rules that define the source and destination of traffic the policy handles. You can also configure static NAT, bandwidth and time quotas, or server load balancing. The **Settings** tab also shows the port and protocol for the policy, and an optional description of the policy. You can use the settings on this tab to set logging, notification, automatic blocking, and timeout preferences.

In each policy, you configure access rules that determine whether the policy allows or denies connections, and define the source and destination of connections the policy applies to.

Disposition (Allowed or Denied)

The *disposition* specifies what action the policy takes for connections that match the rules in the policy. The **Connections are** drop-down list has actions that specify whether the policy allows or denies connections that match the rules in the policy. To configure the disposition, select one of these settings:

Allowed

> The Firebox allows traffic that uses this policy if it matches the rules you set in the policy. You can configure the policy to create a log message when network traffic matches the policy.

Denied

> The Firebox denies all traffic that matches the rules in this policy and does not send a notification to the device that sent the traffic. You can configure the policy to create a log message when a computer tries to use this policy. The policy can also automatically add a computer or network to the Blocked Sites list if it tries to start a connection with this policy.

Denied (send reset)

> The Firebox denies all traffic that matches the rules in this policy. You can configure it to create a log message when a computer tries to use this policy. The policy can also automatically add a computer or network to the Blocked Sites list if it tries to start a connection with this policy.
>
> With this option, the Firebox sends a packet to tell the device that sent the network traffic that the session is refused and the connection is closed. You can set a policy to return other errors instead, which tell the device that the port, protocol, network, or host is unreachable. To make sure that your network operates correctly with other networks, use these options with caution.

Source and Destination

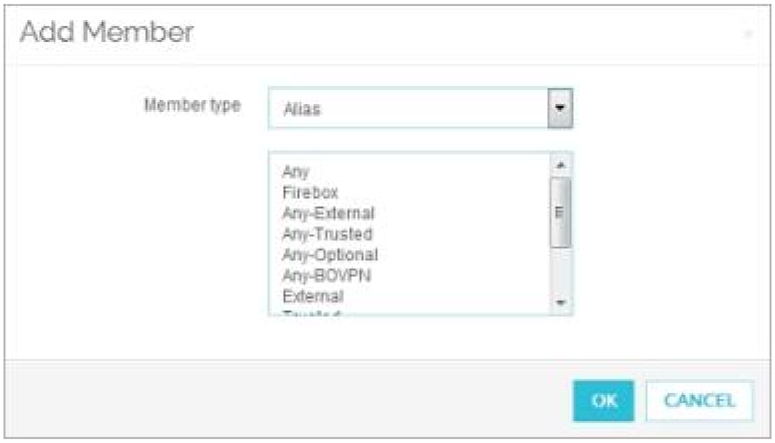
In each policy, you specify the source and destination of connections the policy applies to. A connection must match both the source and destination specified in the policy for the policy to apply to that traffic.

In each policy, you configure:

- A **From** list (or *source*) that specifies the source of connections that this policy applies to.
- A **To** list (or *destination*) that specifies the destination of connections that this policy applies to.

To add source or destination members to a policy, from Fireware Web UI:

1. On the **Settings** tab, below the **From** or **To** list, click **Add**.
   The Add Member dialog box appears.



Add Member

Member type: Alias

   The members list contains the members you can add to the **From** or **To** lists. A member can be an alias, user, group, IP address, range of IP addresses, VPN tunnel, or FQDN (includes wildcard domains).

2. From the **Member Type** drop-down list, select the type of member you want to add.
3. From the member list, select a member.
4. Click **OK**.
   The member appears in the member list on the Settings tab.
5. To add other members to the **From** or **To** list, repeat the previous steps.
6. Click **Save**.

Ports and Protocols

The ports and protocols that the policy applies to are on the **Settings** tab. These are set based on the policy template you chose when you added the policy. You cannot edit the ports and protocols within the policy.

Fireware includes many policy templates for different types of traffic, configured with the standard ports and protocols used for each type of traffic. To create a policy for a custom port and protocol, when you add the policy, select **Custom**, and then add a custom policy template with the custom ports and protocols.

ⓘ The FTP packet filter and proxy policies do transparent connection management for the FTP data channel. The FTP policy is configured for TCP port 21, which is used for the FTP handshake. The FTP policy dynamically opens another negotiated port, and uses that port for data transfer. When the connection is completed, the FTP policy closes the negotiated port. For an FTP connection, the first FTP log message shows the “received on port” while the next FTP log message (response log) shows the negotiated port that will be used for FTP data transfer.

Logging

The Firebox sends traffic log messages as it applies packet filter and proxy policy rules to traffic that goes through the Firewall.

For the Firebox to generate log messages for allowed traffic, you must enable logging of allowed traffic in packet filter policies, or logging for reports in proxy policies. Logging of allowed traffic is enabled by default in the policies created by the Firebox setup wizards.

To enable logging for allowed traffic in a packet filter policy:

1. Edit the policy.
2. In the **Logging** settings, select the **Send a log message** and **Send a log message for reports** check boxes.

To enable logging in a proxy policy:

1. Edit the policy.
2. Select the **Proxy Action** tab.
3. In the proxy action **General** settings, select the **Enable logging for reports** check box.

For more information, see *Audit Logging*.

Policy Precedence

Precedence refers to the order in which the Firebox examines network traffic and applies a policy rule. Only one policy applies to each connection. The Firebox uses the highest-precedence policy to determine whether to allow or deny a connection. Network traffic that does not match any policy is denied as an unhandled packet.

By default, the Firebox policies are configured in Auto-Order mode. In Auto-Order mode, the Firebox automatically sorts policies from the most specific to the most general, based on a comparison of these policy properties:

- Policy (specificity)
- Ports and protocols
- Source and destination
- Disposition
- Schedule

In the policy list, the Order column shows the order of policy precedence.

Policies higher in the list have higher precedence. When the Firebox receives a packet, it applies the highest precedence policy that matches the characteristics of the packet. When Auto-Order mode is enabled, if two policies are equally specific, a proxy policy takes precedence over a packet filter policy. Only the highest precedence policy that matches the port, protocol, source, and destination applies to a packet. You can also disable Auto-Order mode and manually change the order of policies.

Set Precedence Manually

You can change to manual-order mode and set the policy precedence for your Firebox.

To switch to manual order mode, from Fireware Web UI:

1. Select **Firewall > Firewall Policies**.
   The Firewall Policies page appears.
2. Below the policy list, click **Disable policy Auto-Order mode**.
   A confirmation message appears.
3. Click **Yes**.
4. To change the order of a policy, select the check box for a policy and click **Move Up** or **Move Down** to move it higher or lower in the list, or drag it to a new location in the Policy List.
5. Click **Save Policy Order**.

Hidden Policies

Unhandled Packets

The Firebox fails closed. This means that the Firebox denies all traffic that does not match the configured policies. To do this, the Firebox uses two hidden policies that have lower precedence than all the configured policies. These two hidden policies drop unhandled packets.

- **Unhandled Internal Packet** — This policy denies outgoing connections that are not explicitly allowed by another policy.
- **Unhandled External Packet** — This policy denies incoming connections that are not explicitly allowed by another policy.

These policy names appear in log messages when the hidden policies deny unhandled traffic.

Because the Firebox already includes these hidden policies, it is not necessary to add a policy to deny connections that are not allowed by your configured policies.

Stateful Sessions

The Firebox is a stateful network firewall. It tracks the operating state and characteristics of network connections, and allows only packets that match a known active session. The Firebox does not generate a log message for every packet that matches an established session.

Traffic From the Firebox

There is also a hidden policy that allows traffic generated by the Firebox itself. This policy has a higher precedence than all other policies, so that traffic from the Firebox is always allowed.

Any From Firebox — This policy allows connections from the Firebox itself to any network destination.

Examples of Firebox-generated traffic include:

- Signature updates for WatchGuard services such as Gateway AntiVirus, Intrusion Prevention Service, Application Control, Data Loss Prevention, Botnet Detection, and Geolocation.
- Queries to WatchGuard servers for services such as WebBlocker, spamBlocker, and APT Blocker.

Built-In IPSec Policy

The Firebox has a hidden IPSec policy that allows IPSec VPN connections to the Firebox itself.

This hidden policy exists when the **Enable the built-in IPSec Policy** check box is selected in the global VPN settings. This check box is selected by default. If you disable this setting, the hidden policy is removed, and IPSec VPN connections will fail.

Deny All “Reserved for Future Use” Network Traffic

Add a policy to deny all connections where the source or destination address of the network packet is defined as being an address "reserved for future use" as specified in RFC 5735 for IPv4.

To configure the Firebox to deny this traffic and send a log message, add two packet filter policies with these properties:

Deny from reserved IP addresses:

- Packet filter policy template: Any
- Connections are: Denied
- From: 240.0.0.0/4
- To: Any
- Logging: Enabled

Deny to reserved IP addresses:

- Packet filter policy template: Any
- Disposition: Connections are: Denied
- From: Any
- To: 240.0.0.0/4
- Logging: Enabled

Deny Traffic from Invalid IPv4 and IPv6 Protocols

The Firebox blocks invalid ICMPv4 and ICMPv6 traffic by default. To block traffic that uses invalid IPv4 or IPv6 IP protocols, you must create two custom policy templates for the invalid protocol ranges. Then use these custom policy templates to configure policies to deny invalid IPv4 and IPv6 traffic.

Invalid protocols:

- IPv4: IP 101-255
- IPv6: IP 143-255

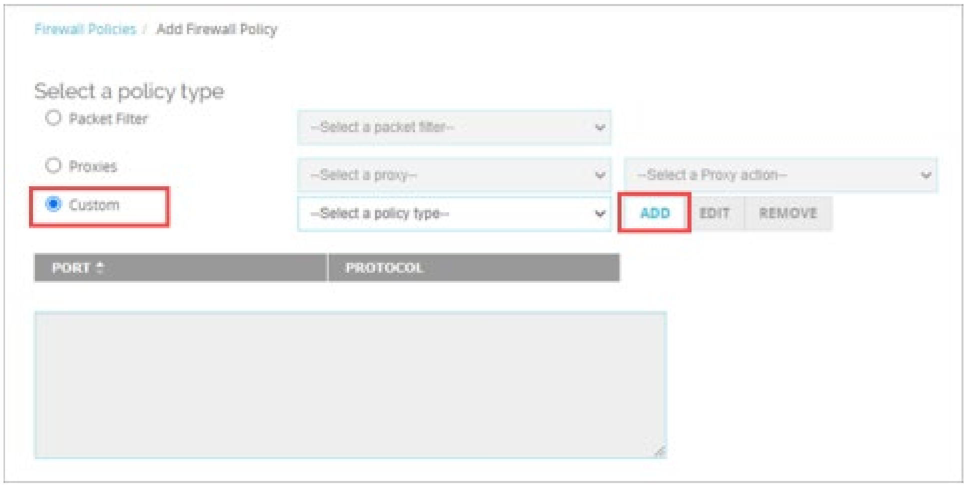
You must create a custom policy template and policy for IPv4 and IPv6.

ⓘ The process to create custom policies in Fireware Web UI can take a long time. To make sure that your session does not time out, we recommend you increase the **Idle Timeout** setting for management sessions to at least 60 minutes before you start to configure these policies. For the new idle timeout to take effect, you must log out and back in to Fireware Web UI. For information about how to change this setting, see *Configure Management Session Timeouts*.

Add a Custom Policy to Deny Invalid IPv4 Protocols

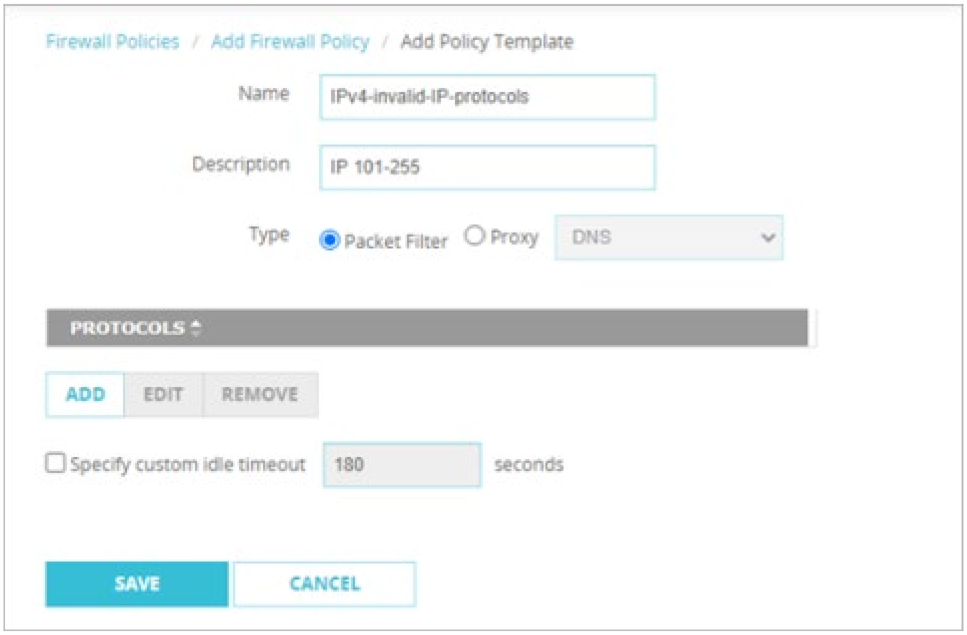
To create a custom policy template and add the policy to deny invalid IPv4 protocols:

1. Select **Firewall > Policies**.
2. Click **Add Policy**.
3. Select **Custom**.



● Custom

4. To add a custom policy template, click **Add**.
5. Type a **Name** and **Description** for the policy template.
6. For the **Type**, select **Packet Filter** (this is the default).


