Sophos Firewall Manager

help

product version: 17.1
## Contents

Introduction............................................................................................................................................... 1  
Using Admin Console.............................................................................................................................. 3  
  Supported Browsers.......................................................................................................................... 4  
  Navigating through the Admin Console......................................................................................... 4  
Menus................................................................................................................................................ 6  
Tool Tips........................................................................................................................................... 7  
Notification pop-ups........................................................................................................................... 8  
Common Operations............................................................................................................................ 8  
Device Configuration............................................................................................................................ 12  
  Device Dashboard............................................................................................................................ 12  
  Policy Configuration Tasks............................................................................................................. 14  
  Monitor and Analyze...................................................................................................................... 16  
  Protect.......................................................................................................................................... 19  
  Configure.................................................................................................................................... 182  
System............................................................................................................................................ 282  
Templates......................................................................................................................................... 315  
System & Monitor............................................................................................................................... 316  
  Device Settings.............................................................................................................................. 316  
  Monitor........................................................................................................................................ 348  
  System Settings............................................................................................................................... 358  
Appendix A - Guides.......................................................................................................................... 399  
Copyright notice.................................................................................................................................. 400
1 Introduction

Sophos Firewall Manager (SFM) provides comprehensive central management of Sophos XG Firewall to Enterprises and MSSPs. With a range of features, SFM simplifies security management for actions like rapid deployment of organization-wide security policies and updates for better protection of dispersed networks, offering benefits of reduced cost, complexity and time. Sophos Firewall Manager (SFM) is available in hardware, software and virtual form-factors to suit any environment.

The Sophos Firewall Manager UI offers you 3 work areas: Device Configuration, Template Configuration, and System Management.

Device Configuration

The Device Configuration work area allows you to manage policies and configurations of individual or group of Sophos XG Firewall devices. You can select an individual device or device group and use menu items in the left panel to edit Policies, Settings and Objects like in your Firewall UI.

Template Configuration

The Template Configuration work area allows you to create re-usable configuration templates allowing you to set up a new firewall at branch or customer office in minimum time. You have an option to add a template using an existing device configuration, clone an existing template, or setup a fresh template. You can edit the template configuration by using menu items in the left panel to edit Policies, Settings and Objects like in your Firewall UI. Once ready, you can provision the template to one or more firewall devices as per your need.

System Management

The System Management work area lets you manage device settings, monitoring settings and your SFM system settings.

- Device settings: You can add or remove managed devices or device groups, add or remove templates, upgrade firmware of managed devices, create and manage dynamic objects, and change control and logging.
- Monitoring settings: You can edit monitoring settings, setup email alerts, view device events and logs, view management system events, and integrate with Sophos iView V2.
- System settings: You can manage SFM users, and set up role-based access, SFM API, Network Settings, Diagnostics, and more.

Dashboards & Monitoring

Sophos Firewall Manager offers multiple dashboards for a quick snapshot and easy monitoring of your managed firewalls.

- Device Monitor
  - Flat view and card view allow you to monitor the status (Critical, Warning, Normal) of managed devices across a set of parameters for Security, Resource, License and Availability, based on their threshold values.
  - In flat view, devices that need attention are automatically listed at the top on the basis of their monitor status.
  - You have the flexibility to customize threshold values for Critical, Warning and Normal levels as per your needs.
- Home and Group-level Dashboard
— Device Info: Summary of managed devices like the count of managed devices, unsynchronized devices, and disconnected devices.

— Device monitor summary: A snapshot of firewall count that requires attention in terms of Security, Resource, License, Availability.

— A list of managed firewalls by their model number, and more.

Group-level dashboard lets you filter the above view for a device group.

• Device Dashboard - It offers you insights into security, resource, license and availability parameters along with device and connection information to enable you to take necessary action

• Alert - Configure alert profiles for one or more firewalls or Firewall group to get alert notifications over email. This includes alert notifications for parameters like subscription expiry, Device disconnected from central management, Device Gateway status change, VPN connection status change, along with counts of Intrusion attack, ATP events exceed, Web virus, Objectionable + Unproductive surfing hits, and percentage of endpoints with Red health exceeding a threshold limit.
2 Using Admin Console

Sophos Firewall Manager uses a Web 2.0 based easy-to-use graphical interface termed as Admin Console to configure and manage the device.

You can access the device for HTTPS web browser-based administration from any of the interfaces. Device when connected and powered up for the first time, it will have a following default Admin Console Access configuration for HTTPS service.

<table>
<thead>
<tr>
<th>Services</th>
<th>Interface/Zones</th>
<th>Default Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>WAN</td>
<td>TCP Port 443</td>
</tr>
</tbody>
</table>

The administrator can update the default port for HTTPS service from **System Management > System Settings > Administration > Settings**

Admin Console Language

The Admin Console supports multiple languages, but by default appears in English. Apart from English, Brazilian-Portuguese, Chinese-Simplified, Chinese-Traditional, French, German, Italian, Japanese, Korean, Russian and Spanish languages are also supported. Administrator can choose the preferred language at the time of logging in.

Administrator can also specify description for various policies, services and custom categories in any of the supported languages.

Log on procedure

The log on procedure authenticates the user and creates a session with the Device until the user logs-off.

To get the login window, open the browser and type LAN IP Address of the device in browser's URL box. A dialog box appears prompting you to enter username and password.

Below are the screen elements with their description:

**Username**

Enter user login name.

If you are logging on for the first time after installation, use the default username.

**Password**

Specify user account password.

Dots are the placeholders in the password field.

If you are logging on for the first time after installation with the default username, use the default password.

**Log on to**

To administer device, select **Admin Console**.

**Login button**

Click to log on the Admin Console.
Home appears as soon as you log on to the Admin Console which provides a quick and fast overview of all the important parameters of your added devices and SFM System.

Log out procedure

To avoid un-authorized users from accessing Sophos Firewall Manager, log off after you have finished working. This will end the session and exit from device.

2.1 Supported Browsers

You can connect to Admin Console of the device using HTTP or a secure HTTPS connection from any management computer using one of the following web browsers:

Latest version of Firefox (recommended), latest version of Chrome, latest version of Safari, or Microsoft Internet Explorer 9 onwards. JavaScript must be enabled.

The minimum screen resolution for the management computer is 1280 X 768.

2.2 Navigating through the Admin Console

The three parts of the admin Console:

• Area Selector
• Navigation Bar
• Content Pane
• Button bar

Use the menus, lists, and configuration pages to configure most settings. Configuration made through Admin Console take effect after some time as it takes time to copy the entire configuration on to the device.

Work Area Selector

The Sophos Firewall Manager UI offers you three work areas: Device Configuration, Template Configuration, and System Management. To select any work area, select the icon on the top right corner of the Home.

Once an area is selected, the Navigation bar changes based on the selected work area.

Device Configuration allows you to navigate through pages through which you can manage Device Groups or individual devices. The navigation bar changes dynamically for Device Group and individual device. You can select device group or any device Device Groups or Device on the Dashboard top panel.

Navigation Bar

The navigation bar on the leftmost side provides access to various configuration pages. Menu consists of sub-menues and tabs. On clicking menu item in the navigation bar, related management
functions are displayed as submenu items. On clicking submenu item, all the associated tabs are displayed. To view page associated with the tab, click the required tab.

The Main menu tree expands and contracts dynamically when clicked on without navigating to a submenu. When you click on a top-level heading, it automatically expands that heading and contracts the heading for the page you are currently on, but it does not navigate away from the current page. To navigate to a new page, first click on the heading, and then click on the submenu you want navigate to. A breadcrumb on the top of the Content Pane displays the entire navigation path.

**Content Pane**

The center part of the page is Content Pane that changes according to the menu item and tab. Information of the menu is displayed in the content pane, which includes list of managed devices and configuration screens.

**Button Bar**

The Button bar on the upper rightmost corner of the every page provides access to several commonly used functions like:

- **Device Search** – Specify a search string and click to search device(s) in SFM. Device(s) can be searched on following criteria:
  
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Device Name</td>
</tr>
<tr>
<td></td>
<td>Model</td>
</tr>
<tr>
<td></td>
<td>Serial Number</td>
</tr>
<tr>
<td></td>
<td>Firmware</td>
</tr>
<tr>
<td></td>
<td>Company</td>
</tr>
<tr>
<td></td>
<td>City</td>
</tr>
<tr>
<td></td>
<td>State</td>
</tr>
<tr>
<td></td>
<td>Country</td>
</tr>
</tbody>
</table>

By default it yields results based on Device Name. Results display following information in tabular form: Device name, Serial number, Company name, Status and Firmware.

Click Device Name to go the dashboard of that device.

- **Alerts** – Click to view list of alerts generated by SFM.
- **Discovery** – Click to view list of devices sending heartbeat packet to the SFM. Click icon to add newly discovered devices using Add Device Wizard or icon to delete the device.
- **Errors** – Displays total number of generated errors.
- **Monitor** - Click to view the Device Monitor graphs which displays critical health status of the managed devices.
- **Help** – SFM includes a Web-based help online help, which can be viewed from any of the page of admin console. Click Help to open the context-sensitive help for the page.
- **Language** - Click to change device language.
- **More** - Click to view more options.
Wizard – Click to run Network Configuration wizard which will guide you step-by-step through configuration of the network parameters like IP address, subnet mask and default gateway for your device.

Console – Click to get immediate access to CLI by initiating a telnet connection with CLI without closing admin console.

Support – Click to open the customer login page for creating a Technical Support Ticket. It is fast, easy and puts your case right into the Technical Support queue.

About Product – Click icon to open the License page.

Reboot Device – Click to reboot the device.

Shutdown Device – Click to shut down the device.

Logout – Click to log out from the Admin Console.

2.3 Menus

The Sophos Firewall Manager UI offers you three work areas: Device Configuration, Templates, and System & Monitor. Select any work area from the top, beside Home.

Once an area is selected, the Navigation bar changes based on the selected work area.

The navigation bar on the leftmost side provides access to various configuration pages. Menu consists of sub-menus and tabs. On clicking menu item in the navigation bar, related management functions are displayed as submenu items. On clicking submenu item, all the associated tabs are displayed. To view page associated with the tab, click the required tab.
2.4 Tool Tips

To view the additional configuration information, use tool tip. Tool tip is provided for many configurable fields. Move the pointer over to view the brief configuration summary.
2.5 Notification pop-ups

A notification pop-up will be displayed at the top of the every page for error messages or action status. You can click the icon to close the pop-up.

2.6 Common Operations

Adding an Entity

You can add a new entity like policy, group, user, rule, or host by clicking the Add button available on most of the configuration pages. Clicking the Add button either opens a new page or pop-up window.

You can add new items for an entity by clicking the Add New Item. Select items by clicking the checkbox and apply to add the selected items. You can also update/delete the items added.

2.6.1 Set Schedule

For the entire group and subgroup level configuration, administrator can update configuration immediately or schedule the update. Whenever any configuration task – add, update and delete, is done, Set Schedule page with following parameters is opened:

Synchronize Configuration - Select the time and date to update the configuration.

Immediately – Changes will be applied immediately to the device(s). However it takes some time to reflect the changes locally.

At: – Specify date and time in the format YYYY –MM-DD Hours:Minutes or select date and time from the given calendar. Configuration will be updated at the scheduled time. All the scheduled tasks are listed at System Settings > Device Settings > Scheduled Task page. If required, scheduled task can also be deleted from Scheduled Tasks page.

Device Time Zone – Select to apply changes as per the device time zone.

Override configuration - Select Yes to override existing configuration of device else select No.

Select Device(s) - Select Device(s) or Device Group(s) for which this task is to be scheduled.

Filter Devices - Click to filter devices on the basis of given criteria.
Select Criteria and specify the value to be matched.

- Model: Specify model.
- Firmware: Specify firmware.
- Company: Specify company name.
- Country: Specify country name.
- State: Specify state name.
- City: Specify city name.
- Device Name: Specify device name.

Note

- Filter Devices is available only if Device is selected in Select Device(s).
- Sophos XG Firewall device(s) below SFOS 16.0.0 will not be displayed for selection.

2.6.2 Synchronize

You can synchronize configuration of selected entities of managed device(s) with the configuration available in SFM. To Synchronize settings, click icon or the button.

2.6.3 Entity Usage Reference

Entity Usage Reference points out the co-dependency of an entity with another entity. Entity Usage Reference lists all the dependent entities related to a particular entity. The list includes the entity, sub-entity and the device group details. Entity Usage Reference is an essential feature for the administrator so that they can identify all co-dependent entities before deleting any particular entity. If the dependency exists, the administrator must remove the dependency before deleting the entity.

To determine the Entity Usage Reference, click

This will display the following information for the selected entity and its dependent entity(ies).

**Details of selected entity**

**Entity**
Displays the selected entity type.

**Sub Entity**
Displays the selected Sub Entity type.

**Entity Name**
Displays the name of the selected entity.

**Details of dependent entities**
2.6.4 Editing an Entity

All the editable entities are hyperlinked. You can edit any entity by clicking either the hyperlink or the icon under the Manage column.

2.6.5 Deleting an Entity

You can delete an entity by selecting the check box and clicking the Delete button or icon.

To delete multiple entities, select individual entity and click the Delete button.

To delete all the entities, select the check box in the heading column and click the Delete button.

2.6.6 Sorting Lists

To organize the list spread over multiple pages, sort the list in ascending or descending order of a column attribute. You can sort a list by clicking a column heading.

- Ascending Order icon in a column heading indicates that the list is sorted in ascending order of the column attribute.
- Descending Order icon in a column heading indicates that the list is sorted in descending order of the column attribute.
2.6.7 Filtering Lists

To search specific information within the long list spread over multiple pages, filter the lists. Filtering criteria vary depending on a column data and can be a number or an IP address or part of an address, or any text string combination.

To create filter, click the Filter icon in a column heading. When a filter is applied to a column, the Filter icon changes to.

2.6.8 Configuring Column Settings

By default on every page all columnar information is displayed but on certain pages where a large number of columnar information is available, all the columns cannot be displayed. It is also possible that some content may not be of use to everyone. Using column settings, you can configure to display only those numbers of columns which are important to you.

To configure column settings, click Select Columns and select the check box against the columns you want to display and clear the check box against the columns which you do not want to display. All the default columns are grayed and not selectable.

2.6.9 Reordering List

You can reorder the Security Policies/Groups by dragging and dropping. On successful reordering, a status message will be displayed. Following can also be reordered:

- IPS Policy Rules
- Application Filter Policy Rules

2.6.10 Summary

For convenience in reviewing the firewall rule, a summary of the firewall rule is auto-populated alongside the configuration windows. In addition to this, you can click any summary element to scroll up or down, directly to the configuration section.
3 Device Configuration

Sophos Firewall Manager (SFM) enables the organization to monitor and manage multiple Firewall devices from a central location. Device Configuration allows sorting of the added devices on the basis of different criteria for better visibility and permits enforcement of global policies for security features like Firewall, VPN, Intrusion Prevention System, Application filter, Anti-spam and Anti-virus on them. It also allows the administrator to create and implement multiple Traffic Shaping policies to stop bandwidth abuse in organization to ensure productivity of the employees.

As soon as a device is added to SFM, SFM connects to the device and starts synchronization process and the status of the device changes to [status]. In the synchronization process, SFM updates its local copy as per the information provided by the device. Once the synchronization is successful, status changes to [status]. SFM maintains the mirror or duplicate copy of the Device configuration. However, the device copy is always considered as the master copy. If due to any reason, if synchronization process fails device status changes to [status].

Once the device is added and synchronized, the device sends the information like device health, network information, various attacks and threats identified by the device to SFM through heartbeat at the regular interval.

Device Configuration has the following Dashboards to view and manage device groups and individual devices:

- Device Group Dashboard
- Device Dashboard

3.1 Device Dashboard

Device Dashboard provides a single screen snapshot of the state and health of the selected managed device. To view the details of individual device, go to Device Configuration and expand the Device Group tree and select any device.

Device Information

Company Name - Name of the company under whose name device is to be registered. For unregistered devices this field will be blank.
Device Name - Name of the device. Click Edit hyperlink to edit the device details.
Host Name - Host Name as configured on the SF device.
Serial Number - Serial number of the SF device.
Model - Model number
Location - Name of the place where SF device is deployed.
Firmware Version - Firmware version running on the device
Time Zone - Time zone of the device
Date & Time (Time calculated based on SFM time) - Date and time of device in Day Mon DD YYYY HH:MM:SS format

Last Good Backup - Date and time in Day Mon DD YYYY HH:MM:SS format when last good backup has been taken.

Last Backup - Date and time in Day Mon DD YYYY HH:MM:SS format when last backup has been taken.

Change Detail - Status of Change Control Settings. If the change control is enabled it displays hyperlink to view change control for the device.

Connection Information

Device IP/Domain - Address IP address of the device

Connection Status - Current connectivity status

Synchronization Status - Synchronization status. Click ‘Sync now’ hyperlink to start synchronization process.

Communication Mode - Communication mode to manage SF device from SFM.

Available Modes:
• Central Management will push updates to this Device
• This Device will fetch updates from Central Management Communicate with SF using Communication protocol – HTTP, HTTPS Port Communication port Test Connection Click “Test Now” to establish the connection between SF and SFM.

Security


Resource

Gives resource utilization information on CPU, Memory, Disk (Report) and Disk (Config).

Availability

License


Signature Information (Applicable only if the device is Registered)

IPS Signature Version - IPS signature database version on the device. Click Synchronize button to update IPS signature database with latest available database version at upgrade server.

Anti Virus Version - Anti Virus engine version on the device. Click Synchronize button to update AV signature database with latest available database version at upgrade version.
Device Monitoring

Packet Capture - Displays time in Day, DD Mon YYYY at HH:MM:SS format when packet capture information is fetched from managed devices through SFM.

Connection Capture - Displays time in Day, DD Mon YYYY at HH:MM:SS format when connection list information is fetched from managed devices through SFM. Connection list provides current or live connection snapshot of managed device in the list form.

Tools - Click to open Tools page of managed device.

CTR - Displays time in Day, DD Mon YYYY at HH:MM:SS format when CTR is generated for managed devices through SFM. DHCP Lease - Displays time in Day, DD Mon YYYY at HH:MM:SS format when DHCP Lease information is fetched from managed devices through SFM.

Live Users - Displays time in Day, DD Mon YYYY at HH:MM:SS format when Live Users information is fetched from managed devices through SFM.

IPSec Connections - Displays time in Day, DD Mon YYYY at HH:MM:SS format when IPSec Connections information is fetched from managed devices through SFM. SSL VPN Users Displays time in Day, DD Mon YYYY at HH:MM:SS format when SSL VPN Users information is fetched from managed devices through SFM.

Live Connection IPv4 - Displays time in Day, DD Mon YYYY at HH:MM:SS format when IPv4 Live Connections information is fetched from managed devices through SFM.

Live Connection IPv6 - Displays time in Day, DD Mon YYYY at HH:MM:SS format when IPv6 Live Connections information is fetched from managed devices through SFM.

CPU usage for last two hours

Displays line graph for CPU usage for last two hours.

Memory usage for last two hours

Displays line graph for Memory usage for last two hours.

Interface Status

Displays status of managed device’s interfaces with details like Interface Name, MTU, Interface Speed, MAC Address, Status of the interface.

3.2 Policy Configuration Tasks

SFM allows following types of configuration:

Group level configuration - Configuration to be applied to all the devices in the group.

Subgroup level configuration - Configuration to be applied to all the devices in the sub group.

Device level configuration - Configuration to be applied to the individual devices only.
For managing and monitoring purpose, SFM groups all the managed devices into various groups. Use All Managed Devices drop down to view list of all the groups.

By default, SFM is shipped with three default Device Groups:

- **All Managed Devices** – Displays list of all the devices by name and their status.
- **All Firmware Versions** – SFM automatically groups all the devices added in SFM as per the device firmware version.
- **All Device Models** – To view the device model wise grouping, under the Device Group, click All Device Models Version.

SFM allows you to create custom Device Groups based on various criteria like Department, Country etc. Please refer System Management > System Settings > Device Settings > Device Group to create and manage Device Groups.

To see the individual devices, use the Manage Policy menu.

Manage Policy drop down menu also displays status of the Devices as:

<table>
<thead>
<tr>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected and synchronized</td>
</tr>
<tr>
<td>Disconnected and synchronized</td>
</tr>
<tr>
<td>Connected and unsynchronized.</td>
</tr>
<tr>
<td>Disconnected and unsynchronized</td>
</tr>
<tr>
<td>Disconnected</td>
</tr>
</tbody>
</table>

SFM displays details of all the added devices as soon as you log on to Web Admin Console in the form of Dashboard. SFM provides two types of dashboards:

- **Device Group Dashboard** – Consolidated dashboard for all the devices of selected device group or device subgroup
- **Device Dashboard** – Dashboard for the selected device only
3.3 Monitor and Analyze

3.3.1 SFM Dashboard

The SFM Dashboard appears when you log in to the SFM. It provides a single screen overview of the state and health of the SFM System and the managed devices.

Device Information

All Managed Devices - Total number of devices in the selected device group or subgroup
Synchronized - Total number of synchronized devices in selected devices group or subgroup
Unsynchronized - Number of unsynchronized devices in selected devices group or subgroup
Connected - Total number of devices currently connected to SFM in selected device group or subgroup
Disconnected - Number of devices in selected device group or subgroup, which are currently disconnected.

Device Monitor Summary

Dashboard Monitoring Graph displays critical health information of the managed Devices in graphical manner. SFM monitors the managed device based on the following health parameters and statuses:

- **Security**: HTTP Attacks, Mail Attacks, Spam Mails, Web Usage Health, IPS Alert.
- **Resource**: CPU, Memory, Disk (Report), Disk (Config).

The Monitoring Dashboard continuously monitors the managed devices for the wide range of security attacks, resource utilization and license statuses which helps the administrator to take informed decisions in resolving the risk landscape.

The administrator can set the threshold values for each of the parameters by clicking on Adjust Thresholds hyperlink. However, if the administrator does not specify the threshold values, the graphs are generated with Device Defaults based on the table below:

Gateway Status

Gateway Name - Name of the gateway
Gateway IP address - IP address of the gateway
Gateway Status - Status of the gateway
Model Wise Information

This area provides the name of device model along with total number of devices of that model number.

Click the hyperlink to view following details of device model:

- Device Name – Name of device
- Device Key – Device key of the managed device
- Company Name – Name of the company where the managed device is deployed
- Model – Model number of the managed device
- Status - Current state of the device

System Information

System Time - System (SFM) time in Day Date Mon YYYY HH:MM:SS format
Up Time - SFM device up time duration in day, hours and minutes format
SFM Version - SFM version number along with the link to check the availability of new version
Model - SFM Device model number
Device Key - SFM device key
Peer Device Key - If the device is deployed in HA (High Availability) node then it displays device key of auxiliary device.
Compatible SF Versions - List of SF device versions which are manageable through SFM
Live Connected Users - Number of connected users. Click to view details of connected users

Messages

Time - Time of sending alert in date and time format
Message - Alert message(s) generated by SFM system to notify the administrator regarding any alarming situation or availability of new SFM version.
3.3.2 Diagnostics

This menu allows checking the health of your device in a single shot. Information can be used for troubleshooting and diagnosing problems found in your device.

Services

View system service status and manage services.

Support access

Use the Support access page to allow a Sophos Support team member to temporarily access your firewall for troubleshooting purpose.

Support access enables the Sophos Support team member to connect to the web admin console of your firewall without requiring admin credentials. When the feature is enabled, an access ID is generated, using which the support team member can access your device. The admin needs to share this ID with the support person.

When Support access is enabled, support can access your XG Firewall over HTTPS on TCP port 22 from the WAN. All connections between XG Firewall and support are initiated by your XG Firewall.

Specify the following:

1. Enable the support access on Sophos XG Firewall under Diagnostics > Support access and click the toggle switch.
2. Confirm the enable message with OK.
3. From the drop-down menu Grant access for select the time the access is valid.
4. Click Apply to update the settings.
5. Click OK.

Sophos XG Firewall establishes a secure control connection to APU (access proxy for UTM) and negotiates a unique access ID.

6. Communicate the Access ID to the support.

The support uses this access ID to login to your XG Firewall. The control connection remains established until the specified time, which is displayed next to Access until.

You can disable the connection manually any time by clicking the toggle switch and confirming the disable message with OK.

Policy Test

With the policy test tool, you can apply and troubleshoot firewall and web policies and view the resulting security decisions. For example, you can create a web policy to block all social networking sites for the specified users and test the policy to see if it blocks only the specified content and users. The results display the details of action taken by the firewall based on the applicable rules and content filters.

Note

If policy routing affects connections to the destination, causing the connection to go through a different network zone, the policy test decision will not reflect the changed zone.
Note
Policy tester assumes that all web traffic is intercepted in transparent mode.

**URL**
URL to be tested. For example, you can test a social networking site, which should be blocked by the category and content filter that are specified in a web policy.

**Authenticated User**
User to be included in the test. For example, you can specify a user, who is the member of a group that you have included in a web policy.

**Time and Day**
Time and day to be included in the test. For example, you can specify a time that is within the constraints (or schedule) of a web policy.

**Test Method**
Possible values are:

- Test Firewall Policy. Source IP and zone that you wish to test.
- Test Web Policy. Web policy that you wish to test.

### 3.4 Protect

#### 3.4.1 Firewall

Firewall rules are security rule-sets to implement control over users, applications or network objects in an organization. Using Firewall rules, you can create blanket or specialized traffic transit rules based on the requirement. Firewall rules provide centralized management for the entire set of device security Firewall rules. Sophos Firewall Manager implements single pane of management to secure all enterprise applications using configuration templates for various types of Firewall rules.

Following sections provide more information on the Firewall section.

- **Introduction**
- **Managing Firewall Rules**
- **Default Firewall Rules**
- **Understanding Icons**
- **Understanding List of Firewall Rules**

**Introduction**

Firewall rules are based on the following configurable templates:

1. Business Application Rule
2. User/Network Rule
Managing Firewall Rules

You can see the entire list of added security Firewall rules from the Firewall page. Using the same page, you can update existing firewall rules, or add new firewall rules.

On the Firewall page, the following action buttons can be found.

- **IPv4**: Select to filter only IPv4 Firewall rules
- **IPv6**: Select to filter only IPv6 Firewall rules
- **Enable Filter**: Select to open filter view and apply the following filters for IPv4 or IPv6 Firewall rules:
  1. Rule Type - Select to filter rules based on Business, User or Network
  2. Source Zone - Select to filter rules based on LAN, WAN, DMZ, VPN or WiFi
  3. Destination Zone - Select to filter rules based on LAN, WAN, DMZ, VPN or WiFi
  4. State - Select to filter rules based on Unused, Disabled, Changed, New
  5. Rule ID - Specify Rule ID to see the specific rule.
- **Reset Filter** (Available if filter is enabled) - Select to reset all filters
- **Disable Filter** (Available if filter is enabled) - Select to close filter view
- **+ Add Firewall Rule** - Select to add a new Firewall Rule among Business Application Rule, or User/Network Rule.

Default Firewall Rules

The following default Firewall Rules are created with first time deployment of SFM:

1. Auto added firewall policy for MTA

**Note**

Default Firewall Rules cannot be deleted.

Understanding Icons

There are various action icons as well as symbolic icons on the Firewall page. Color codes, meanings and associated actions of icons are shown below.

<table>
<thead>
<tr>
<th>Icons</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Business Application Rule Enabled" /></td>
<td>Business Application Rule Enabled</td>
</tr>
<tr>
<td><img src="image2" alt="Business Application Rule Disabled" /></td>
<td>Business Application Rule Disabled</td>
</tr>
<tr>
<td><img src="image3" alt="User Rule Disabled + Action - Accept" /></td>
<td>User Rule Disabled + Action - Accept</td>
</tr>
<tr>
<td>Icons</td>
<td>Meaning</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td><img src="image" alt="User Rule Disabled + Action - Drop/Reject" /></td>
<td>User Rule Disabled + Action - Drop/Reject</td>
</tr>
<tr>
<td><img src="image" alt="User Rule Enabled + Action - Drop/Reject" /></td>
<td>User Rule Enabled + Action - Drop/Reject</td>
</tr>
<tr>
<td><img src="image" alt="User Rule Enabled" /></td>
<td>User Rule Enabled</td>
</tr>
<tr>
<td><img src="image" alt="Network Rule Enabled" /></td>
<td>Network Rule Enabled</td>
</tr>
<tr>
<td><img src="image" alt="Network Rule Disabled + Action - Accept" /></td>
<td>Network Rule Disabled + Action - Accept</td>
</tr>
<tr>
<td><img src="image" alt="Network Rule Disabled + Action - Drop/Reject" /></td>
<td>Network Rule Disabled + Action - Drop/Reject</td>
</tr>
<tr>
<td><img src="image" alt="Network Rule Enabled + Action - Drop/Reject" /></td>
<td>Network Rule Enabled + Action - Drop/Reject</td>
</tr>
<tr>
<td><img src="image" alt="Anti-Virus Scanning Disable" /></td>
<td>Anti-Virus Scanning Disable</td>
</tr>
<tr>
<td><img src="image" alt="Anti-Virus Scanning Enable" /></td>
<td>Anti-Virus Scanning Enable</td>
</tr>
<tr>
<td><img src="image" alt="Application Control Disable" /></td>
<td>Application Control Disable</td>
</tr>
<tr>
<td><img src="image" alt="Application Control Allow All" /></td>
<td>Application Control Allow All</td>
</tr>
<tr>
<td><img src="image" alt="Application Control Deny All" /></td>
<td>Application Control Deny All</td>
</tr>
<tr>
<td><img src="image" alt="Application Control Drop" /></td>
<td>Application Control Drop</td>
</tr>
<tr>
<td><img src="image" alt="Security Heartbeat Disable / No Restriction" /></td>
<td>Security Heartbeat Disable / No Restriction</td>
</tr>
<tr>
<td><img src="image" alt="Security Heartbeat Enable - Green" /></td>
<td>Security Heartbeat Enable - Green</td>
</tr>
<tr>
<td><img src="image" alt="Security Heartbeat Enable - Yellow" /></td>
<td>Security Heartbeat Enable - Yellow</td>
</tr>
<tr>
<td><img src="image" alt="Security Heartbeat - No Restriction + No Heartbeat." /></td>
<td>Security Heartbeat - No Restriction + No Heartbeat.</td>
</tr>
<tr>
<td><img src="image" alt="Security Heartbeat - No Restriction + Green" /></td>
<td>Security Heartbeat - No Restriction + Green</td>
</tr>
<tr>
<td><img src="image" alt="Security Heartbeat - No Restriction + Yellow" /></td>
<td>Security Heartbeat - No Restriction + Yellow</td>
</tr>
<tr>
<td><img src="image" alt="Intrusion Prevention Disable" /></td>
<td>Intrusion Prevention Disable</td>
</tr>
<tr>
<td><img src="image" alt="Intrusion Prevention Enable" /></td>
<td>Intrusion Prevention Enable</td>
</tr>
<tr>
<td><img src="image" alt="NAT Disable" /></td>
<td>NAT Disable</td>
</tr>
<tr>
<td><img src="image" alt="NAT Enable" /></td>
<td>NAT Enable</td>
</tr>
</tbody>
</table>
**Sophos Firewall Manager**

<table>
<thead>
<tr>
<th>Icons</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="QoS" /></td>
<td>Traffic Shaping Policy Disabled</td>
</tr>
<tr>
<td><img src="image" alt="QoS" /></td>
<td>Traffic Shaping Policy Enabled</td>
</tr>
<tr>
<td><img src="image" alt="WEB" /></td>
<td>Web Policy Disable</td>
</tr>
<tr>
<td><img src="image" alt="WEB" /></td>
<td>Web Policy Allow</td>
</tr>
<tr>
<td><img src="image" alt="WEB" /></td>
<td>Web Policy Deny</td>
</tr>
<tr>
<td><img src="image" alt="WEB" /></td>
<td>Web Policy Drop</td>
</tr>
<tr>
<td><img src="image" alt="Rt" /></td>
<td>Routing Enabled</td>
</tr>
<tr>
<td><img src="image" alt="Rt" /></td>
<td>Routing Disabled</td>
</tr>
<tr>
<td><img src="image" alt="ON" /></td>
<td>Firewall Rule enabled. Click to disable the rule.</td>
</tr>
<tr>
<td><img src="image" alt="OFF" /></td>
<td>Firewall Rule disabled. Click to enable the rule.</td>
</tr>
<tr>
<td><img src="image" alt="Edit" /></td>
<td>Edit Rule</td>
</tr>
<tr>
<td><img src="image" alt="Delete" /></td>
<td>Delete Rule</td>
</tr>
</tbody>
</table>

**Color Codes**

<table>
<thead>
<tr>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>Reject/Drop</td>
</tr>
<tr>
<td>Green</td>
<td>Accept/Allow</td>
</tr>
<tr>
<td>Yellow</td>
<td>Drop (In case of policies)</td>
</tr>
<tr>
<td>Blue</td>
<td>On/Enable</td>
</tr>
<tr>
<td>Grey</td>
<td>Off/Disable</td>
</tr>
</tbody>
</table>

**Understanding List of Firewall Rules**

All added Firewall Rules are available in the form of a list. Each Firewall Rule in the list presents a quick snapshot of the rule.

**Details of the rule:**

- **Rule Name**: Name of the rule.
- **Firewall Rule Features**: Status of schedule, Heartbeat, IPS and traffic shaping.
- **Source**: Source zone.
- **Destination**: Destination zone.
- **What**: Displays protected domains/services.
- **Action**: Status of protected servers, status of web and application protection for user.
- **ID**: Rule ID
**User's Policy Applied**: Status of application filter, web policy, AV and AS scanning, NAT policy and route through gateway, if configured

To view details of the Source, Destination, What (type of service) and Features, hover over the Features.

Click for the following options to appear:
- **ON**
- **OFF**
- Edit
- Clone
- Add User/Network Rule
- Add Business Application Rule
- Synchronize
- Delete

**User/Network rule**

User/Network rule is used to define access rights and protection to the network objects/hosts. In a nutshell, if you want to control traffic by source, service, destination, zone, then use a network rule. Additionally, the administrator has the option to attach user identity to a rule in order to customize access of assorted hosts/servers. Such an identity based rule is considered a user rule.

**Add User/Network Rule (IPv4)**

This page is used to define access rights and protection to the network objects/hosts.

1. Click Firewall and select IPv4 using the filter switch. Now, click on **Add Firewall Rule** and select User/Network Rule.
2. Enter rule introduction.

**Rule Name**

Specify a name to identify the policy.

**Note**

Rule Name can only be edited while creating a rule.

**Description**

Specify Policy Description.

**Rule Position**

Specify the position of the rule from the available options.

**Available Options:**

Top Bottom
Note
Rule Position can only be specified while creating a rule.

Action
Select action for the rule traffic from the available options:

- **Accept** – Allow access (selection appears in green)
- **Drop** – Silently discard (selection appears in yellow)
- **Reject** – Deny access (selection appears in red)

Note
“ICMP port unreachable” message is sent to the source

When sending response it might be possible that the response is sent using a different interface than the one on which request was received. This may happen depending on the Routing configuration done on the device.

For example, If the request is received on the LAN port using a spoofed IP Address (public IP Address or the IP Address not in the LAN zone network) and specific route is not defined, the device will send a response to these hosts using the default route. Hence, response will be sent through the WAN port.

![Figure 1: About This Rule](image1)


**Source Zones**
Select the source zone(s) allowed to the user.

**Source Networks and Devices**
Select the source network(s) allowed to the user.
A new network host can be created directly from this page itself or from Objects > Hosts and Services > IP Host page.

**During Scheduled Time**
Select the schedule allowed to the user.
A new network host can be created directly from this page itself or from Objects > Policies > Schedule page.

![Figure 2: Source](image2)

4. Specify Destination & Services details.

**Destination Zones**
Select the destination zone(s) allowed to the user.
**Destination Networks**

Select the destination network(s) allowed to the user.

A new network host can be created directly from this page itself or from **Objects > Assets > IP Host** page.

**Services**

Select the services(s) allowed to the user.

A new network host can be created directly from this page itself or from **Objects > Hosts and Services > Services** page.

![Destination Zones, Destination Networks, Services](image)

Figure 3: Destination

5. Specify **Identity** details. Follow this step if you want to configure a **User Rule**.

**Match known users**

Select to enable rule based on user identity.

**Show Captive Portal to unknown users**

Select the check box to accept traffic from unknown users. Captive portal page is displayed to the user where the user can login to access the Internet.

Clear the check box to drop traffic from unknown users.

**User or Groups. (Applicable only when Match known users is Selected)**

Select the user(s) or group(s) from the list of available options.

**Exclude this user activity from data accounting. (Applicable only when Match rule based on user identity is Selected)**

Select to enable/disable user traffic activity from data accounting.

By default, user’s network traffic is considered in data accounting. Select to exclude certain traffic user data accounting. The traffic allowed through this firewall rule will not be accounted towards data transfer for the user.

![Match known users, User or Groups, Exclude this user activity from data accounting](image)

Figure 4: Identity

6. Specify **Malware Scanning** details.

**Scan HTTP**

Enable HTTP traffic scanning.

**Decrypt & Scan HTTPS**

Enable HTTPS traffic decryption and scanning.

**Detect zero-day threats with Sandstorm**
Send files downloaded using HTTP or HTTPS for analysis by Sandstorm, it protects your network against unknown and unpublished threats ("zero-day" threats).

**Note**
This option is available when **Scan HTTP** or **Decrypt & scan HTTPS** option is enabled.

**Scan FTP**
Enable FTP traffic scanning.

7. Enter Web malware and content scanning details (*available only if Action selected for the traffic is Accept*).

**Scan HTTP**
Enable HTTP traffic scanning.

**Decrypt & scan HTTPS**
Enable HTTPS traffic decryption and scanning.

**Block Google QUIC (Quick UDP Internet Connections)**
Disable QUIC protocol (UDP) traffic for Google services.

**Detect zero-day threats with Sandstorm.**
Send files downloaded using HTTP or HTTPS for analysis by Sandstorm. Sandstorm protects your network against unknown and unpublished threats ("zero-day" threats).

**Scan FTP for malware**
Enable FTP traffic scanning.

![Checkbox Selection]

- Scan HTTP
- Decrypt & Scan HTTPS
- Block Google QUIC (Quick UDP Internet Connections)
- Detect zero-day threats with Sandstorm
- Scan FTP for Malware

Figure 5: Web malware and content scanning

8. Specify **Advanced** details. (*Applicable only when Action for the traffic is Accept*)

**User Applications**

**Intrusion Prevention**
Select IPS Policy for the rule. A new Web Filter Policy can be created directly from this page itself or from Objects > Policies > IPS page.

**Traffic Shaping Policy**
User's Traffic Shaping policy will be applied automatically.

**Web Filter** (*Applicable only if Match rule based on user identity is 'Disabled'*)
Select Web Filter Policy for the rule.

It controls access to application like IM and P2P, VOIP.

A new Web Filter Policy can be created directly from this page itself or from Objects > Policies > Web Filter Policy page.
Apply Web Category based Traffic Shaping Policy (Applicable only if Match rule based on user identity is 'Disabled')

Click to restrict bandwidth for the URLs categorized under the Web category.

A three step configuration is required as follows:


b) Now, assign the created policy for Web Filter.

c) Check to enable Apply Web Category based Traffic Shaping Policy.

Application Control (Applicable only if Match rule based on user identity is 'Disabled')

Select Application Filter Policy for the rule. A new Application Filter Policy can be created directly from this page itself or from Objects > Policies > Application Group page.

Apply Application-based Traffic Shaping Policy (Applicable only if Match rule based on user identity is 'Disabled')

Click to restrict bandwidth for the applications categorized under the Application category.

A three step configuration is required as follows:


b) Now, assign the created policy for Application Control.

c) Check to enable Apply Web based Traffic Shaping Policy.

Synchronized Security

Minimum Source HB Permitted

Select a minimum health status that a source device must have to conform to this rule. Health status can be either Green, Yellow or No Restriction. If the health criterion is not met, access and privileges defined in this rule will not be granted to the user.

Block clients with no heartbeat

Heartbeat-capable devices can be required to send information on their health status in defined intervals - this is called a heartbeat.

Based on that information, you can restrict a source device's access to certain services and networks.

Select the option to require the sending of heartbeats.

Minimum Destination HB Permitted

Select a minimum health status that a destination device must have to conform to this rule. Health status can be either Green, Yellow or No Restriction. If the health criterion is not met, access and privileges defined in this rule will not be granted to the user.

Block request to destination with no heartbeat

Heartbeat-capable devices can be required to send information on their health status in defined intervals - this is called a heartbeat.

Based on that information, you can block requests to destinations not sending heartbeat.

Select the option to require the sending of heartbeats.

NAT & Routing

Copyright © Sophos Limited 27
Rewrite source address (Masquerading)
Select to re-write the source address or specify a NAT policy.

Use Gateway Specific Default NAT Policy (Applicable only if Masquerading is selected and Destination Zone is selected as WAN)
Click to override the default NAT policy with a gateway specific policy.

Override default NAT policy for specific Gateway (Applicable only if Use Gateway Specific Default NAT Policy is selected)
Select to specify gateway and corresponding NAT policy. Multiple Gateways and NAT Policy can be added.

Use Outbound Address (Applicable when Rewrite source address is selected)
Select the NAT policy to be applied the list or available NAT policies.
A new NAT policy can be created directly from this page itself or from Objects > Policies > NAT page.

Default NAT policy is Masquerade.

Primary Gateway
Specify the Primary Gateway. This is applicable only if more than one gateway is defined.

Backup Gateway
Specify the Backup Gateway. This is applicable only if more than one gateway is defined.

DSCP Marking
Select the DSCP Marking. Select DSCP Marking.
DSCP (DiffServ Code Point) classifies flow of packets as they enter the local network depending upon QoS. Flow is defined by 5 elements; Source IP Address, Destination IP Address, Source port, Destination port and the transport protocol.
For available options, refer DSCP Values.

Figure 6: Routing
9. Define logging option for the user application traffic.

Log Firewall Traffic
Click to select logging of permitted and denied traffic.
Add User/Network Rule (IPv6)

Use this page to add a new policy for applications accessed by your users.

1. Click **Firewall** and select **IPv6** using the filter switch. Now, click on **+Add Firewall Rule** and select **User/Network Rule**.

2. Enter rule introduction.

**Rule Name**

Specify a name to identify the policy.

*Note*

Rule Name can only be edited while creating a rule.

**Description**

Specify Policy Description.

**Rule Position**

Specify the position of the rule from the available options.

**Available Options:**

Top Bottom

*Note*

Rule Position can only be specified while creating a rule.

**Action**

Select action for the rule traffic from the available options:

- **Accept** – Allow access (selection appears in green)
- **Drop** – Silently discard (selection appears in yellow)
- **Reject** – Deny access (selection appears in red)

*Note*

“ICMP port unreachable” message is sent to the source

When sending response it might be possible that the response is sent using a different interface than the one on which request was received. This may happen depending on the Routing configuration done on the device.

For example, If the request is received on the LAN port using a spoofed IP Address (public IP Address or the IP Address not in the LAN zone network) and specific route is not defined, the device will send a response to these hosts using the default route. Hence, response will be sent through the WAN port.
Sophos Firewall Manager

3. Specify **Source** details.

**Source Zones**
Select the source zone(s) allowed to the user.

**Source Networks and Devices**
Select the source network(s) allowed to the user.

A new network host can be created directly from this page itself or from **Objects > Hosts and Services > IP Host** page.

**During Scheduled Time**
Select the schedule allowed to the user.

A new network host can be created directly from this page itself or from **Objects > Policies > Schedule** page.

4. Specify **Destination & Services** details.

**Destination Zones**
Select the destination zone(s) allowed to the user.

**Destination Networks**
Select the destination network(s) allowed to the user.

A new network host can be created directly from this page itself or from **Objects > Assets > IP Host** page.

**Services**
Select the services(s) allowed to the user.

A new network host can be created directly from this page itself or from **Objects > Hosts and Services > Services** page.

5. Specify **Identity** details. Follow this step if you want to configure a **User Rule**.

**Match known users**
Select to enable rule based on user identity.

**Show Captive Portal to unknown users**
Select the check box to accept traffic from unknown users. Captive portal page is displayed to the user where the user can login to access the Internet.

Clear the check box to drop traffic from unknown users.

**User or Groups. (Applicable only when Match known users is Selected)**
Select the user(s) or group(s) from the list of available options.

**Exclude this user activity from data accounting. (Applicable only when Match rule based on user identity is Selected)**
Select to enable/disable user traffic activity from data accounting.

By default, user’s network traffic is considered in data accounting. Select to exclude certain traffic user data accounting. The traffic allowed through this firewall rule will not be accounted towards data transfer for the user.

![Image](image.png)

Figure 11: Identity

6. Specify **Malware Scanning** details.

**Scan HTTP**
Enable HTTP traffic scanning.

**Decrypt & Scan HTTPS**
Enable HTTPS traffic decryption and scanning.

**Detect zero-day threats with Sandstorm**
Send files downloaded using HTTP or HTTPS for analysis by Sandstorm, it protects your network against unknown and unpublished threats (“zero-day” threats).

**Note**
This option is available when **Scan HTTP** or **Decrypt & scan HTTPS** option is enabled.

7. Enter Web malware and content scanning details *(available only if Action selected for the traffic is Accept)*.

**Scan HTTP**
Enable HTTP traffic scanning.

**Decrypt & scan HTTPS**
Enable HTTPS traffic decryption and scanning.

**Block Google QUIC (Quick UDP Internet Connections)**
Disable QUIC protocol (UDP) traffic for Google services.

**Detect zero-day threats with Sandstorm.**
Send files downloaded using HTTP or HTTPS for analysis by Sandstorm. Sandstorm protects your network against unknown and unpublished threats (“zero-day” threats).

**Scan FTP for malware**
Enable FTP traffic scanning.

- Scan HTTP
- Decrypt & Scan HTTPS
- Block Google QUIC (Quick UDP Internet Connections)
- Detect zero-day threats with Sandstorm
- Scan FTP for Malware

Figure 12: Web malware and content scanning

8. Specify Advanced details. *(Applicable only when Action for the traffic is Accept)*

**User Applications**

**Intrusion Prevention**
Select IPS Policy for the rule. A new Web Filter Policy can be created directly from this page itself or from **Objects > Policies > IPS** page.

**Traffic Shaping Policy**
User’s Traffic Shaping policy will be applied automatically.

**Web Filter (Applicable only if Match rule based on user identity is 'Disabled')**
Select Web Filter Policy for the rule.
It controls access to application like IM and P2P, VOIP.
A new Web Filter Policy can be created directly from this page itself or from **Objects > Policies > Web Filter Policy** page.

**Apply Web Category based Traffic Shaping Policy (Applicable only if Match rule based on user identity is 'Disabled')**
Click to restrict bandwidth for the URLs categorized under the Web category.
A three step configuration is required as follows:

a) Create Traffic Shaping policy from **Objects > Policies > Traffic Shaping**. Here, specify the Policy Association as ‘Web Categories’.

b) Now, assign the created policy for **Web Filter**.

c) Check to enable Apply Web Category based Traffic Shaping Policy.

**Application Control (Applicable only if Match rule based on user identity is 'Disabled')**
Select Application Filter Policy for the rule. A new Application Filter Policy can be created directly from this page itself or from **Objects > Policies > Application Group** page.

**Apply Application-based Traffic Shaping Policy (Applicable only if Match rule based on user identity is 'Disabled')**
Click to restrict bandwidth for the applications categorized under the Application category.
A three step configuration is required as follows:

a) Create Traffic Shaping policy from **Objects > Policies > Traffic Shaping**. Here, specify the Policy Association as ‘Applications’.

b) Now, assign the created policy for Application Control.
c) Check to enable **Apply Web based Traffic Shaping Policy**.

**NAT & Routing**

**Rewrite source address (Masquerading)**
Select to re-write the source address or specify a NAT policy.

**Use Gateway Specific Default NAT Policy (Applicable only if Masquerading is selected and Destination Zone is selected as WAN)**
Click to override the default NAT policy with a gateway specific policy.

**Override default NAT policy for specific Gateway (Applicable only if Use Gateway Specific Default NAT Policy is selected)**
Select to specify gateway and corresponding NAT policy. Multiple Gateways and NAT Policy can be added.

**Use Outbound Address (Applicable when Rewrite source address is selected)**
Select the NAT policy to be applied the list of available NAT policies.
A new NAT policy can be created directly from this page itself or from **Objects > Policies > NAT page**.
Default NAT policy is **Masquerade**.

**Primary Gateway**
Specify the Primary Gateway. This is applicable only if more than one gateway is defined.

**Backup Gateway**
Specify the Backup Gateway. This is applicable only if more than one gateway is defined.

**DSCP Marking**
Select the DSCP Marking. Select DSCP Marking.
DSCP (DiffServ Code Point) classifies flow of packets as they enter the local network depending upon QoS. Flow is defined by 5 elements: Source IP Address, Destination IP Address, Source port, Destination port and the transport protocol.

For available options, refer **DSCP Values**.
9. Define logging option for the user application traffic.

**Log Firewall Traffic**

Select to enable logging of permitted and denied traffic.

10. Click **Save** to save the settings.

**Business application rule**

Business application rule is used to protect internally or publicly hosted business applications or servers like SalesForce, Sharepoint etc.

**Adding a business application rule**

Using business application rule, the administrator can configure protection of the http and non-http web servers from unauthorized access over the internet. You can also control access of protected server or services through a business application rule.

Several templates are available that cover protection configuration for a variety of different types of http and non-http web servers and application. A list of these application templates appear on the business application rule page.

Go to **Firewall** and select **IPv4**, using the filter switch. Now, click on **Add firewall rule** and select **Business application rule**. You can then select the **Application template** from the list of available templates.
The application template allows you to choose the rule which suits the configuration of the required business application. Once you select the template, you can see the configuration page with few fields pre-populated. The pre-populated values eliminate the need to manually specify the configuration for securing your business application, but you may customize the settings according to your network setup or other requirements.

1. DNAT/Full NAT/load balancing rule: It is used to protect non-web servers, like mail or other servers hosted inside the network (LAN or DMZ). Using this template, you can define access rights of such servers to users who require access over the WAN or internet. Additionally, you can use the following non-web application template:

2. Email server (SMTP): Email server (SMTP) rule is used to protect mail servers which are hosted internally in a network and require protection.

3. Email clients (POP & IMAP): Email clients (POP and IMAP) rule is used to protect mail servers which are hosted publicly (WAN) and require protection.

**Note**
If you delete email clients rule, the emails which are under process by this rule will be queued but will not be delivered.

We recommend to follow below given steps so that you do not lose all the emails processed by this rule:

a) Before deleting this rule, clone this rule by choosing **Clone above** option and change the **Action** to **Drop**. This cloned rule will hold all the incoming emails.

b) Go to Email > Mail spool and check if spool is empty.

c) Once the spool is empty, delete both the firewall rules.

---

**Add Business Application Rule (Web Server Protection (WAF))**
*(only available for IPv4 policy)* This page describes how to configure a policy for controlling access to HTTP-based business applications.

1. Go to Device Configuration > Protect > Firewall and select IPv4. using the filter switch.
2. Click +Add Firewall Rule and Business Application Rule.
3. Specify the general rule details.

**Application Template**
Select **Web Server Protection (WAF)** to define an application filter policy for HTTP based applications.

**Description**
Specify a description for the rule.

**Rule Position**
Specify the position of the rule.

**Available Options:**
- Top
- Bottom

**Rule Name**
Specify a name for the rule.

Figure 15: About this Rule

**Hosted Address**
Select the interface of the hosted server to which the rule applies. It is the public IP address through which Internet users access the internal server/host.

**Note**

When a connection is established by a client device and the client accesses the web server, the web server does not obtain the real client IP address. Reason is that the connection is made through the Web Application Firewall, so the address of the interface the WAF uses for the connection is delivered. To receive the real client IP address, the administrator has to read out the contents of the HTTP header “X-Forwarded-For”.

**Listening Port**

Enter a port number on which the hosted web server can be reached externally over the Internet. Default is port 80 for plaintext communication (HTTP) and port 443 for encrypted communication (HTTPS).

**HTTPS**

Select to enable or disable scanning of HTTPS traffic.

**HTTPS Certificate (only available if HTTPS is selected)**

Select the HTTPS certificate to be used.

**Redirect HTTP (only available if HTTPS is selected)**

Select to redirect HTTP requests.

**Domains**

- *(if HTTPS is disabled)*: Enter the domains the web server is responsible for as FQDN, e.g. shop.example.com.
- *(if HTTPS is enabled)*: According to the selected HTTPS certificate, some domains may be preselected. You can edit or delete these domains or add new ones.

**Path-specific routing**

You can enable path-specific routing to define (a path) to which web servers incoming requests are forwarded.

You can define that all URLs with a specific path, for example, /products/, are sent to a specific web server. On the other hand you can allow more than one web server for a specific request but add rules how to distribute the requests among the servers. Additionally, you can define that each session is bound to one web server throughout its lifetime (sticky session). This may be necessary if you host an online shop and want to make sure that a user sticks to one server during the shopping session. You can also configure to send all requests to one web server and use the others only as a backup.

For each hosted web server, one default site path route (with path /) is created automatically. The device automatically applies the site path routes in the most reasonable way: starting with the strictest, i.e., longest paths and ending with the default path route which is only used if no other more specific site path route matches the incoming request. The order of the site path route list is not relevant. If no route matches an incoming request, (in case the default route was deleted), the request will be denied.

**Add New Path (only available if Path-specific routing is selected)**

Click Add Path to define a new path.

Click Add Path
Add New Path will only be active after at least one web server and one hosted web server have been created.

Web Server (not available if Path-specific routing is selected)
With this option, you select the web servers that are to be protected. Select a web server from Web Server list. The selected web server is displayed on the right side of the table under Selected Web Server(s).
A new web server can be created on the Device Configuration > Protect > Web Server page.

6. Specify Access Permission details (not available if Path-specific routing is selected).

Allowed Client Networks
Select or add the allowed networks that should be able to connect to the hosted web server.

Blocked Client Networks
Select or add the denied networks that should be blocked to your hosted web server.

Authentication
Select a web app authentication profile or click Create new to create a new authentication profile. You can also create an authentication profile from the Device Configuration > Protect > Web Server > Authentication Policies page.

7. Add path Exceptions for the web servers.

Click Add New Exception to specify a new exception.

8. Configure advanced settings.

a) Specify Profiles for Business Applications.

Intrusion Prevention
Select an Intrusion Prevention policy for the rule or create a new one. A new IPS policy can be created directly from this page or from the Device Configuration > Protect > Intrusion Prevention > IPS Policies page. You can also choose to have None intrusion prevention.

Traffic Shaping
The traffic shaping policy allocates & limits the maximum bandwidth usage of the user. Select a traffic shaping policy for the rule or create a new one. A new traffic shaping policy can be created directly from this page or from the Device Configuration > System > Profiles > Traffic Shaping page. You can also choose to have None traffic shaping.

Application Protection
Select an application protection for the server or create a new one. A new application protection policy can be created directly from this page or from the Device
Figure 20: Policies for Business Applications

b) Specify Advanced settings for the added server.

Disable Compression Support

By default, this check box is disabled and the content is sent compressed when the client requests compressed data. Compression increases transmission speed and reduces page load time. However, in case of websites being displayed incorrectly or when users experience content-encoding errors accessing your web servers, it can be necessary to disable compression support. When the checkbox is enabled, the WAF will request uncompressed data from the web servers of this hosted web server and will pass it on uncompressed to the client, regardless of the HTTP request's encoding parameter.

Rewrite HTML

Select this option to have the device rewrite links of the returned webpages in order for the links to stay valid. Example: One of your web server instances has the hostname yourcompany.local but the hosted web server's hostname on the device is yourcompany.com. Thus, absolute links like [a href="http://yourcompany.local/"] will be broken if the link is not rewritten to [a href="http://yourcompany.com/"] before delivery to the client. However, you do not need to enable this option if either yourcompany.com is configured on your web server or if internal links on your webpages are always realized as relative links. It is recommended to use the option with Microsoft's Outlook web access and/or SharePoint portal server.

Note

HTML rewriting affects all files with a HTTP content type of text/* or *xml*, where * is a wildcard. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the HTML rewriting process.

Rewrite cookies (only available if Rewrite HTML is selected)

Select this option to have the device rewrite cookies of the returned web pages.

Pass Host Header

When you select this option, the host header as requested by the client will be preserved and forwarded along with the web request to the web server. Whether passing the host header is necessary in your environment depends on the configuration of your web server.

Figure 21: Advanced

9. Click Save.

Note

As soon as a new HTTP based rule configuration has been created and saved or an existing HTTP based rule configuration has been altered and saved, all HTTP based business rules will be restarted. Any underlying client connection using a HTTP based business rule will get lost and has to be re-established.

The business application rule has been created and appears on the Firewall page when the IPv4 filter is set.
**Exchange Autodiscover**
*(Only available for IPv4 policy)* This page describes how to configure a rule for Exchange Autodiscover.

1. Go to **Device Configuration > Protect > Firewall** and select **IPv4**, using the filter switch.
2. Click **+Add Firewall Rule** and **Business Application Rule**.
3. Specify the general rule details.

**Application Template**

Select **Exchange Autodiscover** to configure a policy for an Exchange Autodiscover environment.

**Description**

Specify a description for the rule.

**Rule Position**

Specify the position of the rule.

**Available Options:**

- Top
- Bottom

**Rule Name**

Specify a name for the rule.

**Hosted Server**

Specify the address of the hosted server to which the rule applies. It is the public IP address through which Internet users access an internal server/host.

**Note**

When a connection is established by a client device and the client accesses the web server, the web server does not obtain the real client IP address. Reason is that the connection is made through the Web Application Firewall, so the address of the interface the WAF uses for the connection is delivered. To receive the real client IP address, the administrator has to read out the contents of the HTTP header "X-Forwarded-For".

**Listening Port**

Enter a port number on which the hosted web server can be reached externally over the Internet. Default is port 80 for plaintext communication (HTTP) and port 443 for encrypted communication (HTTPS).

**HTTPS**

Select to enable or disable scanning of HTTPS traffic.

**HTTPS Certificate** *(only available if HTTPS is selected)*

Select the HTTPS certificate to be used.

**Redirect HTTP** *(only available if HTTPS is selected)*

Select to redirect HTTP requests.

**Domains**

Enter the domains the web server is responsible for as FQDN, e.g. shop.example.com.

**Protected Server(s)**

5. Specify **Protected Server(s)** details.
**Path-specific routing**

You can enable path-specific routing to define (the path) to which web servers incoming requests are forwarded.

You can define that all URLs with a specific path, for example, /products/, are sent to a specific web server. On the other hand you can allow more than one web server for a specific request but add rules how to distribute the requests among the servers. Additionally, you can define that each session is bound to one web server throughout its lifetime (sticky session). This may be necessary if you host an online shop and want to make sure that a user sticks to one server during the shopping session. You can also configure to send all requests to one web server and use the others only as a backup.

For each hosted web server, one default site path route (with path /) is created automatically. The device automatically applies the site path routes in the most reasonable way: starting with the strictest, i.e., longest paths and ending with the default path route which is only used if no other more specific site path route matches the incoming request. The order of the site path route list is not relevant. If no route matches an incoming request, (in case the default route was deleted), the request will be denied.

Default: Enabled

**Add New Path (only available if Path-specific routing is selected)**

Click **Add New Path** to define a new path.

**Add Path**

**Note**

**Add New Path** will only be active only after at least one web server and one hosted web server have been created.

Default: /autodiscover, /Autodiscover, /AutoDiscover

**Web Server (not available if Path-specific routing is selected)**

Web servers are the application servers to be protected. Select a web server from the list of web servers or enter a web server and click **Create** to add a web server.

A new web server can be created directly from this page or from the **Device Configuration > Protect > Web Server > Web Servers** page.

Figure 24: Protected Server(s)

6. **Specify Access Permission details (not available if Path-specific routing is selected).**

**Allowed Client Networks**

Select the allowed host(s)/network(s).

**Blocked Client Networks**

Select the blocked host(s)/network(s).

**Authentication**

Select the web application authentication profile from the list of available profiles.

You can also create a new authentication profile on this page or on the **Device Configuration > Protect > Web Server > Authentication Policies** page.

Figure 25: Access Permission

7. **Add path Exceptions for the web servers.**

Click **Add New Exception** for the web servers.

**Add Exception**
8. Configure advanced settings.
   a) Specify Profiles for Business Applications.

**Intrusion Prevention**

Select an IPS policy for the rule.

A new IPS policy can be created directly from this page or from the Device Configuration > Protect > Intrusion Prevention > IPS Policies page.

**Traffic Shaping**

Select a traffic shaping policy for the rule.

A traffic shaping policy allocates & limits the maximum bandwidth usage of the user.

A new traffic shaping policy can be created directly from this page or from the Device Configuration > System > Profiles > Traffic Shaping page.

**Application Protection**

Select an application protection policy for the server.

A new application protection policy can be created directly from this page or from the Device Configuration > Protect > Web Server > Protection Policies page.

Default: ExchangeAutoDiscover

b) Specify Advanced settings for the added server.

**Disable Compression Support**

By default, this checkbox is disabled and the content is sent compressed when the client requests compressed data. Compression increases transmission speed and reduces page load time. However, in case of websites being displayed incorrectly or when users experience content-encoding errors accessing your web servers, it can be necessary to disable compression support. When the checkbox is enabled, the WAF will request uncompressed data from the web servers of this hosted web server and will send it on uncompressed to the client, independent of the HTTP request's encoding parameter.

Default: Disabled

**Rewrite HTML**

Select this option to have the device rewrite links of the returned webpages in order for the links to stay valid. Example: One of your web server instances has the hostname yourcompany.local but the hosted web server's hostname on the device is yourcompany.com. Thus, absolute links like [a href="http://yourcompany.local"] will be broken if the link is not rewritten to [a href="http://yourcompany.com"] before delivery to the client. However, you do not need to enable this option if either yourcompany.com is configured on your web server or if internal links on your webpages are always realized as relative links. It is recommended to use the option with Microsoft's Outlook web access and/or SharePoint portal server.

**Note**

HTML rewriting affects all files with a HTTP content type of text/* or *xml*, where * is a wild card. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the HTML rewriting feature.
Rewrite cookies (only available if Rewrite HTML is selected)
Select this option to have the device rewrite cookies of the returned web pages.

Note
If Rewrite HTML is disabled the Rewrite cookies option will also be disabled.

Pass Host Header
When you select this option, the host header as requested by the client will be preserved and forwarded along with the web request to the web server. Whether passing the host header is necessary in your environment however depends on the configuration of your web server.

Default: Enabled

Figure 28: Advanced

9. Click Save.

Note
As soon as a new HTTP based policy configuration has been created and saved or an existing HTTP based rule configuration has been altered and saved, all HTTP based business rules will be restarted. Any underlying client connection using a HTTP based business rule will get lost and has to be re-established.

The firewall rule for Microsoft Remote Desktop Gateway 2008 and R2 has been created and appears on the Firewall page when the IPv4 filter is set.

Exchange Outlook Anywhere
(only available for IPv4 policy) This page describes how to configure a rule for Exchange Outlook Anywhere.

1. Go to Device Configuration > Protect > Firewall and select IPv4. using the filter switch.
2. Click +Add Firewall Rule and Business Application Rule.
3. Specify the general policy details.

Application Template
Select Exchange Outlook Anywhere to configure rule for Exchange Outlook Anywhere.

Description
Specify a description for the rule.

Rule Position
Specify the position of the rule.
Available Options: TopBottom

Rule Name
Specify a name for the rule.

Figure 29: About This Rule

Hosted Address
Specify the address of the hosted server to which the rule applies. It is the public IP address through which Internet users access an internal server/host.
Note
When a connection is established by a client device and the client accesses the web server, the web server does not obtain the real client IP address. Reason is that the connection is made through the Web Application Firewall, so the address of the interface the WAF uses for the connection is delivered. To receive the real client IP address, the administrator has to read out the contents of the HTTP header "X-Forwarded-For".

Listening Port
Enter a port number on which the hosted web server can be reached externally over the Internet. Default is port 80 for plaintext communication (HTTP) and port 443 for encrypted communication (HTTPS).

HTTPS
Select to enable or disable scanning of HTTPS traffic.

HTTPS Certificate (only available if HTTPS is selected)
Select the HTTPS certificate to be used.

Redirect HTTP (only available if HTTPS is selected)
Select to redirect HTTP requests.

Domains
Enter the domains the web server is responsible for as FQDN, e.g. shop.example.com.

Path-specific routing
You can enable path-specific routing to define (path) to which web servers incoming requests are forwarded.

You can define that all URLs with a specific path, for example, /products/, are sent to a specific web server. On the other hand you can allow more than one web server for a specific request but add rules how to distribute the requests among the servers. Additionally, you can define that each session is bound to one web server throughout its lifetime (sticky session). This may be necessary if you host an online shop and want to make sure that a user sticks to one server during the shopping session. You can also configure to send all requests to one web server and use the others only as a backup.

For each hosted web server, one default site path route (with path /) is created automatically. The device automatically applies the site path routes in the most reasonable way: starting with the strictest, i.e., longest paths and ending with the default path route which is only used if no other more specific site path route matches the incoming request. The order of the site path route list is not relevant. If no route matches an incoming request, (in case the default route was deleted), the request will be denied.

Add New Path (only available if Path-specific routing is selected)
Click Add New Path to define a new path.
Note
Add New Path will only be active after at least one web server and one hosted web server have been created.

Default: /rpc, /RPC

Web Server (not available if Path-specific routing is selected)
Web servers are the application servers that are to be protected. Select a web server from the list of web servers or click Add New Item to add a web server.

A new web server can be created directly from this page or from the Device Configuration > Protect > Web Server > Web Servers page.

Figure 31: Protected Application Server(s)


Allowed Client Networks
Select the allowed host(s)/network(s).

Blocked Client Networks
Select the blocked host(s)/network(s).

Authentication
Select the web application authentication profile from the list of available profiles. You can also create a new authentication profile from this page or from the Device Configuration > Protect > Web Server > Authentication Policies page.

Figure 32: Access Permission

7. Add path Exceptions for the web servers.

Click Add New Exception to specify new exception.

Add Exception
Default: /rpc/*,/RPC/*.

Figure 33: Exceptions

8. Configure advanced settings.

a) Specify Profiles for Business Applications.

Intrusion Prevention
Select an IPS policy for the rule.

A new IPS policy can be created directly from this page or from the Device Configuration > Protect > Intrusion Prevention > IPS Policies page.

Traffic Shaping
Select a traffic shaping policy for the rule.

A traffic shaping policy allocates & limits the maximum bandwidth usage of the user.

A new traffic shaping policy can be created directly from this page or from the Device Configuration > System > Profiles > Traffic Shaping page.

Application Protection
Select an application protection policy for the server.

A new application protection policy can be created directly from this page or from the Device Configuration > Protect > Web Server > Protection Policies page.

Default: Exchange Outlook Anywhere

Figure 34: Policies for Business Applications
b) Specify Advanced settings for the added server.

**Disable Compression Support**

By default, this check box is disabled and the content is sent compressed when the client requests compressed data. Compression increases transmission speed and reduces page load time. However, in case of websites being displayed incorrectly or when users experience content-encoding errors accessing your web servers, it can be necessary to disable compression support. When the check box is enabled, the WAF will request uncompressed data from the web servers of this hosted web server and will send it on uncompressed to the client, independent of the HTTP request's encoding parameter.

**Rewrite HTML**

Select this option to have the device rewrite links of the returned web pages in order for the links to stay valid. Example: One of your web server instances has the hostname yourcompany.local but the hosted web server's hostname on the device is yourcompany.com. Thus, absolute links like [a href="http://yourcompany.local/"](http://yourcompany.local/) will be broken if the link is not rewritten to [a href="http://yourcompany.com/"](http://yourcompany.com/) before delivery to the client. However, you do not need to enable this option if either yourcompany.com is configured on your web server or if internal links on your web pages are always realized as relative links. It is recommended to use the option with Microsoft's Outlook web access and/or SharePoint portal server.

**Note**

HTML rewriting affects all files with a HTTP content type of text/* or *xml*, where * is a wildcard. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the HTML rewriting feature.

Default: Disabled

**Rewrite cookies (only available if Rewrite HTML is selected)**

Select this option to have the device rewrite cookies of the returned web pages.

**Note**

If Rewrite HTML is disabled the Rewrite cookies option will also be disabled.

**Pass Host Header**

When you select this option, the host header as requested by the client will be preserved and forwarded along with the web request to the web server. Whether passing the host header is necessary in your environment however depends on the configuration of your web server.

Default: Disabled

Figure 35: Advanced

9. Click **Save**.

**Note**

As soon as a new HTTP based rule configuration has been created and saved or an existing HTTP based rule configuration has been altered and saved, all HTTP based business rules will be restarted. Any underlying client connection using a HTTP based business rule will get lost and has to be re-established.
The Exchange Outlook Anywhere rule has been created and appears on the Firewall page when the IPv4 filter is set.

*Exchange General*
*(only available for IPv4 policy)* This page describes how to configure a rule for Exchange General.

1. Go to Device Configuration > Protect > Firewall and select IPv4, using the filter switch.
2. Click Add Firewall Rule and Business Application Rule.
3. Specify the general policy details.

**Application Template**
Select Exchange General to configure a rule for Exchange General.

**Description**
Specify a description for the rule.

**Rule Position**
Specify the position of the rule.

*Available Options: TopBottom*

**Rule Name**
Specify a name for the rule.

**Hosted Server**
Specify the address of the hosted server to which the rule applies. It is the public IP address through which Internet users access an internal server/host.

*Note*
When a connection is established by a client device and the client accesses the web server, the web server does not obtain the real client IP address. Reason is that the connection is made through the Web Application Firewall, so the address of the interface the WAF uses for the connection is delivered. To receive the real client IP address, the administrator has to read out the contents of the HTTP header "X-Forwarded-For".

**Listening Port**
Enter a port number on which the hosted web server can be reached externally over the Internet. Default is port 80 for plaintext communication (HTTP) and port 443 for encrypted communication (HTTPS).