Firewall Policies / Add Firewall Policy / Add Policy Template
PROTOCOLS
ADD
EDIT
REMOVE
SAVE
CANCEL

Name: IPv4-invalid-IP-protocols

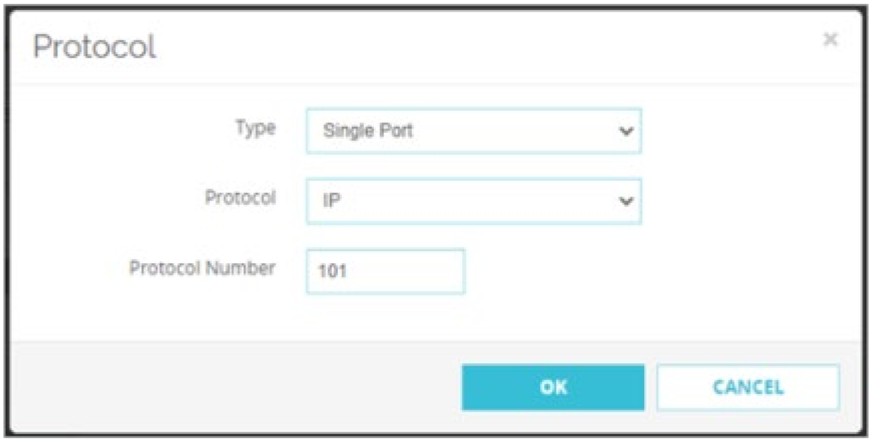
Description: IP 101-255

Type: ● Packet Filter ○ Proxy DNS

□ Specify custom idle timeout 180 seconds

7. In the **Protocols** list, add IP protocols 101 - 255. To add these protocols:
   a. Click **Add**.
   b. From the **Protocol** drop-down list, select **IP**.

- c. In the **Protocol Number** text box, type the protocol number.



Protocol

Type: Single Port

Protocol: IP

Protocol Number: 101

- d. Click **OK**.
- e. Repeat these steps to add each IP protocol.

8. To save the policy template, click **Save**.
   You return to the Add Policy page, with the new custom template selected.
9. To create the policy that uses the new custom policy template, at the bottom of the page, click **Add Policy**.
10. To deny all IPv4 traffic for these protocols, configure the custom policy with these settings:

    - Connections are: Denied
    - From: Network IPv4 address 0.0.0.0/0
    - To: Network IPv4 address 0.0.0.0/0
    - Logging: Enabled

Add a Custom Policy to Deny Invalid IPv6 Protocols

Add another custom policy to deny IPv6 traffic for IP protocols 143-255

To create a custom policy template and add the policy to deny invalid IPv4 protocols:

1. Select **Firewall > Policies**.
2. Click **Add Policy**.
3. Select **Custom**.
4. To add a custom policy template, click **Add**.
5. Type a **Name** and **Description** for the policy template.
6. For the **Type**, select **Packet Filter** (this is the default).
7. In the **Protocols** list, add IP protocols 143 - 255. To add these protocols:
   - a. Click **Add**.
   - b. From the **Protocol** drop-down list, select **IP**.
   - c. In the **Protocol Number** text box, type the protocol number.
   - d. Click **OK**.
   - e. Repeat these steps to add each IP protocol.

8. To save the policy template, click **Save**.
   You return to the Add Policy page, with the new custom template selected.
9. To create the policy that uses the new custom policy template, at the bottom of the page, click **Add Policy**.
10. To deny all IPv6 traffic for these protocols, configure the custom policy with these settings:
    - Connections are: Denied
    - From: Network IPv6 ;;/0
    - To: Network IPv6 ;;/0
    - Logging: Enabled

Configurable Firewall Policy Attributes

This section summarizes configurable policy attributes required for compliance.

- IMCPv4
  - Type — configure in a custom policy template, when you add the IMCP protocol
  - Code — configure in a custom policy template, when you add the IMCP protocol
- IMCPv6
  - Type — configure in a custom policy template, when you add the ICMPv6 protocol
  - Code — configure in a custom policy template, when you add the ICMPv6 protocol
- IPv4
  - Source address — configure in the firewall policy **From** list.
  - Destination address — configure in the firewall policy **To** list.
  - Supported IPv4 address types for source and destination:
    - Host IPv4
    - Network IPv4
    - Host Range IPv4
    - Wildcard IPv4
- Transport Layer Protocol — specified in the policy template. Select a predefined policy template or add a custom policy template.
- IPv6
  - Source address — configure in the firewall policy **From** list.
  - Destination address — configure in the firewall policy **To** list.
  - Supported IPv6 address types for source and destination:
    - Host IPv6
    - Network IPv6
    - Host Range IPv6
  - Transport Layer Protocol — specified in the policy template. Select a predefined policy template or add a custom policy template.
- TCP
  - Source port — in the policy Advanced tab, select one of these options:

    - **Apply this policy to traffic from all source ports**
    - **Apply this policy to traffic from only the specified source ports**
  - Destination port — specified in the policy template. Select a predefined policy template or add a custom policy template.

- UDP
  - Source port — in the policy Advanced tab, select one of these options:
    - **Apply this policy to traffic from all source ports**
    - **Apply this policy to traffic from only the specified source ports**
  - Destination port — specified in the policy template. Select a predefined policy template or add a custom policy template.

Policy Actions and Logging

You can configure firewall policies to either allow or drop traffic that matches the policy settings.

In each firewall policy, the **Connections are** option is the policy action:

- To configure the policy to permit traffic, select **Allowed**.
- To configure the policy to drop traffic, select **Denied** or **Denied (send reset)**

To enable logging for each policy, select **Send a log message**. For more information about Firebox logging and log settings, see *Audit Logging*.

Associate Policies with Network Interfaces

To associated firewall policy rules for traffic to or from a specific interface, specify the interface name as the policy source (From list) or destination (To list), or specify an alias that includes an interface. To specify an interface name, when you add a policy source or destination, select the member type *Alias*, and select the interface name or alias from the list.

Example policy source and destination by interface name

> **FROM: Trusted** — default alias (name) for interface 1
>
> **TO: External** — default alias (name) for interface 0

Example policy source and destination by interface zone

> **FROM: Any-Trusted** (predefined alias that includes all interfaces of type Trusted)
>
> **TO: Any-External** (predefined alias that includes all interfaces of type External)

IPSec VPN

To create a secure connection from the Firebox to any other endpoint, you can configure an IPSec VPN. On the Firebox, this is known as a Branch Office VPN (BOVPN).

You can configure a BOVPN gateway and add one or more BOVPN tunnels that use that gateway. This option enables you to set up a BOVPN tunnel between two Fireboxes, or between a Firebox and another device that uses the same gateway and tunnel settings. When you use this configuration method, the Firebox always routes a packet through the BOVPN tunnel if the source and destination of the packet match a configured BOVPN tunnel.

ⓘ To secure the connection from the Firebox to an external syslog server, configure a BOVPN gateway and tunnel to the location of the syslog server.

Configure a BOVPN Gateway

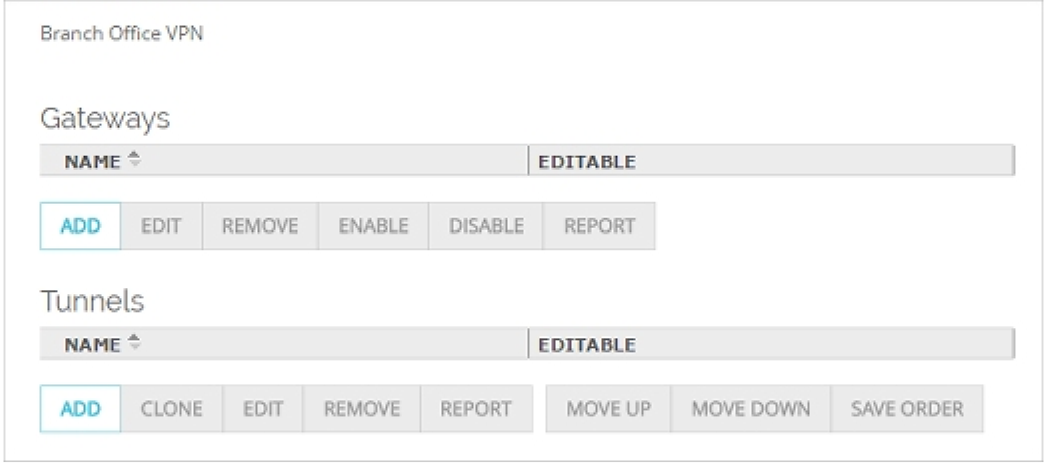
A branch office VPN (BOVPN) gateway is a connection point for one or more tunnels. To create a tunnel, you must set up gateways on both the local and remote endpoint devices.

Add a Gateway

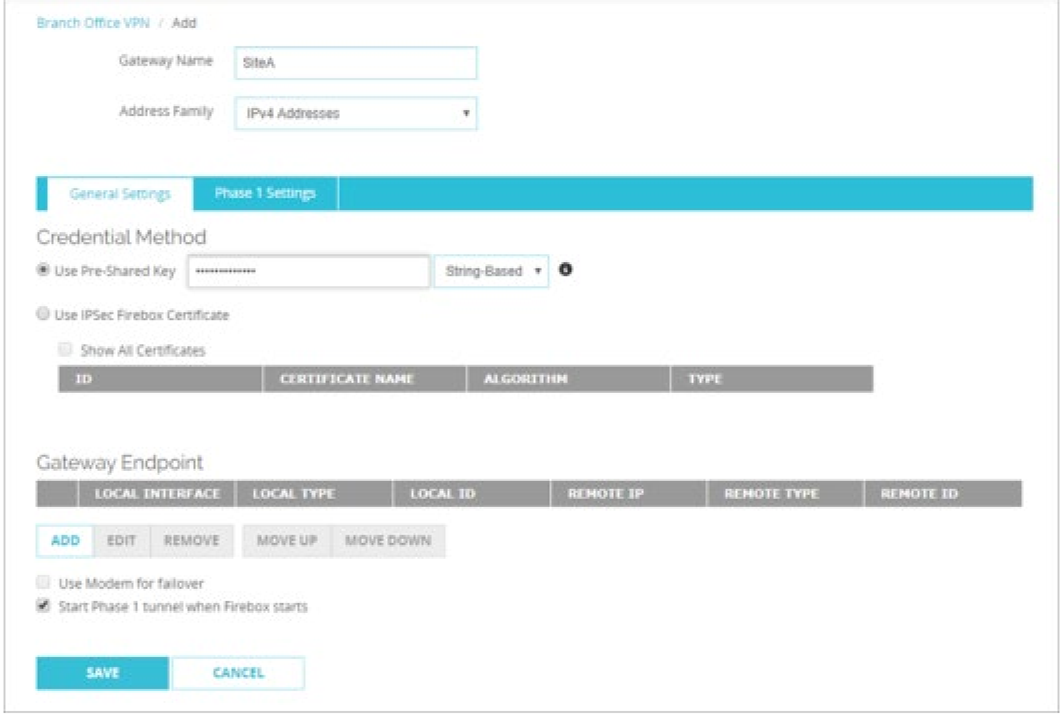
Configure the gateways for each BOVPN endpoint.

To add a gateway, from Fireware Web UI:

1. Select **VPN > Branch Office VPN**.
   The Branch Office VPN configuration page appears.



2. To add a gateway, in the Gateways section, click **Add**.
   The Gateway settings page appears.



Branch Office VPN / Add

Gateway Name: SiteA

Address Family: IPv4 Addresses

Credential Method

● Use Pre-Shared Key: •••••••••••••• String-Based

○ Use IPSec Firebox Certificate

□ Show All Certificates

ID	CERTIFICATE NAME	ALGORITHM	TYPE

Gateway Endpoint

	LOCAL INTERFACE	LOCAL TYPE	LOCAL ID	REMOTE IP	REMOTE TYPE	REMOTE ID

□ Use Modem for failover

☑ Start Phase 1 tunnel when Firebox starts

3. In the **Gateway Name** text box, type a name to identify the gateway for this Firebox.
4. From the **Address Family** drop-down list, select **IPv4 Addresses** or **IPv6 Addresses**.
5. Select either **Use Pre-Shared Key** or **Use IPSec Firebox Certificate** to identify the authentication method for this tunnel.

Use Pre-Shared Key

The pre-shared key is a passphrase used by two devices to encrypt and decrypt the data that goes through the tunnel. The two devices use the same key. To use a pre-shared Key, select whether the pre-shared key is **string-based** or **hex-based**. Type or paste the shared key. You must use the same shared key on the remote device.
A string-based shared key:

- Must include only these characters: A-Z, a-z, 0-9, !@#$%^&*()
- Must be between 1 - 79 characters in length

A hex-based pre-shared key:

- Must include only numbers and the letters a-f or A-F
- Must contain 22 characters

To create a secure pre-shared key, we recommend that you:

- Use a pre-shared key with a minimum of 8 characters. Longer keys provide stronger security.
- Use a combination of uppercase and lowercase ASCII characters, numbers, and special characters.
- Do not use a word from standard dictionaries, even if you use it in a different sequence or in a different language.

- Do not use a business name, familiar name, or the name of a person.

Use IPSec Firebox Certificate

The current certificates on the Firebox appear in the certificates list. This includes the *IP security IKE intermediate* Extended Key Usage (EKU) identifier (OID 1.3.6.1.5.5.8.2.2). You can also select a certificate that does not include an EKU identifier.
To see a list of available certificates that do not include an EKU identifier, select the **Show All Certificates** check box.

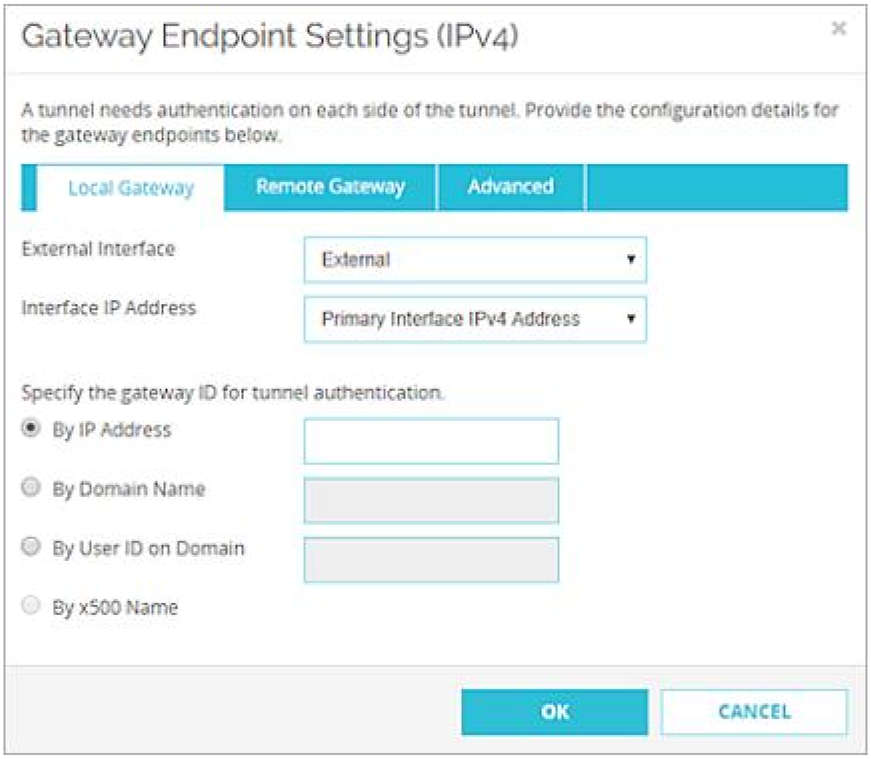
5. Configure local and remote gateway endpoints as described in the next section.

Configure the Gateway Endpoints

Gateway endpoints are the local and remote gateways that a BOVPN connects. The gateway endpoints configuration tells your Firebox how to identify and communicate with the remote endpoint device when it negotiates the BOVPN. It also tells the device how to identify itself to the remote endpoint when it negotiates the BOVPN. You must configure at least one gateway endpoint pair when you add a BOVPN gateway.

To configure the gateway endpoints:

1. From the **Gateway** page, in the **Gateway Endpoint** section, click **Add**.
The New Gateway Endpoints Settings dialog box appears.



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

External Interface: External ▾

Interface IP Address: Primary Interface IPv4 Address ▾

Specify the gateway ID for tunnel authentication.

● By IP Address

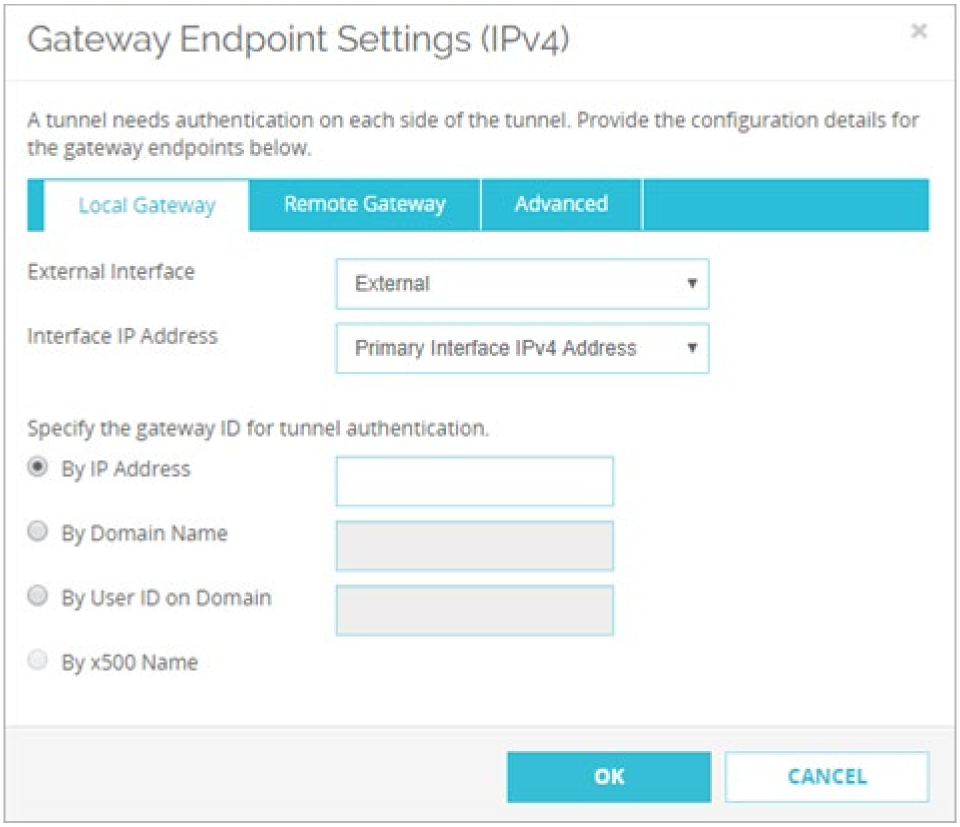
○ By Domain Name

○ By User ID on Domain

○ By x500 Name

2. From the **External Interface** drop-down list, select the interface that has the external (public) IP address of the Site A Firebox.

3. In the **Interface IP Address** drop-down list, select **Primary Interface IP Address** or select a secondary IP address that is already configured on the selected external interface.



Gateway Endpoint Settings (IPv4)

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

External Interface: External

Interface IP Address: Primary Interface IPv4 Address

Specify the gateway ID for tunnel authentication.

● By IP Address

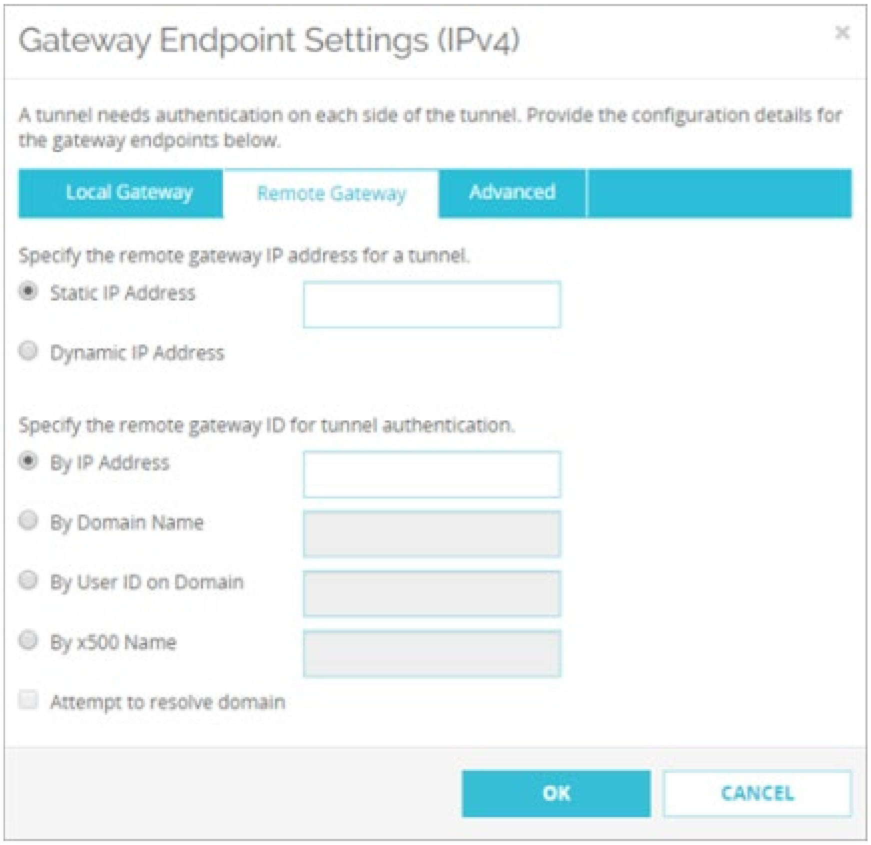
○ By Domain Name

○ By User ID on Domain

○ By x500 Name

4. Select an option and specify the gateway ID:
   - **By IP address** — Type the primary IP address of the Firebox interface.
     If you selected a secondary IP address from the **Interface IP Address** drop-down list, that IP address automatically appears in the **By IP Address** text box.
   - **By Domain Name** — Type your domain name. You must specify 63 characters or fewer.
   - **By User ID on Domain** — Type the user name and domain with the format `UserName@DomainName`. You must specify 63 characters or fewer.
   - **By x500 Name** — This option is automatically selected if you specified a certificate as the credential method.

5. To configure the remote gateway endpoint, select the **Remote Gateway** tab.



Gateway Endpoint Settings (IPv4)

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

Specify the remote gateway IP address for a tunnel.

● Static IP Address

○ Dynamic IP Address

Specify the remote gateway ID for tunnel authentication.

● By IP Address

○ By Domain Name

○ By User ID on Domain

○ By x500 Name

□ Attempt to resolve domain

6. Select the remote gateway IP address type:
   - **Static IP address** — Select this option if the remote device has a static IP address. Type or select the IP address.
   - **Dynamic IP address** — Select this option if the remote device has a dynamic IP address.
7. Select an option and specify the remote gateway ID:
   - **By IP address** — Type the IP address.
   - **By Domain Name** — Type the domain name.
   - **By User ID on Domain** — Type the user ID and domain.
   - **By x500 Name** — Type the x500 name.

   For an IPv4 gateway endpoint, if the domain name of the remote endpoint can be resolved, select the **Attempt to resolve domain** check box.
   When this option is selected, the device automatically does a DNS query to find the IP address associated with the domain name for the remote endpoint. Connections do not proceed until the domain name can be resolved. Select this check box for configurations that depend on a dynamic DNS server to maintain a mapping between a dynamic IP address and a domain name.
8. Click **OK**.
   The gateway pair you defined appears in the list of gateway endpoints.