**HTTPS**
Select to enable or disable scanning of HTTPS traffic.

**HTTPS Certificate (only available if HTTPS is selected)**
Select the HTTPS certificate to be used.

**Redirect HTTP (only available if HTTPS is selected)**
Select to redirect HTTP requests.

**Domains**
Enter the domains the web server is responsible for as FQDN, e.g. shop.example.com.

**Path-specific routing**
You can enable path-specific routing to define (path) to which web servers incoming requests are forwarded.

You can define that all URLs with a specific path, for example, /products/, are sent to a specific web server. On the other hand you can allow more than one web server for a specific request but add rules how to distribute the requests among the servers. Additionally, you can define that each session is bound to one web server throughout its lifetime (sticky session). This may be necessary if you host an online shop and want to make sure that a user sticks to one server during the shopping session. You can also configure to send all requests to one web server and use the others only as a backup.

For each hosted web server, one default site path route (with path /) is created automatically. The device automatically applies the site path routes in the most reasonable way: starting with the strictest, i.e., longest paths and ending with the default path route which is only used if no other more specific site path route matches the incoming request. The order of the site path route list is not relevant. If no route matches an incoming request, (in case the default route was deleted), the request will be denied.

**Add New Path** *(only available if Path-specific routing is selected)*

Click **Add New Path** to define a new path.

**Note**

**Add New Path** will only be active after at least one web server and one hosted web server have been created.

Default: /owa, /OWA, /ecp, /ECP, /oab, /OAB, /ews, /EWS, /oma, /OMA, /Microsoft-Server-ActiveSync

**Web Servers** *(not available if Path-specific routing is selected)*

Web servers are the application servers that are to be protected. Select a web server from the list of web servers or click **Add New Item** to add a web server.

A new web server can be created directly from this page or from the **Device Configuration > Protect > Web Server > Web Servers** page.

**Figure 38: Protected Application Server(s)**

6. Specify **Access Permission** details. *(not available if Path-specific routing is selected)*

**Allowed Client Networks**

Select the allowed host(s)/network(s).

**Blocked Client Networks**

Select the blocked host(s)/network(s).

**Authentication**

Select the web application authentication profile from the list of available profiles. You can also create new authentication profile on this page or on the **Device Configuration > Protect > Web Server > Authentication Policies** page.

**Figure 39: Access Permission**

7. Add path **Exceptions** for the web servers.

Click **Add New Exception** to specify a new exception.
8. Configure advanced settings.

a) Specify Profiles for Business Applications.

**Intrusion Prevention**

Select an IPS policy for the rule.

A new IPS policy can be created directly from this page or from the Device Configuration > Protect > Intrusion Prevention > IPS Policies page.

**Traffic Shaping**

Select a traffic shaping policy for the rule.

A traffic shaping policy allocates & limits the maximum bandwidth usage of the user.

A new traffic shaping policy can be created directly from this page or from the Device Configuration > System > Profiles > Traffic Shaping page.

**Application Protection**

Select an application protection policy for the server.

A new application protection policy can be created directly from this page or from the Device Configuration > Protect > Web Server > Protection Policies page.

Default: Exchange General

b) Specify **Advanced** settings for the added server.

**Disable Compression Support**

By default, this check box is disabled and the content is sent compressed when the client requests compressed data. Compression increases transmission speed and reduces page load time. However, in case of websites being displayed incorrectly or when users experience content-encoding errors accessing your web servers, it can be necessary to disable compression support. When the check box is enabled, the WAF will request uncompressed data from the web servers of this hosted web server and will send it on uncompressed to the client, independent of the HTTP request’s encoding parameter.

Default: Disabled

**Rewrite HTML**

Select this option to have the device rewrite links of the returned webpages in order for the links to stay valid. Example: One of your web server instances has the hostname yourcompany.local but the hosted web server's hostname on the device is yourcompany.com. Thus, absolute links like [a href="http://yourcompany.local/"] will be broken if the link is not rewritten to [a href="http://yourcompany.com/"] before delivery to the client. However, you do not need to enable this option if either yourcompany.com is configured on your web server or if internal links on your web pages are always realized as relative links. It is recommended to use the option with Microsoft's Outlook web access and/or SharePoint portal server.
Note
HTML rewriting affects all files with a HTTP content type of text/* or "xml", where *
 is a wild card. Make sure that other file types, e.g. binary files, have the correct
HTTP content type, otherwise they may get corrupted by the HTML rewriting
feature.

Rewrite cookies (only available if Rewrite HTML is selected)
Select this option to have the device rewrite cookies of the returned web pages.

Note
If Rewrite HTML is disabled the Rewrite cookies option will also be disabled.

Default: Disabled

Pass Host Header
When you select this option, the host header as requested by the client will be
preserved and forwarded along with the web request to the web server. Whether
passing the host header is necessary in your environment however depends on the
configuration of your web server.

Default: Disabled

Figure 42: Advanced

9. Click Save.

Note
As soon as a new HTTP based rule configuration has been created and saved or an existing
HTTP based rule configuration has been altered and saved, all HTTP based business rules will
be restarted. Any underlying client connection using a HTTP based business rule will get lost
and has to be re-established.

The Exchange General rule has been created and appears on the Firewall page when the IPv4 filter is set.

Microsoft Lync
(only available for IPv4 policy) This page describes how to configure a rule for Microsoft Lync.

1. Go to Device Configuration > Protect > Firewall and select IPv4. using the filter switch.
2. Click +Add Firewall Rule and Business Application Rule.
3. Specify the general rule details.

Application Template
Select Microsoft Lync to define Application filter policy for HTTP based applications.

Description
Specify the rule description.

Rule Position
Specify the position of the rule.

Available Options:
• Top
• Bottom
**Rule Name**

Specify a name to identify the rule.

*Figure 43: About This Rule*

4. Specify **Hosted Server** details.

**Hosted Address**

Specify the address of the hosted server to which the rule applies. It is the public IP address through which Internet users access internal server/host.

**Note**

When a connection is established by a client device and the client accesses the web server, the web server does not obtain the real client IP address. Reason is that the connection is made through the Web Application Firewall, so the address of the interface the WAF uses for the connection is delivered. To receive the real client IP address, the administrator has to read out the contents of the HTTP header "X-Forwarded-For".

**Listening Port**

Enter a port number on which the hosted web server can be reached externally over the Internet. Default is port 80 for plaintext communication (HTTP) and port 443 for encrypted communication (HTTPS).

**HTTPS**

Click to enable or disable scanning of HTTPS traffic.

**HTTPS Certificate (available if HTTPS is enabled)**

Select the HTTPS certificate to be used.

**Redirect HTTP (available if HTTPS is enabled)**

Click to redirect HTTP requests.

**Domains**

Enter the domains the web server is responsible for as FQDN, e.g. shop.example.com.

*Figure 44: Hosted Server*

5. Specify **Protected Server(s)** details.

**Path-specific routing**

You can enable path-specific routing to define (the path) to which web servers incoming requests are forwarded.

You can define that all URLs with a specific path, for example, /products/, are sent to a specific web server. On the other hand you can allow more than one web server for a specific request but add rules how to distribute the requests among the servers. Additionally, you can define that each session is bound to one web server throughout its lifetime (sticky session). This may be necessary if you host an online shop and want to make sure that a user sticks to one server during the shopping session. You can also configure to send all requests to one web server and use the others only as a backup.

For each hosted web server, one default site path route (with path /) is created automatically. The device automatically applies the site path routes in the most reasonable way: starting with the strictest, i.e., longest paths and ending with the default path route which is only used if no other more specific site path route matches the incoming request. The order of the site path route list is not relevant. If no route matches an incoming request, (in case the default route was deleted), the request will be denied.
Add New Path (*available if Path-specific routing is enabled*)
Click Add Path to define a new path.

Add Path

Note
Add New Path will only be active after at least one web server and one hosted web server have been created.

Web Server (*available if Path-specific routing is disabled*)
Hosts are the web servers that are to be protected. Select a web server from the list of web servers or click Add New Item to add a web server.

A new web server can be created directly from this page or from the Device Configuration > Protect > Web Server > Web Servers page.

Figure 45: Protected Application Server(s)

6. Specify Access Permission details (*not available if Path-specific routing is selected*).

Allowed Client Networks
Select the allowed host(s)/network(s).

Blocked Client Networks
Select the blocked host(s)/network(s).

Authentication
Select the web application authentication profile from the list of available profiles.
You can also create a new authentication profile on this page or on the Device Configuration > Protect > Web Server > Authentication Policies page.

Figure 46: Access Permission

7. Specify path Exceptions for the web servers.
Click Add New Exception to specify a new exception.
Add Exception

Figure 47: Exceptions

8. Configure advanced settings.

a) Specify Profiles for Business Applications.

Intrusion Prevention (IPS)
Select an IPS policy for the rule.
A new IPS Policy can be created directly from this page or from the Device Configuration > Protect > Intrusion Prevention > IPS Policies page.

Traffic Shaping
Select a traffic shaping policy for the rule.
A traffic shaping policy allocates & limits the maximum bandwidth usage of the user.
A new traffic shaping policy can be created directly from this page or from the Device Configuration > System > Profiles > Traffic Shaping page.

Application Protection
Select an application protection policy for the server.
A new application protection policy can be created directly from this page or from the Device Configuration > Protect > Web Server > Protection Policies page.

Figure 48: Policies for Business Applications
b) Specify Advanced settings for the added server.

**Disable Compression Support**

By default, this check box is disabled and the content is sent compressed when the client requests compressed data. Compression increases transmission speed and reduces page load time. However, in case of websites being displayed incorrectly or when users experience content-encoding errors accessing your web servers, it can be necessary to disable compression support. When the check box is enabled, the WAF will request uncompressed data from the Web Servers of this Hosted web server and will send it on uncompressed to the client, independent of the HTTP request's encoding parameter.

**Rewrite HTML**

Select this option to have the device rewrite links of the returned webpages in order for the links to stay valid. Example: One of your Web Server instances has the hostname yourcompany.local but the Hosted web server's hostname on the device is yourcompany.com. Thus, absolute links like [a href="http://yourcompany.local/"] will be broken if the link is not rewritten to [a href="http://yourcompany.com/"] before delivery to the client. However, you do not need to enable this option if either yourcompany.com is configured on your web server or if internal links on your webpages are always realized as relative links. It is recommended to use the option with Microsoft's Outlook Web Access and/or Sharepoint Portal Server.

*Note*

HTML rewriting affects all files with a HTTP content type of text/* or *xml*, where * is a wildcard. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the HTML rewriting feature.

**Rewrite cookies (available if Rewrite HTML is enabled)**

Select this option to have the device rewrite cookies of the returned webpages.

*Note*

If Rewrite HTML is disabled the Rewrite cookies option will also be disabled.

**Pass Host Header**

When you select this option, the host header as requested by the client will be preserved and forwarded along with the web request to the web server. Whether passing the host header is necessary in your environment however depends on the configuration of your web server.

Figure 49: Advanced

9. Click **Save**.

*Note*

As soon as a new HTTP based rule configuration has been created and saved or an existing HTTP based rule configuration has been altered and saved, all HTTP based business rules will be restarted. Any underlying client connection using a HTTP based business rule will get lost and has to be re-established.

The Microsoft Lync rule has been created and appears on the **Firewall** page when the IPv4 filter is set.
Microsoft Remote Desktop Gateway 2008 and R2
(only available for IPv4 policy) This page describes how to configure a rule for Microsoft Remote Desktop Gateway 2008 and R2.

1. Go to Device Configuration > Protect > Firewall and select IPv4, using the filter switch.
2. Click +Add Firewall Rule and Business Application Rule.
3. Specify the general rule details.

Application Template
Select Microsoft Remote Desktop Gateway 2008 and R2 to configure a rule for Microsoft Remote Desktop Gateway 2008 and R2.

Description
Specify the rule description.

Rule Position
Specify the position of the rule.
Available Options:
• Top
• Bottom

Rule Name
Specify a name to identify the rule.

Hosted Server details.

Hosted Address
Specify the address of the hosted server to which the rule applies. It is the public IP address through which Internet users access an internal server/host.

Note
When a connection is established by a client device and the client accesses the web server, the web server does not obtain the real client IP address. Reason is that the connection is made through the Web Application Firewall, so the address of the interface the WAF uses for the connection is delivered. To receive the real client IP address, the administrator has to read out the contents of the HTTP header "X-Forwarded-For".

Listening Port
Enter a port number on which the hosted web server can be reached externally, over the Internet. Default is port 80 for plaintext communication (HTTP) and port 443 for encrypted communication (HTTPS).

HTTPS
Click to enable or disable scanning of HTTPS traffic.

HTTPS Certificate (available if HTTPS is enabled)
Select the HTTPS certificate to be used.

Redirect HTTP (available if HTTPS is enabled)
Click to redirect HTTP requests.

Domains
Enter the domains the web server is responsible for as FQDN, e.g. shop.example.com.
5. Specify **Protected Server(s)** details.

**Path-specific routing**

You can enable path-specific routing to define (a path) to which web servers incoming requests are forwarded.

You can define that all URLs with a specific path, for example, /products/, are sent to a specific web server. On the other hand you can allow more than one web server for a specific request but add rules how to distribute the requests among the servers. Additionally, you can define that each session is bound to one web server throughout its lifetime (sticky session). This may be necessary if you host an online shop and want to make sure that a user sticks to one server during the shopping session. You can also configure to send all requests to one web server and use the others only as a backup.

For each hosted web server, one default site path route (with path '/') is created automatically. The device automatically applies the site path routes in the most reasonable way: starting with the strictest, i.e., longest paths and ending with the default path route which is only used if no other more specific site path route matches the incoming request. The order of the site path route list is not relevant. If no route matches an incoming request, (in case the default route was deleted), the request will be denied.

**Add New Path (available if Path-specific routing is enabled)**

Click **Add New Path** to define a new path.

**Add Path**

**Note**

**Add New Path** will only be active after at least one web server and one hosted web server have been created.

**Web Server (available if Path-specific routing is disabled)**

Web servers are the application servers that are to be protected. Select from the list of web servers or click **Add New Item** to add a web server.

A new web server can be created directly from this page or from the **Device Configuration > Protect > Web Server > Web Servers** page.

Figure 52: Protected Application Server(s)

6. Specify access permission details. *(Available if Path-specific routing is disabled)*

**Allowed Client Networks**

Select the allowed host(s)/network(s).

**Blocked Client Networks**

Select the blocked host(s)/network(s).

**Authentication**

Select the web application authentication profile from the list of available profiles. You can also create a new authentication profile from this page or from the **Device Configuration > Protect > Web Server > Authentication Policies** page.

Figure 53: Access Permission

7. Specify path **Exceptions** for the web servers.

Click **Add New Exception** to specify new exception.

**Add Exception**

Figure 54: Exceptions
8. Configure advanced settings.
   a) Specify Profiles for Business Applications.

**Intrusion Prevention**

Select an IPS policy for the rule.

A new IPS policy can be created directly from this page or from the Device Configuration > Protect > Intrusion Prevention > IPS Policies page.

**Traffic Shaping**

Select a traffic shaping policy for the rule.

A traffic shaping allocates & limits the maximum bandwidth usage of the user.

A new traffic shaping policy can be created directly from this page or from the Device Configuration > System > Profiles > Traffic Shaping page.

**Application Protection**

Select an application protection policy for the server.

A new application protection policy can be created directly from this page or from the Device Configuration > Protect > Web Server > Protection Policies page.

Default: Microsoft RDG 2008

Figure 55: Policies for Business Applications

b) Specify Advanced Settings for the added server.

**Disable Compression Support**

By default, this check box is disabled and the content is sent compressed when the client requests compressed data. Compression increases transmission speed and reduces page load time. However, in case of websites being displayed incorrectly or when users experience content-encoding errors accessing your web servers, it can be necessary to disable compression support. When the check box is enabled, the WAF will request uncompressed data from the web servers of this hosted web server and will send it on uncompressed to the client, independent of the HTTP request's encoding parameter.

**Rewrite HTML**

Select this option to have the device rewrite links of the returned web pages in order for the links to stay valid. Example: One of your web server instances has the hostname yourcompany.local but the hosted web server's hostname on the device is yourcompany.com. Thus, absolute links like [a href="http://yourcompany.local/"] will be broken if the link is not rewritten to [a href="http://yourcompany.com/"] before delivery to the client. However, you do not need to enable this option if either yourcompany.com is configured on your web server or if internal links on your web pages are always realized as relative links. It is recommended to use the option with Microsoft's Outlook web access and/or SharePoint portal server.

**Note**

HTML rewriting affects all files with a HTTP content type of text/* or *xml*, where * is a wild card. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the HTML rewriting feature.

**Rewrite cookies (Applicable only if Rewrite HTML is enabled)**

Select this option to have the device rewrite cookies of the returned web pages.
Note
If Rewrite HTML is disabled the Rewrite cookies option will also be disabled.

Pass Host Header
When you select this option, the host header as requested by the client will be preserved and forwarded along with the web request to the web server. Whether passing the host header is necessary in your environment however depends on the configuration of your web server.

Figure 56: Advanced
9. Click Save.

Note
As soon as a new HTTP based rule configuration has been created and saved or an existing HTTP based rule configuration has been altered and saved, all HTTP based business rules will be restarted. Any underlying client connection using a HTTP based business rule will get lost and has to be re-established.

The rule for Microsoft Remote Desktop Gateway 2008 and R2 has been created and appears on the Firewall page when the IPv4 filter is set.

Microsoft Remote Desktop Web 2008 and R2
(only available for IPv4 policy) This page describes how to configure a rule for Microsoft Remote Desktop Web 2008 and R2.

1. Go to Device Configuration > Protect > Firewall and select IPv4. using the filter switch.
2. Click +Add Firewall Rule and Business Application Rule.
3. Specify the general rule details.

Application Template
Select Microsoft Remote Desktop Web 2008 and R2 to configure a rule for Microsoft Remote Desktop Web 2008 and R2.

Description
Specify the rule description.

Rule Position
Specify the position of the rule.

Available Options: TopBottom

Rule Name
Specify a name to identify the rule.

Figure 57: About This Rule

Hosted Address
Specify the address of the hosted server to which the rule applies. It is the public IP address through which Internet users access an internal server/host.
When a connection is established by a client device and the client accesses the web server, the web server does not obtain the real client IP address. Reason is that the connection is made through the Web Application Firewall, so the address of the interface the WAF uses for the connection is delivered. To receive the real client IP address, the administrator has to read out the contents of the HTTP header "X-Forwarded-For".

Listening Port

Enter a port number on which the hosted web server can be reached externally over the Internet. Default is port 80 for plaintext communication (HTTP) and port 443 for encrypted communication (HTTPS).

HTTPS

Click to enable or disable scanning of HTTPS traffic.

HTTPS Certificate (available if HTTPS is enabled)

Select the HTTPS certificate to be used.

Redirect HTTP (available if HTTPS is enabled)

Click to redirect HTTP requests.

Domains

Enter the domains the web server is responsible for as FQDN, e.g. shop.example.com.

Figure 58: Hosted Server

5. Specify Protected Server(s) details.

Path-specific routing

You can enable path-specific routing to define (the path) to which web servers incoming requests are forwarded.

You can define that all URLs with a specific path, for example, /products/, are sent to a specific web server. On the other hand you can allow more than one web server for a specific request but add rules how to distribute the requests among the servers. Additionally, you can define that each session is bound to one web server throughout its lifetime (sticky session). This may be necessary if you host an online shop and want to make sure that a user sticks to one server during the shopping session. You can also configure to send all requests to one web server and use the others only as a backup.

For each hosted web server, one default site path route (with path /) is created automatically. The device automatically applies the site path routes in the most reasonable way: starting with the strictest, i.e., longest paths and ending with the default path route which is only used if no other more specific site path route matches the incoming request. The order of the site path route list is not relevant. If no route matches an incoming request, (in case the default route was deleted), the request will be denied.

Add New Path (available if Path-specific routing is enabled)

Click Add New Path to define a new path.

Add Path
Note
Add New Path will only be active after at least one web server and one hosted web server have been created.

Web Server (available if Path-specific routing is disabled)
Web servers are the application servers that are to be protected. Select a web server from the list of web servers or click Add New Item to add a web server.
A new web server can be created directly on this page or on the Device Configuration > Protect > Web Server > Web Servers page.

Figure 59: Protected Application Server(s)


Allowed Client Networks
Select the allowed host(s)/network(s).

Blocked Client Networks
Select the blocked host(s)/network(s).

Authentication
Select the web application authentication profile from the list of available profiles.
You can also create new authentication profile on this page or on the Device Configuration > Protect > Web Server > Authentication Policies page.

Figure 60: Access Permission

7. Add path Exceptions for the web servers.
Click Add New Exception to specify new exception.
Add Exception
Figure 61: Exceptions

8. Configure advanced settings.

a) Specify Profiles for Business Applications.

Intrusion Prevention
Select an IPS policy for the rule.
A new IPS policy can be created directly on this page or on the Device Configuration > Protect > Intrusion Prevention > IPS Policies page.

Traffic Shaping
Select a traffic shaping policy for the rule.
A traffic shaping policy allocates & limits the maximum bandwidth usage of the user.
A new traffic shaping policy can be created directly from this page itself or from the Device Configuration > System > Profiles > Traffic Shaping page.

Application Protection
Select an application protection policy for the server.
A new application protection policy can be created directly on this page itself or on the Device Configuration > Protect > Web Server > Protection Policies page.
Default: Microsoft RD Web 2008

Figure 62: Policies for Business Application

b) Specify Advanced settings for the added server.
Disable Compression Support

By default, this check box is disabled and the content is sent compressed when the client requests compressed data. Compression increases transmission speed and reduces page load time. However, in case of websites being displayed incorrectly or when users experience content-encoding errors accessing your web servers, it can be necessary to disable compression support. When the check box is enabled, the WAF will request uncompressed data from the web servers of this hosted web server and will send it on uncompressed to the client, independent of the HTTP request's encoding parameter.

Default: Disabled

Rewrite HTML

Select this option to have the device rewrite links of the returned webpages in order for the links to stay valid. Example: One of your web server instances has the hostname yourcompany.local but the hosted web server's hostname on the device is yourcompany.com. Thus, absolute links like [a href="http://yourcompany.local/"] will be broken if the link is not rewritten to [a href="http://yourcompany.com/"] before delivery to the client. However, you do not need to enable this option if either yourcompany.com is configured on your web server or if internal links on your web pages are always realized as relative links. It is recommended to use the option with Microsoft's Outlook web access and/or SharePoint portal server.

Note

HTML rewriting affects all files with a HTTP content type of text/* or *xml*, where * is a wild card. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the HTML rewriting feature.

Default: Disabled

Rewrite cookies (available if Rewrite HTML is enabled)

Select this option to have the device rewrite cookies of the returned web pages.

Note

If Rewrite HTML is disabled, the Rewrite cookies option will also be disabled.

Pass Host Header

When you select this option, the host header as requested by the client will be preserved and forwarded along with the web request to the web server. Whether passing the host header is necessary in your environment however depends on the configuration of your web server.

Default: Enabled

Figure 63: Advanced

9. Click Save.

Note

As soon as a new HTTP based rule configuration has been created and saved or an existing HTTP based rule configuration has been altered and saved, all HTTP based business rules will be restarted. Any underlying client connection using a HTTP based business rule will get lost and has to be re-established.
The rule for Microsoft Remote Desktop Web 2008 and R2 has been created and appears on the Firewall page when the IPv4 filter is set.

**Microsoft Sharepoint 2010 and 2013**
*(only available for IPv4 policy)* This page describes how to configure a rule for Microsoft SharePoint 2010 and 2013.

1. Go to **Device Configuration > Protect > Firewall** and select **IPv4**, using the filter switch.
2. Click **+Add Firewall Rule** and **Business Application Rule**.
3. Specify the general rule details.

**Application Template**

Select **Microsoft Sharepoint 2010 and 2013** to configure a rule for Microsoft Sharepoint 2010 and 2013.

**Description**

Specify the rule description.

**Rule Position**

Specify the position of the rule.

**Available Options:**

- Top
- Bottom

**Rule Name**

Specify a name to identify the rule.

**Hosted Address**

Specify the address of the hosted server to which the rule applies. It is the public IP address through which Internet users access an internal server/host.

**Note**

When a connection is established by a client device and the client accesses the web server, the web server does not obtain the real client IP address. Reason is that the connection is made through the Web Application Firewall, so the address of the interface the WAF uses for the connection is delivered. To receive the real client IP address, the administrator has to read out the contents of the HTTP header "X-Forwarded-For".

**Listening Port**

Enter a port number on which the hosted web server can be reached externally over the Internet. Default is port 80 for plaintext communication (HTTP) and port 443 for encrypted communication (HTTPS).

**HTTPS**

Click to enable or disable scanning of HTTPS traffic.

**HTTPS Certificate (available if HTTPS is enabled)**

Select the HTTPS certificate to be used.

**Redirect HTTP (available if HTTPS is enabled)**

Click to redirect HTTP requests.

**Domains**
Enter the domains the web server is responsible for as FQDN, e.g. shop.example.com.

Figure 65: Hosted Server

5. Specify **Protected Server(s)** details.

**Path-specific routing**

You can enable path-specific routing to define (a path) to which web servers incoming requests are forwarded.

You can define that all URLs with a specific path, for example, /products/, are sent to a specific web server. On the other hand you can allow more than one web server for a specific request but add rules how to distribute the requests among the servers. Additionally, you can define that each session is bound to one web server throughout its lifetime (sticky session). This may be necessary if you host an online shop and want to make sure that a user sticks to one server during the shopping session. You can also configure to send all requests to one web server and use the others only as a backup.

For each hosted web server, one default site path route (with path /) is created automatically. The device automatically applies the site path routes in the most reasonable way: starting with the strictest, i.e., longest paths and ending with the default path route which is only used if no other more specific site path route matches the incoming request. The order of the site path route list is not relevant. If no route matches an incoming request, (in case the default route was deleted), the request will be denied.

**Add New Path** *(available if Path-specific routing is enabled)*

Click **Add New Path** to define a new path.

**Add Path**

**Note**

**Add New Path** will only be active after at least one web server and one hosted web server have been created.

**Web Server** *(available if Path-specific routing is disabled)*

Web servers are the application servers that are to be protected. Select a web server from the list of web servers or click **Add New Item** to add a web server.

A new web server can be created directly from this page or from the **Device Configuration > Protect > Web Server > Web Servers** page.

Figure 66: Protected Application Server(s)

6. Specify **Access Permission** details *(available if Path-specific routing is disabled).*

**Allowed Client Networks**

Select the allowed host(s)/network(s).

**Blocked Client Networks**

Select the blocked host(s)/network(s).

**Authentication**

Select the web application authentication profile from the list of available profiles.

You can also create new authentication profile from this page or from the **Device Configuration > Protect > Web Server > Authentication Policies** page.

Figure 67: Access Permission

7. Add path **Exceptions** for the web servers.

Click **Add New Exception** to specify new exception.
Add Exception

Figure 68: Exceptions

8. Configure advanced settings.
   a) Specify Profiles for Business Applications.

Intrusion Prevention (IPS)
   Select an IPS policy for the rule.
   A new IPS policy can be created directly from this page or from the Device Configuration > Protect > Intrusion Prevention > IPS Policies page.

Traffic Shaping
   Select a traffic shaping policy for the rule.
   A traffic shaping policy allocates & limits the maximum bandwidth usage of the user.
   A new traffic shaping policy can be created directly from this page or from the Device Configuration > System > Profiles > Traffic Shaping page.

Application Protection
   Select an application protection policy for the server.
   A new application protection policy can be created directly from this page or from the Device Configuration > Protect > Web Server > Protection Policies page.

Figure 69: Policies for Business Applications
   b) Specify Advanced settings for the added server.

Disable Compression Support
   By default, this check box is disabled and the content is sent compressed when the client requests compressed data. Compression increases transmission speed and reduces page load time. However, in case of websites being displayed incorrectly or when users experience content-encoding errors accessing your web servers, it can be necessary to disable compression support. When the check box is enabled, the WAF will request uncompressed data from the web servers of this hosted web server and will send it on uncompressed to the client, independent of the HTTP request's encoding parameter.
   Default: Disabled

Rewrite HTML
   Select this option to have the device rewrite links of the returned web pages in order for the links to stay valid. Example: One of your web server instances has the hostname yourcompany.local but the Hosted web server's hostname on the device is yourcompany.com. Thus, absolute links like [a href="http://yourcompany.local/"] will be broken if the link is not rewritten to [a href="http://yourcompany.com/"] before delivery to the client. However, you do not need to enable this option if either yourcompany.com is configured on your web server or if internal links on your web pages are always realized as relative links. It is recommended to use the option with Microsoft's Outlook web access and/or SharePoint portal server.
   
   Note
   HTML rewriting affects all files with a HTTP content type of text/* or *xml*, where * is a wild card. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the HTML rewriting feature.
   Default: Disabled
Rewrite cookies *(available if Rewrite HTML is enabled)*

Select this option to have the device rewrite cookies of the returned web pages.

**Note**

If Rewrite HTML is disabled the Rewrite cookies option will also be disabled.

Pass Host Header

When you select this option, the host header as requested by the client will be preserved and forwarded along with the web request to the web server. Whether passing the host header is necessary in your environment however depends on the configuration of your web server.

Default: Enabled

Figure 70: Advanced

9. Click Save.

**Note**

As soon as a new HTTP based rule configuration has been created and saved or an existing HTTP based rule configuration has been altered and saved, all HTTP based business rules will be restarted. Any underlying client connection using a HTTP based business rule will get lost and has to be re-established.

The rule for Microsoft SharePoint 2010 and 2013 has been created and appears on the Firewall page when the IPv4 filter is set.

Add Path

Add Path page allows you to define (path) to which real web servers incoming requests are forwarded.

1. Enable path-specific routing and click Add New Path.
2. Specify the path details.

Path

Enter the path for which you want to create the site path route, Example: /products/.

Real Web Servers

Select the Real web servers which are to be used for the specified path.

Authentication

Select the Web App Authentication profile. Click Add New Item to create a new authentication profile. You can also create Authentication profile from Objects > Assets > Web App Authentication page.

Allow From

Select or add the allowed networks that should be able to connect to the Hosted web server.

Block From

Select or add the denied networks that should be blocked to your Hosted web server.

Enable sticky session cookie

Select this option to ensure that each session will be bound to one real web server. If enabled, a cookie is passed to the user’s browser, which provokes the UTM to route all requests from this browser to the same real web server. If the server is not available, the cookie will be updated, and the session will switch to another web server.

Enable hot-standby mode
Select this option if you want to send all requests to the first selected real web server, and use the other web servers only as a backup. The backup servers are only used in case the main server fails.

As soon as the main server starts functioning, the sessions will switch back - unless you have selected the Enable sticky session cookie option.

---

**Add exception**

*(only available for the HTTP based business application rules)* This page describes how to specify path exceptions for the web servers.

1. Click **Add new exception.**
2. Specify exception details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>Specify the path which you want to exclude.</td>
</tr>
<tr>
<td>Operation</td>
<td>Select the operation among <strong>AND</strong> or <strong>OR</strong> for <strong>Path</strong> and <strong>Source</strong>.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Source</strong></td>
<td>Specify the source networks where the client request comes from and which are to be exempted from the selected check(s).</td>
</tr>
</tbody>
</table>

3. Choose checks to skip.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cookie signing</strong></td>
<td>Click to skip cookie signing. Cookie signing protects a web server against manipulated cookies. When the web server sets a cookie, a second cookie is added to the first cookie containing a hash built of the primary cookie’s name, its value and a secret, where the secret is only known by the WAF. Thus, if a request cannot provide a correct cookie pair, there has been some sort of manipulation and the cookie will be dropped.</td>
</tr>
<tr>
<td><strong>Static URL hardening</strong></td>
<td>Protects against URL rewriting. When a client requests a website, all static URLs of the website are signed. The signing uses a similar procedure as with cookie signing. Additionally the response from the web server is analyzed in respect to the links that can be validly requested next.</td>
</tr>
<tr>
<td><strong>Form hardening</strong></td>
<td>Click to skip form hardening. Form hardening protects against web form rewriting. Form hardening saves the original structure of a web form and signs it. Therefore, if the structure of a form has changed when it is submitted the WAF rejects the request.</td>
</tr>
<tr>
<td><strong>Anti-virus</strong></td>
<td>Select this option to protect a web server against viruses.</td>
</tr>
<tr>
<td><strong>Block clients with bad reputation</strong></td>
<td>Based on GeoIPClosed and RBLClosed information you can block clients which have a bad reputation according to their classification.</td>
</tr>
</tbody>
</table>

4. Choose categories to skip.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protocol violations</strong></td>
<td>Enforces adherence to the RFC standard specification of the HTTP protocol. Violating these standards usually indicates malicious intent.</td>
</tr>
<tr>
<td><strong>Protocol anomalies</strong></td>
<td>Searches for common usage patterns. Lack of such patterns often indicates malicious requests. These patterns include, among other things, HTTP headers like “Host” and “User-Agent”.</td>
</tr>
<tr>
<td><strong>Request limits</strong></td>
<td>Enforces reasonable limits on the amount and ranges of request arguments. Overloading request arguments is a typical attack vector.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HTTP policy</td>
<td>Narrows down the allowed usage of the HTTP protocol. Web browsers typically use only a limited subset of all possible HTTP options. Disallowing the rarely used options protects against attackers aiming at these often less well supported options.</td>
</tr>
<tr>
<td>Bad robots</td>
<td>Checks for usage patterns characteristic of bots and crawlers. By denying them access, possible vulnerabilities on your web servers are less likely to be discovered.</td>
</tr>
<tr>
<td>Generic attacks</td>
<td>Searches for attempted command executions common to most attacks. After having breached a web server, an attacker usually tries to execute commands on the server like expanding privileges or manipulating data stores. By searching for these post-breach execution attempts, attacks can be detected that might otherwise have gone unnoticed, for example because they targeted a vulnerable service by the means of legitimate access.</td>
</tr>
<tr>
<td>SQL injection attacks</td>
<td>Checks for embedded SQL commands and escape characters in request arguments. Most attacks on web servers target input fields that can be used to direct embedded SQL commands to the database.</td>
</tr>
<tr>
<td>XSS attacks</td>
<td>Checks for embedded script tags and code in request arguments. Typical cross-site scripting attacks aim at injecting script code into input fields on a target web server, often in a legitimate way.</td>
</tr>
<tr>
<td>Tight security</td>
<td>Performs tight security checks on requests, like checking for prohibited path traversal attempts.</td>
</tr>
<tr>
<td>Trojans</td>
<td>Checks for usage patterns characteristic of trojans, thus searching for requests indicating trojan activity. It does not, however, prevent the installation of such trojans as this is covered by the antivirus scanners.</td>
</tr>
<tr>
<td>Outbound</td>
<td>Prevents web servers from leaking information to the client. This includes, among other things, error messages sent by servers which attackers can use to gather sensitive information or detect specific vulnerabilities.</td>
</tr>
</tbody>
</table>

5. Specify advanced settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Never change HTML during static URL hardening or form hardening</td>
<td>If selected, no data matching the defined exception settings will be modified by the WAF engine. With this option, e.g., binary data wrongly supplied with a text/html content type by the web server will not be corrupted.</td>
</tr>
</tbody>
</table>
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the other hand, web requests may</td>
<td>On the other hand, web requests may be blocked due to activated URL hardening, HTML rewriting, or form hardening. Those three features use an HTML parser and therefore to some extent depend on the modification of web page content. To prevent undesired blocking, skip URL hardening and/or form hardening for requests affected by blocking; you might need to do this in another/new exception to reflect dependencies between web servers and/or web pages.</td>
</tr>
<tr>
<td>Accept unhardened form data</td>
<td>Even though having an exception for form hardening, it is possible that form data will not be accepted if the form hardening signature is missing. With this option, unhardened form data will be accepted anyway.</td>
</tr>
</tbody>
</table>

6. Click **Save**.

**Add DNAT/Full NAT/Load Balancing Rule**

This page describes how to configure a DNAT/Full NAT/Load Balancing (Non-web) rule.

A DNAT/Full NAT/Load Balancing based rule is used to protect non-web servers, like mail or other servers hosted inside the network (LAN or DMZ). Using this rule, you can define access rights of such servers to users who require access over the WAN or Internet.

1. Go to **Device Configuration > Protect > Firewall** and select between **IPv4** or **IPv6** using the default filter.
2. Now, click **+Add Firewall Rule** and select **Business Application Rule**.
3. Specify the general rule details.

**Application Template**

Select **DNAT/Full NAT/Load Balancing** to configure a rule for generic Non-Web based applications.

**Description**

Specify a rule description.

**Rule Position**

Specify the position of the rule.

**Available Options:** TopBottom

**Rule Name**

Specify a name to identify the rule.

4. Specify **Source** details.

**Source Zones**

Select a source zone or click **Add New Item** to define a new LAN or DMZ zone.

**Allowed Client Networks**

Select the allowed host(s) or add a new one by clicking **Add New Item**.

**Blocked Client Networks**

Select the blocked host(s)/network(s).

5. Specify **Destination & Service** details.

**Firewall Version**

Choose from the following options:
**Available Options:** Firewalls running on SFOS v17
Firewalls running on SFOS v16.x

**Destination Host/Network**
Select the destination host/network to apply rule. It is the public IP address through which users access an internal server/host over the Internet.

**Available Options:** IP Address: Specified IP address is mapped to a corresponding mapped single IP address or a range of IP addresses. If a single IP address is mapped to a range of IP addresses, the device uses a round robin algorithm to load balance the requests.

**IP Range (only available for IPv4):** Specified IP address range is mapped to a corresponding range a corresponding range of mapped IP addresses. The IP range defines the start and end of an address range. The start of the range must be lower than the end of the IP. Select when any of the device port, alias or virtual LAN (VLAN) sub-interface is required to be mapped to the destination host or network.

**Services**
Select the services allowed to the user. A new service can be directly created from this page.

**Add new item**

**Name:** Enter a name to identify the service.

**Type:** Select a protocol for the service.

**Available Options:**
- **TCP/UDP:** Enter Source and Destination port. You can enter multiple ports for the same service. The number of source and destination ports must not exceed 16.
- **IP:** Select Protocol Number for the service. You can select multiple ports for the same service.
- **ICMP:** Select ICMP Type and Code. You can enter multiple types and codes for the same service. Use Add icon to add and delete the parameters respectively.
- **ICMPv6:** Select ICMPv6 Type and Code. You can enter multiple types and codes for the same service. Use Add and Remove to add and delete the parameters.

![Figure 72: Firewalls Running on SFOS v17](image)

**Forward Type**
Select the type of external port from the available options.

**Available Options:** Port Port Range Port List Everything

When **Everything** is selected, all ports are forwarded. Select other options to enable custom port forwarding and specify port forwarding details.
Service Port(s) Forwarded (Not Available if Forward Type selected is Everything)
Specify the public port number for which you want to configure port forwarding.

Protocol (Not Available if Forward Type selected is Everything)
Select the protocol TCP or UDP to be used by forwarding packets.

Figure 73: Firewalls Running on SFOS v16.x

6. Specify Forward To details.

Protected Server(s)
From the available options, select the application server(s) on which the web server is to be hosted.

Available options:
- IP Address – External IP address is mapped to the specified IP address.
- IP Range – External IP address range is mapped to the specified IP address range.
- IP List – External IP address is mapped to the specified IP list.
- FQDN – External IP address is mapped to the specified FQDN. Internal mapped server can be accessed by FQDN. This option is only available for IPv4 Virtual hosts.

Mapped Port Type (Available only if Change Destination Port(s) is selected)
Select the type of mapped port from the available options.

Available Options:
- Port
- Port Range
- Port List

Note
Not applicable for firewalls running on SFOS v17.

Mapped Port (Available only if Change Destination Port(s) is selected)
Specify the mapped port number on the destination network to which the public port number is mapped.

Protected Zone
Select the zone to apply web server rule.

Change Destination Port(s)
Select the check box to specify different mapped port. Clear the check box to use the same Service Port(s) Forwarded as mapped port.

Figure 74: Forward To
7. Specify **Load balancing** details.

**Load Balancing (only available if IP Range or IP List is selected for Protected Server and IP Address is selected for Destination Host/Network)**

Select the method for load balancing from the available options.

Available Options:
- **Round Robin** - In this method, requests are served in a sequential manner where the first request is forwarded to the first server, second request to the second server and so on. When a request is received, the device checks to see which was the last server that was assigned a request. It then assigns this new request to the next available server. This method can be used when equal distribution of traffic is required and there is no need for session-persistence. **First Alive** - In this method, all incoming requests are served by the first server (the first IP address that is configured in the IP range). This server is considered as the primary server and all others are considered as backup. Only when the first server fails, the requests are forwarded to the next server in line. This method is used for failover scenarios. **Random** - In this method, the requests are forwarded to the servers randomly. Nevertheless, the device makes sure that all configured servers receive equally distributed load. Hence, this method is also called uniform random distribution. This method can be used when equal distribution of traffic is required and there is no need for session-persistence or order of distribution. **Sticky IP** - In this method, along with the Round Robin distribution of traffic, the device forwards incoming traffic according to the source IP address. All traffic from a particular source is forwarded only to its mapped server. This means that all requests for a given source IP are sent to the same application server instance. This method is useful in cases where all requests or sessions are required to be processed by the same server. For example: banking websites, E-Commerce websites.

**Health Check (only available if Load Balancing is enabled)**

Click to enable a health check for failover and specify the parameters based on the description shown below.

**Port (Applicable if TCP Probe Health Check Method is selected)**

Specify the port number on the server health is monitored.

Acceptable range: 1 to 65535

**Interval**

Specify the time interval in seconds after which the health will be monitored.

Acceptable range: 5 to 65535 seconds

Default: 60

**Probe Method**

Select the probe method to check the health of the server from the available options.

Available Options: ICMP TCP

**Timeout**

Specify the time interval in seconds within which the server must respond.

Acceptable range: 1 to 10 seconds

Default: 2

**Retries**

Specify the number of tries to probe the health of the server, after which the server will be declared unreachable.

Acceptable range: 1 to 10

Default: 3
Match known users

Match rule based on user identity allows you to check whether the specified user/user group from the selected zone is allowed to access the selected service or not.

Click to attach the user identity.

Enable **check identity** to apply the following policies per user.

Show Captive Portal to unknown users

Select the check box to accept traffic from unknown users. Captive portal page is displayed to the user where the user can login to access the Internet.

Clear the check box to drop traffic from unknown users.

**User or Groups (Available if 'Match known users’ is selected)**

Select the user(s) or group(s) from the list of available options.

Exclude this user activity from data accounting (Available 'if Match known users’ is selected)

Click to enable/disable user traffic activity from data accounting.

By default, user’s network traffic is considered in data accounting. Select to exclude certain traffic from user data accounting. The traffic allowed through this firewall rule will not be accounted towards data transfer for the user.


   a) Specify **Policies for Business Applications**.

**Intrusion Prevention**

Select the required IPS policy. If **Match rule based on user identity** is enabled, user’s IPS policy will be applied automatically, but will not be effective till the respective module is subscribed. A new IPS policy can be created directly from this page or from the **Device Configuration > Protect > Intrusion Prevention > IPS Policies** page.

**Traffic Shaping Policy**

Select the required traffic shaping policy. If **Match rule based on user identity** is enabled, user’s traffic shaping policy will be applied automatically.

You need to select traffic shaping policy for the rule if **Match known users** is not selected.

A new traffic shaping policy can be created directly from this page or from the **Device Configuration > System > Profiles > Traffic Shapping** page.

   b) Specify Security Heartbeat details. *(only available if IPv4 is selected).*

**Minimum Source HB Permitted**

Select a minimum health status that a source device must have to conform to this rule. Health status can be either **Green, Yellow or No Restriction**. If the health criterion is not met, access and privileges defined in this rule will not be granted to the user.

**Block clients with no heartbeat**

Heartbeat-capable devices can be required to send information on their health status in defined intervals - this is called a heartbeat.

Based on that information, you can restrict a source device's access to certain services and networks.

Enable the option to require the sending of heartbeats.

**Minimum Destination HB Permitted (Not available if Protected Zone selected is WAN)**

Select a minimum health status that a destination device must have to conform to this rule. Health status can be either **Green, Yellow or No Restriction**. If the health criterion is not met, access and privileges defined in this rule will not be granted to the user.
Block request to destination with no heartbeat (Not available if Protected Zone selected is WAN)

Heartbeat-capable devices can be required to send information on their health status in defined intervals - this is called a heartbeat.

Based on that information, you can block requests to destinations not sending heartbeat.

Enable/disable the option to require the sending of heartbeats.

c) Specify Routing details.

Rewrite source address (Masquerading)

Enable/disable to re-write the source address or specify a NAT policy.

Create Reflexive Rule

Enable to automatically create a reflexive firewall rule for the protected host.

A reflexive rule has the same policies as those rules configured for the hosted server but instead of source zone to destination zone, this rule is applicable on traffic from destination zone to source zone.

By default, the reflexive rule is not created.

Use Outbound Address (only available if Rewrite source address is enabled)

Select the NAT policy to be applied from the list of available NAT policies.

A new NAT policy can be created directly from this page or from the Device Configuration > System > Profiles > Network Address Translation page.

The default NAT policy is Masquerade.

MASQ (Interface Default IP): IP Address of the selected Protected Zone as configured in Device Configuration > Configure > Network > Interfaces will be displayed instead of (Interface Default IP).

10. Specify the logging option for the user application traffic.

Log Firewall Traffic

Click to enable logging of permitted and denied traffic.

11. Click Save.

The non-web based rule has been created and appears on the Firewall page when the appropriate filter is set.

Email Servers (SMTP)

This page allows you to configure rule for Email Servers (SMTP).

1. Click Policies and select among IPv4 or IPv6 using the filter switch. Now, click on +Add Firewall Policy and select Business Application Rule.

2. Enter policy introduction for About This Rule.

Application Template

Select Email Servers (SMTP) to configure rule for SMTP based Email applications.

Description

Specify Policy Description.

Rule Position

Specify the position of the rule.

Available Options: TopBottom
Note
Rule Position can only be specified while creating a rule.

**Rule Name**
Specify a name to identify the policy.

Note
Rule Name can only be edited while creating a rule.

---

**Figure 75: About this Rule**

3. Specify **Source** details.

**Source Zones**
Click to select the source zone. Click **Add New Item** to define a new LAN or DMZ zone.

**Allowed Client Networks**
Select the allowed host(s) or add a new one by clicking **Add New Item**.

**Blocked Client Networks**
Select the blocked host(s)/network(s).

---

**Figure 76: Source**

4. Specify **Destination & Service** details.

**Firewall Version**
Choose from the following options:

*Available Options:* Firewalls running on SFOS v17/Firewalls running on SFOS v16.x

**Destination Host/Network**
Select the destination host/network to apply rule. It is the public IP address through which users access internal server/host over the Internet.

*Available Options:* IP Address – Specified IP address is mapped to a corresponding mapped single or range of IP addresses. If a single IP address is mapped to a range of IP addresses, the device uses a sticky IP algorithm to load balance the requests. **IP Range** – Specified IP address range is mapped to a corresponding range of mapped IP addresses. The IP range defines the start and end of an address range. The start of the range must be lower than the end of the range. **Interface IP** (only available for IPv4) – Select when any of the device port, alias or virtual LAN (VLAN) sub interface is required to be mapped to the destination host or network.

**Services**
Select the services allowed to the user. A new service can be directly created from this page.
Add new item

**Name:** Enter a name to identify the service.

**Type:** Select a protocol for the service.

**Available Options:**
- **TCP/UDP:** Enter Source and Destination port. You can enter multiple ports for the same service. The number of source and destination ports must not exceed 16.
- **IP:** Select Protocol Number for the service. You can select multiple ports for the same service.
- **ICMP:** Select ICMP Type and Code. You can enter multiple types and codes for the same service. Use Add icon and Remove icon to add and delete the parameters respectively.
- **ICMPv6:** Select ICMPv6 Type and Code. You can enter multiple types and codes for the same service. Use Add and Remove icons to add and delete the parameters.

![Figure 77: Firewalls Running on SFOS v17](image)

**Forward Type**

Select the type of external port from the available options.

**Available Options:** Port
- Port Range
- Port List
- Everything

When **Everything** is selected, all ports are forwarded. Select other options to enable custom port forwarding and specify port forwarding details.

**Service Port(s) Forwarded (Not Available if Forward Type selected is Everything)**

Specify the public port number for which you want to configure port forwarding.

**Protocol (Not Available if Forward Type selected is Everything)**

Select the protocol TCP or UDP to be used by forwarding packets.

![Figure 78: Firewalls Running on SFOS v16.x](image)
5. Specify **Forward To** details.

**Protected Server(s)**

Select from the available options on which the email server is to be hosted.

**Available options:**
- **IP Address** – External IP address is mapped to the specified IP address.
- **IP Range** – External IP address range is mapped to the specified IP address range.
- **IP List** – External IP address is mapped to the specified IP list.
- **FQDN** (available only for IPv4 virtual hosts) – External IP address is mapped to the specified FQDN.

Internal mapped server can be accessed by FQDN.

**Note**
For **IP Range** and **IP List**, you can also use a single external IP address. The device will then use load balancing for handling the requests.

**Mapped Port Type** (Available only if Change Destination Port(s) is selected)

Select the type of mapped port from the available options.

**Available Options:**
- Port
- Port Range
- Port List

**Note**
Not applicable for firewalls running on SFOS v17.

**Mapped Port** (available only if Change Destination Port(s) is selected)

Specify mapped port number on the destination network to which the public port number is mapped. Mapped port must have the same number of ports as specified in the public service, or at least have one port. **Mapped Port** is disabled if:

- No TCP/UDP service is selected.
- Multiple services are selected.
- Service group is selected.
- Selected service is with TCP/UDP combination.

**Protected Zone**

Select the zone to which the email server rule applies.

**Change Destination Port(s)**

Select the check box to specify different mapped port. Clear the check box to use the same **Service Port(s) Forwarded** as mapped port.

Figure 79: Forward To

6. Specify **Load Balancing** details.

**Load Balancing** (Applicable when 'IP Range' or 'IP List' is selected for Protected Server. Also, Source Zone for Hosted Server should be 'WAN')

Select the method for load balancing from the available options.
Available Options

**Round Robin** - In this method, requests are served in a sequential manner where the first request is forwarded to the first server, second request to the second server and so on. When a request is received, the device checks to see which the last server that was assigned a request was. It then assigns this new request to the next available server. This method is can be used when equal distribution of traffic is required and there is no need for session-persistence.

**First Alive** - In this method, all incoming requests are served by the first server (the first IP Address that is configured in the IP Range). This server is considered as the primary server and all others are considered as backup. Only when the first server fails, the requests are forwarded to the next server in line. This method is used for failover scenarios.

**Random** - In this method, the requests are forwarded to the servers randomly. Although, the device makes sure that all configured servers receive equally distributed load. Hence, this method is also called uniform random distribution. This method can be used when equal distribution of traffic is required and there is no need for session-persistence or order of distribution.

**Sticky IP** - In this method, Along with Round Robin distribution of traffic, the device forwards incoming traffic according to the Source IP Address. All traffic from a particular source is forwarded only to its mapped Server. This means that all requests for a given source IP are sent to the same application server instance. This method is useful in cases where all requests or sessions are required to be processed by the same server. For example: Banking websites, E-Commerce websites.

**Health Check (Applicable if Load Balancing is enabled)**

Click to enable health check for failover and specify the parameters based on the description shown below.

**Probe Method**

Select the probe method to check the health of the server from the available options.

**Available Options:**

TCP Probe ICMP Probe

**Port (Applicable if TCP Probe Health Check Method is selected)**

Specify the Port number on the server health is monitored.

Acceptable Range - 1 to 65535

**Interval**

Specify the time interval in seconds after which the health will be monitored.

Acceptable Range (Seconds) - 5 to 65535

Default - 60

**Timeout**

Specify the time interval in seconds within which the server must respond.

Acceptable Range (Seconds) - 1 to 10

Default - 2

**Retries**

Specify the number of tries to probe the health of the server, after which the server will be declared unreachable.
Acceptable Range - 1 to 10
Default – 3

Figure 80: Protected Application Server(s)

7. Specify Identity details.

Match known users

Match known users allows you to check whether the specified user/user group from the selected zone is allowed to access the selected service or not.

Click to attach the user identity.

Show Captive Portal to unknown users

Select the check box to accept traffic from unknown users. Captive portal page is displayed to the user where the user can login to access the Internet.

Clear the check box to drop traffic from unknown users.

User or Groups (available only if Match known users is enabled)

Select the user(s) or group(s) from the list of available options.

Exclude this user activity from data accounting (available only if Match known users is enabled)

Click to enable/disable user traffic activity from data accounting.

By default, user’s network traffic is considered in data accounting. Select to exclude certain traffic from user data accounting. The traffic allowed through this firewall rule will not be accounted towards data transfer for the user.

Figure 81: Identity

8. Specify Scanning details.

Scan SMTP

Click to enable/disable scanning of SMTP traffic.

Scan SMTPS

Click to enable/disable scanning of SMTPS traffic.

Figure 82: Scanning
9. Specify **Advanced** settings details.
   
a) Specify **Policies for Business Applications**.

**Intrusion Prevention**

Select the required IPS policy. If **Match rule based on user identity** is enabled, user’s IPS policy will be applied automatically, but will not be effective till the respective module is subscribed.

A new IPS policy can be created directly from this page or from the **Protect > Intrusion Prevention > IPS Policies** page.

**Traffic Shaping Policy (not available if Match known users is selected)**

Select the required IPS policy. If **Match rule based on user identity** is enabled, user’s QoS policy will be applied automatically.

A new traffic shaping policy can be created directly from this page or from the **System > Profiles > Traffic Shaping** page.

Figure 83: Policies for Business Applications

b) Specify **Security Heartbeat** settings *(available only if IPv4 is selected)*.

**Minimum Source HB Permitted**

Select a minimum health status that a source device must have to conform to this rule. Health status can be either **Green**, **Yellow** or **No Restriction**. If the health criterion is not met, access and privileges defined in this rule will not be granted to the user.

**Block clients with no heartbeat**

Heartbeat-capable devices can be required to send information on their health status in defined intervals - this is called a heartbeat.

Based on that information, you can restrict a source device’s access to certain services and networks.

Enable/disable the option to require the sending of heartbeats.

**Minimum Destination HB Permitted (not available if Protected Zone selected is WAN)**

Select a minimum health status that a destination device must have to conform to this rule. Health status can be either **Green**, **Yellow** or **No Restriction**. If the health criterion is not met, access and privileges defined in this rule will not be granted to the user.

**Block request to destination with no heartbeat (not available if Protected Zone selected is WAN)**
Heartbeat-capable devices can be required to send information on their health status in defined intervals - this is called a heartbeat.

Based on that information, you can block requests to destinations not sending heartbeat.

Enable/disable the option to require the sending of heartbeats.

![Security Heartbeat](image)

Figure 84: Security Heartbeat

c) Specify Routing details.

**Rewrite source address (Masquerading)**

Enable/disable to re-write the source address or specify a NAT policy.

**Use Outbound Address (available only if Rewrite source address is enabled)**

Select the NAT policy to be applied from the list of available NAT policies.

A new NAT policy can be created directly from this page or from the System > Profiles > Network Address Translation page.

The default NAT policy is Masquerade.

**MASQ (Interface Default IP):** IP Address of the selected Protected Zone as configured in Configure > Network > Interfaces will be displayed instead of (Interface Default IP).

**Create Reflexive Rule**

Select ON to automatically create a reflexive firewall rule for the protected host.

The reflexive rule has the same policies as those configured for the hosted server but instead of source zone to destination zone, this rule is applicable on traffic from destination zone to source zone.

By default, the reflexive rule is not created.

![Routing](image)

Figure 85: Routing

10. Specify the logging option for the user application traffic.

**Log Firewall Traffic**
Click to enable logging of permitted and denied traffic.

![Log Firewall Traffic]

Figure 86: Log Traffic

**Email Clients (POP and IMAP)**

1. Go to Device Configuration > Protect > Firewall and select between IPv4 or IPv6 using the default filter.
2. Now, click **Add Firewall Rule** and select **Business Application Rule**.
3. Specify the general rule details.

**Application Template**

Select Email Clients (POP & IMAP) to define a application filter policy for POP and IMAP based email clients.

**Description**

Specify the rule description.

**Rule Position**

Specify the position of the rule.

*Available Options:* Top, Bottom

*Note*

Rule Position can only be specified while creating a rule.

**Rule Name**

Specify a name to identify the rule.

*Note*

Rule Name can only be edited while creating a rule.

4. Specify **Source** details.

**Zone**

Select the allowed source zone(s).

**Networks**

Select the allowed source network(s). A new network host can be created directly from this page or from the Device Configuration > System > Host and Services > IP Hosts page.

5. Specify **Destination** details.

**Zone**

Select the zone to which the rule applies.

**Networks**

Select the network(s) to be protected.

A new network host can be created directly from this page from the Device Configuration > System > Host and Services > IP Hosts page.


**Match rule based on user identity**

Click to enable a rule based on the user identity.
Show Captive Portal to unknown users
Select the check box to accept traffic from unknown users. Captive portal page is displayed to the user where the user can login to access the Internet.
Clear the check box to drop traffic from unknown users.

User or Groups (only available if Match rule based on user identity is enabled)
Select the user(s) or group(s) from the list of available options.

Exclude this user activity from data accounting (only available if Match rule based on user identity is enabled)
Click to enable/disable user traffic activity from data accounting.
By default, user’s network traffic is considered in data accounting. Select to exclude certain traffic from user data accounting. The traffic allowed through this rule will not be accounted towards data transfer for the user.

7. Specify Malware Scanning details.
Scan IMAP/IMAPS/POP3/POP3S/SMTP/SMTPS
Click to enable/disable scanning of IMAP/IMAPS/POP3/POP3S/SMTP/SMTPS traffic.

8. Specify Advanced settings.
   a) Specify Policies for Business Applications.

Intrusion Prevention
Select an IPS policy for the rule. A new IPS policy can be created directly from this page itself or from the Device Configuration > Protect > Intrusion Prevention > IPS Policies page.

Traffic Shaping (Not available if Match rule based on user identity is selected)
Select a traffic shaping policy for the rule.
A traffic shaping policy allocates & limits the maximum bandwidth usage of the user.
A new traffic shaping policy can be created directly from this pager from the Device Configuration > Protect > Intrusion Prevention > IPS Policies page.

   b) Specify Security Heartbeat settings (only available if IPv4 is selected).

Minimum Source HB Permitted
Select a minimum health status that a source device must have to conform to this rule. Health status can be either Green, Yellow or No Restriction. If the health criterion is not met, access and privileges defined in this rule will not be granted to the user.

Block clients with no heartbeat
Heartbeat-capable devices can be required to send information on their health status in defined intervals - this is called a heartbeat.
Based on that information, you can restrict a source device's access to certain services and networks.
Enable/disable the option to require the sending of heartbeats.

Minimum Destination HB Permitted
Select a minimum health status that a destination device must have to conform to this rule. Health status can be either Green, Yellow or No Restriction. If the health criterion is not met, access and privileges defined in this policy will not be granted to the user.

Block request to destination with no heartbeat
Heartbeat-capable devices can be required to send information on their health status in defined intervals - this is called a heartbeat.
Based on that information, you can block requests to destinations not sending heartbeat.
Enable/disable the option to require the sending of heartbeats.

c) Specify Routing details.

**Rewrite source address (Masquerading)**
Enable/disable to re-write the source address or specify a NAT policy.

**Use Gateway Specific Default NAT Policy (only if Masquerading is selected)**
Select to override the default NAT policy with a gateway specific policy.

**Override default NAT policy for specific Gateway (only if Use Gateway Specific Default NAT Policy is selected)**
Select to specify gateway and corresponding NAT policy. Multiple gateways and NAT policies can be added.

**Use Outbound Address (only available if Rewrite source address is enabled and Use Gateway Specific Default NAT Policy is disabled)**
Select the NAT policy to be applied the list or available NAT policies.
A new NAT policy can be created directly from this pager from the Device Configuration > System > Profiles > Network Address Translation page.
The default NAT policy is Masquerade.

**Primary Gateway**
Select the primary gateway to route the request. You can create new gateway from this page itself or from Device Configuration > Configure > Routing > Gateways.

*Note*
On deletion of the gateway, Primary Gateway will display WAN Link Load Balance for WAN Destination Zone and None for other zones. In such case, firewall rule will not make routing decisions.

**Backup Gateway**
Select the backup gateway to route the request. You can create new gateway from this page itself or from Device Configuration > Configure > Routing > Gateways.

*Note*
On deletion of the gateway, Backup Gateway will display None.

9. Specify logging option for the user application traffic.

**Log Firewall Traffic**
Click to enable logging of permitted and denied traffic.

**DSCP value**

DiffServ Code Point (DSCP) uses the 6 bits, thereby giving $2^6 = 64$ different values (0 to 63). describes the standard DSCP values. Remaining DSCP values can be customized as per the QoS requirement.

<table>
<thead>
<tr>
<th>Decimal</th>
<th>DSCP</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Default</td>
<td>Best Effort</td>
</tr>
</tbody>
</table>
### Decimal DSCP Description

<table>
<thead>
<tr>
<th>8</th>
<th>CS1</th>
<th>Class 1 (CS1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>AF11</td>
<td>Class 1, Gold (AF11)</td>
</tr>
<tr>
<td>12</td>
<td>AF12</td>
<td>Class 1, Silver (AF12)</td>
</tr>
<tr>
<td>14</td>
<td>AF13</td>
<td>Class 1, Bronze (AF13)</td>
</tr>
<tr>
<td>16</td>
<td>CS2</td>
<td>Class 2 (CS2)</td>
</tr>
<tr>
<td>18</td>
<td>AF21</td>
<td>Class 2, Gold (AF21)</td>
</tr>
<tr>
<td>20</td>
<td>AF22</td>
<td>Class 2, Silver (AF22)</td>
</tr>
<tr>
<td>22</td>
<td>AF23</td>
<td>Class 2, Bronze (AF23)</td>
</tr>
<tr>
<td>24</td>
<td>CS3</td>
<td>Class 3 (CS3)</td>
</tr>
<tr>
<td>26</td>
<td>AF31</td>
<td>Class 3, Gold (AF31)</td>
</tr>
<tr>
<td>28</td>
<td>AF32</td>
<td>Class 3, Silver (AF32)</td>
</tr>
<tr>
<td>30</td>
<td>AF33</td>
<td>Class 3, Bronze (AF33)</td>
</tr>
<tr>
<td>32</td>
<td>CS4</td>
<td>Class 4 (CS4)</td>
</tr>
<tr>
<td>34</td>
<td>AF41</td>
<td>Class 4, Gold (AF41)</td>
</tr>
<tr>
<td>36</td>
<td>AF42</td>
<td>Class 4, Silver (AF42)</td>
</tr>
<tr>
<td>38</td>
<td>AF43</td>
<td>Class 4, Bronze (AF43)</td>
</tr>
<tr>
<td>40</td>
<td>CS5</td>
<td>Class 5 (CS5)</td>
</tr>
<tr>
<td>46</td>
<td>EF</td>
<td>Expedited Forwarding (EF)</td>
</tr>
<tr>
<td>48</td>
<td>CS6</td>
<td>Control (CS6)</td>
</tr>
<tr>
<td>56</td>
<td>CS7</td>
<td>Control (CS7)</td>
</tr>
</tbody>
</table>

#### 3.4.2 Intrusion prevention

With intrusion prevention, you can examine network traffic for anomalies to prevent DoS and other spoofing attacks. Using policies, you can define rules that specify an action to take when traffic matches signature criteria. You can specify protection on a zone-specific basis and limit traffic to trusted MAC addresses or IP–MAC pairs. You can also create rules to bypass DoS inspection.

**IPS policies**

With IPS policies, you can prevent network attacks using rules. The firewall enforces the actions specified in the rules and logs the corresponding events. The set of default policies prevents network attacks for several common types of traffic. You can create custom policies with rules that meet your traffic requirements.

- To add a policy, click Add and type a name. Then, you can clone the rules from an existing policy.
- To add rules to a policy, click for the policy you want to edit, and then click Add.
IPS policy rules

Rules specify signatures and an action. The firewall matches signatures with traffic patterns and takes the action specified in the rule. The action specified for the rule overrides the action recommended by the signature.

IPS signatures

Signatures identify threats and specify a recommended action to take when the firewall encounters matching traffic. Signatures are specific to applications, services, or platforms. The firewall includes predefined signatures and you also can create custom signatures.

<table>
<thead>
<tr>
<th>SID</th>
<th>ID of the IPS signature.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Category of IPS signature.</td>
</tr>
<tr>
<td>Severity</td>
<td>Degree of threat severity.</td>
</tr>
<tr>
<td>Platform</td>
<td>Signatures that apply to specific platforms (for example, Microsoft Windows).</td>
</tr>
<tr>
<td>Target</td>
<td>Client or server-based signatures.</td>
</tr>
<tr>
<td>Recommended action</td>
<td>Action recommended by the firewall when traffic matches the signature.</td>
</tr>
</tbody>
</table>

Add an IPS policy

1. Go to Intrusion prevention > IPS policies and click Add.
2. Type a name.
3. Optional: Select the policy from which you want to clone the rules.
4. Click Save.

Add rules to the policy

Rules specify signatures and an action. You can select default or custom signatures. The firewall matches signatures with traffic patterns and takes the action specified in the rule. The firewall evaluates rules from top to bottom.

1. Go to Intrusion prevention > IPS policies and click

   for the policy you want to edit.
2. Click Add.
3. Type a name.
4. Select the signatures.
   • Click Select all.
   • Click Select individual signature and select the signatures.

   You can filter signatures based on category, severity, platform, and target. To sort based on search terms, click Select all, type a term in the smart filter, and press Enter.
5. Optional: Click Custom signature and select the signatures.
6. Select the action to take when the firewall finds matching traffic for the signatures in the rule. For packet-based actions, the firewall checks each packet. For session-based actions, it checks until it finds the first matching packet.

**Note**

The action specified for the rule overrides the action recommended by the signature.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended</td>
<td>Default action specified for each signature.</td>
</tr>
<tr>
<td>Allow packet</td>
<td>Allow packet.</td>
</tr>
<tr>
<td>Drop packet</td>
<td>Drop packet.</td>
</tr>
<tr>
<td>Disable</td>
<td>Disable signature. Use this setting to prevent false positives.</td>
</tr>
<tr>
<td>Drop session</td>
<td>Terminate session. Use this setting to prevent an attack.</td>
</tr>
<tr>
<td>Reset</td>
<td>Reset session and send TCP reset packet to the originator.</td>
</tr>
<tr>
<td>Bypass session</td>
<td>Allow traffic and do not scan traffic for the rest of the session. Use this setting to allow certain types of traffic.</td>
</tr>
</tbody>
</table>
7. Click **Save**.
   For the policy to take effect, add it to a firewall rule.

**Custom IPS signatures**

With custom signatures, you can protect your network from vulnerabilities related to network objects such as servers, protocols, and applications. You can create custom signatures and later add them to IPS policy rules.

**Add a custom IPS signature**

1. Go to **Intrusion prevention > Custom IPS signatures** and click **Add**.
2. Type a name.
3. Select a protocol.
4. Specify a custom rule.
   
   | keyword: "credit score" |
   | content: "www.facebook.com" |
   | srcport: 443 |
5. Select the severity.
6. Select the recommended action to take when the firewall finds matching traffic.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow packet</td>
<td>Allow packet.</td>
</tr>
<tr>
<td>Drop packet</td>
<td>Drop packet.</td>
</tr>
<tr>
<td>Drop session</td>
<td>Terminate session. Use this setting to prevent an attack.</td>
</tr>
<tr>
<td>Reset</td>
<td>Reset session and send TCP reset packet to the originator.</td>
</tr>
<tr>
<td>Bypass session</td>
<td>Allow traffic and do not scan traffic for the rest of the session. Use this setting to allow certain types of traffic.</td>
</tr>
</tbody>
</table>

7. Click **Save**.

Add the signature to a policy rule.

**DoS**

**Device Configuration > Protect > Intrusion Prevention > DoS**

The device provides several security options that cannot be defined by the Security Policies. This includes protection from several kinds of “Denial of Service attacks”. These attacks disable computers and circumvent security.

Denial of Service (DoS) attack is a method that hackers use to prevent or deny legitimate users access to a service.

DoS attacks are typically executed by sending many request packets to a targeted server (usually Web, FTP, or Mail server), which floods the server's resources, making the system unusable. Their
Sophos Firewall Manager

goal is not to steal the information but disable or deprive a device or network so that users no longer have access to the network services/resources.

All servers can handle traffic volume up to a maximum, beyond which they become disabled. Hence, attackers send a very high volume of redundant traffic to a system so it cannot examine and allow permitted network traffic. Best way to protect against the DoS attack is to identify and block such redundant traffic. Below are some DoS settings which can be used for identifying DoS attack:

**Packet rate per Source**
Total number of connections or packets allowed to a particular user.

**Burst rate per Source**
Maximum number of packets allowed to a particular user at a given time.

**Packet rate per Destination**
Total number of connections or packets allowed from a particular user.

**Burst rate per Destination**
Maximum of packets allowed from a particular user at a given time.

**How it works**

When the burst rate is crossed, device considers it as an attack. Device provides DoS attack protection by dropping all the excess packets from the particular source/destination. Device will continue to drop the packets till the attack subsides. Because device applies threshold value per IP Address, traffic from the particular source/destination will only be dropped while the rest of the network traffic will not be dropped at all.

Time taken to re-allow traffic from the blocked source/destination = time taken to subside the attack + 30 seconds

**For example:**

Packet rate per Source – 100 packets per second
Burst rate per Source – 200 packets per second

When user starts sending requests, initially user will be able to send 200 packets per second but once the 200 packets are received, in the next phase user will be able to send only 100 packets per second. So in the next phase, if user sends 150 packets per second, device will consider it as an attack and drop 50 (150 -100) packets. Device will accept traffic from the user only after 30 seconds of dropping the packets.

**Threshold values**

Device uses packet rate and burst rate values as a threshold value to detect DoS attack. These values depend on various factors like:

- Network bandwidth
- Nature of traffic
- Capacity of servers in the network

These values are applicable to the individual source or destination requests per user/IP Address and not globally to the entire network traffic. For example, if source rate is 2500 packets/minute and the network consists of 100 users then each user is allowed packet rate of 2500 packets per minute

Configuring high values will degrade the performance and too low values will block the regular requests. Hence it is very important to configure appropriate values for both source and destination IP Address.
DoS Settings

Attack definition can be defined both for source and destination

**SYN Flood**

SYN Flood is the attack in which large numbers of connections are sent so that the backlog queue overflows. The connection is created when the victim host receives a connection request and allocates for it some memory resources. A SYN flood attack creates so many half-open connections that the system becomes overwhelmed and cannot handle incoming requests any more.

Configure Packet Rate (packets/minute) and Burst Rate (packets/second) for source and destination.

Select **Apply Flag** checkbox to apply the SYN flood definition and control the allowed number of packets.

Source Traffic Dropped displays number of source packets dropped in case source packet rate control is applied.

Destination Traffic Dropped displays number of packets dropped in case destination packet rate control is applied.

Click **SYN Flood** to view the real-time updates on flooding. It displays the source IP Address - which was used for flooding and IP Address which was targeted.

**UDP Flood**

User Datagram Protocol (UDP) Flood links two systems. It hooks up one system’s UDP character-generating service, with another system’s UDP echo service. Once the link is made, the two systems are tied up exchanging a flood of meaningless data.

Configure Packet Rate (packets/minute) and Burst Rate (packets/second) for source and destination.

Select **Apply Flag** checkbox to apply the UDP flood definition and control the allowed number of packets.

Source Traffic Dropped displays number of source packets dropped in case source packet rate control is applied.

Destination Traffic Dropped displays number of packets dropped in case destination packet rate control is applied.

Click **UDP Flood** to view the real-time updates on flooding. It displays the source IP Address - which was used for flooding and IP Address which was targeted.

**TCP Flood**

TCP attack sends huge amount of TCP packet so that the host/victim computer cannot handle, thereby denying service to legitimate TCP users.

Configure Packet Rate (packets/minute) and Burst Rate (packets/second) for source and destination.

Select **Apply Flag** checkbox to apply the TCP flood definition and control the allowed number of packets.

Source Traffic Dropped displays number of source packets dropped in case source packet rate control is applied.

Destination Traffic Dropped displays number of packets dropped in case destination packet rate control is applied.
ICMP/ICMPv6 Flood

ICMP/ICMPv6 attack sends huge amount of packet/traffic so that the protocol implementation of the host/victim computer cannot handle, thereby preventing legitimate packets from getting through to their destination.

Configure Packet Rate (packets/minute) and Burst Rate (packets/second) for source and destination.

Select **Apply Flag** checkbox to apply the ICMP flood definition and control the allowed number of packets.

Click **ICMP/ICMPv6 Flood** to view the real time updates on flooding. It displays the source IP Address - which was used for flooding and IP Address which was targeted.

Dropped Source Routed Packets

Select **Apply Flag** checkbox to enable. This will block any source routed connections or any packets with internal address from entering your network.

Disable ICMP/ICMPv6 Redirect Packet

An ICMP redirect packet is used by routers to inform the hosts what the correct route should be. If an attacker is able to forge ICMP redirect packets, he or she can alter the routing tables on the host and possibly weaken the security of the host by causing traffic to flow via another path.

Disable the option to prevent the attacker from forging ICMP redirect packet.

Default - Enabled

ARP Hardening

If enabled, device will send an ARP reply only if the destination IP address is a local address configured on the incoming interface and both the sender and destination IP address are in the same subnet.

DoS Bypass Rule

The device allows to bypass the DoS rule in case you are sure that the specified source will not be used for flooding or ignore if flooding occurs from the specified source. By default, VPN zone traffic is also subjected to DoS inspection. You can also bypass DoS inspection of the traffic coming from certain hosts of VPN zone.

The DoS Bypass Rule page displays list of all the bypass rule. You can filter the list based on IP Family. The page provides option to add a new rule, update the existing rule, or delete a rule.

Create a DoS bypass rule

1. Go to **Intrusion prevention > DoS & spoof protection**.
2. Scroll to **DoS bypass rule** and click **Add**.
3. Select the IP version.
4. Specify the source and destination IP addresses.
5. Select a protocol.
6. Specify the source and destination ports.
   - Wildcards are supported. To specify any IP address or port, type *.
7. Click **Save**.
3.4.3 Web

Web protection keeps your company safe from attacks that result from web browsing and helps you increase productivity. You can define browsing restrictions with categories, URL groups, and file types. By adding these restrictions to policies, you can block websites or display a warning message to users. For example, you can block access to social networking sites and executable files. General settings let you specify scanning engines and other types of protection. Exceptions let you override protection as required for your business needs.

Policies

With policies, you can control traffic using rules and advanced settings. The default set of policies describes some common restrictions.

To create a web policy, click Add Policy.

To expand/collapse any web policy, click icon on the web policy.

Note

• To use an existing policy as a template for a new policy, click the menu button and select Clone.

• The default web policy Default Policy will be expanded by default.

To manage policies, click and select Add Rule, Clone, Edit, Delete, Synchronize and Show Usage References.

Rules

Rules specify the following criteria:

• Users to whom the rule applies. These include groups and individual users.

• Activities that describe the type of usage to restrict. These include user activities, Web categories, URL groups, file types, and dynamic categories.

• Action (Allow, Warn or Block), HTTP Action and HTTPS Action to take when the firewall encounters traffic that matches the rule criteria.

• Time Constraint to schedule the time period during which rule should be applied on the network.

The firewall evaluates rules from highest to lowest. For example, a rule that allows all traffic that precedes a rule that restricts a specific type of traffic takes precedence and the subsequent rule is ignored.

Click on toggle switch next to Constraints section list to enable/disable the rule.

To manage rules, click the menu button

( )
for any rule and select **Add Rule Above**, **Add Rule Below**, **Clone Rule Above**, **Clone Rule Below** or **Delete**.

**Add Policy**

1. Go to **Device Configuration > Firewall > Web > Policies** and click **Add Policy**.
2. Type a name.
3. Click **Add Rule**.

**Tip**

To use an existing rule as a template for a new rule, click the menu button and select **Clone**.

The firewall creates a default rule that blocks all web traffic for all users. The default rule is disabled.

Figure 87: Add Rule

4. Specify users.
   These include groups and individual users.
   a) In the new rule, move the pointer over the user field and click **Add New Item**.
   b) Select users.

   **Tip**
   You can filter the type of users to display by clicking **Show Only** and selecting a user type.

   c) Click **Apply selected items**.

   Figure 88: Select Users

5. Specify activities.
   These include user activities, categories, URL groups, file types, and dynamic categories.
   a) Move the pointer over the activity field and click **Add New Item**.
   b) Select activities.

   **Tip**
   You can filter the type of activities to display by clicking **Show Only** and selecting an activity type.

   c) Click **Apply selected items**.

6. In the Action list, specify an action to take when the firewall encounters HTTP traffic that matches the selected criteria.

   Choose from the following options (where permitted by the action type):

   **Options**
   - **Allow**
   - **Warn**
   - **Block**

7. (Optional) Specify an action to take when the firewall encounters HTTPS traffic that matches the selected criteria.

   **Note**
   Follow these steps only if you want to specify an action for HTTPS traffic that is different from the one you specified for HTTP.
a) Move the pointer to the right of the **Action** drop-down list box. The firewall displays the **HTTPS Use Action** action drop-down list box.

![Figure 89: HTTPS Use Action](image)

b) Select an option.

**HTTPS Use Action**

Use Action: Select this option to use the same action that is currently in effect for HTTP traffic. If you specify a different HTTP action at a later time, HTTPS action will also use that action. Allow: Always allow HTTPS traffic that matches the selected criteria. Warn: Always display a warning message when encountering HTTPS traffic that matches the selected criteria. Block: Always block HTTPS traffic that matches the selected criteria.

8. Move the pointer over the **Constraints** field and select a schedule.

**Tip**

You can create a new schedule by clicking **Create new** and specifying criteria.

9. Click the on/off switch to enable the rule.

![Figure 90: Enable Rule](image)

10. Click and drag the rule handle to position the rule in the hierarchy.

![Figure 91: Position Rule](image)

The firewall evaluates rules from highest to lowest. For example, a rule that allows all traffic that precedes a rule that restricts a specific type of traffic takes precedence and the subsequent rule is ignored.

![Figure 92: Add Policy](image)

11. Click **Advanced Settings** and specify settings for the policy.

**Enable logging and reporting**

Include this policy in logs and reports.

**Prevent downloading of large files**

Prevent downloading files greater than the size specified.

**Restrict login domains for Google Apps**

Restrict logging in to Google Apps only on the domains specified.

**Enable YouTube for Schools**

Restrict YouTube content to videos on [YouTube for Schools](https://youtube.com) (a limited EDU-only site) and to those uploaded using the ID specified.
You must have a YouTube school ID to use this setting.

User Activities

User Activities combine web categories, file types, and URL groups in one container. For example, you can create a User Activity to associate spyware and malware with a list of URLs. You can include User Activities in web policies to control access to websites or files that match any of the specified criteria.

To create a User Activity, click Add.

To delete User Activity(ies), select and click Delete.

To synchronize User Activity(ies), select and click Synchronize.

To filter the list, click the Filter button and specify criteria.

To manage individual User Activities, click and select Edit, or Delete, Synchronize or Show Usage References.

To use an existing template of User Activity for a new one click and select Clone.
Use **Show Usage References** to view Entity Usage Reference for selected User Activity.

Add a user activity

1. Go to **Web > User activities** and click **Add**.
2. Type a name.
3. Click **Add new item** and select categories.

**Note**
The firewall evaluates categories (web categories, file types, and URL groups) using “OR”. Only one category must match for the user activity to apply.
Tip
You can filter the type of categories to display by clicking **Show: All** and selecting a type.

4. Click **Save**.

Categories

With web categories, you can organize and classify domains and keywords in a container. You can use categories within policies to control access to websites.

- To edit a category, click

Within a category, you can create a list of domains and keywords that are specific to your organization or import a database. These include country-specific blacklists and open-source categorization lists. The firewall checks for updates every two hours.

**Classification**

Categorization that lets you filter and manage categories.

**Traffic shaping policy**

Policy that determines usage limits and the bandwidth allocated for upload and download traffic.

Add a category

1. Go to **Web > Categories** and click **Add**.
2. Type a name.
3. Select a classification.
4. Select a traffic shaping policy.
5. Select a configuration type.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>Domains and keywords that are specific to your organization. Acceptable formats are .tar, .gz, .bz, .bz2, and .txt. (Archive files must contain text files.)</td>
</tr>
<tr>
<td>External URL database</td>
<td>Domains and keywords that are created by third-parties, for example, country-specific blacklists.</td>
</tr>
</tbody>
</table>

For text files, observe the following requirements:

- One entry per line.
- Entries can be domains, site paths, or query strings, for example, www.example.com, example.com/path, example.com/path?data=example.
- Entries do not specify a protocol.

6. Specify domains and keywords.

- For local configurations, click **Choose file** and select a file. Optionally, you can type a domain or keyword in the **Search/Add** text box and click **.
• For external URL databases, type a URL in the **Search/Add** text box and click **Add**.

7. Specify advanced settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Override default notification page</td>
<td>Display the message specified to the user when a website is blocked as a result of the category instead of the default message.</td>
</tr>
</tbody>
</table>

8. Click **Save**.

**Edit Web Category**

Modify an existing Web Category.

From the **Device Configuration > Protect > Web > Categories** page, either click the **Name** of an existing category or click the related **Manage** icon on the right. The **Edit Web Category** page is displayed.

1. Select the correct **Classification** for the Web Category.
2. Optionally, from the **Traffic Shaping Policy** drop-down, select an existing policy, or **Create New**.
3. Under **Advanced Settings** you can select **Override Default Denied Message** to modify the block page shown when your Web Category is denied by a policy. This allows you to have present a specific message if a user is blocked.
4. Click **Save**.

**Related tasks**

**Add a category** (page 95)

**URL groups**

URL groups contain one or more domains that you can use in web policies to control access to websites.

• To edit a URL group, click **Add**.

**Add a URL group**

1. Go to **Web > URL groups** and click **Add**.
2. Type a name.
3. Type a domain in the **Search/Add** text box and click **Add**.

Regular expressions are allowed. For example, ^([A-Za-z0-9,-]*)\?example\.com/ matches all subdomains of example.com. Specify pattern matches using ASCII characters. For information about converting non-ASCII characters, refer to RFC 3490.

**Note**

The firewall evaluates domains using “OR”. Only one domain must match for the URL group to apply.

4. Click **Save**.

**Edit URL Group**

On the **Edit URL Group** page you can modify an existing URL Group.
1. Set the **Classification** for the URL Group.
2. Choose an existing **Traffic Shaping Policy**, or select **Create New**.
3. Under **Advanced Settings** you can select **Override Default Denied Message** to modify the block page shown when your URL Group is denied by a policy. This allows you to have present a specific message if a user is blocked.

**Related tasks**

Create a traffic shaping policy (page 287)

**File types**

A file type is a classification that is determined by file extension or MIME type. You can include file types in web policies to control access to files. The default types contain some common criteria and you can create additional types.

- To edit a file type, click

**Add a file type**

1. Go to **Web > File types** and click **Add**.
2. Type a name.
3. Optional: Select a template.
   - Templates organize commonly used file extensions and MIME headers by category, for example, video files. You can use templates instead of typing extensions and MIME headers.
4. Specify file extensions and MIME headers.
   - **Note**
     - Do not type a dot (.) before file extensions.
5. Click **Save**.

**Exceptions**

With exceptions, you can override protection settings for web traffic that matches the specified criteria. For example, you can create an exception to skip HTTPS decryption for sites that contain confidential data. The default set of exceptions specifies some common override behaviors.

Override behaviors now include **Sandstorm**.

**Note**

Existing exceptions that skip malware scanning now also skip **Sandstorm** analysis.

To filter the list, click the Filter button and specify criteria.

To enable an Exception, click the toggle key. To create an Exception, click **Add Exception**.
**Tip**
To use an existing exception as a template for a new exception, click the menu button and select **Clone**.

To manage Exceptions, click and select **Clone, Edit, Delete** or **Synchronize**.

**Add an exception**
1. Go to **Web > Exceptions** and click **Add exception**.
2. Type a name.
3. Specify web traffic criteria.
   - Select the **URL pattern matches** check box, type a pattern in the **Search/Add** text box and click .
     Regular expressions are allowed. For example, ^([A-Za-z0-9.-]*\.)?example\.com/ matches all subdomains of example.com. Specify pattern matches using ASCII characters. For information about converting non-ASCII characters, refer to RFC 3490.
   - Select the **Web site categories** check box, click **Add new item**, and select categories.
   - Select the **Source IP addresses** check box, type an end-user address and click .
   - Select the **Destination IP addresses** check box, type a website address and click .

**Note**
The firewall evaluates all types of criteria using “AND”. For example, if you specify URL patterns and website categories, both types must match for the exception to apply. However, within each category, the firewall evaluates criteria using “OR”.

4. Specify checks or actions to skip when the firewall encounters traffic that matches the criteria.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS decryption</td>
<td>Do not decrypt HTTPS for traffic that meets the specified criteria.</td>
</tr>
</tbody>
</table>
|                       | **Note**
<p>|                       | If you disable HTTPS decryption, the firewall will not perform any other check that relies on decrypted traffic, such as malware scanning. However, the firewall will continue to scan HTTP traffic that matches the exception. |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware and content scanning</td>
<td>Do not scan traffic that meets the specified criteria for malware or content as specified in a content filter.</td>
</tr>
<tr>
<td>Sandstorm</td>
<td>Do not send files that are downloaded using the specified criteria to Sandstorm.</td>
</tr>
<tr>
<td>Policy checks</td>
<td>Do not check policies for traffic that meets the specified criteria.</td>
</tr>
</tbody>
</table>

5. Click **Save**.

Click the On/Off switch to turn the exception on.

**Protection**

The firewall provides several methods for protecting against threats and inappropriate web usage. Use these settings to configure how the firewall scans content for malware and to enable other protection mechanisms.

**Malware Scanning**

Configure general restrictions for scanning and restricting traffic by type and protocol.

**Scan Engine Selection**

Specify the type of scanning to apply.

**Available Options:**

- Single Engine: Scan traffic using the primary anti-virus engine (by default, the Sophos engine). This selection offers optimal performance.
- Dual Engine: Scan traffic using both engines, first by the primary and then by the secondary. Using this setting increases security, but may affect performance.

**Malware Scan Mode**

Specify batch or real-time scanning for HTTP/HTTPS traffic.

In batch mode, virus scanning will start only after the complete file has been downloaded. While this mode offers maximum protection, it may result in slower performance. Switch to real-time scanning to improve performance.

**Content that could not be scanned**

Specify an action to take when the firewall encounters content that could not be scanned.

**Note**

Files that cannot be fully scanned because they are encrypted or corrupted may contain undetected threats. Blocking offers the best protection.

**Do not scan files larger than**

Specify the maximum size of files to be scanned for HTTP(S), in MB. Files that exceed this setting will not be scanned.

Acceptable range: 1 to 256 MB

Default: 1 MB
Advanced Settings

Maximum file scan size for FTP
Specify the maximum size of files to be scanned for FTP, in MB. Files that exceed this setting will not be scanned.

- Acceptable range: 1 to 204 MB
- Default: 1 MB

Scan audio and video files
Scan audio and video content for malware and threats. Scanning may cause issues with streaming audio and video.

Enable pharming protection
Pharming attacks redirect users from legitimate websites to fraudulent websites that have been created to look like the legitimate site.

- Protect users against pharming and other domain name poisoning attacks by repeating DNS lookups before connecting.

Search Engine Enforcement

Enforce SafeSearch
Block websites that contain sexually explicit content from Google, Yahoo, and Bing search results.

Note
This setting is applicable only when the ‘No Explicit Content’ web policy is set to ‘Block’.

Enforce additional image filters
Restrict image search results to images with a Creative Commons license.

HTTPS Decryption and Scanning

HTTPS Scanning Certificate Authority (CA)
Specify the certificate authority for securing scanned HTTPS connections.

Block unrecognized SSL protocols
Prevent traffic that avoids HTTPS scanning by using invalid SSL protocols.

Block invalid certificates
Connect only to sites with a valid certificate.

Apply
Click to Apply changes.
Advanced

Configure advanced web protection such as caching behavior and proxy settings.

Web Content Caching

Enable web content cache
Keep a copy of frequently visited sites to reduce bandwidth consumption and improve performance.

Always cache Sophos Endpoint updates
Keep a copy of Sophos Endpoint updates to improve performance on your network.

Note
If this option is disabled you may experience network congestion when many endpoints attempt to download updates from the Internet at the same time.

Web Proxy Configuration

The firewall intercepts traffic transparently and enforces web protection (for example, policies and malware scanning) when the web proxy service is enabled for a network zone. By default, the service is enabled for LAN and WiFi zones. In transparent mode, the firewall allows HTTP traffic on port 80 and HTTPS traffic on port 443 only.

However, you can also configure the firewall to act as a proxy for configured web browsers by specifying a web proxy listening port. Users who are behind the proxy must specify the LAN or WiFi address and port in the web proxy configuration settings of their browsers. (Refer to the browser documentation for details.)

Specify the web proxy listening port and allowed destination ports when you want the firewall to act as a web proxy for configured web browsers.

Note
IPS policy is applicable on the traffic between proxy and WAN, but not between user and proxy.

Note
Traffic shaping policy is not applicable on the direct proxy traffic.

Web Proxy Listening Port
Specify the port on which the web proxy will listen for HTTP connection requests.

Allowed Destination Ports
The firewall may receive requests to connect to remote servers using a non-standard port. Specify the ports on which the proxy will allow connection. (This setting applies only when the web proxy listening port is set.)

CAUTION
Allowing connection on non-standard ports may pose a security risk.
Sophos Firewall Manager

Type a number and click the Add button

( + )
to add a trusted port. Click the Cancel button

( - )
to delete a trusted port, or the Edit button

( )
to modify a trusted port.

Apply

Click to Apply changes.

Surfing quotas

Surfing quotas allow you to control internet access for users using access settings. Quotas specify access on a cyclical (repeat) or non-cyclical (one-time) basis and the access time allowed. The default quotas specify some commonly used quotas such as unlimited access and block-type access.

Note
When more than one quota applies to a user, the firewall restricts access according to the first policy that reaches its limit.

- To edit a surfing quota, click

The following quota specifies unlimited access for one week on a one-time basis.

Add a surfing quota

1. Go to Web > Surfing quotas and click Add.
2. Type a name.
3. Specify a cycle type.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyclic</td>
<td>Repeat access. Specify the cycle hours. Once the specified time ends, the user receives access again. Users receive the time specified at the start of each cycle. Unused time does not carry over.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Non-cyclic</td>
<td>One-time access. Once the specified time ends, the user will be disconnected.</td>
</tr>
</tbody>
</table>

4. Specify a validity period.
   - Enter the number of days.
   - Select the **Unlimited** check box if you do not want to restrict validity.

5. Specify the maximum hours of access time to be granted by the quota.
   - Enter the hours and minutes. Users will be disconnected after this value has been exceeded even if the validity period of the quota has not yet expired.
   - Select the **Unlimited** check box if you do not want to specify maximum hours.

6. Click **Save**.

**User Notifications**

The firewall displays notifications to users when a web policy is set to block access or warn before connecting. Use these settings to create and preview notifications for multiple firewall devices.

To specify an image to display on notification pages, enable the **Use custom images** check box and choose images.

To create a block notification, enable the **Use custom block message** check box and type a message.

To create a warning notification, enable the **Use custom warn message** check box and type a message.

You can preview current messages by clicking the preview links.

**3.4.4 Applications**

Application protection helps keeps your company safe from attacks and malware that result from application traffic exploits. You can also apply bandwidth restrictions and restrict traffic from applications that lower productivity. Application filters allow you to control traffic by category or on an individual basis. With synchronized application control, you can restrict traffic on endpoints that are managed with Sophos Central. Managing cloud application traffic is also supported.

**Application list**

The application list contains many commonly used applications. You can sort applications according to their category, risk, technology, characteristics, and classification.

When the application signature database is updated, new applications are automatically added to application filters and firewall rules. For example, if a new signature is added for a high-risk application and there is already an application filter that blocks all high-risk applications, the new application will be blocked.
Synchronized Application Control

With Synchronized Application Control, you can manage applications which are discovered on Sophos managed devices.

Application handling

Known applications appear under the correct application category. Unknown applications appear under the category **Uncategorized** or **General Internet**. You can rename and categorize those applications. Apps can be assigned to application filters to control them.

Synchronized Application Control supports up to 10,000 apps.

Device Group

You can filter the devices according to a particular **Device Group**.

**All**: Displays all the Device Groups available.

Devices

You can filter according to a particular Device, based on the **Device Group** selected.

**All**: Displays all the devices available.

**Note**

The Device list is populated when a Device Group is selected.

Cloud applications

By analyzing cloud application traffic, you can mitigate the risks posed by cloud application usage. Options allow you to classify traffic and apply a traffic shaping policy.

Use the filters to refine the search results by date, classification, category, and bytes transferred. For example, you can filter traffic to display only unsanctioned social networking traffic for a specified period.

**Note**

The results include only allowed traffic and only applications that have traffic. Check your blocked application settings.
Note
Upload and download count and file type information can be displayed only for traffic where HTTPS decryption is enabled. Some apps use non-standard methods for sending or receiving file downloads, which can lead to these data points being empty or appearing inaccurate.

- To view traffic details, click

By default, all application traffic is classified as new.
- To apply a different classification, click Classify, select a classification, and click Apply.

Note
The new classification will be applied only to new traffic for the application.

To control bandwidth usage by cloud applications, you can apply a traffic shaping policy. For example, you may want to restrict streaming video traffic.
- To control bandwidth usage, click Traffic shaping, select a policy, and click Save.

Recommended settings
To maximize the effectiveness of cloud traffic reporting, use the following firewall rule settings:
- For basic reporting of bytes consumed (bytes in and out), enable Log firewall traffic.
- For more accuracy and detail, enable Decrypt & scan HTTPS, and set a web policy other than “None”.

Application Filter
The Application Filter page displays list of all the predefined and custom policies.
An Application Filter Policy controls user’s application access. It specifies which user has access to which applications and allows defining powerful security policies based on a number of parameters like:
- Individual users
- Groups of users
- Time of day

The device is shipped with the following predefined application filter policies:
- **Allow All**: By default, allows access to all the categories except the specified categories. Access to the specified categories depends on the strategy defined for each category.
- **Deny All**: By default, denies access to all the categories except the specified categories. Access to the specified categories depends on the strategy defined for each category.
- **Block generally unwanted apps**: Drops generally unwanted application traffic. This includes applications such as file transfer, proxy & tunnel, risk prone, peer to peer networking (P2P) and applications that cause loss of productivity.
- **Block filter avoidance apps**: Drops traffic from applications that tunnel other applications, proxy and tunnel applications, and from applications that can bypass firewall policy. These applications
Sophos Firewall Manager

allow users to anonymously browse the Internet by connecting to servers on the Internet via encrypted SSL tunnels. This, in turn, enables users to bypass network security measures.

- **Block peer to peer (P2P) networking apps**: Drops traffic from applications that are categorized as P2P applications. P2P could be a mechanism for distributing Bots, Spywares, Adware, Trojans, Rootkits, Worms and other types of malwares. It is generally advised to have P2P applications blocked in your network.

- **Block very high risk (Risk Level 5) apps**: Drops traffic from applications that are classified under 'very high risk' applications (Risk Level - 5).

- **Block high risk (Risk Level 4 and 5) apps**: Drops traffic from applications that are classified under 'high risk' applications (Risk Level - 4 and 5).

These predefined policies are immediately available for use until configured otherwise. You can also define custom policies to define different levels of access for different users to meet your organization’s requirements.

The page also provides option to add a new policy, update parameters of the existing policy, delete a policy, add a filtering rule to a policy or delete a filtering rule attached to a policy.

**Add an application filter policy**

1. Go to Applications > Application filter and click Add.
2. Type a name.
3. Optional: Select a template.
   - You can use any application filter policy as a template.
4. Click Save.

Add rules to the policy. For the policy to take effect, add it to a firewall rule.

**Add an application filter policy rule**

1. Go to Applications > Application filter and click for the policy you want to edit.
2. Click Add.
3. Select applications.
   - Click Select All and apply filters to refine the list using any combination of categories, risk, characteristics, technology, or classification. You can also type a term in the smart filter. The smart filter searches the name and description of an application.
   - Click Select Individual Application and apply filters to refine the list. Then, select individual applications from the list.

**Note**
Classification is applicable to cloud applications only. When a classification is updated (for example, with new cloud application traffic), any policy rules in use are updated immediately.

4. Specify an action for the rule.
5. Specify a schedule for the rule.
6. Click Save.
Traffic shaping settings

Use these settings to specify maximum bandwidth, traffic optimization, and bandwidth allocation for internet-bound traffic.

- To view bandwidth usage, click **Show bandwidth usage**.

General settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total available WAN bandwidth</td>
<td>Sum of all WAN links’ maximum limits, in KBps.</td>
</tr>
<tr>
<td>Optimize for real-time (VoIP)</td>
<td>Give priority to real-time traffic such as VoIP. If disabled, priority will</td>
</tr>
<tr>
<td></td>
<td>be applicable only for excess bandwidth, that is, bandwidth remaining after</td>
</tr>
<tr>
<td></td>
<td>guaranteed bandwidth allocation.</td>
</tr>
<tr>
<td>Enforce guaranteed bandwidth</td>
<td>Handle all internet-bound traffic by the traffic-shaping policy applied to</td>
</tr>
<tr>
<td></td>
<td>it. If there is no policy applied to the traffic, it will be handled by the</td>
</tr>
<tr>
<td></td>
<td>default policy.</td>
</tr>
<tr>
<td></td>
<td>Enable this setting if you want to enforce bandwidth restriction on the</td>
</tr>
<tr>
<td></td>
<td>traffic to which a traffic-shaping policy is not applied.</td>
</tr>
<tr>
<td></td>
<td>Disable this setting if you do not want to enforce a bandwidth restriction</td>
</tr>
<tr>
<td></td>
<td>on traffic to which a traffic-shaping policy is not applied. (It will</td>
</tr>
<tr>
<td></td>
<td>handle traffic only on which a traffic-shaping policy is applied.)</td>
</tr>
<tr>
<td>Default policy</td>
<td>Default policy to use for traffic that does not have a traffic-shaping policy</td>
</tr>
<tr>
<td></td>
<td>applied.</td>
</tr>
<tr>
<td></td>
<td>• Guarantee Minimum bandwidth available to the user.</td>
</tr>
<tr>
<td></td>
<td>• Limit Maximum bandwidth available to the user.</td>
</tr>
<tr>
<td></td>
<td>• Priority Set from 1 (highest) to 7 (lowest) depending on the traffic</td>
</tr>
<tr>
<td></td>
<td>required to be shaped.</td>
</tr>
</tbody>
</table>

3.4.5 Wireless

Wireless protection lets you define wireless networks and control access to them. The firewall supports the latest security and encryption, including rogue access point scanning and **WPA2**. Wireless protection allows you to configure and manage access points, wireless networks, and clients. You can also add and manage mesh networks and hotspots.
Wireless networks

A wireless network provides common connection settings for wireless clients. These settings include SSID, security mode, and the method for handling client traffic.

When you add a wireless network to an access point, you define the method of integrating traffic on the wireless network into your local network.

### Table 1: Client traffic types

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Separate zone</td>
<td>The wireless network is handled as a separate network with the specified IP address range. All traffic from a separate zone network is sent to XG Firewall using the VXLAN protocol.</td>
</tr>
<tr>
<td>Bridge to AP LAN</td>
<td>The wireless network is bridged into the network of the selected access point. Clients share the IP address range of the access point.</td>
</tr>
<tr>
<td>Bridge to VLAN</td>
<td>The wireless network is bridged into a VLAN. Use this method when you want access points to be in a common network that is separate from the wireless clients.</td>
</tr>
</tbody>
</table>

### General settings

- **Client traffic**: Method for integrating traffic on the wireless network into your local network.
- **Encryption**: Encryption algorithm to use for network traffic. AES is recommended.
- **Time-based access**: Allow access to the wireless network access according to the specified schedule.
- **Client isolation**: Prevent traffic among wireless clients that connect to the same SSID on the same radio. This setting is typically used on guest networks.
- **Hide SSID**: Do not show the wireless network SSID.
- **Fast transition**: Force wireless networks to use the IEEE 802.11r standard.
- **MAC filtering**: Restrict the MAC addresses allowed to connect to the wireless network. Blacklists allow all MAC addresses except those in the selected list. Whitelists prohibit all MAC addresses except those in the selected list.

### Add a New Wireless Network

This page describes how to create a new wireless network.

The **Add** button on the **Wireless Networks** page allows to define a new wireless network. This can then be used in definitions for access points and access point groups.

1. Go to **Device Configuration > Protect > Wireless > Wireless Networks** and click the **Add** button.
   A new page **General Settings** opens.
2. Make the following settings:

Name
Enter a descriptive name for the network.

Description
Enter a description for the wireless network that helps you to identify it.

SSID
Enter the Service Set Identifier (SSID) for the network which will be seen by clients to identify the wireless network. The SSID may consist of 1-32 ASCII printable characters. It must not contain a comma and must not begin or end with a space.

Security Mode
Select a security mode from the drop-down list. Default is WPA 2 Personal. We recommend to prefer WPA2 over WPA, if possible. For security reasons, we recommend to not use WEP unless there are clients using your wireless network that do not support one of the other methods.

When using an enterprise authentication method, you also need to configure a RADIUS server on the System > Authentication > Authentication Server or Objects > Assets > Authentication Server page. As NAS ID of the RADIUS server enter the wireless network name.

Note
Sophos Firewall OS supports the IEEE 802.11r standard in WPA2 (PSK/Enterprise) networks to reduce roaming times. Clients also need to support the IEEE 802.11r standard.

Passphrase/PSK
Only available with WPA Personal, WPA2Personal and WPA2/WPA Personal security mode.

Enter the passphrase to protect the wireless network from unauthorized access and repeat it in the next field. The passphrase may consist of 8-63 ASCII printable characters.

Key
Only available with WEP Open security mode.

Enter a WEP key here that consists of exactly 26 hexadecimal characters.

Client Traffic
Select a method how the wireless network is to be integrated into your local network.

Separate Zone
Default. The wireless network is handled as a separate network, having an IP address range of its own. Using this option, after adding the wireless network, proceed as described in chapter Next Steps for Seperate Zone Networks.

Note
When switching an existing Separate Zone network to Bridge to AP LAN or Bridge to VLAN, an already configured WLAN interface will be deleted.

Zone
Select a zone where the wireless network should be broadcasted.
Sophos Firewall Manager

Default: WiFi

IP Address
Assign an IP address to the wireless network.

Netmask
Select a subnet mask for the IP address.

Bridge to AP LAN
You can bridge a wireless network into the network of an access point, that means that wireless clients share the same IP address range. Using this option, after adding the wireless network, proceed as described in chapter Next Steps for Bridge to AP LAN Networks.

Bridge to VLAN
Not available for Local WiFi Devices.
You can decide to have this wireless network's traffic bridged to a VLAN of your choice. This is useful when you want access points to be in a common network separate from the wireless clients.

Bridge to VLAN ID
Enter the VLAN ID of the network that the wireless clients should be part of.

Client VLAN ID
Only available with an enterprise security mode.
Select how the VLAN ID is defined.
- **Static**: Uses the VLAN ID defined in the Bridge to VLAN ID field.
- **RADIUS & Static**: Uses the VLAN ID delivered by your RADIUS server: When a user connects to one of your wireless networks and authenticates at your RADIUS server, the RADIUS server tells the access point what VLAN ID to use for that user. Thus, when using multiple wireless networks, you can define per user who has access to which internal networks. If a user does not have a VLAN ID attribute assigned, the VLAN ID defined in the Bridge to VLAN ID is used.

3. Optionally, you can make the following **Advanced Settings**:

Encryption
Only available with WPA, WPA2 or WPA2/WPA encryption modes): Select an encryption algorithm which can be either AES, TKIP or TKIP&AES. For security reasons, it is recommended to use AES.

Frequency Band
Access points assigned to this wireless network will transmit on the selected frequency band(s). The 5 GHz band generally has higher performance, lower latency, and is typically less disturbed. Hence it should be preferred for e.g. VoIP communication. For an overview which APs support the 5 GHz band, see chapter Protection > Wireless Protection > Access Points or Objects > Assets > Access Points.

Time-based Access
Select this option if you want to automatically enable and disable the wireless network according to a time schedule.

Select Active-Time
Select a schedule definition which determines when the wireless network is enabled. You can add a new schedule definition by clicking the **Add** button.

Client Isolation
Clients within a network usually can communicate with one another. If you want to prevent this, for example in a guest network, select **Enabled** from the drop-down list.
Hide SSID

If you want to hide the wireless network’s SSID, select Yes from the drop-down list. Please note that this is no security feature.

Fast Transition

Only available with WPA2 Personal/Enterprise security mode.

Wireless networks with WPA2 security use the IEEE 802.11r standard. If you want to prevent this, select Disabled from the drop-down list.

MAC Filtering

To restrict the MAC addresses allowed to connect to this wireless network, select Blacklist or Whitelist. With Blacklist, all MAC addresses are allowed except those listed on the MAC List. With Whitelist, all MAC addresses are prohibited except those listed on the MAC List.

MAC Hosts added under Objects > Host and Services > MAC Host will be displayed in the MAC List.

Figure 96: Add Wireless Network
4. Click **Save** to save your settings and add the wireless network.

**Related tasks**

_Bridge to AP LAN Networks with Local Devices_ (page 113)
**Sophos Firewall Manager**

**Next Steps for Separate Zone Networks**

When you created a wireless network with the option **Separate Zone**, a new corresponding virtual hardware interface will be created automatically, e.g., wlnet1. To be able to use the wireless network, some further manual configuration steps are required. Proceed as follows:

1. **Enable DHCP for the wireless clients on the respective SF device.**
   For your clients to be able to connect to Sophos Firewall OS, they need to be assigned an IP address and a default gateway on the respective SF device. Therefore, on the **Configure > Network > DHCP** page, set up a DHCP server for the interface.

2. **Create a Network Policy on the Policies page to provide Internet access to the wireless clients.**

**Bridge to AP LAN Networks with Local Devices**

For Local WiFi Devices you need to make some extra setting on the SF device to make bridging to AP LAN work.

1. **Edit the Local WiFi Device on the Protect > Wireless > Access Points page and select the wireless network.**

2. **Create a new bridge interface on the Configure > Network > Interfaces page to use the wireless interface in Bridge mode or Edit the interface and select zone and provide IP Address to use the interface in Gateway mode.**

3. **If you want to use the interface in Gateway mode then create a DHCP server on the Configure > Network > DHCP page so that the client can receive an IP.**

**Mesh networks**

A mesh network is a network topology in which each node relays data for the network, allowing the network to extend over a large area. In a mesh network, access points can act as root or as mesh nodes. You can deploy a mesh network as a wireless repeater or as a wireless bridge.

**Repeater configuration**

When an access point starts, it attempts to connect to the firewall through a wired LAN connection. If it can do so, it assumes the role of root access point. If it cannot, it assumes the role of a mesh access point and joins the network as a client. Mesh access points broadcast the SSID from the root access point.

**Bridge configuration**

In a bridge configuration, you use a mesh network as a wireless connection between two Ethernet networks. To establish a wireless bridge, you connect the second Ethernet segment to the Ethernet interface of the mesh access point.
General settings

**Mesh-ID**
Unique ID for the mesh network. Access points look for others advertising the same mesh ID.

**Frequency band**
Band on which the mesh network operates.

**Access points**
Access points to include in the mesh network.

**Add Mesh Network**
On this page you can create mesh networks and assign access points to them.

The **Add** button on the **Mesh Networks** page allows to define a new mesh network.

1. Go to **Device Configuration > Protect > Wireless > Mesh Networks** and click the **Add** button. A new page **General Settings** opens.
2. Make the following settings:

**Mesh ID**
Enter a unique ID for the mesh network.

**Frequency Band**
Access points assigned to this network will transmit the mesh network on the selected frequency band. Generally, it is a good idea to use a different frequency band for the mesh network than for the broadcasted wireless networks.

**Description**
Optionally, add a description or other information.

<table>
<thead>
<tr>
<th>Mesh-ID *</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency Band</td>
<td>5 GHz</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
</tbody>
</table>

Figure 97: Add Mesh Network

3. Click **Save** to save your settings and add the mesh network.
Access point groups

With access point groups, you can assign wireless networks and specify VLAN tagging to a group of access points. Groups provide a convenient method of managing wireless networks for several access points, rather than individually.

**Note**
If you turn off a group, all included access points will stop broadcasting the wireless networks.

General settings

**Wireless networks**
Wireless networks to include in the group. All networks will be assigned to the access points that you specify.

**VLAN tagging**
Connect the access points with the specified VLAN Ethernet interface.

**Access points**
Access points to which the specified wireless networks will be assigned.

Add an access point group

1. Go to *Wireless > Access point groups* and click *Add*.
2. Type a name.
4. Specify settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN tagging</td>
<td>Connect the access points with the specified VLAN Ethernet interface.</td>
</tr>
</tbody>
</table>

5. In *Access points*, click *Add new item* and select the access points.
6. Click *Save*.

Hotspots

A hotspot is a network node that provides internet connectivity using a Wi-Fi device such as a wireless router. Hotspots are typically used to provide guest access in public areas. When you add an interface to a hotspot, the associated access points act as hotspots. Hotspots support a full suite of protection features and authentication methods.

When you add a hotspot, the firewall creates a corresponding firewall rule. Using this rule, you can enforce policies and scan traffic.

**Note**
In some locations, public hotspots are subject to content and usage restrictions. You may also be required to register your hotspot. Before you deploy a hotspot, check the applicable legislation.

You can redirect users to a captive portal or login page where users must accept terms of usage or authenticate themselves using a generated password or voucher. After login, you can redirect users to a specific URL, for example, your company page.
General settings

Redirect to HTTPS
Redirect traffic over HTTPS using the default IP address or the specified host name.

Redirect to URL after login
Redirect users to the specified page (for example, your company page) after logging on.

Enable customization
Provide a custom login page or voucher.

Add Hotspot
This page describes how to add a hotspot.

Note
A hotspot has to be assigned to an existing interface, typically a WLAN interface. All hosts using this interface will automatically be restricted by the hotspot. Therefore, before you create a hotspot you would typically create a wireless network with client traffic Separate Zone, then create an interface for the respective WLAN interface hardware. For more information see Device Configuration > Protect > Wireless > Wireless Networks.

1. Go to Device Configuration > Protect > Wireless > Hotspots and click Add.
2. Make the following settings:

Name
Enter a descriptive name for hotspot.

Description (optional)
Enter a description or other information.

Interfaces
Select or add the interfaces which are to be restricted by the hotspot. An interface can only be used by one hotspot.

Note
Hotspots will work only on LAN and DMZ member interfaces of the bridge. You should not select an uplink interface here because traffic to the Internet will completely be blocked afterwards. Additionally, we strongly advise against using interfaces used by servers which provide essential services like authentication. You may irreversibly lock yourself out of Sophos Firewall OS!

Users
Select or add users for administrative settings. Administrative users are allowed to create vouchers or change the password of the day in the User Portal. By default nobody is allowed to make administrative settings.

Application Filter Policy (optional)
Select or add an application filter policy for the hotspot.

Web Filter Policy (optional)
Select or add a web filter policy for the hotspot.

IPS Policies (optional)
Select or add IPS policies for the hotspot.

Traffic Shaping Policy (optional)
Select or add a traffic shaping policy for the hotspot.

Redirect to HTTPS *(optional)*
Enable to redirect users to HTTPS.

Hostname Type
Select the hostname type for the hotspot.
- None (IP Address)
- Custom hostname

Hostname *(if Custom hostname is selected)*
Add a hostname for the redirect.

Hotspot Type
Select a hotspot type for the selected interfaces.
- **Terms of Use Acceptance** Customers can access the Internet after accepting the terms of use.

Session Expires
Select the time span after which the access will expire. After that, with the hotspot type Terms of Use Acceptance, the users have to accept the terms of use again to log in. With the hotspot type **Backend Authentication**, the users have to authenticate again.

Terms of Use
Add the text to be displayed as terms of use. Simple HTML markup and hyperlinks are allowed.
- **Password of the Day** A new password will be created automatically once a day. This password will be available in the User Portal on the Hotspots tab which is available to all users specified for this hotspot. Additionally it will be sent to the specified email address(es).

Password Creation Time
The assigned time of the day at which the new password will be created. At this time the former password will immediately get invalid and current sessions will be cut off.

Send Password by Email to *(optional)*
Add email addresses to which the password shall be sent.

Synchronize Password with PSK of Wireless Networks *(optional)*
Select this option to synchronize the new generated/saved password with wireless PSK.

**Note**
With the new PSK all APs that are configured with a separate zone wireless network that is also used as a hotspot interface will be reconfigured and restarted. This means all connections will be dropped.

- **Voucher** With this hotspot type, in the User Portal tokens with different limitations and properties can be generated, printed and given to customers. After entering the code, the customers can then directly access the Internet.

Voucher Definitions
Add or select the voucher definitions you want to use for the hotspot. How to add a voucher definition is explained on the Voucher Definitions page.

Devices per Voucher
Enter the number of devices which are allowed to log in with one voucher during its lifetime. It is not recommended to use the unlimited entry.

**Terms of Use**

*not with hotspot type Terms of Use Acceptance:*
Add the text to be displayed as terms of use. Simple HTML markup and hyperlinks are allowed.

**Users Have to Accept Terms of Use**

*not with hotspot type Terms of Use Acceptance:*
Enable this option if you want the hotspot users to accept your terms of use before accessing the Internet.

**Redirect to URL After Login**

Enable, so that users will be redirected automatically to a particular URL after entering password or voucher data. URLs for example could be your hotel's website or a webpage stating your portal system policies.

**URL**

Enter URL to which the user will be redirected to.
3. Optionally, customize the hotspot.

**Enable Customization**

Enable to use a customized HTML file with your own images and stylesheets. Additionally, you can customize the voucher layout.

**Customization Type**

Select the customization type.
Sophos Firewall Manager

- **Basic** Uses the default login page template. If required, change logo, title, and text.

**Logo**

Upload a logo for the login page. Supported image file types are jpg, jpeg, png and gif. A maximum image width of 300 px and height of 100 px is recommended (depending on the title length).

**Scale Logo to Recommended Size**

If selected, a logo exceeding the recommended width or height will be scaled down and displayed in the recommended size. If not selected, the logo will be displayed in the original size.

**Title**

Add a title for the login page. Simple HTML markup and hyperlinks are allowed.

**Custom Text**

Add an additional text for the login page. You can for example enter the SSID of the wireless network to be used. Simple HTML markup and hyperlinks are allowed.

- **Full** Select an individual login HTML page.

**Login Page Template**

Select the HTML template you want to use for your individual login page. Clicking **Browse**... opens a window where you can select and upload the file. In this template, you can use variables that can dynamically insert information for each hotspot. For example, you can add the company name and administrator information, the terms of use and the login form. See detailed information in chapter **Login Page Template**.

**Images/Stylesheet**

Add files that are referenced in your login page template, e.g., images, stylesheets, or JavaScript files. Clicking **Browse**... opens a window where you can select and upload the files.

**Voucher Template**

*(only with hotspot type Voucher):* Clicking **Browse**... opens a dialog where you can select and upload a PDF file with the voucher layout. By default, a default template is used. The voucher PDF file has to be of PDF version PDF 1.5 or lower. It may have any page size and format—both size and format will be adjusted during voucher creation in the User Portal, depending on page size and number of vouchers per page specified there.

The PDF file may contain the following variables that will be replaced with the respective values during voucher generation in the User Portal:

- Wireless network name (SSID): <?ssid0?> (and <?ssid1?>, <?ssid2?> and so on, if the WLAN has more than one SSIDs)
- Wireless network password: <?psk0?> (and <?psk1?>, <?psk2?> and so on, if the WLAN has more than one SSIDs)
- Voucher code: <?code?>
- Voucher validity time: <?validity?>
- Voucher data limit: <?datalimit?>
- Voucher time limit: <?timelimit?>
- Comment: <?comment?>
- QR code with the hotspot access data encoded: <?qrX?>. The upper left corner of the QR code will be placed on the lower left corner of the variable.
Note
When using variables, the PDF file must include the entire character sets of the fonts used. When a variable is replaced by its value, and one of the substitute characters is not available, it will be displayed incorrectly. We recommend to add the string `<? abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789? >` (for English usage) to your PDF file, which will automatically be removed during voucher generation.

Figure 99: Hotspot Customization

4. Click **Save** to save your settings.

The hotspot is now available and appears in the hotspot list.

You can see if the hotspot is running on the **Monitor and Analyze > Diagnostics > Services** page. There you can also stop or start the hotspot.

**Related concepts**

**Hotspot** (page 126)

**Services** (page 18)
View system service status and manage services.

**Login page template** (page 121)
A login page template contains access information and forms that are required for users to log in to your network through a hotspot. Login pages are written in HTML and contain variables that are replaced during page generation. You can also create conditional blocks that are rendered only if the specified conditions are met. Refer to the login page template in **Wireless > Hotspot settings** for usage examples.
### Table 2: Variables

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;?admin_message?&gt;</td>
<td>“For administrative questions please contact:”</td>
</tr>
<tr>
<td>&lt;?admin_contact?&gt;</td>
<td>Send notifications to email address as defined in Administration &gt; Notification settings.</td>
</tr>
<tr>
<td>&lt;?company_logo?&gt;</td>
<td>Company logo to be used in basic customization as defined in Wireless &gt; Hotspots.</td>
</tr>
<tr>
<td>&lt;?company_text?&gt;</td>
<td>Default company text as defined in Wireless &gt; Hotspots.</td>
</tr>
<tr>
<td>&lt;?error?&gt;</td>
<td>Error returned when attempting to log in</td>
</tr>
<tr>
<td>&lt;?location?&gt;</td>
<td>URL the user requested</td>
</tr>
<tr>
<td>&lt;?location_host?&gt;</td>
<td>Hostname of the URL the user requested</td>
</tr>
<tr>
<td>&lt;?login_form?&gt;</td>
<td>Login form suitable for the hotspot type, for example, user name and password text boxes, a token text box, or an “Accept” check box.</td>
</tr>
<tr>
<td>&lt;?maclimit?&gt;</td>
<td>Number of devices allowed per voucher as defined in Wireless &gt; Hotspots.</td>
</tr>
<tr>
<td>&lt;?numdevices?&gt;</td>
<td>Number of devices used by the voucher as defined in the template.</td>
</tr>
<tr>
<td>&lt;?redirect_host?&gt;</td>
<td>Redirect URL as defined in Wireless &gt; Hotspots.</td>
</tr>
<tr>
<td>&lt;?terms?&gt;</td>
<td>Terms of use as defined in Wireless &gt; Hotspots.</td>
</tr>
<tr>
<td>&lt;?time_total?&gt;</td>
<td>Total time quota allowed by the voucher as defined in Wireless &gt; Hotspot voucher definition.</td>
</tr>
<tr>
<td>&lt;?timeend?&gt;</td>
<td>Validity period specified by the voucher as defined in Wireless &gt; Hotspot voucher definition.</td>
</tr>
<tr>
<td>&lt;?traffic_total?&gt;</td>
<td>Total data volume allowed by the voucher as defined in Wireless &gt; Hotspot voucher definition.</td>
</tr>
</tbody>
</table>

### Table 3: Conditional blocks

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;?if_loggedin?&gt;</td>
<td>Section is displayed when the user has successfully logged in.</td>
</tr>
<tr>
<td>&lt;?if_notloggedin?&gt;</td>
<td>Section is displayed when the user has not yet logged in, for example, because terms of use have to be accepted or because an error occurred.</td>
</tr>
<tr>
<td>&lt;?if_authtype_password?&gt;</td>
<td>Section is displayed when hotspot type is “Password of the day”.</td>
</tr>
<tr>
<td>&lt;?if_authtype_disclaimer?&gt;</td>
<td>Section is displayed when hotspot type is “Terms of use acceptance”.</td>
</tr>
<tr>
<td>&lt;?if_authtype_token?&gt;</td>
<td>Section is displayed when hotspot type is “Voucher”.</td>
</tr>
<tr>
<td>&lt;?if_location?&gt;</td>
<td>Section is displayed when the user has been redirected.</td>
</tr>
</tbody>
</table>
Sophos Firewall Manager
Name

Definition

<?if_redirect_url?>

Section is displayed when Redirect to URL after login
is on.

<?if_not_redirect_url?>

Section is displayed when Redirect to URL after login
is off.

<?if_timelimit?>

Section is displayed when a validity period is set for a
voucher.

<?if_trafficlimit?>

Section is displayed when a data volume is set for a
voucher.

<?if_timequota?>

Section is displayed when a time quota is set for a
voucher.

<?if_maclimit?>

Section is displayed when a Devices per voucher
value is specified.

<?if_terms?>

Section is displayed when Terms of use is turned on
and terms are defined.

<?if_error?>

Section is displayed when an error occurred while
trying to log in.

Custom login forms
You can create a login form instead of using the pre-defined <?login_form?> variable.
Enclose the form in the following tags:
<form action="?action=login" method="POST">

...

</form>

For a “Terms of acceptance” hotspot, add an accept check box:
<input type="checkbox" name="accept" value="true">
For a “Password of the day” or voucher hotspot, add a token text box:
<input type="text" name="token">
Add a means to submit the form, for example, a login button:
<input type="submit" name="login" value="Login">

Hotspot voucher definition
Hotspot voucher definitions specify network access. You can use voucher definitions to limit the validity
period, time quota, and data volume for users who have access to voucher-type hotspots.

General settings
Validity period

Copyright © Sophos Limited

Time for which vouchers of this type will be valid.
The period starts from the first logon.

123


**Time quota**

Maximum connectivity time for vouchers of this type. The quota starts at logon and stops at logoff. Counting stops after five minutes of inactivity.

**Data volume**

Maximum volume of data to be transmitted for vouchers of this type.

**Add a hotspot voucher definition**

1. Go to Wireless > Hotspot voucher definition and click Add.
2. Type a name.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validity period</td>
<td>Time for which vouchers of this type will be valid. The period starts from the first logon.</td>
</tr>
<tr>
<td>Time quota</td>
<td>Maximum connectivity time for vouchers of this type. The quota starts at logon and stops at logoff. Counting stops after five minutes of inactivity.</td>
</tr>
<tr>
<td>Data volume</td>
<td>Maximum volume of data to be transmitted for vouchers of this type.</td>
</tr>
</tbody>
</table>

4. Click Save.

**Rogue AP scan**

A rogue access point refers to any access point connected to your network without authorization. Attackers can use rogue access points for traffic sniffing and other purposes such as man-in-the-middle attacks. You can mitigate these threats by scanning the access points on your network and marking unauthorized access points as rogue access points.

- To schedule scanning, select the Schedule system-triggered scan at check box, specify a schedule, and click Apply.
- To scan your network for rogue access points, click Scan now.
- To authorize an access point, click A.
- To mark an access point as a rogue access point, click R.

**Wireless settings**

Use these settings to enable wireless protection, to set notification timeout, and to configure a RADIUS server for enterprise authentication.

**AP firmware**

If access point firmware is not installed, click the link to download and install.
Global settings

Enable wireless protection
Scan all traffic on the specified zones for threats and malware.

Allowed zone
Network zones that permit access point connectivity. You can deploy access points on the specified zones.

Advanced settings

Timeout
The time, in minutes, between when an access point goes offline and when the firewall sends a timeout notification. After the specified time, the access point will be considered inactive.

RADIUS server
RADIUS server to use for enterprise authentication. Access points communicate with the firewall, not the RADIUS server, for authentication. Port 414 is used for RADIUS communication between the firewall and access points. Access point sends accounting information on port 417 to the firewall. Firewall then forwards the information on the configured accounting port 1813 to the RADIUS server. Interim accounting updates are not supported. Accounting Request or Accounting Response contains accounting related informations. It is separate from access request, response, or challenge.

You must set up the wireless network with 802.1x authentication.

You must enable accounting for your RADIUS server. RADIUS accounting is supported on AP15, AP15C, AP55, AP55C, AP100, AP100C, AP100X, and Wi-Fi enabled devices.

You must add a network translation policy for the access point networks when the RADIUS server is connected to the firewall through an IPsec tunnel. This replaces the source address with the IP address of the firewall that is used to reach the RADIUS server.

Note
Radius SSO feature is not supported in wireless enterprise authentication.

Secondary RADIUS server
A backup RADIUS server for enterprise authentication when the firewall can’t access the primary RADIUS server.
**Wireless client list**
The wireless client list displays all clients that are currently connected to a wireless network through an access point. You can view clients by access point or SSID. Connection characteristics such as signal strength and frequency are also displayed.

**Hotspot**
On this page you can make additional hotspot settings.

**General Voucher Options**
Here you can decide if and after which time interval you want to delete expired vouchers from the database. In the hotspot log you will still find information about deleted vouchers.

**Login Page Certificate**
To ensure login over HTTPS you can select certificates for the page login. You can generate and upload new certificates with on the Device Configuration > Protect > Web Server > Certificate page. Select the requested certificate from the drop-down list and click **Apply** to activate it.

**Walled Garden**
Add or select specific hosts or networks to be always accessible by all users, without entering a password or a voucher code. Hosts can be added on the Device Configuration > System > Hosts and Services > IP Hosts page, networks can be added via the System > Network menu.

**Clear Walled Garden Configuration**
Click **Clear Walled Garden Configuration** to clear the configuration settings.

### 3.4.6 Email

**This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.**

From the email tab, you can configure SMTP/S, POP/S and IMAP/S settings, email security policies, secure PDF eXchange (SPX) and data control.

The device offers comprehensive email security, preventing sophisticated forms of zero-hour threats and blended attacks involving spam, botnets, phishing, spyware and more. The basic email protection configuration includes:

- Creating policies to allow or deny email traffic to and from your email server.
- Apply spam, malware, data and file protection on email traffic.
• SPX
• configuring an email threshold size for scanning
• specifying action to be taken if a virus is detected
• blocking mails based on sender or recipient
• blocking mails with certain file types.

SMTP deployment modes
Two deployment modes are available:
• Legacy mode
• MTA mode

Legacy mode
In legacy mode, Sophos XG Firewall acts as a transparent proxy that scans emails for malware and spam, applies SPX encryption and data protection.

MTA mode
In MTA mode, Sophos XG Firewall acts as a mail transfer agent (MTA). MTA is a service that is responsible for receiving and routing emails to their specified destinations.

Use MTA mode deployment if you need to route emails instead of forwarding email traffic as proxy.

In MTA mode, Sophos XG Firewall performs the following functions:
• Performs relaying and routing of emails. You can configure relaying of emails from Email > Relay settings.
• Protects multiple email servers using SMTP policies. You can define the protection on your email domains from Email > Policies > SMTP policies.
• Displays email messages that are either in-wait or failed to be delivered in the Email > Mail spool.
• Displays logs for all the emails processed by the device from Email > Mail logs.

Email Policies and Exceptions
This page allows configuration of POP-IMAP Malware Scanning and Email Scanning Policy.

This feature requires a subscription in Sophos XG Firewall. It can be configured but cannot be enforced without a valid Email Protection subscription.

This page contains the following sections:
• POP-IMAP Malware Scanning
• Email Policies

POP-IMAP Malware Scanning
The device applies a single policy to all POP and IMAP/S traffic so that whenever a virus gets detected in an Email, the virus-affected attachment is stripped from the Email and the Email body is replaced with a notification message.

Scanning
Specify the type of scanning to be applied.

Available Options:
• **Disable**: No scanning applied.

• **Single Anti-Virus (Maximum Performance)**: Traffic will be scanned only by the Primary Anti Virus Engine. Select the **Primary Anti Virus Engine** from **System > System Services > Malware Protection**.

• **Dual Anti-Virus (Maximum Security)**: Traffic will be scanned by both Anti Virus Engines, first by the Primary and then by the Secondary Engine. Select the **Primary Anti Virus Engine** from **System > System Services > Malware Protection**.

---

### Email Policies

Use this section to add, edit, delete and synchronize POP-IMAP Policy, SMTP Malware Policy, SMTP Scanning Policy and SMTP Profiles. You can filter the list of Policy based on the email sender or recipient.

#### Mode Switch option

Select the mode from the following for which you want to create Policy:

- MTA
- Legacy

#### Add Email Policy

Select to create a new Policy from the following:

- **POP-IMAP Policy**:

  POP-IMAP Scanning Policy can be configured for particular senders and recipients. A Policy defines the action to be taken if an Email is detected as Spam, Probable Spam, part of Virus Outbreak or Probable Virus Outbreak. To reduce the risk of losing legitimate messages, the Spam Quarantine repository - a storage location - provides administrators with a way to automatically quarantine Emails that are identified as spam. This helps in managing spam and probable spam quarantined mails so that the user can take appropriate actions on such emails.

  **Note**

  A default editable POP-IMAP Policy **default-pop-av** is pre-configured in all SF device(s) and applied to all Email traffic as soon as you subscribe to the Email Protection Module.

- **SMTP Profile (available only when MTA mode is enabled)**:

  SFM allows you to create SMTP Profiles for multiple Sophos XG Firewall devices which can be used to protect multiple Domains on your internal Email Server or multiple Email Servers. Using these Profiles, Sophos XG Firewall protects the internal server(s) from remote attacks and additionally provide powerful virus scanning, Email encryption and Email filtering services.

- **SMTP Malware Policy (available only when MTA mode is disabled)**:

  SMTP Malware Scanning Policy allows you to define action to be taken on Emails if they are virus-infected, suspicious or contain a protected attachment. Based on the action defined in Policy, such Emails can be delivered as it is, dropped, or cured and then delivered or quarantined. A SMTP Malware Scanning Policy defines:

  - whether to quarantine the Email
  - whether sender, receiver or Administrator are to be notified
  - whether to block the Email containing a specified file type
  - what action is to be taken if Email is infected/suspicious/ contains a protected attachment: deliver as
it is, drop, cure and then deliver. A default SMTP Malware Scanning Policy is pre-configured in the Device and applied to all Email traffic as soon as you subscribe to the Email Protection Module. It is recommended to create separate Policy fine tuned to your specific network requirements to minimize the possibility of threats.

Note
A default editable SMTP Malware Policy `default-smtp-av` is pre-configured in all SF device(s) and applied to all Email traffic as soon as you subscribe to the Email Protection Module.

- **SMTP Scanning Policy** (available only when MTA mode is disabled):

  SMTP Scanning Policy can be configured for particular senders and recipients. Policy defines action to be taken if an Email is detected as Spam, Probable Spam, part of Virus Outbreak or Probable Virus Outbreak, and lets you specify the action to be performed on the Email. To reduce the risk of losing the legitimate messages, Spam Quarantine repository - a storage location, provides administrators a way to automatically quarantine Emails that are identified as Spam. This helps in managing Spam and probable Spam quarantined mails so that user can take appropriate actions on such mails.

Add POP - IMAP Scanning Policy
This feature requires a subscription in Sophos XG Firewall. It can be configured but cannot be enforced without a valid Email Protection subscription.

The **POP - IMAP Scanning Policy** page allows you to configure scanning policy to detect incoming and outgoing Spam in Email traffic and take appropriate action.

1. Go to **Device Configuration > Protect > Email > Policies**.
2. Click **POP-IMAP Scan** under **Add Policy**.
3. Enter Email Address/Domain Group details.

**Sender**
Specify Email Address(es) of the Sender(s). You can select from the variants:

- **Contains**: Specify keywords to be matched with Sender Email Addresses. Rule applies to Address(es) containing those keywords. For example, if keyword "mail" is specified, rule will apply to Sender Email Addresses john@hotmail.com, sophosmail@sophos.com, etc.

- **Equals**: Specify the exact Email Address(es) of the Sender(s).

You can also add RBLs, list of Email Addresses or keywords using **Create New** link.

**Recipient**
Specify Email Address(es) of the Recipient(s). You can select from the variants:

- **Contains**: Specify keywords to be matched with Recipient Email Addresses. Rule applies to Address(es) containing those keywords. For example, if keyword "mail" is specified, rule will apply to Recipient Email Addresses john@hotmail.com, sophosmail@sophos.com, etc.

- **Equals**: Specify the exact Email Address(es) of the Recipient(s).

You can also add RBLs, list of Email Addresses or keywords using **Create New** link.

4. Select the Filter Criteria.

**Inbound Email is**
All the Emails that are received by the users in their inbox are referred as Inbound.
On configuring Inbound Spam, all the Emails received by the users are scanned for spam and viruses by the Device. Specified action will be taken if the Device has identified the Inbound Email to be one of the following:

- Spam
- Probable Spam
- Virus Outbreak
- Probable Virus Outbreak

**Source IP/Network Address**

Specify IP/Network Address, action will be taken when the Email sender IP Address matches the specified IP/Network Address.

**Message Size**

Specify Message Size, action will be taken when the Email size matches the specified size.

**Message Header**

Specified action will be taken if the message header equals or contains the specified text.

- **Contains**: Specify keywords to be matched with Message Header. Rule applies to Header(s) containing those keywords.
- **Equals**: Specify the exact Header(s) to be scanned.

You can scan message header for Spam in:

- **Subject**: Specified action will be taken if the header contains the matching subject.
- **From**: Specified action will be taken if the header contains the matching text in the From address.
- **To**: Specified action will be taken if the header contains the matching text in the To address.
- **Other**: Specified action will be taken if the matching text is found in the headers.

**None**

Select to create a rule between specific sender and recipient without any conditions. You can set actions for POP/S-IMAP/S mails only on the basis of sender and recipient.

5. Select the action.

- **Accept**: Email is accepted and delivered to the intended recipient.
- **Prefix Subject**: Email is accepted and delivered to the intended recipient but after tagging the subject line. Tagging content is specified in spam policy. You can customize subject tagging in such a way that the recipient knows that the Email is a spam Email. For Example Contents to be prefixed to the original subject: ‘Spam notification from the Device – ‘Original subject: ‘This is a test’ Recipient will receive Email with subject line as: ‘Spam notification from the Device - This is a test’.
6. Click **Save**.

**Add SMTP Policy**

This feature is applicable only on Sophos XG Firewall devices where MTA Mode is enabled.

1. Go to **Device Configuration > Protect > Email > Policies** and click Turn off Legacy Mode.
2. Click **SMTP Route & Scan** under **Add Policy**.
3. Specify values for **Domains and Routing Target**.

**Domain**

Select the Domain(s) (**Address Group (MTA)**) to which the SMTP Policy links. You can also add new Domain(s) using **Create New** link. Address Group (MTA) can be configured from **Device Configuration > Protect > Email > Address Group (MTA)**.

**Route By**

Select the host to which Emails for the listed domains should be forwarded to, for example, the Microsoft Exchange Server on your local network. You can choose between different server types:

- **Available Options:**

- **Static Host:**

  Select **Static Host** to define the target route as a static IP address(es) of the internal Email Server.

- **MX:**

  Select **MX** to route mail to your domain(s) by means of MX record(s). If you select this route type, the Device makes a DNS query requesting the MX record.
for the recipient's domain name, which is the portion of the email address following the "@" character. Make sure that the gateway is not the primary MX for the domain(s) specified above, since it will not deliver mail to itself.

4. Enable Spam Protection section to configure Spam scanning of Email traffic.

Check for Inbound Spam

All the Emails that are received by the users in their inbox are referred to as Inbound.

If you select Check for Inbound Spam, all the Emails received by the users are scanned for spam by the Device.

If Email is detected as a "Spam", selected Spam Action is applied.

If Email is detected as a " Probable Spam", which means that the Anti-spam engine has detected the Email as suspicious but not as Spam, selected Probable Spam Action is applied.

Check for Virus Outbreak

If you select Check for Virus Outbreak, all the Emails received by the users are scanned for viruses by the Device.

If Email is detected to cause a virus outbreak, selected Spam Action is applied.

If Email is detected as suspicious but not confirmed as a virus outbreak, selected Probable Spam Action is applied.

Check for Outbound Spam

Emails that are sent by the user in the network to a remote user on another Email system, are referred as Outbound.

If you select Check for Outbound Spam, all the Emails sent by the local users are scanned for spam by the Device before being delivered.

If Email is detected as a "Spam", selected Spam Action is applied.

If Email is detected as a " Probable Spam", which means that the Anti-spam engine has detected the Email as suspicious but not as Spam, selected Probable Spam Action is applied.

Use Greylisting

Greylisting allows the device to control spam. When greylisting, the device temporarily rejects inbound emails from IP addresses of unknown email servers for a five-minute period. Subsequent to this period, legitimate email servers retry sending rejected emails at regular intervals. The device accepts the re-sent emails and greylists the sender's IP address for a specific period.
Check for RBL
Click to verify the reputation of the sender IP Address. When enabled, the Device dynamically checks the sender’s IP Address of all Emails. If the IP Address is found to be responsible for sending spam email or malicious contents, the Device takes action.

If Email is detected as a "Spam", selected Spam Action is applied.
If Email is detected as a "Probable Spam", which means that the Anti-spam engine has detected the Email as suspicious but not as Spam, selected Probable Spam Action is applied.

Prefix Subject
Specify prefix that is to be added with the email subject.

Note
Available when action as Warn is selected.

Recipient Verification
Available Options:
Off (Not Recommended)
Select if no action is to be taken.
With Callout (Recommended)
Recipient Verification is the process of checking the recipients of an inbound email to one of your Internal mail server. Recipient email address in the message envelope is checked against the email user account on the destination mail server. Mails to non-existent users are rejected. If the mail server is not reachable within the defined timeout period of 90 seconds, the recipient is accepted. This reduces the load on the firewall as it will only process mail for valid recipients and conserve quarantine space.
Turning off recipient verification is not recommended as it might lead to higher spam mails and clogging of quarantine space.

Spam Action
Select action to be taken if Email is detected as Spam.
Available Options:
None:
Select if no action is to be taken.
Warn:
Email is accepted and delivered to the intended recipient but after tagging the subject line.
Quarantine:
Device does not deliver Email but copies it to the Quarantine. You can view the Email details and release the Email, if required, from the Quarantine.
Drop:
Email is dropped.
Default: Drop.

Probable Spam Action
Select action to be taken if Email is detected as suspicious but not confirmed as Spam.
Available Options:
None:
Select if no action is to be taken.

Warn:
Email is accepted and delivered to the intended recipient but after tagging the subject line.

Quarantine:
Device does not deliver Email but copies it to the Quarantine. You can view the Email details and release the Email, if required, from the Quarantine.

Drop:
Email is dropped.

Default: Warn.

5. Enable Malware Protection section to configure malware scanning of Email traffic.

Scanning
Specify the type of scanning to be applied.

Available Options:

Single Anti-Virus: Traffic will be scanned ONLY by the Primary Anti-Virus Engine. Select the Primary Anti-Virus Engine from Device Configuration > System > System Services > Malware Protection. Dual Anti-Virus: Traffic will be scanned by both Anti-Virus Engines, first by Primary and then by the Secondary Engine. Select the Primary Anti-Virus Engine from Device Configuration > System > System Services > Malware Protection.

Anti-virus Action
Select action to be taken if a malware is detected in an Email.

Available Options:

None:
No action to be taken.

Quarantine:
Device does not deliver Email but copies it to the Quarantine. You can view the Email details and release the Email, if required, from the Quarantine.

Drop:
Email is rejected and a rejection notification is NOT sent to the Email sender.
Default: Drop

**Notify Sender**
If enabled, the original message is withheld by the Device and a notification is sent to the sender informing that the Email was infected.

**Quarantine Unscannable and Encrypted Content**
Enable to quarantine emails whose content cannot be scanned.
Unscannable content may include encrypted or corrupt archives, oversized email, or emails not scanned due to internal error.