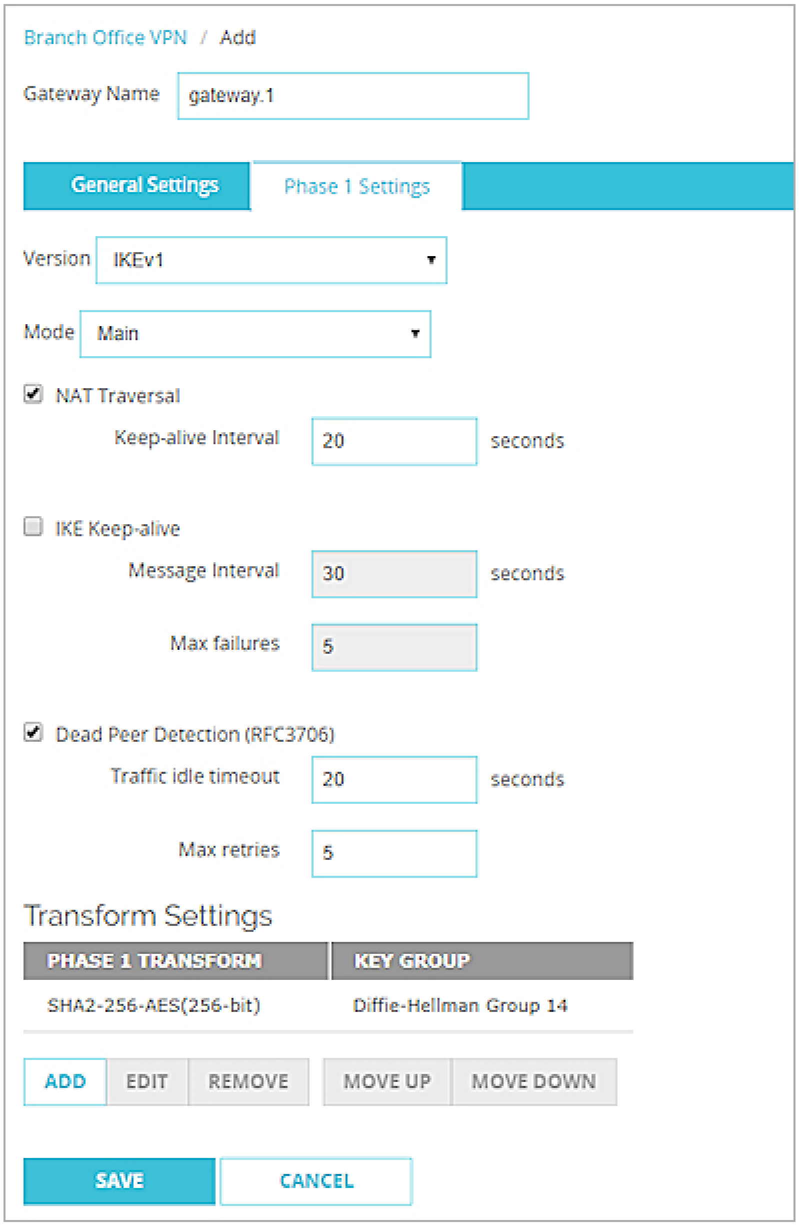
Configure IPSec VPN Phase 1 Settings

You can configure the gateway Phase 1 settings for IKEv1 or IKEv2. If you select IKEv1, you must select Main Mode.

Configure Phase 1 Settings For IKEv1

To configure Phase 1 settings for IKEv1, from Fireware Web UI:

1. Edit the BOVPN gateway.
2. Select the **Phase 1 Settings** tab.
3. From the **Version** drop-down list, select **IKEv1**.



Branch Office VPN / Add

Gateway Name: gateway.1

Version: IKEv1

Mode: Main

☑ NAT Traversal

Keep-alive Interval: 20 seconds

☐ IKE Keep-alive

Message Interval: 30 seconds

Max failures: 5

☑ Dead Peer Detection (RFC3706)

Traffic idle timeout: 20 seconds

Max retries: 5

Transform Settings

PHASE 1 TRANSFORM	KEY GROUP
SHA2-256-AES(256-bit)	Diffie-Hellman Group 14

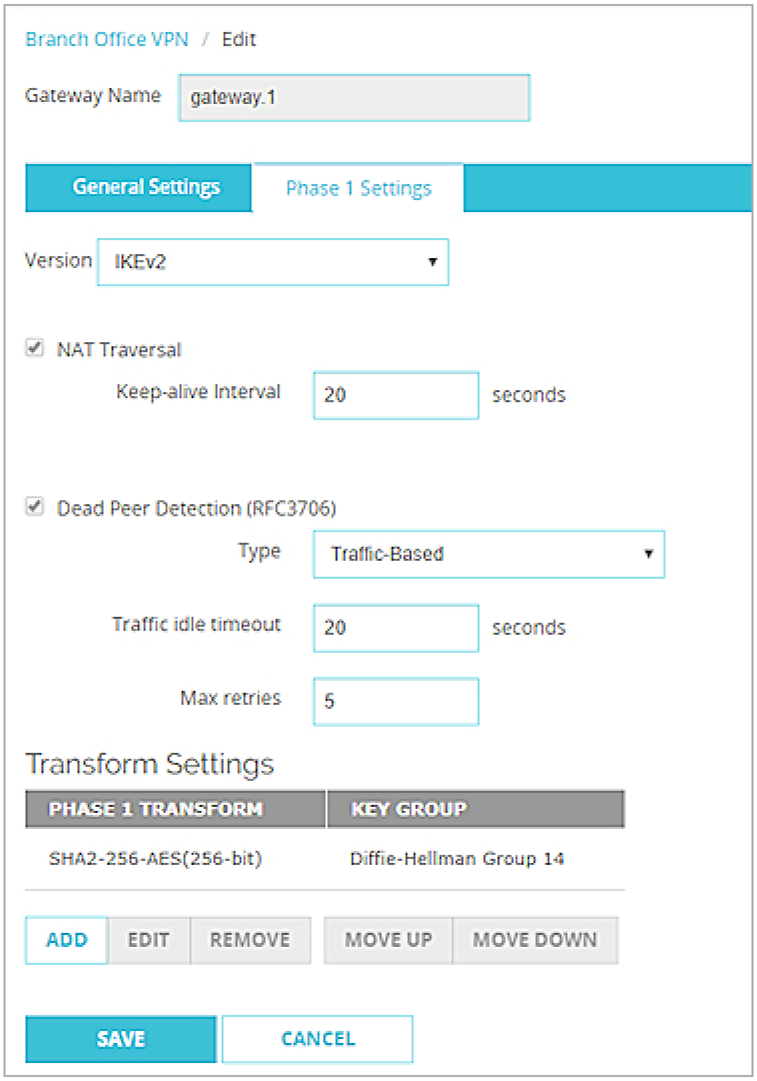
4. From the **Mode** drop-down list, select **Main**.

5. If you want to build a BOVPN tunnel between the Firebox and another device that is behind a NAT device, select the **NAT Traversal** check box. NAT Traversal, or UDP Encapsulation, enables traffic to get to the correct destinations.
6. In the **Keep-alive Interval** text box, type or select the number of seconds that pass before the next NAT keep-alive message is sent.
7. To have the Firebox send messages to the IKE peer to keep the VPN tunnel open, select the **IKE Keep-alive** check box.
8. In the **Message Interval** text box, type or select the number of seconds that pass before the next IKE keep-alive message is sent.
9. To set the maximum number of times the Firebox tries to send an IKE keep-alive message before it tries to negotiate Phase 1 again, type a number in the **Max failures** text box.
10. To enable or disable traffic-based dead peer detection, select or clear the **Dead Peer Detection** check box.
11. In the **Traffic idle timeout** text box, type or select the amount of time (in seconds) that passes before the Firebox tries to connect to the peer.
12. The Firebox contains one default transform set, which appears in the **Transform Settings** list. This transform specifies SHA2 authentication, AES (256-bit) encryption, and Diffie-Hellman Group 14.

Configure Phase 1 Settings For IKEv2

To configure Phase 1 settings for IKEv2, from Fireware Web UI:

1. From the **Version** drop-down list, select **IKEv2**.



Branch Office VPN / Edit

Gateway Name: gateway.1

Version: IKEv2

☑ NAT Traversal

Keep-alive Interval: 20 seconds

☑ Dead Peer Detection (RFC3706)

Type: Traffic-Based

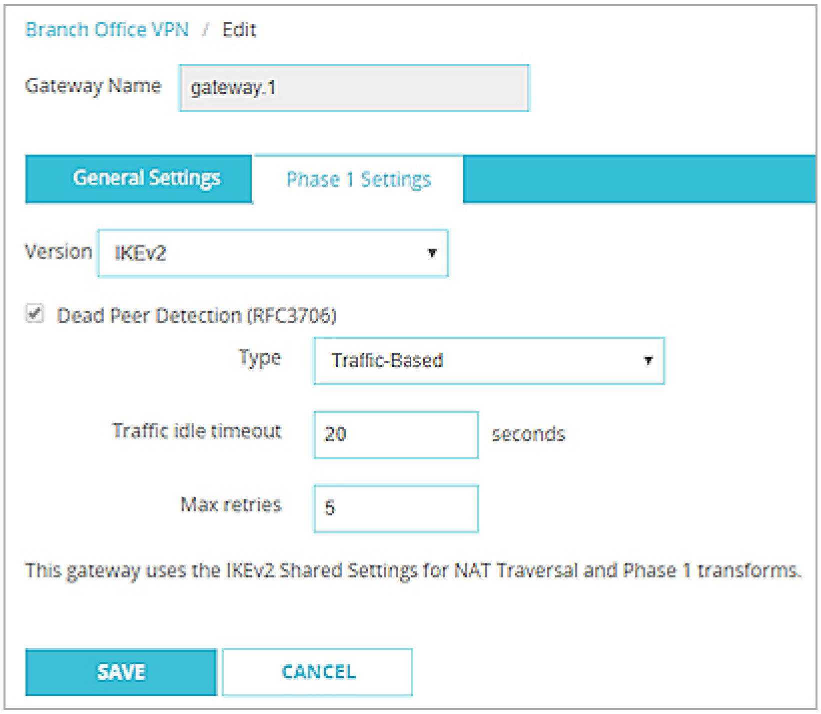
Traffic idle timeout: 20 seconds

Max retries: 5

Transform Settings

PHASE 1 TRANSFORM	KEY GROUP
SHA2-256-AES(256-bit)	Diffie-Hellman Group 14

ⓘ If the gateway has a peer with a dynamic IP address, the gateway uses shared IKEv2 settings and the NAT Traversal and Transform Settings are not visible in the gateway configuration. After you add the gateway, select **VPN > IKEv2 Shared Settings** to see and edit these shared settings.



Gateway Name: gateway.1

Version: IKEv2

☑ Dead Peer Detection (RFC3706)

Type: Traffic-Based

Traffic idle timeout: 20 seconds

Max retries: 5

This gateway uses the IKEv2 Shared Settings for NAT Traversal and Phase 1 transforms.

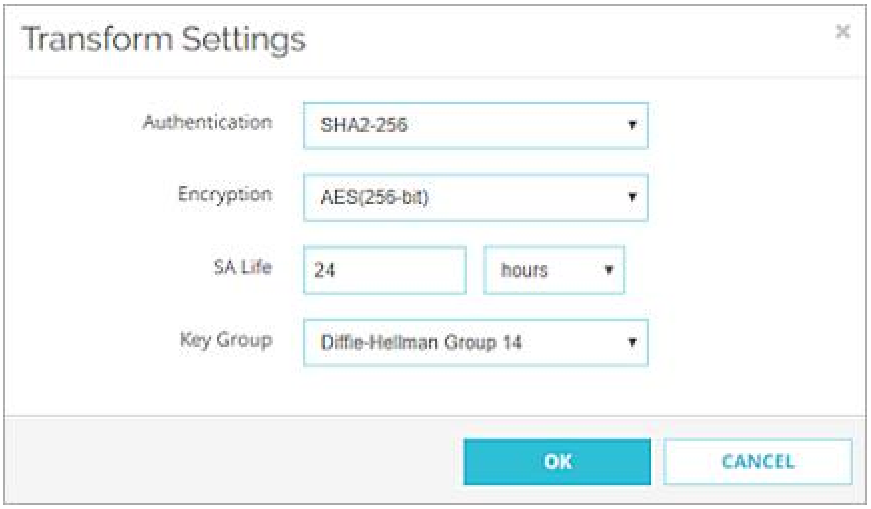
2. For a gateway that does not use IKEv2 shared settings, to change the NAT Traversal keep-alive interval, in the **Keep-alive Interval** text box, type or select the number of seconds between NAT keep-alive messages sent by the Firebox.
3. In the **Dead Peer Detection** settings, from the **Type** drop-down list, select **Traffic-Based** or **Timer-Based**.
4. Configure the DPD settings. The recommended settings are selected by default.
5. For a gateway that does not use IKEv2 shared settings, you can edit the transform settings in the gateway configuration. The Firebox contains one default transform set, which appears in the **Transform Settings** list. This transform specifies SHA2 authentication, AES (256-bit) encryption, and Diffie-Hellman Group 14.

Add a Phase 1 Transform

The default phase 1 transform is compliant with Common Criteria requirements. You can also add other phase 1 transforms.

To add a Phase 1 transform, from Fireware Web UI:

1. When you add or edit a gateway, on the **Gateway** page, select the **Phase 1 Settings** tab.
2. If the gateway uses IKEv2 and has a remote gateway with a dynamic IP address, the BOVPN uses shared Phase 1 settings, and the Phase 1 transform list does not appear in the Phase 1 Settings tab. To edit the shared settings, select **VPN > IKEv2 Shared Settings**.
3. In the **Transform Settings** section, click **Add**.
   The Transform Settings dialog box appears.



Transform Settings

Authentication: SHA2-256

Encryption: AES(256-bit)

SA Life: 24 hours

Key Group: Diffie-Hellman Group 14

3. From the **Authentication** drop-down list, select **SHA1**, **SHA2-256**, **SHA2-384**, or **SHA2-512** as the authentication method.
4. From the **Encryption** drop-down list, select a compliant encryption type.
   - **AES (128-bit)** — AES-CBC algorithm
   - **AES (192-bit)** — AES-CBC algorithm
   - **AES (256-bit)** — AES-CBC algorithm
   - **AES-GCM (128-bit)** — supported with IKEv2 only
   - **AES-GCM (256-bit)** — supported with IKEv2 only
5. To change the SA (security association) life, type a number in the **SA Life** text box, and select **Hour** or **Minute** from the adjacent drop-down list. The SA life must be a number smaller than 596,523 hours or 35,791,394 minutes.
6. From the **Key Group** drop-down list, select Diffie-Hellman Group 14, 19, or 20.
   Diffie-Hellman groups determine the strength of the master key used in the key exchange process. A compliant configuration must use Group 14, 19, or 20.
7. Click **OK**.
   The Transform appears in the New Gateway page in the Transform Settings list. You can add up to nine transform sets.
8. Repeat Steps 2—7 to add more transforms. The transform set at the top of the list is used first.