6. Enable **File Protection** section to configure filtering of specific attachments in Email Traffic.

**Block File Types**
Select file types to be blocked as an attachment to remove all the files that are a potential threat and to prevent virus attacks.
More than one file type can be selected using Ctrl/Shift keys.
Device contains a default list of File Types, with each Type containing relevant file extensions. Refer to **Device Configuration > Objects > Content > File Type** to view the list of file extensions which can be blocked.
Select **All** to block Emails with any type of attachments.
Select **None** to allow Emails with any type of attachments.

**MIME Whitelist**
If one or more File Type is selected in Block File Type, this field is populated with the corresponding MIME Headers that belong to selected File Type(s).
Select the MIME Header(s) of the selected File Type(s). Only selected headers are to be allowed while the rest in the selected File Type are to be blocked during Anti-virus scanning of Email attachments.

**Drop message greater than**
Specify maximum file size in KB of Emails. Emails greater than specified size will be dropped by Device.
7. Enable **Data Protection** section to configure confidential data protection in Email Traffic.

**Data Control List**

Select Data Control List to be applied for scanning and corresponding action, Data Protection Policies can be configured from Protection > Email Protection > Data Protection (MTA).

Available Options for actions:

- **Accept**: Email is accepted and delivered to the intended recipient.
- **Accept with SPX**: Email is accepted and delivered to the intended recipient after being SPX encrypted.
- **Drop**: Email is rejected and a rejection notification is NOT sent to the Email sender.

**Notify Sender**

Enable to notify the sender of an Email if it is found to contain sensitive information as per configured Data Protection policy.

8. Select the action for all traffic applicable to Policy.

**Action**

Select action for all the traffic applicable to the Policy. Available options are **Accept** and **Reject**. Select **SPX Template** in case you select **Accept**.

Default: Accept.

**Add SMTP Malware Scanning Policy**

This feature requires a subscription in Sophos XG Firewall. It can be configured but cannot be enforced without a valid Email Protection subscription.

The SMTP Malware Scanning Policy page allows you to configure scanning policy to detect malware in Email traffic and take appropriate action.

1. Go to Device Configuration > Protect > Email > Policies and click on Switch to Legacy Mode.
2. Click SMTP Malware Scan under Add Policy.
3. Enter Policy details

**Name**

Enter a unique name to identify the scanning Policy.

**Sender**

Select the sender name from the list of users.

Select **Any** if the Policy is to be applied on all the senders.
You can also add a new Email address by clicking Create New link.

**Recipient**

Select the recipient name from the list of users.

Select Any if the Policy is to be applied on all the recipients.

You can also add a new Email Address by clicking Create New link.

**Block File Types**

Select file types to be blocked as an attachment to remove all the files that are a potential threat and to prevent from virus attacks.

More than one file type can be selected using ctrl/shift keys.

Device contains a default list of File Types, with each Type containing relevant file extensions. Refer to Protect > Web > File Type to view the list of file extensions which can be blocked.

Select All to block Emails with any type of attachments.

Select None to allow Emails with any type of attachments.

**MIME Whitelist**

If one or more File Type is selected in Block File Type, this field is populated with the corresponding MIME Headers that belong to selected File Type(s).

Select the MIME Header(s) of the selected File Type(s). Only selected headers are to be allowed while the rest in the selected File Type are to be blocked during Anti Virus scanning of Email attachments.

**Scanning**

Specify the type of scanning to be applied.

**Available Options:**

- **Disable (default):** No scanning applied.

- **Single Anti Virus (Maximum Performance):** Traffic will be scanned ONLY by the Primary Anti Virus Engine. Select the Primary Anti Virus Engine from Protection > Web Protection > Malware Protection or System > System Services > Malware Protection.

- **Dual Anti Virus (Maximum Security):** Traffic will be scanned by both Anti Virus Engines, first by Primary and then by the Secondary Engine. Select the Primary Anti Virus Engine from Protection > Web Protection > Malware Protection or System > System Services > Malware Protection.

**Action**

Enable action to be taken on the mails received, from the available options:

- **Quarantine:** If enabled, copies the Email to the quarantine file list. Email is either delivered to recipient or dropped, as per configured Recipient Action. You can view the Email details like sender and receiver of the Email in the Malware Quarantine. Administrator can access the Quarantine on the SF device from System > Current Activity > Malware Quarantine while user can access from their respective User Portal.

- **Notify Sender:** If enabled, the original message is withheld by the Device and a notification is sent to the sender informing that the Email was infected. The sender will receive the notification only if the Receiver Action is configured as Don't Deliver.
Default - *Disable*

Delivery Option for Infected Attachment/Protected Attachment

**Recipient**

Select the action to be taken on the message that is detected to be Infected, Suspicious or includes a Protected Attachment.

**Available Options:**

- **Don't Deliver** (default value): Receiver will not receive the message and will also not receive the notification regarding the infected Email.

- **Deliver Original**: Receiver receives the original Email.

- **Remove and Deliver**: Infected part of the Email is removed before delivering. Receiver will also receive the notification stating that the Email was infected and infected portion of the Email is removed. Not applicable for Blocked Attachments (Block File Type).

**Note**

Protected attachments are not scanned but receiver will be notified, if not specified otherwise.

**Administrator**

Select the action to notify the Administrator for the message detected to be Infected, Suspicious or includes a Protected Attachment.

**Available Options:**

- **Don't Deliver**: (default value) Administrator will not be notified about the infected Email.

- **Send Original**: Receiver receives the original Email.

- **Remove Attachment**: Recipient receives message without attachment and the Administrator receives the notification that the Email attachment was infected and removed before delivering Email.

**Note**

Protected attachments are not scanned but receiver will be notified, if not specified otherwise.
Add Policy

4. Click **Save** to add the Email Policy.

Add SMTP Scanning Policy

This feature requires a subscription in Sophos XG Firewall. It can be configured but cannot be enforced without a valid Email Protection subscription.

The **SMTP Scanning Policy** page allows you to configure scanning policy to detect incoming and outgoing Spam in Email traffic and take appropriate action.

1. Go to **Device Configuration** > **Protect** > **Email** > **Policies** and click on **Switch to Legacy Mode**.
2. Click **Add Policy** and select **SMTP Spam Scan**.
3. Specify **Name** for SMTP Scanning Policy.
4. Enter Email Address/Domain Group details.

**Sender**

Specify Email Address(es) of the Sender(s). You can select from the variants:

- **Contains**: Specify keywords to be matched with Sender Email Addresses. Policy applies to Address(es) containing those keywords. For example, if keyword "mail" is specified, Policy will apply to Sender Email Addresses john@hotmail.com, sophosmail@sophos.com, etc.

- **Equals**: Specify the exact Email Address(es) of the Sender(s).

You can also add RBLs, list of Email Addresses or keywords using **Create New** link.

**Recipient**

Specify Email Address(es) of the Recipient(s). You can select from the variants:

- **Contains**: Specify keywords to be matched with Recipient Email Addresses. Policy applies to Address(es) containing those keywords. For example, if keyword "mail" is specified, Policy will apply to Recipient Email Addresses john@hotmail.com, sophosmail@sophos.com, etc.

- **Equals**: Specify the exact Email Address(es) of the Recipient(s).

You can also add RBLs, list of Email Addresses or keywords using **Create New** link.

5. Select the Filter Criteria.

**Inbound Email**

All the Emails that are received by the users in their inbox are referred as Inbound.
On configuring Inbound Spam, all the Emails received by the users are scanned for spam and viruses by the Device.

Specified action will be taken if the Device has identified the Inbound Email to be one of the following:

- Spam
- Probable Spam
- Virus Outbreak
- Probable Virus Outbreak

**Outbound Email**

Emails that are sent by the user in the network to a remote user on another Email system, are referred as Outbound.

On configuring Outbound Spam, all the Emails sent by the local users are scanned before being delivered to other users on the Internet for spam and viruses by the Device.

Specified action will be taken if the Device has identified the Outbound Email to be one of the following:

- Spam
- Probable Spam
- Virus Outbreak
- Probable Virus Outbreak

**Source IP/Network Address**

Specify IP/Network Address, action will be taken when the Email sender IP Address matches the specified IP/Network Address.

**Destination IP/Network Address**

Specify IP/Network Address, action will be taken when the Email recipient IP Address matches the specified IP/Network Address.

**Sender Remote Blacklist**

Select Remote Blacklist (RBL), action will be taken when the sender is listed in the specified RBL Group.

**Message Size**

Specify Message Size, action will be taken when the Email size matches the specified size.

**Message Header**

Specified action will be taken if the message header equals or contains the specified text.

- Contains: Specify keywords to be matched with Message Header. Policy applies to Header(s) containing those keywords.
- Equals: Specify the exact Header(s) to be scanned.

**You can scan message header for Spam in:**

- Subject: Specified action will be taken if the header contains the matching subject.
- From: Specified action will be taken if the header contains the matching text in the From address.
• **To:** Specified action will be taken if the header contains the matching text in the To address.

• **Other:** Specified action will be taken if the matching text is found in the headers.

### Data Control List

Specified action will be taken if message contains data matching with the configured Data Protection Policy. You can create Data Protection Policies from **Device Configuration > Protect > Email > Data Protection Policies.**

### None

Select to create a Policy between specific sender and recipient without any conditions. You can set actions for SMTP mails only on the basis of sender and recipient.

6. Select the action.

### Action:

Select action to be taken for the SMTP traffic. **Available Options:**

- **Reject:** Email is rejected and rejection notification is sent to the Email sender.

- **Accept** *(Not available for Outbound Spam)*: Email is accepted and delivered to the intended recipient. Administrator can bind an SPX Template to this action so that the Email is delivered to the intended recipient after being SPX-encrypted.

- **Change Recipient:** Email is accepted but is not delivered to the intended recipient for whom the message was originally sent. Email is sent to the recipient specified in the spam policy.

- **Prefix Subject** *(Not available for Outbound Spam)*: Email is accepted and delivered to the intended recipient but after tagging the subject line. Administrator can bind an SPX Template to this action so that the Email is delivered to the intended recipient after being SPX-encrypted.

- **Drop:** Email is rejected but rejection notification is not sent to the Email sender.

Tagging content is specified in **To** field.

- You can customize subject tagging in such a way that the recipient knows that the Email is a spam Email.

- For Example
  
  Contents to be prefixed to the original subject: ‘Spam notification from the Device –’

  Original subject: ‘This is a test’.

  Recipient will receive Email with subject line as: ‘Spam notification from the Device - This is a test’.

**SPX Template (Legacy):** If action is selected as **Accept** or **Prefix Subject**, select the SPX Template to be applied on the Email. You can create SPX Templates from **Protection > Email Protection > SPX Encryption.**

**Quarantine:** If enabled, does not deliver Email but copies the Email to the quarantine file list. You can view the Email details like sender and recipient of the Email in the quarantined file list.

Select action to be taken for the POP-IMAP traffic.

### Available Options:

- **Accept:** Email is accepted and delivered to the intended recipient.

- **Prefix Subject:** Email is accepted and delivered to the intended recipient but after tagging the subject line. Tagging content is specified in spam policy. You can customize subject tagging in such a way that the recipient knows that the Email is
a spam Email. For Example Contents to be prefixed to the original subject: ‘Spam notification from the Device – ‘Original subject: ‘This is a test’ Recipient will receive Email with subject line as: ‘Spam notification from the Device - This is a test’.

Figure 101: Add Content Scanning Policy

7. Click **Save**.

**Add Exceptions**

Exceptions allow you to skip security checks related to spam, malware, and others for hosts or networks, sender's mail addresses, or recipient's mail addresses.

1. Go to **Email > Policies and Exceptions** and click **Add Exception**.
2. Enter a name for **Exception**.
3. Select security checks to skip.

**Skip these checks**

Select one or more security checks.

In **Spam Protection**, you can select RBL, Antispam, Greylisting, Recipient Verification, IP Reputation, or RDNS/Helo. Under **Malware Protection**, you can select Malware or
Sandstorm. In Other, you can select Data Protection, File Protection, Encryption, or Banner Addition.

Figure 102: Skip these checks

4. Select any of the following to apply the exception:

For these Sources/Hosts
Add source or hosts to skip security checks.

Note
You do not need to create exception for localhost. By default, messages are not scanned for localhost.

Or these sender addresses
Add sender’s mail address to skip security checks. Enter a valid email address (abc@example.com) or a wildcard (*.example.com).

Or these recipient addresses
Add recipient’s mail address to skip security checks. Enter a valid email address (abc@example.com) or a wildcard (*.example.com).

5. Click Save.

Data control list

This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.

This feature is available in Cyberoam models CR15iNG and above, and all Sophos UTM and Sophos Firewall models.

You can create a data control list of confidential data by selecting from the content control list (CCL). The firewall provides CCLs based on expert definitions for common financial and personally
identifiable data types. For example, credit card and social security numbers, postal and email addresses.

Subsequently, you can use data control lists to set data protection for emails.

Add Data Control List (MTA)

This feature requires a subscription in Sophos XG Firewall. It can be configured but cannot be enforced without a valid Email Protection subscription.

This feature is applicable to SF devices where MTA Mode is enabled.

This feature is NOT available in Device Models SF100 and SF200.

The Add Data Control List page is used to configure policy to scan and detect confidential data in Email traffic and take appropriate action.

1. Go to Device Configuration > Protect > Email > Data Control List and click Add.

   Note
   Ensure that MTA Mode is selected for Data Control List page. Click Turn Off Legacy Mode to switch to MTA Mode.

2. Enter policy details.

   Name
   Specify name to identify Data Control List.

   Signatures
   Select one or more Content Control signature(s) to be added to the policy.

   Filter the Content Control List based on Type or Region.

   ![Data Control List](image)

   Figure 103: Data Control List

3. Click Save to create policy.

Add Data Control List (Legacy)

This feature requires a subscription in Sophos XG Firewall. It can be configured but cannot be enforced without a valid Email Protection subscription.

This feature is applicable to SF devices where MTA Mode is disabled.
This feature is NOT available in Device Models SF100 and SF200.

The **Add Data Control List** page is used to configure policy to scan and detect confidential data in Email traffic and take appropriate action.

1. Go to **Device Configuration > Protect > Email > Data Control List** and click on **Switch to Legacy Mode**.
2. Click **Add**.
3. Enter policy details.

**Name**
Specify name to identify Data Control List.

**Signatures**
Select one or more Content Control signature(s) to be added to the policy.

Filter the Content Control List based on **Type** or **Region**.

![Figure 104: Data Control List](image)

4. Click **Save** to create policy.

**Encryption**

This feature requires a subscription in Sophos XG Firewall. It can be configured but cannot be enforced without a valid Email Protection subscription.

**Mode Switch option**
Select the mode from the following for which you want to apply SPX Configuration and manage SPX Templates:

- MTA
- Legacy

**SPX Configuration**

**Default SPX Template**
Select the default SPX Template. SPX Templates can be created from **Device Configuration > Protect > Email > SPX Encryption**. Default Template is used if any user explicitly SPX-encrypts an Email and no template is selected in Content Scanning Rule.

User can SPX-encrypt an Email by:
- Manually setting the Email header **X-Sophos-SPX-Encrypt** to yes.
- Installing the Sophos Outlook Add-in and clicking **Encrypt** before sending the Email.

If Default SPX Template is selected as **None**, then SPX encryption is not applied on Email.

**Allow Secure Reply for**

Enter the maximum time (in days) in which recipient can securely reply to an SPX-encrypted email using the SPX Reply Portal.

**Keep Unused Password for**

Specify the expiry time in days of an unused password.

For example, if **Keep Unused Password for** is set to 30 days, then password will expire at 0 o’clock after 30 days from being generated if no SPX encrypted message was sent for a specific recipient.

Default: 30 days

**Allow Password Registration for**

Specify the time in days after which the link to Password Registration Portal expires.

Default: 10 days

**Send Error Notification To**

Specify whom to send a notification when an SPX error occurs. Select **Sender Only** to send notification to the sender or select **Nobody** if you do not want any notification to be sent. Error messages will always be listed in the SMTP log.

**SPX Portal Settings**

**Hostname**

Specify the IP Address or Domain on which Password Registration Portal is hosted.

**Allowed Network(s)**

Specify the networks from which password registration requests will be accepted.

**Port**

Enter the port on which the SPX reply portal should listen.

Default: 8094
SPX Templates

SPX (Secure PDF Exchange) encryption is a next-generation version of email encryption. It is clientless and extremely easy to set up and customize in any environment. Using SPX encryption, email messages and any attachments sent to the SF device are converted to a PDF document, which is then encrypted with a password. You can configure the SF device to allow senders to select passwords for the recipients, or the server can generate the password for the recipient and store it for that recipient, or the server can generate one-time passwords for recipients.

When SPX encryption is enabled, there are two ways how emails can be SPX encrypted:

- User can download the Sophos Outlook Add-in from SF’s User Portal. After having it installed, an Encrypt button is displayed in the Microsoft Outlook user interface. To encrypt a message, the user needs to click the Encrypt button and then write and send the message. Only if something goes wrong, for example the sender does not enter a valid password, a notification will be sent, if configured.

Note

If you do not use Outlook you can also trigger SPX encryption by setting the header field X-Sophos-SPX-Encrypt to yes.
• In the Data Protection feature, you can enforce SPX encryption for Emails containing sensitive data (see Device Configuration > Protect > Email > Email Scanning Rules).

The encrypted message is then sent to the recipient's mail box. Using any PDF reader, the recipient can decrypt the message with the password that was used to encrypt the PDF. SPX-encrypted email messages are accessible on all popular smartphone platforms that have native or third-party PDF file support, including Android, IOS, Blackberry and Windows Mobile devices.

The SPX template defines the layout of the PDF file, password settings and recipient instructions. You can also define different SPX templates. So, if you are managing various customer domains, you can assign them customized SPX templates containing for example different company logos and texts. Use this section to add, edit and delete SPX Templates for Legacy and MTA modes.

Add SPX Templates (MTA)

This feature requires a subscription in Sophos XG Firewall. It can be configured but cannot be enforced without a valid Email Protection subscription.

This feature is applicable to Sophos XG Firewall devices where MTA Mode is enabled.

This page allows you to define new SPX Templates or modify existing templates.

1. Go to Device Configuration > Protect > Email > Encryption > SPX Templates and click Add.

   Note
   Ensure that MTA Mode is selected for Encryption page. Click Turn Off Legacy Mode to switch to MTA Mode.

2. Enter parameter values for the following basic settings.

   Name
   Specify the name to uniquely identify the template.

   Description
   Specify details of the template.

   Organization Name
   Specify the organization name to be displayed on notifications concerning SPX, sent to the administrator or the email sender, depending on your settings.

   PDF Encryption
   Select the encryption standard of the PDF file.

   Page Size
   Select the page size of the PDF file.

3. Enter Password Settings.

   Password Type
   Select how you want to generate the password for accessing the encrypted email message. Depending on which type you select, the sender always has to take care of transferring the password in a safe way to the recipient, except for Specified by recipient.

   Available Options:

   Specified by Sender:
   Select if the email sender should provide the password. In this case, the sender has to enter the password into the Subject field, using the following format: [secure:<password>]<subject text> where <password> is the password to open the encrypted PDF file and <subject text> is the random subject. Of course, the password will be removed by the SF device before the email is sent to the recipient.
Generated one-time password for every email:
The SF device automatically creates a new password for each affected email. A Notification Email is sent to the Sender containing instructions and the one-time generated password.

The HTML content of this Email can be customized from Notification Subject and Notification Body. You can reset to the default content by clicking Reset button.

Generated and stored for recipient:
The SF device automatically creates a recipient-specific password when the first email is sent to a recipient. This password will be sent to the sender. With the next email, the same password is used automatically. The password will expire when it is not used for a configured time period, and it can be reset by the administrator.

The HTML content of this Sender Notification Email can be customized from Notification Subject and Notification Body. You can reset to the default content by clicking Reset button.

Specified by recipient:
Select if the email recipient should provide the password. In this case, the recipient receives a Notification Email containing link leading to the Password Registration Portal to register a password and Sender receives a failure notification. After registration, the recipient is able to view the current encrypted mail and any future encrypted mails using the same password from this or other senders from the same organization.

Note
The Recipient’s password generated via Specified by recipient method and Generated and stored for recipient are mutually exclusive. Recipient will have to use the respective password when Email is received after SPX Encryption using different methods.

4. Specify Recipient Instructions:
Instructions for Recipient
The body of the email that is sent from the SF device to the email recipient containing instructions concerning the encrypted email. Simple HTML markup and hyperlinks are allowed. You can also use variables, e.g.,

%%ORGANIZATION_NAME%%
**Figure 106: Add SPX Templates**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Organization Name</td>
<td></td>
</tr>
<tr>
<td>PDF Encryption</td>
<td>AES / 128</td>
</tr>
<tr>
<td>Page Size</td>
<td>Letter</td>
</tr>
<tr>
<td>Password Settings</td>
<td></td>
</tr>
<tr>
<td>Password Type</td>
<td>Specified by sender</td>
</tr>
<tr>
<td>Instructions for recipient</td>
<td></td>
</tr>
</tbody>
</table>

This email contains a message that has been sent as an encrypted PDF document in order to ensure the secure delivery of its contents.

To access this message, you should open the attached PDF using Adobe Acrobat Reader version 7.0 or higher. In order to view its contents, you must enter the

**SPX Portal Settings**

Enable SPX Reply Portal: Enable
Tip
The Default SPX Template on this tab contains all available variables and provides a useful example of recipient instructions. The variables used are:

- ENVELOPE_TO: The Recipient for whom password is generated.
- PASSWORD: The password to open SPX encrypted Email
- ORGANIZATION_NAME: The name provided in Organization Name field.
- SENDER: The Sender of the Email.
- REG_LINK: Link of the Registration Portal for registering the password.

5. Enable SPX Portal Settings:

Enable SPX Reply Portal
Click to enable users to securely reply to SPX-encrypted emails using the SPX Reply Portal. You can also select the option Include Original Body in Reply to include original body.

6. Click Save to save the settings.

Add SPX Templates (Legacy)
This feature requires a subscription in Sophos XG Firewall. It can be configured but cannot be enforced without a valid Email Protection subscription.

This feature is applicable to Sophos XG Firewall devices where MTA Mode is disabled.

This page allows you to define new SPX Templates or modify existing templates.

1. Go to Device Configuration > Protect > Email > Encryption and click on Switch to Legacy Mode.
2. Click Add under SPX Templates section.
3. Enter parameter values for the following basic settings.

Name
Specify the name to uniquely identify the template.

Description
Specify details of the template.

Organization Name
Specify the organization name to be displayed on notifications concerning SPX, sent to the administrator or the email sender, depending on your settings.

PDF Encryption
Select the encryption standard of the PDF file.

Page Size
Select the page size of the PDF file.

4. Enter Password Settings.

Password Type
Select how you want to generate the password for accessing the encrypted email message. Depending on which type you select, the sender always has to take care of transferring the password in a safe way to the recipient, except for Specified by recipient.

Available Options:

Specified by Sender:
Select if the email sender should provide the password. In this case, the sender has to enter the password into the Subject field, using the following format:

\[\text{secure:<password>}}\text{<subject text>}\]

where <password> is the password to open the encrypted PDF file and <subject text> is the random subject. Of course, the password will be removed by the SF device before the email is sent to the recipient.

**Generated one-time password for every email:**

The SF device automatically creates a new password for each affected email. A Notification Email is sent to the Sender containing instructions and the one-time generated password.

The HTML content of this Email can be customized from Notification Subject and Notification Body. You can reset to the default content by clicking Reset button.

**Generated and stored for recipient:**

The SF device automatically creates a recipient-specific password when the first email is sent to a recipient. This password will be sent to the sender. With the next email, the same password is used automatically. The password will expire when it is not used for a configured time period, and it can be reset by the administrator.

The HTML content of this Sender Notification Email can be customized from Notification Subject and Notification Body. You can reset to the default content by clicking Reset button.

**Specified by recipient:**

Select if the email recipient should provide the password. In this case, the recipient receives a Notification Email containing link leading to the Password Registration Portal to register a password and Sender receives a failure notification. After registration, the recipient is able to view the current encrypted mail and any future encrypted mails using the same password from this or other senders from the same organization.

**Note**

The Recipient's password generated via Specified by recipient method and Generated and stored for recipient are mutually exclusive. Recipient will have to use the respective password when Email is received after SPX Encryption using different methods.

5. Specify Recipient Instructions:

**Instructions for Recipient**

The body of the email that is sent from the SF device to the email recipient containing instructions concerning the encrypted email. Simple HTML markup and hyperlinks are allowed. You can also use variables, e.g.,

\[\%\%\text{ORGANIZATION\_NAME}\%\%\]
Tip
The Default SPX Template on this tab contains all available variables and provides a useful example of recipient instructions. The variables used are:

- ENVELOPE_TO: The Recipient for whom password is generated.
- PASSWORD: The password to open SPX encrypted Email
- ORGANIZATION_NAME: The name provided in Organization Name field.
- SENDER: The Sender of the Email.
- REG_LINK: Link of the Registration Portal for registering the password.

6. Click **Save** to save the settings.

General Settings

This feature requires a subscription in Sophos XG Firewall. It can be configured but cannot be enforced without a valid Email Protection subscription.
Email Configuration allows configuring the general settings on Email traffic. This page contains the following sections.

SMTP Deployment Mode

MTA mode is available only in Sophos XG Firewall, XG105, Cyberoam CR25iNG, Sophos UTM, SG105, and higher models.

To switch between MTA mode and legacy mode, click the button.

In MTA mode, Sophos XG Firewall acts as a mail transfer agent (MTA). In legacy mode, it acts as a transparent proxy.

As an MTA, Sophos XG Firewall routes emails of the protected email servers. You can configure inbound and outbound mail relay, create SMTP profiles to protect multiple domains on the internal email server or multiple email servers, view emails that are waiting for delivery or have generated an error, and view mail logs.

Default: MTA mode is enabled.

Note
- When you turn on MTA mode, a firewall rule is created automatically to allow SMTP/SMTPS traffic.
- If you have migrated from CyberoamOS or SFOS v15 to SFOS v16, legacy mode is enabled by default.

Outbound Banner Settings

Email Banner Mode

Select the mode of appending banner to outgoing emails.

Available options:
- Inline, no conversion: Appends banner inline.
- MIME part: Appends banner as a separate MIME part.
- Off: Does not append banner.

Note
For banner to be appended, select Scan SMTP and Scan SMTPS under Malware scanning in the applicable Business application rules.

Email Banner

Specify banner to be added to all the outgoing Emails. Only text banners are allowed.

Example:
SMTP Settings

SMTP Hostname

Specify the SMTP hostname to be used in HELO and SMTP banner strings. By default, Sophos XG Firewall uses ‘Sophos’ as hostname.

Note
For legacy mode, this hostname is applicable only to system-generated notification emails.

Don't Scan Emails Greater Than

Specify maximum file size (in KB) for scanning. Files exceeding this size received through SMTP/S will not be scanned.

Default - 0 KB
Specify 0 to increase the default file size scanning restriction to 51200 KB.

Action for Oversize Emails

Specify the action for Oversize Emails.

Available Options
Accept: All the oversize mails are forwarded to the recipient without scanning. Reject: All the oversize mails are rejected and sender is notified. Drop: All the oversized mails are dropped, without notifying the sender. Default - Accept

Bypass Spam Check for SMTP/S Authenticated Connections (available only in legacy mode)

Enable to bypass Spam Scanning for Email messages received over SMTP/S connections authenticated by the Email Server.

Verify Sender's IP Reputation

Click to verify the reputation of the sender IP Address. When enabled, Device dynamically checks the sender’s IP Address of all Emails. If the IP Address is found to be responsible for sending Spam Emails or malicious contents, Device takes action as per configured Scanning Rules.

If enabled, specify action for Confirmed Spam Emails and Probable Spam Emails.

Available Options
Accept: All the spam Emails are forwarded to the recipient after scanning as per the configuration. Reject: All the spam mails are rejected and a notification is sent to the Email sender. Drop: All the spam mails are dropped, without notifying the sender.

As it is a global option, if Spam scanning is enabled, all the mails will be first subjected to IP Reputation filtering followed by filtering based on actions configured in Spam policy.
SMTP DoS Settings
Enable to configure SMTP DoS Settings which protect the network from SMTP DoS Attacks.
If enabled, specify values for Maximum Connections, Maximum Connections/Host, Maximum Emails/Connection, Maximum Recipients/Email, Email Rate per Minute/Host and Connections Rate per Second/Host.

Maximum Connections (available if SMTP DoS settings enabled)
Specify maximum number of connections that can be established with the Email Server.
Default - 1024
Range - 1 - 20000

Maximum Connections/Host (available if SMTP DoS settings enabled)
Specify maximum number of connections allowed to the Email Server from a particular host.
Default - 64
Range - 1 - 10000

Maximum Emails/Connection (available if SMTP DoS settings enabled)
Specify maximum number of Emails that can be sent in a single Connection.
Default - 512
Range - 1 - 1000

Maximum Recipients/Email (available if SMTP DoS settings enabled)
Specify maximum number of Recipients for a single Email.
Default - 100
Range - 1 - 256

Email Rate per Minute/Host (available if SMTP DoS settings enabled)
Specify number of Emails to be sent from a particular host in one Minute.
Default - 512
Range - 1 - 20000

Connection Rate per Second/Host (available if SMTP DoS settings enabled)
Specify number of Connections allowed to the Email Server from a particular host in one Second.
Default - 8
Range - 1 - 20000
figure 110: smtp/s settings

pop/s and imap/s settings

don't scan emails greater than
specify maximum file size (in KB) for scanning. Files exceeding this size received through pop/imap will not be scanned.

default - 1024 KB
specify 0 to increase the default file size restriction to 10240 KB.

recipient headers
specify header value to detect recipient for pop3/imap.

default - delivered-to, received, x-rcpt-to

figure 111: pop/s and imap/s settings
**SMTP TLS Configuration**

**TLS Certificate**
Select the CA for scanning SMTP traffic over SSL from the available options.

**Available Options**
DefaultApplianceCertificateSecurityAppliance_SSL_CAList of custom CAs if added.
You can create the custom CA from Device Configuration > Configure > VPN > Certificate Authority and custom Server certificate from Certificates > Certificates.

**Allow Invalid Certificate**
If enabled, SMTP over SSL connections will be allowed with invalid certificate from the Email Server. Disable to reject such connections.
Default - Enable

**Disable legacy TLS protocols**
If enabled, protocols earlier than TLS 1.1 will be disabled. To overcome TLS vulnerabilities, we recommend that you disable legacy TLS protocols.
Default: Disable

**Require TLS Negotiation**
Select the remote host (mail server) or network from available options on whose connections TLS encryption is to be enforced. In other words, the device will always initiate TLS-secured connections when emails are to be sent or received. If TLS is enforced but connection cannot be established, then emails to/from that remote host/network are discarded.

**Require Sender Email Domain**
Specify the sender domain on whose email connections TLS encryption is to be enforced.
Sender domain is the domain of the email sender. Emails from the specified sender domain will be received over TLS-encrypted connections only. If TLS is enforced but the connection cannot be established, then emails from that sender domain are discarded.

**Skip TLS Negotiation Hosts/Nets**
Select the remote host (Email Server) or network from available options on whose connections TLS encryption is to be skipped or bypassed. When configured, SMTP connections to selected hosts will be established in clear text and unencrypted.

Figure 112: SMTP TLS Configuration
POP and IMAP TLS Configuration

**TLS Certificate**
Select the CA for scanning POP and IMAP traffic over SSL from the available options.

**Available Options**
- DefaultSecurityAppliance_SSL_CA
- List of custom CAs if added Default - Default

**Allow Invalid Certificate**
If enabled, POP and IMAP over SSL connections will be allowed with invalid certificate from the Mail Server. Disable to reject such connections.
- Default - Enable

**Apply**
Click to save the configuration.

Figure 113: POP and IMAP TLS Configuration

**Email Journaling (available only in legacy mode)**

Email being one of the most important communication and business tool in use by organizations, Email Journaling has become an integral part of every organization. An email journal is a repository to preserve Emails for compliance and operational purposes.

Using Device Email Journal, the administrator can archive all Emails, Emails of a specific recipient or a group of recipients coming into the organization and thereby keep a close watch over data leakage.

The Device can archive all Emails intended for a single or multiple recipients and can forward to the single administrator or multiple administrators.

This section displays list of journals created and provides option to add a new journal, update the parameters of existing journal, or delete the journal. You can filter the list based on recipient name.

**Allowed and blocked senders (available only in MTA mode)**

You can specify IP addresses, FQDNs, and email addresses to receive emails over SMTP/S connections to bypass RDNS, greylisting, IP reputation, recipient verification, as well as scanning for inbound-outbound spam, DLP, and RBL.

**Blocked email addresses**
To block email addresses, add them here. The device blocks email addresses that belong to both allowed and blocked lists.
Malware Protection

Sophos Firewall OS offers Dual Anti-Virus Scanning, wherein traffic is scanned by Two (2) Anti-Virus Engines. Traffic is first scanned by the Primary Engine, and then the Secondary Engine. You can configure managed SF device(s) for Malware Protection using the following settings:

Note
Dual Anti-Virus is not available in SF device Models SF100 and SF200. For them, ONLY Single Anti-Virus CYREN is available.

Note
You can also view and manage these settings from Device Configuration > Configure > System Services > Malware Protection.

Note
You can manage the Anti-Virus service from Device Configuration > Monitor and Analyze > Diagnostics > Services.

Primary Anti-Virus Engine
Select the Primary Anti-Virus Engine to be used for traffic scanning. For Dual Scan, packets are first scanned by the Primary Engine and then by the Secondary Engine. For Single Scan, only the Primary Engine is used.

Available Options
- Sophos Engine
- Avira Engine

Apply
Click to save the configuration.

Smarthost Settings

A smarthost is a Mail Transfer Agent (MTA) which acts as an intermediate server between the sender’s and recipient's mail servers. On configuring a smarthost, the device redirects outbound emails to the designated server, which are then routed to the recipient's mail server.

You can enable Use Smarthost from Device Configuration > Protect > Email > General Settings.

Hostname
Select the host that will act as a smarthost.
You cannot configure Smarthost as the device's interface IP address. It will result in a routing loop.

**Port**

Enter the port number.

Default: 25

**Authenticate Device with Smarthost**

Select if the smarthost requires the device to authenticate before routing emails. Both plain and login authentication types are supported. Enter a **Username** and password.

---

**Advanced SMTP Settings (available only in MTA mode)**

**Reject invalid HELO or missing RDNS**

Select this option if you want to reject hosts that send invalid HELO/EHLO arguments or lack RDNS entries. Select **Do strict RDNS checks** if you want to additionally reject email from hosts with invalid RDNS records. An RDNS record is invalid if the found hostname does not resolve back to the original IP address.

**Scan Outgoing Mails**

Enable to scan all outgoing email traffic. Email is quarantined if found to be malware infected, or marked as Spam.

**Apply**

Click to save the configuration.
Add an email journal

Email journal is available only in legacy mode, in which the firewall acts as a transparent proxy.

This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.

Add email journal allows you to forward copies of emails of specific recipients to a different email address. For example, you can specify an administrator as the recipient.

1. Go to Email > General settings and click Add under Email journaling.
2. Enter a name.
3. For Recipient, select Any to journal all incoming emails. Alternatively, select the address groups, copies of whose emails are to be forwarded to a different email address.
4. For Send copy of email to, enter the email address to which a copy of the emails is to be forwarded.

Note
You can send copies of emails only for SMTP/S protocol.

5. Click Save.

Relay settings

Relay settings appears only when MTA (Mail Transfer Agent) mode is enabled. MTA mode is available only in Sophos Firewall XG105, Cyberoam CR25iNG, Sophos UTM SG105, and higher models.

This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.

Sophos XG Firewall can be configured to act as an email relay which allows specific hosts to relay (i.e. send) emails through it to specified domains.

Host based relay

Allow relay from hosts/networks

Select the hosts/networks which can use Sophos XG Firewall as an email relay. You can use the Create new link to create a new host. Click Apply to save the configuration.
Note
It is extremely important not to select Any in allowed hosts/networks, because this would result in an open relay, allowing anyone on the internet to send messages through Sophos XG Firewall. Spammers will quickly recognize this, leading to massive email traffic. In the worst case, you will be listed on third-party spammer blacklists. In most configurations, the only hosts that should be allowed to relay emails are the mail servers in your network.

Note
The firewall will scan and reject IP addresses that you’ve allowed for host-based relay if they fail the scan.

**Blocked relay from hosts/networks**
Specify the hosts/networks that should be blocked by device. You can use the Create new link to create a new host. Click Apply to save the configuration.

**Upstream host**

**Allow relay from hosts/networks**
Specify the upstream hosts/networks from whom you are to allow inbound emails, typically your ISP or external MX. You can use Create new link to create a new host.

**Block relay from hosts/networks**
Specify the hosts/networks whose inbound emails should be blocked by device. You can use the Create new link to create a new host.

Note
The “Allow” list for both host-based relay and upstream host is given higher priority than the “Block” list. For example, if a host/network appears both in the allow list and the block list, Sophos XG Firewall will allow relay from that host/network.

**Authenticated relay settings**

**Enable authenticated relay**
Enable to allow the authenticated users or groups selected below to use device as an email relay.

**Users or groups**
Select the users or groups to be allowed to use device as an email relay. You can use the Create new link to create a new user or group.
Address Group

Email Policies are applied on Email Addresses. To make configuration easier and simpler, Administrator can group the addresses that require the same scanning policy. The policy applied to the address group is applicable to all the group members. Hence when group is used in number of rules, it becomes much easier to add or remove addresses from the group rather than updating individual rules. Hence, just with the one update, Administrator can re-align the rules.

Address Group is grouping of:

- Email Address or Domain
- IP Address
- RBL (Real-time Blackhole List) (applicable only for the Spam mails)

An address can be a member of multiple groups.

RBL is a list of IP Addresses whose owners are responsible for Spam or are hijacked for Spam Relay. These IP Addresses might also be used for spreading virus. The Device checks each RBL for the connecting IP Address and action configured in the policy is taken if IP Address is found in any of the RBL list. Administrator can directly use the two default RBL groups shipped with the Device or update them as per the requirement:

- Premium RBL Services
- Standard RBL Services

The Address Group page displays list of all the default and custom groups and provides option to add a new group, update the parameters, import addresses in the existing group, or delete the group. You can sort the list based on address group name.

Use this page to add, edit and delete Address Groups for Legacy and MTA modes. Use the Mode Switch option on the page to switch between Legacy and MTA modes.

Add Address Group (MTA)

This feature is applicable to SF devices where MTA Mode is enabled.

This page allows you to add a new Email Address Group, or edit existing groups.

1. Go to Device Configuration > Protect > Email > Address Group and click Add.

   Note
   Ensure that MTA Mode is selected for Address Group page. Click Turn Off Legacy Mode to switch to MTA Mode.

2. Specify the parameter values of the following Address Group Settings.

   **Name**
   Enter a name to identify the Group. A group name must be unique.

   **Description**
   Provide the description for the address group.

   **Group Type**
   Select type of addresses you want to group from the available options.

   **Available Options:**
   RBL (IPv4) and RBL(IPv6):
RBL is a list of IPv4 and IPv6 Addresses, respectively, whose owners refuse to stop the proliferation of spam, i.e. are responsible for spam or are hijacked for spam relay. The Device will check each RBL for the connecting IP Address. If the IP Address matches to the one on the list then the specified action in policy is taken. Specify Domain Name to be added as RBL to the Address Group.

**Email Address / Domain:**

Import or manually specify Email Address or Domain Name to be added to the Address Group.

- **Import** – Select to browse and import a CSV file or a text file to add the Email Address/Domain to address group.
- **Manual** – Select to manually add the Email Address/Domain to address group.

![Figure 116: Address Group](image)

3. Click **Save** to create Address Group.

**Add Address Group (Legacy)**

*This feature is applicable to SF devices where MTA Mode is disabled.*

This page allows you to add a new Email Address Group, or edit existing groups.

1. Go to **Device Configuration > Protect > Email > Address Group** and click on **Switch to Legacy Mode**.
2. Click **Add**.
3. Specify the parameter values of the following Address Group Settings.

**Name**

Enter a name to identify the Group. A group name must be unique.

**Description**

Provide the description for the address group.

**Group Type**

Select type of addresses you want to group from the available options.

**Available Options:**

- **RBL (IPv4) and RBL(IPv6):**
RBL is a list of IPv4 and IPv6 Addresses, respectively, whose owners refuse to stop the proliferation of spam, i.e. are responsible for spam or are hijacked for spam relay. The Device will check each RBL for the connecting IP Address. If the IP Address matches to the one on the list then the specified action in policy is taken. Specify Domain Name to be added as RBL to the Address Group.

**Email Address / Domain:**

Import or manually specify Email Address or Domain Name to be added to the Address Group.

Import – Select to browse and import a CSV file or a text file to add the Email Address/Domain to address group.

Manual – Select to manually add the Email Address/Domain to address group.

![Address Group](image)

Figure 117: Address Group

4. Click **Save** to create Address Group.

**Quarantine digest**

**Quarantine digest is available only in Sophos Firewall XG105, Cyberoam CR25iNG, Sophos UTM SG105, and higher models.**

This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.

The quarantine digest is an email containing a list of quarantined emails filtered by the device and held in the user quarantine area. If it is configured, the user receives a quarantine digest as per the frequency defined on this page. The digest also provides a link to the user portal from where the user can access quarantined emails and take the required action.

The quarantine digest settings can be configured globally for all the users or for individual users. The user receives the quarantine digest as per the configured frequency.

The quarantine digest provides the following information for each quarantined message:

- Date and time: Date and time when the message was received
- Sender: Email address of the sender
- Recipient: Email address of the receiver
- Subject: Subject of the message

**Note**
Quarantine digest is not applicable to Wi-Fi devices.

## Configuring the quarantine digest for all users

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable quarantine digest</strong></td>
<td>Enable the quarantine digest to configure the digest service for all the users.</td>
</tr>
<tr>
<td><strong>Email frequency</strong></td>
<td>Specify the mailing frequency for digest.</td>
</tr>
<tr>
<td></td>
<td>Digests can be mailed every hour, every day at configured time, or every week on the configured day and time.</td>
</tr>
<tr>
<td><strong>From email address</strong></td>
<td>Specify the email address from which the email should be sent.</td>
</tr>
<tr>
<td><strong>Display name</strong></td>
<td>Specify the email sender name. Digest email will be sent with this name.</td>
</tr>
<tr>
<td><strong>Send test email</strong></td>
<td>Click this and provide an email address to which the message is to be sent for email address verification.</td>
</tr>
<tr>
<td><strong>Reference user portal IP</strong></td>
<td>Select Interface/Port IP from the Reference user portal IP drop-down list.</td>
</tr>
<tr>
<td></td>
<td>The user portal link in the digest mail will point to this IP address. The user can click the link to access his quarantined messages and take the required action. Users who do not come under the specified interface will have to access the quarantine email directly from their account.</td>
</tr>
<tr>
<td><strong>Skip quarantine reports</strong></td>
<td>Click Add and enter the email address whose quarantined emails you want to exclude from the quarantine digest. For example, you can add the alias email address “<a href="mailto:sales@organization.com">sales@organization.com</a>” to exclude its quarantined emails from the quarantine digest sent to users who are part of the alias.</td>
</tr>
<tr>
<td><strong>Change user’s quarantine digest settings</strong></td>
<td>Click to change the digest settings of the individual users.</td>
</tr>
<tr>
<td></td>
<td>This allows you to select the group and update the quarantine digest setting of group members.</td>
</tr>
</tbody>
</table>
Overriding quarantine digest settings for a specific user(s)

Click **Change user's quarantine digest settings** to change the digest settings for individual users. This opens a new pop-up window named **Manage quarantine digest**, which allows you to search groups and users.

You can individually search for user and user groups.

Select the checkbox against a user to enable the quarantine digest. If it is enabled, the configured quarantine digest settings are applicable for the user.

**File types**

A file type is a classification that is determined by file extension or MIME type. You can include file types in web policies to control access to files. The default types contain some common criteria and you can create additional types.

- To edit a file type, click **Add a file type**.

**Add a file type**

1. Go to **Web > File types** and click **Add**.
2. Type a name.
3. Optional: Select a template.
   - Templates organize commonly used file extensions and MIME headers by category, for example, video files. You can use templates instead of typing extensions and MIME headers.
4. Specify file extensions and MIME headers.

   **Note**

   Do not type a dot (.) before file extensions.

5. Click **Save**.

**3.4.7 Web server**

You can protect web servers against Layer 7 (application) vulnerability exploits. These attacks include cookie, URL, and form manipulation. Use these settings to define web servers, protection policies, and authentication policies for use in Web Application Firewall (WAF) rules. General settings allow you to protect web servers against slow HTTP attacks.

- To manage the WAF service, go to **System services > Services**.

**Web servers**

Define the servers to be protected. Web servers specify a host, a type, and other connection settings. You can protect plain text (HTTP) and encrypted (HTTPS) servers.

**Add a Web Server**

This page describes how to add a web server.

1. Go to **Device Configuration > Protect > Web Server > Web Servers** and click **Add**.
2. Make the following settings:
Name

Enter a descriptive name for the web server.

Description

Enter a description or other information.

Host

Add or select a host, which can either be of the type Host or DNS Host.

Note

DNS Host is recommended here because hosts listed with their IP address transmit empty host headers which leads to problems with some browsers.

Type

Select a real web server type. Whether you want the communication between Sophos Firewall OS and the real server to be encrypted (HTTPS) or plaintext (HTTP).

- Encrypted (HTTPS): Browser-based access to real web server via HTTPS.
- Plaintext (HTTP): Browser-based access to real web server via HTTP. Default.

Port

Enter a port number for the real web server. By default the standard port of the selected real server type is selected.

Keep alive

Enable Keep alive to keep the connection between Sophos XG Firewall and the real server open instead of opening a new connection for every single request.

Note

In rare cases where the real web server does not support keep alive properly, this feature can provoke reading errors or timeouts and should then be disabled for the affected real server.

Timeout

Enter a timeout for the Keep alive option. Values between 1 and 65535 seconds are allowed. Default is 300 seconds.
3. Click **Save** to save your settings.

The server is created and appears in the web servers list.

**Protection policies**

Using policies, you can define protection against vulnerability exploits such as cookie, URL, and form manipulation. Policies also mitigate common threats such as protocol violations and cross-site scripting (XSS) attacks. The firewall provides default policies for use with some common web services.

**Protection Settings**

**Cookie signing**

Using cookie signing, you can mitigate attempts to obtain private session data and engage in fraudulent activity by tampering with cookies. When the web server sets a cookie, a second cookie is added to the first cookie containing a hash built from the name and value of the primary cookie and a secret that is known only by the firewall. If a request cannot provide a correct cookie pair, the cookie will be dropped.

**Static URL hardening**

Static URL hardening prevents users from manually constructing “deep links” that lead to unauthorized access. When a client requests a website, all static URLs of the website are signed using a procedure similar to cookie signing. Also, the response from the web server is analyzed regarding what links can be validly requested next.
Form hardening
To prevent SQL injection and other exploits, form hardening saves the original structure of a web form and signs it. If the structure of a form has changed when it is submitted, the firewall rejects the request.

Anti-virus
Protect a web server against viruses.

Block clients with bad reputation
Block clients that have a bad reputation according to real-time blackhole lists (RBLs) and GeoIP information. For RBLs, the firewall uses Cyren IP reputation intelligence and SORBS. For GeoIP, the firewall uses Maxmind. The firewall blocks clients that belong to the A1 (anonymous proxies or VPN services) and A2 (satellite ISP) classifications.

Common Threat Protection

Protocol violations
Enforce adherence to the RFC standard specification of the HTTP/S protocol. Violating these standards usually indicates malicious intent.

Protocol anomalies
Search for common usage patterns. Lack of such patterns often indicates malicious requests. These patterns include, among other things, HTTP headers such as “Host” and “User-Agent”.

Request limits
Enforce reasonable limits on the number and ranges of request arguments. Overloading request arguments is a typical attack vector.

HTTP policy
Narrow the allowed usage of the HTTP protocol. Web browsers typically use only a limited subset of all possible HTTP options. Disallowing the rarely-used options protects against attackers aiming at these options.

Bad robots
Check for usage patterns characteristic of bots and crawlers. By denying them access, possible vulnerabilities on your web servers are less likely to be discovered.

Generic attacks
Search for attempted command executions common to most attacks. After having breached a web server, an attacker usually tries to execute commands on the server like expanding privileges or manipulating data stores. By searching for these post-breach execution attempts, attacks can be detected that might otherwise have gone unnoticed, for example because they targeted a vulnerable service by the means of legitimate access.

SQL injection attacks
Check for embedded SQL commands and escape characters in request arguments. Most attacks on web servers target input fields that can be
used to direct embedded SQL commands to the database.

**XSS attacks**
Check for embedded script tags and code in request arguments. Typical cross-site scripting attacks aim at injecting script code into input fields on a target web server, often in a legitimate way.

**Tight security**
Perform tight security checks on requests, such as checking for prohibited path traversal attempts.

**Trojans**
Check for usage patterns that are characteristic of trojans.

*Note*
This setting does not prevent the installation of trojans. Trojan protection is provided by anti-virus scanning.

**Outbound**
Prevent web servers from leaking information to the client. This includes, among other things, error messages sent by servers which attackers can use to gather sensitive information or detect specific vulnerabilities.

**Add Application Protection Policy**
This page describes how to add an application protection policy.

1. Go to *Device Configuration > Protect > Web Server > Protection Policies* and click *Add*.
2. Specify the following:

**Name**
Specify a unique name for the protection policy.

**Description**
Specify a description for the policy.

**Pass Outlook Anywhere**
Enable this to allow external Microsoft Outlook clients to access the Microsoft Exchange Server via the Web Application Protection. Microsoft Outlook traffic will not be checked or protected by the Web Application Protection.

**Mode**
Select a mode from the drop-down list:
- **Monitor**: HTTP requests are monitored and logged.
- **Reject**: HTTP requests are rejected.

**Cookie Signing**
Enable this to protect a web server against manipulated cookies. When the web server sets a cookie, a second cookie is added to the first cookie containing a hash built of the primary cookie's name, its value and a secret, where the secret is only known by the Web Application Protection. Thus, if a request cannot provide a correct cookie pair, there has been some sort of manipulation and the cookie will be dropped.

**Static URL Hardening**
Enable this to protect against URL rewriting. For that, when a client requests a website, all static URLs of the website are signed. The signing uses a similar procedure as with cookie signing. Additionally the response from the web server is analyzed.
regarding what links can be validly requested next. Moreover, static hardened URLs can furthermore be bookmarked and visited later.

Note
Static URL hardening affects all files with a HTTP content type of text/* or *xml*, where * is a wildcard. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the URL hardening feature. It does not work for dynamic URLs created by client, for example: JavaScript.

Note
You can find more information about Static URL Hardening and Form Hardening under: Additional Information on Static URL Hardening and Form Hardening (page 176)

Entry URLs (only applicable if Static URL Hardening is enabled)
Specify a URL for static URL hardening:

Form Hardening
Enable this to protect against web form rewriting. Form hardening saves the original structure of a web form and signs it. Therefore, if the structure of a form has changed when it is submitted the Web Application Protection rejects the request.

Note
Form hardening affects all files with a HTTP content type of text/* or *xml*, where * is a wildcard. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the form hardening feature.

Note
You can find more information about static URL hardening and form hardening under: Additional Information on Static URL Hardening and Form Hardening (page 176)

Anti-Virus
Enable this to protect a web server against viruses.

Mode
Select a mode from the available options.
• Avira
• Sophos
• Dual Scan

Direction
Select from the drop-down list whether to scan only uploads or downloads or both.
• Uploads
• Downloads
• Uploads and Downloads

Block unscannable content
Enable this to block files that cannot be scanned. The reason for that may be, among other things, that files are encrypted or corrupt.

**Limit scan size**

Enable this to enter the scan size limit into an additional field. Provide the limitation in megabytes.

**Note**

Please note that the scan size limit refers to the entire upload volume, not to a single file. If, for example, you limit the scan size to 50 MB and make an upload containing multiple files (45 MB, 5 MB and 10 MB), the last file will not be scanned. Thus a virus being in the last file would not be detected due to the limitation.

**Note**

If you do not specify a limitation value at all, the limit scan size will be saved with '0' megabytes, which means the limitation is not active and every uploaded/downloaded file will be scanned.

**Block clients with bad reputation**

Enable this to block clients which have a bad reputation according to their classification, based on GeoIPClosed and RBLClosed information. Sophos uses the following classification providers: RBL sources:

- Commtouch IP Reputation (ctipd.org)
- http.dnsbl.sorbs.net

The GeoIP source is Maxmind. The WAF blocks clients that belong to one of the following Maxmind categories:

- A1: Anonymous proxies or VPN services used by clients to hide their IP address or their original geographical location.
- A2: Satellite providers are ISPs that use satellites to provide Internet access to users all over the world, often from high risk countries.

**Skip remote lookups for clients with bad reputation (only applicable if Block clients with bad reputation is enabled)**

Enable to use GeoIP-based classification which uses cached information only and is therefore much faster. As reputation lookups include sending requests to remote classification providers, using reputation-based blocking may slow down your system.

**Common Threat Filter**

Enable this to protect your web servers from several threats. You can specify the threat filter categories you want to use in the Threat Filter Categories section below. All requests will be checked against the rule sets of the selected categories. Depending on the results, a notice or a warning will be shown in the live log or the request will be blocked directly.

**Rigid Filtering**

Enable this to tighten several of the selected rules. This may lead to false positives.

**Skip Filter Rules**

Some of the selected threat categories may contain rules that lead to false positives. To avoid false positives induced by a specific rule, add the rule number that you want to skip in this field.

**Protocol Violations**
Enforces adherence to the RFC standard specification of the HTTP protocol. Violating these standards usually indicates malicious intent.

**Protocol Anomalies**

Searches for common usage patterns. Lack of such patterns often indicates malicious requests. These patterns include, among other things, HTTP headers like 'Host' and 'User-Agent'.

**Request Limits**

Enforces reasonable limits on the amount and ranges of request arguments. Overloading request arguments is a typical attack vector.

**HTTP Policy**

Narrows down the allowed usage of the HTTP protocol. Web browsers typically use only a limited subset of all possible HTTP options. Disallowing the rarely-used options protects against attackers aiming at these often less well-supported options.

**Bad Robots**

Checks for usage patterns characteristic of bots and crawlers. By denying them access, possible vulnerabilities on your web servers are less likely to be discovered.

**Generic Attacks**

Searches for attempted command executions common to most attacks. After having breached a webserver, an attacker usually tries to execute commands on the server like expanding privileges or manipulating data stores. By searching for these post-breach execution attempts, attacks can be detected that might otherwise have gone unnoticed, for example because they targeted a vulnerable service by the means of legitimate access.

**SQL Injection Attacks**

Checks for embedded SQL commands and escape characters in request arguments. Most attacks on web servers target input fields that can be used to direct embedded SQL commands to the database.

**XSS Attacks**

Checks for embedded script tags and code in request arguments. Typical cross-site scripting attacks aim at injecting script code into input fields on a target web server, often in a legitimate way.

**Tight Security**

Performs tight security checks on requests, like checking for prohibited path traversal attempts.

**Trojans**

Checks for usage patterns characteristic of trojans, thus searching for requests indicating trojan activity. It does not, however, prevent the installation of such trojans as this is covered by the antivirus scanners.

**Outbound**
Prevents web servers from leaking information to the client. This includes, among other things, error messages sent by servers which attackers can use to gather sensitive information or detect specific vulnerabilities.

### Figure 119: Add Application Protection

| Name * |  
| Description |
| Pass Outlook Anywhere | ON |
| Mode * | Please select |
| Cookie Signing | ON |
| Static URL Hardening | OFF |
| Form Hardening | ON |
| Anti-virus | ON |
| Mode | Avira |
| Direction | Uploads |
| Block unscannable content | ON |
| Limit scan size | ON |
| Megabytes * |  
| Block clients with bad reputation | OFF |
| Common Threat Filter | OFF |

3. Click **Save**.

### Additional Information on Static URL Hardening and Form Hardening

It would be best practice to always enable both URL hardening and form hardening because those two functions are complementary, especially in the way that they prevent issues you may have when enabling just one of them:

- **Only form hardening is activated:** When a webpage contains hyperlinks with appended queries (which is the case with certain CMSs), e.g. http://example.com/?view=article&id=1, such page requests are blocked by form hardening because it expects a signature, which is missing.
• Only URL hardening is activated: When a web browser appends form data to the action URL of the form tag of a web form (which is the case with GET requests), the form data becomes part of the request URL sent to the webserver, by that rendering the URL signature invalid.

The reason why activating both functions solves those issues is that in case either form hardening or URL hardening find that a request is valid, the WAF accepts the request.

Related tasks
Add Application Protection Policy (page 172)
This page describes how to add an application protection policy.

Authentication policies

Using authentication policies, you can provide basic or form-based reverse-proxy authentication for your web servers. You can also use them to control access to the paths specified in firewall rules. The firewall supports basic HTTP authentication as described in RFC 7617. Authentication policies specify an authentication method and users.

Add an authentication policy

1. Go to Web server > Authentication policies and click Add.
2. Type a name.
3. Choose a client authentication mode.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>Users authenticate with HTTP basic authentication, that is, by typing their user name and password. No session cookies will be generated and a dedicated sign-out is not possible.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> As the credentials are sent unencrypted, use this mode with HTTPS.</td>
</tr>
<tr>
<td>Form</td>
<td>Users type their credentials in a form. Session cookies will be generated and a dedicated sign-out is possible.</td>
</tr>
</tbody>
</table>

4. Specify additional client authentication settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic prompt</td>
<td>For basic authentication, the string that provides instructions to users, for example, “Please enter your credentials”.</td>
</tr>
<tr>
<td>Authentication template</td>
<td>For form-based authentication, the form that will be presented to users.</td>
</tr>
<tr>
<td>Users or groups</td>
<td>Users or user groups that should be assigned to this profile.</td>
</tr>
</tbody>
</table>

5. Specify an authentication forwarding mode.

The mode must match the web server’s authentication settings.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>Authentication works with HTTP basic authentication, providing user name and password.</td>
</tr>
<tr>
<td>None</td>
<td>No authentication between the firewall and the web servers.</td>
</tr>
</tbody>
</table>

**Note**
Even if your web servers do not support authentication, users will be authenticated through the frontend mode.

6. Specify additional authentication forwarding settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username affix</td>
<td>For basic authentication, type of affix to be added automatically to the user name. Affixes are useful when working with domains and email addresses.</td>
</tr>
</tbody>
</table>

**Note**
Prefix and suffix will be added if users enter a user name only.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove basic header</td>
<td>For no authentication, do not send the basic header from the firewall to the web server.</td>
</tr>
</tbody>
</table>

7. Optional: For form-based authentication, specify user session settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session timeout</td>
<td>If no activity is detected within the specified interval, force the user to log on again.</td>
</tr>
<tr>
<td>Session lifetime</td>
<td>Limit the time users may remain logged on to the specified interval, regardless of the activity.</td>
</tr>
</tbody>
</table>

8. Click **Save**.

**Authentication templates**

Authentication templates define HTML forms for use in form-based authentication policies.

**Add an authentication template**

1. Go to **Web server > Authentication templates** and click **Add**.
2. Type a name.
3. Choose an HTML template.
4. Optional: Choose one or more images, stylesheets, or JavaScript files that are used by the selected template.
5. Click **Upload**.
6. Click **Save**.
**General Settings**

You can activate SlowHTTP protection and define the TLS version.

The **SlowHTTP Protection** page helps to protect against Slow HTTP attacks by setting a timeout for request headers.

1. Go to **Device Configuration > Protect > Web Server > General Settings**.
2. Specify the details for SlowHTTP Protection:

**Timeout for request headers**

- **Enable** to activate SlowHTTP Protection.

**Soft limit**

Enter the minimum amount of time in second(s) to receive a request header.

Default value: 10.

**Hard limit**

Enter the maximum amount of time in second(s) to receive a request header.

Default value: 30.

**Extension rate**

Enter the amount of data volume in byte(s) which extends the timeout.

With the extension rate, you can increase the minimal timeout according to the data volume. For example, the soft limit allows at least 10 seconds to receive request headers, the extension rate is 500, and the hard limit is set to 30. If the client now sends data, the soft limit timeout increases 1 second for every 500 bytes received. After 30 seconds the client will be disconnected.

Default value: 5000.

**Skipped Networks/Hosts**

Select or add networks/hosts that should not be affected by SlowHTTP Protection.

3. Click **Apply**.

**TLS Version Settings**

1. Select the minimal TLS version that is allowed to connect to the WAF.

   - If you select TLS version 1.2, clients using Microsoft Internet Explorer 6, 7, or 8, or Microsoft Windows XP will not be able to connect to the WAF.

2. Click **Apply**.
3.4.8 Advanced Threat

Advanced threat protection

Advanced threat protection analyzes incoming and outgoing network traffic (for example, DNS requests, HTTP requests, and IP packets) for threats. Using ATP, you can quickly detect compromised clients in your network and raise an alert or drop the traffic from those clients.

- To turn on advanced threat protection, click the on/off switch.
- To specify an action when ATP detects a threat, select Log only to log the data packet or Log and drop to log and drop the packet. (By default, logging is enabled for ATP events.)
- To specify known hosts that you want to be ignored by ATP, click Add new item and select hosts.
- To add destination IP addresses or domain names that you want to skip from being scanned for threats by ATP, type an address and click the Add button.

CAUTION
By excluding sources or destinations you may expose your network to severe risks.

Security Heartbeat

Heartbeat connects cryptographically secure endpoint and Sophos Firewall OS via Sophos Cloud. This allows to exchange information between endpoint devices and Sophos Firewall OS. These information give a comprehensive overview of the network security. The administrator is able to define policies for network access based on the health status of the endpoint.

Endpoint devices and users need to authenticate via Sophos Cloud to connect to Sophos Firewall OS. The authentication works via a client which is available on Sophos Cloud and must be installed on the endpoint device. After the installation the endpoint uses the Sophos Endpoint Security and Control which is an integrated suite of security software, for example, antivirus, behavior monitoring and live protection. Sophos Endpoint Security and Control ensures that the endpoint device belongs to the system and has the permission to access the network.

Note
For more information and documentation about Sophos Endpoint Security and Control visit the Sophos Website.

The endpoint sends a heartbeat signal in regular intervals to the Sophos Firewall OS to show that it is alive. Furthermore the endpoint also informs the Sophos Firewall OS about potential threats. If Sophos Endpoint Security and Control detects any threats, the endpoint sends this information to Sophos Firewall OS which declares the endpoints health status. According to the user policy, which defines the permission of the different colors, the endpoint is not able to connect to networks, zones or services.
You can enable Security Heartbeat and set the Minimum Heartbeat Permitted in the User Application Policy which is managed on the Firewall page in the Security Heartbeat section.

Please find a description of the endpoints health status colors on the Health Status page.

To use security heartbeat you need to register with your Sophos Cloud account. If you do not have an account you can create a new one. You can find more information about Sophos Cloud under: https://secure2.sophos.com/en-us/products/cloud.aspx.

Synchronized Security
The Synchronized Security menu allows you to configure Security Heartbeat to share health information and the Enhanced Application Control.

This page describes how to login with your Sophos Cloud account and enable Security Heartbeat.

1. Go to Device Configuration > Protect > Synchronized Security.
2. Enter Sophos Cloud login details in the Registration section.

Email Address
Enter the email address of your Sophos Cloud account.

Password
Enter the password of your Sophos Cloud account.

Figure 120: Registration
3. Click Register to register your Sophos Cloud account to the Sophos Firewall OS.

Figure 121: Security HeartBeat
Missing heartbeats will be detected only in these zones.

Note
If a zone is blocked by a policy but no zone is added here, the Security Heartbeat widget in the Control Center shows “Missing”.

5. Enable Enhanced Application Control and click Apply.
Sophos Firewall Manager

Figure 122: Enhanced Application Control

The devices for which the Security Heartbeat is enabled are listed in Devices enabled for Security Heartbeat.

To clear your registration from Sophos Firewall OS, click Clear Registration.

Sandstorm settings

Use these settings to specify a data center and to exclude files from Sandstorm analysis.

**Sandstorm data center location**

Files to be analyzed are transmitted to a Sandstorm data center in the cloud over a secure SSL connection. By default, the firewall selects the closest data center. However, you can override this behavior by selecting a data center.

**CAUTION**

Changing the data center may cause the loss of analyses in progress.

**Exclude file types**

Exclude the selected types of email attachments and web downloads from Sandstorm analysis. (The file type is determined by file extension and MIME header.)

**Note**

Archives that include files of the selected types will also be excluded, regardless of what other types of files they contain.

**Note**

Although you can exclude any file type, many types that are considered safe (for example, images) are never sent for analysis. Only risky file types that Sandstorm can detonate and analyze will be sent.

3.5 Configure

3.5.1 VPN

**VPN** section allows you to configure required IPSec, L2TP, PPTP VPN connections.

A Virtual Private Network (VPN) is a tunnel that carries private network traffic from one endpoint system to another over a public network such as the Internet without the traffic, being aware that
there are intermediate hops between the endpoints or the intermediate hops being aware they are carrying the network packets that are traversing the tunnel. The tunnel may optionally compress and/or encrypt the data, providing enhanced performance and some measure of security. VPN allows you to pretend you are using a leased line or a direct telephone call to communicate between the endpoints. VPNs allow users and telecommuters to connect to their corporate intranets or extranets. VPNs are cost-effective because users can connect to the Internet locally and tunnel back to connect to corporate resources. This not only reduces overhead costs associated with traditional remote access methods, but also improves flexibility and scalability. For all business people traveling or working from home, connecting securely to the corporate network is essential. With the Device, setting up a VPN is almost effortless.

The two endpoints in Device VPN are referred to as:

- **Local** - First endpoint is the local machine itself.
- **Remote** - Second endpoint is the remote peer - the machine you are trying to establish a VPN connection to, or the machine which is trying to establish a VPN connection with you.

Device VPN automatically encrypts the data and sends it to the remote site over the Internet, where it is automatically decrypted and forwarded to the intended destination. By encrypting, the integrity and confidentiality of data is protected even when transmitted over the un-trusted public network. Device uses IPSec standard i.e. IPSec protocol to protect traffic. In IPSec, the identity of communicating users is checked with the user authentication based on Digital Certificates, public keys or Preshared Keys.

Device ensures that all the VPN traffic passing through the VPN tunnels is threat free. All the Firewall Rules and policies are applicable to the traffic going into the VPN tunnels and coming out of the VPN tunnels. Device inspects all the traffic passing through the VPN tunnels and makes sure that there are no viruses, worms, Spam, and inappropriate content or intrusion attempts in the VPN traffic. As VPN traffic is, by default subjected to the DoS inspection, Device provides a facility by which one can bypass scanning of traffic coming from certain hosts from VPN zone. The above functionality is achieved by adding one additional zone called VPN zone. VPN traffic passes through VPN zone and Firewall Rule can be applied to VPN zone.

Device can be used to establish VPN connection between sites, LAN-to-LAN and Client-to-LAN connection. VPN is the bridge between Local & Remote networks/subnets.

Device supports following protocols to authenticate and encrypt traffic:

- Internet Protocol Security (IPSec)
- Layer Two Tunneling Protocol (L2TP)
- Point-to-Point Tunneling Protocol (PPTP)
- Secure Socket Layer (SSL)

**IPsec connections**

Internet Protocol Security (IPsec) is a suite of protocols that support cryptographically secure communication at the IP layer. With IPsec connections, you can provide secure access between two hosts, two sites, or remote users and a LAN. The firewall supports IPsec as defined in RFC 4301. Use these settings to create and manage IPsec connections and to configure failover.

- To add a connection, click **Add**.
- To add a connection using the connection wizard, click **Wizard**.
- To activate a connection, click the Active status indicator.
- To connect, click the connection status indicator.
To download a connection, click.

Table 4: Connection status indicators

<table>
<thead>
<tr>
<th>Status</th>
<th>Connection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Connection is active but not connected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Connection is active and connected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Connection is active but only partially connected. When multiple subnets are configured for the LAN or remote network, the device creates a sub-connection for each subnet. This status indicates that one of the sub-connections is not active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Connection is inactive.</td>
<td></td>
</tr>
</tbody>
</table>

Failover groups

A failover group is a sequence of IPsec connections. If the primary connection fails, the secondary (or subsequent) active connection in the group automatically takes over and keeps traffic moving.

During a connection failure, the firewall checks the health of a primary connection every 60 seconds. When the primary connection is restored, the secondary connection falls back to its original position in the group.

• To activate a group and establish the primary connection, click the Active status indicator.

Turning off a failover group disables the active tunnel used in that group.

Device supports the following IPSec connection types:

• **Remote Access** – This type of VPN is a user-to-internal network connection via a public or shared network. Many large companies have employees that need to connect to the internal network from the field. These field agents access the internal network by using remote computers and laptops without static IP Address.

• **Site to Site** – A Site to Site VPN connects an entire network (such as a LAN or WAN) to a remote network via a network-to-network connection. A network-to-network connection requires routers on each side of the connecting networks to transparently process and route information from one node on a LAN to another node on a remote LAN.

• **Host to Host** – Host to Host VPN connects one desktop or workstation to another by way of a host-to-host connection. This type of connection uses the network to which each host is connected to create a secure tunnel with each other.

Add IPSec Remote Access Connection

Page describes how you can create an IPSec Remote Access Connection

1. Go to Device Configuration > Configure > VPN > IPSec Connections and click Add under IPSec Connections. Select Connection Type as Remote Access.

2. Enter the parameter values as below.

Banner Settings
Name
Specify a unique name to identify IPSec Connection.

Description
Provide description for IPSec VPN Connection.

Connection Type
Select Remote Access.

Policy
Select policy to be used for connection.
Policy can also be added by clicking on “Create New” link.

Action on VPN Restart
Select the Action to be taken on the connection when VPN services or Device restarts.

Available Options
Respond Only – Keeps connection ready to respond to any incoming request.
Disable – Keeps connection disabled till the user activates.

Figure 123: Banner Settings

Authentication Details

Authentication Type
Select Authentication Type. Authentication of user depends on the type of connection.