9. To change the priority of a transform set, select the transform set and click **Up** or **Down**.
10. Click **OK**.

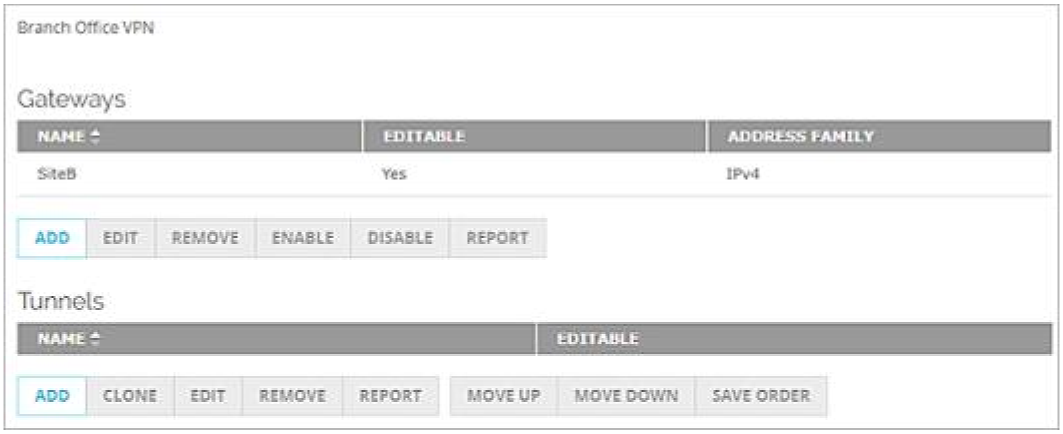
Configure a BOVPN Tunnel

After you define manual VPN gateway endpoints, you can make tunnels between them. To make a tunnel, you must define the tunnel, and configure Phase 2 settings for the Internet Key Exchange (IKE) negotiation. This phase sets up security associations for the encryption of data packets.

Add a Tunnel

To add a tunnel, from Fireware Web UI:

1. Select **VPN > Branch Office VPN**.
   The Branch Office VPN page appears.



Branch Office VPN

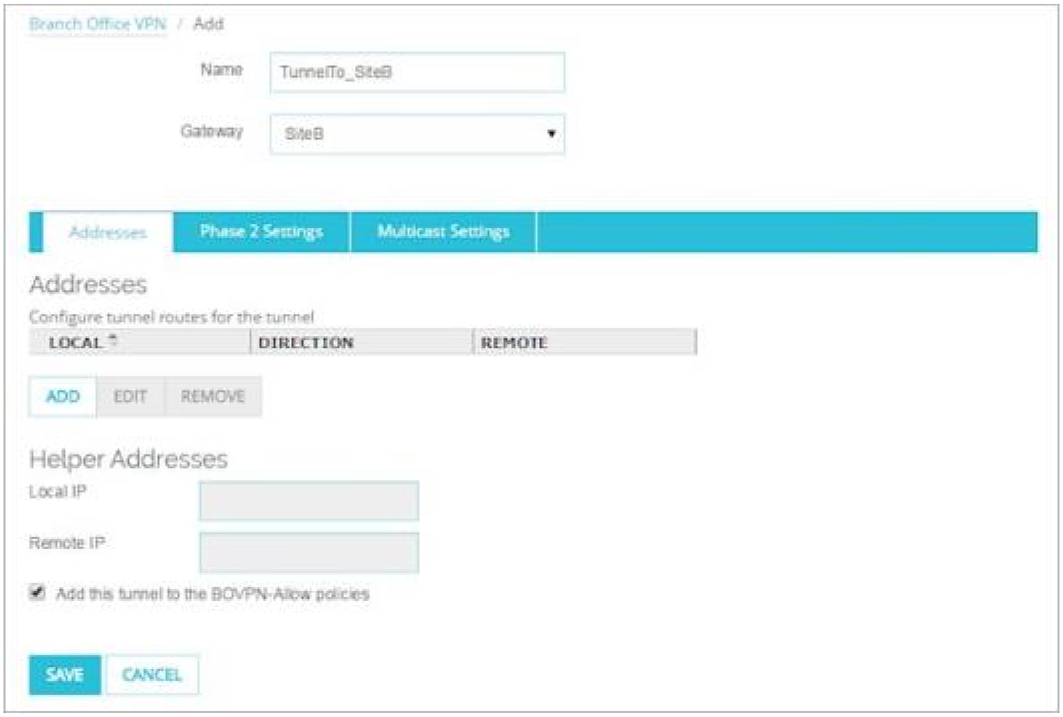
Gateways

NAME	EDITABLE	ADDRESS FAMILY
SiteB	Yes	IPv4

Tunnels

NAME	EDITABLE

2. In the **Tunnels** section, click **Add**.
   The New Tunnel dialog box appears.



Branch Office VPN / Add

Name: TunnelTo_SiteB

Gateway: SiteB

Addresses

Configure tunnel routes for the tunnel

LOCAL	DIRECTION	REMOTE

Helper Addresses

Local IP:

Remote IP:

☑ Add this tunnel to the BOVPN-Allow policies

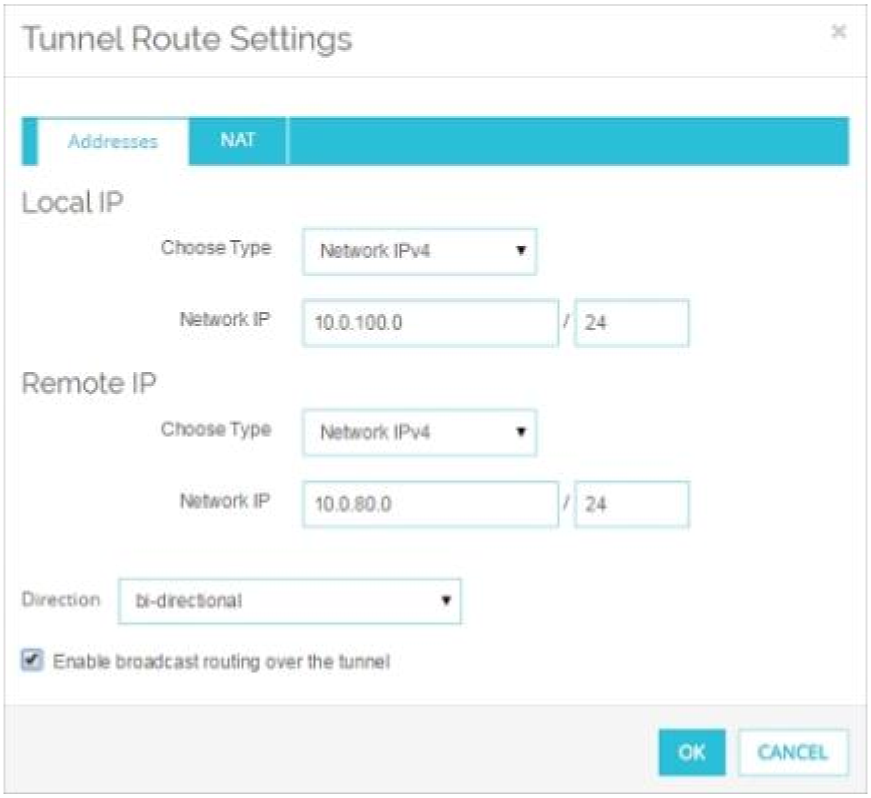
3. In the **Name** text box, type a name for the tunnel.
4. From the **Gateway** drop-down list, select the BOVPN gateway for this tunnel to use.
5. To add the tunnel to the BOVPN-Allow.in and BOVPN-Allow.out policies, select the **Add this tunnel to the BOVPN-Allow policies** check box. These policies allow all traffic that matches the routes for this tunnel.
   To restrict traffic through the tunnel, clear this check box and create custom policies for types of traffic that you want to allow through the tunnel.
6. Add at least one tunnel route, as described in the next section.

Add a Tunnel Route

Tunnel routes define what traffic is allowed through the tunnel.

To add a tunnel route, from Fireware Web UI:

1. On the **Addresses** tab of the **Tunnel** dialog box, click **Add**.
   The Tunnel Route Settings dialog box appears.



Local IP

Choose Type: Network IPv4

Network IP: 10.0.100.0 / 24

Remote IP

Choose Type: Network IPv4

Network IP: 10.0.80.0 / 24

Direction: bi-directional

☑ Enable broadcast routing over the tunnel

2. In the **Local IP** and **Remote IP** sections, select the address type from the **Choose Type** drop-down list. You can specify a host IP address, network address, or a range of host IP addresses. You can also select **Any IPv4** or **Any IPv6**.
3. In the adjacent text boxes, type the values. The IP address you specify must be of the same address family (IPv4 or IPv6) as the gateway.
4. In the **Direction** drop-down list, select the direction for the tunnel. The tunnel direction determines which direction traffic can flow through the tunnel.
5. If you want to enable broadcast routing over this tunnel, select the **Enable broadcast routing over the tunnel** check box.
6. You can use the NAT tab to enable 1-to-1 NAT and dynamic NAT for the tunnel if the address types and tunnel direction you selected are compatible.
7. Click **OK**.

Configure Phase 2 Settings

Phase 2 settings include settings for a security association (SA), which defines how data packets are secured when they are passed between two endpoints. The SA keeps all information necessary for the Firebox to handle traffic between the endpoints. Parameters in the SA can include:

- Encryption and authentication algorithms used.
- Lifetime of the SA (in seconds or number of bytes, or both).
  - Valid SA lifetime (Force Key Expiration) ranges:
    - **Time**: 1 minute - 35791394 minutes
    - **Traffic**: 24576 - 2147483647 kilobytes
  - Preconfigured Phase 2 proposals have a lifetime of 8 hours (480 minutes) and do not expire based on traffic.
- The IP address of the device for which the SA is established (the device that handles IPSec encryption and decryption on the other side of the VPN, not the computer behind it that sends or receives traffic).
- Source and destination IP addresses of traffic to which the SA applies.
- Direction of traffic to which the SA applies (there is one SA for each direction of traffic, incoming and outgoing).

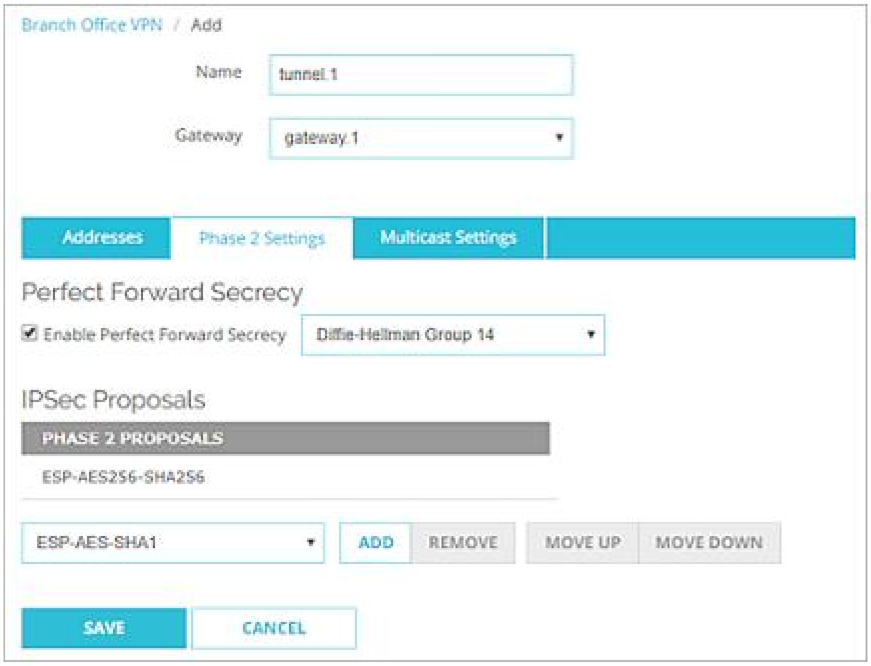
You can add more than one Phase 2 proposal in the Phase 2 Settings tab. However, you cannot add AH and ESP phase 2 proposals to the IPSec Proposals list for the same VPN tunnel.

If you plan to use the IPSec pass-through feature, you must use a proposal with ESP (Encapsulating Security Payload) as the proposal method. IPSec pass-through supports ESP but not AH.

The Phase 2 Settings also include a setting for Perfect Forward Secrecy (PFS). Perfect Forward Secrecy gives more protection to keys that are created in a session. Keys made with PFS are not made from a previous key. If a previous key is compromised after a session, your new session keys are secure.

To configure Phase 2 settings, from Fireware Web UI:

1. From the **Branch Office VPN** page for a tunnel, select the **Phase 2 Settings** tab.



Branch Office VPN / Add

Name: tunnel.1

Gateway: gateway.1

Perfect Forward Secrecy

☑ Enable Perfect Forward Secrecy: Diffie-Hellman Group 14

IPSec Proposals

PHASE 2 PROPOSALS
ESP-AES256-SHA256

ESP-AES-SHA1

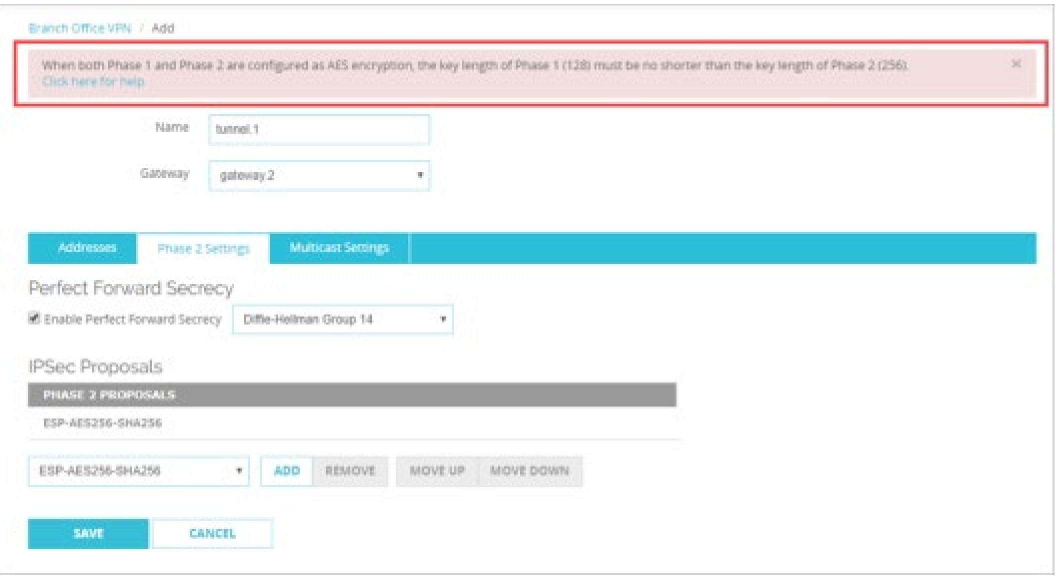
2. By default, Perfect Forward Secrecy (PFS) is enabled, and Diffie-Hellman Group 14 is specified.

> ⓘ To be compliant, the Phase 2 proposal must have PFS enabled, and must use Diffie-Hellman group 14, 19, or 20.

3. By default, a VPN tunnel contains one default proposal, which appears in the **IPSec Proposals** list. This proposal specifies the ESP data protection method, AES 256-bit encryption, and SHA2-256 authentication. You can select a different proposal from the drop-down list and click **Add**.

If the proposal you want to use is not in the list, you can add an additional proposal, as explained in the next section.

> ⓘ The security strength of the Phase 2 settings for a VPN Tunnel cannot exceed the security strength of the Phase 1 settings configured in the VPN gateway. For example, if you attempt to configure the IPSec Proposal for a tunnel to use a longer key than is configured in the gateway Phase 1 transform settings, an error message appears and you cannot save the tunnel configuration.



When both Phase 1 and Phase 2 are configured as AES encryption, the key length of Phase 1 (128) must be no shorter than the key length of Phase 2 (256).
Click here for help

Name: tunnel.1

Gateway: gateway.2

☑ Enable Perfect Forward Secrecy: Diffie-Hellman Group 14

ESP-AES256-SHA256

ESP-AES256-SHA256

Example error message when Phase 2 security settings are stronger than Phase 1 settings.

Add a New Phase 2 Proposal

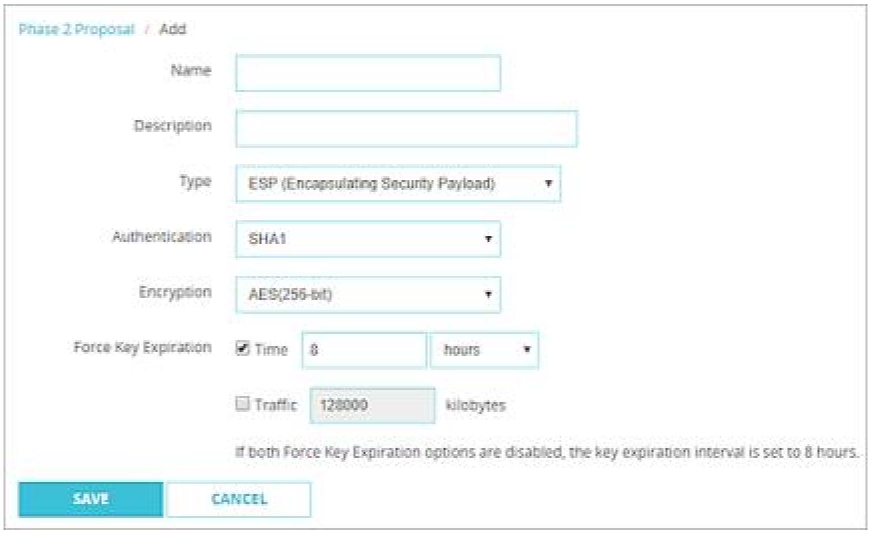
You can configure a tunnel to offer a peer more than one proposal for Phase 2 of the IKE. For example, you could specify [ESP]-[AES256]-[SHA2-256] in one proposal and [ESP]-[AES128]-[SHA1] in a second proposal. When traffic passes through the tunnel, the security association can use either [ESP]-[AES256]-[SHA2-256] or [ESP]-[AES128]-[SHA1] to match the transform settings on the peer.

You can add a maximum of eight proposals to a tunnel configuration. The tunnel uses the configured proposals in the order they are listed in the tunnel configuration.

There are 11 preconfigured Phase 2 proposals, which are not editable. The names follow the format <Type>-<Authentication>-<Encryption>. For all six, the **Force Key Expiration** setting for **Time** is configured for 8 hours.

To create a new Phase 2 proposal, from Fireware Web UI:

1. Select **VPN > Phase 2 Proposals**.
2. Click **Add**.



Phase 2 Proposal / Add

Name

Description

Type: ESP (Encapsulating Security Payload)

Authentication: SHA1

Encryption: AES(256-bit)

Force Key Expiration: ☑ Time 8 hours

☐ Traffic 128000 kilobytes

If both Force Key Expiration options are disabled, the key expiration interval is set to 8 hours.

3. In the **Name** text box, type a name for the new proposal.
4. (Optional) In the **Description** text box, type a description to identify this proposal.
5. From the **Type** drop-down list, select **ESP** or **AH**.
6. From the **Authentication** drop-down list, select one of these authentication methods: **SHA1**, **SHA2-256**, **SHA2-384**, and **SHA2-512**.
7. If you selected **ESP** from the **Type** drop-down list, from the **Encryption** drop-down list, select the encryption method.
   Select one of these options: **AES (128-bit)**, **AES (192-bit)**, **AES (256-bit)**, **AES-GCM (128-bit)**, **AES-GCM (256-bit)**.
8. To force the gateway endpoints to generate and exchange new keys after a quantity of time or amount of traffic passes, configure the settings in the **Force Key Expiration** section.
   - Select the **Time** check box to expire the key after a quantity of time. Type or select the quantity of time that must pass to force the key to expire.
   - Select the **Traffic** check box to expire the key after a quantity of traffic. Type or select the number of kilobytes of traffic that must pass to force the key to expire. This option provides better VPN interoperability with third-party devices.
   - If both Force Key Expiration options are disabled, the key expiration interval is set to 8 hours.

Use a Certificate for BOVPN Authentication

By default, the BOVPN uses a shared secret for authentication. You can also use a certificate for BOVPN authentication.

To use a certificate for BOVPN authentication:

- The certificate must be a web server certificate.
- Certificates for the devices at each gateway endpoint must use the same algorithm. Both endpoints must use DSS, RSA, or EC. The algorithm for certificates appears on the Branch Office VPN page in the **Gateway** list.
- The Subject Alternative Name (SAN) value in the certificate must not contain more than one IP address.

Import the Certificate

Before you can configure the BOVPN to use a certificate for authentication, you must import a web server certificate to the Firebox. When you import the web server certificate, you must also import the CA certificate and any intermediate certificates in the chain of trust.

For information about how to create and import the web server certificate, see *Web Server Certificate*.

Configure the BOVPN to Use the Certificate

After you import a web server certificate, you can use it in your BOVPN configuration.

To use a certificate for BOVPN tunnel authentication, from Fireware Web UI:

1. Select **VPN > Branch Office VPN**.
2. To create a new gateway, in the **Gateways** section, click **Add**.
   Or, select an existing gateway and click **Edit**.
3. Select **Use IPSec Firebox Certificate**.
4. Select the **Show All Certificates** check box.
   All available certificates appear.
5. Select the web server certificate to use.

After you select the web server certificate, you can specify a CA certificate for remote endpoint verification:

1. In the **Gateway Endpoints** section, edit the gateway endpoint.
2. Click **Edit**.
3. Select the **Advanced** tab.
4. In the **CA Certificate** section, select the **Specify a CA certificate for remote endpoint verification** check box.
5. From the **CA Certificate** drop-down list, select the root or intermediate CA certificate.
6. Click **OK**.
7. Click **Save**.

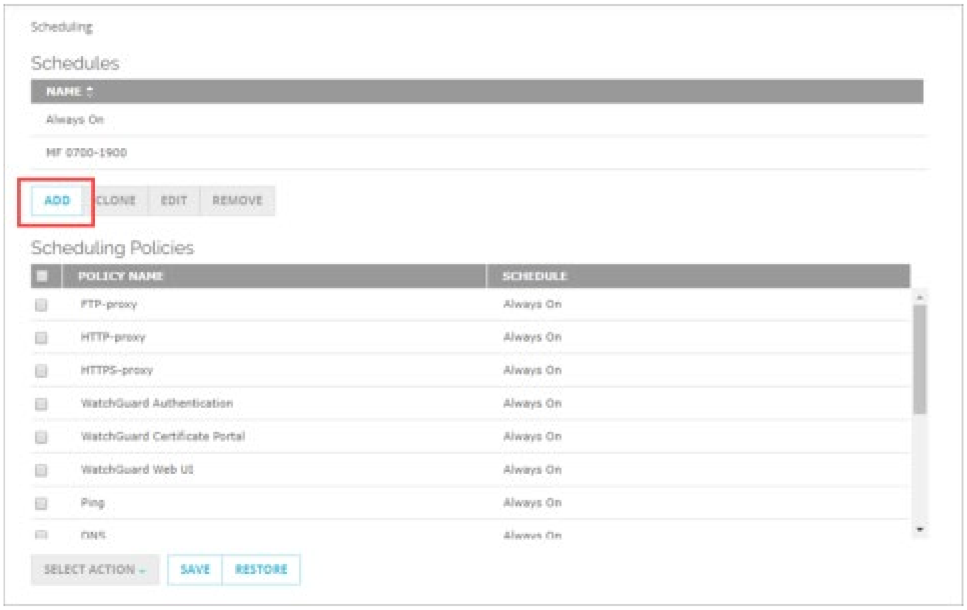
Control VPN Connections Based on Time of Day

Tunnel policies are sets of rules that apply to connections through a BOVPN tunnel. By default, any new manual VPN tunnel you add is automatically added to the **BOVPN-Allow.in** and **BOVPN-Allow.out** policies, which allow all traffic through the tunnel. In the tunnel settings, you can clear the **Add this tunnel to the BOVPN-Allow policies** check box so that the tunnel is not added to these policies.

By default, tunnel policies are always on. To allow BOVPN connections only at specific times of day, you can edit the schedule for these policies.