Available Options:
Preshared Key
Preshared Key authentication is a mechanism whereby a single key is used for encryption and decryption. Both the peers should possess the Preshared Key. Remote peer uses the Preshared Key for decryption. On selecting this option the user shall require to provide the following details:
Preshared Key – Specify the Preshared Key to be used. Preshared Key should be of minimum 5 characters.
Confirm Preshared Key – Provide the same Preshared Key to confirm it.
This Preshared Key will have to be shared or communicated to the peer at the remote end. At the remote end, client will have to specify this key for authentication.
If there is a mismatch in the key, user will not be able to establish the connection.

**Digital Certificate**

Digital Certificate authentication is a mechanism whereby sender and receiver both use Digital Certificate issued by the Certificate Authority. Both sender and receiver must have each other’s Certificate Authority.

**Local Certificate** – Select the local certificate that should be used for authentication by the Device.

**Remote Certificate** – Select the remote certificate that should be used for authentication by remote peer.

![Authentication Details](image)

**Endpoint Details**

**Local**

Select Local WAN port from the list.

IP Aliases created for WAN interfaces will be listed along with the default WAN interfaces.

**Remote**

Specify an IP Address or domain name of the remote peer.

![Endpoints Details](image)

**Network Detail**

**IP Family**

IP family will be enabled automatically according to the IP selected in Local WAN port.

**Local Subnet**

Select Local LAN Address.

Add and Remove LAN Address using Add Button and Remove Button.

**Local ID**

For Preshared Key and RSA Key, select any type of ID from the available options and specify its value.

**Available Options:**

DNS IP Address
Email Address
DER ASN1 DN(X.509)
Note
In case of Local Certificate, ID and its value is displayed automatically as specified in the Certificate.

Allow NAT Traversal
Enable NAT traversal if a NAT device is located between your VPN endpoints i.e. when remote peer has private/non-routable IP Address.
At a time only one connection can be established behind one NAT-box.

Remote LAN Network
Select IP Hosts from the list of IP Hosts available. You can also add a new IP Host and include in the list by clicking on “Add New Item” link.

Remote ID
For Preshared Key and RSA Key, select any type of ID from the available options and specify its value.

Available Options:
DNS IP Address Email Address
DER ASN1 DN(X.509)

Note
In case of Local Certificate, ID and its value is displayed automatically as specified in the Certificate.

User Authentication

User Authentication Mode
Select whether User Authentication is required at the time of connection or not from the available options.
**Available Options:**

Disabled – Click Disable if user authentication is not required.
Enable as Client – If enabled as client, specify username and password.
Enable as Server – If enabled as server, add all the users which are to be allowed to connect.

![User Authentication Mode]

Figure 127: User Authentication

**Quick Mode Selectors**

**Protocol**

Select all the protocols that are to be allowed for negotiations.
Tunnel will pass only that data which uses the specified protocol.

**Available Options:**

All ICMP UDP TCP

**Local Port**

Specify Local Port number that the local VPN peer uses to transport the traffic related to TCP or UDP protocol.
Local port Range: 1 – 65535
To specify any local port, enter *.

**Remote Port**

Specify Remote Port number that the remote VPN peer uses to transport the traffic related to TCP or UDP protocol.
Local port Range: 1 – 65535
To specify any local port, enter *.

![Protocol, Local Port, Remote Port]

Figure 128: Quick Mode Selectors

**Advanced Settings**

**Disconnect when tunnel is idle**

Click this option to allow Device to delete an Idle VPN Session if it exceeds the specified Idle session time interval.
Default - Disable

**Idle session time interval (Only if Disconnect when tunnel is idle option is “Enabled”)**

Specify the time limit after which an Idle VPN Session will be deleted by Device.
Acceptable Range - 120 to 999

Figure 129: Advanced Settings

3. Click **Save** to create connection.

**Add IPSec Site to Site Connection**

Page describes how you can create an IPSec Site to Site Connection

1. Go to **Device Configuration > Configure > VPN > IPSec** and click **Add** under **IPSec Connections**. Select **Connection Type** as **Site to Site**.

2. Enter the parameter values as below.

**Banner Settings**

**Name**

Specify a unique name to identify IPSec Connection.

**Description**

Provide description for IPSec VPN Connection.

**Connection Type**

Select Site to Site.

**Bind With an Interface**

Enable to bind the IPSec VPN tunnel with an interface for configuring Route-based VPN.

In Route-based VPN approach, routing decides which packets to route through the VPN tunnel.

On creation of an interface-based tunnel, a virtual tunnel interface will be created which will be displayed along with other interfaces for configuring Static and Dynamic routes.

**Policy**

Select policy to be used for connection.

Policy can also be added by clicking “Create New” link.

**Action on VPN Restart**

Select the Action to be taken on the connection when VPN services or Device restarts.

**Available Options**

- **Respond Only** – Keeps connection ready to respond to any incoming request.
- **Initiate** – Activates connection on system/service start so that the connection can be established whenever required.
- **Disable** – Keeps connection disabled till the user activates.

**Route-based IP Address Details (Only if Bind With an Interface is enabled)**

**Local IP Address**

Specify local IP Address for the tunnel interface.

You must configure this interface detail, if you want to use the interface in configuring dynamic routing.
Remote IP Address

Specify remote IP Address for the tunnel interface.

You must configure this interface detail, if you want to use the interface in configuring dynamic routing.

Figure 130: Banner Settings

Authentication Details

Authentication Type

Select Authentication Type. Authentication of user depends on the type of connection.

Available Options:

Preshared Key

Preshared Key authentication is a mechanism whereby a single key is used for encryption and decryption. Both the peers should possess the Preshared Key. Remote peer uses the Preshared Key for decryption. On selecting this option the user shall require to provide the following details:

Preshared Key – Specify the Preshared Key to be used. Preshared Key should be of minimum 5 characters.

Confirm Preshared Key – Provide the same Preshared Key to confirm it.

This Preshared Key will have to be shared or communicated to the peer at the remote end. At the remote end, client will have to specify this key for authentication. Refer to VPN Client guide, Phase 1 Configuration.

If there is a mismatch in the key, user will not be able to establish the connection.

Digital Certificate

Digital Certificate authentication is a mechanism whereby sender and receiver both use Digital Certificate issued by the Certificate Authority. Both sender and receiver must have each other’s Certificate Authority.

Local Certificate – Select the local certificate that should be used for authentication by the Device.

Remote Certificate – Select the remote certificate that should be used for authentication by remote peer.

RSA Key
RSA Key authentication is a mechanism whereby two keys – Local and Remote RSA - are used for encryption and decryption.

Local RSA Key – It is known only to the owner and never transmitted over network. Displays automatically generated key which cannot be modified.

Remote RSA Key – It can be regenerated from CLI Console. Refer to Console guide for more details.

Figure 131: Authentication Details

Endpoint Details

Local

Select Local WAN port from the list.

IP Aliases created for WAN interfaces will be listed along with the default WAN interfaces.

Remote

Specify an IP Address or domain name of the remote peer.

Click Add icon against the option “Remote” to add new endpoint pairs or click Remove icon to remove the endpoint pairs.

Figure 132: Endpoints Details

Network Detail

IP Family

Select IP family to configure IPSec VPN tunnels with mixed IP families.

Available Options:

IPv4 IPv6

By default, IPv4 will be selected.

Four types of IPSec VPN tunnels can be created:

4 in 4 (IPv4 subnets with IPv4 gateway)
6 in 6 (IPv6 subnets with IPv6 gateway)
4 in 6 (IPv4 subnets with IPv6 gateway)
6 in 4 (IPv6 subnets with IPv4 gateway)

Local Subnet
Select Local LAN Address.
Add and Remove LAN Address using Add Button and Remove Button.

**NAT Local LAN**
Enable to NAT the LAN IP Address.

**NATed LAN (only if NAT Local LAN is configured)**
Select IP Host or Network Host from the available list. The Device assigns the configured IP address to differentiate between LANs at both the ends of VPN tunnel.
IP Host can also be added by clicking “Add IP Host” link.

**Local ID**
For Preshared Key and RSA Key, select any type of ID from the available options and specify its value.

**Available Options:**
DNS IP Address Email Address
DER ASN1 DN(X.509)

**Note**
In case of Local Certificate, ID and its value is displayed automatically as specified in the Certificate.

**Allow NAT Traversal**
Enable NAT traversal if a NAT device is located between your VPN endpoints i.e. when remote peer has private/non-routable IP Address.
At a time only one connection can be established behind one NAT-box.

**Remote LAN Network**
Select IP Addresses and netmask of remote network which is allowed to connect to the Device server through VPN tunnel. Multiple subnets can be specified. Select IP Hosts from the list of IP Hosts available. You can also add a new IP Host and include in the list.

**Remote ID**
For Preshared Key and RSA Key, select any type of ID from the available options and specify its value.

**Available Options:**
DNS IP Address Email Address
DER ASN1 DN(X.509)

**Note**
In case of Local Certificate, ID and its value is displayed automatically as specified in the Certificate.

In a single connection, same subnet for LAN and Remote Network cannot be configured.
User Authentication

User Authentication Mode

Select whether User Authentication is required at the time of connection or not from the available options.

Available Options:

Disabled – Click Disable if user authentication is not required.
Enable as Client – If enabled as client, specify username and password.
Enable as Server – If enabled as server, add all the users which are to be allowed to connect.

Quick Mode Selectors

Protocol

Select all the protocols that are to be allowed for negotiations.
Tunnel will pass only that data which uses the specified protocol.

Available Options:

All ICMP UDP TCP

Local Port

Specify Local Port number that the local VPN peer uses to transport the traffic related to TCP or UDP protocol.

Local port Range: 1 – 65535

To specify any local port, enter *. 
Sophos Firewall Manager

**Remote Port**

Specify Remote Port number that the remote VPN peer uses to transport the traffic related to TCP or UDP protocol.

Local port Range: 1 – 65535

To specify any local port, enter *.

![Quick Mode Selectors](image)

**Advanced Settings**

**Disconnect when tunnel is idle**

Click this option to allow Device to delete an Idle VPN Session if it exceeds the specified Idle session time interval.

Default - Disable

**Idle session time interval (Only if Disconnect when tunnel is idle option is “Enabled”)**

Specify the time limit after which an Idle VPN Session will be deleted by Device.

Acceptable Range - 120 to 999

![Advanced Settings](image)

3. Click **Save** to create connection.

**Add IPSec Host to Host Connection**

Page describes how you can create an IPSec Host to Host Connection

1. Go to **Device Configuration > Configure > VPN > IPSec** and click **Add** under **IPSec Connections**. Select **Connection Type** as **Host to Host**.

2. Enter the parameter values as below.

**Banner Settings**

**Name**

Specify a unique name to identify IPSec Connection.

**Description**

Provide description for IPSec VPN Connection.

**Connection Type**

Select Host to Host.
Select policy to be used for connection.
Policy can also be added by clicking “Create New” link.

**Action on VPN Restart**

Select the Action to be taken on the connection when VPN services or Device restarts.

**Available Options**

- **Respond Only** – Keeps connection ready to respond to any incoming request.
- **Initiate** – Activates connection on system/service start so that the connection can be established whenever required.
- **Disable** – Keeps connection disabled till the user activates.

![Banner Settings Form](image)

**Figure 137: Banner Settings**

**Authentication Details**

**Authentication Type**

Select Authentication Type. Authentication of user depends on the type of connection.

**Available Options:**

**Preshared Key**

Preshared Key authentication is a mechanism whereby a single key is used for encryption and decryption. Both the peers should possess the Preshared Key. Remote peer uses the Preshared Key for decryption. On selecting this option the user shall require to provide the following details:

- **Preshared Key** – Specify the Preshared Key to be used. Preshared Key should be of minimum 5 characters.
- **Confirm Preshared Key** – Provide the same Preshared Key to confirm it.

This Preshared Key will have to be shared or communicated to the peer at the remote end. At the remote end, client will have to specify this key for authentication. Refer to VPN Client guide, Phase 1 Configuration.

- **Digital Certificate**

Digital Certificate authentication is a mechanism whereby sender and receiver both use Digital Certificate issued by the Certificate Authority. Both sender and receiver must have each other’s Certificate Authority.
Local Certificate – Select the local certificate that should be used for authentication by the Device.

Remote Certificate – Select the remote certificate that should be used for authentication by remote peer.

**RSA Key**

RSA Key authentication is a mechanism whereby two keys – Local and Remote RSA - are used for encryption and decryption.

Local RSA Key – It is known only to the owner and never transmitted over network. Displays automatically generated key which cannot be modified.

Remote RSA Key – It can be regenerated from CLI Console. Refer to Console guide for more details.

![Authentication Details](image)

**Endpoint Details**

**Local**

Select Local WAN port from the list. IP Aliases created for WAN interfaces will be listed along with the default WAN interfaces.

**Remote**

Specify an IP Address or domain name of the remote peer. Click Add icon against the option “Remote” to add new endpoint pairs or click Remove icon to remove the endpoint pairs.

![Endpoints Details](image)

**Network Detail**

**IP Family**

IP family will be enabled automatically according to the IP selected in Local WAN port.

**Local ID**

For Preshared Key and RSA Key, select any type of ID from the available options and specify its value.

**Available Options:**

DNS IP Address Email Address
Note
In case of Local Certificate, ID and its value is displayed automatically as specified in the Certificate.

Allow NAT Traversal
Enable NAT traversal if a NAT device is located between your VPN endpoints i.e. when remote peer has private/non-routable IP Address.

At a time only one connection can be established behind one NAT-box.
Default-Enabled

Remote LAN Network
Select IP Addresses and netmask of remote network which is allowed to connect to the Device server through VPN tunnel. Multiple subnets can be specified. Select IP Hosts from the list of IP Hosts available on the Web Admin Console.

You can also add a new IP Host.

Remote ID
For Preshared Key and RSA Key, select any type of ID from the available options and specify its value.

Available Options:
DNS IP Address Email Address
DER ASN1 DN(X.509)

Note
In case of Local Certificate, ID and its value is displayed automatically as specified in the Certificate.

Figure 140: Network Detail
User Authentication

User Authentication Mode

Select whether User Authentication is required at the time of connection or not from the available options.

Available Options:

Disabled – Click Disable if user authentication is not required.
Enable as Client – If enabled as client, specify username and password.
Enable as Server – If enabled as server, add all the users which are to be allowed to connect.

Figure 141: User Authentication

Quick Mode Selectors

Protocol

Select all the protocols that are to be allowed for negotiations. Tunnel will pass only that data which uses the specified protocol.

Available Options:

All ICMP UDP TCP

Local Port

Specify Local Port number that the local VPN peer uses to transport the traffic related to TCP or UDP protocol.
Local port Range: 1 – 65535
To specify any local port, enter *.

Remote Port

Specify Remote Port number that the remote VPN peer uses to transport the traffic related to TCP or UDP protocol.
Local port Range: 1 – 65535
To specify any local port, enter *.

Figure 142: Quick Mode Selectors

Advanced Settings

Disconnect when tunnel is idle
Click this option to allow SF to delete an Idle VPN Session if it exceeds the specified Idle session time interval.

Default - Disable

**Idle session time interval (Only if Disconnect when tunnel is idle option is “Enabled”)**

Specify the time limit after which an Idle VPN Session will be deleted by SF.

Acceptable Range - 120 to 999

![Figure 143: Advanced Settings](image)

3. Click **Save** to create new connection.

**VPN Wizard**

The VPN Connection Wizard takes you step-by-step through the configuration of Site-to-Site IPSec VPN connection between a Head Office (HO) device and multiple Branch Office (BO) devices simultaneously. After the configuration is complete, the wizard creates new IPSec VPN connections on the HO and BOs.

**VPN Wizard set-up**

The VPN Wizard takes you step-by-step through the configuration of VPN connection between two managed devices simultaneously.

1. Go to **Device Configuration** > **Configure** > **VPN** > **VPN Wizard** and click **Add**.

   On clicking **Add**, the VPN Wizard starts which contains the following three sections:

   a) **Select Device**
   b) **Device Details**
   c) **Security Information**

2. Select the managed Head Office and Branch Office devices respectively based on the description shown below.

**Head Office**

**Select Device**

Select the Head Office device from the drop-down list of available devices.

**Note**

Only one device can be selected as the Head Office device.

**Note**

The list of available devices shows only those added devices which are Connected and Synchronized with Sophos Firewall Manager.

**Tunnel Name**

Specify name to identify the tunnel for Head Office.

**IP Family**

Specify the IP type of the Head Office device subnet or Local End Point.
Description

Provide description for the Head Office device.

Branch Office

Select Devices

Select the Branch Office device from the drop-down list of available devices. You can select multiple devices at a time.

Description

Provide description for the Branch Office device.

3. Configure connection details for the Head Office and Branch Office devices respectively.

Head Office Device

Policy

Select policy to be used for Head Office VPN connection. To create a new policy or go to Device Configuration > Configure > VPN > IPSec page.

Local End Point

Select Local WAN port of the Head Office device from the list.

IP/Domain

Specify IP Address or domain name of the selected Head Office device.

Subnet

Select Local LAN Address of the Head Office device. Click Add IP Host to create a new IP Host.

Branch Office Devices

Policy

Select policy to be used for Head Office VPN connection. To create a new policy or go to Device Configuration > Configure > VPN > IPSec page.

Note

Select a policy that is compatible with Head Office Policy.

Local End Point

Select Local WAN port of the Head Office device from the list.

Override End Point

Select to override interface assignment and specify the Default End Point interface for all selected devices. Alternatively, you can create dynamic interfaces for each device. To add more interfaces, click the + icon to add more dynamic interfaces.

Subnet

Specify Local LAN Subnet for each managed Branch Office device.


Specify Preshared Key for Head Office and all Branch Office devices.

Note

Preshared Key should be of minimum 5 characters.
5. Click **Finish** to save the settings. On completing the VPN Wizard, all IPSec connections will be created. The connections can later be managed from the VPN Wizard main page.

**SSL VPN (Remote Access)**

The remote access SSL feature of SFM is realized by OpenVPN, a full-featured SSL VPN solution. You can create point-to-point encrypted tunnels between remote employees and your company, requiring both SSL certificates and a username/password combination for authentication. This enables access to internal resources. In addition, a secure User Portal is offered, which can be accessed by each authorized user to download a customized SSL VPN client software bundle. This bundle includes a free SSL VPN client, SSL certificates and a configuration that can be handled by a simple one-click installation procedure. The SSL VPN client supports most business applications such as native Outlook, native Windows file sharing, and many more.

**Device Configuration > Configure > VPN > SSL VPN (Remote Access)**

Following is a description of the table elements:

**Name**
Displays the name of the SSL VPN remote access policy.

**Use as Default Gateway**
Displays if and which default gateway is used for the policy.

**Description**
Displays the description which was entered for the policy.

**Manage**
Displays the available managing options for the policy:

- **Edit**: Allows you to edit the policy.
- **Delete**: Allows you to delete the policy.

**Add a remote access policy**

1. Go to **VPN > SSL VPN (remote access)** and click **Add**.
2. Type a name.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy members</td>
<td>Users or groups who should have access to the network resources.</td>
</tr>
</tbody>
</table>

4. Specify tunnel access settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use as default gateway</td>
<td>Use this remote access policy as default gateway. When on, all traffic, including external internet requests, is forwarded to a default gateway. When off, internal and external traffic is handled by different gateways.</td>
</tr>
<tr>
<td>Permitted network resources</td>
<td>Resources (for example, interfaces) that this policy is permitted to access.</td>
</tr>
</tbody>
</table>

5. Specify idle timeout settings.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disconnect idle clients</td>
<td>Disconnect idle clients from the session after the specified time.</td>
</tr>
<tr>
<td>Override global timeout</td>
<td>Time after which idle clients will be disconnected.</td>
</tr>
</tbody>
</table>

6. Click **Apply**.

Go to **Administration > Device access** and enable the LAN and WAN zones for the user portal.

**SSL VPN (Site to Site)**

Site-to-site VPN tunnels can be established via an SSL connection. SSL VPN connections have distinct roles attached. The tunnel endpoints act as either client or server. The client always initiates the connection, the server responds to client requests. Keep in mind that this contrasts IPsec where both endpoints normally can initiate a connection.

**Device Configuration > Configure > VPN > SSL VPN (Site to Site)**

**Server Connections**

This section lists all existing SSL VPN site-to-site server connections. Following is a description of the table elements:

**Status**
Displays if the connection is activated or not. You can activate/deactivate the connection with help of the displayed toggle switch.

**Connection Name**
Displays the name of the connection.

**Local Networks**
Displays the local networks that are allowed to be accessed remotely.

**Remote Networks**
Displays the remote networks that are allowed to connect to the local network(s).

**Manage**
Displays the available managing options for the connection:

- **Edit**: Allows you to edit the connection.
- **Delete**: Allows you to delete the connection.

A connection can be added or deleted by pressing the concerning buttons.

**Client Connections**

This section lists all existing SSL VPN site-to-site client connections. Following is a description of the table elements:

**Status**
Displays if the connection is activated or not. You can activate/deactivate the connection with help of the displayed toggle switch.
**Connection Name**
Displays the name of the connection.

**Use HTTP Proxy Server**
Displays the HTTP proxy server which is used for the connection.

**Manage**
Displays the available managing options for the connection:
- **Edit**: Allows you to edit the connection.
- **Delete**: Allows you to delete the connection.

A connection can be added or deleted by pressing the concerning buttons.

**Add SSL VPN Site-to-Site Server Connection**
This page describes how to add a SSL VPN site-to-site server connection.

1. Go to **Device Configuration > Configure > VPN > SSL VPN (Site to Site)** and click **Add** in the **Server** section.
2. Enter values for the following settings:

**Connection Name**
Enter a descriptive name for the connection.

**Use Static Virtual IP Address (optional)**
Only select this option if the IP address pool is not compatible with the client's network environment: By default clients are assigned an IP address from a Virtual IP pool. Rarely, it may happen that such an IP address is already in use on the client's host. In that case enter a suitable IP address in the **Static Peer IP** field which will then be assigned to the client during tunnel setup.

**Local Networks**
Select or add one or more remote networks that are allowed to connect to the local network(s).

**Remote Networks**
Select or add one or more remote networks that are allowed to connect to the local network(s).

**Description (optional)**
Enter a description or other information.
3. Click **Save** to save your settings.

The new SSL server connection appears on the **Server** list.

To either edit or delete a server connection, click the corresponding buttons in the **Server** list.

The next step is the client configuration which has to take place on client side and not on server side.

Download the client configuration file with help of the provided button in the **Server** list.

**Note**

If you want to send the file via mail it is recommended to use the encryption option which is provided in the download dialog.

How to configure the client is described in chapter **System > VPN > SSL VPN Site-to-Site > Add Client Site-to-Site**.

**Add SSL VPN Site-to-Site Client Connection**

This page describes how to add a SSL VPN site-to-site client connection.

1. Go to **Device Configuration > Configure > VPN > SSL VPN (Site to Site)** and click **Add** in the **Client** section.
2. Enter values for the following settings:

**Connection Name**

Enter a descriptive name for the connection.

**Configuration File**

Click the **Browse...** icon, browse for the client configuration file and click **Open**.

**Note**

The file has to be in `.apc` or `.epc` format.

**Password (optional)**
If the file has been encrypted, enter the password.

**Use HTTP Proxy Server (optional)**

Activate if the client is located behind a proxy and enter the proxy settings:

- **Proxy Server**: Select or add a proxy server.
- **Proxy Port**: Enter a proxy port.
- **Proxy Requires Authentication (optional)**: Select the checkbox if the client needs to authenticate against the proxy and enter **Username** and **Password**.

**Override Peer Host Name (optional)**

Select the checkbox and add or enter a hostname if the server system’s regular hostname cannot be resolved from the client host.

**Description (optional)**

Add a description or other information.

---

![Add SSL Connection](image)

**Figure 145: Add SSL Connection**

3. Click **Save**.

The new SSL VPN client connection appears on the **Client** list.

To either edit or delete a client connection, click the corresponding buttons in the **Client** list.

**L2TP (remote access)**

The Layer Two Tunneling Protocol (L2TP) enables you to provide connections to your network through private tunnels over the internet. The firewall supports L2TP as defined in RFC 3931.

**Note**

To activate a connection, you must first enable L2TP. Click **Show VPN settings** and click the **L2TP** tab.

- To activate a connection, click the Active status indicator.
- To connect, click the connection status indicator.
### Table 5: Connection status indicators

<table>
<thead>
<tr>
<th>Active</th>
<th>Connection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="active_icon" alt="Active" /></td>
<td><img src="connection_icon" alt="Connection" /></td>
<td>Connection is active but not connected.</td>
</tr>
<tr>
<td><img src="active_icon" alt="Active" /></td>
<td><img src="connection_icon" alt="Connection" /></td>
<td>Connection is active and connected.</td>
</tr>
<tr>
<td><img src="active_icon" alt="Active" /></td>
<td><img src="connection_icon" alt="Connection" /></td>
<td>Connection is active but only partially connected. When multiple subnets are configured for the LAN or remote network, the device creates a sub-connection for each subnet. This status indicates that one of the sub-connections is not active.</td>
</tr>
<tr>
<td><img src="inactive_icon" alt="Active" /></td>
<td><img src="connection_icon" alt="Connection" /></td>
<td>Connection is inactive.</td>
</tr>
</tbody>
</table>

**Add L2TP Connection**

Page describes how you can create an L2TP Connection

1. Go to **Device Configuration > Configure > VPN > L2TP Connections** and click **Add**.
2. Enter the parameter values as below.

**Banner Settings**

**Name**

Specify a unique name to identify L2TP Connection.

**Description**

Provide description for L2TP Connection.

**Policy**

Select policy to be used for connection.

Policy can also be added by clicking **Create New** link.

**Action on VPN Restart**

Select the Action to be taken on the connection when VPN services or Device restarts.

**Available Options**

- **Respond Only** – Keeps connection ready to respond to any incoming request.
- **Disable**

  Keeps connection disabled till the user activates.
Figure 146: Banner Settings

**Authentication Details**

**Authentication Type**

Select Authentication Type. Authentication of user depends on the type of connection.

**Available Options:**

**Preshared Key**

Preshared Key authentication is a mechanism whereby a single key is used for encryption and decryption. Both the peers should possess the Preshared Key. Remote peer uses the Preshared Key for decryption. On selecting this option the user shall require to provide the following details:

Preshared Key – Specify the Preshared Key to be used. Preshared Key should be of minimum 5 characters.

Confirm Preshared Key – Provide the same Preshared Key to confirm it.

This Preshared Key will have to be shared or communicated to the peer at the remote end. At the remote end, client will have to specify this key for authentication.

If there is a mismatch in the key, user will not be able to establish the connection.

**Digital Certificate**

Digital Certificate authentication is a mechanism whereby sender and receiver both use Digital Certificate issued by the Certificate Authority. Both sender and receiver must have each other’s Certificate Authority.

Local Certificate – Select the local certificate that should be used for authentication by the Device.

Remote Certificate – Select the remote certificate that should be used for authentication by remote peer.
**Local Network Detail**

**Local WAN Port**

Specify the Local Port number that the local VPN peer uses to transport traffic related to TCP or UDP protocol.

Acceptable Range - 1 to 65535

To specify any local port, enter *.

**Local ID**

For Preshared Key and RSA Key, select any type of ID from the available options and specify its value.

**Available Options:**

DNS IP Address Email Address

DER ASN1 DN(X.509)

(DER ASN1 DN (X.509) is not applicable. In case of Local Certificate, ID and its value is displayed automatically as specified in the Local Certificate)

![Figure 148: Local Network Details](image)

**Remote Network Details**

**Remote Host**

Specify IP Address or host name of remote end-point. Specify * for any IP Address.

**Allow NAT Traversal**

Enable NAT traversal if a NAT device is located between your VPN endpoints i.e. when remote peer has private/non-routable IP Address.

At a time only one connection can be established behind one NAT-box.

Default-Enabled

**Remote LAN Network**

Select IP Addresses and netmask of remote network which is allowed to connect to the Device server through VPN tunnel. Multiple subnets can be specified. Select IP Hosts from the list of IP Hosts available on the Admin Console.

You can also add a new IP Host by click [Create New](#) link.

**Remote ID**

For Preshared Key and RSA Key, select any type of ID from the available options and specify its value.

**Available Options:**

DNS IP Address Email Address

DER ASN1 DN(X.509) (DER ASN1 DN (X.509) is not applicable.)
Quick Mode Selectors

Local Port

Specify Local Port number that the local VPN peer uses to transport the traffic related to TCP or UDP protocol.

Default: 1701
Local port Range: 1 – 65535
To specify any local port, enter *.

Remote Port

Specify Remote Port number that the remote VPN peer uses to transport the traffic related to TCP or UDP protocol.

Default: *
Local port Range: 1 – 65535
To specify any local port, enter *.

Advanced Settings

Disconnect when tunnel is idle

Click this option to allow Device to delete an Idle VPN Session if it exceeds the specified Idle session time interval.

Default - Disable

Idle session time interval (Only if Disconnect when tunnel is idle option is “Enabled”)

Specify the time limit after which an Idle VPN Session will be deleted by Device.
Acceptable Range - 120 to 999 seconds.
3. Click Save to create new connection.

**PPTP (Remote Access)**

Point-to-Point Tunneling Protocol allows organizations to extend their own private network through private tunnels over the public Internet.

The Device supports several authentication options including Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft Challenge Handshake Authentication Protocol (MS-CHAPv2).

The Configuration page provides option to configure the Device as PPTP server and provide access or disable remote access through PPTP to various users.

**Enable PPTP**

Click to enable PPTP.

**Assign IP From**

Specify IP Address range. PPTP server will lease IP Address to the PPTP client from the specified IP Address range. The PPTP client uses the assigned IP Address as its source address for the duration of the connection.

Do not specify the same IP Address range in L2TP configuration and PPTP configuration.

**Allow leasing IP Address from Radius server for L2TP, PPTP and CISCO VPN Client**

Click to lease IP Address to the PPTP users through the Radius Server.

Radius Server is a protocol that allows network devices to authenticate users against a central database. It can also store technical information used by network devices.

If enabled, the configured IP Address is overridden with the IP Address provided by the Radius Server.

Default - Disable

**Primary DNS Server**

Specify DNS Server to be used at the client end.

**Secondary DNS Server**

Specify Alternate DNS server to be used at the client end.

**Primary WINS Server**

Specify WINS Server to be used at the client end.

**Secondary WINS Server**

Specify Alternate WINS Server to be used at the client end.

**Add Member(s) Button**

Click to select users who are to be allowed remote access through PPTP.

**Show Members**

Click to view list of PPTP members.

**Add PPTP Members**

The Add PPTP Members page allows you to select users who are to be allowed remote access through PPTP.

1. Click Add Member(s) button to add user or user groups. A window displays list of users and user groups.

2. Select users or user groups who are to be allowed remote access through PPTP. You can add single or multiple users or user groups.
3. Click **Apply** to add these users and user groups to the PPTP members list.

**Show PPTP Members**

Use **Show Members** page to view list of PPTP members and remove members for whom remote access through PPTP is to be disabled.

The **Show Members** page allows you to view list of PPTP members and remove members for whom remote access through PPTP is to be disabled.

1. Click **Show Members** button to view list of PPTP members. A window displays list of L2TP users who are allowed access through PPTP connection.
2. Select the users for whom you want to disable PPTP access. You can select multiple users or user groups.

3. Click **Delete** button.

**Clientless Access**

For the bookmark function you can define clientless access policies.

**Note**

With Safari browser on Mac OSX or iOS, users have to import the CA certificate of SFOS first before they can use clientless access. The CA certificate can be downloaded under **Device Configuration > Configure > Authentication > Certificate Authority**. Usually its name is "Default".

Following is a description of the table elements:

**Name**
Displays the name of the clientless access policy.

**Restrict Web Applications**
Displays if the web application restriction is activated (**Yes**) or not (**No**).

**Description**
Displays the description which was entered for the policy.

**Manage**
Sophos Firewall Manager

Displays the available managing options for the policy:

- **Edit**: Allows you to edit the policy.
- **Delete**: Allows you to delete the policy.

**Related tasks**
- Add a clientless access policy (page 212)
- Add a Bookmark (page 221)
- Add a Bookmark Groups (page 225)

**Add a clientless access policy**

To be able to configure a policy, you must create at least one bookmark.

1. Go to **VPN > Clientless access** and click **Add**.
2. Type a name.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy members</td>
<td>Users or groups who should have access to the bookmarks.</td>
</tr>
</tbody>
</table>

4. Specify clientless portal settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Published bookmarks</td>
<td>Bookmarks or bookmark groups to which policy members have access.</td>
</tr>
<tr>
<td>Restrict web applications</td>
<td>Do not display the secure web browsing section in the user portal. This restricts users to the URLs specified in the bookmarks.</td>
</tr>
</tbody>
</table>

5. Click **Apply**.

**IPsec policies**

Internet Protocol Security (IPsec) profiles specify a set of encryption and authentication settings for an Internet Key Exchange (IKE). You can use profiles when setting up IPsec or L2TP connections. The default set of profiles supports some commonly used VPN deployment scenarios.

- To duplicate a profile, click

**General settings**

- **Key exchange**: Internet Key Exchange (IKE) version to use.
  - IKEv2 requires less bandwidth than IKEv1 and has EAP authentication and NAT traversal included, among other improvements.

- **Authentication mode**: Mode to use for exchanging authentication (phase 1) information.

- **Key negotiation tries**: Maximum number of key negotiation trials.
### Allow re-keying
Allow the negotiation to be initiated automatically by either peer before the current key expires.

### Pass data in compressed format
Pass data in compressed format to increase throughput.

### SHA2 with 96-bit truncation
Available only for IKEv1. Enable truncation of SHA2 to 96 bits.

## Phase 1

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key life</strong></td>
<td>Lifetime of the key, in seconds.</td>
</tr>
<tr>
<td><strong>Re-key margin</strong></td>
<td>Time, in seconds, of the remaining life of the key after which the negotiation process should be re-attempted.</td>
</tr>
<tr>
<td><strong>Randomize re-keying margin by</strong></td>
<td>Factor by which the re-keying margin is randomized.</td>
</tr>
<tr>
<td><strong>DH group</strong></td>
<td>Diffie–Hellman group to use for encryption.</td>
</tr>
<tr>
<td><strong>Algorithm combinations</strong></td>
<td>Combination of encryption and authentication algorithms to use to ensure the integrity of the data exchange.</td>
</tr>
</tbody>
</table>

## Phase 2

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PFS group</strong></td>
<td>Perfect Forward Secrecy group (Diffie–Hellman group) to use to force a new key exchange for each phase 2 tunnel.</td>
</tr>
<tr>
<td><strong>Key life</strong></td>
<td>Lifetime of the key, in seconds.</td>
</tr>
<tr>
<td><strong>Algorithm combinations</strong></td>
<td>Combination of encryption and authentication algorithms to use to ensure the integrity of the data exchange.</td>
</tr>
</tbody>
</table>

## Dead peer detection

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dead peer detection</strong></td>
<td>Check at specified interval to see whether peer is active.</td>
</tr>
<tr>
<td><strong>Check peer after every</strong></td>
<td>Interval, in seconds, at which peer is checked.</td>
</tr>
<tr>
<td><strong>Wait for response up to</strong></td>
<td>Time, in seconds, to wait for a peer response.</td>
</tr>
<tr>
<td><strong>Action when peer unreachable</strong></td>
<td>Action to take when peer is determined to be inactive.</td>
</tr>
</tbody>
</table>

### Add an IPsec policy
1. Go to VPN > IPsec policies and click Add.
2. Type a name.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key exchange</strong></td>
<td>Internet Key Exchange (IKE) version to use. IKEv2 requires less bandwidth than IKEv1 and has EAP authentication and NAT traversal included, among other improvements.</td>
</tr>
</tbody>
</table>
| **Authentication mode**      | Mode to use for exchanging authentication (phase 1) information.  
Main mode: Executes the Diffie–Hellman key exchange in three two-way exchanges.  
Aggressive mode: Executes the Diffie–Hellman key exchange in three messages. A tunnel can be established faster as fewer messages are exchanged during authentication and no cryptographic algorithm is used to encrypt the authentication information. Use this option when the remote peer has dynamic IP addresses.  
**Warning**  
Aggressive mode is insecure and, therefore, not recommended. |
| **Key negotiation tries**    | Maximum number of key negotiation trials.                                                                                                                                                       |
| **Allow re-keying**          | Enable re-keying to start the negotiation process automatically before the key expires.  
The negotiation can be initiated by the local or remote peer. Depending on PFS, the negotiation will use the same key or generate a new key. Configure key life for phase 1 and 2 if enabled.  
Disable to start negotiation process only when peer sends re-keying request. If the peer is configured for not to re-key the connection, the connection uses the same key during its lifetime. It becomes an insecure configuration as the new key is not generated. The purpose is to limit the time that security associations can be used by a third party who has gained control of the peer. |
| **Pass data in compressed format** | Pass data in compressed format to increase throughput.                                                                                                                                            |
| **SHA2 with 96-bit truncation** | Available only for IKEv1. Enable truncation of SHA2 to 96 bits.                                                                                                                                  |

4. **Specify phase 1 settings.**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key life</strong></td>
<td>Lifetime of the key, in seconds.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Re-key margin</td>
<td>Time, in seconds, of the remaining life of the key after which the negotiation process should be re-attempted. For example, if the key life is 8 hours, and the re-key margin is 10 minutes, the negotiation process will start after 7 hours and 50 minutes.</td>
</tr>
<tr>
<td>Randomize re-keying margin by</td>
<td>Factor by which the re-keying margin is randomized. For example, if the key life is 8 hours, the re-key margin is 10 minutes, and the randomization is set to 20%, the negotiation attempts will start after 8 minutes and end at 12 minutes.</td>
</tr>
<tr>
<td>DH group</td>
<td>Diffie–Hellman group to use for encryption. The group specifies the key length used for encryption.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The remote peer must use the same group.</td>
</tr>
<tr>
<td>Algorithm combinations</td>
<td>Combination of encryption and authentication algorithms to use to ensure the integrity of the data exchange.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The remote peer must use at least one of the defined combinations.</td>
</tr>
</tbody>
</table>

5. Specify phase 2 settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PFS group</td>
<td>Perfect Forward Secrecy group (Diffie–Hellman group) to use to force a new key exchange for each phase 2 tunnel.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Using PFS is more secure, although re-keying may take longer. Not all vendors support PFS. Check your hardware specifications before selecting a group.</td>
</tr>
<tr>
<td>Key life</td>
<td>Lifetime of the key, in seconds. Key life of phase 2 must be shorter than that of phase 1.</td>
</tr>
<tr>
<td>Algorithm</td>
<td>Combination of encryption and authentication algorithms to use to ensure the integrity of the data exchange.</td>
</tr>
<tr>
<td>combinations</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dead peer detection</td>
<td>Check at specified interval to see whether peer is active. For connections with static endpoints, the tunnel will be re-negotiated automatically. Connections with dynamic endpoints require the remote side to re-negotiate the tunnel.</td>
</tr>
<tr>
<td>Check peer after every</td>
<td>Interval, in seconds, at which peer is checked.</td>
</tr>
<tr>
<td>Wait for response up to</td>
<td>Time, in seconds, to wait for a peer response. If the response is not received within the specified interval, the peer is considered inactive.</td>
</tr>
<tr>
<td>Action when peer unreachable</td>
<td>Action to take when peer is determined to be inactive.</td>
</tr>
</tbody>
</table>

7. Click **Save**.

**SSL VPN settings**

Make the global SSL VPN settings here.

The Show SSL VPN settings tab allows you to define parameters requested for remote access such as protocols, server certificates and IP addresses for SSL clients. The SSL VPN client supports most business applications such as native Outlook, native Windows file sharing, and many more.

1. Go to **VPN > Show SSL VPN settings**.
2. Select the protocol to be used.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>TCP guarantees (in-order) packet delivery. It is slower but more secure than UDP. It is recommended to be used for emailing, web-surfing, FTP, SSH.</td>
</tr>
<tr>
<td>UDP</td>
<td>With UDP data could be lost. It is faster than TCP and usually used for streaming media, DNS, VoIP, TFTP.</td>
</tr>
</tbody>
</table>

3. Select a local SSL certificate to be used by the SSL VPN server to identify itself against the clients.

   **Note**
   You can use self-signed certificates by using the corresponding option in the **Certificates** menu.

4. Specify the settings as required.
### Option | Description
--- | ---
Override hostname | Set the server IP address for client VPN connection. Usually this should be the external IP address of Sophos XG Firewall.  
IPv4 lease range | IP address range which is used to distribute IP addresses to the SSL clients.  
Subnet mask | Netmask for the IP address range above.  
**Note**  
The netmask must not be greater than 29 bits, because OpenVPN cannot handle address ranges whose netmask is /30, /31, or /32. The netmask is limited to a minimum of 16.  
IPv6 lease (IPv6/prefix) | Set the IPv6 prefix in the first field and the netmask in the last field to lease IPv6 addresses to clients.  
**Note**  
You also have to select **IPv4 and IPv6 both** as **Lease mode**.
Lease mode |  
IPv4 DNS |  
IPv4 WINS |  

#### Lease mode
Select if you want to only lease IPv4 addresses to SSL clients or both IPv4 and IPv6 addresses.

#### IPv4 DNS
Specify up to two IPv4 DNS servers, primary and secondary, of your organization.

#### IPv4 WINS
Specify up to two IPv4 WINS servers, primary and secondary, of your organization.

**Windows Internet Naming Service (WINS)** is Microsoft’s implementation of NetBIOS Name Server (NBNS) on Windows operating systems. Effectively, WINS is to NetBIOS names what DNS is to domain names—a central mapping of hostnames to IP addresses.

#### Domain name
Enter the hostname of your Sophos XG Firewall as a fully qualified domain name (FQDN). The FQDN is an unambiguous domain name that specifies the node’s absolute position in the DNS tree hierarchy, for example sf.example.com. A hostname may contain alphanumeric characters, dots, and hyphens. At the end of the hostname there must be a TLD (top level domain) such as com, org, or de. The hostname will be used in notification messages to identify the Sophos XG Firewall.

#### Disconnect dead peer after
Enter a time limit in seconds after which a dead connection will be terminated by Sophos XG Firewall.
Default: 180 seconds.

**Disconnect idle peer after**
Enter a time limit in minutes when an idle connection will be terminated.
Default: 15 minutes.

5. Specify the **Cryptographic settings**.

**Encryption algorithm**
Specify the algorithm used for encrypting the data sent through the VPN tunnel. The following algorithms are supported and all in Cipher Block Chaining (CBC) mode:
- DES-EDE3-CBC
- AES-128-CBC (128 bit)
- AES-192-CBC (192 bit)
- AES-256-CBC (256 bit)
- BF-CBC (Blowfish (128 bit))

**Authentication algorithm**
- SHA-1 (160 bit) (not recommended)
- SHA2 256 (256 bit)
- SHA2 384 (384 bit)
- SHA2 512 (512 bit)
- MD5 (128 bit) (not recommended)

**Key size**
The key size (key length) is the length of the Diffie-Hellman key exchange. The longer this key is, the more secure the symmetric keys are. The length is specified in bits. You can choose between a key size of 1024 or 2048 bits.

**Key lifetime**
Enter a time period after which the key will expire.
Default: 28,800 seconds

6. Specify the **Compression settings**.

**Compress SSL VPN traffic**
If enabled, all data sent through SSL VPN tunnels will be compressed prior to encryption.

7. Specify the **Debug settings**.

**Enable debug mode**
When enabling debug mode, the SSL VPN log file will contain extended information useful for debugging purposes.

8. Click **Apply**.

**L2TP**
On this page you can enable L2TP and configure the settings for L2TP connections.

**Device Configuration > Configure > VPN > L2TP Settings**
Following is a description of the settings of this page:
Enable L2TP

Click this checkbox to enable/disable L2TP.

General Settings

Assign IP From

Set an IP address range which is used to distribute IP addresses to L2TP clients. This should be a private IP address range.

Allow leasing IP address from RADIUS server for L2TP, PPTP and CISCO VPN Client

If this option is enabled and if the user is authenticated via a RADIUS server, the configured IP address (static and the IP address range) is overridden with the IP address provided by the RADIUS server. If no IP addresses are configured on the RADIUS server, the static IP address configured for the user will be assigned, else an IP address will be leased from configured IP address range.

Client Information

Primary/Secondary DNS Server

Specify up to two DNS servers of your organization. If there is no DNS server available in the list, you can select Other and enter the IP address of a DNS server into a textfield.

Primary/Secondary WINS Server

Specify up to two WINS servers of your organization. If there is no WINS server available in the list, you can select Other and enter the IP address of a WINS server into a textfield.

Related tasks

Add L2TP Member (page 219)
Show/Remove L2TP Member (page 220)

Add L2TP Member

This page describes how to add an L2TP member. Before you can add L2TP members, L2TP must be enabled. See chapter L2TP (page 218).

1. Go to Device Configuration > Configure > VPN > L2TP Settings and click Add Members at the bottom of the page.
2. Select users and groups from the table that should be enabled for L2TP.

Figure 154: Add L2TP Member

3. Click Apply.
   All selected entries will be added as L2TP members.
Related concepts
L2TP (page 218)
On this page you can enable L2TP and configure the settings for L2TP connections.

Related tasks
Show/Remove L2TP Member (page 220)

Show/Remove L2TP Member
This page describes how to see which users or groups are members of L2TP and how to remove L2TP members. Before you can show L2TP members, L2TP must be enabled. See chapter L2TP (page 218).

1. Go to Device Configuration > Configure > VPN > L2TP Settings and click Show Members at the bottom of the page.
   
   A dialog opens that shows all current members of L2TP.

2. Select users or groups from the table that should be removed from L2TP.

   ![](image)

   Figure 155: Show L2TP Members

3. Click Delete.
   
   All selected entries will be removed as L2TP members.

Related concepts
L2TP (page 218)
On this page you can enable L2TP and configure the settings for L2TP connections.

Related tasks
Add L2TP Member (page 219)

Bookmarks

Bookmarks are the resources whose access will be available through the user portal. Bookmarks are applied through the Clientless Access policy and are available to users who have web or application access.

Device Configuration > Configure > VPN > Bookmarks

The bookmark feature enables users from external networks to access internal resources via pre-configured connection types, using only a browser as a client, without installing plug-ins. To do so, the user logs in to the User Portal. On the SSL VPN tab, a list of all connections available to this user is shown. Clicking the Connect button initiates the connection to the defined internal resource. As an administrator you have to generate these connections beforehand, specifying the allowed users, the connection type and other settings. Internal resources can be accessed using different connection types: for example Remote Desktop Protocol (RDP) or Virtual Network Computing (VNC) to access remote desktops, a browser to use web applications (HTTP/HTTPS), or Telnet/Secure Shell (SSH) for terminal sessions. However, the portal does not permit to download content, e.g. via HTTP, to the user's local computer. Using this feature it is possible to give multiple users access to internal resources which do not support multi-user access themselves (e.g., network hardware like switches).
or easily provide very granular access to just one specific service instead of giving access to entire systems or networks.

The page displays all existing bookmarks. You can add new bookmarks, update or delete them. Following is a description of the table elements:

**Name**
Displays the name of the bookmark.

**Type**
Displays the type of the bookmark.

**URL**
Displays the URL which is defined for the bookmark.

**Description**
Displays the description of the bookmark.

**Related tasks**
*Add a clientless access policy* (page 212)

**Add a Bookmark**

This page describes how to add a bookmark.

1. Go to **Device Configuration > Configure > VPN > Bookmarks** and click **Add**.
2. Enter values for the following settings:

**Name**
Enter a descriptive name for the bookmark.

**Type**
Select a bookmark type. Depending on the selected connection type, different parameters are displayed. The following types are available:

- **HTTPS**: Browser-based access to web applications via HTTPS.
- **HTTP**: Browser-based access to web applications via HTTP.

**Note**
The URL used for the HTTP/HTTPS connection is composed of the destination, the port and the path options for this connection.

- **RDP**: Remote access using the *Remote Desktop Protocol (RDP)*, e.g., to open a remote desktop session to a Windows host.
- **TELNET**: Terminal access using the Telnet protocol, e.g., to give access to a switch or a printer.
- **SSH**: Terminal access using SSH.
- **FTP**: *File Transfer Protocol* for exchanging files over packet-switched networks.
- **FTPS**: Extension of FTP. Additionally supports TLS and SSL protocols.
- **SFTP**: *SSH File Transfer Protocol*, or *Secure File Transfer Protocol*, is a separate protocol packaged with SSH that works in a similar way over a secure connection.
- **SMB**: The *Server Message Block (SMB)* Protocol is a network file sharing protocol.
• **VNC**: Remote access using *Virtual Network Computing (VNC)*, e.g., to open a remote desktop of a Linux/Unix host.

**Note**
Currently only VNC classic authentication (password only) is supported. Make sure your server is set up accordingly.

**Note**
The default port is displayed next to the drop-down menu.

**URL**
Enter the URL of the website for which the bookmark is to be created.

**Note**
Note the examples displayed below the text box.

**Port**
Enter a port number for the bookmark. By default the standard port of the selected bookmark type is given.

**Automatic Login**
If enabled, users can log in without knowing the authentication data. In this case, you have to provide the authentication data. The displayed options depend on the selected connection type:

**Username**
Enter the username users should use to connect.

**Password**
Enter the password users should use to connect.

**Note**
When using the connection type **Telnet**, for security reasons automatic login only works when the banner length sent from the Telnet server does not exceed 4096 characters (including the password prompt). If the banner is longer, automatic login fails. In this case reduce the banner length or switch to manual login.

**Referred Domains**
*(only with bookmark type **HTTPS** or **HTTP)*
Search/add one or more domain(s)/URL(s) which are required by the bookmark URL to render it appropriately.

**Domain**
*(only with bookmark type **RDP** or **SMB)*
Enter a domain name.

**Protocol Security**
*(only with bookmark type **RDP)*
Select the security protocol for the Remote Desktop session. You can choose between **RDP**, **TLS** and **NLA** (Network Level Authentication). Your settings have to comply with the server settings.
Note
NLA requires to enable Automatic Login above.

Public Host Key
*(only with bookmark type SSH, FTPS or SFTP)*
Add the public key of the SSH host.

Init Remote Folder
*(only with bookmark type FTP, FTPS, SFTP or SMB)*
Specify the remote directory path.

Note
After successful authentication the user is redirected to the path on the remote server.

Authentication Method
*(only with bookmark type SFTP)*
Select the authentication method. You can either provide the Password for the selected username or add the Private Key for the SFTP connection.

Share Session
Select this option to allow users to use the connection simultaneously and see the same screen.

Description
Enter a description or other information.
3. Click **Save** to save your settings.

The bookmark is now available and appears in the **Bookmark** list.

To either edit or delete a bookmark, click the corresponding buttons.

**Bookmark Groups**

This page displays all bookmark groups. You can update a group to include bookmarks as group members. Single bookmarks can be member of multiple groups. You are not allowed to delete groups which contain bookmarks which are part of any of the SSL VPN policies.

**Device Configuration > Configure > VPN > Bookmark Group**

You can add new groups, update or delete them. Following is a description of the table elements:

**Name**

Displays the name of the bookmark group.

**Description**

Displays the description of the bookmark group.

**Manage**

Displays the available managing options for the bookmark group:

- **Edit**: Allows you to edit the bookmark group.
- **Delete**: Allows you to delete the bookmark group.

To either add or delete a bookmark group, click the corresponding buttons.
Related tasks
Add a clientless access policy (page 212)

Add a Bookmark Groups
This page describes how to add a bookmark group.

1. Go to Device Configuration > Configure > VPN > Bookmark Groups and click Add.
2. Enter values for the following settings:

   **Name**
   Enter a descriptive name for the bookmark group.

   **Select Bookmark**
   Select the bookmark(s) you want to add to the new bookmark group from the Bookmark List.

   **Description**
   Enter a description or other information.

![Figure 157: Add Bookmark Group](image)

3. Click Save to save your settings.

   The bookmark group is saved. It appears in the Bookmark Groups list.

   To either edit or delete a bookmark group, click the corresponding buttons.

### 3.5.2 Network

Network objects let you enhance security and optimize performance for devices behind the firewall. You can use these settings to configure physical ports, create virtual networks, and support Remote Ethernet Devices. Zones allow you to group interfaces and apply firewall rules to all member devices. Network redundancy and availability is provided by failover and load balancing. Other settings allow you to provide secure wireless broadband service to mobile devices and to configure advanced support for IPv6 device provisioning and traffic tunnelling.

**RED Device Management**

RED Device Management page allows you to view and manage added RED devices. To add new or manage added RED devices go to Device Configuration > Configure > Network > RED Device Management page.

The following options are available:
Status
The toggle switch next to the branch name shows the status of the RED device. Click it to turn it on/off.

Edit
This link leads you to the page where you can edit the RED device settings. Find further descriptions on the Add RED page.

Delete RED
With this option you can delete the RED devices from the list. You will get a message which configurations that the deletion will affect.

Related tasks
Add RED (page 226)

Add RED
You can configure RED from this page.
1. Ensure that RED is activated. This can be done from Configure > System Services > RED.
2. Go to Device Configuration > Configure > Network > RED Device Management and click Add.
3. Enter the RED settings.

Branch Name
Enter the name for the remote location where the RED will be set up.

Type
Select the client type from the drop-down list depending on the type of RED device you want to connect:
• RED 10
• RED 15
• RED 15w
• RED 50
• Firewall-RED-Server
• Firewall-RED-Client
• Firewall RED Server Legacy
• Firewall RED Client Legacy

Note
Firewall RED Server Legacy and Firewall RED Client Legacy are used to connect Sophos XG Firewall and Sophos UTM via RED Site2Site.

Using Firewall-RED-Server and Firewall-RED-Client you can configure a RED Site-to-Site tunnel between two SF devices which are connected through the RED technology. One device acts as server while the other is the client.
For more information, refer Configure RED Site-to-Site Tunnel (page 232).

**Firewall Device**
Select the firewall device from the list of available devices.

**RED ID**
Enter the RED ID.
The RED ID is a 15-character string printed on a sticker located on the back of the RED. If you do not want to open the package, you can also find it on the outer carton sticker.

**Tunnel ID**
Enter the Tunnel ID.
By default, **Automatic** is selected, this will number tunnels consecutively.

**Unlock Code (optional)**
Enter the unlock code.
The Unlock code is an 8-character string that is generated when a RED is added to a SF. If this RED is now being deployed for the first time, the unlock code is not required. If this RED has been deployed before, you will need to enter the unlock code here. The unlock code is generated during the deployment of a RED device, and is emailed instantly to the address you provided by activating RED. is emailed instantly to the address you provided for activating RED. This is a security feature, which ensures that a RED device cannot simply be removed and installed elsewhere.

For manual deployment via USB stick and automatic deployment via Provisioning Service (see below), two separate unlock codes are generated. If you switch a RED device from one deployment method to the other, make sure to use the corresponding unlock code: For manual deployment, provide the unlock code of the last manual deployment; for automatic deployment, provide the unlock code of the last automatic deployment.

**2nd Firewall/Hostname (only applicable for client types RED 15 and RED 50)**
Enter the hostname of the second Sophos XG Firewall.

**Use 2nd IP/Hostname for (only applicable for client types RED 15 and RED 50)**
Select from the following options:
- **Failover**: Select this option if you want to use the second Sophos XG Firewall in case the primary Sophos XG Firewall fails. The second host will then take over automatically without loss of connection.
- **Load Balancing**: Select this option if you want to distribute traffic equally on both, the primary and the second Sophos XG Firewall.

**Firewall IP /Host Name**
Enter the hostname of the SF.
The SF hostname must be a publicly resolvable DNS name or IP address for this SF. The RED will use this name or IP to connect back to the SF.

**Description (optional)**
Enter a description for the RED settings.

**Device Deployment**
Select the deployment method:
- **Automatically via Provisioning Service**
- **Manually via USB Stick**
**Note**
If you select manual deployment, it is extremely important to keep the unlock code, which is sent by email. If you lose the unlock code, you can never again connect the RED device to another SF.

By default, the SF provides the RED's configuration data automatically via Sophos' RED

- Manually via USB Stick

**Note**
If you select manual deployment, it is extremely important to keep the unlock code, which is sent by email. If you lose the unlock code, you can never again connect the RED device to another SF.

By default, the SF provides the RED's configuration data automatically via Sophos' RED Provisioning Service. In this case, the RED device receives its configuration via Internet. If for example your RED does not have an Internet connection, you can provide the configuration manually, via USB stick. If you deploy a RED device manually, you have to ensure that SF is acting as NTP server. Therefore activate NTP on the SF and allow the correct network or at least the IP address of the RED.

Figure 158: RED Setting

4. Enter the uplink settings.

**Uplink Connection**
Select the connection type for the uplink:

- **DHCP**: The RED pulls an IP address from a DHCP server.
- **Static**: Enter an IPv4 address, a corresponding netmask, a gateway and a DNS server.

**3G/UMTS Failover**
Enable/disable the 3G/UMTS failover function.
Note
The RED device offers a USB port, where you can plug in a 3G/UMTS USB stick. If selected, this stick can serve as Internet uplink failover in case of a WAN interface failure. For the necessary settings please refer to your Internet provider's data sheet.

- **Mobile Network**: Select the mobile network type, which is either GSM or CDMA.
- **Username/Password (optional)**: If required, enter a username and password for the mobile network.

Note
Available only for **CDMA** Mobile Network.

- **PIN (optional)**: Enter the PIN of the SIM card if a PIN is configured.

Note
If you enter a wrong PIN, in case of a WAN interface failure, the connection via 3G/UMTS cannot be established. Instead, the **3G/UMTS Failover** checkbox of the RED device will automatically be unselected. Thus, the wrong PIN will only be used once. When the WAN interface comes up again, a warning will be displayed for the RED device: *A wrong PIN was entered for 3G/UMTS failover uplink. Please change the login data.* When you open the **Edit RED** dialog box, a message is displayed which tells you that the 3G/UMTS failover was automatically unselected. Correct the PIN before selecting the checkbox again. Please note that after three connection attempts with a wrong PIN, the SIM card will be locked. Unlocking cannot be done via the RED device or the SF.

Note
Available only for **GSM** Mobile Network.

- **APN (only with **GSM**)**: Enter your provider's access point name information.
- **Dial String (optional)**: If your provider uses a different dial string, enter it here. Default is *99# for GSM and #777 for CDMA.

![Uplink Settings](image)

Figure 159: Uplink Settings

5. Enter the RED network settings.

**RED Operation Mode**

You can define how the remote network will be integrated into your local network:

- **Standard/Unified**: The SF completely controls the network traffic of the remote network. Additionally, it serves as DHCP server and as default gateway. All remote network traffic will be routed through the SF.
• **Standard/Split**: The SF completely controls the network traffic of the remote network. Additionally, it serves as DHCP server and as default gateway. In contrast to the Unified mode, only certain traffic will be routed through the SF. Define local networks in the Split Networks box below which can be accessed by remote clients.

  **Note**
  VLAN tagged frames cannot be handled with this operation mode. If you use a VLAN behind your RED device, use the standard operation mode instead.

• **Transparent/Split** The SF does not control the network traffic of the remote network, it does neither serve as DHCP server nor as default gateway. On the contrary, it pulls an IP address from the DHCP server of the remote network to become a part of that network. However, you can enable access for remote clients to your local network. For that you need to define Split Networks that are allowed to be accessed by the remote network. Additionally, you can define one or more Split Domains to be accessible. If your local domains are not publicly resolvable, you need to define a Split DNS Server, which can be queried by remote clients.

  **Note**
  VLAN tagged frames cannot be handled with this operation mode. If you use a VLAN behind your RED device, use the standard operation mode instead.

**RED IP**

*Not for Transparent/Split*

Enter the IP address of the RED device.

**RED Netmask**

*Not for Transparent/Split*

Select the netmask from the drop-down menu.

**Zone**

Select the requested zone:

• LAN
• DMZ
• VPN
• WiFi

**Configure DHCP**

Enable if you want to configure a DHCP range for RED.

**RED DHCP Range**

*Only if Configure DHCP is enabled*

Enter the DHCP range.

**Split Network**

*Not for Standard/Unified*

Add one or more split networks.
Note
Only traffic targeted to networks listed in the **Split Network** box is redirected to your local SF. All traffic not targeted to the defined split networks is directly routed to the Internet. Example: You have a branch office and you want it to have access to your local intranet or you want to route traffic of the remote network via your SF for security reasons, e.g. to have the traffic checked for viruses or to use an HTTP proxy.

**Split Domains**

*(only for Transparent/Split)*

Add one or more split domains.

Note
Since the SF is only a client of the remote network, routing traffic to the split networks the same way as with the other modes is not possible. Therefore, the RED device intercepts all traffic: Traffic targeting to a network listed in the **Split Network** box or going to a domain listed in the **Split Domain** box is redirected to the SF interface. This is accomplished by replacing the default gateway's MAC address in the respective data packets with the SF's MAC address. Example: There is a partner or a service provider who should have access to your intranet or a certain server in your local network. Using a RED device, that partner's network will stay completely independent of your network, but they can access a defined part of your network for certain purposes, as if they were connected via LAN.

**MAC Filtering Type**

To restrict the MAC addresses allowed to connect to this RED device, select **Blacklist** or **Whitelist**. With **Blacklist**, all MAC addresses are allowed except those listed on the MAC address list selected below. With **Whitelist**, all MAC addresses are prohibited except those listed on the MAC address list selected below.

**MAC Address:** The list of MAC addresses used to restrict access to the RED device. MAC address lists can be created on the **Objects > Host and Services > MAC Host** page. Note that for RED 10, a maximum of 200 MAC addresses is allowed, whereas for RED 50, the list may contain up to 400 MAC addresses.

Note
- MAC filtering only works for RED rev. 2 or newer.
- If no MAC Addresses are configured then "No Configured MAC address lists found" will be displayed.

**Tunnel Compression**

Enabling tunnel compression will compress all traffic that is sent through the RED tunnel. Data compression might increase the throughput of the RED device in areas with a very slow Internet connection such as 1-2 Mbps. However, any performance increase mainly depends on the entropy of the data being sent (for example, already compressed data such as HTTPS or SSH cannot be compressed any further). In some circumstances it might therefore be possible that enabling data compression could actually reduce the throughput of the RED device. In that case, please disable data compression.
Configure RED Site-to-Site Tunnel

This page describes how to set up a RED Site-to-Site Tunnel.

For such a connection, you need a RED server and a RED client. Ensure that RED is activated on client and server devices. Go to Device Configuration > Configure > System Services > RED and enable RED for client and server devices.

1. Configure the Firewall RED server on the server machine.
   a) Go to Device Configuration > Configure > Network > RED Device Management, and click Add.
   b) Specify Branch Name.
   c) Select Type as "Firewall-RED-Server".
   d) Select Firewall Device.
   e) Select Tunnel ID. It is recommended to set it to “Automatic”. Ensure that both ends of the tunnel use the same tunnel ID.
   f) Specify Description.
   g) As RED IP, enter the LAN IP of the new RED server interface.
   h) Select RED Netmask.
   i) Select Zone.
   j) Enable Tunnel compression if required.

Figure 160: RED Network Setting

Note
Tunnel compression is not available for RED 10 rev.1.

6. Click Save to save your settings.

The RED interface is created and appears in the RED Device Management list.
k) Click **Save**.
The RED interface will be created and listed on the **RED Device Management** page.
l) On the new RED interface, click the icon and select **Download Provisioning File**.

2. Configure the Firewall RED Client on the client machine.
   a) Go to **Device Configuration > Configure > Network > RED Device Management**, and click **Add**.
   b) Specify **Branch Name**.
   c) Select **Type** as “Firewall-RED-Client”.
   d) Select **Firewall Device**.
   e) As **Firewall IP/Hostname** specify the IP address of the machine on which the Firewall RED Server was defined.
   f) Upload the **Provisioning File** downloaded after configuring Firewall-RED-Server.
   g) Specify **Description**.
   h) As **RED IP**, enter the LAN IP of the new RED client interface.
   i) Select **RED Netmask**.
   j) Select **Zone**.
   k) Click **Save**.
The RED interface will be created and listed on the **RED Device Management** page.

   The RED interface will be created and listed on the **RED Device Management** page.

**Add RED Tunnel Wizard**
This page describes how to set up a RED Site-to-Site Tunnel using wizard.

For such a connection, you need a RED server and a RED client. Ensure that RED is activated on client and server devices. Go to **Device Configuration > Configure > System Services > RED** and enable RED for client and server devices.

1. Configure the RED Server.
   a) Go to **Device Configuration > Configure > Network > RED Device Management**, and click **Add RED Wizard**.
   b) Specify **Branch Name**.
   c) Select **Type** as “Firewall-RED-Server”.
   d) Select **Firewall Device**.
   e) Select **Tunnel ID**. It is recommended to set it to “Automatic”. Ensure that both ends of the tunnel use the same tunnel ID.
   f) Specify **Description**.
   g) As **RED IP**, enter the LAN IP of the new RED server interface.
   h) Select **RED Netmask**.
   i) Select **Zone**.
   j) Enable **Tunnel compression** if required.
   k) Click **Next** to generate Provisioning File.

2. Provisioning File generation.
a) The generation of Provisioning File will start automatically after you Click Next in the RED Server section.

b) The Provisioning File will be attached to the RED Client in the next step automatically after the generation process is over.

c) Click Continue to configure RED Client.

3. Configure the RED Client.
   
a) Specify Branch Name.

b) Select Type as "Firewall-RED-Client".

c) Select Firewall Device.

d) As Firewall IP/Hostname specify the IP address of the machine on which the Firewall RED Server was defined.

e) Upload the Provisioning File downloaded after configuring Firewall-RED-Server.

f) Specify Description.

g) As RED IP, enter the LAN IP of the new RED client interface.

h) Select RED Netmask.

i) Select Zone.

j) Click Finish.

The RED Site-to-Site tunnel will be established and active.

Zones

A zone is a grouping of interfaces. Zones also specify the services that can be used to administer devices and authenticate users. When used with firewall rules, zones provide a convenient method of managing security and traffic for a group of interfaces.

Table 6: Default zones

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN</td>
<td>Groups interfaces with different network subnets so that you can manage them as a single entity. By default, traffic to and from this zone is blocked. However, traffic between ports within the same zone is allowed.</td>
</tr>
<tr>
<td>DMZ</td>
<td>(De-militarized zone) Use for publicly accessible servers. You can group physical ports in this zone.</td>
</tr>
<tr>
<td>WAN</td>
<td>Use for internet services.</td>
</tr>
<tr>
<td>VPN</td>
<td>Use for simplifying secure, remote connectivity. When a VPN connection is established, the interface used by the connection is automatically added to this zone.</td>
</tr>
<tr>
<td>WiFi</td>
<td>Use for wireless internet services.</td>
</tr>
</tbody>
</table>

Adding a Zone

Use the Add page to create a new Zone.

The Add Zone page allows you to enter zone details.

1. Go to Device Configuration > Configure > Network > Zones and click Add.

2. Enter the zone details.
Name
Provide a name to identify the zone.

Type
Select the type of Zone from the available options. **LAN** - Depending on the device in use and network design, one can group one to six physical ports in this zone. Group multiple interfaces with different network subnets to manage them as a single entity. Group all the LAN networks under this zone.

By default the traffic to and from this zone is blocked and hence the highest secured zone. However, traffic between ports belonging to the same zone will be allowed.

**DMZ (DeMilitarized Zone)** - This zone is normally used for publicly accessible servers. Depending on the device in use and network design, one can group one to five physical ports in this zone.

**Note**
By default, entire traffic will be blocked except LAN to Local zone service likes Administration, Authentication, and Network.

Members
Displays all the member ports.
Click the checkbox to select the ports. All the selected ports are moved to ‘Selected port’ list.

Description
Provide the description for the zone.

Device Access
Device access defines the type of administrative access permitted on zone.

**Admin Services** - Enable Administrative Services that should be allowed through Zone:
- **HTTP** - Allow HTTP connection to the Admin Console through this zone
- **HTTPS** - Allow secure HTTPS connection to the Admin Console through this zone
- **Telnet** – Allow Telnet connection to CLI through this zone
- **SSH** – Allow SSH connection to CLI through this zone

**Authentication Services** – Enable Authentication Services that should be allowed through Zone:
- Windows/Linux Client
- Captive Portal
- NTLM
- Radius SSO

**Network Services** - Enable Network Services that should be allowed through Zone:
- **DNS** – Allow this zone to respond to DNS requests
- **Ping/Ping6** – Allow this zone to respond to pings

**Other Services** - Enable other Services that should be allowed through Zone:
- **Web Proxy**
- **SSL VPN**

3. Click **Save** to add Zone with the options you have configured.
Note
- If DMZ uses Private IP Address, use NATing to make them publicly accessible.
- One cannot add zone if the device is deployed as Bridge.
- Local and VPN zone cannot be updated or deleted.

**DNS**

Use DNS page to configure the DNS settings of the Device.

DNS server is configured at the time of installation. You can add additional DNS servers to which device can connect for name resolution. If multiple DNS are defined, they are queried in the order as they are entered.

Note
You can also view and manage the DNS server status on the Monitor and Analyze > Diagnostics > Services page.

When you want external domains names to be resolved through internal DNS Servers in your network, you can add routes to such Servers. This will decrease the Internet traffic over the network and speed up DNS Client requests as queries will not be forwarded outside the network. Also, DNS information would be less exposed on the Internet thus enhancing security.

**IPv4**

**Obtain DNS from DHCP**
Click to override the device DNS with the DNS address received from DHCP server.
Option is available if enabled from Network Configuration Wizard or if a DHCP interface is configured.

**Obtain DNS from PPPoE**
Click to override the device DNS with the DNS address received from PPPoE server.
Option is available if enabled from Network Configuration Wizard or if a DHCP interface is configured.

**Static DNS**
Select to provide static IPv4 DNS server address.
A maximum of three static DNS IPv4 addresses can be provided.

**IPv6**

**Obtain DNS from DHCP**
Click to override the device DNS with the DNS address received from DHCP server.
Option is available if enabled from Network Configuration Wizard or if a DHCP interface is configured.

**Static DNS**
Select to provide static IPv6 DNS server address.
A maximum of three static DNS IPv6 addresses can be provided.

DNS Query Configuration

Choose server based on incoming requests record type
Select to choose the DNS server to be used for resolving the domain name on the basis of the incoming requests record type. Incoming request can be of A or AAAA type.