To create a policy schedule, from Fireware Web UI:

1. Select **Firewall > Scheduling**.
   The Scheduling page appears.



Scheduling

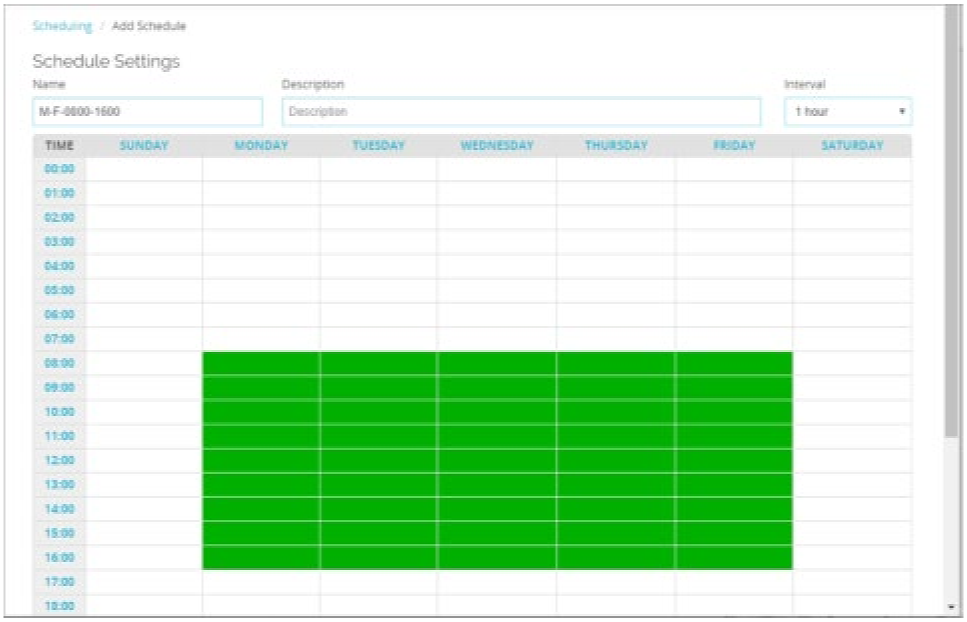
Schedules

NAME ⇕
Always On
MF 0700-1900

Scheduling Policies

☐	POLICY NAME	SCHEDULE
☐	FTP-proxy	Always On
☐	HTTP-proxy	Always On
☐	HTTPS-proxy	Always On
☐	WatchGuard Authentication	Always On
☐	WatchGuard Certificate Portal	Always On
☐	WatchGuard Web UI	Always On
☐	Ping	Always On
☐	DNS	Always On

2. In the **Schedules** section, click **Add**.



Scheduling / Add Schedule

Schedule Settings

Name: M-F-0800-1600

Description: Description

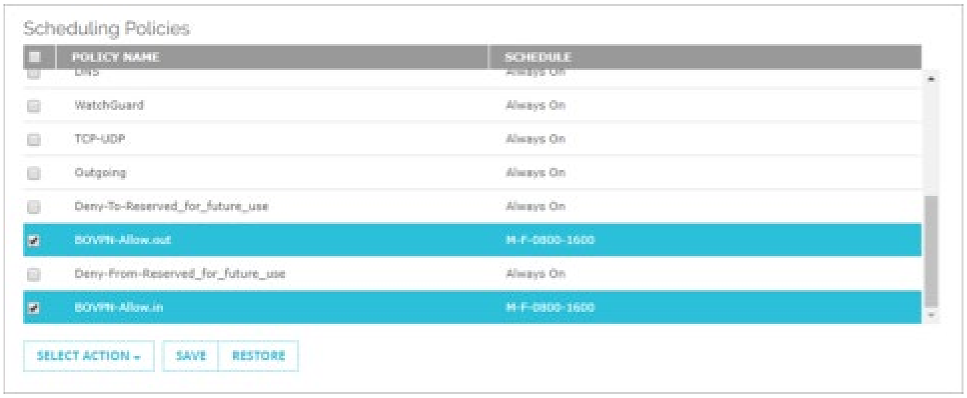
Interval: 1 hour

TIME	SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
00:00							
01:00							
02:00							
03:00							
04:00							
05:00							
06:00							
07:00							
08:00		🟩	🟩	🟩	🟩	🟩	
09:00		🟩	🟩	🟩	🟩	🟩	
10:00		🟩	🟩	🟩	🟩	🟩	
11:00		🟩	🟩	🟩	🟩	🟩	
12:00		🟩	🟩	🟩	🟩	🟩	
13:00		🟩	🟩	🟩	🟩	🟩	
14:00		🟩	🟩	🟩	🟩	🟩	
15:00		🟩	🟩	🟩	🟩	🟩	
16:00		🟩	🟩	🟩	🟩	🟩	
17:00							
18:00							

3. In the **Name** text box, type a descriptive name for the schedule.
4. Click the grid to select the times for the schedule to operate for each day of the week.
5. To save the schedule, click **Save**.

To apply the new schedule to the default BOVPN policies:

1. In the **Scheduling Policies** list, select the check box for the **BOVPN-Allow.out** and **BOVPN-Allow.in** policies.
2. From the **Select Action** drop-down list, select a schedule to apply to the policies you selected.



Scheduling Policies

□	POLICY NAME	SCHEDULE
□	DNS	Always On
□	WatchGuard	Always On
□	TCP-UDP	Always On
□	Outgoing	Always On
□	Deny-To-Reserved_for_future_use	Always On
☑	BOVPN-Allow.out	M-F-0800-1600
□	Deny-From-Reserved_for_future_use	Always On
☑	BOVPN-Allow.in	M-F-0800-1600

3. Click **Save**.

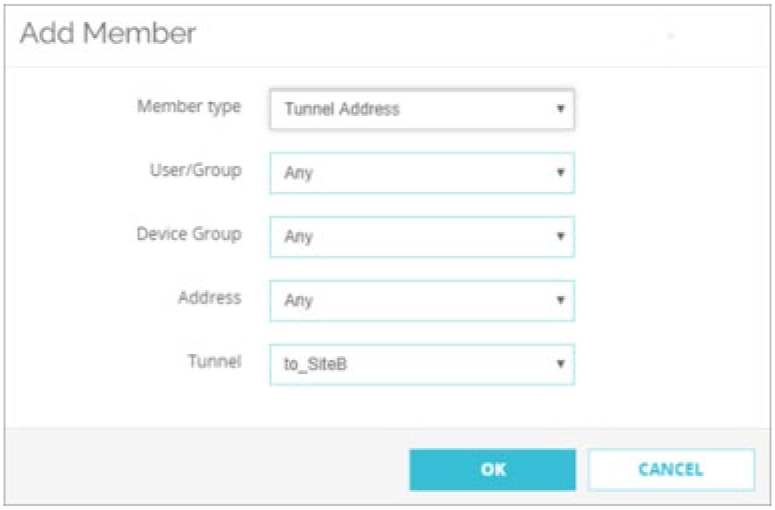
To apply policy schedules to custom firewall policies that apply to VPN traffic, or to any other policy, follow the same steps, and select the policy to apply the schedule to. You can also edit the policy schedule when you edit the Firewall policy.

Add Custom Firewall Policies for VPN Traffic

The default BOVPN policies allow all traffic through all VPN tunnels. You can also add firewall policies to control specific types of inbound and outbound traffic through a specific tunnel. To create a firewall policy that applies to traffic to or from a BOVPN tunnel, specify the tunnel name in the policy source (From) or destination (To) lists.

To specify a tunnel as the source or destination of a firewall policy,

1. Select **Firewall > Policies**.
2. Add or edit the firewall policy for the type of traffic to allow.
3. On the **Settings** tab, below the **From** or **To** list, click **Add**.
   The Add Member dialog box appears.
4. From the **Member Type** list, select **Tunnel**.



Add Member

Member type: Tunnel Address
User/Group: Any
Device Group: Any
Address: Any
Tunnel: to_SiteB

5. From the **Tunnel** drop-down list, select the VPN tunnel.
6. Click **OK**.
   The tunnel name is added to the policy From or To list.

For more information about policy properties, see *Firewall Policies and Security Services*.

Troubleshoot Connections to External IT Entities

For the Firebox to function, it must be able to connect to some external IT entities, such as NTP servers and syslog servers.

For the Firebox to connect to an external IT entity, the Firebox must have:

- Functioning DNS to resolve domain names.
- A network route to the external IT entity.
- A Firewall policy to allow the connection.
- A consistent network connection.
- For a connection through a VPN, a correctly configured VPN connection.

To troubleshoot connection issues, you can try these basic steps:

- Verify that cables are securely and correctly connected, and are not damaged.
- Verify that both devices are powered on and have a connection to the intermediate network.
- To reset all connections, reboot both the external IT entity and the Firebox.
- To identify errors, examine log messages on both the external IT entity and the Firebox.

On the Firebox, you can use the **Dashboard** and **System Status** pages to see the status of Firebox connections, and to run diagnostic tasks and reports useful for connection troubleshooting. These are described in the sections below.

To troubleshoot general connection issues:

- Verify Interface Connection Status
- Verify DNS Functionality
- Run Network Diagnostic Tasks

To troubleshoot connections through a VPN:

- Run the VPN Diagnostics Report
- Force a VPN Tunnel Rekey

Other dashboards and system status pages in Fireware Web UI might provide additional information needed to troubleshoot connection issues.

Verify Interface Connection Status

Verify the status of interfaces from Fireware Web UI. On the **Dashboard > Interfaces** page, three tabs show detailed information about each Firebox interface:

- Bandwidth — Amount of data sent and received on all interfaces
- Details — Link status (up or down), interface status (enabled or disabled), link speed
- SD-WAN — Loss, latency, and jitter metrics for monitored interfaces.

Look at Firebox Log Messages

The Firebox generates log messages when it denies a connection. You can look at the log messages on your syslog server, if you have one. If you do not have an external syslog server, or if the Firebox cannot send messages to your syslog server, you can look at recent messages on the Firebox for troubleshooting. To see log messages on the Firebox, select **Dashboard > Traffic Monitor**. You can monitor the log messages while the Firebox tries to connect, to see if a policy blocks the connection. In Traffic Monitor you can search log messages and filter by log message type. To see denied connections, search for log messages that contain **Deny**.

For more information about Traffic Monitor, see *Audit Logging*.

Verify DNS Functionality

If the Firebox uses a domain name to connect to an external IT entity, it must be able to resolve the domain name to an IP address. If you suspect DNS resolution is a problem, you can use Fireware Web UI to see DNS servers and test DNS resolution from the Firebox. If necessary, you can also update the DNS server configuration.

To see the DNS servers the Firebox currently uses, from Fireware Web UI:

1. Select **Dashboard > Interfaces**.
2. Select the **Detail** tab.
   The DNS Servers list is below the list of interfaces.

To test DNS resolution to a specific host, from Fireware Web UI:

1. Select **System Status > Diagnostics**.
2. Select the **Network** tab.
3. From the **Task** drop-down list, select **DNS Lookup**.
4. In the **Address** text box, type the domain name to look up.
5. Click **Run Task**.

To configure DNS servers the Firebox connects to, from Fireware Web UI:

1. Select **Network > Interfaces**.
   The Interfaces configuration page appears.
2. Select the **DNS/WINS** tab.
3. (Optional) In the **Domain Name** text box, type a domain name that a DHCP client adds to unqualified host names.
4. In the **DNS Server** text box, type the primary IP address for the DNS server.
5. Click **Add**.
6. Click **Save**.

Run Network Diagnostic Tasks

You can use the Diagnostic Tasks tool in Fireware Web UI to help you debug problems on your network. You can ping the source or destination IP address, trace the route to the source or destination IP address, look up DNS information for an IP address, or see information about the packets transmitted across your network (TCP dump). You can also include arguments in your task details to narrow the results. Firebox diagnostics supports these tasks:

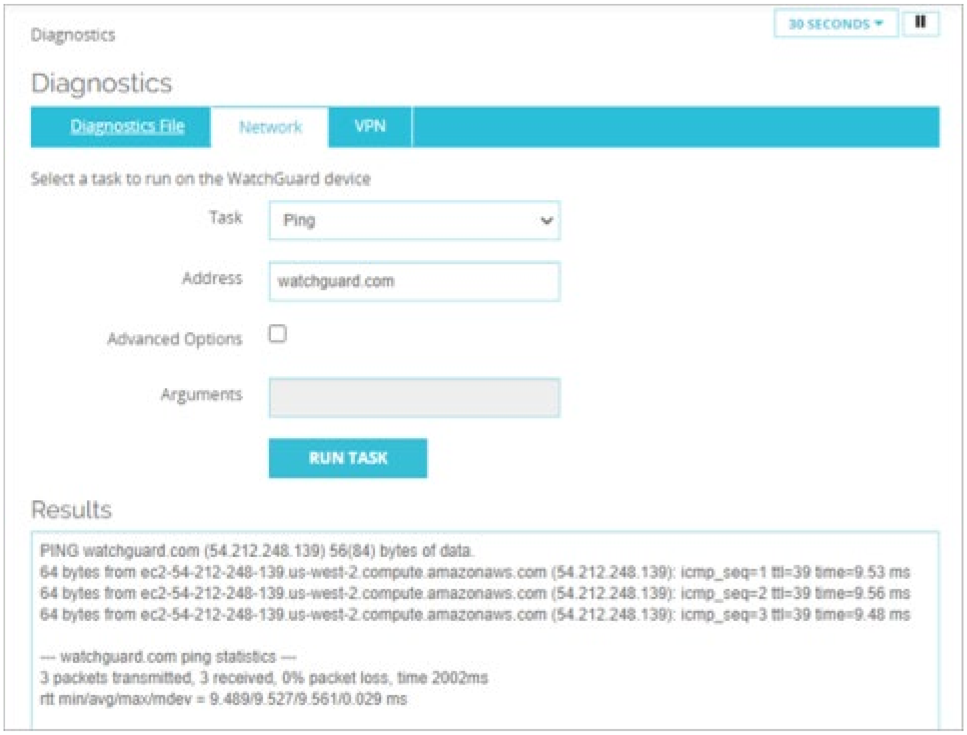
- Ping
- traceroute
- DNS Lookup
- TCP Dump

To run diagnostic tasks for your Firebox:

1. Select **System Status > Diagnostics**.
   The Diagnostics page appears with the Diagnostics File tab selected.
2. Select the **Network** tab.
3. Run a basic or advanced diagnostic task, as described in the next sections.

Run a Basic Diagnostics Command

1. From the **Task** drop-down list, select a command.
2. If you select **Ping**, **traceroute**, or **DNS Lookup**, in the **Address** text box, type an IP address or host name.
   If you select **TCP Dump**, from the **Interface** drop-down list, select an interface.
3. Click **Run Task**.
   The output of the command appears in the Results window.



Select a task to run on the WatchGuard device

Task: Ping

Address: watchguard.com

Advanced Options ☐

Arguments

```
PING watchguard.com (54.212.248.139) 56(84) bytes of data.
64 bytes from ec2-54-212-248-139.us-west-2.compute.amazonaws.com (54.212.248.139): icmp_seq=1 ttl=39 time=9.53 ms
64 bytes from ec2-54-212-248-139.us-west-2.compute.amazonaws.com (54.212.248.139): icmp_seq=2 ttl=39 time=9.56 ms
64 bytes from ec2-54-212-248-139.us-west-2.compute.amazonaws.com (54.212.248.139): icmp_seq=3 ttl=39 time=9.48 ms

--- watchguard.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 9.489/9.527/9.561/0.029 ms
```

Example output for the Ping diagnostic task.

Use Command Arguments

1. From the **Task** drop-down list, select a command.
2. Select the **Advanced Options** check box.
   The Arguments text box is enabled and the Address or Interface text box is disabled.
3. In the **Arguments** text box, type the command arguments.
   To see the available arguments for a command, leave the **Arguments** text box blank.
4. Click **Run Task**.
   The output of the command appears in the Results window and the Stop Task button appears.
5. To stop the diagnostic task, click **Stop Task**.

Download a PCAP File

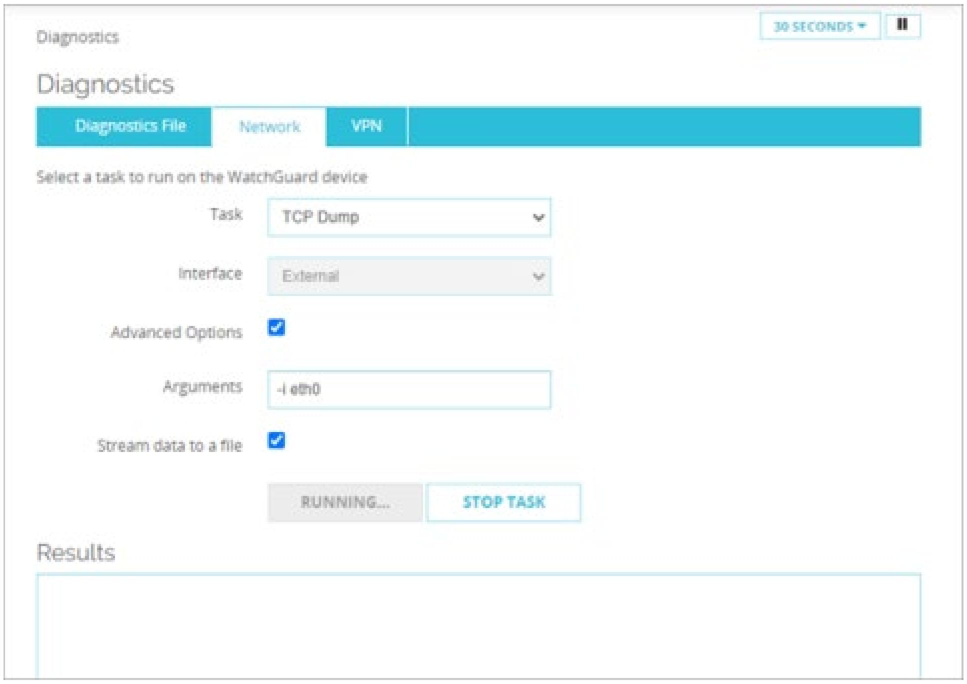
From the **Diagnostics** page, you can download a packet capture (PCAP) file to help you diagnose problems with the traffic on your network. The PCAP file captures the results of the most recent TCP dump task that you run so you can review the protocols found in the task results outside of the **Diagnostics** page.

When you enable the **Advanced Options** to include arguments in the TCP dump task, you must specify an interface. This can be a physical interface on the Firebox (such as *eth0*), a Link Aggregation interface (such as *bond0*), or a VLAN interface (such as *vlan10*). If you specify a VLAN or bridge interface, and the traffic matches a proxy rule, TCP dump only captures the first incoming packet on that interface. To capture all packets, you must run the TCP dump task on the physical interface from where the packets originate.

You can save a PCAP output to a file. To open the PCAP file, you use a third-party application, such as Wireshark. You can then review the protocols included in the file and resolve issues in your network configuration. The maximum size of the PCAP file is 30 MB. If your Firebox has limited memory, the size of the PCAP file is constrained relative to the available memory available on your device.

To save the TCP dump data directly to a PCAP file:

1. Select **System Status > Diagnostics**.
   The Diagnostics page appears with the Diagnostics File tab selected.
2. Select the **Network** tab.
   The Network page appears.
3. From the **Task** drop-down list, select **TCP Dump**.
   The Interface drop-down list appears.
4. Select the **Advanced Options** check box.
   The advanced options appear.



Task: TCP Dump

Interface: External

Advanced Options: ☑

Arguments: -i eth0

Stream data to a file: ☑

5. In the **Arguments** text box, type the parameters for the search. Parameters are case-sensitive. For example, to capture PCAP data for the default external interface, type `-ieth0` or `-i eth0`.
6. Select the **Stream data to a file** check box.
7. Click **Run Task**.
   The task runs and the Stop Task button and Open or Save File dialog box appear.
8. Save or open the PCAP file.
   If you choose to save the PCAP file, specify a location to save the file and a name for the file.
   If you choose to open the PCAP file, select the third-party application to use to open the file.
9. Click **OK**.
10. When the TCP dump has collected enough results, click **Stop Task**.

Run the VPN Diagnostic Report

To troubleshoot a connection to an external IT entity through a VPN, you can use the VPN Diagnostic Report to see configuration and status information for a VPN gateway and the associated branch office VPN tunnels. When you run the report, the Firebox temporarily increases the log level for the selected gateway. The completed report shows the gateway and tunnel configuration, as well as information about the status of any active tunnels for the selected gateway.

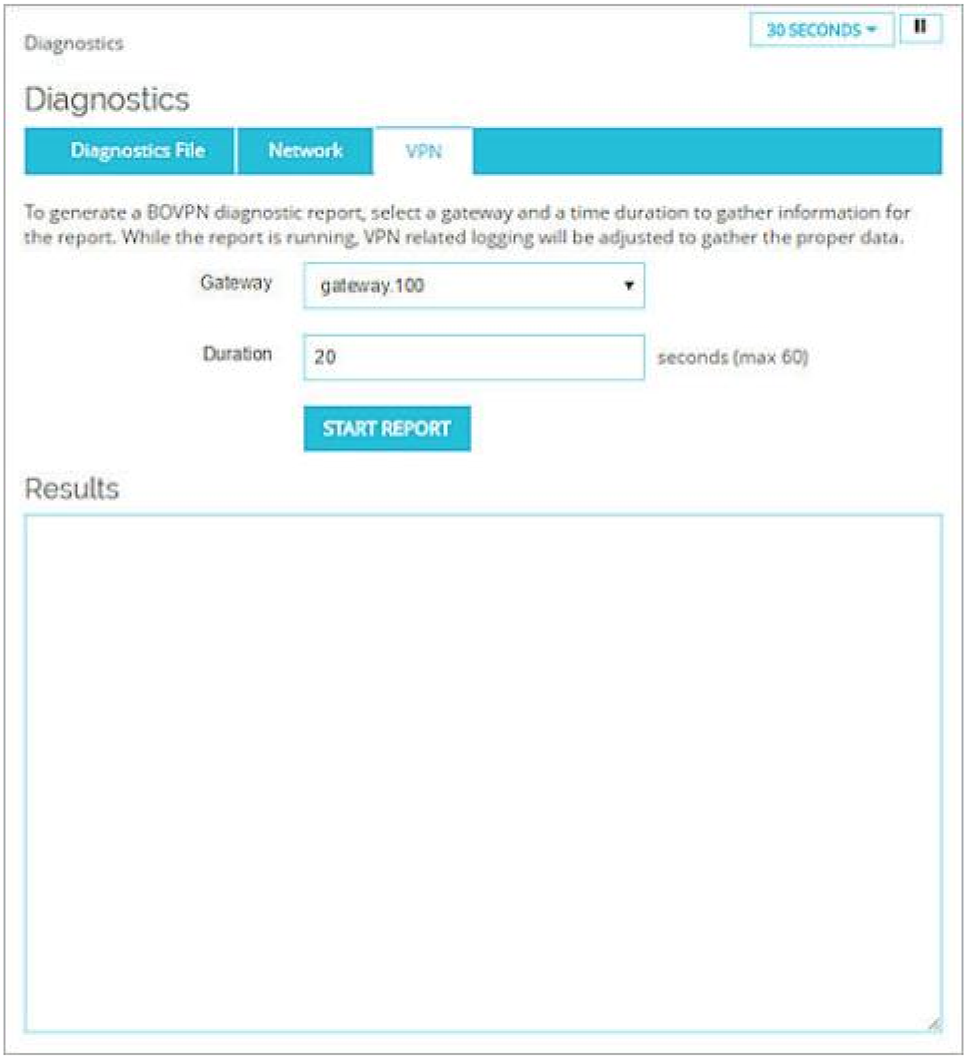
To run the VPN Diagnostic Report from the **Diagnostics** page:

1. Select **System Status > Diagnostics**.

   The Diagnostics page appears with the Diagnostics File tab selected.

2. Select the **VPN** tab.

   The VPN Diagnostic Report options appear.



To generate a BOVPN diagnostic report, select a gateway and a time duration to gather information for the report. While the report is running, VPN related logging will be adjusted to gather the proper data.

Gateway: gateway.100

Duration: 20 seconds (max 60)

3. From the **Gateway** drop-down list, select a VPN gateway.
4. In the **Duration** text box, type the number of seconds to run the VPN Diagnostic Report.

5. Click **Start Report**.
   The diagnostic task starts.

The Firebox collects log messages for the duration you specified. When the task is completed, details about the gateway and tunnel configuration and information about the status of any active tunnels for the selected gateway appear in the **Results** section. The log level is then returned to the previously set level.

VPN Diagnostic Report Details

The VPN Diagnostic Report includes these sections:

Conclusion

This is the complete report summary and can include information about actions you can take to resolve any issues identified by the report. For each tunnel route, the report shows whether the tunnel route was established, whether traffic was detected after the report started, and error messages related to the tunnel. Some error messages include information about what you can do to correct a problem with the VPN tunnel.

Gateway Summary

This is a summary of the gateway configuration and each configured gateway endpoint.

Tunnel Summary

This is a summary of the tunnel configuration for all tunnels that use the selected gateway. This includes both active and inactive tunnels.

Run-time Info (bvpn routes)

This section only appears when you run the diagnostic report for a branch office VPN virtual interface. It includes the static and dynamic routes that use the BOVPN virtual interface, and the metric for each route.

Run-time Info (gateway IKE_SA)

The status of the IKE (Phase 1) security association for the gateway.

Run-time Info (tunnel IPSEC_SA)

The status of the IPSec tunnel (Phase 2) security association for active tunnels that use the gateway.

Run-time Info (tunnel IPSec_SP)

The status of the IPSec tunnel (Phase 2) security policy for active tunnels that use the gateway.

Address Pairs in Firewalld

The status of the address pairs for each tunnel. This section does not appear when you run the report for a branch office VPN virtual interface.

Policy checker result

The policies that manage inbound and outbound traffic for each tunnel route.

Related Logs

If tunnel negotiation occurs while the Diagnostic Report runs, the tunnel negotiation log messages appear in this section. If the remote device attempts to negotiate or rekey the tunnel while the report runs, the log messages that appear in this section include more informative details.

Force a VPN Tunnel Rekey

Gateway endpoints automatically generate and exchange new keys after a specified amount of time or traffic passes, as defined in the VPN tunnel Phase 2 settings. If you want to immediately generate new keys instead of waiting for them to expire (particularly when you troubleshoot VPN tunnels), you can choose to rekey one or more IPSec Branch Office VPN (BOVPN) tunnels.

To rekey IPSec VPN tunnels, from Fireware Web UI:

1. Select **System Status > VPN Statistics**.
2. Click the gateway to see the tunnels for that gateway.
3. To rekey a single tunnel, on the line for the VPN tunnel, click **Rekey tunnel**.
4. To rekey all tunnels that use a gateway, on the gateway line, click **Rekey tunnels**.
5. To rekey all branch office VPN tunnels, click **Rekey All Tunnels**.

To change the key expiration settings, edit the Force Key Expiration settings in the Phase 2 Proposals settings for the VPN. For more information, see *IPSec VPN*.