Choose IPv6 DNS server over IPv4
Select to first choose IPv6 DNS server for resolving the DNS and then IPv4 DNS Server. If both IPv6 and IPv4 DNS servers are configured, then it first selects IPv6 DNS server for all requests followed by IPv4 DNS server.

Choose IPv4 DNS server over IPv6
Select to first choose IPv4 DNS server for resolving the DNS and then IPv6 DNS Server. If both IPv6 and IPv4 DNS servers are configured, then it first selects IPv4 DNS server for all requests followed by IPv6 DNS server.

Choose IPv6 if request originator address is IPv6, else IPv4
Select to choose IPv6 DNS server if request is received from IPv6 source or choose IPv4 DNS server, if request is received from IPv4 source.

Test Name Lookup
Click and provide IP Address or host name for testing the connectivity with the DNS server.

DNS Host Entry
The DNS Host Entry page displays the list of all the configured host entries. You can filter list based on Host/Domain name. The page provides the option to add, update, or delete the entries.

DNS Request Route
This section displays list of all the configured DNS Request Routes. You can also update the route configuration and delete the routes.

Add a DNS host entry
You can resolve requests for specific host or domain names using DNS host entries. If the host requested by the user matches the DNS host entry, the device resolves the query using the IP address specified.

1. Go to Network > DNS.
2. Scroll to the DNS host entry section and click Add.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host/Domain name</td>
<td>Fully qualified domain name (FQDN) for the host or domain.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Entry type</td>
<td>Type an IP address for the host or select an interface to configure as the host.</td>
</tr>
<tr>
<td>IP address</td>
<td>IP address of the host.</td>
</tr>
<tr>
<td>Time-to-live</td>
<td>Time, in seconds, for which the record retrieved from the host for the requested domain name will be cached.</td>
</tr>
<tr>
<td>Weight</td>
<td>Weight for load balancing the traffic. The device distributes traffic across the links in proportion to the ratio of weights assigned to individual links. The weight determines how much traffic will pass through a particular link relative to the other link(s).</td>
</tr>
<tr>
<td>Publish on WAN</td>
<td>Publish the DNS host entry on the WAN.</td>
</tr>
<tr>
<td>Add reverse DNS lookup for this host entry</td>
<td>Allow the IP address to be resolved to its designated domain name.</td>
</tr>
</tbody>
</table>

The following restrictions apply to reverse DNS lookup:

- If there are multiple hosts resolving to the same IP address, reverse DNS lookup can be configured for only one of the IP addresses.
- Only A, AAAA, and PTR type DNS records are supported.
- Address (A) records point a hostname to an IP address and return a 32-bit IPv4 address.
- AAAA records point a hostname to an IP address and return a 128-bit IPv6 address.
- Pointer records (PTR) are used for reverse lookups. They map the IP address to a hostname.
- Maximum DNS entries supported is 1024.
- If the device interface is used as a DNS in the client system, a query is sent to the configured DNS servers prior to querying the ROOT servers.

4. Click **Save**.

**DNS Request Route**
To configure DNS Request routes to internal DNS Servers.

**Add/Edit DNS Request Route**

**Host/Domain Name**
Specify the domain for which you want to use internal DNS Server.

**Target Servers**
Select DNS Server to resolve the domain specified above. You can also add IP Address from this page.
Maximum of eight IP Addresses can be added.
DHCP Relay

The DHCP Relay Agent allows to place DHCP clients and DHCP servers on different networks. Deploying DHCP in a single segment network is easy. All DHCP messages are IP broadcast messages, and therefore all the computers on the segment can listen and respond to these broadcasts. But things get complicated when there is more than one subnet on the network. This is because the DHCP broadcast messages do not, by default, cross the router interfaces.

The DHCP Relay Agent makes it possible for DHCP broadcast messages to be sent over routers that do not support forwarding of these types of messages. The DHCP Relay Agent enables DHCP clients to obtain IP Addresses from a DHCP server on a remote subnet, or which is not located on the local subnet. If DHCP Relay Agent is not configured, clients would only be able to obtain IP Addresses from the DHCP server which is on the same subnet.

The DHCP Relay page displays list of all the interfaces configured as a relay agent and you can filter the list based on relay agent name and IP Family. The page also provides option to:

- Add a new relay agent
- Update relay agent parameters
- Delete an Agent

Add a DHCP Relay

Using a DHCP relay, you can provide dynamic address allocation for clients that are not on the same subnet as the DHCP server.

1. Go to Network > DHCP and click Add in the Relay section.
2. Type a name.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP version</td>
<td>IP version to be supported by the DHCP relay. Allocation will occur only for the type selected.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface to use for the DHCP server. The firewall listens for DHCP queries on the selected interface.</td>
</tr>
<tr>
<td>DHCP server IP</td>
<td>DHCP servers to which all packets will be forwarded. The active server will service the</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Relay through IPsec</td>
<td>Relay DHCP messages through an IPsec VPN tunnel.</td>
</tr>
</tbody>
</table>

**Note**

The firewall does not support simultaneous DHCPv6 servers and DHCPv6 relay agents.

4. Click **Save**.

### 3.5.3 Routing

This section provides options to configure both static and dynamic routes.

#### Upstream proxy

If your enterprise contains numerous internal branches, an upstream proxy can bundle the requests from the internal network before passing the traffic on to the external network/internet.

This page allows you to configure an upstream proxy for IPv4/IPv6.

**IPv4 parent proxy**

- **Parent proxy**
  
  Click to enable the parent proxy, if the web traffic is intercepted by an upstream gateway.
  
  If enabled, the device forwards all the HTTP requests to the parent proxy server.

- **Domain name/IPv4 address**
  
  Specify a domain name or IPv4 address for the parent proxy.

- **Port**
  
  Specify the port number, which is to be used for the parent proxy.
  
  Default: 3128

- **Username**
  
  Specify a username for authentication.

- **Password**
  
  Specify a password for authentication.

Click **Apply**.

**IPv6 parent proxy**

- **Parent proxy**
  
  Click to enable the parent proxy, if the web traffic is intercepted by an upstream gateway.
  
  If enabled, the device forwards all the HTTP requests to the parent proxy.
**Domain name/IPv6 address**
Specify a domain name or IPv6 address for the parent proxy.

**Port**
Specify the port number to be used for the parent proxy.
Default: 3128

**Username**
Specify a username for authentication.

**Password**
Specify a password for authentication.

Click **Apply**.

**Static Routing**

A route provides the device with the information it needs to forward a packet to a particular destination. A static route causes packets to be forwarded to a destination other than the configured default gateway.

By specifying through which interface the packet will leave and to which device the packet should be routed, static routes control the traffic exiting the device.

Static Routing menu allows configuring IPv4 and IPv6 Unicast Routes.

**IPv4 Unicast Route**
The IPv4 Unicast Route section displays list of all the configured IPv4 unicast routes. You can filter the list based on IP address, gateway, Interface, or distance. The page also provides option to add, update the route configuration and delete the route.

**IPv6 Unicast Route**
The IPv6 Unicast Route section displays list of all the configured IPv6 unicast routes. You can filter the list based on IP address, gateway, Interface, or distance. The page also provides option to add, update the route configuration and delete the route.

**Add unicast route**

1. For an IPv4 unicast route, go to **Routing > Static routing** and click **Add** under **IPv4 unicast route**.
   For an IPv6 unicast route, click **Add** under **IPv6 unicast route**.
2. Enter unicast route details.

**Destination IP/Prefix**
Specify the destination IPv4 or IPv6 address and select the prefix of subnet mask from the drop-down list.

**Gateway**
Specify the gateway IPv4 or IPv6 address. The gateway address specifies the next-hop router to which traffic will be routed.

**Interface**
Select an interface from the drop-down list.

**Distance**
Specify the distance for routing:

- For IPv4

---

Copyright © Sophos Limited 2023

241
3. Click **Save**.
The unicast route has been created and appears on the **Static routing** page.

### 3.5.4 Authentication

You can set up authentication using an internal user database or third-party authentication service. To authenticate themselves, users must have access to an authentication client. However, they can bypass the client if you add them as clientless users. The firewall also supports two-factor authentication, transparent authentication, and guest user access through a captive portal.

**Servers**

On this page you can manage databases and backend servers of external user authentication services. External user authentication allows you to validate user accounts against existing user databases or directory services on other servers of your network.

**Device Configuration > Configure > Authentication > Servers**

Authentication services currently supported are:

- Novell's eDirectory
- Microsoft's Active Directory
- RADIUS
- TACACS+
- LDAP

The page displays all existing authentication servers. You can add an authentication server, update or delete them. Following is a description of the table elements:

- **Name**
  Displays the name of the authentication server.

- **IP**
  Displays the IP address of the authentication server.

- **Port**
  Displays the Port of the authentication server.

- **Type**
  Displays the type of the authentication server.

- **Domain/Admin**
  Displays the domain or admin of the authentication server.

- **Manage**
  Displays the available managing options for the authentication server:
  - **Edit**: Allows you to edit the authentication server.
  - **Delete**: Allows you to delete the authentication server.

To either add or delete a authentication server, click on the corresponding buttons.
Related concepts
Add an External Server (page 243)
On this page you can create one or more authentication servers. Follow the links to create them:

Add an External Server
On this page you can create one or more authentication servers. Follow the links to create them:

Active Directory

Active Directory (AD) is Microsoft's implementation of a directory service and is a central component of Windows 2000/2003 servers. It stores information about a broad range of resources residing on a network, including users, groups, computers, printers, applications, services, and any type of user-defined objects. As such it provides a means of centrally organizing, managing, and controlling access to these resources. The Active Directory authentication method allows you to register Sophos Firewall OS at a Windows domain, thus creating an object for Sophos Firewall OS on the primary domain controller (DC). Sophos Firewall OS is then able to query user and group information from the domain.

Note
Sophos Firewall OS supports Active Directory 2003 and newer.

Add Active Directory Server (page 244)

LDAP

LDAP, an abbreviation for Lightweight Directory Access Protocol, is a networking protocol for querying and modifying directory services based on the X.500 standard. Sophos Firewall OS uses the LDAP protocol to authenticate users for several of its services, allowing or denying access based on attributes or group memberships configured on the LDAP server.

Add LDAP Server (page 245)

RADIUS

RADIUS, the acronym of Remote Authentication Dial In User Service is a widespread protocol for allowing network devices such as routers to authenticate users against a central database. In addition to user information, RADIUS can store technical information used by network devices, such as supported protocols, IP addresses, routing information, and so on. This information constitutes a user profile, which is stored in a file or database on the RADIUS server. The RADIUS protocol is very flexible, and servers are available for most operating systems. The RADIUS implementation on Sophos Firewall OS allows you to configure access rights on the basis of proxies and users. Before you can use RADIUS authentication, you must have a running RADIUS server on the network. Whereas passwords are encrypted using the RADIUS secret, the username is transmitted in plain text.

Add RADIUS Server (page 247)

TACACS+

TACACS+ (the acronym of Terminal Access Controller Access Control System) is a proprietary protocol by Cisco Systems, Inc. and provides detailed accounting information and administrative
control over authentication and authorization processes. Whereas RADIUS combines authentication and authorization in a user profile, TACACS+ separates these operations. Another difference is that TACACS+ utilizes the TCP protocol (port 49) while RADIUS uses the UDPClosed protocol.

Add TACACS+ Server (page 250)

eDirectory

Novell eDirectory is an X.500 compatible directory service for centrally managing access to resources on multiple servers and computers within a given network. eDirectory is a hierarchical, object-oriented database that represents all the assets in an organization in a logical tree. Those assets can include people, servers, workstations, applications, printers, services, groups, and so on.

Add eDirectory Server (page 249)

Add Active Directory Server

Use the Add External Server page to configure Active Directory Server settings.

The Add External Server page allows to configure Active Directory which in turn allows the device to map the users and groups from ADS for the purpose of authentication.

1. Go to Device Configuration > Configure > Authentication > Authentication Server and click Add.
2. On the Add External Server page, select Active Directory for Server Type. If a user is required to authenticate using ADS, the device needs to communicate with the ADS server for authentication.
3. Enter Active Directory details.

Server Name

Enter a descriptive name for the Active Directory server.

Server IP/Domain

Enter an IP address or domain for the Active Directory server.

Port

Enter the port of the Active Directory server. By default, this is port 389.

NetBIOS Domain

Enter a NetBIOS domain for the Active Directory server.

ADS Username

Enter a username for the admin user of the Active Directory server.

Password

Enter a password for the admin user of the Active Directory server.

Connection Security

Select the type of security to be implemented on the established connection. It provides a method to login to the external server by sending the username and password in encrypted format instead of clear text. We strongly recommend using the encryption method to protect user credentials.

- **Simple:** User credentials will be send unencrypted, for example, as clear text.
- **SSL:** Secure Sockets Layer. This is the most common method used for secured connection. The Port will then change from 389 (LDAPClosed) to 636 (ldaps = LDAP over SSL).
- **TLS:**

Validate Server Certificate
(not with Simple connection security)
Enable to validate the certificate on the external server.

Display Name Attribute
(optional)
Enter the name for the AD server which is displayed as AD username.

Email Address Attribute
(optional)
Enter the alias for the configured email address which is displayed to the user.

Domain Name
Specify the domain name for which the query is to be added.

Search Queries
Click Add to enter the search query. Use the Move Up and Move Down buttons to move the search queries in the list. Use Remove to remove the selected item.

If you do not know search DN, refer to NetBIOS name, FQDN and Search DN.

Figure 162: Add External Server

4. Click Test Connection to check the connectivity between Active Directory server and the Sophos XG Firewall. It also validates Active Directory server user credentials.

5. Click Save.

The AD server is now available and appears in the Authentication Server list.

Add LDAP Server
This page describes how to add a LDAP server.
1. Go to **Device Configuration > Configure > Authentication > Authentication Server** and click **Add**.
2. Select the server type **LDAP Server**.
3. Enter values for the following settings:

**Server Name**
- Enter a descriptive name for the LDAP server.

**Server IP/Domain**
- Enter an IP address or domain for the LDAP server.

**Port**
- Enter the port of the LDAP server. By default, this is port 389.

**Version**
- Select the version of the LDAP server.

**Anonymous Login**
- Enable to send anonymous requests to the LDAP server. Disable to bind user with the server.

**Username** *(not with Anonymous Login)*
- Enter a name for the bind user.

**Password** *(not with Anonymous Login)*
- Enter a password for the bind user.

**Connection Security**
- Select the connection security for the LDAP server:
  - **Simple**: User credentials will be send unencrypted, for example, as clear text.
  - **SSL**: Secure Sockets Layer. This is the most common method used for secured connection. The **Port** will then change from 389 (LDAPClosed) to 636 (ldaps = LDAP over SSL).
  - **TLS**: Transport Layer Security. Same secure connection as SSL but uses the default port.

**Validate Server Certificate** *(not with Simple Connection Security)*
- Enable to validate the certificate on the external server.

**Client Certificate**
- Select a client certificate from the list to establish a secured connection. If you do not want a client certificate, select **None**.

**Note**
- You can manage client certificates under **Objects > Identity > Certificate**.

**Base DN**
- Enter the Base DN for the LDAP server. The Base DN is the starting point relative to the root of the LDAP tree where the users are included who are to be authenticated. Note that the Base DN must be specified by the Fully Distinguished Name (FDN) in LDAP notation, using commas as delimiters (e.g., O=Example,OU=RnD).

**Get Base DN**
Click **Get Base DN** if you are not aware about the Base DN. The Base DN is automatically retrieved from the directory.

**Authentication Attribute**

Enter an authentication attribute for searching the LDAP directory. The user authentication attribute contains the actual login name each user is prompted for, for example by remote access services.

**Display Name Attribute**

Enter the name for the LDAP server which is displayed as LDAP username.

**Email Address Attribute**

Enter the alias for the configured email address which is displayed to the user.

**Group Name Attribute**

Enter the alias for the configured group name which is displayed to the user.

**Expire Date Attribute**

Enter the user expire date displayed to the user. The attribute specifies how long a user account is valid.

![Figure 163: Add External Server](image)

4. Click **Test Connection** to check the connectivity between LDAP and the Sophos Firewall OS. It also validates LDAP user credentials.

5. Click **Save**.

The LDAP server is now available and appears in the **Authentication Server** list.

**Add RADIUS Server**

This page describes how to add a RADIUS server.
1. Go to Device Configuration > Configure > Authentication > Authentication Server and click Add.
2. Select the server type RADIUS Server.
3. Enter values for the following settings:

**Server Name**
- Enter a descriptive name for the RADIUS server.

**Server IP**
- Enter an IP address for the RADIUS server.

**Authentication Port**
- Enter the authentication port of the RADIUS server. By default, this is port 1812.

**Enable Accounting**
- Enable accounting on RADIUS server.
- Sophos Firewall OS sends the following information to the RADIUS server as soon as the user logs in:
  - Accounting start request
  - User login time
- Sophos Firewall OS sends the following information to the RADIUS server the moment the user logs out:
  - Accounting stop request
  - User logout time

**Note**
- Supported client types: Windows Client, HTTP Client, Linux Client, Android, iOS, iOS HTTP Client, Android HTTP Client, API Client.

**Note**
- The accounting stop message is not sent to the RADIUS server when Sophos Firewall OS shuts down or reboots.

**Accounting Port**
* (only if Enable Accounting is active)
- Enter a RADIUS port number through which the Sophos Firewall OS can communicate with RADIUS.

**Shared Secret**
- Enter the shared secret which is a text string that serves as a password between a RADIUS client and a RADIUS server.

**Group Name Attribute**
- Enter the alias for the configured group name which is displayed to the user.

4. Optional. Click Enable Additional Settings and specify settings.

**NAS-identifier**
- String identifying the NAS originating from access request, for example, an FQDN.

**NAS-port-type**
- Type of the physical port of the NAS which authenticates the user.
Figure 164: Add External Server

5. Click **Test Connection** to check the connectivity between the RADIUS server and the Sophos XG Firewall. It also validates RADIUS server user credentials.

6. Click **Save**.

The RADIUS server is now available and appears in the **Authentication Server** list.

**Add eDirectory Server**

This page describes how to add an eDirectory server.

1. Go to **Device Configuration > Configure > Authentication > Authentication Server** and click **Add**.
2. Select the server type **eDirectory**.
3. Enter values for the following settings:

   **Server Name**
   Enter a descriptive name for the eDirectory server.

   **Server IP/Domain**
   Enter an IP address or domain for the eDirectory server.

   **Port**
   Enter the port of the eDirectory server. By default, this is port 389.

   **Connection Security**
   Select the connection security for the eDirectory server:
   - **Simple**: User credentials will be sent unencrypted, for example, as clear text.
   - **SSL**: Secure Sockets Layer. This is the most common method used for secured connection. The **Port** will then change from 389 (LDAPClosed) to 636 (ldaps = LDAP over SSL).
   - **TLS**: Transport Layer Security. Same secure connection as SSL but uses the default port.

   **Validate Server Certificate**
   *(not with Simple)*
   Enable to validate the certificate on the external server.

   **Client Certificate**
   Select a client certificate from the list to establish a secured connection. If you do not want a client certificate, select **None**.
Note
You can manage client certificates under **Objects > Identity > Certificate**.

### Base DN
Enter the Base DN for the eDirectory server. The Base DN is the starting point relative to the root of the eDirectory tree where the users are included who are to be authenticated. Note that the Base DN must be specified by the Fully Distinguished Name (FDN) in LDAP notation, using commas as delimiters (e.g., O=Example,OU=RnD).

### Get Base DN
Click **Get Base DN** if you are not aware about the Base DN. The Base DN is automatically retrieved from the directory.

![Server Configuration Form]

Figure 165: Add External Server

4. Click **Test Connection** to check the connectivity between the eDirectory server and the Sophos XG Firewall. It also validates eDirectory server user credentials.

5. Click **Save**.

The eDirectory server is now available and appears in the **Authentication Server** list.

### Add TACACS+ Server
This page describes how to add a TACACS+ server.

1. Go to **Device Configuration > Configure > Authentication > Authentication Server** and click **Add**.
2. Select the server type **TACACS+ Server**.
3. Enter values for the following settings:

**Server Name**

Enter a descriptive name for the TACACS+ server.

**Server IP**

Enter an IP address for the TACACS+ server.
Port

Enter the port of the TACACS+ server. By default, this is port 49.

Shared Secret

Enter the shared secret which is a text string that serves as a password between a TACACS+ client and a TACACS+ server.

Figure 166: Add External Server

4. Click Test Connection to check the connectivity between the TACACS+ server and the Sophos Firewall OS. It also validates TACACS+ server user credentials.

5. Click Save.

The TACACS+ server is now available and appears in the Authentication Server list.

Services

This menu allows you to configure Authentication for Firewall, VPN and Admin traffic. You can also configure Global Settings, NTLM Settings, Web Client Settings, Captive Portal parameters and Radius Client settings for Single Sign-On Server.

Note

You can also view and manage the authentication status on the Device Configuration > Monitor and Analyze > Diagnostics > Services page.

Once you have deployed the device, default access policy is automatically applied which will allow complete network traffic to pass through the device. This will allow you to monitor user activity in your Network based on default policy.

As device monitors and logs user activity based on IP Address, all the reports are also generated based on IP Address. To monitor and log user activities based on usernames or logon names, you have to configure the device for integrating user information and authentication process. Integration will identify access request based on usernames and generate reports based on usernames.

When the user attempts to access, the device requests a user name and password and authenticates the user’s credentials before giving access. User level authentication can be performed using the local user database on the device, External ADS server, LDAP, RADIUS or TACACS+ server.

To set up user database

1. Integrate ADS, LDAP, RADIUS or TACACS+ if external authentication is required.
2. Configure for local authentication.
3. Register user
The device provides policy-based filtering that allows defining individual filtering plans for various users of your organization. You can assign individual policies to users, or a single policy to a number of users (Group).

Device detects users as they log on to a Windows domain in your network via client machines. Users are allowed or denied access based on username and password. In order to authenticate a user, you must select at least one database against which device should authenticate users.

To filter the Internet requests based on policies assigned, the device must be able to identify a user making a request.

The administrator can configure authentication based on the type of – Administrator, Firewall, VPN, and SSL VPN with multiple servers.

Below are the screen elements with their description:

**Firewall Authentication Methods**

**Authentication Server List**

Select Authentication server.

Authentication Server List displays all the configured servers while Selected Authentication Server List displays servers that will be used for authentication when the user tries to login.

In case of multiple servers, authentication request is forwarded as per the order configured in the Selected Authentication Server List.

**Default Group**

Select the default group for firewall authentication.

**VPN (IPSec/L2TP/PPTP) Authentication Methods**

**Set Authentication Methods Same As Firewall**

Enable to use the same authentication method as configured for firewall traffic. If enabled all the authentication servers configured for the firewall traffic will be available for VPN traffic authentication configuration.

Authentication Server List displays all the configured servers while Selected Authentication Server List displays servers that will be used for authentication when user tries to login.

Override authentication method for VPN traffic by selecting or deselecting any Authentication server.

In case of multiple servers, authentication request will be forwarded as per the order configured in the Selected Authentication server List.

If RADIUS server authenticates users then PPTP and L2TP connections established using MSCHAPv2 or CHAP protocol can be authenticated through RADIUS.

**Administrator Authentication Methods**

Administrator can configure and manage authentication settings for all the Administrator Users except for the super administrator from this page.

**Set Authentication Methods Same As Firewall**

Select to use the same authentication method as configured for firewall traffic. If enabled all the authentication servers configured for the firewall traffic will be available for administrator traffic authentication configuration.

Authentication Server List displays all the configured servers while Selected Authentication Server list displays servers that will be used for authentication when user tries to login.
Override authentication method for administrator traffic by selecting or deselecting any Authentication server.

In case of multiple servers, authentication request will be forwarded as per the order configured in the Selected Authentication server List.

**Global Settings**

**Maximum Session Timeout**

Specify the timeout duration in minutes.

Acceptable Range (minutes) - 3 to 1440

Authentication Session timeout is the time in minutes a user is logged into the device. Exceeding the period, the user will be logged out automatically and the user must re-authenticate. This is applicable to administrative sessions only.

Enable “Unlimited” to allow the users to remain logged in.

**Simultaneous Logins**

Specify the maximum number of concurrent logins allowed to the user.

Acceptable Range – 1 to 99 concurrent logins

OR

Enable “Unlimited” to allow unlimited concurrent logins to the user.

Login restriction is applicable to only those users who are added after this configuration.

**NTLM Settings**

**Inactivity Time**

Specify the inactivity time in minutes.

User Inactivity timeout is the inactive/idle time in minutes after which user will be logged out and has to re-authenticate.

Acceptable Range (Minutes) - 6 to 1440

Default – 6

**Data Transfer Threshold**

Specify the minimum data to be transferred.

If the minimum data is not transferred within the specified time, the user will be marked as inactive.

Default – 1024 Bytes

**HTTP challenge redirect on Intranet Zone**

Select to Enable or Disable the redirection of NTLM HTTP challenge on Intranet Zone.

When any site hosted on the Internet initiates the NTLM web proxy challenge for authentication, the client is transparently authenticated by the browser through device by sending credentials over the Internet.

To secure and to prevent the user credential from going out on the Internet, device will redirect NTLM authentication challenge on Intranet Zone. Client will be transparently authenticated through device’s Local Interface IP and credentials will be exchanged in Intranet zone only.

Default - Enable

**Web Client Settings (iOS and Android and API)**

**Inactivity Time**
Specify the inactivity time in minutes.

User Inactivity timeout is the inactive/idle time in minutes after which user will be logged out and has to re-authenticate.

Acceptable Range (Minutes) - 6 to 1440
Default – 6 minutes

**Data Transfer Threshold**

Specify the minimum data to be transferred.

If the minimum data is not transferred within the specified time, the user will be marked as inactive.

Default – 1024 Bytes

**SSO using radius accounting request**

Device can authenticate users transparently who have already authenticated on an external RADIUS server. Click to add, to delete or Edit hyperlink to edit Radius Client configurations.

**Radius Client IPv4**

Specify IPv4 Address of Radius Client.

Only request from specified IP Address will be considered for SSO.

**Shared Secret**

Provide Shared Secret for authentication.

Click Show to view the configured Shared Secret.

**Captive Portal Settings**

**Unauthenticated users redirection**

Select "Yes" to redirect the access request of unauthenticated user either to the Captive Portal or Custom Message page.

Select "No" to display "Access Denied" message to unauthorized user.

**Unauthenticated users settings**

Configure where the unauthenticated user access requests should be redirected.

**Available Options:**

- Captive Portal
- Custom Message

Select Captive Portal, if an unauthenticated user access request is to be forwarded to captive portal.

**HTTPS Redirection**

Enable to provide access of the Captive portal page through secure channel.

**User Portal Link**

Enable/Disable to make the “User Portal” link available on the Captive Portal page.
**URL Redirection after Login**
Enable to redirect request to the user requested page or custom page.

**URL to redirect**
If request is to be redirected to the custom page, click **Custom URL** and specify URL, else click **User requested URL**.

**Preserve captive portal after login**
Select “Yes” to minimize the captive portal popup, once the user is successfully authenticated.
Selecting “No” lets the Captive Portal to be displayed on system screen after successful authentication.

**Keep Alive Request For Captive Portal**
Keep-Alive request is constantly exchanged between the device and user to check whether user has logged out or idle. If the device does not receive the response, user is logged out automatically.

More number of concurrent HTTP Captive Portal users, more number of keep-alive requests. In case of more concurrent HTTP Captive Portal users we recommend to disable it.

**User Inactivity Timeout**
User Inactivity timeout is the inactive/idle time in minutes after which user will be logged out and has to re-authenticate.
Enable and specify timeout duration in minutes.
Acceptable Range (minutes) - 3 to 1440
Default - Disable

**Data Transfer Threshold**
Specify threshold value in Bytes for Data Transfer.
If the minimum data is not transferred within the specified time, the user will be marked as inactive.

Select Custom Message, if unauthenticated user is to be displayed custom message.
Enable to publish a link to download the Windows Corporate Client in the custom message.

**Linux Corporate Client Download Link**
Enable to publish a link to download the Linux Corporate Client in the custom message.

**MAC Corporate Client Download Link**
Enable to publish a link to download the MAC Corporate Client in the custom message.

**Page Header Image**
Display the default image shipped with the device at the top of the custom message page or use Browse and upload the custom image.

- Supported Image format - JPG, PNG or GIF
- Size - 700 X 80 pixels

**Page Footer Image**
Display the default image shipped with the device at the bottom of the custom message page or use Browse and upload the custom image.

- Supported Image format - JPG, PNG or GIF
- Size - 700 X 80 pixels

**Custom Message**
Specify message. You can customize the message to include client IP Address, category, and URL.

**Blink Custom Message**
Enable Blink Custom Message to display blinking message.

**Preview**
Preview and check how message will be displayed before saving the configuration.

**SSL VPN Authentication Methods**
Enable to use the same authentication method as configured for VPN or Firewall or configure authentication server for SSL VPN.

**Authentication Server List** displays all the configured servers while **Selected Authentication server** list displays servers that will be used for authentication when user tries to login.

Override authentication method for SSL VPN traffic by selecting or deselecting any Authentication server.

In case of multiple servers, authentication request will be forwarded as per the order configured in the Selected Authentication server List.

**One-time password**
You can implement two-factor authentication using one-time passwords, also known as passcodes. Passcodes are generated by Sophos Authenticator on a mobile device or tablet without the need for an internet connection. When users log on, they must provide a password and a passcode.

**One-time password service**
You can configure two-factor authentication using the one-time password (OTP) service.
• To configure two-factor authentication, click **Settings** and turn on **One-time password**.

**OTP tokens**

To log on using two-factor authentication, users must first obtain a token. Tokens are deployed as a QR code in the user portal. Users scan the code with Sophos Authenticator, which then generates passcodes.

• To automatically create OTP tokens, click **Settings** and turn on **Auto-create OTP tokens for users**.

• To manually create OTP tokens, click **Add** and specify settings. Then, view the token and send it to the user.

• To view the token assigned to a user, click .

• To synchronize the time offset with the server, click and type the passcode.

**Add OTP Token**

This page enables you to add and edit one-time password tokens.

1. Go to **Device Configuration > Configure > Authentication > One-time Password** and click the **Add** button.

2. Specify the following details while adding an OTP token:

**Secret**

This is the shared secret of the user's hardware token or soft token. A hardware token has an unchangeable secret, given by the hardware producer. The soft token is created randomly by Firewall, when **Auto-create OTP tokens for users** is enabled in OTP Settings. The secret should have a hexadecimal format and consist of at least 32 characters.

**User (optional)**

Select the user to whom the token should be assigned.

**Note**

Clientless Users cannot be assigned.

**Description (optional)**

Add a description upto 255 characters. This text will be displayed for the administrator with the QR code. If you define different tokens for one person, e.g., a hardware token and a soft token for the mobile phone, it is useful to enter some explanation here as the user will be displayed all QR codes side by side.

**Use custom token timestep**

If you need another timestep for a token than the default token timestep defined in the OTP Settings section, enable this toggle switch and enter the value. The timestep defined here has to correspond with the timestep of the user's password generation device, otherwise authentication fails.

**Timestep**

Enter the value for the timestep.

Acceptable range: 10 - 300 seconds.
Additional Codes (Available only when editing OTP token)
You can add one-time passwords manually for a token. Click the Plus icon to generate the one-time passwords (maximum 10). These one-time passwords are not time-limited. A one-time password will be deleted automatically when the user has logged in with it.

![Add OTP Token](image)

Figure 167: Add OTP Token

3. Click Save.

The OTP token for the specific user will be created and will appear in the one-time password list on the One-time Password page. Default Status of the token will be enabled.

One-time Password Settings
This page allows you to enable and configure the one-time password service.

1. Go to Device Configuration > Configure > Authentication > One-time Password and click the Settings button.
2. Activate the one-time password service by clicking on the One-time Password ON/OFF switch.
3. Specify the OTP service status.

OTP for all users
If enabled, all users have to use one-time passwords. If only specific users should use one-time passwords, disable this option and select Add New Item and add users or groups from the list.

Auto-Create OTP Tokens for users
If enabled, a QR code for configuring the mobile device software will be presented to the authorized users the next time they log in to the User Portal. For this to work, make sure that the users have access to the User Portal. When a user logs in to the User Portal, the respective token will appear in the OTP Tokens list. Enabling this feature is recommended when you are using soft tokens on mobile devices. If your users only use hardware tokens you should instead disable this option and add the tokens before enabling the OTP feature.

Enable OTP for facilities
Here, you select the SF device facilities that should be accessed with one-time passwords by the selected users. When you select the Auto-create OTP tokens for users option, the User Portal needs to be enabled for security reasons: As the User Portal gives access to the OTP tokens, it should have no weaker protection itself.
Note
When selecting WebAdmin you have to ensure that the selected users have access to the one-time password tokens. Otherwise you may log them out permanently.

4. Specify the timestep settings.

Default token timestep in seconds
To synchronize one-time password generation on the mobile device and on the SFM, the timestep has to be identical on both sides. Some hardware tokens use 60 seconds. Other software OTP tokens use a timestep of 30 seconds which is the default value here. If the timestep does not match, authentication fails.

Acceptable Range: 10 - 300 seconds
Default: 30 seconds

Maximum passcode offset steps
With help of this option you can set the maximum passcode offset steps. This means for example you set 3 steps you restrict the clock of a token to drift no more than 3 timesteps between two logins.

Acceptable range: 0 - 10 steps
Default: 1 step

Maximum initial passcode offset steps
With help of this option you can set the maximum initial passcode offset steps. This means for example you set 10 steps you restrict the clock of a token to drift no more than 10 timesteps between two logins. This option is only applied when the user employs the token for the very first time.

Acceptable range: 0 - 600 steps
Default range: 10 steps
Figure 168: OTP Settings

5. Click **Apply**.
6. Select SF device(s) on which you want to apply this configuration and click **Save**.

The one-time password settings will be saved and immediately applicable.

**Groups**

Groups contain policies and settings that you can manage as a single unit. With groups, you can simplify policy management for users. For example, you may want to create a grouping of settings that specifies a surfing quota and limits the access time for guest users.

- To view the list of members in a group, click **Show group members**.
To add members to a group, click the pencil icon, and then click Add members.

Add a group:
1. Go to Authentication > Groups and click Add.
2. Type a name.
3. Select a type.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Require users to log on using a device with a client component.</td>
</tr>
<tr>
<td>Clientless</td>
<td>Do not require users to log on using a client. Access control is performed through the IP address.</td>
</tr>
</tbody>
</table>

4. Select policies.

**Note**
Policies specified at the user level take precedence over those specified at the group level.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Surfing quota</td>
<td>Access based on a defined period and type. This policy can include a cycle type, hours, validity, and maximum hours.</td>
</tr>
<tr>
<td>Access time</td>
<td>Access or denial based on a defined recurring period.</td>
</tr>
<tr>
<td>Network traffic</td>
<td>Access based on bandwidth usage.</td>
</tr>
<tr>
<td>Traffic shaping</td>
<td>Access based on QoS traffic shaping policy. This policy can include a policy association, priority, and specific limits for uploading and downloading.</td>
</tr>
<tr>
<td>Remote access</td>
<td>Access to be applied to remote users through VPN.</td>
</tr>
<tr>
<td>Clientless</td>
<td>Access to be granted to users using only a browser as a client. This policy can include bookmarks or resources that clientless users are allowed to access.</td>
</tr>
</tbody>
</table>

5. Specify settings.

**Note**
Settings specified at the user level take precedence over those specified at the group level.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarantine digest</td>
<td>Send a list of the email messages held in the quarantine in digest form.</td>
</tr>
<tr>
<td>MAC binding</td>
<td>Require users to log on through specified devices.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>L2TP</td>
<td>Allow access through L2TP connections.</td>
</tr>
<tr>
<td>PPTP</td>
<td>Provide access through PPTP connections.</td>
</tr>
<tr>
<td>Login restriction</td>
<td>Allow access from the specified nodes. You can specify no restriction (any node), named nodes, or a node range.</td>
</tr>
</tbody>
</table>

6. Click **Save**.

**Adding Users to the Existing Groups**

Use **Add Group Member** page to add a user to the existing groups.

This page allows you to add group member to the existing groups.

1. Go to **Device Configuration > Configure > Authentication > Groups**.
2. Select the Group in which you want to add the users by clicking Manage icon in the Manage column.
3. Click Add Member(s) button. A pop-up Add Group Member appears providing list all the users along their details that can be added in the group. To search user filter the list based on Username and/or current group.
4. Select the user you want to add in the group. You can select single or multiple users on a single page.
5. Click **Apply** and click **OK** to confirm adding member in the group.

**Viewing List of Group Members**

Use this page to view group members.

This page displays the list of group members.

1. Go to **Device Configuration > Configure > Authentication > Groups**.
2. Click the Group in which you want to add the users by clicking Manage icon in the Manage column.
3. Click Show Group Member(s) button. A pop-up Group Members appears providing the list all the users with the details who are member of the selected group.
4. Click **Close** or Close icon to close the Group Member pop-up.

**User**

The **User** page displays the list of all the users added in the device.

Users are identified by an IP Address or a Username and assigned to a user group. All the users in a group inherit the policies defined for that group.

Media Access Control (MAC) Address is a unique identifier (hardware address) assigned to a host by the manufacturer for identification and is intended to be immutable. MAC Addresses are 48 bit values that are expressed in 6 byte hex-notation separated by colon for example 01:23:45:67:89:AB.

To improve the security of your network and provide spoofing protection, you can enable User-MAC Address binding. By binding User to MAC Address, you are mapping user with a group of MAC Addresses. It means a user would be able to login through a group of pre-specified machines only making it more difficult for a hacker using random MAC Addresses or spoofing a MAC Address to gain access to your network.
**User types**

Device supports five types of Users:

- Normal
- Clientless
- Single Sign on
- Thin Client User
- WWAN User

Normal User has to logon to the device. Requires client (client.exe) on the User machine or user can use HTTP Client component and all the policy-based restriction are applied.

Clientless does not require client component (client.exe) on the User machines.

Users are automatically logged to the device if Single sign on settings are configured.

Use the given decision matrix below to choose which type of the user should be created.

**Table 7: Decision matrix for adding a User**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Normal User</th>
<th>Clientless User</th>
<th>Single Sign On User</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Login required</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Type of Group</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Normal</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Clientless</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Apply Login restriction</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Apply Surfing Quota policy</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Apply Access Time policy</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Apply Traffic Shaping policy</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Apply Web Filter Policy</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Apply Application Group policy</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Apply Network Traffic policy</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

You can filter the list of user's Name, Username, Group, Web and Application Filter policy applied to the user, and date on which users were added.

**Note**

You can also view and manage live users on the Monitor and Analyze > Current Activity > Live Users page. *(Only at appliance level)*

The page also provides options to:

- Register new user
- Reset User Accounting
Register a user

1. Go to Authentication > Users and click Add.
2. Type a user name to be used for authentication.
3. Type a name.
   
   **Note**
   This is the user record name, not the user name.

4. Type a password to be used for authentication.
5. Select a type.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>End users who are connecting to the internet from behind the firewall.</td>
</tr>
<tr>
<td>Administrator</td>
<td>Users who have access to firewall objects and settings as defined in a profile.</td>
</tr>
</tbody>
</table>

6. Type an email address.

   **Note**
   If a user has been imported from Active Directory, XG Firewall overwrites the email addresses given in user registration with the email addresses given by Active Directory at the time of authentication.

7. Select policies.

   **Note**
   Policies specified at the user level take precedence over those specified at the group level.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>Group to which the user is to be added. The user will inherit all the polices assigned to the group.</td>
</tr>
<tr>
<td>Surfing quota</td>
<td>Access based on a defined period and type. This policy can include a cycle type, hours, validity, and maximum hours.</td>
</tr>
<tr>
<td>Access time</td>
<td>Access or denial based on a defined recurring period.</td>
</tr>
<tr>
<td>Network traffic</td>
<td>Access based on bandwidth usage.</td>
</tr>
<tr>
<td>Traffic shaping</td>
<td>Access based on QoS traffic shaping policy. This policy can include a policy association,</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Remote access</td>
<td>Access to be applied to remote users through VPN.</td>
</tr>
<tr>
<td>Clientless</td>
<td>Access to be granted to users using only a browser as a client. This policy can include bookmarks or resources that clientless users are allowed to access.</td>
</tr>
</tbody>
</table>

8. Specify settings.

Note
Settings specified at the user level take precedence over those specified at the group level.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2TP</td>
<td>Allow access using L2TP. Optionally, specify an IP address to be leased to the user for L2TP access.</td>
</tr>
<tr>
<td>PPTP</td>
<td>Allow access using PPTP. Optionally, specify an IP address to be leased to the user for PPTP access.</td>
</tr>
<tr>
<td>Sophos Connect client</td>
<td>Allow remote access using a configured CISCO VPN client. Optionally, specify an IP address to be leased to the user for CISCO VPN access</td>
</tr>
<tr>
<td>Quarantine digest</td>
<td>Send a list of the email messages held in the quarantine in digest form.</td>
</tr>
<tr>
<td>Simultaneous logins</td>
<td>Number of concurrent sessions that will be allowed for the user. Use the value specified in the global settings or specify a value.</td>
</tr>
<tr>
<td>MAC binding</td>
<td>Require users to log on through the specified devices.</td>
</tr>
<tr>
<td>Login restriction</td>
<td>Allow access from the specified nodes. You can specify no restriction (any node), named nodes, or a node range.</td>
</tr>
</tbody>
</table>

9. For administrator users, click **Administrator advanced settings** and specify settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule for device access</td>
<td>Allow access the device only during the time selected.</td>
</tr>
<tr>
<td>Login restriction for device access</td>
<td>Allow access from the specified nodes. You can specify no restriction (any node), named nodes, or a node range.</td>
</tr>
</tbody>
</table>

10. Click **Save**.

*Reset User Accounting*

This option lets you reset the usage accounting i.e. internet usage time and data transfer of the user.
1. Edit the user account of the user whose data accounting you want to reset by clicking Manage icon in the Manage column.
2. Click **Reset User Accounting** and **OK** button to confirm.

**Note**
You cannot reset user accounting for live user.

**View Usage**
This option lets you view the Internet usage and data transfer usage.
1. Edit the User account of the user whose data usage you want to view by clicking Manage icon under the Manage column.
2. Click **View Usage** button. A pop-up displays information of policies applied on the user account, upload and download data transferred by the user.

**Importing User Information**
The **Import Users** page allows you to add new users by importing user details from the file.
Instead of creating users again in the device, if you already have users detail in a csv file, you can upload csv file.
Click the Import Button to import csv file. Select the complete path for migrating user’s information file.

**csv file format and processing:**
1. Header (first) row should contain field names. Format of header row:
2. Compulsory field: username
3. Optional fields: password, name, group, email address.
4. Fields can be configured in any order.
5. Subsequent rows should contain values corresponding to each field in header row.
6. Number of fields in each row should be same as in the header row.
7. Error will be displayed if data is not provided for any field specified in the header.
8. Blank rows will be ignored.
9. If password field is not included in the header row then it will set same as username.
10. If group name is not included in the header row, administrator will be able to configure group at the time of migration.

**Exporting Users**
Click the **Export** button to export the user details in a csv file. csv file is generated with the following headers: Name, Username, Enc_password, Email Address, and Group.

**Purging Active Directory Users**
This page allows you to purge AD Users.
Click Purge AD Users button to synchronize the device’s Active Directory users with external Active Directory server.
Note

- Purge operation will not interrupt user login/logout and accounting events.
- If HA is configured, user details are deleted from both, the Primary Device as well as Auxiliary Device at the same time.

Change Status

Select a user and click on the **Change Status** button to change the status of the user. If the current status is ‘Active’, the status of the user will change to ‘Inactive’ when clicked on this button and vice-versa.

Clientless users

Clientless users are not required to authenticate using a client to access the internet. Instead, the firewall authenticates these users by matching a user name to an IP address.

- To change user status from active to inactive (and back), select a user and click **Change status**.

Add a single clientless user

1. Go to **Authentication > Clientless users** and click **Add**.
2. Specify settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Name to be used by the user behind the firewall for authentication.</td>
</tr>
<tr>
<td>IP address</td>
<td>IP address for the user.</td>
</tr>
<tr>
<td>Group</td>
<td>Group to which the user is to be added. The user will inherit all the policies assigned to the group.</td>
</tr>
<tr>
<td>Name</td>
<td>User record name.</td>
</tr>
<tr>
<td>Email</td>
<td>User’s email address.</td>
</tr>
<tr>
<td>Quarantine digest</td>
<td>Send a list of the email messages held in the quarantine in digest form.</td>
</tr>
</tbody>
</table>

3. Click **Save**.

Go to **Authentication > Clientless users** and click **Manage** for the user. Specify policies and settings as required.

**Reset User Accounting**

This option lets you reset the usage accounting i.e. internet usage time and data transfer of the user.

1. Edit the user account of the user whose data accounting you want to reset by clicking **Manage** icon in the Manage column.
2. Click **Reset User Accounting** and **OK** button to confirm.
You cannot reset user accounting for live user.

View Usage
This option lets you view the Internet usage and data transfer usage.

1. Edit the User account of the user whose data usage you want to view by clicking Manage icon under the Manage column.
2. Click View Usage button. A pop-up displays information of policies applied on the user account, upload and download data transferred by the user.

Add multiple clientless users

1. Go to Authentication > Clientless users and click Add range.
2. Specify settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From IP</td>
<td>Starting IP address for the range.</td>
</tr>
<tr>
<td>To IP</td>
<td>Ending IP address for the range.</td>
</tr>
<tr>
<td>Group</td>
<td>Group to which all users are to be added. The users will inherit all the policies assigned to the group. You can change the policies applied to the user by editing the user details. Settings specified at the user level take precedence over those specified at the group level.</td>
</tr>
</tbody>
</table>

3. Click Save.

Go to Authentication > Clientless users and click

for each user added. Specify policies and settings as required.

Changing Policies of the Clientless User
This page lets you change the policies configured of the clientless user.

Change the policies applied to the user by updating the user details. If you change the policies for the user, user specific policies will take precedence over user group policies.

1. Go to System > Authentication > Clientless Users or Objects > Identity > Clientless Users.
2. Select the user for which you want to change the policies by clicking Manage icon in the Manage column.
3. Update the user details.

**Username**
Name with which user logs in.

**Name**
Name of the User.

**IP Address**
IP Address (IPv4/IPv6) from which the user logs in.
Group in which user is added. User will inherit all the policies assigned to the group.
Change the group, if required.

Email
Email Address of the user.

Description
Provide the clientless user description.

Internet Usage Time
Displays total Internet usage time information.

4. Update the policy details.

Traffic Shaping
Traffic Shaping policy applied to the user.
Change the policy, if required.
Policy applied here will take the precedence over the group policy.

Quarantine Digest
Configure Quarantine Digest.
Quarantine Digest is an Email and contains a list of quarantined spam messages filtered by the device and held in the user quarantine area. If configured, device will mail the Quarantine Digest every day to the user. Digest provides a link to User My Account from where user can access his quarantined messages and take the required action.

Available Options: Enable - User will receive the Quarantine Digest daily and overrides Group setting. Disable - User will not receive Quarantine Digest and overrides Group setting.

5. Click Save to update the changes made to the user.

Captive Portal

Device provides flexibility to customize the Captive portal Login page. This page can include your organization name and logo.

External users, who need to use authentication services, are required to log in over the Captive Portal once before they get access to the User Portal. External users can access the Captive Portal by browsing to https://<Sophos Device IP Address>:8090. After login, external users have access to the User Portal and are listed on the Device Configuration > Configure > Authentication > User page. External users can access the User Portal by browsing to https://<Sophos Device IP Address> or clicking "Click here for User My Account" on the Captive Portal page.

Below are the screen elements with their description:

General Settings

Logo
Click "Custom" to upload the custom logo and specify Image file name to be uploaded else click “Default”.
Use “Browse” to browse and select the complete path.
The image size should not exceed 125 X 70 pixels.

Logo URL
Provide a URL to be redirected to on clicking the Logo.
Page Title

Provide a title to modify the Page title.
Default - Network Authentication

Login Page Header

Provide the text to be displayed on the Captive Portal login page.

Login Page Footer

Provide message to be displayed in the footer of Captive Portal login page.

Username Caption

Provide label for the textbox to be displayed on the Captive Portal login page.
Default - Username

Password Caption

Provide label for textbox to be displayed on the Captive Portal login page.
Default - Password

Login Button Caption

Provide label for the button to be displayed on the Captive Portal login page.
Default – Login

Logout Button Caption

Provide label for the button to be displayed on the Captive Portal login page.
Default - Logout

User Portal Link Caption

Provide a text to be displayed for User Portal login page link. By clicking the link, user will be directed to the User Portal login page.
Default - Click here for User Portal

Color Scheme

Customize the color scheme of the Captive portal if required. Specify the color code or click the square box to pick the color.

Custom HTML Template

Use Custom HTML Template

Select to fully customize captive portal using custom HTML code.

HTML Text

Provide HTML code to render captive portal according to your requirement. Dynamic contents like banners from external web servers, customizable “Message of the day” box and so on can be integrated in the HTML code.

By default, sample HTML will be displayed.

Note

It is essential to have one HTML div element in the HTML text. Device’s Login box will be placed in this div element.

Preview Button
Click to view the custom settings before saving the changes.

Reset to Default Button
Click to revert to default settings.

Related concepts
Servers (page 242)
On this page you can manage databases and backend servers of external user authentication services. External user authentication allows you to validate user accounts against existing user databases or directory services on other servers of your network.

SophosTransparent Authentication Suite (STAS)

STAS Activation Settings
Enable Sophos Transparent Authentication Suite
Enable or disable Sophos Transparent Authentication Suite.

Activate STAS/Confirm Removal of STAS configuration
Use to apply/remove STAS Activation Configuration.

STAS Settings
Enable User Inactivity
Select to enable or disable user inactivity setting.
When users logs in the Device and performs no activity, remaining idle for specific time span, they are considered inactive. By default, User Inactivity is disabled.

Inactivity Timer (Only if Enable User Inactivity is enabled)
Specify the inactivity time in minutes.
The user inactivity timeout is the inactive/idle time in minutes after which the user will be logged out and has to re-authenticate.
Acceptable Range (Minutes) - 3 to 1440 Default - 3 minutes

Data Transfer Threshold (Only if Enable User Inactivity is enabled)
Specify the minimum data to be transferred. Default - 100 bytes

Apply
Click to apply configuration changes.

Collector
Add
Collector collects the user authentication request from multiple agents, processes the request and sends to SFM for authentication.
Click to add collector IP address and Port for clientless single sign on configuration. Refer Add Collector for details.

VPN Zone Network
Add
Click to add VPN Zone Network. Refer Add VPN Zone Network (page 272) for details.
Add Collector
Use the Add Collectors.

Collector
1. Go to Device Configuration > Configure > Authentication > STAS > Collector and click Add.
2. Enter Collector details:
   - **Collector IP**: Enter IP for Collector.
   - **Collector Port**: Enter port for Collector.
   - **Collector Group**: Enter group for Collector.

![Figure 169: Add Collector](image)

3. Click **Save**.

Add VPN Zone Network
Use this to add VPN Zone Networks.

VPN Zone Network
1. Go to Device Configuration > Configure > Authentication > STAS > VPN Zone Network and click Add.
2. Enter VPN Zone Network details:
   - **Network**: Enter network name for VPN Zone.
   - **NetMask**: Select net mask for VPN Zone.

![Figure 170: VPN Zone Network](image)

3. Click **Save**.

**Guest user details**

Guest users are users who do not have an account and want to connect to your network in order to access the internet. You can add (register) guest users or allow them to register themselves through the guest user portal. Specify policies and settings as required.

- To change a password, click **Change password**.
- To view internet traffic statistics, click **View usage**.
• To reset the internet traffic statistics and restart the user’s network traffic quota, click **Reset user accounting.**

### Policies

**Note**  
Policies specified at the user level take precedence over those specified at the group level.

<table>
<thead>
<tr>
<th>Group</th>
<th>Group to which the user is to be added. The user will inherit all the policies assigned to the group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Surfing quota</td>
<td>Access based on a defined period and type. This policy can include a cycle type, hours, validity, and maximum hours.</td>
</tr>
<tr>
<td>Access time</td>
<td>Access or denial based on a defined recurring period.</td>
</tr>
<tr>
<td>Network traffic</td>
<td>Access based on bandwidth usage.</td>
</tr>
<tr>
<td>Traffic shaping</td>
<td>Access based on QoS traffic shaping policy. This policy can include a policy association, priority, and specific limits for uploading and downloading.</td>
</tr>
<tr>
<td>Remote access</td>
<td>Access to be applied to remote users through VPN.</td>
</tr>
<tr>
<td>Clientless</td>
<td>Access to be granted to users using only a browser as a client. This policy can include bookmarks or resources that clientless users are allowed to access.</td>
</tr>
</tbody>
</table>

### Settings

**Note**  
Settings specified at the user level take precedence over those specified at the group level.

<table>
<thead>
<tr>
<th>L2TP</th>
<th>Allow access using L2TP. Optionally, specify an IP address to be leased to the user for L2TP access.</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPTP</td>
<td>Allow access using PPTP. Optionally, specify an IP address to be leased to the user for PPTP access</td>
</tr>
<tr>
<td>Sophos Connect client</td>
<td>Allow remote access using a configured CISCO VPN client. Optionally, specify an IP address to be leased to the user for CISCO VPN access</td>
</tr>
<tr>
<td>Quarantine digest</td>
<td>Send a list of the email messages held in the quarantine in digest form.</td>
</tr>
<tr>
<td>Simultaneous logins</td>
<td>Number of concurrent sessions that will be allowed for the user. Use the value specified in the global settings or specify a value.</td>
</tr>
</tbody>
</table>
MAC binding

Require users to log on through the specified devices.

Login restriction

Allow access from the specified nodes. You can specify no restriction (any node), named nodes, or a node range.

Configure an SMS gateway

1. Go to Authentication > Guest user settings, scroll to SMS gateway, and click Add.
2. Type a name.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>URL of the SMS gateway for sending an SMS request.</td>
</tr>
<tr>
<td>HTTP method</td>
<td>Method for sending an SMS request to the SMS gateway. Select Get to request data from a specified resource. Select Post to submit data to be processed by a specified resource.</td>
</tr>
<tr>
<td>Cell number format</td>
<td>Use country code with cell number.</td>
</tr>
<tr>
<td>Number prefix</td>
<td>Prefix to be used with the cell number. Can include alpha-numeric and ASCII special characters.</td>
</tr>
</tbody>
</table>

4. Enter request parameters specified by your service provider.

If the request URL is

http://www.example.com/sms.aspx?
user=joey&pass=joey123&mbno=9792234567&msg=Test

then the request parameters are

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>joey</td>
</tr>
<tr>
<td>pass</td>
<td>joey123</td>
</tr>
<tr>
<td>mbno</td>
<td>9792234567</td>
</tr>
<tr>
<td>msg</td>
<td>Test</td>
</tr>
</tbody>
</table>

5. Enter the response format specified by your service provider.

If the response received is

status=302&message=Limit Exceeded

then the response format should be

status={0}&message={1}

6. Enter the response parameter specified by your service provider.

If the response format is

status={0}&message={1}
then the response parameters are

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>status</td>
</tr>
<tr>
<td>1</td>
<td>message</td>
</tr>
</tbody>
</table>

7. Click **Save**.

Click **Test connection** and type a mobile phone number. If you are able to connect to the gateway, you will receive an SMS message.

**Testing Connectivity with SMS Gateway**

Once you configure SMS Gateway, check whether you are able to connect with the gateway or not from this page.

1. Go to **Device Configuration > Configure > Authentication > Guest User Settings > SMS Gateway** and click **Test Connection**.
2. Enter Cell Phone Number details.

**Cell Phone Number**

- Provide cell phone number.

You will receive SMS through the gateway configured if you are able to connect to the gateway.

### 3.5.5 System Services

System Services allows configuration of device components along with the associated services.

**Available Configurations:**

- **Security Heartbeat** - Allows to configure Heartbeat settings.
- **Web Proxy** - Web proxy is the engine used to enforce web protection policies.
- **Authentication Services** - Authentication allows to configure profile attributes for Firewall, VPN and Administration servers. You can also configure NTLM settings, Captive Portal parameters, Web Client settings, Radius Client settings for Single Sign-On Server, global settings like Session Timeout and Simultaneous Logins.
- **Guest User Settings** - Guest User Settings allows configuring general parameters to provide secured internet access for guest user.
- **DoS** - Configure general settings for DoS protection.
- **Web Content Filter** - Allows to configure and manage web filtering through the device, includes scanning and restricting all the HTTP/HTTPS/FTP traffic.
- **Traffic Shaping Settings** - QoS traffic shaping allows network bandwidth to be limited or guaranteed.
- **RED** - Sophos RED allows seamless, encrypted, and tightly integrated connections between branch locations.
- **Wireless** - Allows to configure your firewall to act as a wireless controller for Sophos access points.
- **Advanced Threat Protection** - Allows to enable and configure ATP features to secure ingress and egress traffic.
- **Malware Protection** - Allows to configure Dual Anti Virus Scanning.
Traffic shaping settings

Use these settings to specify maximum bandwidth, traffic optimization, and bandwidth allocation for internet-bound traffic.

- To view bandwidth usage, click **Show bandwidth usage**.

General settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total available WAN bandwidth</strong></td>
<td>Sum of all WAN links’ maximum limits, in KBps.</td>
</tr>
<tr>
<td><strong>Optimize for real-time (VoIP)</strong></td>
<td>Give priority to real-time traffic such as VoIP. If disabled, priority will be applicable only for excess bandwidth, that is, bandwidth remaining after guaranteed bandwidth allocation.</td>
</tr>
<tr>
<td><strong>Enforce guaranteed bandwidth</strong></td>
<td>Handle all internet-bound traffic by the traffic-shaping policy applied to it. If there is no policy applied to the traffic, it will be handled by the default policy.</td>
</tr>
<tr>
<td></td>
<td>Enable this setting if you want to enforce bandwidth restriction on the traffic to which a traffic-shaping policy is not applied.</td>
</tr>
<tr>
<td></td>
<td>Disable this setting if you do not want to enforce a bandwidth restriction on traffic to which a traffic-shaping policy is not applied. (It will handle traffic only on which a traffic-shaping policy is applied.)</td>
</tr>
<tr>
<td><strong>Default policy</strong></td>
<td>Default policy to use for traffic that does not have a traffic-shaping policy applied.</td>
</tr>
<tr>
<td></td>
<td>• Guarantee Minimum bandwidth available to the user.</td>
</tr>
<tr>
<td></td>
<td>• Limit Maximum bandwidth available to the user.</td>
</tr>
<tr>
<td></td>
<td>• Priority Set from 1 (highest) to 7 (lowest) depending on the traffic required to be shaped.</td>
</tr>
</tbody>
</table>

**RED**

A Remote Ethernet Device is a network appliance that provides a secure tunnel between a remote site and the firewall. The RED provisioning service supports RED deployment and provides security options.

- To turn on the RED provisioning service, click the on/off switch, specify details, and click **Apply**.
- To force REDs to use only TLS 1.2, enable **Force TLS 1.2** and click **Apply**. TLS 1.2 is recommended for enhanced security.
Note
For devices to support TLS 1.2, a firmware upgrade may be necessary. Check your device specifications before enabling this option.

• To automatically deauthorize REDs after they have been disconnected, enable **Automatic device deauthorization**, specify a time, and click **Apply**. When a RED attempts to reconnect after being deauthorized, it will be disabled. This option is recommended to prevent unauthorized devices from connecting to the firewall.

Note
This option does not apply to firewall REDs.

**Troubleshooting**

If you receive the message “Registering with RED service failed”, check if you can reach the RED service through telnet. Type the following on the command line:

```
telnet red.astaro.com 3400
```

If you can reach the service, the connection error may be due to high network load. In this case, try connecting again later.

**Configure RED**

This page describes how to configure RED.

1. Go to **Device Configuration > Configure > System Services > RED**.
2. Make the following settings:

**Organization Name**

Enter the name of the organization.

**City**

Enter the city where the organization is located.

**Country**

Select the country where the organization is located.

**Email**

Enter an email address.
Figure 171: RED Configuration

3. Click **Apply to Managed Devices** to apply the settings to managed devices. On clicking **Apply to Managed Devices**, Set Schedule page opens where the settings can be pushed to all or selected devices.

You can enable the **Automatic Device Deauthorization**.

**Related tasks**

Automatic Device Deauthorization (page 278)

**Automatic Device Deauthorization**

When RED is enabled, you can specify if disconnected RED appliances should automatically be deauthorized after a certain time span. With this feature, you can prevent stolen RED appliances from connecting to Sophos XG Firewall.

**Note**

The **Automatic Device Deauthorization** does not work for a RED Tunnel between 2 Sophos XG Firewall Devices.

1. Ensure that RED is activated.
2. Select **Enable** next to **Automatic Device Deauthorization**.
3. Enter a time span for **Deauthorize After**.
4. Click **Apply**.

Automatic Device Deauthorization has been successfully configured.

When a RED appliance reconnects after being disconnected for a time span longer than the defined time span, it will automatically be disabled.

**Malware Protection**

Sophos XG Firewall offers Dual Anti Virus Scanning, wherein traffic is scanned by Two (2) Anti Virus Engines. Traffic is first scanned by the Primary Engine, and then the Secondary Engine.
Note
Dual Anti Virus is not available in Device Models SF100 and SF200. For them, ONLY Single Anti Virus CYREN is available.

Note
You can also view and manage the Anti Virus status on the Device Configuration > Monitor and Analyze > Diagnostics > Services

General Settings

Primary Anti Virus Engine
Select the Primary Anti-Virus Engine to be used for traffic scanning. For Dual Scan, packets are first scanned by the Primary Engine and then by the Secondary Engine. For Single Scan, only the Primary Engine is used.

Available Options
Sophos Engine Avira Engine

Log Settings

Device Configuration > Configure > System Services > Log Settings
Device provides extensive logging capabilities for traffic, system and network protection functions. Detailed log information and reports provide historical as well as current analysis of network activity to help identify security issues and reduce network abuse. To view logs, relevant modules must be subscribed.

Device can log many different network activities and traffic including:

- Security Policies log
- Anti Virus infection and blocking
- Web filtering, URL and HTTP content blocking
- Signature and anomaly attack and prevention
- Spam filtering
- Administrator logs
- User Authentication logs
- SSL VPN logs
- WAF logs
- Advanced Threat Protection logs

Device can either store logs locally or send logs to external syslog servers for storage and archival purposes. Traffic Discovery logs can be stored locally only.

Syslog is an industry standard protocol/method for collecting and forwarding Logs from devices to a server running a syslog daemon usually via UDP Port 514. Logging to a central syslog server helps in aggregation of logs and alerts.

If configured, device sends a detailed log to an external syslog server in addition to the standard event log. Device Syslog support requires an external server running a syslog daemon on any of the
UDP Port. When configuring logging to a syslog server, one needs to configure the facility, severity and log file format. One can also specify logging location if multiple syslog servers are defined.

Device logs all activity and includes every connection source and destination IP Address (IPv4 / IPv6), IP service, and number of bytes transferred.

A Syslog service simply accepts messages, and store them in files or prints. This form of logging is the best as it provides a central logging facility and a protected long-term storage for logs. This is useful both in routine troubleshooting and in incident handling.

Use this page to configure below settings:
- Syslog Servers - Configure Syslog server for logs storage and archival purposes.
- Log Settings - Configure logs to be sent to the Syslog server.

Syslog Servers

The Syslog Servers section displays list of configured syslog servers. You can sort the list based on server name. The page also provides option to add, update, or delete the server.

Log Settings

After configuring syslog server, configure logs to be sent to the syslog server. If multiple syslog servers are configured, you can send various logs on different servers.

To record logs you must enable the respective log and specify logging location. Administrator can choose between On-Device (local) logging or Syslog logging. Administrator can also disable logging temporarily. Below are the screen elements with their description:

Log Type (System)

Security Policy

Security Policy Log records invalid traffic, local ACL traffic, DoS attack, ICMP redirected packets, source routed and fragmented traffic.
- Policy Rules
  Log records the entire traffic for Firewall.
- Invalid Traffic
  Log records the dropped traffic that does not follow the protocol standards, invalid fragmented traffic and the traffic whose packets or device is not able to relate to any connection.
- Local ACLs
  Log records the entire (allowed and dropped) incoming traffic.
- DoS Attack
  The DoS Attack Log records attacks detected and prevented by the device i.e. dropped TCP, UDP and ICMP packets.

To generate logs, go to System > System Services > DoS and click Apply Flag against SYN Flood, UDP Flood, TCP Flood, and ICMP/ICMPv6 Flood individually.

- Dropped ICMP Redirected Packet
  Log records all the dropped ICMP redirect packets.

To generate log, go to System > System Services > DoS and click Apply Flag against Disable ICMP/ICMPv6 Redirect Packet.
• Dropped Source Routed Packet
  Log records all the dropped source routed packets.
  To generate log, go to System > System Services > DoS and click Apply Flag against Drop Source Routed Packets.

• Dropped Fragmented Traffic
  Log records the dropped fragmented traffic.

• MAC Filtering
  Log records the dropped packets when filtering is enabled from Spoof prevention.

• IP-MAC Pair Filtering
  Log records the dropped packets when filtering is enabled from Spoof prevention.

• IP Spoof Prevention
  Log records the dropped packets when filtering is enabled from Spoof prevention.

• SSL VPN Tunnel
  Log records of SSL VPN traffic.

• Virtual Host
  Log records of Virtual Host traffic.

**IPS**
Records detected and dropped attacks based on unknown or suspicious patterns (anomaly) and signatures.

**Anti Virus**
Virus detected in HTTP, SMTP, FTP, POP3, IMAP4, HTTPS, SMTPS, IMAPS and POPS traffic.

**Anti Spam**
SMTP, POP3, IMAP4, SMTPS, POPS, IMAPS spam and probable spam mails.

**Content Filtering**
Web filtering and Application Filtering logs.
Log records of the name of applications/URLs accessed and their categories.

**Note**
To view the logs:
• Web Filter and Application Filter Policies should be applied in Security Policy.
• Log Firewall Traffic under Policies should be enabled.

**Events**
Admin Events: Log records of configurations done through Admin Console.
Authentication Events: Log records of all authentication related events.
System Events: Log records of all system related events like Gateway Up/Down, Anti Virus updates etc.

**WAF**
WAF Events.
Note

Advanced Threat Protection
ATP Events: Log records of drop or alert event.

Heartbeat
Endpoint Status: Log records of the health status of the endpoint.

System Health
Usage: Log records of CPU usage, memory usage, no. of live users, interface and disk partition information.

Sandbox
Sandbox Event: Log records of all Sandstorm events.

Add a syslog server
1. Go to System services > Log settings and click Add.
2. Type a name.
   
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address/domain</td>
<td>IP address or domain name of the syslog server. Logs will be sent to the server.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number for communication with the syslog server.</td>
</tr>
<tr>
<td>Facility</td>
<td>Syslog facility to use for sending logs. The facility indicates the log source, for example, an operating system, process, or application.</td>
</tr>
<tr>
<td>Severity level</td>
<td>Minimum severity level of messages to be logged. For example, select Error to log all messages tagged as error and all messages tagged as critical, alert, and emergency. Select Debug to include all messages.</td>
</tr>
<tr>
<td>Format</td>
<td>Log format.</td>
</tr>
</tbody>
</table>

4. Click Save.

Go to System services > Log settings and select logs.

3.6 System

3.6.1 Profiles

Device Configuration > System > Profiles
Profiles describes the security parameters used for establishing and maintaining a secure connection between two peers.
This section covers the following topics:

- **Schedule** - Schedule defines a time schedule for applying Firewall Rule or Web & Application Filter policy. This page displays a list of schedules and also provides various options to manage it.

- **Access Time** - Schedule Internet access for individual users by defining Access Time policy. This page displays list of all the default as well as custom policies.

- **Surfing Quota** - Control individual user surfing time by defining Surfing Quota policy. This page displays the list of all policies and also provides option to add, update or delete surfing quota policies.

- **Network Traffic Quota** - Limit total as well as individual upload and/or download data transfer by defining Network Traffic Quota. This page displays default as well as custom policies. The page also provides option to manage these policies.

- **Network Address Translation** - The Network Address Translation page displays list of all the NAT policies and you can sort the list based on policy name. The page also provides option to add a new policy, update the parameters of the existing policy, or delete a policy.

- **IPSec** - An IPsec policy defines IKE (Internet Key Exchange) and IPsec proposal parameters of an IPsec connection. This page displays list all the preconfigured and custom IPsec policies. It also provides option to add a new policy, update the parameters of an existing policy, or delete the policy.

- **Intrusion Prevention** - Create and deploy IPS Policies to block malicious or suspicious traffic and increase security and productivity. This page displays the list of all the pre-defined and custom IPS policies.

- **Traffic Shaping** - Traffic Shaping policy allocates & limits the maximum bandwidth usage of the user and controls the web and network traffic. This page displays list of predefined and custom policies and also provides various options to manage it.

- **Web App Protection** - The page displays all existing web application protection objects. The page also provides option to add new protocol security objects, edit or delete them.

- **Web App Authentication** - The page displays all existing web application authentication profiles. The page also provides option to add new application authentication profiles, edit or delete them.

- **Device Access Profile** - This page shows the default and custom profiles and also provides options to manage these profiles.

- **Application Filter** - This page displays list of all the predefined and custom policies. The page also provides option to add a new policy, update parameters of the existing policy, delete a policy, add a filtering rule to a policy or delete a filtering rule attached to a policy.

- **Hotspot Voucher Definition** - This page displays a list of hotspot voucher definition and also provides various options to manage it.

### Schedule

Schedules specify the duration for which rules and policies are in effect. You can create recurring and one-time schedules. You can then apply these to firewall rules, web, application, traffic shaping, and access time policies, and trigger scans for rogue access points. The firewall specifies some commonly used default schedules.

- To edit a schedule, click
To delete a schedule that's in use, apply a different schedule to or delete the rule or policy, then delete the schedule.

Add a schedule

1. Go to Profiles > Schedule and click Add.
2. Type a name.
3. Specify the type of recurrence.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recurring</td>
<td>Use this to control recurring events.</td>
</tr>
<tr>
<td>One-time</td>
<td>Select the start and end dates. Use this to control one-time events, for example, conferences and guest user access.</td>
</tr>
</tbody>
</table>

Note
You can apply one-time schedules only to firewall rules.

4. Specify the timing.

Note
To apply a different start-stop time for different days of the week, click and select the values.

5. Click Save.

For the schedule to take effect, add it to a rule or policy.

Access Time

The Access Time page displays list of all the default as well as custom policies.

Access time is the time period during a day in which user can be allowed/denied the Internet access. An example would be “only office hours access” for a certain set of users.

Access time policy enables to set time interval - days and time - for the Internet access with the help of schedules. See Schedules for more details.

A time interval defines days of the week and times of each day of the week when the user will be allowed/denied the Internet access.

Two strategies based on which Access time policy can be defined:

- Allow strategy - By default, allows access during the schedule
- Deny strategy - By default, denies access during the schedule

Device is shipped with the following predefined policies: Allowed all the time, Denied all the time, Allowed only during Work Hours, Denied during Work hours. These predefined policies are immediately available for use until configured otherwise. You can also define custom policies to define different levels of access for different users to meet your organization’s requirements.
The page also provides option to add, update, or delete the access time policies.

**Note**
Among all the policies applied, device takes into account the policy that first reaches its threshold limit.

**Add an access time policy**

1. Go to **Profiles > Access time** and click **Add**.
2. Type a name.
3. Specify the action for internet access.
   - Allow
   - Deny
4. Specify the schedule during which you want to apply the action.

**Note**
You can apply only recurring schedules to access time policies.

5. Click **Save**.

For the access time policy to take effect, add it to users, groups, or guest users.

**Surfing quotas**

Surfing quotas allow you to control internet access for users using access settings. Quotas specify access on a cyclical (repeat) or non-cyclical (one-time) basis and the access time allowed. The default quotas specify some commonly used quotas such as unlimited access and block-type access.

**Note**
When more than one quota applies to a user, the firewall restricts access according to the first policy that reaches its limit.

- To edit a surfing quota, click **.**

The following quota specifies unlimited access for one week on a one-time basis.
Add a surfing quota

1. Go to **Web > Surfing quotas** and click **Add**.
2. Type a name.
3. Specify a cycle type.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyclic</td>
<td>Repeat access. Specify the cycle hours. Once the specified time ends, the user receives access again. Users receive the time specified at the start of each cycle. Unused time does not carry over.</td>
</tr>
<tr>
<td>Non-cyclic</td>
<td>One-time access. Once the specified time ends, the user will be disconnected.</td>
</tr>
</tbody>
</table>

4. Specify a validity period.
   - Enter the number of days.
   - Select the **Unlimited** check box if you do not want to restrict validity.
5. Specify the maximum hours of access time to be granted by the quota.
   - Enter the hours and minutes. Users will be disconnected after this value has been exceeded even if the validity period of the quota has not yet expired.
   - Select the **Unlimited** check box if you do not want to specify maximum hours.
6. Click **Save**.

Network traffic quota

With network traffic quota policies, you can control data transfer by users and groups. You can specify quotas for total data transfer or individually for upload and download. Quotas can be cyclic and non-cyclic. Cyclic policies can have quotas for the cycle and for maximum traffic. The firewall specifies some commonly used default quotas.

- To edit a network traffic quota policy, click **Profiles Network traffic quota**.

Add network traffic quota policy

1. Go to **Profiles Network traffic quota** and click **Add**.
2. Type a name.
3. Specify the restriction for data transfer.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total network traffic</td>
<td>Quota for total data transfer</td>
</tr>
<tr>
<td>Individual network traffic (Upload &amp; download)</td>
<td>Individual quotas for upload and download</td>
</tr>
</tbody>
</table>

4. Specify a cycle type.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyclic</td>
<td>Quota for each cycle. Unused quota doesn't accumulate and quota is reset for each cycle.</td>
</tr>
<tr>
<td>Non-cyclic</td>
<td>Quota for a single cycle period.</td>
</tr>
</tbody>
</table>

5. Based on the restriction and cycle type, select the cycle period, traffic quota for the cycle, and maximum traffic quota.
Note
If you want to specify maximum traffic quota, clear the check box. Maximum quota must be higher than the cycle quota.

Note
When the user consumes the cycle or maximum traffic quota, the firewall disconnects the user. To reconnect the user, you need to reset user accounting.

6. Click **Save**.

For the network traffic quota policy to take effect, add it to a user or group.

**Network address translation**

With network address translation (NAT) policies, you can allow internal hosts to access the internet through the firewall’s public IP addresses. The firewall maps internal IP addresses to the public IP addresses.

- To edit a NAT policy, click.

**Note**
The default NAT policy automatically masquerades traffic, using the firewall’s WAN IP address.

**Add a NAT policy**

1. Go to **Profiles > Network address translation** and click **Add**.
2. Type a name.
3. Specify an IP address or range or create a new one.
4. Click **Save**.

To apply a NAT policy, add it to a firewall rule.

**Traffic shaping**

Using traffic shaping policies, you can manage bandwidth and prioritize network traffic to reduce the impact of heavy bandwidth usage. Policies specify an association type. For example, you can create policies to be used to restrict bandwidth for users or applications. You can limit the effectiveness of a policy by specifying a schedule.

**Create a traffic shaping policy**

1. Go to **System services > Traffic shaping** and click **Add**.
2. Type a name.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy association</td>
<td>Category to which the policy can be applied. For example, to create a policy that can be applied to users and groups, select Users.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Rule type</td>
<td>Limit User cannot exceed the defined bandwidth limit. Guarantee User is guaranteed the specified bandwidth and can draw on bandwidth up to the specified limit, if available. Allowing users to draw on additional bandwidth can ensure constant service levels during peak periods.</td>
</tr>
<tr>
<td>Limit upload/download separately</td>
<td>Disable Do not enforce separate upload and download limits. Enable Limit upload and download bandwidth according to the values specified.</td>
</tr>
<tr>
<td>Priority</td>
<td>Traffic type to which bandwidth priority is to be allocated. By default, priority is assigned to real-time traffic.</td>
</tr>
<tr>
<td>Tip</td>
<td>To control the default behavior for optimization for real-time traffic, go to System services &gt; Traffic shaping settings. When priority is allocated to real-time traffic, the ability of non-real time policies to receive their guaranteed bandwidth is determined by the bandwidth remaining in the total available bandwidth after real-time policies have been serviced.</td>
</tr>
<tr>
<td>Bandwidth usage type</td>
<td>Individual Allocated bandwidth is only for the user, firewall rule, web category, or application to which this policy is first assigned. Shared Allocated bandwidth is shared among all the users, firewall rules, web categories, or applications that have been assigned this policy.</td>
</tr>
</tbody>
</table>

4. Optional: To specify a schedule for the policy, scroll to the Add schedule section, click Add, and specify details.

5. Click Save.

For the policy to take effect, add it to a user, firewall rule, web category, or application record.

Schedule Traffic Shaping Policy

Use the Add Traffic Shaping (QoS) Policy Detail page to schedule a traffic shaping policy.

The page allows you to add a schedule-wise traffic shaping policy to override default traffic shaping policy details.

1. Go to Device Configuration > System > Profiles > Traffic Shaping.

2. Click on the Manage icon under the Manage column.
3. Click on the **Add** button.

**Name**
Displays policy name.

**Policy Type**
Displays default Policy Type set at the time of creation of policy, modify if required.

**Note**
Configured policy type will override the default policy and will be applicable only for the selected scheduled time interval.

**Limit Upload/Download Separately**
Displays default implementation strategy set at the time of creation of policy, modify if required.

**Note**
Configured policy type will override the default policy and will be applicable only for the selected scheduled time interval.

**Limit (in KBps) (Only if Policy Type is 'Limit'and Limit Upload/Download Separately is disabled)**
Displays allocated Total bandwidth. Modify if required.

**Note**
The modified bandwidth restriction is applicable only for the selected time interval.

**Upload Bandwidth (in KBps) (Only if Policy Type is 'Limit'and Limit Upload/Download Separately is enabled)**
Displays allocated Individual upload bandwidth. Modify if required.

**Note**
The modified bandwidth restriction is applicable only for the selected time interval.

**Download Bandwidth (in KBps) (Only if Policy Type is 'Limit'and Limit Upload/Download Separately is enabled)**
Displays allocated Individual download bandwidth. Modify if required.

**Note**
The modified bandwidth restriction is applicable only for the selected time interval.

**Guarantee -Limit (in KBps) (Only if Policy Type is ‘Guarantee’ and Limit Upload/Download Separately is disabled)**
Displays range for total guaranteed bandwidth. Modify if required.
Total Bandwidth Range: 2 – 2560000KBps

**Guarantee - Limit Upload (in KBps) (Only if Policy Type is 'Guarantee' and Limit Upload/Download Separately is enabled)**
Displays range for guaranteed upload bandwidth. Modify if required.
Total Bandwidth Range: 2 – 2560000KBps
**Guarantee - Limit Download (in KBps) (Only if Policy Type is ‘Guarantee’ and Limit Upload/Download Separately is enabled)**

- Displays range for guaranteed download bandwidth. Modify if required.
- Total Bandwidth Range: 2 - 2560000KBps

**Schedule**

- Select Schedule from the available list during which the traffic shaping policy will be applied.
- Only Recurring Schedule can be applied.
- If you are not sure about the Schedule details, check Schedule to view the details.

![Traffic Shaping Policy Form](image)

**Figure 172: Add Traffic Shaping (QoS) Policy Detail**

5. Click **Save** to add a schedule-wise traffic shaping policy.

**Device Access**

**Device Configuration > System > Profiles > Device Access**

Role-based administration capabilities are provided to offer greater granular access control and flexibility.

It allows an organization to separate super administrator's capabilities and assign through Profiles. Profiles are a function of an organization's security needs and can be set up for special-purpose administrators in areas such as policy administration, network administration, and logs administration. Profiles allow granting permissions to individual administrators depending on their role or job need in the organization.

The profile separates device features into access control categories for which you can enable none, read only, or read-write access.

The Profiles list shows the default and custom profiles you have created and enables you to add, edit, and delete the profiles.

For ease of use, by default the device provides 5 profiles:
• Administrator – super administrator with full privileges
• Audit Admin – read-write privileges for Logs & Reports only
• Crypto Admin – read-write privileges for Certificate configuration only
• HA Profile – read-only privileges. If HA is configured, any user accessing Web Admin Console of Auxiliary device will have privileges as defined in HA Profile.
• Security Admin – read-write privileges for all features except Profiles and Log & Reports

An Administrator with full privileges can create other custom administrators and assign them restricted/full privileges. A custom administrator so created, if has restricted privileges, can only update their Email Address and password.

Note
• You cannot delete the default profiles.
• You cannot delete the profile which is already assigned to administrator.

Access Denied page

Device provides role-based administration capabilities and privileges are assigned to the Administrator through Profiles. Administrator can have read only, read-write or no access privilege for the pages of Web Admin Console.

Access denied page is displayed when the Administrator tries to access a page or perform the operation, which is not allowed to him/her.

Add a device access profile

1. Go to Profiles > Device access and click Add.
2. Type a name.
3. To specify the configuration, select the administrator's level of access for the menus.
   • None
   • Read-only
   • Read-write

   Note
   To specify different access levels for sub-menus, click +

4. Click Save.

For the device access profile to take effect, apply it to a user whose type is set to administrator.
3.6.2 Hosts and services

Hosts and services allows defining and managing system hosts and services.

IP host

The IP host page displays the list of all the dynamic hosts, default hosts and manually added hosts.

Hosts allow the entities to be defined once, which can be re-used in multiple referential instances throughout the configuration. For example, consider an internal mail server with an IP address 192.168.1.15. Rather than repeated use of the IP address while configuring security policies or NAT policies, it allows to create a single entity internal mail server as a hostname with an IP address 192.168.1.15. This host, internal mail server can then be selected in any configuration that uses host as a defining criterion.

By using host name instead of numerical address, you only need to make changes in a single location, rather than in each configuration where the IP address appears.

Using hosts, reduces the error of entering incorrect IP addresses, makes it easier to change IP addresses, and increases readability.

You can group multiple entities performing the same function within a single hostname.

The IP host page displays the list of all the dynamic hosts which are automatically added on creation of VPN remote access connections (IPsec and SSL) and the default hosts (IPv6 and IPv4) for remote access connection - ##ALL_RW, ##WWAN1, ##ALL_IPSEC_RW and ##ALL_SSLVPN_RW along the manually added hosts. The page also provides option to add a new host, update the existing host, or delete a host.

Note

- System hosts cannot be updated or deleted.
- Dynamic hosts which are automatically added on creation of VPN remote access connections cannot be deleted.
- Default hosts (IPv6 and IPv4) for remote access connection - ##ALL_RW, ##WWAN1, ##ALL_IPSEC_RW and ##ALL_SSLVPN_RW cannot be updated or deleted.

Add IP host

Add IP host allows you to assign a hostname to a network, IP address, range or list.

1. Go to Hosts and services > IP host and click Add.
2. Enter the hostname.
3. Select the IP family.
   
   **Available options:**
   
   - IPv4
   - IPv6
4. Select the host Type.
   
   **Available options:**
   
   - IP
   - Network
   - IP range
• IP list (IP addresses which belong to different networks or are not within a range.)

5. If the selected host type is IP, Network or IP range:
   a) Enter the IP address, subnet or range based on the host type.
   b) Select an IP host group or create a new one.

   **Note**
   A single host can be the member of multiple host groups. A host group cannot include both IPv4 and IPv6 hosts.

6. If the selected host type is IP list, enter the List of IP addresses.

   **Note**
   Only class B IP addresses can be added to an IP list. You can add or remove an IP address from the IP list.

7. Click **Save**.

**IP host group**

The IP host group page displays the list of all the host groups.

Host group is a grouping of hosts. Security policies can be created for the individual host or host groups.

**Note**
Dynamic host groups which are automatically added on creation of VPN remote access connections cannot be deleted.

The page also provides option to add a new host group, update the parameters of the existing host group, add members to the existing host group, or delete a host group.

**Add an IP host group**

The **Add IP host group** page allows you to configure an IP host group.

1. Go to **Hosts and services > IP host group** and click **Add**.
2. Enter IP host group details.

   **Name**
   Enter a name to identify the IP host group.

   **Description**
   Enter a description for the IP host group.

   **IP family**
   Select the type of IP family from the options available:

   **Available options:**
   - IPv4
   - IPv6

   **Select host**
   The host list displays all the hosts including default hosts. Click the corresponding checkbox(es) to select the host(s). A single host can be a member of multiple host groups.
A group with IPv4 and IPv6 hosts cannot be created.

3. Click **Save**.

The IP host group has been created and appears on the **IP host group** page.

**MAC host**

The device allows you to assign a hostname to one or more MAC addresses.

**Add a MAC host**

The **Add MAC host** page allows you to manually create a MAC host of either a single MAC address or multiple MAC addresses.

1. Go to **Hosts and services > MAC host** and click **Add**.
2. Enter MAC host details.

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter a name to identify a MAC host.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Select the MAC host type.</td>
</tr>
<tr>
<td><strong>MAC address</strong></td>
<td>Specify MAC address based on the host type selected in the form of 00:16:76:49:33:CE or 00-16-76-49-33-CE.</td>
</tr>
<tr>
<td><strong>List of MAC addresses</strong></td>
<td>Specify MAC address based on the host type selected in the form of 00:16:76:49:33:CE or 00-16-76-49-33-CE. Use comma to configure multiple MAC addresses.</td>
</tr>
</tbody>
</table>

3. Click **Save**.

The MAC host has been created and appears on the **MAC host** page.

**FQDN host**

The FQDN host page displays the list of all the available FQDN host.

FQDN (fully qualified domain name) hosts allow entities to be defined once and be re-used in multiple referential instances throughout the configuration. For example, www.example.com has an IP address as 192.168.1.15. Rather than remembering the IP address of the intended website while accessing it, you can simply type www.example.com in the browser. The FQDN www.example.com will now be mapped to its respective IP address, and the intended webpage opens.

The page also provides option to add a new FQDN host, update the existing host, or delete a host.

**Add an FQDN host**

Use the **Add FQDN host** page to create a new FQDN host.

The **Add FQDN host** page allows you to manually configure a new FQDN host.

1. Go to **Hosts and services > FQDN host** and click **Add**.
2. Enter FQDN host details.

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Specify a name to identify the FQDN host.</th>
</tr>
</thead>
</table>
**FQDN**

**FQDN host group**

Specify an FQDN address.

Select an FQDN host group or add a new one. A single FQDN host can be member of multiple host groups. You can add a new FQDN host group on this page or on the **Hosts and services > FQDN host group** page.

3. Click **Save**.

**FQDN host group**

FQDN host group allows you to add individual FQDN hosts to one or more host groups.

**Add an FQDN host group**

The **Add FQDN host group** page allows you to configure a new FQDN host group.

1. Go to **Hosts and services > FQDN host group** and select **Add**.
2. Enter FQDN host group details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name to identify the FQDN host group.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the FQDN host group.</td>
</tr>
<tr>
<td>Select host</td>
<td>The host list displays all the hosts including default hosts. Click the corresponding checkbox(es) to select the host(s). A single host can be a member of multiple host groups.</td>
</tr>
</tbody>
</table>

3. Click **Save**.

**Country**

The **Country** page displays the list of all the available Countries.

This page is not available in Sophos XG Firewall for version SFOS 16.01.0 and above. This page is maintained in SFM for maintenance and compatibility purposes for Sophos XG Firewall Devices on version SFOS 15.01.0.

**Adding a Country Host**

Use the **Add Country Host** page to create country based host.

The **Add Country Host** page allows you to manually enter details to add a country based host.

1. Go to **Device Configuration > System > Hosts and Services > Country Host** and click **Add**.
2. Enter details.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name to identify the Country Host.</td>
</tr>
<tr>
<td>Country</td>
<td>Select the Country.</td>
</tr>
<tr>
<td>Country Host Group</td>
<td>Select Country Host Group. Single host can be member of multiple host groups. You can add a new Country Host Group from this page itself or from <strong>Objects &gt; Assets &gt; Country Host Group</strong> page.</td>
</tr>
</tbody>
</table>
3. Click **Save**.

**Country group**

The device offers predefined country groups based on their continent. It also offers the list of countries which appears when you create a firewall rule. You can create custom country groups.

**Note**

On factory reset, the device resets to predefined country groups.

**Note**

You can edit or delete predefined and custom country groups.

**Add a country group**

The **Add country group** page allows you to manually configure parameters to add a new country group.

1. Go to **Hosts and services > Country group** and click **Add**.
2. Enter country group details.
   - **Name**
     - Enter a name to identify the country group.
   - **Description**
     - Country group description.
   - **Select country**
     - Click **Add new item** to select and add countries in the group.
     - A country can be a member of multiple country groups.

3. Click **Save**.

**Services**

The Services page displays the list of all the default and custom services.

Services are definitions of certain types of network traffic and combine information about a protocol such as TCP, ICMP or UDP as well as protocol-related options such as port numbers. You can use services to determine the types of traffic allowed or denied by the firewall.
Certain well-known traffic types have been predefined in services. These predefined services are defaults, and cannot be updated or deleted. If you require service definitions that are different from the predefined services, you can add them as custom services.

The page also provides option to add a new service, update the parameters of the existing service, or delete a service.

**Note**
- Service used by security policies cannot be deleted.
- Default services can neither be updated nor deleted.

**Add service**
The *Add service* page allows you to manually configure parameters to add a new service.

1. Go to **Hosts and services > Services** and click **Add**.
2. Enter service parameters.

   **Name**
   Enter a name to identify the service.

   **Type**
   Select a protocol for the service.

   **Available options:**
   - TCP/UDP - Enter source and destination port. You can enter multiple ports for the same service.
   - IP - Select protocol number for the service. You can select multiple ports for the same service.
   - ICMP - Select ICMP type and code. You can enter multiple types and codes for the same service. Use Add icon and Remove icon to add and delete the parameters respectively.
   - ICMPv6 - Select ICMPv6 type and code. You can enter multiple types and codes for the same service.

3. Click **Save**.

**Service group**
The *Service group* page displays the list of all the default and custom service groups.

Service group is a grouping of services. Custom and default services can be grouped in a single group.

Use to configure security policies to:
- block group of services for specific zone
- limit some or all users from accessing group of services
- allow only specific user to communicate using group of service
Create groups of services and then add one firewall to allow or block access for all the services in the group. A service group can contain default services as well as custom services in any combination. A single service can be a member of multiple service groups.

The page also provides option to add a new group, update the parameters of the existing group, add members to the existing group, or delete a group.

**Note**
- Default service groups can neither be updated nor deleted.
- Service group used by the security policies cannot be deleted.

**Add a service group**
Use the *Add service group* page to add a new customized service group.

The *Add service group* page allows you to manually enter details and configure a new service group.

1. Go to *Hosts and services > Service group* and click *Add*.
2. Enter service group details.
   - **Name**
     Enter a name to identify the service group.
   - **Description**
     Service group description.
   - **Select service**
     Service list displays all the services including default services. Click the checkbox to select the service. All the selected services are moved to the selected service list. Single service can be a member of multiple groups. Use search to search a service from the list. You can create a group containing IPv4 and IPv6 services.
3. Click *Save*.

**3.6.3 Administration**

Administration allows you to manage device licenses and time, administrator access, centralized updates, network bandwidth and device monitoring and user notifications.

**Admin Settings**

**Device Configuration > System > Administration > Settings**

Use Settings page to make modifications in the general port settings and Web Admin Login parameters. Make changes to the login parameters for restricting the local and remote users based on the time.

**Admin Port Settings**

**Web Admin HTTP Port**

Provide the port number to configure HTTP Port for Admin Console access.

Default - 80
Web Admin HTTPS Port

Provide the port number to configure HTTPS Port for secured Admin Console access.
Default - 4444

User Portal HTTPS Port

Provide the port number to configure HTTPS Port for Secured User Portal access.
Default - 443

Certificate

Certificate to be used by User Portal and Captive Portal.

Login Security (Remote Admins)

To prevent the unauthorized access to the Admin Console and CLI, configure Admin Session Lock, Admin Session Logout time and Block Admin Login to block the access after number of failed login attempts.

Lock Admin Session After

Configure inactivity time (in minutes) for the administrative session after which the device will be locked automatically. This configuration will be applicable to following components:

- Admin Console
- Telnet Console
- IPSec Connection Wizard
- Network Wizard
- Group Import Wizard
Default - 3 Minutes

Logout Admin Session After

Configure time of admin inactivity in minutes after which the administrator will be logged out automatically.
Default - 10 Minutes

Note

Admin Session Logout time value must be greater than Lock Admin Session time.

Block Admin Login

Enable to block login to the Admin Console and CLI after configured number of failed attempts within configured time span.

Configure number of allowed failed login attempts from the same IP Address within the time limit.

Specify number of minutes for which the administrator will not be allowed to login. The administrator account will locked for the configured minutes if allowed failed login attempts exceeds.

Administrator Password Complexity Settings

Password Complexity can be configured to ensure that administrators are using secure passwords.

Enable Password Complexity Settings to enforce following constraints:

- Minimum Password length. Configure minimum characters required in the password.
  Default - 8 Characters
Sophos Firewall Manager

- Require minimum one upper and lower case alphabet
- Require minimum one number (0 - 9)
- Require at least one special character e.g. @, $, %
- Password cannot be same as username.

**Note**
All the enabled constraints are applied to password of administrator user only.

**Login Disclaimer Settings**
The Login Disclaimer allows setting a written message that administrators must read and agree prior to logging on to the Admin Console and CLI for device administration. If a disclaimer is set, it must be accepted before administrator can login.

Default disclaimer can be customized as per the requirement from the Messages page **System > Administration > Messages**. One can also review the customized message before setting.

**Sophos Adaptive Learning**
The product sends information periodically to Sophos which is used for the purpose of improving stability, prioritizing feature refinements, and protection effectiveness. It includes configuration and usage information, and Application usage and threat data.

Configuration and usage data such as Device information (hardware version, vendor), Firmware version and license information (not the owner), Features in use (status, on / off, count, HA status, Central Management status), amount of configured objects (count of hosts, policies), Product errors, CPU, memory and disk usage (in percentage), is collected by default.

No user-specific information or personalized information is collected. The information is transmitted to Sophos over HTTPS.

**Send App & Threat data**
Following Application usage and Threat data is gathered:
- Unclassified applications to improve and enlarge the network visibility and application control library.
- Data for IPS alerts, virus detected (also URL for which virus found), spam, ATP threats such as threat name, threat URL/IP, source IP, and applications used.

Default - Enable

**SFOS Hot-fix**
Allow auto-install of important Hot-fixes Hot-fixes are applied automatically if available. Disable if you do not want to apply hot-fix. Default - Enable

**Licensing**
After migrating firewall device from **CyberoamOS (CR-OS)** to **Sophos Firewall OS (SFOS)**, one has to upgrade license of the firewall device by navigating to **Device Configuration > System > Admin > Licensing**. Available options are:

- **30 Day Full Guard Trial (Evaluating)** - All module licenses will be applied to the firewall for 30 days. The existing Cyberoam licenses will remain intact. During this period, seamless rollback to CR-OS is possible by rebooting the firewall device with the Cyberoam firmware.
- **Migrate License** - All the existing CR-OS licenses will be migrated to SFOS. This will result in a license of equivalent value to your current one.
License Migration

Migrate CR licenses to SFOS

Click to migrate your Cyberoam (CR) licenses that are currently on 30 Day Full Guard Trial (Evaluating) to SFOS licenses on selected firewall devices. This will migrate your CR licenses permanently to SFOS with no roll-back possible. This can also be done using Migrate License option from Sophos XG Firewall.

Note
This page will be applicable to only those managed devices that are on 30 Day Full Guard Trial (Evaluating) mode.

Notification settings

Notification settings allows you to configure the mail server IP address, port, and email address to send and receive alert emails.

The device allows you to configure email notifications for system-generated events and reports to inform the administrator about:

- Change in gateway status
- Change in HA (high availability) link status (if HA cluster is configured)
- Change in the state of IPsec tunnels

1. Mail server settings

   Click to Send notifications via:

   Built-in email server

   Select if you want to use the built-in email server in XG Firewall to send system-generated emails.

   External email server

   Select to configure an external email server to send system-generated emails.

   a) Specify the Mail server IPv4 address or FQDN address and port number. Default port: 25

   b) Select Authentication required to authenticate the user before sending an email. Specify Username and Password.

   c) Select Connection security mode to be used for establishing a secured connection between an SMTP client and the SMTP server for SMTP mail notification. Available options:

      - None
      - STARTTLS
      - SSL/TLS

      Default: None

   d) Select a Certificate to be used for authentication by the SMTP client and the SMTP server.

      Default: ApplicanceCertificate

2. Email settings

   Enter the sender and recipient email addresses.
3. **Email notification**

Select **IPsec tunnel up/down** to enable receipt of email notifications if IPsec VPN tunnel connectivity is lost.

Email alerts are sent to the configured email address.

An email is sent only when host-to-host and site-to-site tunnel connections are disconnected for one of the following reasons:

- A peer is found dead (DPD)
- Failed to re-establish connection after Dead Peer Detection (DPD)
- IPsec Security Association (SA) has expired and needs to be re-established.
- IPsec tunnel comes up without administrator intervention after losing connectivity.

**Note**

- For site-to-site connections with multiple local/remote networks, an email is sent for each subnet pair.
- Description of IPsec tunnel connection is included in the email only if the administrator has provided the information.
- Emails are sent at an interval of 60 seconds to reduce the number of emails. Events that happen within an interval are sent in a single email.

4. **Test mail**

Click to preview and edit the email address details.

Click **Send**.

**Note**

Mail server configuration changes automatically when the changes are made from the network configuration wizard and vice versa.

---

**Device Access**

**Device Configuration > System > Administration > Device Access**

Device access allows limiting the Administrative access of the following device services from various default zones, LAN, WAN, DMZ, VPN and custom zones:

- Admin Services – HTTP, HTTPS, Telnet, SSH
- Authentication Services – Client Authentication, NTLM, Captive Portal, Radius SSO
- Network Services – DNS, Ping/Ping6
- Other Services – Wireless Protection, SSL VPN, Web Proxy, User Portal, Dynamic Routing

**Default ACL**

When device is connected and powered on for the first time, it will have a default Access configuration.

Admin Services – HTTP (TCP port 80), HTTPS (TCP port 443), Telnet (TCP port 23) and SSH (TCP port 22) services will be enabled for administrative functions in LAN and WiFi zone. HTTP
(TCP port 80), HTTPS (TCP port 443), Telnet (TCP port 23) and SSH (TCP port 22) services will be enabled for administrative functions in WAN zone. HTTP (TCP port 80) services will be enabled for administrative functions in DMZ zone.

Authentication Services – Client Authentication (UDP port 6060), Captive portal Authentication (TCP port 8090) and Radius SSO will be enabled for User Authentication Services in LAN and WiFi zone. User Authentication Services are not required for any of the Administrative functions but required to apply user based internet surfing, bandwidth, and data transfer restrictions.

Network Services – Ping/Ping6 and DNS services will be enabled for LAN, WAN and WiFi zone.

Other Services – Web Proxy service will be enabled for LAN and WiFi zone. SSL VPN (TCP port 8443) service will be enabled for LAN, WAN, DMZ and WiFi zone. User Portal and Dynamic Routing service will be enabled for LAN and WAN zone.

Local Service ACL

Use access control to limit the access to the device for administrative purposes from the specific authenticated/trusted networks only.

**Admin Services** – Enable/disable access to the device using following service from the specified zone: HTTP, HTTPS, Telnet and SSH.

**Authentication Services** – Enable/disable following service from the specified zone: Client Authentication, Captive Portal, NTLM, Radius SSO.

**Network Services** – Enable/disable following service from the specified zone: DNS, Ping/Ping6.

**Other Services** – Enable/disable following service from specified zone: Wireless Protection, SSL VPN, Web Proxy, User Portal and Dynamic Routing.

Local Service ACL Rule

Use Local Service ACL Rule to allow access to the device Admin Services from specified network/host. The section displays list of all the configured IPv4 and IPv6 Local Service ACL rules. The page provides option to add, update and delete the rules.

Default Admin Password Settings

The device is shipped with one global super admin with the credentials – username & password as “admin”. Both the consoles – Admin Console and CLI, can be accessed with the same credentials. This administrator is always authenticated locally i.e. by device itself.

**Note**

We recommend you to change the password for this user name immediately after deployment.

You can change the default password from this section. The screen elements and their description are mentioned below:

**Username**

The default admin username is –“admin”.

**Current Password**

Enter the current admin password.

**New Password**
Password - Specify new admin password.
Confirm Password - Confirm the specified new admin password.

Reset to Default
Click to reset the password to factory default password.

Public Key Authentication
Use this to configure Public Key Authentication on multiple Sophos XG Firewall devices.

Username
The default admin username is —“admin”.

Public key authentication for admin
Select this to enable public key authentication for admin.

Authorized keys for admin
Add or remove authorized SSH keys from here.

Devices on which configuration was pushed in the last session
This displays list of devices on which configuration was pushed in the last session.

Select devices that have same admin password.
Select this to enable selecting devices with same admin password. If this is not selected then passwords for all the devices have to be specified separately.

Device
Select device(s) on which public key authentication is to be applied.

Password
Specify password for the device(s).

Add Local Service ACL Rule
Use Local Service ACL Rule to allow access to the device Admin Services from specified network/host.
You can add Local Service ACL rule from this page.
1. Go to Device Configuration > System > Administration > Device Access and click Add under Local Service ACL Rule
2. Enter Rule details.

Rule Name
Specify name to identify the rule.

Description
Provide a description for the rule.

IP Family
Select the type of IP Family from the options available:
Available Options:
IPv4 IPv6

Network/Host
Click Add New Item button to select host or network address to which the rule applies.
You can also create new Network/Host from this page itself by clicking Create New button.

Services
Click Add New Item to select Admin Services to which the rule applies.
Available Options:
HTTP HTTPSTelnetSSH

3. Click **Save** to add the rule.

**Time**

**Device Configuration > System > Administration > Time**

Device current date and time can be set according to the device’s internal clock or synchronized with an NTP server. Device clock can be tuned to show the right time using global Time servers so that logs show the precise time and device internal activities can also happen at a precise time.

Below are the screen elements and their description for setting the Time and Date for the Device:

**Current Time**

Displays the current system time.

**Time Zone**

Select time zone according to the geographical region in which the device is deployed.

**Use pre-defined NTP Server**

Select to use the pre-defined NTP servers – asia.pool.ntp.org & in.pool.ntp.org.

NTP stands for Network Time Protocol, and it is an Internet standard protocol used to synchronize the clocks of device to some time reference.
**Use Custom NTP Server**

Specify the NTP server IPv4 Address or IPv6 Address or domain name to synchronize time with it. If custom NTP server is defined, time is synchronized with custom server and not with pre-defined servers.

Devices use NTP Version 3 (RFC 1305). One can configure up to 10 NTP servers. At the time of synchronization, it queries each configured NTP server sequentially. When the query to the first server is not successful, device queries second server and so on until it gets a valid reply from one of the NTP servers configured.

**Sync Status**

Click **Sync Now** to synchronize device clock with the NTP Server.

**Do Not use NTP Server**

Select to configure the date and time for device’s clock.

**Date**

Specify the date by clicking calendar.

**Time**

Specify the time in HH:MM:SS format.

**SNMP**

**Device Configuration > System > Administration > SNMP**

Simple Network Management Protocol (SNMP) is used as the transport protocol for network management. Network management consists of a station or manager communicating with network elements such as hosts, routers, servers, or printers. The agent is the software on the network element (host, router, and printer) that runs the network management software. In other words, agent is the network element. The agent will store information in a Management Information Base (MIB). Management software will poll the various network elements/agents and get the information stored in them. The manager uses UDP port 161 to send requests to the agent and the agent uses UDP port 162 to send replies or messages to the manager. The manager can ask for data from the agent or set variable values in the agent. Agents can reply and report events.

SNMP collects information in two ways, if SNMP agent is installed on the devices:

- The SNMP management station/manager will poll the network devices/agents.
- Network devices/agents will send trap/alert to SNMP management station/Manager.
SNMP terms

• **Trap** - An alert that is sent to a management station by agents.

• **Agent** - A program at devices that can be set to watch for some event and send a trap message to a management station if the event occurs.

• **SNMP community** – An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. The community name is used to identify the group. A SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities.

Use SNMP to configure agent, community and the SNMPv3 users. Device supports SNMPv1 & SNMPv2c protocols. Agent configuration page is used to configure agent name, agent port and the contact person for the program. The community page is used for adding, managing and deleting the communities for protocols SNMPv1 and SNMPv2c. Use SNMPv3 user page to add, manage and delete v3 users. Apart from IPv4 Addresses, SNMP now supports IPv6 Addresses also.

Below are the screen elements with their description:

**Agent Configuration**

Use Agent configuration section to configure SNMP agents. The configuration details include name, description, location, contact person, agent port and manager port.

Below are the screen elements with their description:

**Enable SNMP Agent**

Select to enable SNMP Agent.

**Name**

Specify a name to identify the agent.

**Description**

Specify Agent Description.

**Location**

Specify the physical location of the device.

**Contact Person**

Specify the contact information for the person responsible for the maintenance of above specified device.

**Agent Port**

Specify the port which device should use to send traps.

Default - 161

**Manager Port**

Remote SNMP Management station/Manager uses this port to connect to the device.

Default - 161

**Community**

Community is a group of SNMP Managers. SNMP Agent may belong to one or more than one community. Agents do not respond to the requests from management stations that do not belong to its communities.
Each Community can support SNMPv1, SNMPv2c or both. Device sends traps to all the communities. You must specify a trap version for each community.

The section provides list of all the communities added and you can sort the list based on community name. The section also provides the option to add a new community, update the parameters of the existing community, or delete the community.

v3 User

SNMP version 3 has the capability of using authentication. Only the authenticated user can request the information.

The section displays the list of all the v3 users. The section also provides the option to add a new v3 user, update the password of the user, or delete the user.

Add community

1. Go to Administration > SNMP and click Add.
2. Enter a name.
3. Enter the description.
4. Enter the IP address (IPv4/IPv6) of the SNMP manager.
5. Select the SNMP protocol version. SNMP v1 and v2c-compliant SNMP managers have read-only access to device system information and can receive device traps.
6. Select the version for trap support. Traps are sent only to SNMP managers that support the specified versions.
7. Click Save.

Add a new V3 User

You can add V3 user from this page.

1. Go to Device Configuration > System > Administration > SNMP > v3 User and click Add.
2. Enter User details.
   Name
   Enter a name to identify the v3 user.
   Password
   Provide a password for authentication.
   Confirm the password for authentication.
3. Click Save to add v3 User.

Netflow

Netflow allows you to add, update, or delete Netflow servers. The device offers Netflow, a network protocol, to monitor network bandwidth usage and traffic flow. Netflow records of source, destination and volume of traffic are exported to the Netflow server. The records help you identify the protocols, policies, interfaces and users consuming high bandwidth. Data analyzing tools like Open Source Data Analyzer and PRTG software can generate reports from the Netflow records.

Netflow configuration

1. Enter the Netflow Server name.
2. Enter the Netflow server IP/domain. You can enter IPv4 or IPv6 addresses.
3. Enter the **Netflow server port** number (UDP port). Records are sent to the Netflow server over the specified port.
   
   Default: 2055

**Note**

Traffic of only those firewall rules that have **Log firewall traffic** enabled is sent to the Netflow server.

**Note**

You can configure up to five Netflow servers.

**Note**

Sophos supports Netflow v5. You can export all the parameters of v5.

### Messages

Use messages to notify users and issue administrative alerts.

You can send messages of up to 256 characters to a single user or multiple users simultaneously.

You can edit

- the message, save
- the changes or reset

You can send notifications related to the following events:

- Authentication: Login and logout confirmation, login failure and disconnection
- SMTP: Blocked and received emails
- Administration: Disclaimer for admin login
- SMS customization: Login information to guest users

### Updates

**Device Configuration > System > Administration > Updates**

By default pattern updates are updated automatically. **Updates** page displays the status of various patterns for different models like Sophos AV, IPS, WAF. The page also allows to update patterns or set auto-update time interval.

Below are the screen elements with their description:

#### Updates Status

**Pattern**

Pattern name whose definitions are updated.

**Current Version**

Version of the Pattern
Last Successful Update

Status along with date of the last update

Update Pattern Now Button

Click 'Update Pattern Now' button to update the pattern definitions.

Pattern Download/Installation

Auto Update

To update pattern definitions automatically, enable "Auto Update".

Interval

If "Auto Update" is set as off, set the time limit in which you want to receive updates.

Available Options: Every hour Every 2 hours Every 4 hours Every 12 hours Daily Every 2 days

3.6.4 Certificates

Digital certificates provide verification of ownership of a user or computer (example: VPN) or an organization (example: websites) over the internet, and are issued by a certificate authority (CA). Certificate signing requests (CSR) enable you to provide the information required for the CA to issue a certificate. CAs issue certificates which can include the owner’s public key, the certificate’s validity period, owner information and the private key. Verification is completed through the private key which is held by the owner.

Certificates are revoked when the private key is lost, stolen or updated. CAs maintain a list of valid and revoked certificates. Self-signed certificates that are revoked are automatically added to the certification revocation list (CRL).

The device allows you to:

• generate a self-signed certificate, upload a third-party certificate, or to generate a CSR.
• use the device as the CA or add an external CA.
• revoke a self-signed certificate or upload an external CRL.

Add certificate

Add certificate allows you to upload a certificate, generate a self-signed certificate, or to generate a certificate signing request (CSR).

1. Go to Certificates > Certificates and click Add.
2. Select from the following options.
   • Upload certificate
   • Generate self-signed certificate
   • Generate certificate signing request

Upload certificate

1. Enter the Certificate name.
2. Select the format of certificate file.
   • PEM (.pem): Base64 encoded form of DER certificate. Certificate and private key are stored in different files.
**DER (.der):** Binary form of PEM certificate used on Java platform. Certificate and private key are stored in different files.

**PEM (.pem):** Base64 encoded form of DER certificate. Certificate and private key are stored in different files.

**DER (.der):** Binary form of PEM certificate used on Java platform. Certificate and private key are stored in different files.

**CER (.cer):** Binary form. Contains certificate owner information and public and private keys.

**PKCS7 (.p7b):** ASCII code. Contains the certificate but not the private key.

**PKCS12 (.pfx or .p12):** Binary form used on Windows platforms. Stores the private key with the public key.

3. Upload certificate and private key.
4. Enter the CA passphrase and re-enter to confirm.
5. Click **Save.**

**Generate self-signed certificate**

1. Go to **Certificates > Certificates** and click **Add.**
2. Set **Action** to **Generate self-signed certificate.**
3. **Certificate details**
   a) Enter the **Certificate name.**
   b) Specify the certificate’s validity period.
      Default: 1 day
   c) Select the number of bits used to construct the key from the list.

   **Note**
   Larger keys offer greater security, but take longer to encrypt and decrypt data.
   Default: 2048
   d) Select to encrypt the key. Enter a passphrase or the pre-shared key and re-confirm
   e) Specify the certificate ID for one of the following options:
      • DNS
      • IP address (IPv4/IPv6 address)
      • Email
      • DER ASN1 DN (X.509)
4. **Identification attributes**
   a) Select the country in which the device is deployed.
   b) Enter the state within the country.
   c) Enter the locality in which the certificate is to be used.
   d) Enter the name of the certificate owner (example: Sophos Group).
   e) Enter the name of the department to which the certificate is to be assigned (example: marketing).
   f) Enter the common name or FQDN (example: marketing.sophos.com).
   g) Enter the contact person’s email address.
5. Click **Save** to generate self-signed certificate.

### Generate certificate signing request

The device allows you to generate a certificate signing request (CSR) which can be sent to a CA.

1. Go to **Certificates** and click **Add**.
2. Set **Action** to **Generate certificate signing request (CSR)**.
3. **Certificate details**
   a) Enter the **Certificate name**.
   b) Specify the certificate’s validity period.
      Default: 1 day
   c) Select the number of bits used to construct the key from the list.

   **Note**
   Larger keys offer greater security, but take longer to encrypt and decrypt data.
   Default: 2048
   d) Select to encrypt the key. Enter a passphrase or the pre-shared key and re-confirm
   e) Specify the certificate ID for one of the following options:
      • DNS
      • IP address (IPv4/IPv6 address)
      • Email
      • DER ASN1 DN (X.509)
4. **Identification attributes**
   a) Select the country in which the device is deployed.
   b) Enter the state within the country.
   c) Enter the locality in which the certificate is to be used.
   d) Enter the name of the certificate owner (example: Sophos Group).
   e) Enter the name of the department to which the certificate is to be assigned (example: marketing).
   f) Enter the common name or FQDN (example: marketing.sophos.com).
   g) Enter the contact person’s email address.
5. Click **Save**.

Once the certificate is created, you need to download and send this certificate to the remote peer with whom the connection is to be established.

### Download certificate

The device allows you to download self-signed certificates and certificate signing requests.

1. Go to **Certificates > Certificates**.
2. Go to the **Manage** column and click ![download_icon] against the certificate. The certificate is downloaded as a .tar.gz file.
Revoke certificate

1. Go to **Certificates > Certificates**.
2. Go to the **Manage** column and click against the certificate. You can revoke lost, stolen or updated self-signed certificates.

Revoked certificates are automatically added to the certificate revocation list (CRL).

3.6.5 Configuration

**Device Configuration > System > Configuration**

Configuration menu allows basic administrative settings for the device.

Use this menu to configure below details:

- **CLI Configuration** - Configure CLI settings.

**CLI Configuration**

To configure SFM CLI settings go to **Device Configuration > System > Configuration > CLI Configuration**.

**IPS MAX Packets**

Set **IPS MAX Packets**

Set number of packets to be sent for Application Classification.

- **All** - pass all of the session packets for application classification
- **Default** - pass first 8 packets of the session of each direction for application classification (total 16)
- **Value** – any number between 8 and 65535

**Route Precedence**

**Route List**

- Static System Routes
- VPN Routes

**Change the Order**

Use Move Up & Move Down buttons to change the order of routes.

**Note**

Do not forget to click Apply after changing the order.

**HTTPS Unknown Protocol**

**Deny HTTPS Unknown Protocol**

Select action for HTTPS unknown protocol.

**Available options:**
On: Deny invalid traffic through HTTPS port  Off: Allow invalid traffic through HTTPS port  
By default, it is On.

Note  
Do not forget to click Apply after changing the action.

HTTPS Certificate

Invalid HTTPS Certificate
If you enable HTTPS scanning, you need to import SSL Proxy certificate in Internet Explorer, Firefox Mozilla or any other browsers for decryption on SSL Inspection otherwise browser will always give a warning page when you try to access any secure site. “Invalid Certificate error” warning appears when the site is using an invalid SSL certificate. The device blocks all such sites. Allow or block access to such sites.

Note  
Do not forget to click Apply after changing the action.

Thin Client

Add
Click to add IP address of a Citrix server.

IP Address
List of added Citrix servers IP addresses.

Manage
Click to remove Citrix server.
4 Templates

Template is a customizable set of policy configuration including commonly used objects, services and other configurations. SFM allows the administrator to define templates for storing global configurations. The configuration stored in a template can be directly applied to any managed Device(s) or Device group(s).

Template enables ease-of-administration by eliminating the need of configuring same entities on the Devices individually. Policy configuration using templates reduces administrative efforts in large enterprises and MSP networks where new Devices are added frequently.

Note
All policy configuration entities for Device Group level can be added to a template, except the following entities, which are outside the scope of templates:

• Administrator Password
• Synchronize
5 System & Monitor

System Management menu is meant to manage and configure the basic system options for the Sophos Firewall Manager. This includes the basic network settings to connect the Sophos Firewall Manager to the corporate network, the configuration of administrators and their access privileges, managing and updating firmware for the Sophos Firewall Manager, as well as managed Devices.

System allows you to configure the following settings:

- Device Settings
- Monitoring
- System Settings

5.1 Device Settings

Device Settings menu enables the administrator to add devices to the Sophos Firewall Manager. Once the devices are added, they can be organized into groups based on various criteria. The administrator can manage and configure devices or groups from Device Management menu. The administrator can also add dynamic objects for all managed devices. The menu also allows administrator to take and download backup of managed devices and restore it later on. Additionally, it gives visibility and control over scheduled tasks and Change Control events for managed devices.

Device Settings lets you configure the following settings:

- Managed Devices
- Maintenance
- Firmware
- Schedule Tasks
- Dynamic Objects
- Change Control

5.1.1 Managed Devices

Use the Managed Devices menu to add and manage devices using the Sophos Firewall Manager. Managed Devices menu allows you to configure the following settings:

- Devices
- Device Discovery
- Device Group
- Template

Devices

Use the Devices page to add, edit, delete and reboot devices from the Sophos Firewall Manager.
To add or edit device details, go to **System Management > Device Settings > Managed Devices > Device Configuration**

You can configure the following Device Settings:

- **Add/Edit**
- Reboot – Click the reboot icon in the Manage column against the device to be rebooted. The device can be rebooted immediately or scheduled at a later time.
- **More**
  1. **Add Device Wizard**
  2. **Export Device List**
  3. **Export Device IP Change Report**

**Add Device**

Use the Add Device page to add new devices or edit device details.

1. Go to **System Management > Device Settings > Managed Devices > Device Configuration** and click **Add**.
2. Specify Device details based on the given description.

**Device Name**

Specify device name, which uniquely identifies the Device.

**Description**

Specify description for the device.

**Serial Number**

Specify the device serial number.

**IP/Domain**

Specify IP address assigned to the WAN Interface of the device.

**Admin Username**

Specify Administrator Username of the device.

**Password and Confirm Password**

Specify Administrator Password of the device.

**Communication Mode**

Specify communication mode to manage the device from Sophos Firewall Manager.

**Available options: Central Management will push updates to this Device:**

Select if the managed device is directly accessible from Sophos Firewall Manager i.e. there is no intermediate NAT box. Specify **Access Protocol** and **Access Port** number to communicate with managed device.

**This Device will fetch updates from Central Management:**

Select if the managed device is behind NAT box e.g. ADSL. In that case the device will first poll Sophos Firewall Manager in interval of 1 (one) minute for any configuration updates available. If the updates are available the managed device will pull those updated configuration settings.

**Enable Change Control (CCL)**

Enabling Change Control allows the administrator to maintain list of configuration revisions. Configuration Revisions are the configuration changes synchronized by the Sophos Firewall Manager.
The administrator can update the CCL settings from **System Management > Device Settings > Change Control** page.

**Template**
Select configuration template which has to be applied on the device.

**Users**
Add Sophos Firewall Manager's Administrator who can manage the device.

**Administrator Information**
Click hyperlink to add additional information of administrator.

**Administrator Name**
Specify name of the Administrator.

**Contact Number**
Specify contact number of the Administrator.

**Email ID**
Specify email ID of the Administrator.

**Test Connection**
Click to test the connectivity between Firewall manager and the managed device.
3. Click **Save**.

**Add Device Wizard**

The Add Device Wizard takes you step-by-step through the process of Device addition and configuration of certain core features of Device management like firmware, backup & restore and template configuration.

Wizard is divided into six sections:

1. Device
2. Communication
3. Firmwares
4. Backup
5. Template
6. Summary
1. Go to **System Management > Device Settings > Managed Devices > Device Configuration** and select **More > Add Device Wizard**. You can also run Add Device Wizard from Device Discovery notification.

2. Add Device Details.
   a) Specify Device name, which uniquely identifies the Device.
   b) Specify Device Key. If you are running the wizard from Device Discovery notification then this field will reflect Device key automatically.
   c) Specify IP address assigned to the WAN Interface of the Device.
   d) Specify Administrator Username of the Device.
   e) Password for the above mentioned Administrator Username of the Device.
   f) Specify description if required.
   g) Click to enable Enable Change Control (CCL).
   h) Click hyperlink to add additional information of Sophos Firewall Manager Administrator.
   i) Specify name of the Administrator.
   j) Specify contact number of the Administrator.
   k) Specify email ID of the Administrator.
   l) Click **Next** to go to Communication Mode details or **Done** to complete the wizard.

3. Configure Communication Mode Details.
   a) Specify device communication mode to manage the device from Sophos Firewall Manager.
   
   **Central Management will push updates to this device**
Select if the managed device is directly accessible from Sophos Firewall Manager i.e. there is no intermediate NAT box. Specify access protocol and port number to communicate with the managed device.

**This device will fetch updates from Central Management**

Select if the managed device is behind NAT box e.g. ADSL. In that case Managed device will first poll Sophos Firewall Manager device in interval of 1 (one) minute for any configuration updates available. If the updates are available the managed device will pull those updated configuration settings.

b) Specify Protocol that is to be used to access the device for pushing configuration and synchronizing i.e. Protocol used to communicate with the device.

c) Specify Port through which device and Sophos Firewall Manager should communicate.

d) Specify Sophos Firewall Manager Administrator who can manage the device.

e) Click Back to go to Add device Details or Next to go to Firmware Management or Done to complete the wizard

![Figure 177: Define Communication Mode](image)


Displays current firmware version of managed and availability of latest firmware version.

a) If the device model is already added in Sophos Firewall Manager the latest version will be displayed automatically else click Check for Upgrades to check availability of latest firmware version.

b) To upgrade the device with latest available firmware click Yes against Do you want to upgrade the device. By default it is disabled.

c) Click Back to go to Communication Details and Next to go to Backup Management or Done to complete the wizard
5. Configure Backup Management.
   a) Click Yes against Do you want to restore any existing configuration backup in new device? to restore backup of any existing device in device to be added. By default it is disabled.
   b) Select an existing device and backup to restore it in device to be added else browse the backup file from your machine and restore it in device to be added.
   c) Click Back to go to Firmware Management or Next to go to Template Management or Done to complete the wizard.

6. Configure Template Management.
   a) Click Yes against Do you want to apply any configured template to the device? to add an device with existing configuration template. By default it is disabled.
   b) Select template to be applied.
   c) Click Next to view Summary of Add Device wizard or Back to go to Backup Management. Click Done to complete the wizard.
Figure 180: Select Template to Configure Device

7. Review configuration summary.

Summary page displays summary of the added device which includes Device Name, Device Key, IP/Domain, Admin Username, Communication Mode, Access Protocol, Access Port, Firmware Upgrade status, Restore Backup status, Template application status.

Click **Finish** to complete the wizard or **Back** to go to Template Management.

![Figure 181: Summary](image)

**Export Device List**

Export Device List option is used to export the list of all managed devices added in the Sophos Firewall Manager.

The list is exported in excel format containing the following details for each device which includes Device Name, Device Key, IP/Domain, Connection Status, Firmware Version, IPS Version, AV Version, Webcat Version, License Subscription Expiration, Last backup Time, Upstream Bytes and Downstream Bytes.

Device List report is generated automatically at 11:50 PM Daily by default and the previous report is overwritten by the new report. To see the last generated report, go to **System Management > Device Settings > Managed Devices > Device Configuration** and select **More > Export > Device List**

To generate and download the report manually, follow the steps shown below.
1. Go to **System Management > Device Settings > Managed Devices > Device Configuration** and select More> Export > Device List.
2. Click **Generate** to generate the report.
3. You should see the **Download** hyperlink for the generated report. Click the hyperlink to download the report.

**Note**
The manually generated report will overwrite the previously generated report.

**Export Device IP Change Report**

Export Device IP Change Report option is used to export the IP Address revisions for each added device.

Device IP Change Report displays IP address changes or revisions for last 30 days. 
This report is generated automatically 11:50 PM Daily.

To download the report, follow the steps shown below.

2. Click **Download** to download the report in Excel file format.

**Note**
The report is exported in the excel format which includes IP change information based on Device Name, Device Key, Time, Old IP and New IP.

**Device Discovery**

Use the Device Discovery page to view the devices which are sending heartbeat packet to the Sophos Firewall Manager. This page allows you to add these Devices to SFM. 
You can View, Add or Delete the discovered devices. Adding discovered devices is similar to adding new devices.

**Device Groups**

Device Groups are logical grouping of managed devices for ease of administration. 
Administrator may want to divide the managed devices into groups for the following reasons:

- Configure group-shared settings and then update the configurations on the devices at once. For example, group all the devices that need to upgrade subscription and upgrade all the devices simultaneously.
- Manage a great number of devices more efficiently.
- Group the devices according to their locations (country/state/city), ownership/company/departments, firmware, device name and device models.

**Note**
Single device can be part of different groups.

Using Device Groups page, you can:
Add/Edit device groups
Delete existing device groups

Add Device Groups

1. Go to System Management > Device Settings > Managed Devices > Device Groups. Click Add to create a new group or Edit Icon to modify the details of the group.
2. Specify group name, which uniquely identifies group.
3. Specify Devices to be grouped based on the available options.
   - Model
   - Firmware
   - Company
   - Country
   - State
   - City
   - Device Name: Specify group condition criterion.

   Available options: Starts with, Contains, Substring, Ends with.

   ![](image)

   Figure 182: Add Device Group

   Note
   You can select Device Name as a criterion multiple times. All the Devices starting with specified name prefix will be grouped dynamically.

4. Click Save.

Templates

Template is a customizable set of policy configuration including commonly used objects, services and other configurations. SFM allows the administrator to define templates for storing global configurations. The configuration stored in a template can be directly applied to any managed Device(s) or Device group(s).

Template enables ease-of-administration by eliminating the need of configuring same entities on the Devices individually. Policy configuration using templates reduces administrative efforts in large enterprises and MSP networks where new Devices are added frequently.
Note
All policy configuration entities for Device Group level can be added to a template, except the following entities, which are outside the scope of templates:

- Administrator Password
- Synchronize

Template Dashboard
Template dashboard displays summary of the selected template along with the recent activity log. To view the details of individual template, go to Template Configuration and select a template. This page displays following information for selected template:

- Template Summary
- Recent Activities

Template Summary
Displays the name of configuration entity along with number of entries for each entity.

Policies
Displays the name of Policies configured along with number of entries.

Protection
Wireless Protection
Displays name of the Wireless Protection configurations along with number of entries:

- Wireless Networks
- Mesh Networks
- Access Point Groups
- Hotspots
- Hotspot Voucher Definition
- Rogue AP Scan

Web Protection
Displays name of the Web Protection configurations along with number of entries:

- Web Proxy
- Web Content Filter > Configurations
- Web Filter Policies
- Custom Web Category
- URL Group
- Surfing Quota
- File Type
- Malware Protection

Application Protection
Displays name of the Application Protection configurations along with number of entries:

- Application Filter
• Traffic Shaping Settings

Web Server Protection
Displays name of the **Web Server Protection** configurations along with number of entries:
• Web Servers
• Web App Protection Policies
• Web App Authentication Policies
• Web App Auth Templates
• Certificate
• Certificate Authority
• Certificate Revocation Lists

Email Protection
Displays name of the **Email Protection** configurations along with number of entries:
• Email Configuration
• Scanning Rules > SMTP/S Malware Scanning Rules
• Scanning Rules > POP3/S and IMAP/S Malware Scanning Rules
• Scanning Rules > Content Scanning Rules
• SPX Configuration
• SPX Templates
• Data Protection
• Address Group
• Email Archiver
• Quarantine Digest Settings
• Trusted Domain
• Malware Protection

System Networks
Displays name of the **Network** configurations along with number of entries:
• Wireless Networks
• Mesh Networks
• DNS > DNS Configuration
• DNS > DNS Host Entry
• DNS > Request Routing
• DHCP Relay

Routing
Displays name of the **Routing** configurations along with number of entries:
• Upstream Proxy
• Static Route
VPN

Displays name of the **VPN** configurations along with number of entries:
- IPSec
- L2TP Settings
- L2TP Connections
- PPTP
- SSL VPN Settings
- SSL VPN (Site to Site) > Server Connection
- SSL VPN (Site to Site) > Client Connection
- SSL VPN (Remote Access)
- Clientless Access
- Bookmark
- Bookmark Group
- Certificate
- Certificate Authority
- Certificate Revocation Lists

Administration

Displays name of the **Administration** configurations along with number of entries:
- Settings
- Device Access
- Device Access >> Local Service ACL Exception Rule
- Updates
- Messages
- Notification
- Time
- SNMP > Agent Configuration
- SNMP > Community
- SNMP > v3 User
- Netflow

Authentication

Displays name of the **Authentication** configurations along with number of entries:
- Authentication Server
- Groups
- User
- Clientless Users
- Captive Portal
- Guest User Settings
• Guest User Settings > SMS Gateway
• Hotspots
• Hotspot Settings

System Services
Displays name of the **System Services** configurations along with number of entries:
• Web Proxy
• Authentication
• Guest User Settings
• Guest User Settings > SMS Gateway
• DoS > Settings
• DoS > Bypass Rules
• Web Content Filter > Configurations
• Web Content Filter > HTTP Scanning Rules
• Web Content Filter > HTTPS Scanning Exceptions
• Traffic Shaping Settings
• RED
• Wireless
• Advanced Threat Protection
• Malware Protection
• Log Settings
• Log Settings > Syslog Servers

Configuration
Displays name of the **Configuration** configurations along with number of entries:
• CLI Configuration
• Transparent Authentication

Objects

Assets
Displays name of the **Assets** configurations along with number of entries:
• Authentication Server
• Access Point Groups
• Web Servers

Content
Displays name of the **Content** configurations along with number of entries:
• File Type
• Custom IPS Patterns
• Custom Web Category
• URL Group
• Web App Auth Templates
Identity

Displays name of the **Identity** configurations along with number of entries:

- Certificate
- Certificate Authority
- Certificate Revocation Lists
- Groups
- User
- Clientless Users

Policies

Displays name of the **Policies** configurations along with number of entries:

- Schedule
- Access Time
- Surfing Quota
- Network Traffic Quota
- NAT
- IPSec
- IPS
- Web Filter
- Traffic Shaping
- Web App Protection
- Web App Authentication
- Device Access Profile
- Global App Traffic Shaping
- Application Group
- Hotspot Voucher Definition

Hosts and Services

Displays name of the **Hosts and Services** configurations along with number of entries:

- IP Host
- IP Host Group
- MAC Host
- FQDN Host
- FQDN Host Group
- Country Host
- Country Host Group
- Services
- Service Group

Provision Template
Click to provision the template configuration. On clicking Provision Template, Template Provision Summary window is displayed.

**Template Provision Summary**
Displays list of configuration entries. Select required entities and click Confirm. On clicking Confirm, Set Schedule window is displayed.

**Recent Activities**

**Time**
Displays time of the event in YYYY-MM-DD HH:MM format. The administrator can view following details for an activity: User, IP, Entity, Sub Entity, Action, Status.

**Message**
Details of change.

**Add Template**
Use the Add Device page to add new templates. Edit Template page has same parameters.

1. Go to **System Management > Device Settings > Managed Devices > Templates** and click **Add**.
2. Specify template name, which uniquely identifies the template.
3. Select the type of template to be added from the available options.

**New Template**
Select to store global configuration available at Sophos Firewall Manager in the form of template.

**Import Device Configuration**
Select to store configuration available at selected device in the form of template.

**Clone Template**
Select to add a new template with configuration stored in existing Template.

4. Select a device from the list of managed devices to store configuration available at that device in the form of template.
5. Select the template to be cloned.

![Figure 183: Add Template](image)

7. Click **Save**.
Provision Template

Provision Template page allows you to export a Template to Device(s). To provision a Template, refer the step shown below.

1. Go to System Management > Device Settings > Managed Devices > Template and click the Provision icon against the template to be exported.

   **Note**
   You can also provision a template from Device Configuration > Template Dashboard.

2. Click to apply the template configuration. On clicking Apply, Template Provision Summary window is displayed.

3. Select required entities and click Confirm to save the settings.

5.1.2 Maintenance

Maintenance facilitates handling the maintenance of the managed devices.

Using the Maintenance menu, you can configure following operation:

- **Backup & Restore** - Allows to manually take backup or schedule backup of the managed devices.
- **Compatibility Management** - Allows you get the compatibility information or acquire compatibility of upcoming OS versions.
- **Inactive Users Maintenance** - Allows you to get report on the inactive users, also to delete the inactive users.

Backup & Restore

Use Backup & Restore page to take backup of the managed devices and store on the Firewall Manager. Sophos Firewall Manager acts as a Backup repository for device backups. Administrator can restore this backup on the device whenever required. Sophos Firewall Manager automatically takes backup of all the managed devices at the predefined intervals and if required administrator can also take backup manually.

Administrator can schedule the backup or manually take the backup from System Management > Device Settings > Maintenance > Backup & Restore.

Schedule Backup

**Backup Frequency**

Select backup frequency.

In general, it is the best to schedule backup on regular basis. Depending on how much information you add or change will help you determine the schedule.

**Available options:**

- Never – Select this option if you do not want to take backup
- Daily – Configure time at which the backup should be taken.
- Weekly – Configure day and time at which the backup should be taken.
- Monthly – Configure day and time at which the backup should be taken.

**Backup Mode**
Select backup mode.

**Available options:**

- Local – Select this option to store Device backup file(s) on local machine.
- FTP – Select this option if you want to store Device backup file(s) on any configured FTP server.
- FTP Server IP – Specify IP address of FTP server
- FTP Path – Specify path of backup folder on FTP server
- Username – Specify FTP server username
- Password – Specify FTP server password
- Mail – Select this option to send backup file(s) on any configured email address.

![Backup Options](image)

Figure 184: Schedule Backup

**Manage Backup**

**Select Device**

Select the Device to take backup.

**Take Backup**

Click to take backup of the selected Device manually.

**Backup Date**

Date and time in DD/MM/YYYY HH:MM:SS format on which backup was taken

**Backup Type**

Type of backup – Manual or Scheduled

**Last Good Backup**

Select a backup to be stored as 'last good backup'. This backup will not be purged.

You can take maximum five backups including 'last good backup'.

**Restore**

Click to restore the downloaded backup.

**Download**

Click to download the backup.

Maximum 5 backups of every Device will be preserved but the Last good backup will be preserved all the time.
Sophos Firewall Manager

Compatibility Management

Sophos Firewall Manager allows the administrator to add and manage firewall devices.

As soon as a firewall device with new SFOS version is discovered in Sophos Firewall Manager, Firewall Manager automatically acquires the compatibility for the new SFOS version(s) from root server and displays it in the list of compatible SFOS versions.

With the new template compatibility support introduced, user can now create a template in Sophos Firewall Manager by importing configuration from a firewall running on a latest version released after the Sophos Firewall Manager.

Use this page to check the status of SFOS template compatibility in Sophos Firewall Manager.

Go to System & Monitor > Device Settings > Maintenance > Compatibility Management to manage compatible OS versions.

Firmware(# of devices)
Displays list and number of compatible OS versions.

Configuration Support
Displays the compatibility status of OS version.
Available options:
Compatible Incompatible

Template Support
Displays the compatibility status of template.
Available options:
Compatible Incompatible Not Available

Manage
Displays the firmware compatibility status.
Available options:
Remove Download

Enable
Click Enable to acquire compatibility list for the selected firmware.

Disable
Click Disable to remove device compatibility for the selected firmware.
Refresh List

Click to refresh the list of available OS versions.

Inactive User Maintenance

Inactive User Maintenance page is used to Manage Inactive Users. The following management options are available:

• Inactive Users Report – To generate and download Inactive User Reports.
• Delete Inactive Users – To delete Inactive Users.

To manage Inactive Users, go to System Management > Device Settings > Maintenance > Inactive User Maintenance.

Inactive Users Report

Generate Report

Specify the number of days after which the user is considered Inactive if not logged-on and the date from which the report is to be generated using calendar. Click Generate to generate the report.

Report

Shows the last generated Inactive Users Report. Click Download to download the generated reports.

![Generate report for users who have not logged-on for 865 days from 10/14/2015](image)

Figure 186: Inactive Users Report

Delete Inactive Users

Specify the number of days after which the users are to be deleted if not logged-on and the start date using calendar. Click Delete to delete the Inactive Users.

![Delete users who have not logged-on for 365 days from 10/14/2015](image)

Figure 187: Delete Inactive Users

5.1.3 Firmware

Use Firmware page to check for the latest available firmware for managed devices. To check for the availability of the latest firmware, go to System Management > Device Settings > Firmware.

Check for Latest Firmware

Click to check availability of latest firmware.

Model

Device Model number.

Applicable devices

Click ‘List device’ to view list of devices which can be upgraded with available firmware.

Applicable Version

Applicable firmware version.
**Size**
Size of downloadable firmware image in MB.

**Type**
Displays the type of firmware.
*Available Options:* BetaGA

**Action**
Click to apply downloaded firmware on the selected device(s).

**Apply Firmware**

**Schedule**
Click to schedule firmware upgrade. You can upgrade the selected device(s) with downloaded firmware immediately or you can choose to upgrade it later.

**Device**
Select the device to be upgraded with downloaded firmware.

### 5.1.4 Scheduled Task

Any configuration changes done on the Sophos Firewall Manager for managed devices can be applied to the device or group of device(s) immediately or can be scheduled at a later time.

**Scheduled Task**
Scheduled Tasks are the configurations which are to be executed at a set time or interval.

Go to [System Management > Device Settings > Schedule Task Schedule Task](#) to view list of task that are scheduled. You can delete or reschedule any scheduled task.

The page displays details of the task — event, entity and sub entity name, device for which task is scheduled and the schedule time.

### 5.1.5 Dynamic Objects

Dynamic objects — Host, Zone, Interface and Gateway are the network objects whose configurations vary from one device to another. Administrator can configure these objects in Sophos Firewall Manager and map them to individual devices. Administrator can use these objects while creating Firewall rule and various policies.

All of the dynamic objects are created using a similar method - create object and then specify the dynamic object-device mappings.

With dynamic objects, configuration of common objects like mail server, radius servers becomes easy as they need to be configured only once and then can be mapped.

This section covers the following topics:

- **Host** - View the list of dynamic hosts, add new hosts and manage all the configured hosts.
- **Zone** - Provides the list of all the zones including system zones and the administrator can manage the zones from this page.
- **Interface** - View port wise network (physical interface) and zone details.
- **Gateway** - Allows to manage gateway.
Host

Host is a logical building block used in defining security policies or NAT. By default, the numbers of hosts equal to the ports in the device are already created.

Host represents various types of addresses, including IP addresses, networks and Ethernet MAC addresses.

Hosts allow entities to be defined once and then be re-used in multiple refrential instances throughout the configuration. For example, an internal Mail Server with an IP address as 192.168.1.15. Rather than repeated use of the IP address while constructing security policies or NAT Policies, it allows creating a single entity called “Internal Mail Server” as a Host name with an IP address as 192.168.1.15. This host, “Internal Mail Server” can then be easily selected in any configuration screen that uses Hosts as a defining criterion.

By using hosts instead of numerical addresses, you only need to make changes in a single location, rather than in each configuration where the IP address appears. Using Hosts reduces the error of entering incorrect IP addresses, makes it easier to change addresses and increases readability.

Administrator can view the list of all the dynamic hosts from System Management > Device Settings > Dynamic Objects > Host.

Add Dynamic Host

The Add Dynamic Host page allows you to manually add IP host.

1. Go to System Management > Device Settings > Dynamic Objects > Host and select Add.
2. Enter dynamic host details.

Name

Name to identify the Host.

IP Family

Select IP family of the host.

Available Options: IPv4IPv6

Type

Select the type of host.

Available Options: Single IP Address Network IP Address with subnet IP Range

IP list to add assorted IP addresses. Use comma to specify assorted multiple IP addresses. Please note only Class B IP addresses can be added in IP list. IP addresses can be added or removed from IP list.

• MAC Address
• MAC list

![Figure 188: Add Dynamic Host details](image)

3. Enter Device - Host Mapping details.

Default

Select the host that is to be mapped with the particular device host.
Device

Select the device whose host is to be mapped with the above selected host.

Host

Select the host which is to be mapped.

![Device-Host Mapping](image)

4. Select **Save**.

Zone

A Zone is a logical grouping of ports/physical interfaces and/or virtual subinterfaces if defined. Zones provide a flexible layer of security for the firewall. With the zone-based security, the administrator can group similar ports and apply the same policies to them, instead of having to write the same policy for each interface.

Default - Zone Types

**LAN** – Depending on the device in use and network design, one can group one to six physical ports in this zone. Group multiple interfaces with different network subnets to manage them as a single entity. Group all the LAN networks under this zone.

By default the traffic to and from this zone is blocked and hence the highest secured zone. However, traffic between ports belonging to the same zone will be allowed.

**DMZ (DeMilitarized Zone)** - This zone is normally used for publicly accessible servers. Depending on the device in use and network design, one can group one to five physical ports in this zone.

**WAN** - This zone is used for Internet services. It can also be referred as Internet zone.

**VPN** - This zone is used for simplifying secure, remote connectivity. It is the only zone that does not have an assigned physical port/interface. Whenever the VPN connection is established, port/interface used by the connection is automatically added to this zone and on disconnection; port is automatically removed from the zone. Like all other default zones, scanning and access policies can be applied on the traffic for this zone.

**Local** – Entire set of physical ports available on your device including their configured aliases are grouped in LOCAL zone. In other words, IP addresses assigned to all the ports fall under the LOCAL zone.

To manage zones, go to **System Management > Device Settings > Dynamic Objects > Zone**.

Add Dynamic Zone

This page allows you to enter zone details.

1. Go to **System Management > Device Settings > Dynamic Objects > Zone** and select **Add**.
2. Enter Dynamic Zone details.

**Name**

Name to identify the zone.
Type

Select Zone Type - LAN, DMZ

Available Options: LAN - Depending on the device in use and network design, one can group one to six physical ports in this zone. Group multiple interfaces with different network subnets to manage them as a single entity. Group all the LAN networks under this zone.

Note
By default the traffic to and from this zone is blocked and hence the highest secured zone. However, traffic between ports belonging to the same zone will be allowed.

DMZ (DeMilitarized Zone) - This zone is normally used for publicly accessible servers. Depending on the device in use and network design, one can group one to five physical ports in this zone.

![Add Zone details](image)

Note
By default, entire traffic will be blocked except LAN to Local zone services like Administration, Authentication and Network.

3. Enter Device-Zone Mapping details.

**Default**
Select the zone that is to be mapped with the particular device zone.

**Device**
Select the device whose zone is to be mapped with the above selected zone.

**Zone**
Select the zone which is to be mapped.

![Device-Zone Mapping](image)

4. Select **Save**.
Interface

Use Interface page to view port wise network (physical interface) and zone details.

If virtual subinterface is configured for the physical interface, it is also displayed beneath the physical interface. Virtual subinterface configuration can be updated or deleted.

To manage Interfaces, go to System Management > Device Settings > Dynamic Objects > Interface.

Add Dynamic Interface

This page allows you to configure interfaces.

1. Go to System Management > Device Settings > Dynamic Objects > Interface and select Add.
2. Enter Dynamic Interface details.

Name

Name to identify the Interface.

IP Family

Select IP Family of the Interface.

Available Options: IPv4, IPv6

Type

Select Interface Type - Route and Bridge

For Route interface type you need to select Zone type:

Available Options: LAN – Depending on the device in use and network design, one can group one to six physical ports in this zone. Group multiple interfaces with different network subnets to manage them as a single entity. Group all the LAN networks under this zone.

Note

By default the traffic to and from this zone is blocked and hence the highest secured zone. However, traffic between ports belonging to the same zone will be allowed.

WAN - This zone is used for Internet services. It can also be referred as Internet zone.

DMZ (DeMilitarized Zone) - This zone is normally used for publicly accessible servers. Depending on the device in use and network design, one can group one to five physical ports in this zone.

Note

By default, entire traffic will be blocked except LAN to Local zone service likes Administration, Authentication, and Network.
3. Enter Device-Interface Mapping.

**Device**
Select the device.

**Interface**
Select the interface which is to be mapped.

4. Select **Save**.

**Gateway**

Device supports multiple gateways to cope with gateway failure problems. However, simply adding one more gateway is not an end to the problem. Optimal utilization of all the gateways is also necessary. Device’s Multi Link Manger provides link failure protection by detecting the dead gateway and switching over to the active link and provides a mechanism to balance traffic between various links.

To manage Gateway, go to **System Management > Device Settings > Dynamic Objects > Gateway**.

**Gateway Parameters**
This page allows you to add a new Gateway.

1. Go to **System Management > Device Settings > Dynamic Objects > Gateway** and select **Add**.
2. Enter Dynamic Gateway details.

**Name**
Name to identify the Gateway.

**IP Family**
Select IP family of the Gateway.

*Available Options:* IPv4,IPv6
3. Enter Device-Gateway Mapping details.

**Device**
Select the device.

**Gateway**
Select the gateway.

![Gateway Details](image)

**Figure 194: Add Gateway details**

3. Enter Device-Gateway Mapping details.

4. Select **Save**.

### 5.1.6 Change Control

Change Control page allows the administrator to view and manage list of revisions for the managed devices. Revisions are the configuration changes synchronized by the Sophos Firewall Manager and stored in Sophos Firewall Manager’s repository. Each revision has a unique Change List ID. Additionally, Export Configuration can be used to export configuration and the change list of devices or device groups.

**Change Control**

Change Control page allows the administrator to view and manage list of revisions for the managed devices. Revisions are the configuration changes synchronized by Sophos Firewall Manager and stored in Sophos Firewall Manager’s repository. Each revision has a unique Change List ID.

This page also allows the administrator to view list of affected configuration settings, compare different versions of configurations and roll back to previous configurations.

**View the list of Change Control**

**Devices**
Select the device to view configuration revisions.

**Refresh Button**
Click to refresh configuration revision list.

**View Revision**
Click to view device revision history.

**Create Snapshot**
Click to take snapshot of the current system configuration manually. In general, Firewall Manager takes snapshot of the system on set frequency. System Snapshot can be identified by * displayed against the entity name ‘System Snapshot’.

**Purge**

Click to purge revision history. This option is available only for those devices which are no longer managed by Sophos Firewall Manager.

**Time**

Revision time in YYYY-MM-DD HH:MM format.

**Change List**

Unique Change List ID.

**User Name**

Name of the user who has done configuration changes.

**IP Address**

IP address of the User.

**Entity**

Type of Entity.

**Entity Name**

Name of the Entity.

**Component**

Name of the component used for configuration change.

Possible components:

- Central Management
- GUI
- API

**Action**

Action performed on the configuration.

Possible Actions:

- Update
- Insert
- Delete
- Reorder
- Enable/Disable
- Custom

**Reverted Change List**

Displays list of Change List IDs on mouse over. Changes associated with the listed IDs have been reverted.

**Manage Details Icon**

Click to view details of the revision. Details include listing of all dependent entities.
Sophos Firewall Manager

For example if there is a change in policy, details will display list of dependent policies.

**Revert up to this change list Icon**

Click

![Up Arrow Icon](image)

to revert the changes done in the revision.

**Restore Icon**

Click

![Restore Icon](image)

to restore the configuration revision.

**Purge Icon**

Click

![Purge Icon](image)

to purge the configuration revision.

**View Revision History**

<table>
<thead>
<tr>
<th>Entity</th>
<th>Type of Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity Name</td>
<td>Name of the Entity</td>
</tr>
<tr>
<td>Time</td>
<td>Change List ID</td>
</tr>
<tr>
<td>Change List</td>
<td>Change List ID</td>
</tr>
<tr>
<td>Username</td>
<td>Name of the user</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the User.</td>
</tr>
<tr>
<td>Component</td>
<td>Name of the component used for configuration change.</td>
</tr>
<tr>
<td></td>
<td>Possible components:</td>
</tr>
<tr>
<td></td>
<td>• Central Management</td>
</tr>
<tr>
<td></td>
<td>• GUI</td>
</tr>
<tr>
<td></td>
<td>• API</td>
</tr>
<tr>
<td>Action</td>
<td>Action performed on the configuration.</td>
</tr>
<tr>
<td></td>
<td>Possible Actions:</td>
</tr>
<tr>
<td></td>
<td>• Update</td>
</tr>
<tr>
<td></td>
<td>• Insert</td>
</tr>
<tr>
<td></td>
<td>• Delete</td>
</tr>
<tr>
<td></td>
<td>• Reorder</td>
</tr>
</tbody>
</table>
• Enable/Disable
• Custom

Revision
Revision number. Click to view revision details.

Details Icon
Click details icon to view details of the revision in XML format.

Difference with Previous Version Icon
Click difference icon to compare revision versions.

View the Change List Details

Time
Revision time in YYYY-MM-DD HH:MM format.

User Name
Name of the user who has done configuration changes.

IP Address
IP address of the User.

Entity
Type of Entity

Component
Name of the component used for configuration change.
Possible components:
• Central Management
• GUI
• API

Action
Action performed on the configuration.
Possible Actions:
• Update
• Insert
• Delete
• Reorder
• Enable/Disable
• Custom

Revision
Revision number. Click to view revision details.
Details Icon
Click to view details of the revision in XML format.

Difference
Click to compare revision versions.

View Revision Details

Entity
Type of entity.

Sub Entity
Name of the sub entity.

Entity Name
Name of the entity.

Time
Revision time in YYYY-MM-DD HH:MM format.

Change List
Unique Change List ID.

Username
Name of the user who has done configuration changes.

IP Address
IP address of the User.

Component
Name of the component used for configuration change.
Possible components:
• Central Management
• GUI
• API

Action
Action performed on the configuration.
Possible Actions:
• Update
• Insert
• Delete
• Reorder
• Enable/Disable
• Custom
Revision

Revision number.

Details of change Icon

Click to view details of the revision in XML format.

Difference with Previous Version Icon

Click to compare revision versions.

Revert the Revision

Entity

Name of entity to be reverted.

Entity Name

Name of entity to be reverted.

Last Revision

Number of revisions. Click to view revision details.

Action

Action to be performed on the entity.

Possible Actions:

- Update
- Insert
- Delete
- Reorder
- Enable/Disable
- Custom

Details

Click to compare the revisions. It displays XML for current version and previous version configurations. The changes are highlighted by different color codes.

Export Configuration

Export Configuration allows the administrator to export configuration and the change list of Devices or Device groups. Multiple Devices or Device groups can be selected for export. To
export configuration go to **System Management > Device Settings > Change Control > Export Configuration**.

Select the Device or Device Groups from the drop down list and click **Export** to generate the configuration file in .TAR file format. To stop the export process, click **Cancel**.

![Export Configuration](image)

The .TAR file contains selected Device configuration along with the change list applicable to the Device or Device group. After generating, the .TAR file can be downloaded by clicking **Download**. The .TAR file must be extracted at preferred location to view configuration details and change list details including Device Name, Device Key and Time.

### 5.2 Monitor

Firewall Manager helps administrator to monitor the managed devices for surfing trends, attacks and outages. Graph and Alert Profiles can be used to monitor single device or group of devices.

It normally required Administrator to log on to individual device to view system resources and information but with profiles, administrator can view that same information for all the devices from Firewall Manager itself.

Firewall Manager also provides email alerts for monitoring device in case Administrator cannot log on to Firewall Manager to monitor system resources. Alert informs when an important event occurs on an device, such as a hard disk getting too full. Dashboard Monitoring Graph displays critical health information of the managed devices in graphical manner.

### 5.2.1 Device Monitor

Dashboard Monitoring Graph displays critical health information of the managed devices in graphical manner. SFM monitors the managed Device based on the following health parameters and statuses.

Administrator can also set Dashboard Monitoring thresholds specific to Models, Devices or a graphical manner. SFM monitors the managed device based on the following health parameters and statuses:

Administrator can also set Dashboard Monitoring thresholds specific to Models, Devices or a combination of both.
Device Monitor Settings

The administrator can set the threshold values for each of the monitoring parameter. For each parameter, the administrator can provide the threshold for 'Critical' and 'Warning' states.

You can set thresholds specific to Models, Devices or a combination of both. To set the threshold values for Model/Device/Model-Device, click Adjust Threshold and select among Model or Device, then click the manage icon to specify custom threshold values.

To save the values, click Apply.

However, if the administrator does not specify custom threshold values, the graphs are generated with Device Defaults.

Device Monitor Details

Device Monitor details page provides detailed information on the selected device card. The following information will be displayed for the device card.

Basic Information

Device Name
Displays the name the device.

Note
Manage Device Policy option can be used to directly take you to the device dashboard of the selected device. You can change the device policy configurations based on your observation in the Device Card.

Model Number
Displays Device Model.

Device IP
Displays the IP Address of the managed device.

Host Name
Host Name as configured on the Sophos XG Firewall device.

Security

Level and Count (Last 2 hours) are displayed for the following Security parameters:
- Web Virus
- Mail Virus
- Spam Mails
- Web Usage health
- Intrusion Attacks
- ATP Events
- Endpoint Health (Includes Red Health and missing Heartbeat)

License

Level and Status Expiry are displayed for the following License parameters:
- Base Firewall
- Network Protection
- Web Protection
Sophos Firewall Manager

- Email Protection
- Web Server Protection
- Sandstorm
- Enhanced Support
- Enhanced Plus Support
- Registered Email ID

**Note**

Click **Synchronize** to synchronize your device licenses.

**Resource**

**Level Percentage** and **(Last 2 hours)** are displayed for the following Resource parameters:

- CPU
- Memory
- Disk (Report)
- Disk (Config)

**Availability**

**Level, Status** and **Duration** are displayed for the following Availability parameters:

- Device Interface status
- Connection to Central Console
- Device Gateway status
- RED Status

**Device Monitor**

Device Monitor displays critical heath information of the Managed Devices in graphical manner. SFM monitors the Managed Devices based on the following heath parameters and statuses:

- Resource: CPU, Memory, Disk (Report) and Disk (Config).
- Availability: Connection to Central Management, Interface status, Gateway Status and RED Status.

**Note**

**Connection to Central Management** parameter is not available for the auxiliary device deployed in Active-Passive HA mode.

Device Monitor continuously monitors the Managed Devices for the wide range of security attacks, resource utilization and license statuses which helps the administrator to take informed decisions in resolving the risk landscape.
Flat view and card view allows you to monitor the status (Critical, Warning, Normal) of Managed Devices across a set of parameters for Security, Resource, License and Availability, based on their threshold values. In flat view, devices that need attention are automatically listed at the top on the basis of their monitor status.

You have the flexibility to customize threshold values for Critical, Warning and Normal levels as per your needs, using Device Monitor Settings.

**Open in Full Screen** allows you to display Device Monitor in full screen view.

**Note:** **Open in Full Screen** is available only if accessed from System Management > Monitor > Device Monitor.

### 5.2.2 Graphs

Graphs menu allows you to do the following:

- Add Profile
- View Graphs

### Profile

Profiles are used to generate graphs based on specific parameters. Administrator can add multiple profiles. Administrator can add profile for group of devices or single device. Tab for each profile is added on Graphs page.

Profile consists of following component:

**Device:** Select the devices to be included in the graph.

**Category:** Select from the list of categories to be included in graph.

- CPU Usage (%)
- Memory Usage (%)
- Disk Usage (%)
- Total Virus Attacks (Hits)
- Web Virus Attacks (Hits)
- Mail Virus Attacks (Hits)
- IPS Threats (Hits)
- Spam Mails (Hits)
- User Surfing Pattern (Hits)

Administrator can customize number of components for each profile.

To add or edit profile, go to **System Management > Monitoring > Graphs > Profile** and click **Add** or **Edit** Icon to modify profile details.

### Profile Parameters

**Title**
Specify name of the profile.

**Devices**
Select device(s) whose details are to be displayed on the profile. If the device(s) is/are deployed in HA (High Availability) mode then it displays Primary device.
Category

Select the components to be displayed on the profile for the device(s) selected in the above field.

Available options:

- CPU Usage (%)
- Memory Usage (%)
- Disk Usage (%)
- Total Virus Attacks (Hits)
- Web Virus Attacks (Hits)
- Mail Virus Attacks (Hits)
- IPS Threats (Hits)
- Spam Mails (Hits)
- User Surfing Pattern (Hits)

If the devices are deployed in HA (High Availability) mode, the graphs for the following categories will display information for both the devices separately.

- CPU Usage (%)
- Memory Usage (%)
- Disk Usage (%)

Add Profile

Profiles are used to generate graphs based on specific parameters. Administrator can add multiple profiles. Administrator can add profile for group of devices or single device. Tab for each profile is added on Graphs page.

Profile consists of following component:

**Device:** Select the devices to be included in the graph.

**Category:** Select from the list of categories to be included in graph.

- CPU Usage (%)
- Memory Usage (%)
- Disk Usage (%)
- Total Virus Attacks (Hits)
- Web Virus Attacks (Hits)
- Mail Virus Attacks (Hits)
- IPS Threats (Hits)
- Spam Mails (Hits)
- User Surfing Pattern (Hits)

Administrator can customize number of components for each profile.
Graphs

To view graphs based on profiles, go to **System Management > Monitoring > Graphs > Graphs**.

If multiple profiles are added, Tab for each profile is displayed.

Depending on the components selected at the time of adding profile, profile displays line graphs for the usage status of the CPU, memory and hard disk, user surfing pattern grouped into Neutral, Productive, Non Working and Unhealthy categories, virus, HTTP and mail attacks, IPS threats and spam mails.

If multiple devices are grouped under single profile, line graph of each device is plotted in each component.

### 5.2.3 Alerts

Firewall Manager allows administrator to create and send email alerts to the specified email address(es) based on predefined criteria. Firewall Manager alert notification ensures the concerned person receive an alert in situations like excess CPU, disk and memory usage or alarming count of viruses or IPS attacks.

**Profile**

SFM alert profile is a combination of Device(s), email address(s), and criteria to send alert notifications.

**DefaultAlertProfile** is a pre-configured alert profile. It can be modified but can’t be deleted.
Profile page can be used to view, add or edit alert profiles. Alert Status can be disabled or enabled from the Status column itself.

Add Alert Profile

Use this page to add or edit Profile parameters.

1. Go to System management > Monitor > Alerts > Profile > and click Add to add a new Alert Profile.
2. Specify the parameters based on description shown below.

Profile name
Specify a name to identify the Profile.

Send email(s) alert to
Specify comma separated recipient email address(s) to send alert notification through email.

You need to configure email server from System management > System settings > System > Notification > to send email alerts on specified email address(s).

Even if a mail server is not configured, the created alert will be displayed under Alerts tab.

Device(s)
Select devices or device groups.

Email type
Select Composite to send emails with alerts of all devices managed by Sophos Firewall Manager. Alternatively, select By device to send individual emails for alerts of each device.

Note
The email subject displays the firewall name and serial number, the SFM serial number, and the specified profile name of the alert.

Alerts criteria
Configure alert criteria. Select checkbox against criterion to be configured and specify value for the criterion.

Available criteria:

- Any subscription module expires within
- CPU usage exceeds
- Memory usage exceeds
- Disk usage exceeds
- Total Intrusion attack count exceeds
- Critical Intrusion attack count exceeds
- Web virus count exceeds
- Mail Virus count exceeds
- Total virus count exceeds
- Spam Mail count exceeds
- Objectionable + Unproductive surfing hits
- ATP events exceed
- End-points with Security Heartbeat in Red state exceeds
- End-points Security Heartbeat changed to Red state exceeds
- End-points with missing Security Heartbeat exceeds
- Device connected/disconnected from central management
- Device Gateway status change
- VPN connection status change
- HA status change
- RED tunnel status change
- Hostname Change

Specify the duration of sending notifications in Notify me field. The duration can be in hours or minutes.

**Description**

Specify description of the alert profile.

---

![Alert Profile Interface](image)

**Figure 198: Add Alert Profile**

3. Click **Save**.

**Alerts**

Firewall Manager allows you to view the list of generated alerts based on configured alert profiles. You can view these alerts from **System Management > Monitor > Alerts > Alerts**.
5.2.4 Event Viewer

Audit and System logs are an important part of any secure system that provides a comprehensive view into the current and past state of almost any type of complex system, and they need to be carefully designed in order to give a faithful representation of system activity.

They can identify what action was taken by whom and when. The existence of such logs can be used to enforce correct user behavior, by holding users accountable for their actions as recorded in the audit log. They are the simplest, yet also one of the most effective forms of tracking temporal information. The idea is that any time something significant happens you write some record indicating what happened and when it happened.

Device Events

Device Events page allows you to do the following operations:

- **View**: Load archived file to view and search. Click checkbox against the file and click View Data link, which opens a new page from where you can search the log. This process may take some time depending on the size of data. Note that this option is available if and only if Sophos iView is integrated with Firewall Manager. To configure iView integration, go to System Management > System Settings > Administration > iView >.

- **Unload**: Unload archived file. Click against the file to be unloaded.

- **Search Archived Logs**: Perform a refined search based on multiple criteria.

Search Archived Logs

Search Archived log page allows you to perform a refined search based on multiple criteria.

1. Go to System Management > Monitoring > Event Viewer > Device Events > and click the View Data link.
2. Under Advanced Search, select **Match all of the following** to get search result based on all criteria or **Match any of the following** to get search result based on any of the specified criterion.
3. Add searching criterion from the available options.

   **Available options**:
   - Upload Time
   - Log Component
   - Status
   - Username
   - IP address
   - Message

   The search can be performed using multiple search criteria. Click **+** to add a new search criterion and **-** to remove a search criterion.
4. Click **Search** to perform the search or **Clear All** to reset.
5. Select the view for search result display.
Graphs – Displays logs in graphical format. This option is available for following file types:

- System Logs
- Anti Virus
- IPS
- Authentication
- Audit Logs
  - Anti Virus
  - IPS

Formatted Logs: Displays logs in syslog format.

Raw Logs: Displays logs in syslog format.

View Graphical Search Results – Anti Virus

**Top Viruses Graph**

Graph displays number of counts per protocol.

**Top Web Viruses**

Graph displays number of counts per web virus.

**Top FTP Viruses**

Graph displays number of counts per FTP virus.

**Top Mail Viruses**

Graph displays number of counts per mail virus.

View Graphical Search Results – IPS

**Top Attacks Graph**

Graph displays number of counts per attack.

**Top Attackers Graph**

Graph displays number of counts per attacker IP address.

**Top Victims Graph**

Graph displays number of counts per victim IP address.

**Top Users Graph**

Graph displays number of counts per User.

Device Logs

Device Logs page allows to view the logs for modules like Application Filter, Web Filter, Malware and Firewall. This page gives consolidated information about all the events that have occurred.

To view logs of any of the managed Device, go to System & Monitor > Monitor > Event Viewer > Device Logs > and select module and Device and click Get Data.

Click Open PCAP to view packet capture. It will display the packet captures that are automatically filtered based on the values of the currently selected packet.

Click Download to export the logs in a CSV file. Hover over module icons for a detailed view.

Available Log Modules:
System – System logs provide information about all the system-related logs, including the logs for VPN events.

Web Filter – Web filter logs provide web surfing details like accessed/blocked sites, users trying to access the blocked websites etc. and the action taken by the device (Allowed or Blocked).

Application Filter – Application filter logs provide details about applications to which access was denied by the device.

Malware – Malware logs provide information about the viruses identified by the device.

Email – Email logs provide information about the mail traffic processed by the device.

Firewall – Firewall logs provide information about how much traffic passes through a particular firewall rule and through which interfaces.

IPS – IPS logs provide information about the intrusion attempts detected/blocked by the device.

Authentication – Authentication logs provide information about all the authentication logs including firewall, VPN and User Portal authentication.

Admin – Admin logs provide information about administrator event and tasks.

WAF – WAF logs provide information about HTTP/S requests and action taken on the same.

Advanced Threat Protection - ATP logs provide information related to threats detected/blocked by the device.

Security Heartbeat - Security Heartbeat logs provide information on Heartbeat connection and status.

Management System Events

Event Viewer page allows to view the events for various modules – Policy Configuration, System, System Events. This page gives consolidated information about all the events that occurred for the respective modules and information can be filtered based on Event ID, Username or IP address.

To view Firewall Manager events, go to System > Monitoring > Event Viewer > Management System Events >, select date and any of the following modules:

- Policy Configuration Events – Provides information of the administrative events and task occurred at global and device level.
- System Management – Provides information of the administrative events and task occurred at Firewall Manager.
- System Events – Provides information of the system events and tasks occurred at Firewall Manager.

Note
In the combined filter for User Name and IP Address, you can enter value in either one of them or a combination of both.

5.3 System Settings

System Settings allows configuration and administration of SFM Device for secure and remote management as well as administrative privilege that you can assign to admin users. It also provides the basic system settings of the Web Admin console. Configuration of several non-network features, such as SNMP, custom messages, portal setting and themes can also be done through System.
System also allows basic configuration of SFM including GUI localization, mail server, customized messages, web & parent proxy settings, themes and outlook for the Captive portal. You can also configure Network entities, Firmware, Signatures and Diagnostic utilities for Firewall Manager using System Settings.

5.3.1 Administration

Administration allows you to manage device licenses and time, administrator access, centralized updates, network bandwidth and device monitoring and user notifications.

Settings

Use Settings page to configure administrative access settings. The page also allows you to configure localization, signature port and change control settings.

To manage the administration settings, go to System Management > System Settings > Administration > Settings >.

Web Admin Settings

**HTTP Port**

Provide the port number to configure HTTP Port.

By default, the HTTP Port number is 80.

**HTTPS Port**

Provide the port number to configure HTTPS Port for Secured Web Admin Console access.

By default, the HTTP Port number is 443.

**Syslog Port**

Displays Syslog port number configured to communicate with managed SFOS.

**Syslog (Secure)**

Displays Secure Syslog port number configured to communicate with managed SFOS.

**Certificate**

Certificate that will be used by Administrator of Firewall Manager Web Admin Console.

![Web Admin Settings](image)

Figure 199: Web Admin Settings

Content Distribution Port Settings
**Content Distribution Port**

Provide the port number to distribute updates for pattern.

![Content Distribution Port](image)

Figure 200: Content Distribution Port Settings

**Administrator Password Complexity Settings**

Password Complexity can be configured to ensure that administrators are using secure passwords.

- Enable Password Complexity Settings to enforce following constraints:
  - Minimum Password length. Configure minimum characters required in the password. By default, the Minimum Password length is eight (8) characters.
  - Require minimum one Upper and lower case alphabet
  - Require minimum one number i.e. 0 - 9
  - Require at least one special character e.g. @, $, %
  - Password cannot be same as username.

![Enable Password Complexity Check](image)

Figure 201: Administrator Password Complexity Settings

All the enabled constraints are applied to administrator user password.

**Change Control Settings**

**Enable Change Control**

Click to enable Change Control in devices which will be added to Firewall Manager.

**Cascade on all managed devices**

Click to enable Change Control in all existing managed devices.

**Create a system snapshot on of (X) every month**

Specify the date on which you want to auto-generate System Snapshot. If you specify "5", Firewall Manager will auto-generate system snapshot on 5th date of every month. Default value is 1st date of every month.
Sophos Adaptive Learning

The product sends information periodically to Sophos which is used for the purpose of improving stability and protection effectiveness, and prioritizing feature refinements. It includes configuration and usage information, and monitoring threshold data.

Configuration and usage data such as Device information (e.g. model, hardware version), Firmware and License information, Features in use [status, on / off, count] (e.g. configuration applied to 1 or more devices, signature distribution status), amount of configured objects and items (e.g. count of managed devices and groups, count of hosts, policies), Product errors, CPU, memory and disk usage (in percentage), is collected by default.

No user-specific information or personalized information is collected. The information is transmitted to Sophos over HTTPS.

Send Monitoring Threshold data

Monitoring Threshold data includes (enabled by default, excluded when option is deselected) the following to improve the default threshold settings and alert criteria given with the product across models:

- Monitoring Threshold values per model.
- Alert threshold criteria/values per model.

Disk Usage Alerts

Use the settings below to configure sending automatic email alerts to a specified email address, when the hard disk usage of your SFM device exceeds the specified threshold value.

Send Email Alert

Select this to receive email alerts when disk usage exceeds configured Disk Usage Threshold.

Disk Usage Threshold

Enter disk usage threshold value in percentage above which email alerts should be sent.

Current Disk Usage
Displays current available used disk space in percentage.

Note: Three emails will be sent one per day after disk usage exceeds configured Threshold Value.

For virtual SFM once the disk usage exceeds the configured Threshold Value you can increase the size of disk, follow below steps to do so for various virtual machines:

1. **VMware Virtual Machine:**
   a) Open VMware Virtual Machine where SFM is deployed.
   b) Click **Edit virtual machine settings**.
   c) Click Hard Disk 2 then click on **Expand...**.
d) Enter **Maximum disk size** as required and click **Expand**.
2. **Xen Virtual Machine:**

   a) Open Xen virtual machine where SFM is deployed.

   b) Switch to *Storage* tab, right click on disk-2 and select *Properties*.

   c) Click on *Size and Location*. 
d) Update disk size as required.

e) Click on OK to save.

3. **KVM**: Disk size for KVM can be increased by using the following command:

```
qemu-img resize AUXILIARY-DISK.qcow2 +(disk_size)GB
```

To execute this command, navigate to `AUXILIARY-DISK.qcow2` file. For example if your file is stored in SFM folder then navigate to SFM (/home/SFM/) and execute the command (qemu-img resize AUXILIARY-DISK.qcow2 +500 GB).

4. **Hyper-V virtual machine**:

a) Open Hyper-V virtual machine where SFM is deployed.

b) Go to File > Settings.

c) Select IDE Controller1 Auxilary Hard disk and click on Edit.

d) Go to Choose Action > Configure Disk.

e) Update disk size as required and click on Finish.
Access Profile

Use the Access Profile page to create profiles for Administrators. Role-based administration capabilities are provided to offer greater granular access control and flexibility. Profile sets up access levels for the administrative users. Profile determines the privileges of the administrator and the administrator’s access to managed Sophos XG Firewall Device and SFM features.

Access profile page is divided into access control categories for which you can enable None, Read-only, or Read-Write access. For ease of use by default, SFM Device is shipped with profile “Administrator” with full privileges and “Device Administrator” with privileges over specific Devices.

To manage default and custom profiles, go to System Management > System Settings > Administration > Access Profile.

Note

• You cannot delete the default profiles.
• You cannot delete profile assigned to any user.

You can view added profiles, add new profiles or edit or delete existing profiles.

Add Access Profile

Use this page to add an Access Profile.

1. Go to System Management > System Settings > Administration > Access profile and click Add.
2. Enter Profile details.

Profile Name
Name to identify the profile. By default Firewall Manager is shipped with two profiles.

- Administrator – super administrator with full privileges device
- device Administrator – read-write privileges for selected device(s)

**Configuration**

Click on the access level you want to provide to a profile. There are three levels of access each of the created profile can have.

**Available Options:**

- **None**: No access to any page
- **Read-Only**: View the pages
- **Read-Write**: Modify the details

Access levels can be set for individual menus as well. You can either set a common access level for all the menus or individually select the access level for each of the menu.

Click the **+** icon against a menu to view the items under that menu.

For example, if you set access level as Read-Only against the Web Filter, the profile user would only be able to view the Web Filter menu but would not be able to make any modifications.

To make modifications, Read-Write option is to be used.
3. Click **Save**.

**Users**

Use the **Users** page to add administrators. It allows configuring administrator access to the Sophos XG Firewall device, including the level of access and which devices administrator have access to. All administrator settings can be configured only when you are logged in as the admin administrator. The admin administrator is the only user with complete access to the entire Firewall Manager device options.

To manage users, go to **System Management > System Settings > Administration > Users >**.

You can view added users, add new users or edit or delete existing users.
Add User

1. Go to **System Management > System Settings > Administration > Users >** and click **Add** to register a new user.
2. Specify user details based on the description shown below.

**Username**
Specify username, which uniquely identifies user and will be used for login.

**Authentication Type**
Select type of authentication for the user:
- Local
- External – LDAP, Radius, TACACS+
Refer Authentication Server page for details.

**Status**
Select the status of the user.

**Available Options:**
- Active
- Inactive

**Password/Confirm Password**
Specify Password for the user.

**Email ID**
Specify Email address of the user.

**Access Profile**
Select the Profile.
Administrator will get access of various Web Admin console menus as per the configured profile.
You can create a new profile directly from this page itself and attach to the user.

**Accessible Device**
Select the device to be assigned to the user.

**Device Group**
Select the Device Group for the user. The user will be able to manage all devices in the group, in addition to the individual devices selected earlier.

**Note**
Only Super Administrator of Firewall Manager will be able to assign or update device groups.
3. Click **Save**.

**Device Access**

Device access allows limiting the Administrative access of the following device services from various ports:

- HTTP
- HTTPS
- Telnet
- SSH
- Ping
- Syslog
- Syslog (Secure)

To manage access to device, go to System Management > System Settings > Administration > Device Access.
Default Access Control Configuration

When Firewall Manager is connected and powered up for the first time, it will have a default access configuration. HTTP, HTTPS, Telnet, SSH, Ping, Syslog services will be enabled for administrative functions from Port A and B.

Custom Access Control Configuration

Use access control to limit the access to Firewall Manager for administrative purposes. Enable/disable access to Firewall Manager using following services from the specified port: HTTP, HTTPS, Telnet, SSH, Ping, Syslog, Syslog (Secure).

Live Users

Live Users page displays list of currently logged on users and their important parameters. Use Live User page to manage live users of Firewall Manager.

To manage live users, go to System Management > System Settings > Administration > Live Users > .

iView

iView page allows administrator to configure Sophos iView as centralized reporting server for all managed Devices.

To configure iView as the reporting server, refer the steps shown below.

1. Go to System Management > System Settings > Administration > iView > and click Enable iView Integration.
2. Specify the iView Server details based on the description shown below.

Username

Displays Username of iView administrator user i.e. admin. This field cannot be updated.

Password

Specify password of iView administrator user.

Re-enter the password to confirm.

Note

Password can only be edited if Enable iView Integration is selected.

iView internal IP address

Specify LAN IP address of iView Web Admin Console.

Web Admin Port

Specify port number to access iView Web Admin Console over LAN.

iView external IP address

Specify WAN IP address of iView Web Admin Console.
Specify port number to access iView Web Admin Console over Internet.

Select Syslog Server
Select Syslog Server to send log data of all managed Devices. The syslog server can be configured from Policy > System > Configuration > Log Settings > Syslog Servers.

Sync Configuration Changes only
Click to synchronize only newly added or updated entries immediately.

Sync Full Configuration
Specify the time interval at which entire device-user repository will be synchronized.

3. Click **Apply**.

API Explorer
Application Programming Interface (API) is an interface which allows third party applications to communicate with Firewall Manager.

This page enables the administrator to access Firewall Manager’s XML based API to retrieve a certain set of information from Firewall Manager.

Firewall Manager API supports ‘get’ API request type to retrieve the information.

To access Firewall Manager API, go to System Management > System Settings > Administration > API.

API Explorer

API Request
Write the API query. Based on the API query, API response will be displayed.

Submit
Click to submit XML query.

API Response
Displays response of submitted XML query.

5.3.2 System

Use **System** pages to configure mail server, set administrator email ids, set system date and time and NTP server.

This section covers the following topics:

- **Certificate** - Use to generate self-signed certificate or upload a certificate.
- **Authentication Server** - Use to manage authentication server.
- **Authentication Preferences** - Allows to set preference for authentication server(s) to decide the order in which they will be used.
- **Notification** - Allows to configure mail-server settings.
- **Time** - Use to configure time settings.
- **HA** - Use to configure or disable HA.
Certificate

Certificate page allows you to upload a certificate. A digital certificate is a document that guarantees the identity of a person or entity and is issued by the Certificate Authority (CA). Certificates are generated by the third party trusted CA. They create certificates by signing public keys and identify the information of the communicating parties with their own private keys. This way it is possible to verify that a public key really belongs to the communicating party only and not been forged by someone with malicious intentions.

Certificate page allows you to upload third party certificate. To manage Certificates, go to System Management > System Settings > System > Certificate.

Add Certificate

Use the Add Certificate page to add new certificate.

2. Specify Certificate details based on the given description.

Name

Name to identify the Certificate.

Password

Password for a Certificate used for authentication.

Confirm Password

Re-enter password for confirmation.

Certificate

Specify certificate to be uploaded. Use Browse to select the complete path.

Private Key

Specify private key for the certificate. Use Browse to select the complete path.

![Figure 206: Upload Certificate](image)

3. Click OK.

Authentication Server

Device supports user authentication against:

- an LDAP Server
- a RADIUS Server
- an internal database defined in Device

User authentication can be performed using local user database, RADIUS, LDAP or any combination of these.

Local Authentication
Device provides a local database for storing user information. You can configure device to use this local database to authenticate users and control their access to the network. Choose local database authentication over LDAP or RADIUS when the number of users accessing the network is relatively small. Registering dozens of users takes time, although once the entries are in place they are not difficult to maintain. For networks with larger numbers of users, user authentication using LDAP or RADIUS servers can be more efficient.

Combination of external and local authentication is useful in large networks where it is required to provide guest user accounts for temporary access while a different authentication mechanism like RADIUS for VPN and SSL VPN users provides better security as password is not exchanged over the wire.

**External Authentication**

External Authentication Servers can be integrated with the device for providing secure access to the users of those servers.

To manage external authentication servers, go to **System Management > System Settings > System > Authentication Server**.

**Add Authentication Server**

To manage external authentication servers, go to **System Management > System Settings > System > Authentication Server** and select **Add**.

**Server Type**

Select the service with which you want to use your network.

**Available Options:** LDAP Server, RADIUS Server, TACACS+ Server

**Configure LDAP Server**

Configure LDAP Server allows you to configure an LDAP server to authenticate users for SFM login.

To log in, users need to use their Windows authentication tokens. SFM authentication request to the LDAP server, which authenticate the user based on the token.

1. Go to **System & Monitor > System Settings > System > Authentication Server** and select **Add**.
2. Select **Server Type** as LDAP Server.
3. Enter LDAP details.

**Server Name**

Name to identify the server.

**Authentication Server IP**

Specify LDAP Server IP address.

**Port**

Specify Port number through which Server communicates.

Default port is 389.

**Version**

Select LDAP version. For example, 2. Default value is Version 3.

**Base DN**

Specify the base distinguished name (Base DN) of the directory service, indicating the starting point for searching user in the directory service. If you are not aware about Base DN, click Get Base DN to retrieve base DN.

The top level of the LDAP directory tree is the base, referred to as the "Base DN". A base DN usually takes one of the three forms: Organization name, Company’s Internet Domain name or DNS domain name. For example dc=google, dc=com

**Administrator**

Specify Username for the user with Administrative privileges for LDAP server.
**Password**

Specify Password for the user with Administrative privileges for LDAP server

**Authentication Attribute**

Set authentication attribute. It is the attribute used to perform user search.

By default, LDAP uses uid attribute to identify user entries. If you want to use a different attribute (such as given name), specify the attribute name in this field.

![Figure 207: Add LDAP Server](image)

4. Click **Test Connection** button to check the connectivity between LDAP and the device.
5. Click **Save**.

**Note**

SFM will not fetch user directly from LDAP server. SFM admin must create user with **Authentication Type - External** from **System & Monitor > System Settings > Administration > User**.

**Configure RADIUS Server**

Configure RADIUS Server allows you to configure a RADIUS server to authenticate users for SFM login.

RADIUS stands for Remote Authentication Dial In User Service and is a protocol for allowing network devices to authenticate users against a central database. In addition to user information, RADIUS can store technical information used by network devices such as protocols supported, IP addresses, telephone numbers, routing information, and so on. Together this information constitutes a user profile that is stored in a file or database on the RADIUS server.

RADIUS servers provide authentication, authorization, and accounting functions but device uses only the authentication function of the RADIUS server.

Before you can use RADIUS authentication, you must have a functioning RADIUS server on the network.

1. Go to **System & Monitor > System Settings > System > Authentication Server** and select **Add**.
2. Select Server Type as RADIUS Server. If user is required to authenticate using a RADIUS server, device needs to communicate with RADIUS server for authentication.
Sophos Firewall Manager

3. Enter the details.

**Server Name**
Name to identify the RADIUS Server.

**Server IP**
Specify RADIUS Server IP address.

**Authentication Port**
Specify port number through which server communicates.
Default port - 1812

**Shared Secret**
Specify share secret, which is to be used to encrypt information passed to the device.

![Figure 208: Add RADIUS Server](image)

4. Click **Test Connection** button to check the connectivity between RADIUS and the device.

5. Click **Save**.

**Note**
SFM will not fetch user directly from RADIUS server. SFM admin must create user with **Authentication Type** - **External** from **System & Monitor > System Settings > Administration > User**.

**Configure TACACS+ Server**

**Configure TACACS+ Server** allows you to configure a TACACS+ server to authenticate users for SFM login.

TACACS+ (Terminal Access Controller Access Control System Plus) provides access control for routers, network access servers and other networked computing devices via one or more centralized servers.

TACACS+ provides separate authentication, authorization and accounting services but the device uses only the authentication function of the TACACS+ server.

Before you can use TACACS+ authentication, you must have a functioning TACACS+ server on the network.

1. Go to **System & Monitor > System Settings > System > Authentication Server** and select **Add**.
2. Select Server Type as TACACS+ Server. If the user is required to authenticate using a TACACS+ server, device needs to communicate with TACACS+ server for authentication.
3. Enter the details.

**Server Name**
Enter name to identify the TACACS+ Server.

376 Copyright © Sophos Limited
**Server IP**

Specify TACACS+ Server IPv4 Address.

**Port**

Specify port number on the TACACS+ server to which the device sends the authentication request.

Default - 49

**Shared Secret**

Provide shared secret, which is used to encrypt information passed to the device.

![Figure 209: Add TACACS+ Server](image)

4. Click **Test Connection** button to check the connectivity between TACACS+ and the device.
5. Click **Save**.

**Note**

- SFM will not fetch user directly from TACACS+ server. SFM admin must create user with **Authentication Type** - **External** from **System & Monitor > System Settings > Administration > User**.
- Device supports CHAP & PAP authentication methods to authenticate L2TP/PPTP users against TACACS+ server.
- Device supports PAP authentication protocol to authenticate Firewall/Administrator/VPN users against TACACS+ server.

**Authentication Preferences**

You can set preference for authentication server(s) to decide the order in which they will be used. Set preferences for added external servers from **System Management > System Settings > System > Authentication Preferences**.

Enter External Authentication Server details.

**Authentication Servers List**

Select authentication server from Authentication Servers list. Selected servers will be displayed under ‘Selected Authentication Server’ list.
Note

Figure 210: Authentication Preference

- Selected Authentication Server list order displays preferences.
- Do not forget to click Apply after adding.

Notification

Configure mail server IP address, port and email address where the Firewall Manager has to send and receive alert emails.

To configure mail server settings, go to System Management > System Settings > System > Notification.

Mail Server Settings

Mail Server IP Address/FQDN - Port

Specify Mail server IP address or FQDN and port number.

Authentication Required

If Enabled, specify authentication parameters i.e. username and password.

Figure 211: Mail Server Settings

Email Settings

From Email Address

Specify the email address from which the notification is to be mailed.
**Send Notification to Email Address**

Specify the email address to which the notification should be mailed.

<table>
<thead>
<tr>
<th>From Email Address *</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Notifications to Email Address *</td>
<td></td>
</tr>
</tbody>
</table>

Figure 212: Email Settings

**Time**

Device's current date and time can be set according to the device's internal clock or synchronized with an NTP server. Device clock can be tuned to show the right time using global time servers so that logs show the precise time and the device's internal activities can also happen at a precise time.

To configure time settings, go to **System Management > System Settings > System > Time**.

**Current Time**

Current system time.

**Time Zone**

Select time zone according to the geographical region in which the device is deployed.

**Set Date & Time**

Select to set device's date and time.

**Date**

Set the date of device's internal clock.

**Time**

Set the time of device's internal clock.

**Sync with NTP server**

Select if you want device to synchronize automatically its time with an NTP server.

**Use pre-defined**

Use the pre-defined NTP servers - asia.pool.ntp.org & in. pool.ntp.org or specify NTP server IP address or domain name to synchronize time with a specific NTP server.

**Use Custom**

If custom NTP server is defined, time will be synchronized with custom server and not the pre-defined servers.

Firewall Manager uses NTP Version 3 (RFC 1305). One can configure up to 10 NTP servers. At the time of synchronization, it queries each configured NTP server sequentially. When the query to the first server is not successful, device queries second server and so on until it gets a valid reply from one of the NTP servers configured.

**Sync Status**

Click on ‘Sync Now’ Button to synchronize device clock with the NTP Server.
High Availability (HA)

Hardware failure such as a failure of the power supply, hard disk, or processor is the main reason behind the failure of Internet security system and/or a firewall. To provide reliable and continuous connection to the Internet and to provide central management, two devices can be configured to function as a single device and provide HA.

Note
This feature is available only in hardware devices.

Clustering Technology is used to ensure HA. In a cluster, two devices are grouped together and instructed to work as single entity.

This section covers the following topics:
- HA terminology
- Configuring HA

How Cluster works

Device offers high availability by using Virtual MAC Address shared between a Primary device and an Auxiliary device linked together as a “cluster”.

Primary and Auxiliary device are physically connected over a dedicated HA link port.

Typically, traffic enters your network by passing through a network switch but in HA one of the devices in the cluster has a Virtual MAC Address and traffic is forwarded to the device which has the virtual MAC Address.
The device which has virtual MAC Address is the Primary device and other peer is Auxiliary device. Primary device acts as a load balancer and forwards the traffic to the Auxiliary device for processing. Auxiliary device can process traffic only if cluster is operating in the Active-Active mode.

If configured in Active-Passive mode, Primary device processes the entire traffic while Auxiliary device waits in a ready mode to operate as the Primary device, in case Primary device or any of the monitored links fail.

Auxiliary device monitors the Primary device through the dedicated HA link and if it does not receive any communication within the pre-configured time, the Primary device is considered to have failed. In this case, Auxiliary device takes ownership of the virtual MAC Address from Primary device and acts as temporarily as Primary device. Once Primary device is up it automatically takes over from the Auxiliary device.

The device from which HA is enabled goes in Standalone state while the other device rebooted. Once the other device comes up, synchronization process starts. It synchronizes time zone, signatures (Anti Virus, Web Categorization, IPS and Application), database configurations (Firewall Manager and Managed devices), backups (Firewall Manager and Managed devices) and logs (Managed devices).

After a successful synchronization, the two Firewall Manager devices come into Primary – Auxiliary state. In this state every event which takes place on Primary device gets reflected in Auxiliary device immediately.

When the Primary device goes down an automatic Failover takes place and the Auxiliary device goes into Standalone state. This process may take 10 to 15 seconds depending on size of data. During this transition period the administrator may lose access to Firewall Manager HA cluster for a while.

**HA terminology**

1. **HA Cluster**
   Group of two devices instructed to work as a single entity. Every HA Cluster has one Primary device and one Auxiliary device. The Primary device controls how the cluster operates. The roles that the Primary and Auxiliary devices play in the cluster depend on the configuration mode.

2. **HA Configuration Modes**

   **Active-Active**
   A configuration of HA cluster consists of a Primary device and one Auxiliary device. In this mode, both Primary device and Auxiliary device process traffic while primary unit is in charge of balancing the traffic. Decision of load balancing is taken by the Primary device. Auxiliary device can take over only in case of a primary unit failure. (Currently Firewall Manager can not be deployed in Active-Active HA mode).

   **Active-Passive**
   A configuration of HA cluster which consists of a Primary device and an Auxiliary device. In this mode, only the Primary device processes traffic while Auxiliary device remains in standby mode, ready to take over if a Primary device failure occurs.

3. **Primary device**
   The Primary device also tracks the status of all cluster devices. In an Active-Active cluster, the Primary device receives entire network traffic and acts as the load balancer to redirect traffic to Auxiliary device.
In an Active-Passive cluster, the Primary device processes the network traffic while Auxiliary device does not process any traffic but remains ready to take over if Primary device fails.

4. Auxiliary device
Auxiliary device is always waits to become the Primary device.

In an active-active cluster, Auxiliary device processes the network traffic assigned to it by the Primary device. In case Primary device fails, Auxiliary device becomes the Primary device. In an active-passive cluster, Auxiliary device does not process network traffic and is in stand-by. It becomes active only when Primary device is not available to process the traffic.

5. Dedicated HA Link Port
Dedicated HA link is a direct physical link between the devices participating in HA cluster.

6. Load Balancing
An ability of HA cluster of balancing the traffic between nodes in the HA cluster.

7. Monitored Interface
Set of interfaces that are selected to be monitored. Each device monitors its own such interface and if any of them is goes down, device will remove itself from the cluster and failover occurs.

8. Virtual MAC
It is a MAC Address associated with the HA cluster. This address is sent in response when any of the machines make an ARP request to HA cluster. It is not the actual MAC Address and is not assigned to any interface of any unit in the cluster.

A Primary device owns the MAC Address and is used for routing network traffic. All external clients use this address to communicate with the HA cluster. In case of failover, new Primary device will have the same MAC Address as the failed Primary device. The cluster device which has a Virtual MAC Address acts as a Primary device.

9. Primary State
In Active-Active mode, the device that is in charge of receiving all the traffic and load balancing is said to be in "Primary" state. An device can be in "Primary" state only when the other device is in "Auxiliary" state.

In Active-Passive mode, the device in charge of processing all the traffic is said to be in the "Primary" state. An device can be in "Primary" state only when the other device is in "Auxiliary" state.

10. Auxiliary State
In Active-Active mode, the device that receives the traffic to be processed by it from the Primary device is called to be in "Auxiliary" state. An device can be in "Auxiliary" state only when the other device is in "Primary" state

In Active-Passive mode, the device which is not processing the traffic is called to be in "Auxiliary" state. An device can be in "Auxiliary" state only when the other device is in "Primary" state.

11. Standalone State
An device is called to be in Standalone state when it can still process network traffic and when the other device is not in position to process network traffic (i.e. in "Fault" state or shut down).

12. Fault State
An device is in fault state when it cannot process network traffic if a device or link fails.

13. Peer
Once the HA cluster is configured, cluster devices are termed as Peers i.e. for Primary device, Auxiliary device is its peer device and vice versa.
14. **Synchronization**
   The process of sharing the various cluster configuration, between Cluster devices (HA peers). Reports generated are not synchronized.

15. **Device failover**
   If an device does not receive any communication within the predetermined period of time from the HA peer, the peer device is considered to have failed. This process is termed as Device Failover as when this occurs, the peer device is taken over.

16. **Link Failover**
   Both the device in an HA cluster continuously monitor the dedicated HA link and the interfaces configured to be monitored. If any of them fails it is called link failure.

17. **Session failover**
   Whether it is a device or link failover, session failover occurs for forwarded TCP traffic except for the virus scanned sessions that are in progress, VPN sessions, UDP, ICMP, multicast, and broadcast sessions and Proxy traffic.

   Device normally maintains session information for TCP traffic which is not passing through proxy service. Hence, in case of failover, the device which takes over will take care of all the sessions (TCP session not passing through proxy application). The entire process is transparent for the end users.

**Configure HA**

Use to
- Configuring Primary/Auxiliary Devices
- Disable HA

**Points to be noted**

**Behavior**
- HA can be disabled from Primary device only which results into disabling HA on both the devices.
- After disabling HA, Primary device IP schema will not change.
- After disabling HA, Auxiliary device will reboot with Factory Default settings (if connected).
- All administrators can login to auxiliary device but the device will be accessible as read-only.
- Make sure that the IP Address of HA link port of Primary and Auxiliary devices are in same subnet.
- Disabling HA is required to restore backup.

**Before configuring HA**

Before attempting to configure two devices as an HA pair for Hardware Failover, check the following requirements:
- Both devices in the HA cluster i.e. Primary and Auxiliary device must be registered and have same number of interfaces. Both the member devices should be of the same model.
- Both devices in the HA cluster must have the same version installed on it.
- Two separate licenses are required, one for the Primary device and other for the Auxiliary device.
- Cables to all the monitored ports on both the devices must be connected. Connect dedicated HA link port of both the devices with crossover cable.
- Dedicated HA link port should have a unique IP Address on both the devices. SSH should be enabled for both the devices on DMZ Zone.

*Configuring Primary/Auxiliary Devices*
Use this page to configure the Primary/Auxiliary device.

**Note**
- No changes in the firewall configuration. Only need to enable SSH on the dedicated interface.
- Allow SSH traffic for dedicated HA link port on both the devices through Device Access.

1. Go to **System Management > System Settings > System > HA**.
2. Enter High Availability details.

**Serial Number**
Displays Serial Number of Device.

**Peer Serial Number**
Displays peer’s Serial Number if HA is enabled.
In case of Primary Device, it displays the Auxiliary Serial Number.
In case of Auxiliary Device, it displays the Primary Serial Number.

**Initial HA Device State**
Select to set initial device state from the available options.
Available Options:
- Primary
- Auxiliary

**Passphrase**
- **Passphrase** - Specify a passphrase for communication.
- **Confirm Passphrase** - Confirm the specified passphrase.

**Note**
To configure HA, both devices in the cluster must have the same passphrase.

**Dedicated HA Link Port**
Specify HA link port.
HA peers are physically connected using a crossover cable through this port. The same port must be used as an HA link port on peer Device also.
For example, if port E is configured as HA link port on Primary Device then use port E only as HA link port on Auxiliary Device. Make sure that the IP Address of HA link port for both, the Primary Device and Auxiliary Devices are in same subnet and SSH is enabled on both. Cluster Devices use this link to communicate cluster information and to synchronize with each other.

**Peer HA link IP**
Specify IP Address configured on the HA link port of the peer Device.

**Note**
Available only for Primary Device.

**Peer Administration Port**
Specify Administration Port for Auxiliary Device. This port can be used for administration purpose.
Note  
Available only for Primary Device.

Peer Administration IP  
Specify Administration IP Address for Auxiliary Device.  
With this IP Address, the Admin Console of Auxiliary Device can be accessed. Any user accessing Web Admin Console of Auxiliary Device will be logged-in with HA Profile and have read-only rights.

Note  
Available only for Primary Device.

Select Ports to be Monitored  
Select the ports to be monitored.  
Both the Devices will monitor their own ports and if any of the monitored port goes down, Device will leave the cluster and failover will occur.

Note  
This feature is not supported in Virtual Security Devices.

Note  
Available only for Primary Device.

3. Click **Enable HA** to enable HA.

Note  
The Device from which HA is enabled, acts as a primary Device while the peer Device acts as auxiliary Device.

Note  
This feature is not supported in Virtual Security Devices.

Note  
Available only for Primary Device.
If everything is cabled and configured properly and HA is enabled successfully:

- Both Devices will have the same configuration except the HA link port IP Address.
- By default, as soon as HA is enabled successfully, both the Devices will synchronize automatically.

**Disable HA**

HA can be disabled from this page.

Go to **System Management > System > System Services > HA** and click **Disable HA**

### 5.3.3 Network

Use **Network** pages to configure Firewall Manager Device to operate in your network.

This section covers the following topics:

- **Interface** - Configure and manage the ports/interfaces of the device.
- **DNS** - Manage DNS servers to be used by the Device, DNS Host Entries and routing of specific requests.
- **WAN Link Manager** - Manage device’s WAN Link.
- **Unicast Route** - Allows to manage unicast routes.

**Interface**

Use **Interface** page to view port wise network (physical interface) and zone details. Alias details is nested and displayed beneath the respective physical interface, if configured.
To manage interfaces, go to **System Management > System Settings > Network > Interface**.

**Add Alias**

Alias allows binding multiple IP addresses onto a single physical interface. It is another name of the interface that will easily distinguish this interface from another.

1. Go to **System Management > System Settings > Network > Interface** and select **Add Alias**.
2. Enter alias details.

**Physical Interface**

Select Physical Interface for which Alias is to be bounded.

**IP Family**

Select IP family to add an alias.

*Available Options*: IPv4 | IPv6

**Alias**

Select type of IP address to be assigned to Alias.

*Available Options*: Single | Range

**IP Address**

Specify IP Address.

**Netmask**

Select the network subnet mask.

![Figure 215: Add Alias](image)

3. Select **Save**.

**Edit Interface**

This page allows you to change IP address and sub netmask of the Interface and gateway (if defined).

1. Go to **System Management > System Settings > Network > Interface** and click on the manage icon under the Manage tab.
2. Enter general settings details.

**Physical Interface**

Physical Interface for example, Port A, Port B and so on. It cannot be modified.
Note
For the following SFM models, port names will be displayed as alphanumeric characters (for example, Port 1, Port 2 and so on) instead of alphabetic characters:

• SFM200
• SFM300
• SFM400

IPv4/Netmask
Specify IP Address and Netmask for the IPv4 Interface.

IPv6/PREFIX
Specify IP Address and Prefix for the IPv6 Interface.

Gateway Name
Specify name of the gateway (It is available only when the gateway is defined on the interface)

IP Address
Specify IP Address of the gateway.

IPv6 Address (Available if IPv6 Configuration is enabled)
Specify IPv6 Address of the gateway.

3. Enter advanced setting details.

Interface Speed
Select Interface speed for synchronization.

Speed mismatch between Firewall Manager and 3rd party routers and switches can result into errors or collisions on interface, no connection, traffic latency or slow performance.

Available Options: Auto Negotiate, 10 Mbps - Full duplex, 10 Mbps - Half duplex, 100 Mbps - Full duplex, 100 Mbps - Half duplex, 1000 Mbps - Full duplex, 1000 Mbps - Half duplex
Default - Auto Negotiate

MTU
Specify MTU value (Maximum Transmission Unit)
MTU is the largest physical packet size, in bytes, that a network can transmit. This parameter becomes an issue when networks are interconnected and the networks have different MTU sizes. Any packets larger than the MTU value are divided (fragmented) into smaller packets before being sent.

Default - 1500
Input range - 576 to 1500

4. Select Save.

DNS
The Domain Name System (DNS) is a system that provides a method for identifying hosts on the Internet using alphanumeric names called fully qualified domain names (FQDNs) instead of using difficult to remember numeric IP addresses. In other words, it translates domain names to IP addresses and vice versa.
DNS server is configured at the time of deployment. You can add additional IP addresses of the DNS servers to which device can connect for name resolution. When multiple DNS are configured, they are queried in the order as they are entered.

To configure DNS, go to **System Management > System Settings > Network > DNS.**

**DNS List IPv4**

Specify the DNS IP Address based on priority in DNS 1, DNS 2 and/or DNS 3.

![DNS List](image)

**Figure 216: DNS List**

**Note**

Do not forget to click **Apply** after adding new IP address to the DNS list.

**WAN Link Manager**

WAN Link routes traffic between the networks. By default, Firewall Manager supports only one WAN Link. You must have configured the IP address for a default WAN Link at the time of deployment. You can change this configuration any time if required.

To configure WAN Link, go to **System Management > System Settings > Network > WAN Link Manager**

**Edit WAN Link**

This page allows you to edit the WAN Link.

1. Go to **System Management > System Settings > Network > WAN Link Manager**
2. Select the Gateway which you want to edit by clicking the Manage icon in the Manage column.
3. Modify the gateway details.

**Name**

Gateway Name

**IPv4 Address**

Specify IP Address

**IPv6 Address**

Specify IPv6 Address

**Interface**

Specify Ethernet Port number that is to act as a Gateway.
4. Select Save.

**Unicast Route**

This page allows you to manage unicast routes. To configure unicast static routes, define the destination IP address and netmask of packets that the device is intended to intercept, and provide a (gateway or next hop) IP address for those packets. The gateway address specifies the next-hop router to which traffic will be routed. Also, provide the interface and the approximate distance for routing.

To manage unicast routes, go to System Management > System Settings > Network > Unicast Route.

**Add Unicast Route**

This page allows you to configure Unicast Route.

1. For IPv4 Unicast Route, navigate to System Management > System Settings > Network > Unicast Route and click Add under IPv4 Unicast Route. For IPv6 Unicast Route, navigate to System Management > System Settings > Network > Unicast Route and click Add under IPv6 Unicast Route.

2. Enter the details.

**Destination IP/Prefix**

Specify Destination IP Address and prefix.

**Gateway**

Specify Gateway IP Address.

**Interface**

Select Interface from the list.

**Distance**

Specify Distance for routing. Range of value is from 0 to 255.
5.3.4 Maintenance

Maintenance facilitates handling the maintenance of the managed devices.

Using the Maintenance menu, you can configure the following operations:

- **Backup & Restore**: Allows you to manually take a backup or schedule a backup of the managed devices.
- **Compatibility Management**: Allows you to get compatibility information or acquire compatibility of upcoming OS versions.
- **Inactive Users Maintenance**: Allows you to get a report on inactive users and also to delete these inactive users.

### Backup & Restore

Backup is the essential part of data protection. Backups are necessary in order to recover data from the loss due to the disk failure, accidental deletion, or file corruption. There are many ways of taking backups and just as many types of media to use as well.

The Backup and Restore menu enables you to back up and restore your Firewall Manager. It is a good idea to back up the Firewall Manager configuration on a regular basis to ensure that, should the system fail, you can quickly get the system back to its original state with minimal effect to the network. It is a good idea to back up the configuration after making any changes to the configuration of the Firewall Manager or settings that affect the managed devices.

Once the backup is taken, you need to upload the file for restoring the backup. Restoring data older than the current data will lead to the loss of current data.

Administrator can schedule Firewall Manager backup or manually take the backup from **System Management > System Settings > Maintenance > Backup & Restore**.

### Backup Restore

To take the backup manually and restore, go to **System Management > System Settings > Maintenance > Backup & Restore** and click **Backup Now** and then select the backup to be restored and click **Upload and Restore**. Alternatively, use the **Browse** button to select the complete path.
Sophos Firewall Manager

Figure 220: Backup Restore

Note
Sophos Firewall Manager Password will not be restored during this process.

Schedule Backup

Backup Frequency
Select backup frequency.
In general, it is best to schedule backup on regular basis. Depending on how much information you add or change will help you determine the schedule.

Available Options: Never - Select this option if you do not want to take backup. Daily - Configure time at which the backup should be taken. Weekly - Configure day and time at which the backup should be taken. Monthly - Configure day and time at which the backup should be taken.

Backup Mode
Select how and to whom backup files should be sent.

Available Options: FTP - If backup is to be stored on FTP server, configure FTP server IP/Domain address, username and password to be used. Mail - If backup is to be mailed, specify Email Address on which backup is to be mailed.

Manage Backup
This section displays the list of last five backups along with the time and size of the backup. It also provides an option to download the backup and restore it.

Firmware

System > Maintenance > Firmware
Firmware
Firmware page displays the list of available firmware versions downloaded. Maximum two firmware versions are available simultaneously and one of the two firmware versions is active.

**Upload firmware**
- Administrator can upload a new firmware. Click to specify the location of the firmware image or browse to locate the file. You can simply upload the image or upload and boot from the image. The uploaded firmware can only be active after the next reboot.

In case of Upload & Boot, firmware image is uploaded and upgraded to the new version, closes all sessions, restarts, and displays the login page. This process may take few minutes since the entire configuration is also migrated in this process.

**Boot from**
- Option to boot from the downloaded image and activate the respective firmware.

**Boot with factory default configuration**
- Device is rebooted and loads default configuration.

**Available Latest Firmware**

**Check For New Firmware**
- Displays if any new firmware is available.

**Firmware Version**
- List of available firmware versions that can be downloaded.

**Type**
- Different types of firmware.
  
  **Available Options:** BetaGA

**Actions**
- **Download** Button to download the firmware. Once the firmware is downloaded, click the **Install** button to install the firmware.

**Note**
- You can find more details in the Compatibility Guide.

**SFOS Hotfix**

**Allow auto-install of important Hot-fixes**
- Hotfixes are applied automatically if available. Disable if you do not want to apply hotfix.
  
  **Default - Enable**
Licensing

This page displays Firewall Manager device’s registration information.

Device Registration Details
Model
Firewall Manager device model number.

Version
Firewall Manager firmware version number.

Company Name
Name of the company under whose name the device is registered.

Contact Person
Name of the contact person from the company.

Registered Email ID
Email address used at the time of device registration.

Module Subscription Details
Enhanced Support
Subscription status and Expiry Date (if the module is subscribed).

Possible status: Subscribed, Unsubscribed, Expired, Evaluating

Enhanced Plus Support
Subscription status and Expiry Date (if the module is subscribed).

Possible status: Subscribed, Unsubscribed, Expired, Evaluating

Manage Subscription Online
Displays alert message if the Firewall Manager device is not registered.

Synchronize Device Licenses
Click to synchronize device licenses with Customer My Account.

Link to Customer My Account to register device or to update and renew subscription modules.

Activate Subscription
Click to avail subscriptions e.g. support using the Subscription Key.

Activate Subscription
This page allows you to enter Subscription Key for SFM.

1. Go to System Management > System Settings > Maintenance > Licensing and click on Activate under Manage Subscription Online section.
2. Enter the Subscription Key and click Verify to verify the key.

5.3.5 Content Distribution

Content Distribution page is used to manage or view the status of various pattern updates for security services. To manage content distribution, go to System Management > System Settings > Content Distribution.

Updates Status
Pattern
Displays the pattern type. Available types are:

- AP Firmware
- ATP
- Authentication Clients
- Avira AV
- IPS
- RED Firmware
- Sophos AV
- SSLVPN Clients
- WAF

Model
Displays the model of the Sophos XG Firewall device for which the pattern is applicable.

Version
Displays version of the pattern.

Update Type
Displays update type for the pattern. Available types are:

- Full Upgrade - Shows that the upgrade is to the latest version of the pattern.
- Upgrade to next version - Shows that the upgrade is to the immediate next version of the pattern.
- Incremental Upgrade from (base version) to (incremental version) - Shows that the upgrade is from a base version to an incremental version of the pattern.

Example: Suppose Version A, Version B, Version C and Version D are various versions of a pattern in sequence, then following is applicable for various Update Types:

- If upgrade is from Version A to Version B then that update is categorized as Upgrade to next version.
- If upgrade is from Version A to Version C then that update is categorized as Incremental Upgrade from Version A to Version C.
- If upgrade is from Version A to Version D then that update is categorized as Full Upgrade.

Last Successful Download
Displays the time of last successful download in HH:MM:SS, Mon DD YYYY format.

Update Pattern Now
Click to update available patterns.

Pattern download/installation

Auto Update
Click to enable automatic updates for patterns.

Interval
Select the frequency of the updates. Available options are:

- Every hour
5.3.6 Diagnostics

This menu allows checking the health of your device in a single shot. Information can be used for troubleshooting and diagnosing problems found in your device.

Tools

This page provides diagnostic tools to test and troubleshoot network issues such as packet loss, connectivity errors or discrepancies in the Firewall Manager network.

Go to System Management > System Settings > Diagnostics > Tools to view the various statistics.

- Ping
- Trace route
- Name lookup
- Route lookup

Ping

Ping is a most common network administration utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer.

Ping sends ICMP echo request/replies to test connectivity to other hosts. Use standard ICMP ping to confirm that the server is responding. Ping confirms that the server can respond to an ICMP ping request.

Use Ping diagnostically to:

- Ensure that a host computer you are trying to reach is actually operating or address is reachable or not
- Check how long it takes to get a response back
- Get the IP address from the domain name
- Check for the packet loss

IP Address/Host Name

IP Address or fully qualified domain name to be pinged.

It determines network connection between Firewall Manager and host on the network. The output shows if the response was received, packets transmitted and received, packet loss if any and the round-trip time. If a host is not responding, ping displays 100% packet loss.

Interface
Interface through which the ICMP echo requests are to be sent.

**Size**

Ping packet size
Range - 1 to 65507

**Trace Route**

Trace Route is a useful tool to determine if a packet or communications stream is being stopped at the Firewall Manager, or is lost on the Internet by tracing the path taken by a packet from the source system to the destination system, over the Internet.

Use traceroute to:
- find any discrepancies in the Firewall Manager network or the ISP network within milliseconds
- trace the path taken by a packet from the source system to the destination system, over the Internet

**IP Address/Host Name**

IP Address or fully qualified domain name.

It determines network connection between Firewall Manager and host on the network.
The output shows all the routers through which data packets pass on way to the destination system from the source system, maximum hops and Total time taken by the packet to return measured in milliseconds.

**Interface**

Interface through which the requests are to be sent.

**Name Lookup**

Name lookup is used to query the Domain Name Service for information about domain names and IP addresses. It sends a domain name query packet to a configured domain name system (DNS) server. If you enter a domain name, you get back the IP address to which it corresponds, and if you enter an IP address, then you get back the domain name to which it corresponds. In other words, it reaches out over the Internet to do a DNS lookup from an authorized name server, and displays the information in the user understandable format.

**IP Address/Host Name**

IP address or fully qualified domain name that needs to be resolved.

**DNS Server IP**

DNS server to which the query is to be sent.

**Route Lookup**

If you have routable networks and wish to search through which Interface Firewall Manager routes the traffic then lookup the route for the IP address.

**IP Address**

IP address that needs to be resolved.

**Troubleshoot Report**

To help Support team to debug the system problems, troubleshooting report can be generated which consists of the system’s current status file and log files. File contains details like list of all the processes currently running on system, resource usage etc. in the encrypted form.

Customer has to generate and mail the saved file at support@sophos.com for diagnosing and troubleshooting the issue. File will be generated with the name: _TSR_<APPKEY>_<MM_DD_YY>
Where, APPKEY is the device key of the device for which the report is generated and MM_DD_YY is the date (month date year) on which the report is generated.

Go to **System Management > System Settings > Diagnostics > Troubleshoot Report** to generate Consolidated Troubleshooting Report (TSR).

Enter Consolidating Troubleshooting Report details:

**Generate Troubleshoot Report for**
- Select components for which troubleshoot report has to be generated.

**Available Options:** System SnapshotLog Files

**Reason**
- Specify reason to generate troubleshoot report.

**Generate Button**
- Click to generate troubleshoot report.

**System Graph**

Use System Graph page to view CPU and Memory usage of Firewall Manager device for last two hours. The usage is displayed in the form of graphs.

Go to **System Management > System Settings > Diagnostics > System Graph** to view the CPU and memory usage.
6 Appendix A - Guides

To complement the Online help, following documents are also available:

- Getting Started Guide
- You can find the Release Notes on our Up2Date Blog.
Copyright notice

Copyright 2016–2017 Sophos Limited. All rights reserved.

Sophos is a registered trademark of Sophos Limited and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.